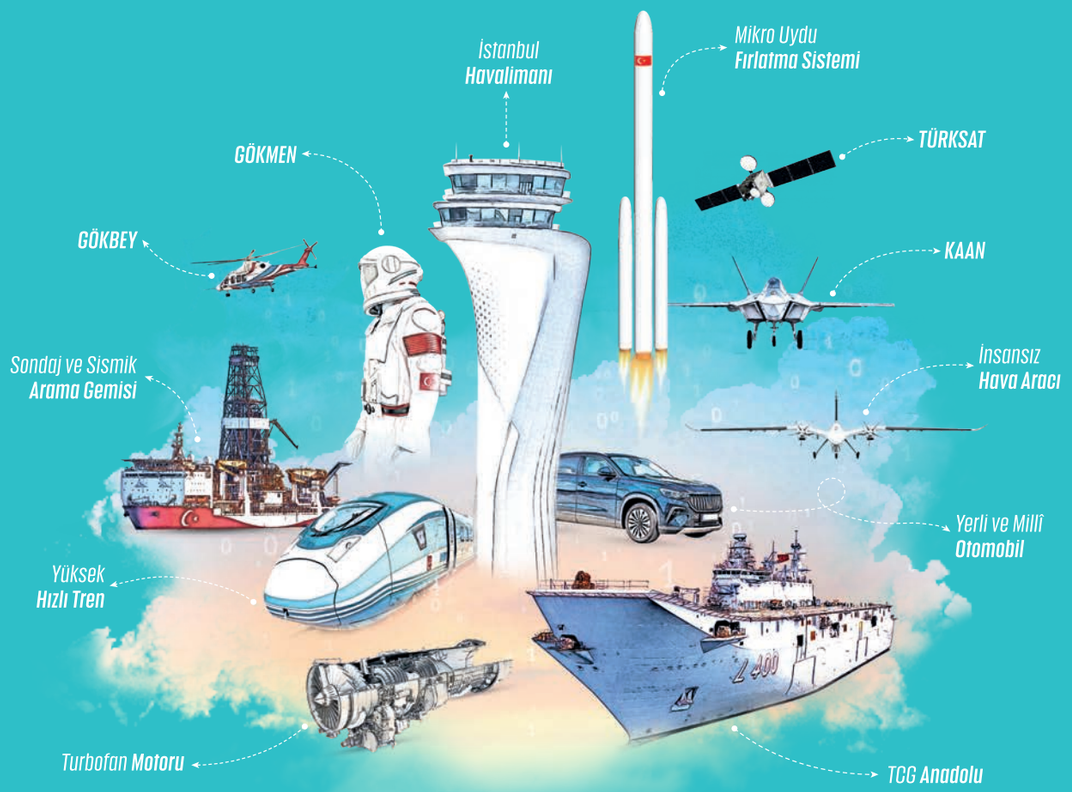
Bu kitaba sığmayan daha neler var!

eba
www.eba.gov.tr

Karekodu okut, bu kitapla ilgili EBA içeriklerine ulaş!

Teknoloji Yolculuğumuz



ISBN: 978-975-11-8862-5

MESLEKİ VE TEKNİK ANADOLU LİSESİ | **GAZETECİLİK** (PROTOKOL) ALANI

GAZETECİLİK (PROTOKOL) ALANI **MEDYADA SİBER GÜVENLİK** **10** DERS MATERYALİ

MEDYADA SİBER GÜVENLİK

10 DERS MATERYALİ

MESLEKİ VE TEKNİK ANADOLU LİSESİ

GAZETECİLİK (PROTOKOL) ALANI

MEDYADA SİBER GÜVENLİK

10

DERS MATERYALİ

Yazarlar
ENGİN KILIÇ
MURAT KARATAŞ

MİLLÎ EĞİTİM BAKANLIĞI YAYINLARI .....: 9909
YARDIMCI VE KAYNAK KİTAPLAR DİZİSİ .....: 3361

HAZIRLAYANLAR

Dil Uzmanı	Merve SERBEST ERTOĞAN
Program Geliştirme Uzmanı	Seçkin Seçil BAŞARAN
Rehberlik Uzmanı	Fatih DÜĞENCİ
Ölçme ve Değerlendirme Uzmanı	Filiz İSNAÇ
Görsel Tasarım Uzmanı	Tümay ALDEMİR

ISBN: 978-975-11-8862-5

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 Hak'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

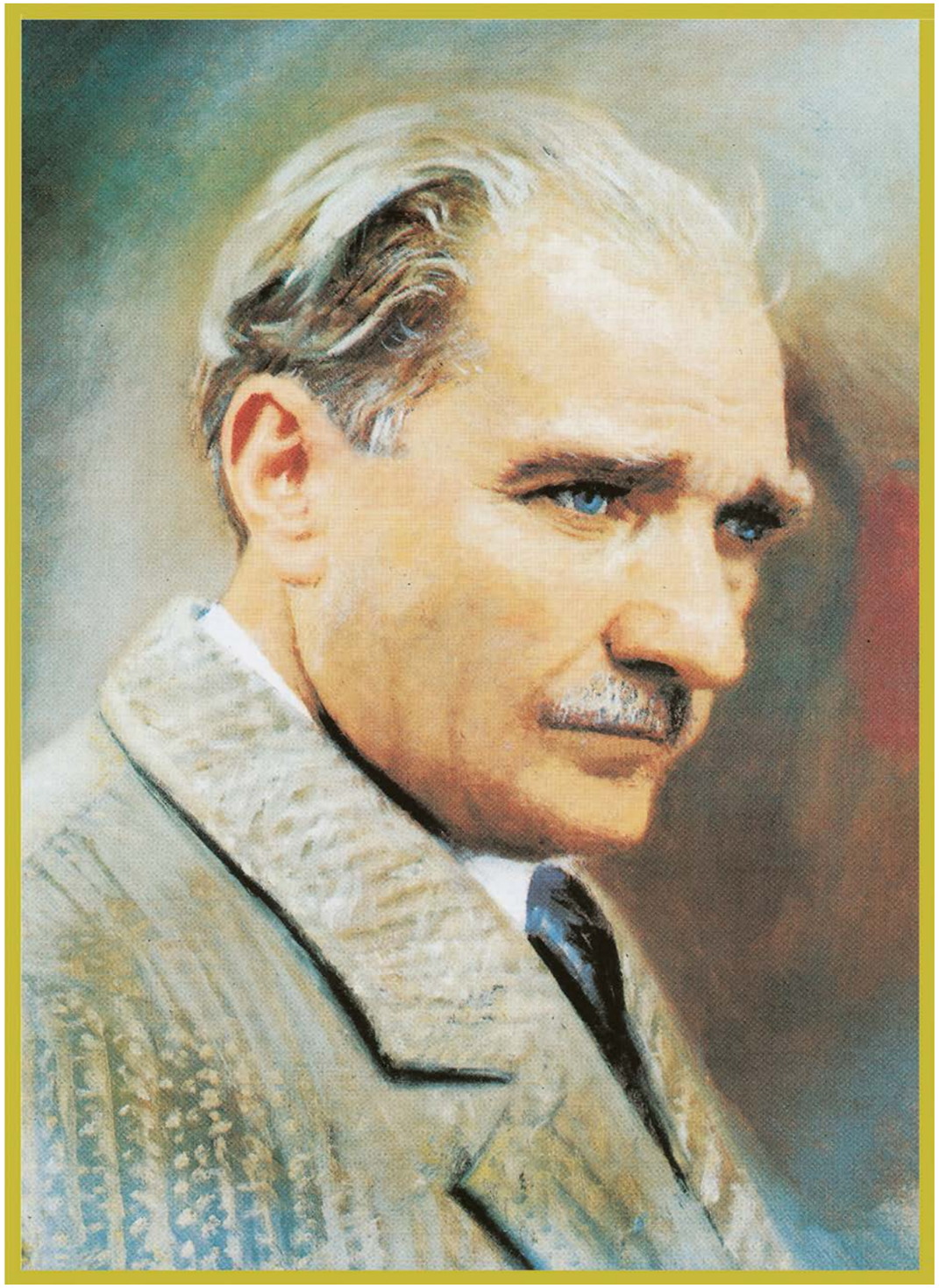
GENÇLİĞE HİTABE

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 biriminin numarasını gösterir.

Karekod okuyucu ile taratılarak resim, video, soru çözümleri vb. ilave kaynaklara ulaşılabilecek karekod bölümünü gösterir.

Öğrenme biriminde yer alan konuları gösterir.

Öğrenme biriminde neler öğreneceğinizi gösterir.

Öğrenme biriminde yer alan anahtar kavramları gösterir.

Derse başlamadan önce yapılacak hazırlıkları gösterir.

Öğrenme biriminin adını gösterir.

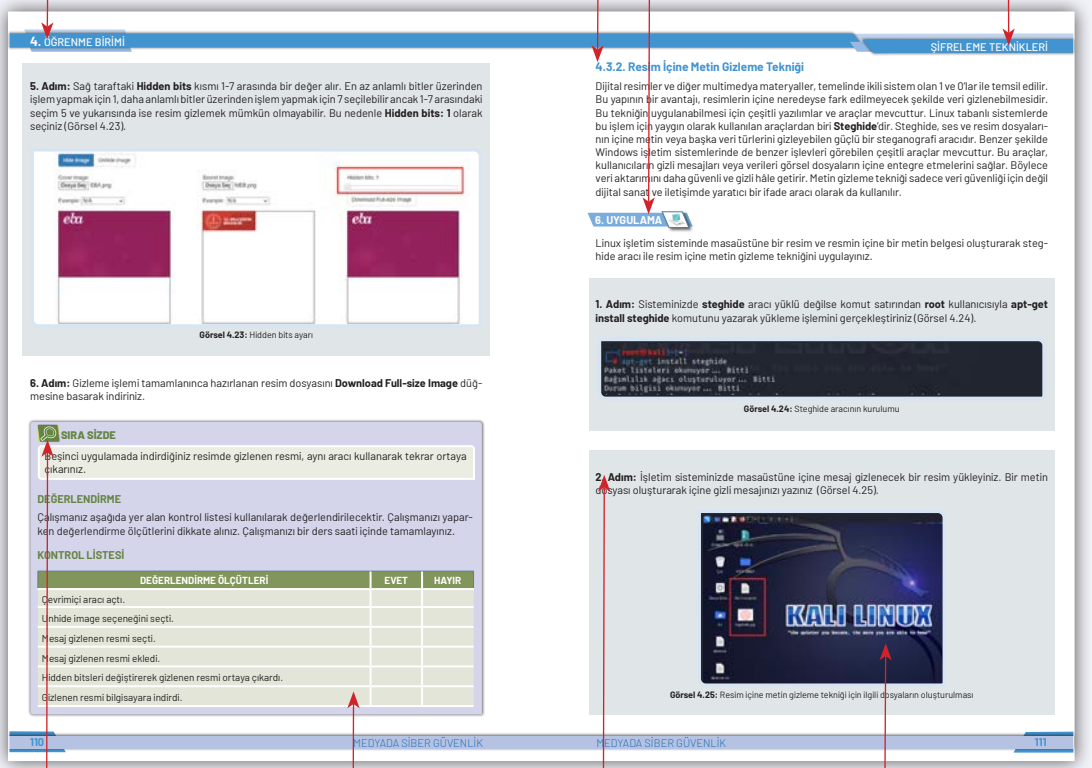
DERS MATERYALİNİN TANITIMI

Öğrenme biriminin adını gösterir.

Öğrenme birimindeki alt konu başlıklarını gösterir.

Öğrenme birimindeki uygulamaları gösterir.

Öğrenme biriminin numarasını gösterir.



4. ÖĞRENME BİRİMİ

ŞİFRELEME TEKNİKLERİ

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 gizlemek mümkün olmayabilir. Bu nedenle **Hidden bits: 1** olarak seçiniz (Görsel 4.23).

Görsel 4.23: Hidden bits ayarı

6. Adım: Gizleme işlemi tamamlanınca hazırlanan resim dosyasını **Download Full-size Image** düğmesine basarak indiriniz.

SIRA SİZDE

Beşinci uygulamada indirdiğiniz resimde gizlenen resmi, aynı aracı kullanarak tekrar ortaya çıkarınız.

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız. Çalışmanızı bir ders saati içinde tamamlayınız.

KONTROL LİSTESİ

DEĞERLENDİRME ÖLÇÜTLERİ	EVET	HAYIR
Çevrimiçi aracı açtı.		
Unhide image seçeneğini seçti.		
Mesaj gizlenen resmi seçti.		
Mesaj gizlenen resmi ekledi.		
Hidden bitsleri değiştirerek gizlenen resmi ortaya çıkardı.		
Gizlenen resmi bilgisayara indirdi.		

110 MEDYADA SİBER GÜVENLİK

4.3.2. Resim İçine Metin Gizleme Tekniği

Dijital resimler ve diğer multimedya materyaller, temelinde ikili sistem olan 1 ve 0'lar ile temsil edilir. Bu yapının bir avantajı, resimlerin içine neredeyse fark edilmeyecek şekilde veri gizlenebilmesidir. Bu tekniğin uygulanabilmesi için çeşitli yazılımlar ve araçlar mevcuttur. Linux tabanlı sistemlerde bu işlem için yaygın olarak kullanılan araçlardan biri **Steghide**'dir. Steghide, ses ve resim dosyalarının içine metin veya başka veri türlerini gizleyebilen güçlü bir steganografi aracıdır. Benzer şekilde Windows işletim sistemlerinde de benzer işlevleri görebilen çeşitli araçlar mevcuttur. Bu araçlar, kullanıcıların gizli mesajları veya verileri görsel dosyaların içine entegre etmelerini sağlar. Böylece veri aktarımını daha güvenli ve gizli hâle getirir. Metin gizleme tekniği sadece veri güvenliği için değil dijital sanat ve iletişimde yaratıcı bir ifade aracı olarak da kullanılır.

6. UYGULAMA

Linux işletim sisteminde masaüstüne bir resim ve resmin içine bir metin belgesi oluşturarak steghide aracı ile resim içine metin gizleme tekniğini uygulayınız.

1. Adım: Sisteminizde **steghide** aracı yüklü değilse komut satırından **root** kullanıcısıyla **apt-get install steghide** komutunu yazarak yükleme işlemini gerçekleştiriniz (Görsel 4.24).

Görsel 4.24: Steghide aracının kurulumu

2. Adım: İşletim sisteminizde masaüstüne içine mesaj gizlenecek bir resim yükleyiniz. Bir metin dosyası oluşturarak içine gizli mesajınızı yazınız (Görsel 4.25).

Görsel 4.25: Resim içine metin gizleme tekniği için ilgili dosyaların oluşturulması

MEDYADA SİBER GÜVENLİK 111

Öğrenme birimindeki sıra sizde çalışmalarını (bölümünü) gösterir.

Sıra Sizde çalışmasının değerlendirme ölçütlerini gösterir.

Uygulamada yapılacak adımları gösterir.

Öğrenme birimi ile ilgili görselleri gösterir.

1. ÖĞRENME BİRİMİ

SİBER GÜVENLİĞE GİRİŞ

KONULAR

1.1. HACKER VE HACKİNG KAVRAMLARI
1.2. ETİK VE GÜVENLİK
1.3. AĞ GÜVENLİĞİ TEMELLERİ

NELER ÖĞRENECEKSİNİZ?

- Hacker kavramı ve hacker türleri
- Hacking teknikleri
- Bilişimde etik ve siber güvenlik
- Bilgi gizliliği
- Bilgi güvenliği ve yasal problemler
- Bilişimde güncel tehditler ve saldırılar
- Ağ güvenliğinin önemi ve etkileri
- Ağ saldırıları

ANAHTAR KAVRAMLAR

Adli bilişim, beyaz şapka, bilişim etiği, gri şapka, hacker, hacking, malware, siber güvenlik, siber saldırı, siber tehdit, siyah şapka, virüs

HAZIRLIK ÇALIŞMALARI

1. Medya sektörünü hedef alan siber saldırılar neler olabilir? Düşüncelerinizi arkadaşlarınızla paylaşınız.

2. Medya sektörüne yönelik gerçekleştirilen siber saldırılar ne tür sorunlara yol açabilir? Düşüncelerinizi arkadaşlarınızla tartışınız.

3. Kişisel verilerin izinsiz kullanılmasının ortaya çıkaracağı sorunlar nelerdir? Düşüncelerinizi arkadaşlarınızla paylaşınız.

1.1. HACKER VE HACKİNG KAVRAMLARI

İnsanoğlunun var olduğundan beri en temel ihtiyaçlarından biri güvenliktir. Teknolojinin gelişmesi ve bilginin dijitalleşmesiyle birlikte güvenliğin fiziksel ihtiyaç olmasının yanı sıra sanal ihtiyaç hâline geldiği görülür.

1.1.1. Hacker

Kişisel verilerin çok hızlı bir şekilde dijitalleşmesiyle güvenlik açısından bazı kavramlar ortaya çıkmıştır. Bu kavramların başında **hacking** ve **hacker** yer alır. **Hackleme** anlamına gelen **hacking**; bilgisayarlara, taşınabilir cihazlara ve ağ cihazlarına izinsiz şekilde zararlı yazılımlar yükleyerek bu cihazlardaki verilere yetkisiz erişim sağlanması anlamına gelir.

Türk Dil Kurumu Güncel Türkçe Sözlük'e göre hacker, **bilgisayar korsanı** anlamına gelir. Bilgisayar korsanları (hackerlar), yetkisi olmadığı hâlde bilişim cihazlarına erişim sağlamaya çalışarak, bu cihazların doğru bir şekilde çalışmasını engelleyen veya bu cihazlar üzerindeki verilere erişerek bu verileri amacı dışında kullanan kişilerdir (Görsel 1.1). Bununla birlikte bazı bilgisayar korsanları, bilişim sistemlerinin açıklarını tespit ederek bu açıkların giderilmesi için çalışmalar yapabilir.

Görsel 1.1: Bilgisayar korsanı

Gerekli teknik bilgi ve beceriye sahip hackerlar; bilişim sistemleri, bilgisayar ağları, yazılım, nesnelerin interneti (IoT) üzerine uzmanlaşmış kişilerdir. Bilgisayar korsanları, bilgi ve becerilerini bilişim sistemlerinin açıklarını tespit ederek zarar vermek veya yetkisiz erişim sağlamak için kullanabilecekleri gibi bu güvenlik açıklarını ortadan kaldırmak için de kullanabilir. Aynı zamanda hackerlar, kötü amaçlı veri erişimi sağlayabilmek için sosyal mühendislik yoluyla normal bir şekilde iletişime geçtiği kullanıcıyı kandırarak kullanıcının verilerini rahatlıkla elde edebilirler. Bu yöntem, sistem hackleme yönteminden çok daha basittir.

ARAŞTIRMA

Ülkemizde bilgisayar korsanlarını engellemek amacıyla yapılan siber güvenlik faaliyetlerini araştırınız. Araştırma sonucunu arkadaşlarınızla paylaşınız.

1.1.2. Hacker Türleri

Hackerlar; niteliklerine ve amaçlarına göre siyah şapkalı, beyaz şapkalı ve gri şapkalı olmak üzere üç gruba ayrılır.

1.1.2.1. Siyah Şapkalı Hackerlar

Bilişim sistemlerine zarar veren, maddi kazanç sağlamak amacıyla verileri ele geçiren, ele geçirdiği verilere şifreleme yaparak erişimi engelleyen veya eriştiği verileri tamamen ortadan kaldıran, kötü niyetli bilgisayar korsanlarıdır.

1.1.2.2. Beyaz Şapkalı Hackerlar

Bilişim sistemlerinin güvenlik açıklarını tespit etmek amacıyla yazılımlar üreten ve tespit ettiği güvenlik açıklarını ilgili kurumlarla paylaşarak güvenlik açıklarının giderilmesini sağlayan bilgisayar korsanlarıdır. Kurumların zarar görmesinin önüne geçtikleri ve gerekli tedbirlerin alınmasını sağladıkları için maddi kazanç elde edebilirler. Bu tür bilgisayar korsanlarına **etik hackerlar** da denir.

1.1.2.3. Gri Şapkalı Hackerlar

Bilişim sistemlerine yasa dışı yollardan sızmaya çalışan, sızma sonrasında bulduğu açıkları raporlayarak güvenlik açıklarının kapatılmasını sağlayan bilgisayar korsanlarıdır. Gri şapkalı hackerlar bazen siyah şapkalı hackerlar gibi davranarak yasa dışı yollardan maddi kazanç elde etmeye çalışabilirler.

SIRA SİZDE

Tablo 1.1'de verilen hacker türlerinin karşısına ilk satırdaki gibi bir örnek olay yazınız. Yazdığınız örnek olayları arkadaşlarınızla paylaşınız.

Tablo 1.1: Hacker Türlerine Göre Örnek Olaylar

HACKER TÜRÜ	ÖRNEK OLAY
Siyah Şapkalı Hacker	Bilgisayar korsanı, bir firmanın ticari verilerine izinsiz şekilde ulaşarak verileri güçlü bir şifreleme yöntemiyle şifrelemiştir ve ardından firmaya ulaşarak ücret karşılığında şifreyi onlarla paylaşacağını belirtmiştir.
Siyah Şapkalı Hacker	
Beyaz Şapkalı Hacker	
Gri Şapkalı Hacker	

1.1.3. Hacking Teknikleri

Bilgisayar korsanlarının kullandığı çeşitli hacking teknikleri vardır. Arka kapı (backdoor) ve kötü amaçlı yazılım teknikleri en çok kullanılanlardandır.

1.1.3.1. Arka Kapı Tekniği

Arka kapı, bir yazılıma veya bilişim sistemine erişim sağlanabilmesi için bilinçli veya bilinçsiz şekilde bırakılmış açıktır. Arka kapılar, bilgisayar korsanlarının kimlik doğrulaması yapmadan sisteme erişmelerine izin verir. Birçok zararlı yazılım, bir sisteme bulaştığında arka kapı oluşturmaya çalışır. Bu arka kapılar sayesinde bilgisayar korsanları, sisteme daha kolay erişim sağlayabilir. Arka kapılar bazen geliştiriciler tarafından sistemi test etmek amacıyla oluşturulur. Oluşturulan arka kapılar kapatılmadığı takdirde kötü niyetli bilgisayar korsanları tarafından kullanılabilir. Arka kapı, geliştirici tarafından oluşturulmuşsa bunu oluşturan kod satırları değiştirilmeli veya silinmelidir.

Bilişim sistemlerinde arka kapı olup olmadığını tespit edebilmek için yapılması gerekenler şunlardır:

- Ağ trafiğini kontrol ederek varsa anormallikleri saptamak.
- Şüpheli çalışan programları tespit etmek.
- Virüs programlarıyla sistemi kontrol etmek.
- Firewall (güvenlik duvarı) kullanmak.

1.1.3.2. Kötü Amaçlı Yazılım

Kötü amaçlı yazılım (malware); bir bilgisayara veya ağ sistemine zarar vermek, kişisel ve gizli bilgileri ele geçirmek, sistemin işleyişini engellemek veya yavaşlatmak, ele geçirilen verileri silmek veya şifrelemek amacıyla oluşturulmuş yazılımlardır (Görsel 1.2).

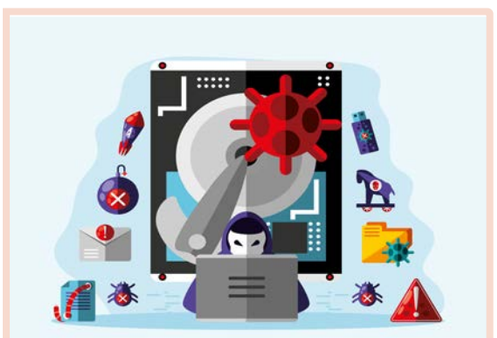
Görsel 1.2: Kötü amaçlı yazılım

Kötü amaçlı yazılımlar genellikle son kullanıcı bilgisayarlarına veya mobil cihazlarına bulaştırılmak amacıyla geliştirilir. Kötü amaçlı yazılımlar şu yollarla cihazlara bulaşabilir:

- Güvenilir olmayan web sayfalarını ziyaret etmek.
- Güvenilir olmayan web sayfalarından indirme işlemi yapmak.
- Güvenilir olmayan e-posta eklerini açmak ve ekleri cihaza indirmek.
- Lisanslı olmayan programları veya mobil uygulamaları yüklemek.
- Güvenilir olmayan web sayfalarından program güncellemeleri almak.
- Güvenilir olmayan FTP (dosya aktarım protokolü) sunucularından veri indirmek.
- Güvenilir olmayan taşınabilir cihazlardan veri transferi yapmak.

1.1.3.3. Kötü Amaçlı Yazılım Türleri

Bilgisayarlar ve bilgisayar ağ sistemleri üzerinden haberleşme yaygınlaştıkça kötü amaçlı oluşturulan yazılımların da arttığı görülür. Bunlar genellikle virüsler, solucanlar, Truva atları, casus yazılımlar, fidye yazılımları, reklam yazılımları, tuş tutucular (keyloggerlar), korku yazılımları ve kök kullanıcı takımı yazılımlarıdır (Görsel 1.3).



Görsel 1.3: Kötü amaçlı yazılım türleri

Virüs (Virus): Bilgisayarın veya taşınabilir cihazın işletim sistemine olumsuz etki eden, sisteme kötü amaçlı yazılım yükleyebilen zararlı yazılım türüdür. Virüsler kendi kendine çoğalabilir. Taşınabilir bellekler, e-posta ekleri, güvenilir olmayan web sayfası indirmeleri vasıtasıyla kolaylıkla sisteme bulaşabilir. Virüslerin enfekte olduktan sonra sisteme verebileceği zararlar çeşitlilik gösterir. Virüsler, sistemdeki dosya ve klasörlere zarar verebildiği gibi verilerin kötü amaçlı sızdırılmasına da neden olabilir. Sistemi virüslerden korumak amacıyla lisanslı virüs programları geliştirilir.

SIRA SİZDE

Dünya genelinde yayılan ve bilgisayar sistemlerine büyük zarar veren virüslerin etkilerine dair bir sunu hazırlayınız. Hazırladığınız sunuyu arkadaşlarınızla paylaşınız.

Solucan (Worm): Ağ üzerinden kendini kopyalayarak çoğalabilen, kendi kendine yayılabilen kötü amaçlı yazılımlardır. Genellikle bilgisayar ağlarında bulunan güvenlik açıklarından faydalanırlar. Bir bilgisayara girdiğinde ağ üzerinden diğer bilgisayarlara da sızabilirler. Ağ bant genişliğini kullanarak ağda büyük bir trafik oluşturur ve iletişimin yavaşlamasına neden olurlar. Kullanıcıya ait kişisel verilerin çalınmasına neden olabilirler.

Truva Atı (Trojan): Zararsız bir uygulama gibi davranarak kendini bilgisayara indirip kullanmaları için son kullanıcıları kandırır. Kullanıcılar bu yazılımı bir defa çalıştırdıktan sonra oluşturulma amaçlarına göre kişisel verileri çalabilir, işletim sistemine zarar verebilir, yeni zararlı yazılımlar indirebilir, bilgisayarda bulunan dosya ve klasörleri silebilir veya kopyalayabilir.

Casus Yazılımı (Spyware): Sisteme sızdıktan sonra gizli kalarak sistem ve kullanıcı hakkında sürekli bilgi toplar. Kimlik bilgileri, kullanıcı bilgileri, kredi kartı bilgileri gibi önemli verileri toplayarak bilgisayar korsanlarına iletir.

Fidye Yazılımı (Ransomware): Yasa dışı para kazanmak amacıyla bilgisayar korsanları tarafından üretilmiş yazılımlardır. Genellikle kullanıcılara e-posta eki olarak gönderilen bu yazılım türü, bilgisayara yüklendiği takdirde kullanıcının önemli verilerini şifreler. Şifreleme işlemi sonrası bilgisayar korsanları, kullanıcıyla iletişime geçerek şifreyi çözme veya verme karşılığında fidye talep ederler. Bilgisayar korsanları, kurbandan fidyeyi genellikle kripto para olarak isterler.

Reklam Yazılımı (Adware): Kullanıcıya sürekli reklam göndermek amacıyla oluşturulur. Bu tür yazılımlar genellikle son kullanıcıların bilgisayara indirdiği ücretsiz programlarla birlikte yüklenir. Kullanıcı, yazılımın gönderdiği reklamı açtığında bilgisayar korsanları kazanç elde eder.

Tuş Tutucu (Keylogger): Kullanıcının klavyeden bastığı her tuşu kaydederek bilgisayar korsanına gönderebilir. Özellikle kişisel bilgiler, kullanıcı bilgileri, kredi kartı bilgileri gibi veriler bu yazılım sayesinde saldırgana ulaşabilir.

Korku Yazılımı (Scareware): Saldırganlar bu tür yazılımlar sayesinde kullanıcıları korkutarak sahte yazılım almalarına neden olabilir. Genellikle kurban, güvenilir olmayan bir web sitesini açtığında bilgisayarına **Uyarı: Virüs Tehdidi** gibi sahte mesajlar gönderilir. Bu durum, kurbanların korkmasına ve saldırganın yönlendirdiği sahte yazılımları almasına neden olur.

Kök Kullanıcı Takımı (Rootkit): Saldırganlar bu yazılım sayesinde sisteme ayrıcalıklı kullanıcı yetkileriyle erişim sağlar. İşletim sistemlerinin çekirdeğine yerleştiği için kök kullanıcı takımının tespit edilmesi çok zordur.

SIRA SİZDE

Tablo 1.2'de verilen örnek olayların karşısına ilk satırdaki gibi kötü amaçlı bir yazılım türü yazınız. Yazdığınız kötü amaçlı yazılım türlerini arkadaşlarınızla paylaşınız.

Tablo 1.2: Kötü Amaçlı Yazılım Türlerine Göre Örnek Olaylar

ÖRNEK OLAY	KÖTÜ AMAÇLI YAZILIM TÜRÜ
Bir şehir hastanesi, çalışanlarının e-posta hesaplarına gelen bir e-posta aracılığıyla saldırıya uğrar. Saldırganlar, hastanenin kritik verilerini şifreleyerek dosyaları açmanın karşılığında yüksek bir fidye talep ederler. Hastane, acil durumlarda hasta bakımını sürdürebilmek için fidyeyi ödemek zorunda kalır.	**Ransomware**
Bir kullanıcı sahte bir yazılım güncellemesi indirdiğinde kötü amaçlı yazılım, kullanıcının sistemine gizli bir şekilde bulaşır. Kötü amaçlı yazılım, vakti geldiğinde ortaya çıkarak kullanıcının kişisel bilgilerini çalmaya başlar ve elde ettiği verileri, kullanıcı farkında olmadan bir hacker'a gönderir. Sonuç olarak kullanıcının banka hesapları tehlikeye girer.	
Bir kullanıcı, güvenilir olmayan bir web sitesine şifresini kaydederek girmeye çalışırken arka planda çalışan bir kötü amaçlı yazılım, kullanıcının klavye giriş bilgilerini kaydeder. Hacker, bu bilgileri kullanarak kullanıcının e-posta hesabına ve diğer kişisel hesaplarına erişim sağlar.	
Bir yazılım geliştirme şirketi, çalışanı tarafından yerleştirilen bir açıklık nedeniyle siber saldırıya uğrar. Bu açık sebebiyle sistem yöneticileri, farkında olmadan sistemin kontrolünü kaybeder. Saldırgan, şirketin hassas projelerini çalmak için bu erişimi kullanır.	

1.1.3.4. Medya Sektörüne Yönelik Bilinen Kötü Amaçlı Yazılım Saldırıları

Medya şirketleri için siber güvenliğin her geçen gün daha önemli bir konu hâline geldiği görülür. Dijitalleşen medya sektörü, geçmişe kıyasla saldırılara daha açık hâldedir. Medya sektörünün ürettiği tüm ürünler dijitalleştiği için ürünlerin bilgisayar korsanları tarafından çalınma riski vardır. Hizmetleri yavaşlatabilecek veya hizmetlerin durmasına neden olabilecek dağıtılmış bir hizmet reddi saldırısı [Distributed Denial of Service (DDoS)] tehdidi, medya şirketlerinin karşılaştığı güvenlik sorunlarının başında gelir. SQL enjeksiyonları, içerik korsanlığı, alan adı sistemi [Domain Name System (DNS)] saldırıları gibi saldırılar medya endüstrisine yönelik tehditler arasındadır. Sistemlerin ihlal edilmesi ve müşteri ağlarına sızma potansiyeli de söz konusudur. Bilgisayar korsanları; saldırgan ve tehdit edici içerik kullanma, taklit biletler, kullanıcı hesaplarına erişim, kimliğe bürünme, veri ihlalleri dâhil olmak üzere farklı yollarla medya kuruluşlarına yönelik saldırılar gerçekleştirir. Medya sektörüne yönelik kötü amaçlı yazılım saldırılarına örnek olarak bilgisayar korsanlarının 2017 yılında bir dijital içerik üretici platformun sunucularına sızmaları, bir dizinin henüz yayınlanmamış bölümlerini almaları ve karşılığında fidye talep etmeleri gösterilebilir.

ARAŞTIRMA

Dünya üzerinde medya sektörüne yönelik yapılmış saldırıları araştırınız. Araştırma sonucunu arkadaşlarınızla paylaşınız.

1.2. ETİK VE GÜVENLİK

Bilişim sistemleri, ağ sistemleri ve taşınabilir haberleşme cihazlarının kullanımının yaygınlaşması; kişisel ve ticari verilerin haberleşme ortamında bulunan cihazlarda tutulması; hacker, hackleme gibi kavramların ortaya çıkmasıyla birlikte bilişimde etik ve siber güvenlik olgularının önemli hâle geldiği görülür.

1.2.1. Etik

Etik, ahlaki davranışların temelindeki değerleri sorgulayan bir felsefe disiplinidir. Ahlaki değerler olan iyi ve kötünün ne olduğunu sorgulayarak insan davranışlarının ilke ve kurallarını inceleyen etik, evrensel değerlere ulaşmaya çalışır. Etik genel anlamda ahlak üzerine düşünme olarak tanımlansa da farklı uygulama alanlarına etkisinden söz edilebilir.

1.2.1.1. Bilişim Etiği

Bilişim teknolojilerinin hızla gelişmesi, kişileri ve toplumları davranışsal açıdan etkilemiştir. Bu etkilerin ahlaki sorumlulukları artırması, **bilişim etiği** kavramının ortaya çıkmasına neden olmuştur (Görsel 1.4).

Görsel 1.4: Bilişim etiği

İnternet kullanımının yaygınlaşması, sosyal medya platformları üzerinden yapılan bilgi dezenformasyonları, kişisel veya ticari verilerin yasa dışı yollardan elde edilmesi ve kullanılması, siber zorbalık gibi durumlar bilişim teknolojilerinde etik kavramının önemini ortaya çıkarır. Bilişim etiği, güvenilir ve doğru bilgiye ulaşmanın önemini vurgular. 1980'li yılların sonlarında ABD'de kurulan Bilgisayar Etik Enstitüsü [Computer Ethics Institute (CEI)], bilgisayar kullanımına ait etik ilkelerin temelini oluşturan on temel maddeyi şöyle sıralar:

- Bilgisayar, başkalarına zarar vermek için kullanılmamalıdır.
- Bir başkasının bilgisayar üzerinde yaptığı çalışmalar izinsiz incelenmemelidir.
- Bir başkasının bilgisayarındaki dosya ve klasörler izinsiz incelenmemelidir.
- Bilgisayar, hırsızlık amaçlı kullanılmamalıdır.

- Bilgisayar, doğru olmayan bilgiyi yaymak için kullanılmamalıdır.
- Lisanslı yazılımlar, ödeme yapmadan kullanılmamalıdır.
- Bir başkasının bilgisayar kaynakları, izin almadan veya ödeme yapmadan kullanılmamalıdır.
- Bir başkasının fikrî mülkiyetleri sahiplenilmemelidir.
- Yazılımcı veya tasarımcı, ortaya çıkardığı ürünün toplum üzerinde oluşturabileceği sosyal etkilerini dikkate almalıdır.
- Kullanıcı, bilgisayarı diğer insanları dikkate alarak ve saygı göstererek kullanmalıdır.

1.2.1.2. Etik Hacking

Bilgi güvenliği uzmanları tarafından bir sistemde veya bilgisayar ağındaki olası veri ihlallerini ve tehditleri tespit etmek için sistem güvenliğinin bilinçli olarak aşılmasına **etik hacking** denir. Bilgi güvenliği uzmanları, bir kurumda bilgi güvenliğini sağlamakla sorumlu kişilerdir (Görsel 1.5). Bilgi güvenliği uzmanlarının amacı, çalıştığı kurumu ve paydaşlarını olası ağ saldırılarından ve doğabilecek zararlardan korumaktır.

Görsel 1.5: Bilgi güvenliği uzmanı

Etik hackleme, bir plan dâhilinde yapılır ve işlem sonrasında sisteme kötü niyetli kişiler tarafından yapılabilecek saldırıları engellemeye yönelik gerekli önlemler alınır. Bilgi güvenliği uzmanlarının en çok üzerinde durduğu ve tespit etmeye çalıştığı sistem açıkları şu şekilde sıralanır:

- Sistem güvenlik ayarlarındaki değişiklikler
- SQL enjeksiyon saldırıları
- Kimlik doğrulama protokolünün ihlalleri
- Ağda kullanılan erişim noktalarında oluşabilecek açıklar
- Önemli verilerin açığa çıkma olasılıkları

Bilgi güvenliği uzmanları, sistemin özelliklerinden kaynaklı oluşabilecek diğer özel durumları da tespit ederek sorunları giderirler.

1.2.1.3. Bilgi Güvenliği Uzmanlarının Ahlaki Sorumlulukları

Bilgi güvenliği uzmanlarının hackleme işlemi yaptığı ticari kuruluş ve paydaşlarına karşı yasal ve ahlaki sorumlulukları bulunur. Bu sorumluluklardan bazıları şunlardır:

- Hackleme işlemine başlamadan önce kuruma ve paydaşlarına haber vermek.
- Tespit edilen bütün ihlalleri ve açıkları bildirmek.
- Elde edilen bilgileri gizli tutmak ve sadece ilgililer ile paylaşmak.
- Dürüstlük, doğruluk, tarafsızlık gibi etik ilkelere uymak.
- Hak ihlallerinden kaçınmak.
- Kişisel menfaat sağlamaktan kaçınmak.

1.2.1.4. Medya Etiği ve Siber Güvenlik Arasındaki İlişki

Bilgi ve iletişim teknolojilerindeki gelişmelerle birlikte internet ortamından yapılan bilgi manipülasyonlarına karşı siber güvenliğin önemli bir kavram hâline geldiği görülür. Bilgiye ulaşmanın son derece kolay olduğu günümüzde yazılı, görsel ve sosyal medya üzerinden sunulan yanıltıcı bilgilerin önüne geçebilmek için haber kaynaklarından elde edilen verilerin öncelikle uzmanlar tarafından süzgeçten geçirilmesi gereklidir. Bilgi, doğruluğu kanıtlandıktan sonra medya araçlarında yayınlanmalıdır. Bu yüzden medya kuruluşlarının hem bilginin güvenirliğinin tespiti hem de var olan ticari verilerinin korunması amacıyla bilgi güvenliği uzmanlarına ihtiyaçları bulunur.

ARAŞTIRMA

Yaygın medya kuruluşları tarafından yapılan kaynağı belirsiz, doğruluğu kanıtlanmamış haberleri araştırınız. Araştırma sonucunu arkadaşlarınızla paylaşınız.

1.2.2. Siber Güvenlik

Siber güvenlik; bilgisayarları, bilgisayar ağlarını, taşınabilir cihazları, IoT cihazlarını ve bu cihazlardaki verileri saldırılardan korumak için yapılan iş ve işlemler bütünüdür (Görsel 1.6).

Görsel 1.6: Siber güvenlik

Siber güvenlik, verinin ve veri iletişiminin olduğu her ortamda en üst seviyede tutulmalıdır. Bu bağlamda siber güvenlik kavramı şu kategorilere ayrılır:

Ağ Güvenliği: Bilgisayar ağlarının izinsiz erişimlerden, kötü amaçlı yazılımlardan korunmasıdır.

Uygulama Güvenliği: Bilgisayar, bilgisayar ağları, taşınabilir cihazlar ve IoT cihazları üzerindeki yazılım ve uygulamaların güvenlik açıklarına karşı korunmasıdır.

Bilgi Güvenliği: Depolanan veya ağ iletişimi üzerinde bulunan verilerin bütünlüğünün ve gizliliğinin korunmasıdır.

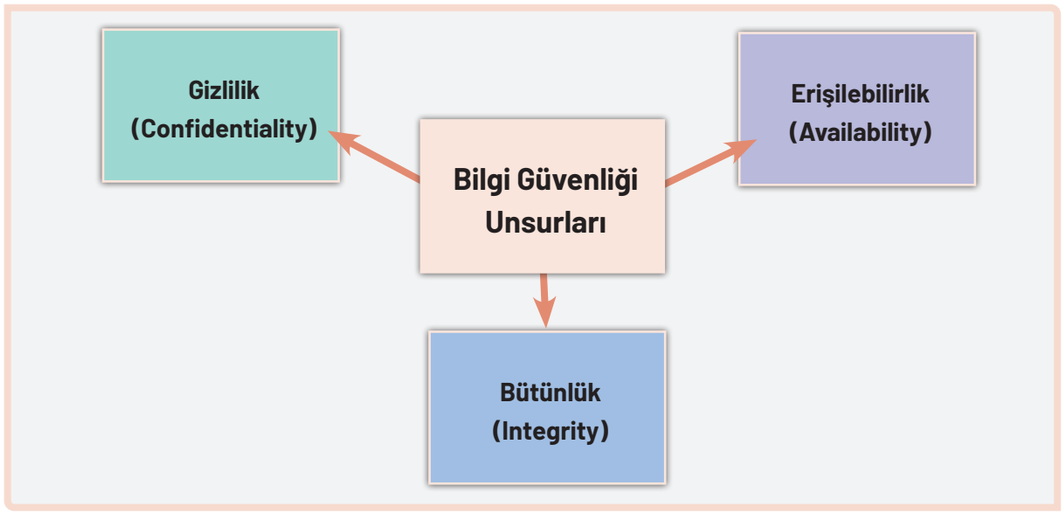
Operasyonel Güvenlik: Ağ erişimleri denetlenen kullanıcıların sahip olduğu izinler doğrultusunda veriye erişebilmesi; veriyi kullanabilmesi, paylaşabilmesi ve depolayabilmesidir.

Olağanüstü Durum Kurtarma ve Süreklilik: Bir kuruluşun bilgisayar ağları, iletişim cihazları veya verilerine karşı gerçekleşebilecek saldırılara yönelik olağanüstü eylemler bütünüdür.

1.2.2.1. Bilgi Güvenliği

Bilgi, verilerin bilişim araçlarıyla işlendikten sonra aldığı hâldir. Bilgiye anlamlandırılmış veriler bütünü de denebilir. Bilgi güvenliği; bireysel kullanıcıların veya kurum ve kuruluşların bilgisayar ve bilgisayar ağları üzerindeki verilerinin elde edilmesi, erişim sağlanması, silinmesi, değiştirilmesi veya çalınmasına yönelik alınan tedbirler bütünüdür.

Bilgi güvenliği, bilgiye karşı oluşabilecek tehditlerle ilgilenir. Bu bağlamda bilgi güvenliği; gizlilik (confidentiality), bütünlük (integrity) ve erişilebilirlik (availability) olmak üzere üç temel unsurdan oluşur. Bu unsurlara **CIA üçlüsü** adı verilir (Görsel 1.7).



Görsel 1.7: CIA üçlüsü

Gizlilik: Bilgiye yetkisiz kişilerin ulaşmasının engellenmesidir. Mobil bankacılık bilgileri, sosyal ağ erişim bilgileri, e-posta erişim bilgileri veya web portal yetkili kullanıcı erişim bilgileri gibi verilerin saldırganların eline geçmesi gizlilik ilkesinin ihlaline yol açar. Gizliliği kalıcı olarak sağlamak için doğru kişilerin yetkilendirilerek verilere erişimi sağlanmalıdır. Bu bağlamda özellikle kurum ve kuruluşlarda kullanıcı grupları oluşturularak kullanıcıların yetkilendirilmeleri son derece özenli bir şekilde yapılmalıdır.

Bütünlük: Bilginin bütünlüğü, doğru ve eksiksiz olarak saklanması ve aktarılmasıyla mümkündür. Saldırganlar; veri tabanında bulunan veri bütününe yeni veriler ekleyerek, var olan verilerin bir kısmını silerek veya değiştirerek bütünlük ilkesine zarar verebilir.

Erişilebilirlik: Bilgiye ihtiyaç duyulduğu zaman herhangi bir yerden erişebilme ilkesidir. Saldırganların, bir web sitesi veya veri tabanı sunucularına erişimi engellemesi bu ilkeye zarar verir. Özellikle sunucu hizmeti veren kuruluşların bu ilkeye son derece dikkat etmesi gerekir. Oluşabilecek saldırılara karşı önlemler alınmadığı takdirde sunucu hizmeti veren kuruluşun ticari imajı zedelenir.

1.2.2.2. İnternet Gizliliği ve Önemi

Dünya üzerindeki dijital bilgi miktarının her geçen gün arttığı görülür. Bunların büyük bir kısmı, kişisel ve ticari bilgilerdir. Bankacılık işlemleri, sosyal ağ kullanımları, yeni nesil mobil cihaz uygulamaları, IoT cihaz uygulamaları gibi birçok uygulama interneti kullanarak dijital bilgiyi bir noktadan bir başka noktaya iletir. Kişisel ve ticari bilginin maddi karşılığının olması, internet üzerinden bilginin aktarılması esnasında gizlilik ilkesine uyulmasını önemli kılar.

İnternet gizliliği; kişisel ve ticari bilgilerin bulutta depolanması, gerektiğinde kullanılması ve gerekli kişi veya kuruluşlarla paylaşılmasıyla ilgili gizlilik hakkını ifade eder. İnternet gizliliği, dijital bilginin korunması amacını taşır (Görsel 1.8).

Görsel 1.8: İnternet gizliliği

İnternet gizliliğini tehdit eden farklı internet saldırı yöntemleri bulunur. Bunların arasında en yaygın olanı **kimlik avı (phishing)** saldırılarıdır. Saldırgan, bir e-posta veya kısa mesaj yoluyla bir bağlantı veya eki açması için kullanıcıyı kandırmaya çalışır. Bu tür bir saldırıya maruz kalmamak için kullanıcılar, gelen e-postaların veya kısa mesajların kurumsal kullanıcılardan iletildiğine emin olmalıdır. Örneğin kullanıcılar, bir bankanın kurumsal e-posta adresine benzeyen bir adres kullanılarak gönderilen e-postayla rahatlıkla kandırılabilir. Böyle bir e-postadan gelen bağlantıyı veya eki açmak, kullanıcının kişisel bilgilerinin saldırganın eline geçmesine neden olabilir. Bunun dışında saldırganlar, kötü amaçlı yazılımlar kullanarak kullanıcıların kişisel veya ticari verilerine ulaşabilirler. Bu nedenle internet üzerinde yapılan her eylemde kullanıcılar çok dikkatli olmalı, ziyaret ettikleri internet sitelerinin güvenli aktarım protokolü olan **HTTPS** protokolünü kullanmasına özellikle özen göstermelidir.

1.2.3. Yasal Problemler ve Telif Hakları

Bilişim teknolojilerinin ve bilgisayar ağ sistemlerinin gelişimiyle verinin oldukça hızlı bir şekilde aktarılabilmesi, beraberinde yasal problemleri getirir. Ayrıca veri kaynağının tespitinin ve aktarım kontrolünün zorluğu, telif haklarının kolayca ihlal edilebilmesine sebep olabilir.

1.2.3.1. Bilgi Güvenliğiyle İlgili Yasal Problemler

Bilginin ağ sistemleri üzerinden iletilmesi, bulut üzerinde depolanması ve kullanılması birçok ihlali ve suç teşkil edebilecek eylemi beraberinde getirebilir. Bu durum, hukuksal sorunların ortaya çıkmasına neden olabilir. Bu hukuksal sorunlardan bazıları şunlardır:

- Veri hırsızlığı
- Gizlilik ihlalleri
- Yanıltıcı haberler
- Lisanssız yazılım kullanımı
- Telif ihlalleri (korsan yayıncılık)
- Finansal manipülasyon
- Ticari bilgilerin üçüncü şahıslar ile paylaşılması
- Yasa dışı şans oyunları
- Yetkisiz patent kullanımı
- Yetkisiz erişimler (sosyal ağ, internet bankacılığı, e-posta vb.)
- Erişimi kısıtlama

Kişisel verilerin korunması amacıyla 2010 yılında yapılan anayasa değişikliği ile Türkiye Cumhuriyeti Anayasasının 20. maddesine bir fıkra eklenerek **özel hayatın gizliliği ve korunması hakkı** kapsamında kişisel verilerin anayasal güvence altına alındığı anlaşılır. Ayrıca **Kişisel Verilerin Korunması Kanunu'**nun 24 Mart 2016 tarihinde TBMM'de kabul edilerek kanunlaştığı ve 6698 sayılı 7 Nisan 2016 tarih ve 29677 sayılı Resmî Gazete'de yayımlanıp, yürürlüğe girerek ülkemizde kişisel verilerin korunması için gerekli hukuksal altyapının tamamlandığı görülür. Kişisel Verilerin Korunması Kanunu ve sonrasında çıkan yönetmelikler hakkında detaylı bilgi almak için Kişisel Verileri Koruma Kurumunun internet sitesi (https://www.kvkk.gov.tr) ziyaret edilebilir (Görsel 1.9).

Görsel 1.9: Kişisel Verileri Koruma Kurumu

1.2.3.2. Telif Hakları ve Siber Güvenlik

Telif hakkı, kişinin her türlü fikrî emeğiyle meydana getirdiği ürünler üzerinde hukuken sağlanan haklardır. Telif hakkının doğması için tescile gerek yoktur. Fikir ve sanat eserleri üzerindeki haklar, eserin üretilmesiyle birlikte doğar. Telif hakları soyut niteliğe sahiptir. Ülkemizde 1 Ocak 1952 yılında çıkan ve çeşitli yıllarda değişikliğe uğrayan 5846 sayılı Fikir ve Sanat Eserleri Kanunu ile telif haklarının hukuksal güvence altına alındığı görülür.

Telif hakkına sahip eserlerin bilişim teknolojileri araçlarıyla yasa dışı olarak kolaylıkla çoğaltılabilmesi ve dağıtılabilmesi, bu alanda da siber güvenlik tedbirlerinin ve 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun uygulanmasını gerekli kılar.

Kültür Bakanlığına bağlı Telif Hakları Genel Müdürlüğü, ülkemizde telif hakları sisteminin işleyişini sağlamak amacıyla kuruludur. Telif hakları konusunda daha detaylı bilgi almak için genel müdürlük internet sitesi (https://telifhaklari.ktb.gov.tr) ziyaret edilebilir.

1.2.3.3. ISO 27001 Bilgi Güvenliği Yönetim Sistemi

Kurum ve kuruluşlarda bilgi, iş devamlılığının sağlanmasında büyük pay sahibidir. Bilginin gizliliği ve bütünlüğü, kurum ve kuruluşların tüm paydaşları için oldukça önemli bir olgudur. ISO 27001 Bilgi Güvenliği Yönetim Sistemi, kurum ve kuruluşların finansal ve fikrî haklarını korumalarına yardımcı olan uluslararası standarttır (Görsel 1.10). Ticari ve kişisel bilgilerin güvenliğini sağlamak amacıyla uygulanması gereken adımların prosedürlerle tanımlandığı, uluslararası geçerliliğe sahip ve denetime açık bir standarttır.

Görsel 1.10: ISO 27001 Bilgi Güvenliği Yönetim Sistemi

ISO 27001 Bilgi Güvenliği Yönetim Sistemi; bilgi güvenliğinin temelindeki gizlilik, bütünlük, erişilebilirlik unsurlarının sağlanmasını amaçlar. Bu sistem, kurum ve kuruluşlarda oluşabilecek bilgi güvenliği risklerini en aza indirmek için alınacak tedbirleri ve bu tedbirlerin uygulanış biçimini uygulayıcılara bir çerçevede sunar.

1.2.3.4. Avrupa Birliği'nde Verilerin Korunması ve Gizlilik

Avrupa Birliği Genel Veri Koruma Tüzüğü'nün (GDPR), 4 Mayıs 2016 tarihinde Avrupa Birliği (AB) Resmî Gazetesi'nde yayımlanarak 25 Mayıs 2018 tarihinden itibaren uygulandığı görülür. Bu tüzük; kişisel verileri işlenen kişilerin haklarını, veri işleme faaliyetinde bulunanların yükümlülüklerini, kurallara uyum sağlama yöntemlerini ve kurallara uymayanlar hakkında uygulanacak yaptırımları öngörür. GDPR, giderek daha fazla kişisel verinin işlendiği günümüzde veri gizliliği ve güvenliği konusunda uluslararası aktörleri ve üçüncü ülkeleri de etkileyen bir düzenlemedir.

1.2.3.5. Medya Sektöründe Güvenlik Politikaları ve Uygulamaları

Medya kuruluşları için bilgi güvenliği birincil öncelikli hususdur. Medya kuruluşları; bilgi güvenliğinin temel unsurları olan gizlilik, bütünlük ve erişebilirliği sağlamak için öncelikle ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standartlarını uygulamalıdır. BGYS'deki prosedürler tanımlanırken kurum ve kuruluşun müşteri, çalışan ve paydaş özellikleri açık ve net bir şekilde belirtilmelidir.

Kurum ve kuruluşlar sadece kendilerine ait dijital varlıklarını korumakla kalmayıp özellikle sosyal ağlarda bulunan takipçileri ve çevrimiçi toplulukları da saldırgan tehditlerinden koruyacak siber güvenlik politikaları geliştirmelidir. Medya kuruluşları, benimsedikleri güvenlik politikalarını tüm paydaşlarıyla paylaşarak onların bilgi sahibi olmalarını sağlamalıdır. Gerektiği takdirde çevrimiçi eğitimlerle paydaşlar, siber güvenlik tehditleri ve bunlara karşı alınabilecek önlemler konusunda bilgilendirilmelidir.

1.2.4. Siber Tehditler ve Saldırılar

İnternetin yaygınlaşması ve dünya genelinde hızlanmasıyla birlikte siber suçların da çeşitlenerek arttığı görülür.

1.2.4.1. Güncel Siber Tehditler ve Saldırılar

Kullanıcılar sadece virüsler veya kötü amaçlı yazılımlarla değil aynı zamanda kimlik hırsızlığı, fidye yazılım saldırıları, veri ihlalleri gibi tehditlerle karşı karşıyadır.

Yapay Zekâ ve Makine Öğrenimi: Yapay Zekâ [Artificial Intelligence (AI)] tabanlı saldırıların arttığı görülür. Saldırganlar, yapay zekâ sayesinde güvenlik açıklarını bulup saldırılarını kolaylıkla gerçekleştirirler. Böylelikle antivirüs yazılımlarının tespit edemeyeceği kötü amaçlı yazılımları oluşturarak güvenlik duvarlarını aşmayı amaçlarlar.

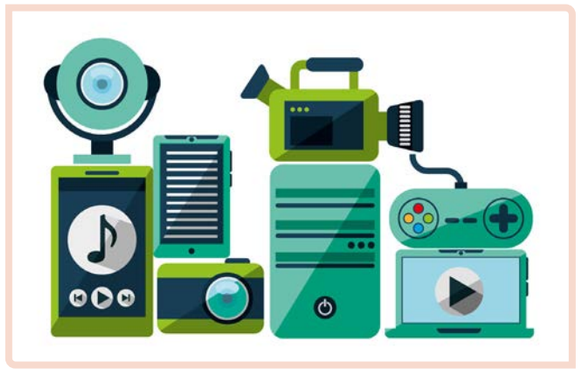
Deepfake Teknolojisi: Yapay zekâ ve makine öğrenmesi kullanarak sahte video veya ses kaydı oluşturmayı ifade eder. Saldırganlar, bu teknolojiyle kişilerin ses ve görüntülerinin benzerlerini oluşturup saldırılar düzenleyebilirler. Özellikle telefonla arayarak, sahte sesli mesajlar göndererek kurbanlardan para transferi veya hassas bilgi talep edebilirler.

Mobil Cihazlarda Siber Suçlar: Saldırganlar, taşınabilir cihazlar üzerinden sahte mesajlar göndererek veya sosyal mühendislik taktikleri kullanarak kullanıcıları kandırmaya çalışabilirler.

Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği: Nesnelerin İnterneti (IoT) teknolojisini kullanan cihazların artmasıyla birlikte IoT güvenlik protokollerinin öneminin de arttığı görülür. Bu tür cihazlarda güvenli kimlik doğrulama protokolleri ve şifreleme teknikleri kullanılmadığı takdirde saldırganlar, bu cihazlara ve cihazların kontrol ettiği nesnelere rahatlıkla erişim sağlayabilirler.

1.2.4.2. Dijital Medyaya Yönelik Siber Tehditler

Siber saldırıların artmasıyla birlikte dijital medya kuruluşlarının da büyük tehditlerle karşılaştığı görülür (Görsel 1.11).



Görsel 1.11: Dijital medya araçları

Bu saldırılardan en belirgin olanları ve saldırılara karşı korunma yöntemleri şu şekildedir:

Deepfake ve Sahte Haberler: Deepfake teknolojisi kullanılarak saldırganlar tarafından oluşturulabilecek sahte haberler, haber kaynağının doğruluğu ve güvenilirliği test edilmeden yayınlandığı takdirde yayını yapan medya kuruluşunun itibarını zedeleyerek yasal sıkıntılar yaşamasına neden olabilir.

İçerik Manipülasyonu: İnternet üzerinden yayın yapan medya kuruluşlarının web sitelerine ve sosyal ağ hesaplarına ait kullanıcı bilgilerinin yetkisiz kişilerin eline geçmesi sonucunda yanlış veya uygunsuz içerik oluşturulması, kuruluşun takipçileri veya okuyucuları arasında güven ve kullanıcı kaybına sebep olabilir.

Bu tarz saldırılara maruz kalmamak için kurum ve kuruluşların web sitesi yönetici portallarında kullanıcı ve grup yetkilendirmelerini uygun bir şekilde yapması, kullanıcıların da güçlü parolalar belirlemesi gereklidir. Bununla birlikte çok faktörlü kimlik doğrulama yöntemlerinin kullanılması, yetkisiz erişimlerin önüne geçer. Ayrıca dijital medya kuruluşlarının çalışanlarına siber güvenlik tehditleri ve tehditlerle başa çıkma yolları hakkında farkındalık eğitimleri ve seminerler vermesi, tehditlerle başa çıkma konusunda yardımcı bir seçenektir.

1.2.4.3. Haber Sitelerindeki Veri Sızıntıları ve Manipülasyonlar

Kullanıcılar tarafından en fazla takip edilen haber sitelerinde okuyucu bilgileri, içerik yönetim sistemi gibi son derece önemli ve hassas bilgiler bulunur. Veri ihlalleri, bu bilgilerin saldırganlar tarafından çalınmasına ve kötüye kullanılmasına neden olabilir. Ayrıca çalınan veriler, fidye yazılım saldırıları veya kimlik hırsızlığı için kullanılabilir.

Dijital ve sosyal medya üzerinden yayılan manipülasyon içerikli haberler önemli bir siber güvenlik tehdidir. Bu tarz manipülatif haberlerin siber güvenlikle ilişkisi; bireyleri, kurumları hatta ülkelerin güvenliğini etkileyebilecek çok ciddi sonuçlara neden olabilir. Ülkelerin ulusal güvenlik önlemleri arasında bu tarz manipülasyon içerikli haberlerin önlenmesi oldukça önemli bir yer tutar.Manipülasyon içerikli haberleri engellemenin en temel yolu, kullanıcıların ve çalışanların siber güvenlik konusunda eğitilmesidir. Güvenilir kaynaklardan alınan bilginin ayırt edilmesi ve güvenilir olmayan kaynaklara kullanıcı tarafından rağbet gösterilmemesi, bu tarz sahte ve yönlendirici haberlerin etkisini azaltabilir. Sahte haberlerin tespit edilmesi ve yayılmasının önüne geçilebilmesi için gelişmiş algoritmalar ve yapay zekâ destekli doğrulama mekanizmaları kullanılmalıdır.

ARAŞTIRMA

Dünya genelindeki dijital medya kuruluşları tarafından yapılan sahte ve yönlendirici haber içeriklerini araştırınız. Araştırma sonucunu arkadaşlarınızla paylaşınız.

1.2.4.4. Medya Kuruluşlarının Fidye Yazılımı Saldırılarına Maruz Kalması

Medya kuruluşlarının dijital platformlar, sunucular veya ağ sistemleri üzerinden fidye yazılımı saldırılarına maruz kalması, ciddi operasyonel ve maddi sorunlara yol açabilecek bir siber güvenlik tehdidir (Görsel 1.12). Medya kuruluşlarının çalışanlarına gönderilen e-posta ve mesajlarda bulunan ekler, kötü amaçlı fidye yazılımlarının sisteme bulaşmasına neden olabilir. Ayrıca fidye yazılımları; kurum ve kuruluşlarda kullanılan yazılım ve işletim sistemlerindeki güvenlik açıkları, güncellenmemiş veya lisanssız yazılımlar üzerinden sızabilir. Günümüzde uzaktan çalışma yöntemi yaygındır. Dijital medya sektörü de uzaktan çalışmaya uygun alanlardan biridir. Bu alanda çalışanların kullandıkları kendilerine ait taşınabilir cihazlar, ev ağları veya farklı zaman ve mekânlarda internete eriştikleri ortak ağlar, kurumsal düzeyde güvenilir olmadığı için fidye yazılımları karşısında daha savunmasızdır.

Görsel 1.12: Fidye yazılımı saldırısı

Fidye yazılımları, dijital medya kuruluşlarının yayınlarını kısa süreli veya uzun süreli sekteye uğratabilir. Özellikle canlı yayın yapan kuruluşlar için bu tür kesintiler, büyük maddi zarara ve imaj kaybına neden olabilir. Fidye yazılımı saldırıları sonucunda şifrelenen ve çalınan veriler hem kuruluşun hem de paydaşlarının gizliliğini tehlikeye atabilir. Saldırı sonucu yapılacak olası fidye ödemeleri, geri alınan verilerin kontrolü için harcanacak zaman ve kesintiye uğrayan yayın sebebiyle elde edilemeyen reklam gelirleri kurumlara maddi açıdan ciddi zararlar verebilir.

Fidye yazılımı saldırılarından korunmak için kullanıcıların farkındalık düzeyinin en üst seviyede olması, güçlü şifreleme ve güvenlik protokollerinin kullanılması, kullanılan verilerin düzenli olarak yedeklenmesi, bu yedeklerin çevrimdışı bir ortamda tutulması, gelişmiş güvenlik yazılımlarının kullanılması ve olası bir vaka için acil durum eylem planının yapılması son derece önemlidir.

1.2.5. Dijital Adli Bilişim

Bilişim ve ağ sistemlerinin kullanımının artması, internet ortamında gerçekleşen bazı suç unsurlarını beraberinde getirir. Bu suç unsurlarıyla mücadele edebilmek için çeşitli yasal düzenlemelerin yapıldığı ve **adli bilişim** kavramının ortaya çıktığı görülür. **Dijital adli bilişim,** bilişim teknolojileri cihazları ve veri saklama ortamlarından elde edilen bilgilerin adli olaylarda delil olarak kullanılmasıdır. Dijital adli bilişim, siber suçların açığa çıkarılmasında ve veri ihlallerinin araştırılmasında önemli rol oynar.

1.2.5.1. Sahte Haber ve Bilgi Manipülasyonunu Tespit Etmede Dijital Adli Bilişim

Sahte haber ve bilgi manipülasyonu, bireyler ve toplumlar üzerinde ciddi etkiler yaratabilir. Dijital adli bilişim, bu tip yanlış ve yanıltıcı haberleri tespit ederek haberlerin yayılmasının önüne geçmede önemli rol oynar. Sahte haber tehdidini engellemek için dijital adli bilişim tekniklerini kullanmak gerekir. Bu teknikler şunlardır:

Kanıt Toplama, Veri Analizi ve İzleme: Bir iddianın doğruluğunu tespit etmek için toplanan nesne veya belgelere **kanıt** denir. Adli bilişimde kanıtlar genellikle dijital ortamlarda bulunur. Bu tür kanıtlara **dijital kanıt** denir. Sabit diskler, bulut depolama alanları, taşınabilir haberleşme cihazları, taşınabilir depolama aygıtları, ses ve görüntü kayıt cihazları, sosyal ağ hesapları, web siteleri ve haber portalları dijital kanıtların elde edilebileceği ortamlardır. Adli bilişim uzmanları, bu kanıtların içindeki verileri araştırarak analiz eder. Özel yazılımlar ve tecrübelere dayalı olarak internet ortamında kullanılacak anahtar kelimeler yardımıyla özellikle sahte haberlerin kaynağı ve yayılımı izlenebilir.

Kaynak Doğrulama: Sahte haber ve manipülatif bilgilerin kaynağı, dijital adli bilişim teknikleriyle doğrulanabilir. Böylelikle haber kaynağının güvenilir olup olmadığının tespiti yapılır.

İçerik Analizi: Haber içeriklerindeki metinler, görseller ve videolar analiz edilerek doğru olup olmadığı anlaşılır. Deepfake gibi teknolojilerle oluşturulmuş ses veya görüntü içerikleri, dijital bilişim araçlarıyla analiz edilerek sahte içerik tespiti yapılır.

Sosyal Ağ Analizi: Sahte haberlerin paylaşıldığı sosyal ağ kullanıcı hesaplarını belirlemek için dijital adli bilişim uzmanları tarafından sosyal ağ analizi yapılır.

Kullanıcı ve paydaşların sahte haberlerin tespitini yapabilmeleri için açık kaynak web platformları mevcuttur. Bu web platformlarının yanı sıra üniversiteler ve araştırma kurumları, sahte haber ve manipülatif bilgi tespiti için çeşitli çalışmalar yapar.

1.2.5.2. Dijital Adli Bilişim ve Medya Hukuku

Ülkemizde bilişim suçlarına yönelik özel bir kanun yoktur. Bilişim suçları ile ilgili en kapsamlı düzenleme 5237 sayılı Türk Ceza Kanunu'nda yer alır. Türk Ceza Kanunu'nun onuncu bölümünde bilişim alanında suçlar başlığı altında bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme ile banka ve kredi kartlarının kötüye kullanılması konularında düzenleme bulunur. Türk Ceza Kanunu'nun 243, 244, 245. maddelerinde bilişim suçlarına yönelik düzenlemeler görülür. Türk Ceza Kanunu'na göre doğrudan bilişim suçları kapsamına giren suçlar şunlardır:

- Bilişim sistemine girme suçu (Madde 243)
- Sistemi engelleme, bozma, erişilmez kılma, verileri yok etme veya değiştirme suçu (Madde 244)
- Banka veya kredi kartının kötüye kullanılması suçu (Madde 245)
- Yasak cihaz veya program kullanma suçu (Madde 245/a)

Ayrıca Türk Ceza Kanunu'nun farklı maddelerinde bilişim teknolojileri araçlarıyla işlenen suçlara yönelik düzenlemeler mevcuttur. Bu kapsamda işlenen suçlar şunlardır:

- Eğitim ve öğretim hakkının engellenmesi (Madde 112)
- Kamu hizmetlerinden yararlanma hakkının engellenmesi (Madde 113)
- Hakaret suçu (Madde 125)
- Haberleşmenin gizliliğini ihlal (Madde 132)
- Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (Madde 133)
- Özel hayatın gizliliğini ihlal (Madde 134)
- Kişisel verilerin kaydedilmesi (Madde 135)
- Verileri hukuka aykırı olarak verme veya ele geçirme (Madde 136)
- Verileri yok etmeme (Madde 138)
- Bilişim sistemlerinin kullanılması suretiyle hırsızlık (Madde 142/2-e)
- Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık (Madde 158/1-f)
- Halk arasında korku ve panik yaratmak amacıyla tehdit (Madde 213)
- Suç işlemeye tahrik (Madde 214)
- Suçu ve suçluyu övme (Madde 215)
- Halkı kin ve düşmanlığa tahrik veya aşağılama (Madde 216)
- Kanunlara uymamaya tahrik (Madde 217)
- Müstehcenlik suçu (Madde 226)
- Kumar oynanması için yer ve imkân sağlama (Madde 228)
- 5464 sayılı Kanun'a muhalefet
- 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Oyunları Düzenlemesi Hakkında Kanun'a muhalefet
- 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun'a muhalefet

SIRA SİZDE

5237 sayılı Türk Ceza Kanunu'nda yer alan 243, 244, 245. maddeleri inceleyerek bu maddelerin içeriğini özetleyen bir sunu hazırlayınız. Hazırladığınız sunuyu arkadaşlarınızla paylaşınız.

1.3. AĞ GÜVENLİĞİ TEMELLERİ

Bilgisayar ağları (network), birden fazla bilgisayarın veya haberleşme cihazının (mobil cihazlar, IoT cihazları vb.) kablolu veya kablosuz teknolojilerle birbirine bağlanarak kullanıcıların veri aktarımının sağlandığı haberleşme sistemidir (Görsel 1.13).

Görsel 1.13: Bilgisayar ağı

Kullanıcıların veya ticari kuruluşların kişisel ve maddi değeri olan verileri, bilgisayar ağları üzerinden iletilir. Bu sebeple ağ iletişimi, saldırganlar tarafından sürekli olarak tehdit altındadır. Oluşabilecek bu tür saldırıların önlenmesi veya önlenemediği takdirde en az zararla atlatılması için iyi bir ağ güvenliği altyapısı oluşturulmalıdır.

1.3.1. Ağ Güvenliğinin Önemi

Ağ güvenliği; kullanıcıların ağ üzerindeki verilerinin ve tüm donanımların saldırı, yetkisiz erişim, verilerin yok edilmesi gibi durumlardan korunmasıdır. Kurum veya kuruluşların ürün ve hizmetlerini güvenli ve sürekli bir şekilde sunabilmesi için tüm tehditlere karşı savunması hazır olmalıdır. Altyapısı planlı bir şekilde oluşturulmuş ağ güvenlik yönetim sistemi, kurum ve kuruluşlara karşı gerçekleştirilebilecek saldırılara veya veri hırsızlığına yönelik riskleri ortadan kaldırır (Görsel 1.14).

Görsel 1.14: Ağ güvenliği

Kurum veya kuruluşların ağ güvenliği yönetim sistemi; bilgi güvenliğinin üç temel unsuru olan gizlilik (confidentiality), bütünlük (integrity) ve erişilebilirlik (availability) ilkelerini sağlayacak şekilde oluşturulmalıdır.

1.3.2. Medyada Güvenlik İhlallerinin Etkileri ve Sonuçları

Medya sektöründe güvenlik ihlalleri ve alınmayan veya yetersiz alınan önlemler sonucunda oluşabilecek güvenlik zafiyetleri, kuruluş ve paydaşları açısından ciddi sonuçlara sebep olabilir. Bu durum, kurum ve kuruluşlar için şu sonuçlara yol açabilir:

İtibar Kaybı: Güvenlik ihlalleri sonucunda kuruluşların güvenirliliği zedelenir. Bu durum, paydaşların kuruma olan güvenini sarsar. Ayrıca güvenlik ihlalinin ve oluşabilecek maddi ve manevi zararın büyüklüğüne göre kamuoyunun medya kuruluşuna yönelik tepkisi yüksek olabilir.

Maddi Kayıplar: Güvenlik ihlalleri sonucunda oluşabilecek veri çalınması veya değişimi, medya kuruluşlarını para cezalarıyla karşı karşıya bırakabilir. Özellikle kişisel verilerin korunmasına yönelik düzenlenen yasalara aykırılık, maddi kayıplara yol açabilir. Ayrıca itibar kaybı sonucunda reklam ve sponsor gelirlerinde ciddi azalmalar meydana gelebilir.

Önemli Verilerin İfşası: Medya kuruluşlarının web portallarına üye olan paydaşlarına ait kişisel verilerin çalınması ve bu verilerin yetkisiz kuruluşlar tarafından ticari amaçlı kullanılması büyük sorunlar yaratabilir. Ayrıca yayınlanmamış haber, video, ses kaydı gibi verilerin çalınması ve farklı kişi veya kuruluşların eline geçmesi sektörel rekabette geride kalmaya sebep olabilir.

Operasyonel Aksaklıklar: Güvenlik ihlalleri sonucunda medya kuruluşlarının yayın akışlarında aksaklıklar ve kesintiler olabilir. Ayrıca kuruluşların web platformlarında erişim sıkıntıları yaşanabilir.

Yasal Sonuçlar: Güvenlik ihlalleri sonucunda kuruluşlar hem hukuki süreçle hem de denetleyici kamu kurumlarının yaptırımlarıyla karşı karşıya kalabilir.

Paydaşların Güveni ve Etkileşim: Güvenlik ihlalleri; okuyucu, izleyici veya üye kaybına neden olabilir. Ayrıca bu durum, kuruluşların etkileşimli web platformlarındaki kullanıcı etkileşim ve katılım oranlarının düşmesine neden olabilir.

Medya kuruluşlarının bu tür ihlalleri önleyebilmesi için öncelikli olarak güçlü bir ağ güvenliği yönetimi ve sistem altyapısı oluşturması gerekir. Bunun için ilk yapılması gereken doğru ağ güvenlik planını oluşturmaktır.

1.3.3. Ağ Güvenlik Planı

Kurum ve kuruluşlar için verilerinin, ağ sistemlerinin ve sunucularının güvenliğini sağlamak oldukça hassas bir konudur. Kurum ve kuruluşlara ait ağ altyapısını ve verileri, dış tehditlerden korumak için gereken güvenlik önlemlerinin bütününe **ağ güvenlik planı** denir. Ağ güvenlik planı, çalışanlar ve tüm paydaşlar tarafından anlaşılacak şekilde sade ve net olmalıdır. Etkili bir ağ güvenlik planı oluşturmak için doğru ve açık bir şekilde belirlenmesi gereken adımlar şunlardır:

Potansiyel Güvenlik Risklerinin Belirlenmesi: Kötü amaçlı yazılımlar, veri ihlalleri, erişim kurallarının ihlalleri gibi kuruluşun karşılaşabileceği tüm tehditler belirlenmelidir.

Mevcut Güvenlik Tedbirlerinin Değerlendirilmesi: Kuruluşta hâlihazırda uygulanan güvenlik tedbirlerinin güçlü ve zayıf yönleri değerlendirilerek rapor edilmelidir.

Güvenlik Açıklarının Belirlenmesi: Kuruluşun daha önce karşılaştığı risklerden yola çıkılarak mevcut güvenlik açıklarının olup olmadığı belirlenmelidir.

Önleyici Tedbirlerin Belirlenmesi ve Uygulanması: İlk üç adım gerçekleştirildikten sonra saldırılara karşı alınacak önlemlerin belirlenmesi, belirlenen önlemlerin özellikle çalışanlar ve tüm paydaşlarla net bir şekilde paylaşılarak uygulamaya konması gereklidir. Kurum çalışanları ve paydaşlarının süreç içinde yer almadığı ağ güvenlik önlemleri başarıya ulaşamaz. Bu nedenle ağ güvenlik planı, tüm paydaşlarla net bir şekilde paylaşılmalı ve dönütlere göre gerekirse planda değişiklikler yapılmalıdır.

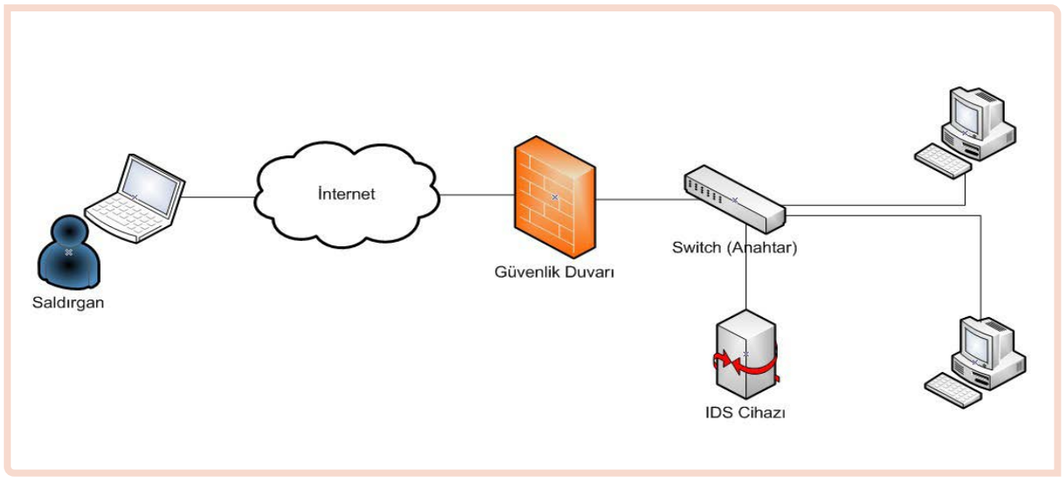
Sürekli İzleme ve Bakım: Ağ güvenlik planının etkililiğini kontrol etmek için süreç periyodik olarak gözden geçirilmeli, planın güçlü ve zayıf yönleri tespit edilmeli ve bu tespitlere göre gerekirse plan güncellenmelidir.

1.3.4. Ağ Saldırılarını Algılama ve Önleme

Ağ saldırılarını algılama ve önleme sistemleri (Instrusion detection and prevention systems); kurum ve kuruluşların verilerini, ağ sistemlerini, sunucularını korumak ve güvenlik açıklarının olup olmadığını tespit ederek ortadan kaldırmak için kullanılır.

1.3.4.1. Ağ Saldırılarını Algılama Teknikleri

Saldırı algılama sistemleri [Intrusion Detection Systems (IDS)]; ağ trafiğindeki paketleri izleyen, saldırıları tespit etmek üzere kurgulanmış, yazılım veya donanım olarak çalışan siber güvenlik sistemidir. Sistem donanımı, genel ağdaki anahtar (switch) cihazına bağlanır (Görsel 1.15).



Görsel 1.15: IDS cihazı bağlantısı

Saldırı algılama sistemleri, saldırıları tespit ederek raporlar. Saldırı tespit sistemleri, çalışma tekniğine göre şu şekilde sınıflandırılır:

Ağ Saldırı Tespit Sistemi: Ağdaki tüm cihazlardan gelen trafiği inceler. Görsel 1.16'daki gibi ağ içinde bir anahtar cihazına bağlanır. Ağ trafiğini izlemek için tıkanma noktalarına yerleştirilmiş sensörler bulunur. Bu sensörler, ağın trafiğini analiz ederek alt ağlardan geçen trafiği daha önceden bilinen saldırılarla eşleştirir. Bir saldırı olduğunu tespit ettiğinde ağ yöneticisine uyarı verir.

Ana Bilgisayara (Host) İzinsiz Giriş Tespit Sistemi: Ağdaki bağımsız ana bilgisayar üzerinde çalışır. Gelen ve giden paketleri sadece ana bilgisayar üzerinden izler. Bir anormallik tespit ettiğinde ağ yöneticisine uyarı verir.

Protokol Tabanlı Saldırı Tespit Sistemi: Bir istemci ve sunucu arasındaki protokolü kontrol ederek yorumlar. HTTPS protokol akışını izleyerek web sunucusunu korur.

Uygulama Protokolü Tabanlı Saldırı Tespit Sistemi: Genellikle sunucuda bulunan bir sistemdir. Protokoller üzerindeki iletişimi izleyerek saldırıları tespit eder ve uyarı verir.

Hibrit Saldırı Tespit Sistemi: Birden fazla saldırı tespit yaklaşımının kullanıldığı durumlara verilen genel bir addır. Bu sistem, diğerlerine göre daha etkilidir.

Sanal Makine Tabanlı Saldırı Tespit Sistemi: Bir bilgisayar üzerine kurulan sanal makine ile ağ üzerinde izleme sağlar. Ayrıca bir IDS cihazına ihtiyaç yoktur. Düşük maliyetli bir saldırı tespit sistemidir.

1.3.4.2. Medya Kuruluşlarının Karşılaştığı Yaygın Ağ Saldırıları ve Bu Saldırıları Algılama Teknikleri

Medya kuruluşları; hassas bilgi ve içeriklere sahip olması, geniş kitlelere hizmet sağlaması nedeniyle sürekli tehdit altındadır. Medya kuruluşlarına karşı kullanılan en yaygın ağ saldırıları ve bu saldırıları algılama teknikleri şu şekilde sıralanabilir:

Dağıtılmış Hizmet Reddi Saldırıları: Ağın veya sunucunun aşırı yüklenerek hizmet veremez hâle gelmesi için büyük miktarda trafik oluşturularak yapılan saldırıdır. Ağda oluşan aşırı trafik, IDS cihazıyla algılanarak rapor edilir.

Kimlik Avı Saldırıları: Kullanıcıları kandırarak kişisel bilgilerini öğrenmek için gönderilen e-posta veya kısa mesajlardır. Bu tür saldırılar, makine öğrenmesi veya imza tabanlı algılama yöntemiyle algılanabilir.

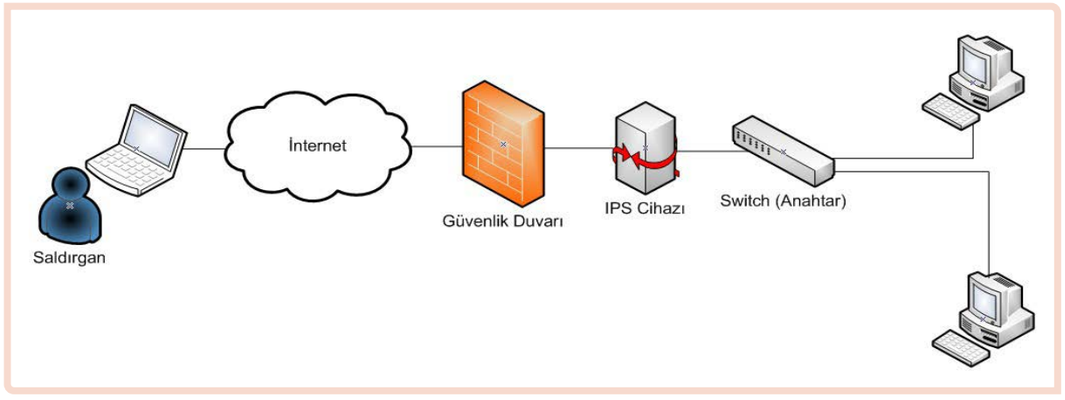
Fidye Yazılımları: Kuruluşun veri veya içeriklerinin şifrelenerek erişimin engellenmesi ve şifre karşılığında fidye istenmesidir. Bu tür saldırılar, davranış tabanlı ve imza tabanlı algılama yöntemleriyle algılanabilir.

SQL Enjeksiyonları: Veri tabanına zararlı sorgu komutları enjekte ederek yetkisiz erişim sağlamayı amaçlayan saldırılardır. Bu tür saldırılar, durum tabanlı ve imza tabanlı algılama yöntemleriyle algılanabilir.

İçeriden Gelen Tehditler: Kurum çalışanları veya paydaşlarının yetkisiz erişimlerinden ve kötü niyetli yaklaşımlarından kaynaklanan saldırılardır. Bu tür saldırılar, davranış tabanlı algılama ve makine öğrenmesi yöntemleriyle algılanabilir.

1.3.4.3. Ağ Saldırılarını Önleme Teknikleri

Saldırı önleme sistemleri [Intrusion Prevention Systems (IPS)] genellikle güvenlik duvarının arkasına bağlanır (Görsel 1.16). Üzerinden geçen veri trafiğini bölmeden paketleri inceler ve saldırı niteliği taşıyan paketleri tespit ederek ağı koruma altına alır. IPS cihazı, tespit ettiği saldırıyı henüz ağa ulaşmadan ve etkili olmadan önler. IPS cihazları, siber saldırılara karşı iki tür çalışma prensibine sahiptir.



Görsel 1.16: IPS cihazı bağlantısı

İmza Tabanlı IPS Cihazları: Ağ trafiğini kendi veri tabanındaki saldırılara ait imzalarla (kural listeleri) karşılaştırır ve eşleşen veri paketlerini tespit ettiğinde bu paketlerin trafik akışını engeller. Bu tür cihazların dezavantajı, veri tabanında bulunmayan bir saldırıyla karşılaştığında saldırıyı tespit edememesidir.

Davranış Tabanlı IPS Cihazları: Ağ üzerinden farklı zamanlarda trafik örnekleri alır. Bu örnekleri, ağın normal davranışıyla karşılaştırır. Bir anormallik tespit edilirse anormallik yaratan paketler engellenir. Bu tür cihazların dezavantajı, saldırı içermeyen paketleri de engelleme olasılığıdır.

1.3.4.4. Medya Şirketlerinin Ağ Saldırılarından Korunma Stratejileri

Medya kuruluşlarının ağ saldırılarından korunma stratejileri, tehdit ve saldırılara karşı etkili olacak şekilde belirlenmelidir. Bu stratejiler şu şekilde sıralanabilir:

Saldırı Tespit ve Önleme Sistemleri (IDS/IPS): Saldırı tespit ve önleme sistemleri kullanılarak ağ trafiği anlık olarak izlenmeli, saldırılar tespit edilmelidir.

Güvenlik Duvarları: Gelişmiş güvenlik duvarları kullanılarak veri trafiği kontrol edilmelidir.

Düzenli Güncellemeler: Sistem içinde bulunan tüm yazılım ve donanımlar güncel olmalıdır.

Güçlü Kimlik Doğrulama: Özellikle kritik veri ve içeriklere erişim için çok faktörlü kimlik doğrulama yöntemleri kullanılmalıdır.

Erişim Kontrolü: Kullanıcıların sadece gerekli kaynaklara erişimini sağlayacak şekilde rolleri atanmalıdır. Yetkisiz erişimin önüne geçilmelidir.

Veri Şifreleme: Hem depolanan hem de ağ üzerinde iletilen veriler şifrelenmelidir. Veri şifreleme, herhangi bir saldırı veya ihlal durumunda verilerin okunamaz olmasını sağlar.

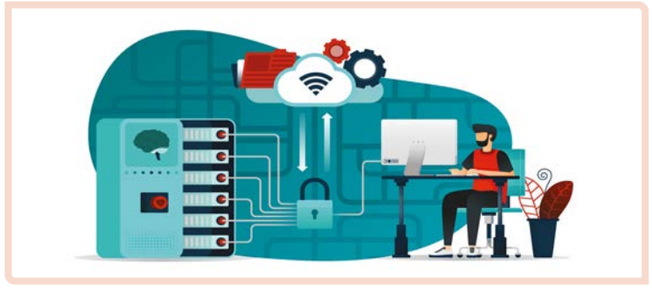
Kullanıcı ve Paydaş Eğitimleri: Tüm kullanıcı ve erişim hakkına sahip paydaşlar, düzenli olarak ağ güvenlik planı ve stratejileri hakkından eğitim almalıdır. Böylelikle sistem daha bilinçli kullanılır.

Güvenlik Testleri: Düzenli olarak zafiyet testleri ve sızma testleri yapılarak sistemin güvenlik açıkları tespit edilmelidir.

Fiziksel Güvenlik: Sistemin, veri merkezi gibi kritik öneme sahip merkezlere fiziksel erişimi kısıtlı olmalıdır. Ayrıca bu tip kritik öneme sahip alanlarda güvenlik kameraları ve fiziksel alarmlar kullanılmalıdır.

1.3.5. Ağ Trafiğinin Kontrolü

Ağ izleme (network monitoring); bir ağdaki trafiği izlemek, olayları analiz etmek ve kayıt altına almak için kullanılan süreçtir. Gelen ve giden paketlerin (verilerin) kontrol altında tutulması, saldırıların önlenmesi ve güvenliğin sağlanması için oldukça önemlidir. Ağ izleme; ağdaki trafiği izleyerek ağda oluşabilecek aşırı yüklemeleri, gecikmeleri, bant genişliği sorunlarını tespit etmeyi ve önlemeyi sağlar. Ağ yöneticileri, ağ izleme araçlarından gelen veriler doğrultusunda tespit edilen sorunları engellemek için gerekli müdahaleleri yaparlar (Görsel 1.17).



Görsel 1.17: Ağ yöneticisi

NOT **Bant genişliği,** bir haberleşme kanalının diğer bir deyişle ağın en yüksek veri aktarım hızıdır.

1.3.5.1. Ağ Trafiğini Kontrol Altına Alma Teknikleri

Ağ trafiğinin kontrol altında tutulması ve ağ güvenliğinin sağlanabilmesi için güvenlik duvarı kullanılmalıdır. Ayrıca güvenlik duvarını geçebilecek saldırı paketlerine karşılık bu tip paketlerin tespiti ve önlenebilmesi için güvenlik duvarıyla birlikte saldırı tespit ve önleme sistemleri (IDS ve IPS) kullanılmalıdır.

Güvenlik Duvarı (Firewall): İnternet üzerinden kişisel veya kurumsal ağlara gelen verileri filtreleyen, yetkisiz erişimlerin önüne geçen yazılımlar ile donanım cihazlarıdır. Yazılımsal güvenlik duvarları, daha çok bireysel kullanıcılar ve küçük ölçekli kuruluşlar tarafından kullanılır. Donanımsal güvenlik duvarı ise ağ üzerinde bulunan, daha çok profesyonel kurum ve kuruluşlar tarafından tercih edilen ve ağ trafiğini kontrol eden donanımsal cihazlardır. Ağ üzerindeki yönlendiricilere (router) entegre edilmiş güvenlik duvarları da mevcuttur.

Birleşik Tehdit Yönetimi [Unified Threat Management (UTM)]: Ağ üzerinde oluşabilecek tüm tehditleri engelleyebilecek tümleşik güvenlik sistemidir. Temelde güvenlik duvarı gibi çalışan birleşik tehdit yönetimi cihazları; saldırı tespit önleme sistemleri, web ve içerik filtreleme, casus yazılım engelleme gibi görevleri de üstlenir.

Yeni Nesil Güvenlik Duvarı [Next Generetion Firewall (NGFW)]: Saldırı tespit ve önleme sistemleri (IDS-IPS), veri kaybını önleme sistemleri [Data Loss Prevention (DLP)], içerik filtreleme gibi güvenlik sistemlerini bir arada toplayan tümleşik bir donanımdır. Geleneksel güvenlik duvarının daha gelişmiş hâlidir. Yeni nesil güvenlik duvarlarında kimlik kontrol özelliği bulunur. Bu özellik, sistem üzerindeki bir kullanıcının IP adresi değişse de kullanıcının aynı yetkilerle ağa ulaşabilmesini sağlar. Böylece ağ üzerindeki kullanıcıların kontrol altında tutulması mümkündür. Bu tür güvenlik duvarları, bir port üzerinde çalışan uygulama ve cihazların kontrolünü de sağlar. Tüm ağ protokollerini kontrol ederek güvenli bir katman oluşturur.

Web Uygulama Güvenlik Duvarı [Web Application Firewall (WAF)]: İnternet ağı trafiği üzerinde robot yazılımlar, SQL enjeksiyon saldırıları, hizmet reddi saldırıları gibi kötü amaçlı saldırılara ve gereksiz ağ trafiğine karşı koruma sağlar.

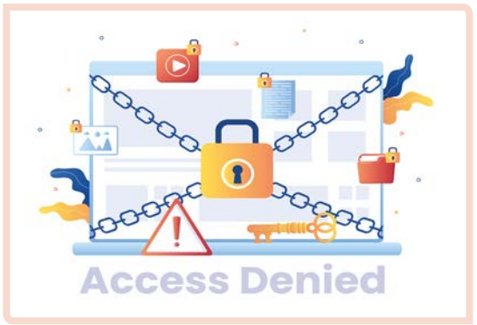
1.3.5.2. Medya Sektöründe Büyük Veri ve Yüksek Trafikli Ağ Yönetimi

Medya sektöründe büyük veri ve yüksek trafikli ağ yönetimi; veri trafiğinin etkili bir şekilde yönetilmesi, iç ve dış paydaşların ağ kullanımlarının en uygun şekilde sağlanması açısından kritik öneme sahiptir.

Medya kuruluşları, ağdaki trafiği kontrol altında tutabilmek için yeni nesil güvenlik duvarları kullanmanın yanı sıra hizmet aldıkları sunucuların da güvenli veri depolama ve ağ trafiği konusunda yetkin olmalarına dikkat etmelidir. Ayrıca saldırı tespit ve önleme sistemleri, kurum ağlarında mutlaka kullanılarak sürekli devrede tutulmalıdır. Olası bir saldırı durumunda oluşabilecek herhangi bir büyüklükteki veri veya erişim sıkıntısı, kurumun itibarını zedeleyebilir.

1.3.6. Yetkisiz Erişimin Engellenmesi

Ağ üzerinde yetkisiz erişimin engellenmesi, ağ güvenliğinin en temel bileşenidir (Görsel 1.18). Yetkisiz erişim engelleme hem donanımsal hem de yazılımsal olarak yapılabilir. Yerel ağa bağlanan bir saldırgan, o ağa zarar verebilir. Kablosuz ağların yaygınlaşması, yetkisiz erişimin artmasına neden olur.



Görsel 1.18: Yetkisiz erişimi engelleme

Yetkisiz erişimi engellemek amacıyla alınabilecek önlemler şunlardır:

- Güvenlik duvarı kullanılmalıdır.
- Saldırı tespit ve önleme sistemleri kullanılmalıdır.
- Sanal özel ağlar (VPN) kullanılmalıdır.
- Yerel ağa bağlı cihazlar mantıksal olarak gruplandırılmalıdır. Gruplar arasında trafiği düzenlemek ve güvenlik için sanal ağ (VLAN) oluşturulabilir.
- Switch cihazına bağlanan her cihazın MAC adresi, portlara statik olarak ayarlanmalıdır.
- Kullanıcı kimlik doğrulamada güçlü ve karmaşık parola politikaları benimsenerek çok faktörlü doğrulama yapılmalıdır.
- Ağ üzerinde veriler şifrelenerek aktarım sağlanmalıdır.
- Depolanan kişisel ve kritik veriler şifrelenmelidir.
- Ağ trafiği gerçek zamanlı izlenmelidir.
- Kablosuz ağlarda gizli ağ adı (SSID) kullanılmalıdır.
- Kablosuz ağ SSID ve parolaları belirli periyotlarla değiştirilmelidir.

ARAŞTIRMA

Sanal özel ağları araştırınız. Araştırma sonucunu arkadaşlarınızla paylaşınız.

1.3.7. Kullanıcı Verilerinin Güvenliği ve Medya Kuruluşlarının Gizlilik Politikaları

Medya kuruluşları için kullanıcı verilerinin güvenliği ve gizlilik politikaları hem yasalara uygunluk hem de kullanıcı güvenini sağlamak açısından oldukça önemlidir. Kullanıcı verilerinin güvenliğini sağlamak için veri şifreleme, erişim kontrolü, veri maskeleme, verileri yedekleme ve kurtarma, olası saldırıları tespit etme ve önleme işlemleri kuruluş tarafından en yüksek önem seviyesinde tutulmalıdır. Bu önlemlerden herhangi birinin alınmaması veya eksik alınması sonucunda verilerin istenmeyen üçüncü kişilerin eline geçmesi ve oluşabilecek veri kaybı, kuruluşun itibarını zedelemekle kalmayıp yasal sorumlulukların yerine getirilmemesi sebebiyle maddi zararlara da neden olur.

Medya kuruluşları, veri politikalarını açık ve şeffaf bir şekilde kullanıcılarına bildirmelidir. Veri politikalarına erişim kolay olmalıdır. Kullanıcı verileri alınırken kullanıcının açık rızası ve onayı alınmalıdır. Çerez politikaları konusunda kullanıcı mutlaka bilgilendirilmelidir. Kullanıcılar, herhangi bir güvenlik ihlali ve olası saldırı durumunda haberdar edilmelidir. Gizlilik politikaları, yasalara uygun ve kullanıcıyı koruma amaçlı hazırlanmalıdır. Kuruluşun marka itibarını yüksek seviyede tutmak için kullanıcı güveni sağlanmalıdır.

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

1. ( ) Bilişim sistemlerine yasa dışı yollardan sızmaya çalışan ve başarılı olduğunda sızdığı sistemlere zarar veren hacker türüne beyaz şapkalı hacker denir.

2. ( ) Deepfake teknolojisi, yapay zekâ ve makine öğrenmesini kullanarak sahte video veya ses kaydı oluşturmayı ifade eder.

3. ( ) Güvenlik duvarı, yazılımsal olarak kurulabildiği gibi ağ üzerine donanımsal olarak da kurulur.

4. ( ) Kimlik avı saldırılarında saldırganlar, kullanıcıların verilerini şifreleyerek şifreyi çözmenin karşılığında fidye isterler.

5. ( ) Bilgi güvenliği; gizlilik (confidentiality), bütünlük (integrity) ve erişilebilirlik (availability) olmak üzere üç temel unsurdan oluşur.

B) Aşağıdaki sorularda doğru cevabı işaretleyiniz.

6. Aşağıdakilerden hangisi kötü amaçlı yazılımların bilişim veya ağ sistemlerine bulaşma nedenlerinden değildir?

A) Güvenilir olmayan web sayfalarının ziyaret edilmesi
B) Güvenilir olmayan web sayfalarından program güncellemelerinin alınması
C) Lisanslı programların veya mobil uygulamaların kullanılması
D) Güvenilir olmayan e-posta eklerinin açılması ve bu eklerin cihaza indirilmesi
E) Güvenilir olmayan taşınabilir cihazlardan veri transferinin gerçekleştirilmesi

7. Aşağıdakilerden hangisi bir medya kuruluşunun ağ sistemine yapılan dağıtılmış hizmet reddi saldırıları sonucunda sistem üzerinde oluşan durumdur?

A) Veri tabanında yetkisiz erişim olması
B) Ağın veya sunucunun aşırı yüklenerek hizmet veremez hâle gelmesi
C) Kuruluşun veri veya içeriklerinin şifrelenmesi
D) Kritik öneme sahip görsel ve videoların çalınması
E) Kullanıcı ile paydaşların kişisel ve ticari verilerinin saldırganlar tarafından ele geçirilmesi

8. Aşağıdakilerden hangisi kullanıcılara sürekli reklam göndermek amacıyla geliştirilmiş kötü amaçlı yazılımdır?

A) Adware
B) Ransomware
C) Trojan
D) Virüs
E) Worm

9.

I. Potansiyel güvenlik risklerinin belirlenmesi
II. Sürekli izleme ve bakım
III. Güvenlik açıklarının belirlenmesi
IV. Mevcut güvenlik tedbirlerinin değerlendirilmesi
V. Önleyici tedbirlerin belirlenmesi ve uygulanması

Yukarıda verilen bilgilere göre etkili bir ağ güvenlik planını oluşturma aşamaları aşağıdaki seçeneklerin hangisinde doğru sıra ile verilmiştir?

A) I-IV-III-II-V
B) IV-I-III-V-II
C) I-II-III-IV-V
D) III-IV-I-V-II
E) I-IV-III-V-II

10. Aşağıdakilerden hangisi bilgi güvenliği uzmanlarının sorumlulukları arasında gösterilemez?

A) Tespit edilen ihlalleri ve güvenlik açıklarını kuruma ve kurum paydaşlarına bildirmek.
B) Hak ihlallerinden kaçınmak.
C) Elde edilen bilgileri gizli tutmak ve sadece ilgililer ile paylaşmak.
D) Kişisel menfaat sağlamak.
E) Dürüstlük, doğruluk, tarafsızlık gibi etik ilkelerine uymak.

2. ÖĞRENME BİRİMİ

BİLGİ TOPLAMA TEKNİKLERİ

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 online port tarama işlemi

ANAHTAR KAVRAMLAR

Ağ haritalama, Archive.org, bing, dnsenum, dnsrecon, Google Dork, Google Hacking Database, IP tarama, LBD, Nmap, port tarama, servis tarama, SHODAN, sublist3r, theHarvester, whois sorgusu

HAZIRLIK ÇALIŞMALARI

1. Bir haber hakkında internet üzerinden bilgi toplamak istediğinizde bu eylemi nasıl gerçekleştirirsiniz? Düşüncelerinizi arkadaşlarınızla paylaşınız.

2. Bir olayın tanıklarıyla iletişim kurarak bilgi toplama işlemini nasıl gerçekleştirirsiniz? Düşüncelerinizi arkadaşlarınızla paylaşınız.

2.1. PASİF BİLGİ TOPLAMA YÖNTEMLERİ UYGULAMALARI

Doğru ve etkili bilgi toplama, bilginin güvenirliği ve bütünlüğü açısından medya sektöründe büyük önem arz eder. Bilgi toplama işlemi gerçekleştirilirken çok fazla yöntem ve teknik uygulanır. Bilgi toplama amaçlanan sistem veya ağla doğrudan iletişime geçilmediğinde pasif bilgi toplama yöntemleri kullanılır. İnternet kaynakları ve çeşitli arama motorları kullanılarak yapılan pasif bilgi toplama işlemlerinde hedef sistemin bilgisi olmaz ve herhangi bir iz bırakılmadan işlem uygulanır. Pasif bilgi toplama işleminde detaylı bilgilere erişmek mümkün olmasa da hedef sistemle ilgili işe yarayacak birçok bilgi elde edilir ve sonraki aşamalarda bu bilgiler kullanılır. Pasif bilgi toplama işlemi; IP adresleri üzerinden bilgi toplama, domain üzerinden bilgi toplama ve web sayfalarını kullanarak bilgi toplama yöntemlerini içerir.

2.1.1. IP Adresleri Üzerinden Bilgi Toplama

Ağ üzerinden cihazların haberleşebilmesi için IP adreslerine ihtiyaç vardır. IP adresleri, veri paketlerinin hedefe ulaşabilmesinde önemli bir role sahiptir. IP adresleri üzerinden bilgi toplanarak potansiyel güvenlik açıkları ve zafiyetleriyle ilgili savunma mekanizmaları geliştirilir. IP adreslerini dağıtmakla ICANN (Internet Corporation for Assigned Names and Numbers) isimli kâr amacı gütmeyen merkez sorumludur.

2.1.1.1. Whois

Whois sorgusu; alan adı sahibi, kayıt kuruluşu, kayıt tarihleri, alan adı durumu, iletişim bilgileri, IP adresi gibi bilgileri listeler. Alan adı veya IP adresi sahipleri, bu bilgilerin sorgulanarak listelenmesini istemeyebilir. Bu durumda whois gizleme servisi aktif edilerek bilgilerin gizlenmesi sağlanır. Whois sorgusu; web sitesi, çevrimiçi araçlar, işletim sistemleri, komut satırları veya üçüncü parti araçlar kullanılarak yapılır. Web sitesi kullanılarak sorgusu yapılan domainin kayıtları Görsel 2.1'de görüldüğü gibi listelenir.

İnternetin yönetimi ve düzenlenmesiyle ilgili ICAAN dışında çeşitli uluslararası ve bölgesel kuruluşlar da bulunur. Bu kuruluşlar; internetin güvenliği, erişilebilirliği ve sürdürülebilirliği konularında ICAAN ile iş birliği yaparak çalışır. İlgili kuruluşların isimleri ve görevleri şu şekildedir:

IETF (Internet Engineering Task Force): İnternet protokolleri ve standartlarının geliştirilmesinde rol oynar. Teknik standartların belirlenmesinde etkili bir gruptur.

IEEE (Institute of Electrical and Electronics Engineers): Elektrik mühendisliği ve bilgisayar bilimi için standartlar geliştiren bir organizasyondur.

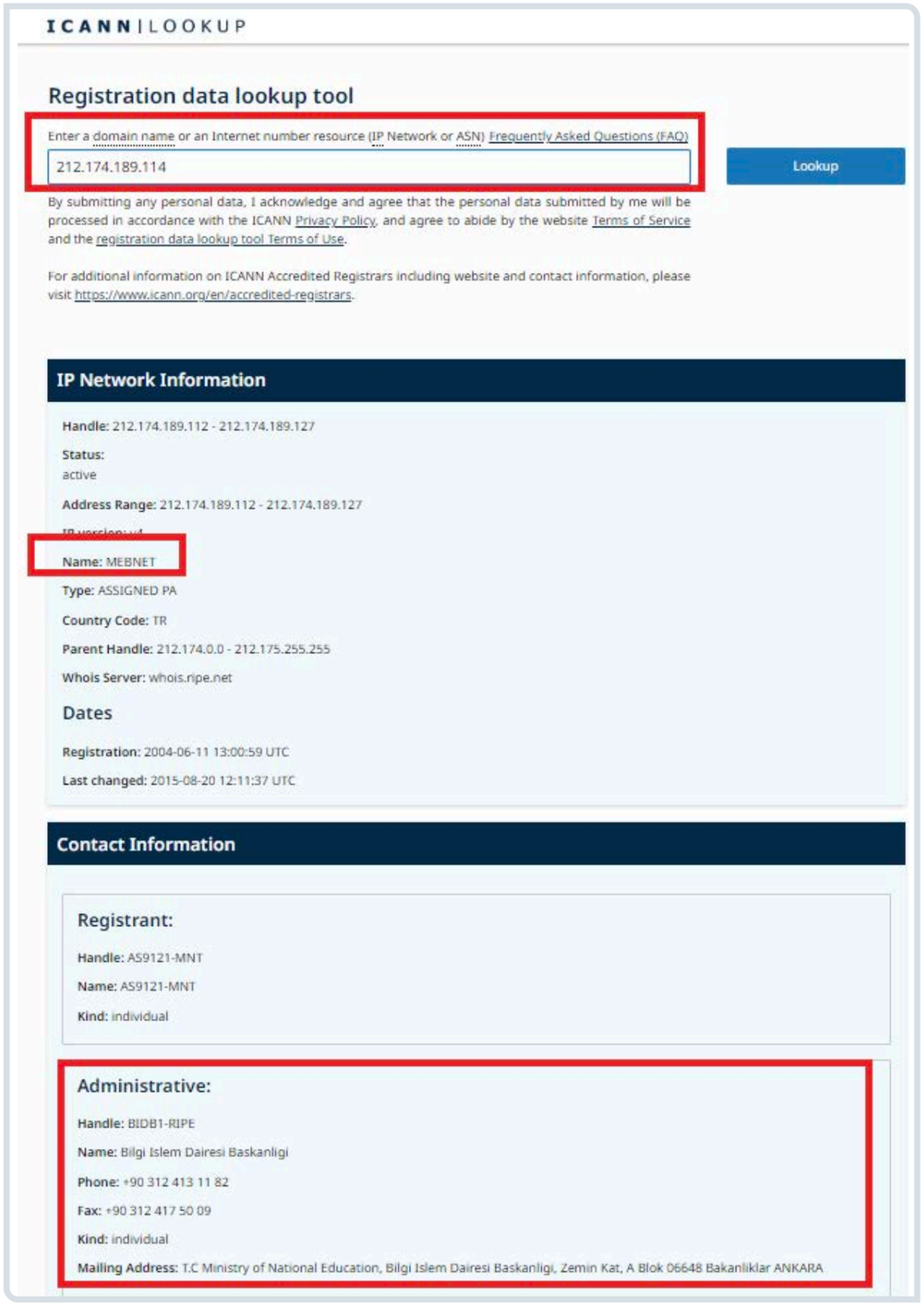
IANA (Internet Assigned Numbers Authority): IP adresleri ve protokol numaralarının dağıtımını yönetir ve ICANN'a bağlıdır.

IAB (Internet Architecture Board): İnternetin mimari yönleriyle ilgilenen bir kuruldur ve IETF'ye danışmanlık yapar.

RIR (Regional Internet Registries): IP adreslerinin bölgesel dağıtımını yöneten kuruluşlardır. Bu kuruluşlara ARIN (Kuzey Amerika), RIPE NCC (Avrupa, Orta Doğu, Orta Asya) ve APNIC (Asya-Pasifik) örnek verilebilir.

W3C (World Wide Web Consortium): Web standartlarını geliştiren bir kuruluştur. Web teknolojilerinin yaygınlaşmasını sağlar.

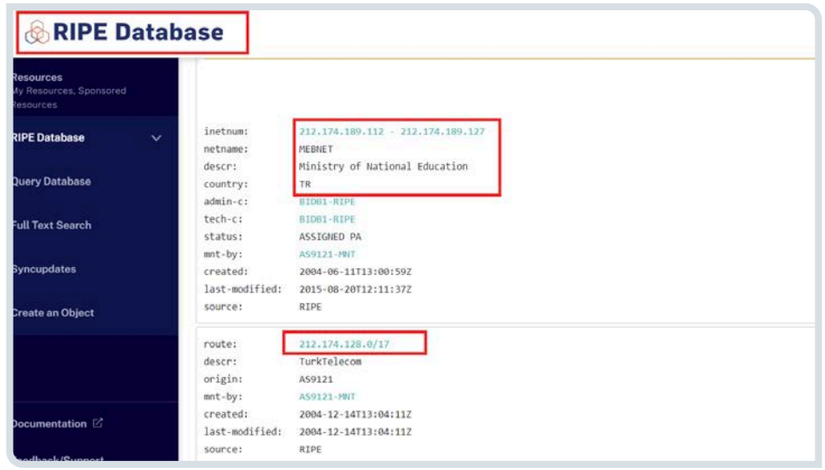
ISOC (Internet Society): İnternetin gelişimini ve erişimini destekleyen küresel bir sivil toplum kuruluşudur.



Görsel 2.1: Web sitesi kullanılarak yapılan whois sorgusu

2.1.1.2. RIPE NCC

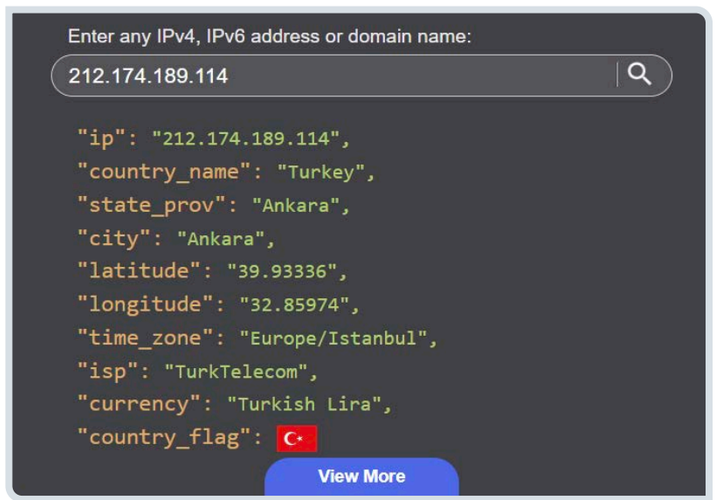
RIPE NCC (Réseaux IP Européens Network Coordination Centre); Avrupa, Orta Doğu ve bazı Orta Asya ülkelerinde IP adreslerinin yönetiminden ve dağıtımından sorumlu bölgesel internet kayıt kuruluşudur. Belirtilen bölgelerde yer alan IP adreslerine ilişkin pasif bilgi sorgulaması yapmak için https://www.ripe.net internet adresinden yararlanılır. İlgili web sayfasına bilgisi istenen IP adresi yazılarak sorgulama yapılır (Görsel 2.2).



Görsel 2.2: RIPE Database kullanılarak yapılan whois sorgusu

2.1.1.3. IP Location

IP Location, sorgusu yapılan IP adresinin coğrafi konumunu tespit eder. IP adreslerinin coğrafik yerinin bilinmesi birçok sektör için avantaj sağlar. İnternet güvenliğinin yanı sıra reklamcılıkta ve lokasyon bazlı içerik üretilen diğer alanlarda faydalıdır. IP Location ile alınan bilgilerle kullanıcının şehir, ülke hatta bazı durumlarda tam adresine kadar konum bilgisi öğrenilir (Görsel 2.3).



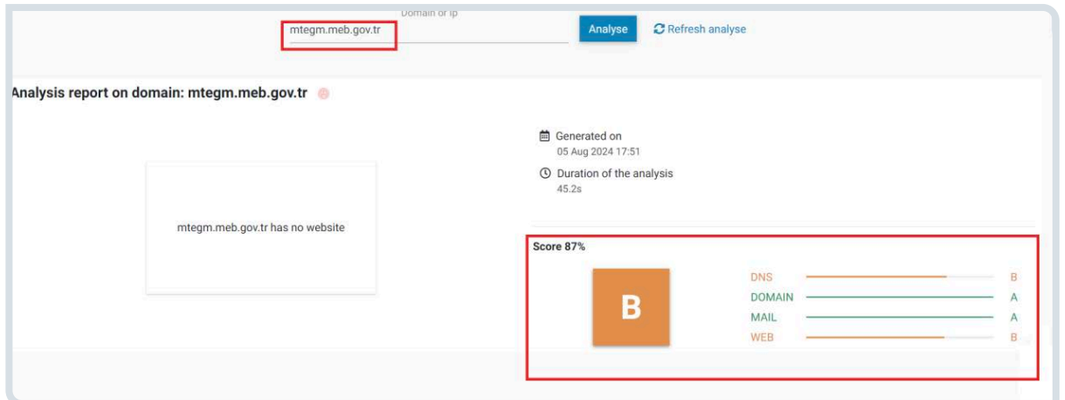
Görsel 2.3: IP Location kullanılarak yapılan whois sorgusu

2.1.2. Domainler Üzerinden Bilgi Toplama

Web sitelerine erişim için IP adreslerini kullanmak, akılda kalması zor bir yöntemdir çünkü ulaşılmak istenen bütün web sitelerine ait IP adreslerinin bilinmesi gerekir. IP adreslerinin tamamının akılda tutulması mümkün olmadığı için IP adresleri yerine domain (alan adı) isimleri kullanılır. Alan adları, IP adreslerinin karşılığı olan isimlerdir. Bir web sitesi hakkında pasif bilgi toplanmak istendiğinde domainler kullanılarak çeşitli araçlarla bu işlem gerçekleştirilir.

2.1.2.1. NS.TOOLS

NS.TOOLS, alan adı analizini çevrimiçi gerçekleştirmek için kullanılan bir araçtır. Bu araç kullanılarak bilgi toplanan domain adresinin aktifliği veya pasifliği öğrenilir. NS.TOOLS aracılığıyla araması yapılan domain adresine ait DNS, IP, e-mail gibi bilgiler de toplanır (Görsel 2.4).



Görsel 2.4: NS.TOOLS ile bilgi toplama

2.1.2.2. theHarvester

theHarvester; belirli bir alan adı hakkında e-posta adresleri, alt alan adları, IP adresleri ve ilgili diğer bilgileri toplamak için tasarlanmış bir uygulamadır. Çeşitli arama motorları, sosyal medya platformları ve diğer kaynakları kullanarak bu bilgileri toplar (Görsel 2.5). Kali Linux dağıtımı üzerinde kurulu hâlde gelir. Aksi hâlde uygulamanın bilgisayara yüklenmesi gerekir.

theHarvester için örnek kullanım şu şekildedir:

theHarvester -d example.com -b google

Örnek kullanımdaki parametreler ve açıklamaları şu şekildedir:

-d: Hedef alan adı

-l: Toplanacak maksimum sonuç sayısı

-b: Kullanılacak veri kaynağı (google, bing vb.)

Görsel 2.5: theHarvester ile bilgi toplama

2.1.2.3. Maltego

Maltego, hedef kurum ve kişiler hakkında bilgi toplanabilecek bir araçtır. Kali Linux işletim sistemiyle beraber gelir. Verileri çeşitli kaynaklardan toplar. Bu verileri görsel şekilde haritalayarak ilişkileri ve bağlantıları ortaya çıkarır. Maltego; sosyal medya profillerini, e-posta adreslerini ve diğer kişisel bilgileri araştırmak için kullanılır.

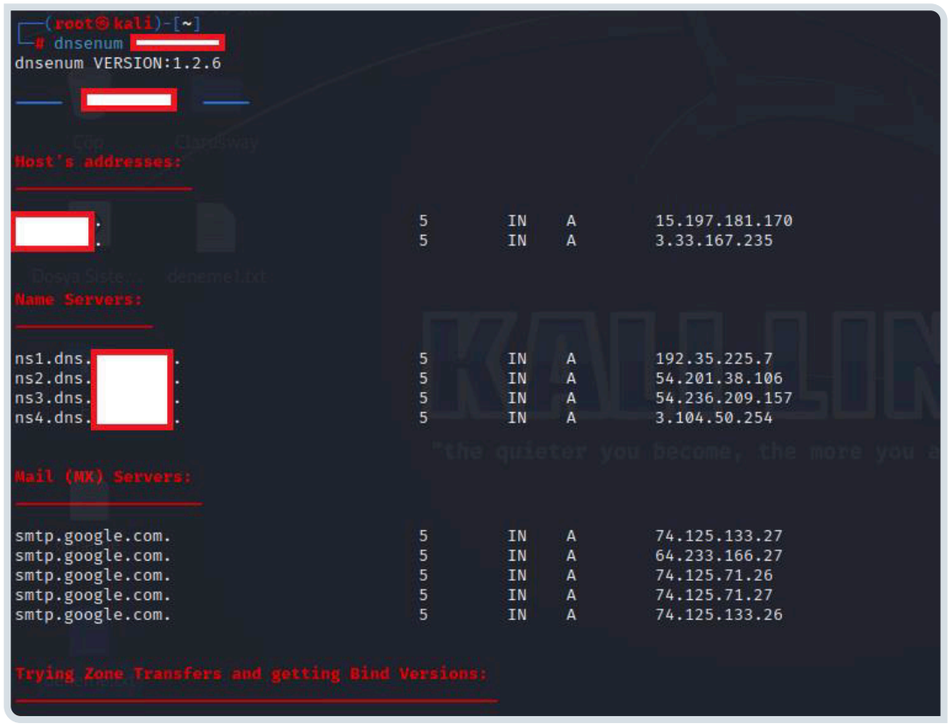
2.1.2.4. dnsenum

dnsenum; bir hedef domain hakkında kapsamlı bilgi toplayarak alt alan adları, mail sunucuları ve diğer DNS kayıtlarını ortaya çıkarabilir (Görsel 2.6). dnsenum'un temel özellikleri şunlardır:

Alt Alan Adları Keşfi: Hedef domainin altındaki subdomainleri bulur.

Zone Transfer Denemeleri: DNS zone transferlerini test eder ve başarılı olursa zone dosyalarını alır.

DNS Kayıtlarını Çözümleme: MX, NS ve diğer DNS kayıtlarını çözer.



Görsel 2.6: dnsenum sorgusunun sonuçları

2.1.3. Web Sayfalarından Bilgi Toplama

İnternet, her türlü bilgiye hızlı ve kolay erişim sağladığı için en önemli kaynaklardan biridir. Web sayfalarından bilgi toplamak özellikle medya, araştırma ve siber güvenlik alanları için çok önemlidir. Bilgi toplama süreci; bir web sitesinde bulunan metin, resim, video ve diğer veri türlerinin çeşitli teknikler kullanılarak analiz edilmesini ve toplanmasını içerir. 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. Archive.org

Archive.org diğer adıyla **Internet Archive;** dijital içerikleri koruma ve halka açık hâle getirme görevine sahip, kâr amacı gütmeyen bir organizasyondur. 1996 yılında kurulan bu platform; web sitelerinin, yazılımların, müziklerin, videoların, kitapların ve daha birçok dijital içeriğin arşivlenmesini ve erişilebilir olmasını sağlar. En popüler hizmetlerinden biri olan **Wayback Machine,** kullanıcıların belirli web sayfalarının geçmiş versiyonlarını görmelerine olanak tanır. İlgili web sayfasındaki arama çubuğuna bilgi toplanmak istenen web sitesinin adresi yazılır ve **Enter** tuşuna basılır (Görsel 2.7). Archive.org'un kullanım alanları şunlardır:

Tarihsel Araştırmalar: Geçmişteki web sayfalarını ve dijital içerikleri incelemek için kullanılır.

Medya ve Gazetecilik: Eski haberleri, medya içeriklerini doğrulamak ve incelemek için kullanılır.

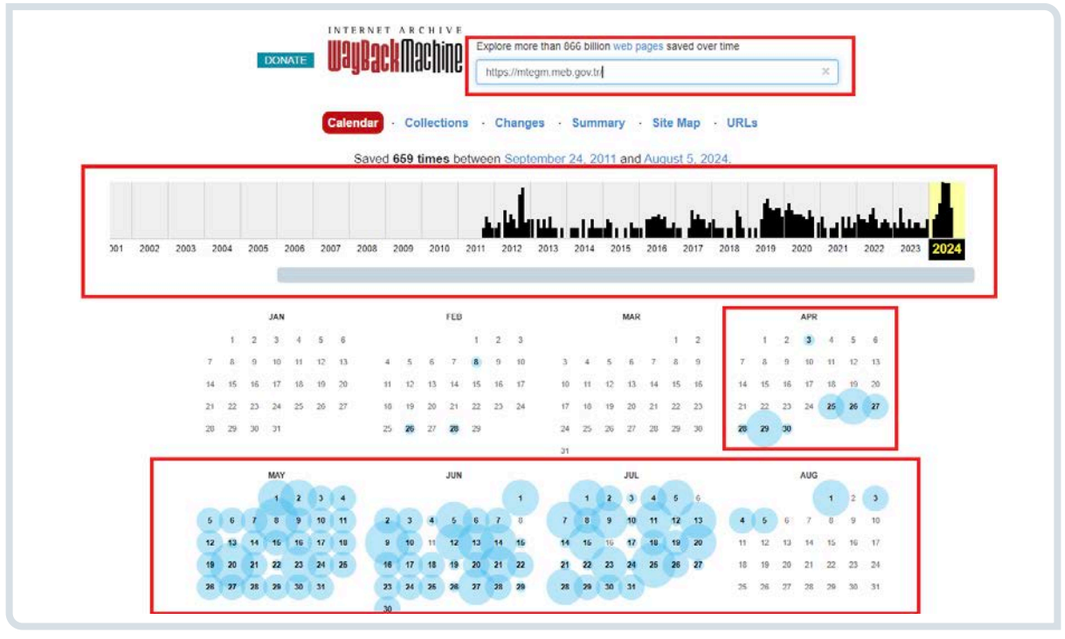
Akademik Çalışmalar: Dijital kitaplar, makaleler ve diğer kaynaklara erişim sağlamak için kullanılır.

Dijital Koruma: Web sitelerine ve dijital içeriklere gelecekte de erişebilmek için kullanılır.

Siber Güvenlik: Web sitelerinin geçmiş görüntülerinden yararlanarak bilgi toplamak için kullanılır.

Görsel 2.7: Web sitesinin eski görüntüsünü sorgulama

Wayback Machine ile yayından kaldırılan veya yayında olan web sitelerinin eski görüntülerine erişilebilir. Web sitelerinin yıllara, aylara ve günlere göre anlık görüntülerine ulaşılabilir (Görsel 2.8).

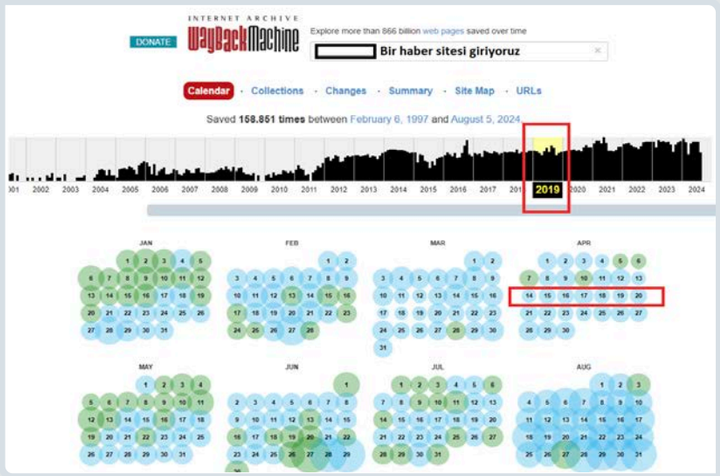


Görsel 2.8: Anlık görüntü takvimi

1. UYGULAMA

İşlem adımlarına göre 15.04.2019 tarihinde yaşanan ve oldukça ses getiren FBI personel kayıtlarının ele geçirilmesi olayının medya kuruluşlarında nasıl haberleştirildiğini pasif bilgi toplama araçları kullanarak inceleyiniz.

1. Adım: Archive.org sitesine giderek bir medya sitesinin adresini giriniz ve medya sitesinin 15 Nisan 2019 tarihinden alınmış eski bir görüntüsünü açınız (Görsel 2.9).



Görsel 2.9: Haber sitelerine ait eski görüntüler takvimi

2. Adım: Eski görüntülerden ilgili haberi bularak nasıl raporlandığını görüntüleyiniz (Görsel 2.10).

Görsel 2.10: İlgili haber görüntüsü

SIRA SİZDE

Eski tarihlerde meydana gelen ve ses getiren olayların nasıl raporlandığını farklı medya sitelerinin adreslerini kullanarak Archive.org sitesi aracılığıyla inceleyiniz.

DEĞERLENDİRME

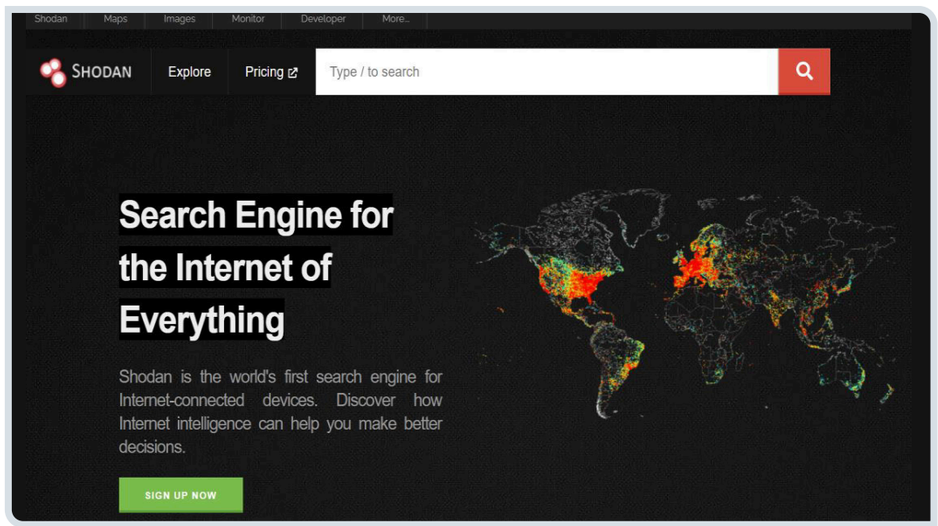
Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız. Çalışmanızı bir ders saati içinde tamamlayınız.

KONTROL LİSTESİ

DEĞERLENDİRME ÖLÇÜTLERİ	EVET	HAYIR
Archive.org web sitesini kullanarak Wayback Machine içeriğine ulaştı.		
Belirlediği medya portalının geçmişteki bir içeriğine Wayback Machine servisini kullanarak ulaştı.		
Zamanı verimli kullandı.		

2.1.3.2. Shodan.io

SHODAN (Sentient Hyper-Optimised Data Access Network); internet üzerindeki cihazları ve hizmetleri tarayarak bu cihazlara ait açık portlar, çalışan hizmetler ve diğer özellikler hakkında bilgi sağlayan bir arama motorudur. Kullanıcılara cihazların IP adresleri, açık portları, kullanılan protokoller ve daha fazlasıyla ilgili bilgi sunar. Bu bilgiler, güvenlik açıklarını tespit etmede ve güvenlik değerlendirmelerinde oldukça faydalıdır. Saldırganlar, pasif keşif aşamasında hedef sistemlerin altyapılarına erişebilmek ve daha ayrıntılı bilgi toplayabilmek için shodan.io web sitesini kullanabilirler (Görsel 2.11). Bu nedenle SHODAN, hackerların arama motoru olarak bilinir. Bu arama motoru, dünya üzerinde internete bağlı olan farklı türlerdeki bilgi işlem sistemlerini tespit eder. Bilgi işlem sistemlerinde yer alan cihazlar hakkında bilgi toplar.



Görsel 2.11: SHODAN arama motoru

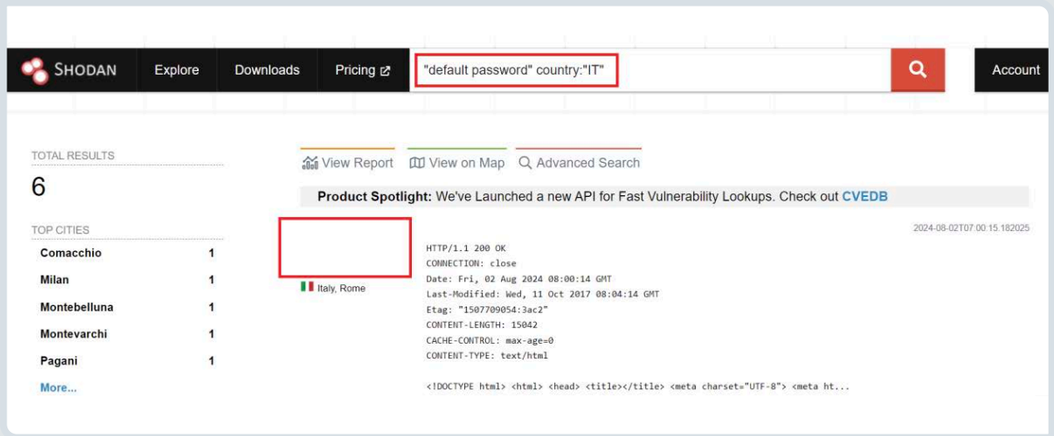
SHODAN arama motoru kullanılarak ülke ve şehir bazlı filtreleme yapılabilir. Filtreleme sonucunda tespit edilen sistem üzerindeki IP adreslerine, port ve servis bilgilerine ulaşılabilir. Kullanıcılar tarafından bu arama motorunda IoT cihazları, IP kameraları, sunucuları, SCADA sistemleri, nükleer santraller, açık trafik ışığı sistemleri aratılabilir. Hatta bu arama motoruyla deniz uydu alıcıları aratılarak gemilerin isimleri, konumları, iletişim numaraları dâhil birçok bilgi tespit edilebilir. 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.

2. UYGULAMA

İşlem adımlarına göre İtalya'da varsayılan parola kullanan sistemlerin bilgisini shodan.io arama motorunu kullanarak toplayınız.

1. Adım: shodan.io web sitesine giderek arama kısmına **"default password" country:"IT"** ifadesini yazınız ve sonuçları görüntüleyiniz (Görsel 2.12).



Görsel 2.12: shodan.io kullanarak bilgi toplama

2. Adım: Sorgulama tamamlandığında varsayılan parolayı kullanan sistemlere ilişkin bilgileri inceleyiniz.

SIRA SİZDE

Bulunduğunuz şehirde Windows 7 işletim sistemini kullanan cihazlarla ilgili bilgi toplama işlemini gerçekleştiriniz.

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız. Çalışmanızı bir ders saati içinde tamamlayınız.

KONTROL LİSTESİ

DEĞERLENDİRME ÖLÇÜTLERİ	EVET	HAYIR
shodan.io arama motoruna erişim sağladı.		
shodan.io arama motorunu kullanarak yaşadığı şehirde bulunan ve Windows 7 işletim sistemi kullanan cihazlar hakkında bilgi topladı.		
Zamanı verimli kullandı.		

2.1.3.3. Google Dorking ve Google Hacking Database

Google Dorking veya Google Hacking, Google'ın arama motorunu kullanarak hedef bilgi ve verilerde daha hassas ve derinlemesine arama yapma yöntemidir. Bu teknik, belirli arama sorguları ve operatörleri kullanarak internet üzerindeki genellikle gizli veya erişilmesi zor bilgilere ulaşmayı sağlar.

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. İndeksleme işlemi sonucunda bu motorların arama özellikleri, kötü amaçlar için kullanılabilir ve zafiyetli noktalar tespit edilebilir. Google arama motorundan bilgi toplamak için kullanılabilecek bazı dorklar şunlardır:

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

Belirli Google Dorking sorguları kullanılarak medya şirketinin web sitesindeki potansiyel güvenlik açıkları araştırılabilir. Google Dorking sorgularına örnek olarak şunlar verilebilir:

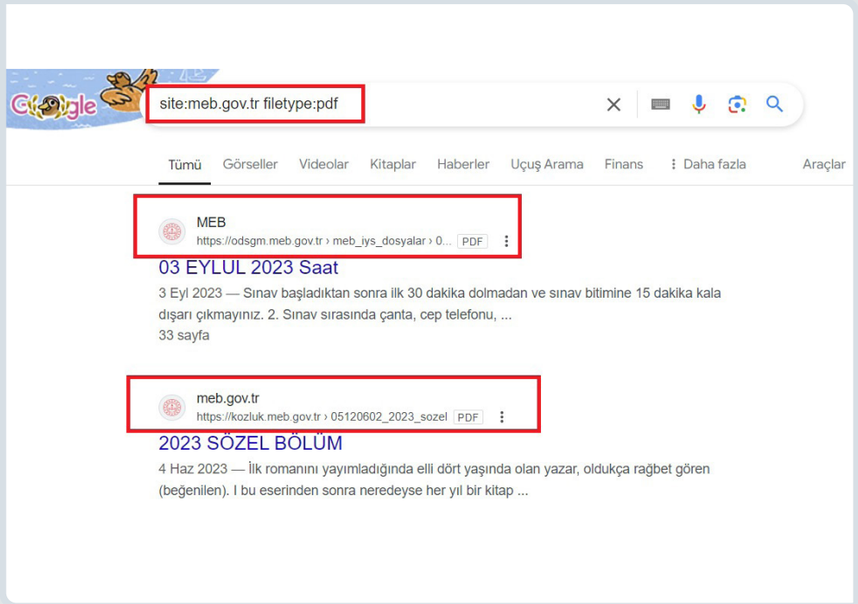
- site: orneksiteadi.com inurl:admin (Admin paneline erişim sağlayan URL'leri arar.)
- site: orneksiteadi.com filetype:pdf (PDF dosyalarını arar ve potansiyel hassas bilgileri tespit eder.)

3. UYGULAMA

İşlem adımlarına göre Google arama motoru sitesine girerek meb.gov.tr adresindeki pdf uzantılı dosyaları bulmaya yarayan **dork** sorgusunu yapınız.

1. Adım: Google web sitesine giderek arama kısmına **site:meb.gov.tr filetype:pdf** ifadesini yazınız.

2. Adım: Yapılan dork sorgusunun sonuçlarını görüntüleyiniz (Görsel 2.13).



Görsel 2.13: Google dork sorgusu ve sonuçları

SIRA SİZDE

passwd parola dosyalarına sahip web sitelerini listeleyen dork sorgusunu gerçekleştiriniz.

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız. Çalışmanızı bir ders saati içinde tamamlayınız.

KONTROL LİSTESİ

DEĞERLENDİRME ÖLÇÜTLERİ	EVET	HAYIR
Google arama motoruna erişim sağladı.		
passwd parola dosyalarına sahip web sitelerini listeleyen dork sorgusunu gerçekleştirdi.		
Zamanı verimli kullandı.		

Google Hacking Database (GHDB), Google Dorking ile ilgili çeşitli arama sorgularının ve tekniklerinin toplandığı bir veri tabanıdır. GHDB, Google Dorking ile yapılan aramaları ve bu aramalardan elde edilen bilgileri listeler. Bu veri tabanına **https://www.exploit-db.com/google-hacking-database** bağlantısından erişilebilir (Görsel 2.14). GHDB kullanılarak kullanıcı adı, parolalar, kritik bilgiler içeren hata mesajları ve güvenlik zafiyetleri bulunabilir. İlgili veri tabanında yer alan güncel dorklar kullanılarak önemli bilgiler toplanabilir.

Görsel 2.14: Google Hacking Database web sitesi

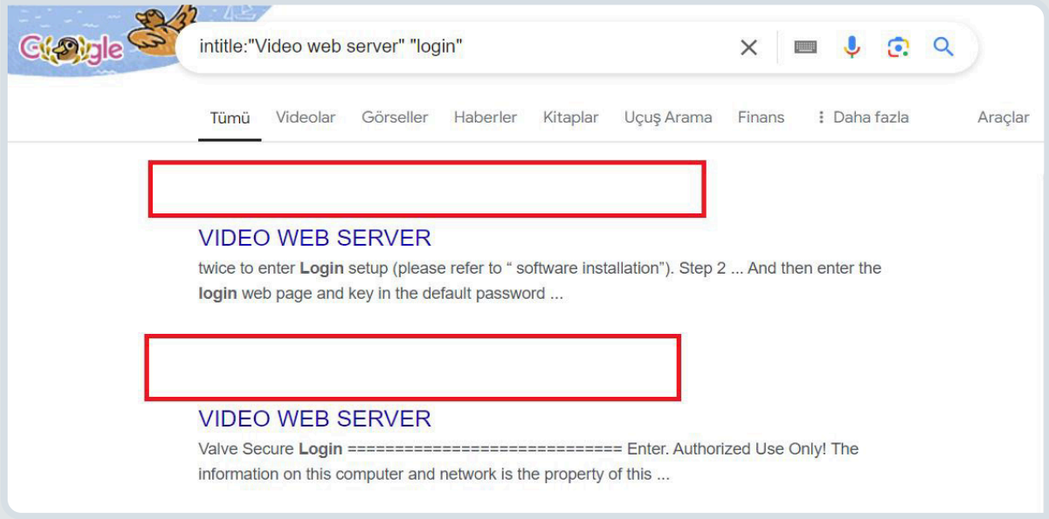
4. UYGULAMA

İşlem adımlarına göre Google Hacking Database filtreleme sistemini kullanarak, **video** ifadesi geçen dorkları Google arama motoruna yazıp sonuçlarını görüntüleyiniz.

1. Adım: Google Hacking Database sitesine girerek arama kısmına **video** kelimesini yazınız ve güncel dork ifadelerini görüntüleyiniz (Görsel 2.15).

Görsel 2.15: Google Hacking Database aramasının sonuçları

2. Adım: Yapılan dork sorgularından örnekler alarak Google arama motoruna yazınız ve sonuçlarını görüntüleyiniz (Görsel 2.16).



Görsel 2.16: Dork sorgusunun sonuçları

SIRA SİZDE

Bir şirketin stratejik planlarını veya finansal bilgilerini içerebilecek dosyaları (.pdf veya .docx uzantılı olabilir.) araştıran dork sorgularını Google'a yazarak bilgi toplama işlemini gerçekleştiriniz. Bu işlem; Excel dosyaları, kullanıcı bilgileri veya parola listeleri gibi hassas verileri de içerebilir. Şirketin Excel dosyalarını da araştırarak, içinde password ifadesi geçen kelimeleri aratıp bilgi toplama işlemini tamamlayınız.

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız. Çalışmanızı bir ders saati içinde tamamlayınız.

KONTROL LİSTESİ

DEĞERLENDİRME ÖLÇÜTLERİ	EVET	HAYIR
Google arama motoruna erişim sağladı.		
Daha önce belirlediği bir kuruluşun .pdf ve .docx uzantılı dosyalarına ulaştı.		
Aynı kuruluşun .xlsx uzantılı dosyalarına ulaştı.		
Zamanı verimli kullandı.		

2.2. AKTİF BİLGİ TOPLAMA YÖNTEMLERİ UYGULAMALARI

Siber güvenlik alanında sistemlerin ve ağların güvenliğini sağlamak için aktif bilgi toplama yöntemlerinin kullanılması çok önemlidir. Bu yöntemler, hedef sistemlerin ve ağların potansiyel zayıflıklarını ve güvenlik açıklarını tespit etmek amacıyla uygulanan çeşitli araç ve teknikleri içerir. Aktif bilgi toplama, gerçek zamanlı veri analizi ve tarama işlemleriyle sistemlerin savunmasız yönlerini belirleyerek güvenlik önlemlerinin etkin bir şekilde uygulanmasını sağlar. Aktif bilgi toplama yöntemlerinde bilgi alınmak istenen hedef ağ veya sistemle doğrudan iletişime geçilir. Bu nedenle hedef sistemde log kaydı oluşturulur ve iz bırakılır. Aktif bilgi toplama, saldırgan açısından en riskli bilgi toplama yöntemidir. Aktif bilgi toplama yöntemlerinde hedeflenen bilgiler şunlardır:

Ağ Topolojisi ve Yapısı: Hedef ağın fiziksel ve mantıksal yapısını anlamak için kullanılan bilgileri, ağ cihazlarının yerleşimini ve bağlantılarını içerir.

Ağ Cihazları ve Sunucular: Aktif tarama ve analizler yoluyla ağ üzerindeki sunucular, yönlendiriciler, anahtarlar, diğer cihazların türleri ve yapılandırmaları belirlenir.

Açık Portlar ve Protokoller: Sistemlerde açık olan portlar ve kullanılan protokoller tespit edilir. Böylece potansiyel giriş noktaları ve iletişim yolları hakkında bilgi edinilir.

Hizmetler ve Uygulamalar: Çalışan hizmetler ve uygulamalar hakkında bilgi toplanır. Hizmet ve uygulamaların sürümleri, yapılandırmaları ve güvenlik açıkları belirlenir.

Zayıflıklar ve Güvenlik Açıkları: Sistemlerin ve uygulamaların zayıf noktaları, yapılandırma hataları veya bilinen güvenlik açıkları tespit edilir.

Kullanıcı ve Sistem Bilgileri: Kullanıcı hesapları, izinler, erişim hakları gibi bilgiler toplanarak yetkisiz erişim riskleri değerlendirilir.

Web Uygulamaları ve API'ler: Web uygulamaları ve API'ler üzerindeki potansiyel güvenlik açıkları, parametreler ve veri giriş noktaları araştırılır.

Yazılım ve Sürüm Bilgileri: Sistemlerde kullanılan yazılımlar ve bu yazılımların sürümleri belirlenerek, bilinen güvenlik açıklarına karşı sistemin savunmasız olup olmadığı değerlendirilir.

2.2.1. Network Mapping (Ağ Haritalama)

Bilgisayar ağlarındaki kabloların ve cihazların yerleşimine **fiziksel topoloji** denir. Veri paketlerinin kaynaktan hedefe doğru iletilip alınma şekline ise **mantıksal topoloji** denir. Cihazların IP adresleri, MAC adresleri ve verinin iletimini sağlayan diğer protokoller mantıksal topoloji kapsamına girer.

Ağ haritalama; ağın fiziksel ve mantıksal olarak yapısını ortaya koyan görsel bir dokümandır. Bir sistemde kullanılan cihazlar, cihazların bulunduğu noktalar, kablolama, iletişim yolları, kullanılan protokoller gibi ağın tamamının anlaşılabildiği teknik belgelemenin yapılmasını sağlar. Ağ haritalamanın amacı; daha etkin bir ağ yönetimi, sorunlara hızlıca çözüm sağlama ve ağ güvenlik raporlamalarının verimli şekilde yapılmasıdır. Ağ haritalama işlemi şu adımları içerebilir:

Cihaz Keşfi: Ağda yer alan tüm cihazları tanımaya yarar. Bu aşama ile sunucular, yönlendiriciler, anahtarlar, güvenlik duvarları, bilgisayarlar ve diğer ağ cihazları tespit edilir.

Bağlantı ve Topoloji Bilgileri: Cihazlar arasındaki ağ ve bağlantı hakkında bilgi edinmeye yarar. Cihazların birbirine bağlı olduğunu ve veri alışverişi yaptığını anlamaya katkı sağlar.

Hizmet ve Protokol Bilgileri: Kullanılan teknoloji hakkında bilgi toplama adımını içerir. Ağın nasıl çalıştığını ve hangi uygulamaların kullanıldığını anlamak için önemlidir.

Segmentasyon ve Alt Ağlar: Ağın daha küçük parçalara bölünmesi ve bu parçaların yönetilmesini ifade eder. Bu süreç, ağ yönetimini kolaylaştırır ve güvenlik önlemlerini artırır.

Görselleştirme: Ağ yapısını şemalar ve çizimler yerine haritalandırarak daha net görselleştirmeye ve anlaşılabilir hâle getirmeye yarar.

NOT Ağ haritalama işlemi için ücretli, ücretsiz veya açık kaynak kodlu birçok araç kullanılabilir. Nmap, Ms Visio, SolarWinds bu araçlar arasında en yaygın olanlarıdır.

2.2.2. Nmap Parametreleriyle Açık Sistemlerin Tespiti

Nmap (Network Mapper) yazılımı, ağ haritası oluşturmada kullanılır. Açık kaynak kodlu Nmap, kullanılan en etkin ağ tarama yazılımıdır. Başlangıçta yalnızca ağ tarama amacıyla kullanılsa da zamanla birçok ek özellik kazanarak ağ güvenliği alanında vazgeçilmez bir araç hâline gelmiştir.

Nmap ile ağ üzerinde hangi cihazların aktif olduğu, cihazların açık olan portları, açık portlarda çalışan servislerin türleri, işletim sistemleri, çalışan servislerin versiyonları bulunur. TCP/IP sistemlerini keşfetmek ve zafiyetlerini tespit etmek amacıyla da yaygın biçimde kullanılır. Nmap aracı, Kali Linux içinde kurulu gelir. Nmap aracını kullanmak için hedef sisteme ait bir IP adresi veya alan adı gerekir. Bir IP adresine ait ağ haritasının çıkarılması için kullanılan Nmap aracının en basit komutu **nmap <ip adresi>** şeklindedir (Görsel 2.17).

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.1.27
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-06 09:58 EDT
```

Görsel 2.17: Nmap'in temel kullanımı

Görsel 2.17'de kullanılan komut, hedef IP adresi **192.168.1.27** üzerindeki açık portları ve temel ağ bilgilerini tespit etmeye yarar. Varsayılan olarak Nmap hızlı bir tarama gerçekleştirir ve yaygın olarak kullanılan 1000 portu kontrol eder. Nmap taraması sonucunda Görsel 2.18'deki ekran ile karşılaşılır.

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.1.27
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-06 09:58 EDT
Nmap scan report for LAPTOP-S7UE957R.home (192.168.1.27)
Host is up (0.014s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 11.29 seconds
```

Görsel 2.18: Nmap taramasının sonucu

Bu komut çalıştırıldığında şu bilgilere ulaşılabilir:

Host Durumu: Hedef cihazın ağda aktif olup olmadığını gösterir (up veya down). Görsel 2.18'deki örnek Nmap taramasında hedef cihazın **host is up** konumunda olduğu görülür.

Açık Portlar: Hedef cihaz üzerindeki açık portları listeler. Görsel 2.18'deki örnek Nmap taraması incelendiğinde 5 adet portun açık, 995 adet portun ise filtreli olduğu görülür.

Servisler: Açık portlarda çalışan servisleri tanımlar.

OS Tespiti (Varsayılan olarak değil.): Hedef cihazın işletim sistemine dair bilgiler görülür (Varsayılan tarama, OS tespiti yapmaz. Bu durum, ayrı bir komutla belirtilmelidir.).

Nmap, ağ güvenliği ve yönetimi için vazgeçilmez bir araç olup ağ üzerinde açık sistemlerin tespit edilmesi ve analizi için çeşitli parametreler sunar. Bu parametreler, güvenlik uzmanlarının ve ağ yöneticilerinin sistemlere ait açık portları ve hizmetleri belirleyerek olası güvenlik açıklarını değerlendirmelerine olanak tanır. Yaygın olarak kullanılan Nmap parametreleri ve örnek kullanımları Tablo 2.1'de verilmiştir.

Tablo 2.1: Nmap Parametrelerinin Tanımları ve Örnek Kullanımları

Parametre	Tanım	Örnek Kullanım
-sn	Port taramasını devre dışı bırakarak aktif hostların tespiti için sadece ping atar.	nmap -sn 192.168.1.0/24
-Pn	Ping göndermeden tarar. Her IP adresini aktif kabul eder.	nmap -Pn 192.168.1.27
-PS	TCP SYN ping atarak keşif yapar.	nmap -PS 22,80 192.168.1.0/24
-PA	TCP ACK ping atarak keşif yapar.	nmap -PA 22 192.168.1.0/24
-PU	UDP ping atarak keşif yapar.	nmap -PU 53 192.168.1.0/24
-PE	ICMP Echo Request ping atarak keşif yapar.	nmap -PE 192.168.1.0/24
-PP	ICMP Timestamp ping atarak keşif yapar.	nmap -PP 192.168.1.0/24
-n	Asla DNS çözümlemesi yapmaz.	nmap -n 192.168.1.27
-R	Her zaman DNS çözümlemesi yapar.	nmap -R 192.168.1.27
—traceroute	Traceroute özelliğini aktif hâle getirir.	nmap —traceroute 192.168.1.27
-sS	TCP SYN taraması yapar. Gizli tarama olarak bilinir.	nmap -sS 192.168.1.27
-sT	TCP bağlantılı tarama yapar.	nmap -sT 192.168.1.27
-sA	TCP ACK taraması yapar.	nmap -sA 192.168.1.27

-sU	UDP taraması yapar.	nmap -sU 192.168.1.27
-sN	TCP NULL taraması yapar.	nmap -sN 192.168.1.27
-sF	TCP FIN taraması yapar.	nmap -sF 192.168.1.27
-sO	IP protokolü taraması yapar.	nmap -sO 192.168.1.27
-p	Belirtilen portları tarar.	nmap -p 22,80 192.168.1.27
-F	Daha hızlı tarama yapar. En çok kullanılan 100 portu tarar.	nmap -F 192.168.1.27
—top-ports <sayı>	Belirtilen sayı kadar sık kullanılan portları tarar.	nmap —top-ports 10 192.168.1.27
-sV	Açık portta çalışan servisin versiyonunu tespit eder. -sC ile birlikte kullanılır.	nmap -sV 192.168.1.27
-sC	-sV ile versiyon tespiti yapılırken nmap scriptlerini kullanır.	nmap -sC 192.168.1.27
-O	İşletim sistemi bilgisini tespit eder.	nmap -O 192.168.1.27
-v, -vv	Ekranda gösterilecek detayları artırır.	nmap -v 192.168.1.27
—reason	Port durumunun nedenini gösterir.	nmap —reason 192.168.1.27
—open	Sadece açık portları gösterir.	nmap —open 192.168.1.27
-p-	Bir IP üzerinde bulunması muhtemel 0-65535 arasındaki tüm portları tarar.	nmap -p- 192.168.1.27
-A	Agresif tarama yapar.	nmap -A 192.168.1.27
-T	Zamanlama şablonu belirtir.	nmap -T4 192.168.1.27

2.2.3. Nmap Tarama Teknikleri

Nmap, ağ güvenliği alanında yaygın olarak kullanılan güçlü bir araçtır ve çeşitli tarama teknikleriyle ağların güvenliğini değerlendirmek için kullanılır. Bu teknikler; ağ üzerindeki cihazları ve servisleri keşfetmek, açık portları tespit etmek ve potansiyel güvenlik açıklarını ortaya çıkarmak için oldukça önemlidir. Nmap tarama teknikleri; IP tarama, port tarama ve portlarda servis tarama olmak üzere üç şekilde sınıflandırılır.

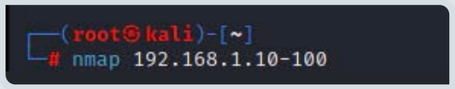
2.2.3.1. IP Tarama Teknikleri

IP adresi, IP adres aralıkları ve ağ adresleri kullanılarak yapılan tarama tekniğidir.

5. UYGULAMA

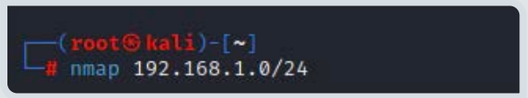
İşlem adımlarına göre lokal ağınızdaki IP adreslerinin en bilinen 1000 portunu tarama işlemini gerçekleştiriniz.

1. Adım: Kali Linux işletim sistemi terminalini ve Nmap aracını kullanarak 192.168.1.10 ve 192.168.1.100 IP adres aralığının taramasını yapan komutu giriniz (Görsel 2.19).



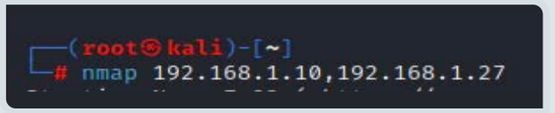
Görsel 2.19: IP adres aralığının taramasını yapan nmap komutu

2. Adım: Kali Linux işletim sistemi terminalini ve Nmap aracını kullanarak 192.168.1.0 ağının taramasını yapan komutu giriniz (Görsel 2.20).



Görsel 2.20: Ağ taraması yapan nmap komutu

3. Adım: Kali Linux işletim sistemi terminalini ve Nmap aracını kullanarak 192.168.1.10 ve 192.168.1.27 IP adreslerinin taramasını yapan komutu giriniz (Görsel 2.21).



Görsel 2.21: IP adreslerinin taramasını yapan nmap komutu

SIRA SİZDE

scanme.nmap.org alan adının Nmap taramasını gerçekleştiriniz ve doğru parametreyi kullanarak sonuçların detaylı bir şekilde verilmesini sağlayınız.

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız. Çalışmanızı bir ders saati içinde tamamlayınız.

KONTROL LİSTESİ

DEĞERLENDİRME ÖLÇÜTLERİ	EVET	HAYIR
Kali Linux işletim sistemi terminalini açtı.		
Nmap aracını kullanarak scanme.nmap.org alan adını uygun parametrelerle taradı.		
Zamanı verimli kullandı.		

2.2.3.2. Port Tarama Teknikleri

Hedef sistemlere ait portları taramak amacıyla kullanılan tekniklerdir.

6. UYGULAMA

İşlem adımlarına göre lokal ağınızdaki aktif IP adreslerinin tespitini yapan tarama işlemini gerçekleştiriniz.

1. Adım: Kali Linux işletim sistemi terminalini ve Nmap aracını kullanarak, 192.168.87.0/24 ağında **-sn** parametresiyle ping atıp aktif hostları belirleyen komutu giriniz (Görsel 2.22).

```
┌──(root㉿kali)-[~]
└─# nmap -sn 192.168.87.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-10 10:22 EDT
Nmap scan report for 192.168.87.2
Host is up (0.00013s latency).
MAC Address: 00:50:56:F8:8A:08 (VMware)
Nmap scan report for 192.168.87.254
Host is up (0.00015s latency).
MAC Address: 00:50:56:FD:3C:D9 (VMware)
Nmap scan report for 192.168.87.129
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 6.21 seconds
```

Görsel 2.22: Nmap ile aktif host taraması

2. Adım: Tarama sonucunda aktif olan hostlardan birinin (192.168.87.129) 80 numaralı portunun açık veya kapalı olduğunu belirleyen komutu giriniz (Görsel 2.23).

```
┌──(root㉿kali)-[~]
└─# nmap -p 80 -n 192.168.87.129
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-10 10:29 EDT
Nmap scan report for 192.168.87.129
Host is up (0.000082s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Görsel 2.23: Nmap ile port taraması

SIRA SİZDE

Lokal ağınızda aktif olan hostların taramasını yapınız. Aktif hostlarda 80 ve 443 numaralı portların açık olup olmadığını tarayan komutu giriniz. Ayrıca seçeceğiniz aktif bir hostun açık portlarının neler olduğunu **-open** parametresiyle görüntüleyen komutu giriniz.

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız. Çalışmanızı bir ders saati içinde tamamlayınız.

KONTROL LİSTESİ

DEĞERLENDİRME ÖLÇÜTLERİ	EVET	HAYIR
Kali Linux işletim sistemi terminalini açtı.		
Lokal ağdaki aktif hostları tespit etti.		
Aktif olan hostların 80 ve 443 numaralı portlarını kontrol etti.		
Aktif olan hostlardan birinin açık olan portlarını görüntüledi.		
Zamanı verimli kullandı.		

2.2.3.3. Portlarda Servis Tarama Teknikleri

Hedef sistemlere ait portlardaki servisleri taramak amacıyla kullanılan tekniklerdir.

7. UYGULAMA

İşlem adımlarına göre lokal ağınızdaki 192.168.87.129 hostu üzerinde servis tarama işlemini gerçekleştiriniz.

1. Adım: Kali Linux işletim sistemi terminalini ve Nmap aracını kullanarak 192.168.87.129 hostunda **–script** parametresiyle zafiyet tespiti yapmak için 445 numaralı port üzerinden **microsoft-ds** servisini kontrol ediniz (Görsel 2.24).

```
┌──(root㉿kali)-[~]
└─# nmap -n -p 445 --script smb-vuln-ms17-010 192.168.87.129
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-10 10:35 EDT
Nmap scan report for 192.168.87.129
Host is up (0.000061s latency).
```

Görsel 2.24: Windows işletim sisteminde microsoft-ds servisini tarama

2. Adım: Yapılan servis sorgusunun sonucunu görüntüleyiniz (Görsel 2.25).

```
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 2.25: Servis tarama işleminin sonucu

2.2.4. Online Port Tarama Teknikleri

Port tarama işlemi, Kali Linux işletim sistemi ve Nmap aracıyla yapıldığı gibi çeşitli çevrimiçi araçlar kullanılarak da yapılabilir. Online port tarama için **https://viewdns.info/portscan** web sitesi kullanılabilir (Görsel 2.26).

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. HT 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 2.26: Online port taramasının sonucu

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

1. ( ) Whois sorgusuyla IP adresi bilgisi elde edilemez.
2. ( ) Saldırganlar, SHODAN'ı pasif keşif aşamasında hedef sistemlerin altyapısına erişebilmek ve daha ayrıntılı bilgi toplayabilmek için kullanılır.
3. ( ) Google Dorking, belirli arama sorguları ve operatörleri kullanarak internet üzerinde gizli veya erişilmesi zor bilgilere ulaşmayı sağlar.
4. ( ) Network mapping (Ağ haritalama), ağın fiziksel ve mantıksal yapısını detaylı bir şekilde görsel olarak belgelendirir.
5. ( ) Pasif bilgi toplama sırasında hedef sistemin bilgisi olmaz.

B) Aşağıdaki sorularda doğru cevabı işaretleyiniz.

6. Aşağıdakilerden hangisi belirli bir IP adresindeki açık portları taramak amacıyla kullanılan nmap komutunun parametresidir?

A) -n B) -o C) -R D) -Ss E) - T

7. Aşağıdakilerden hangisi web sayfasının geçmiş anlık görüntülerine ulaşmak için kullanılır?

A) Archive.org B) Kali.linux C) NS.TOOLS D) Ripe.net E) Shodan.io

8. Aşağıdaki ifadelerden hangisi aktif ve pasif tarama yöntemlerinin farkını doğru bir şekilde açıklar?

A) Aktif tarama, hedef sistemle doğrudan iletişime geçilerek bilgi toplanmasını içerirken pasif tarama, hedef sistemle doğrudan iletişim kurulmadan bilgi toplar.
B) Aktif tarama, sistemlerin ağ üzerindeki trafiğini izleyerek bilgi toplarken pasif tarama ise sadece web sayfalarından veri çeker.
C) Aktif tarama, hedef sistemle doğrudan etkileşim kurarak portları tarar ve sistem yanıtlarını beklerken pasif tarama yalnızca ağda bulunan cihazların yerini belirler ve verileri analiz eder.
D) Pasif tarama, ağ üzerinden veri paketlerini gönderir ve yanıtları toplarken aktif tarama sadece açık kaynaklardan bilgi toplar.
E) Aktif tarama sadece ağ trafiğini izlerken pasif tarama, hedef sistemlere doğrudan saldırı gerçekleştirerek zafiyetleri belirler.

9. Aşağıdaki nmap komutlarından hangisi belirli bir IP adresinde açık olan HTTP portunu tarar?

A) nmap -T4 192.168.1.1 B) nmap -sS 192.168.1.1 C) nmap -O 192.168.1.1
D) nmap -sP 192.168.1.1 E) nmap -p 80 192.168.1.1

10. İnternetteki cihazları ve hizmetleri tarayarak bu cihazlara ait açık portlar, çalışan hizmetler ve diğer özellikler hakkında bilgi sağlayan web sitesi aşağıdakilerden hangisidir?

A) Archive.org B) Kali Linux C) NS.TOOLS D) Shodan.io E) Whois.com

NOT

3. ÖĞRENME BİRİMİ

SNIFFING YÖNTEMİ VE UYGULAMALARI

KONULAR

3.1. SNIFFER ARAÇLARINI KULLANMA

3.2. SNIFFING SALDIRILARININ TESPİTİ

NELER ÖĞRENECEKSİNİZ?

- Ağ üzerindeki protokolleri dinleme
- Wireshark programıyla ağı dinleme
- Ettercap komutlarını kullanma
- TCPDump komutlarını kullanma
- MAC flooding (MAC seli) saldırı yöntemi ve bu saldırıya karşı alınacak önlemleri uygulama
- ARP poisoning (ARP zehirlenmesi) saldırı yöntemi ve bu saldırıya karşı alınacak önlemleri uygulama

ANAHTAR KAVRAMLAR

ARP poisoning, Kali Linux, MAC flooding, Man in the Middle, sniffing, TCPDump, Wireshark

HAZIRLIK ÇALIŞMALARI

1. Şifrelenmemiş bir ağ trafiğini dinleyen kişiler hangi bilgileri ele geçirebilir? Düşüncelerinizi arkadaşlarınızla paylaşınız.
2. Kamuya açık bir ağda sosyal medya hesaplarınıza girerken veya online alışveriş yaparken nelere dikkat edersiniz? Düşüncelerinizi arkadaşlarınızla paylaşınız.
3. Ağınızdaki kritik verilerin güvenliğini sağlamak için ağ trafiğini izlerken kullanacağınız teknikler ve odaklanacağınız potansiyel güvenlik açıkları neler olabilir? Düşüncelerinizi arkadaşlarınızla paylaşınız.

3.1. SNIFFER ARAÇLARINI KULLANMA

Sniffing ifadesinin Türkçe karşılığı teknik anlamda koklama veya dinlemedir. Bu yöntem, bir ağ üzerindeki paketleri izlemek veya yakalamak için kullanılır. Sniffing, bir ağdaki trafiği gözlemlemek ve içeriğini analiz etmek amacıyla yapılır. Saldırganlar açısından **snif etmek** terimi özellikle ağ trafiğini izinsiz olarak izlemek ve gizli bilgileri ele geçirmek için kullanılan zararlı bir yöntem olarak bilinir. Örneğin saldırganlar; şifrelenmemiş verileri yakalayarak kullanıcı adı, parola, kredi kartı bilgileri vb. hassas verileri elde etmek için bu yöntemi kullanabilir (Görsel 3.1).

Görsel 3.1: Bilgisayar ağlarının izlenmesi

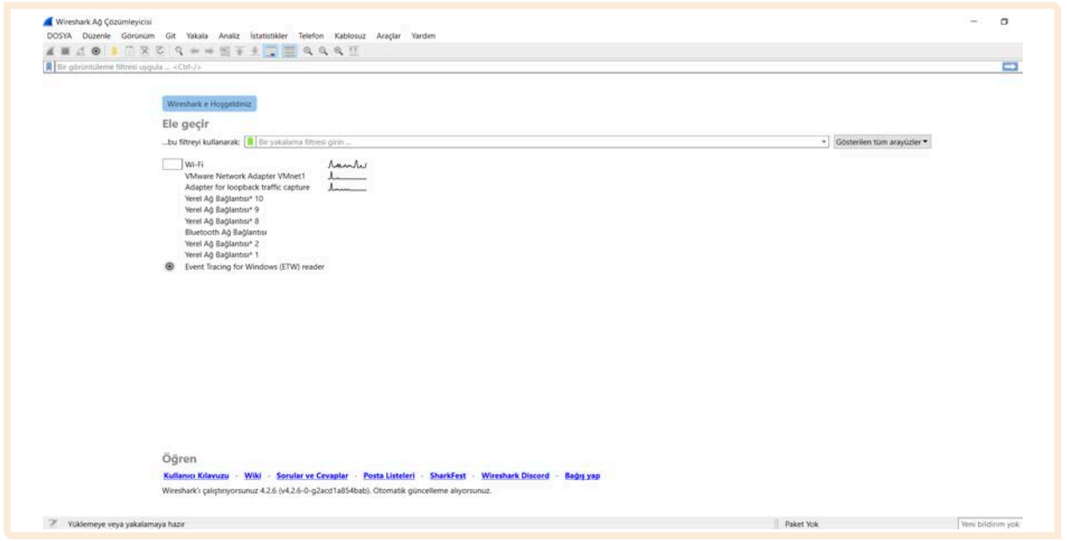
Sniffer araçları, ağ güvenliği ve trafiğinin izlenmesinde kritik rol oynayan yazılım ve donanımlardır. Bu araçlar, ağ üzerindeki veri paketlerini yakalayarak detaylı analizler yapmayı mümkün kılar. Böylece ağ yöneticileri; performans takibi, sorun giderme, güvenlik açıklarını tespit etme gibi görevleri yerine getirebilir. Bu güçlü araçlar, kötü niyetli kişiler tarafından izinsiz veri toplama ve hassas bilgilere erişme amacıyla da kullanılabilir. Bu nedenle sniffer araçlarının kullanımı, yasal ve etik sorumluluklar çerçevesinde titizlikle değerlendirilmelidir. Sniffing işlemlerinde birçok araç kullanılmakla birlikte yaygın olarak kullanılan bazı uygulamalar şunlardır:

- Wireshark
- TCPDump
- Ettercap
- Cain & Abel

NOT İlgili araçlar, ağ güvenliği uzmanları tarafından yasal ve etik amaçlarla kullanıldığında son derece yararlı olabilir ancak kötü niyetli kişiler tarafından kullanılırsa ciddi güvenlik tehditlerine yol açabilir.

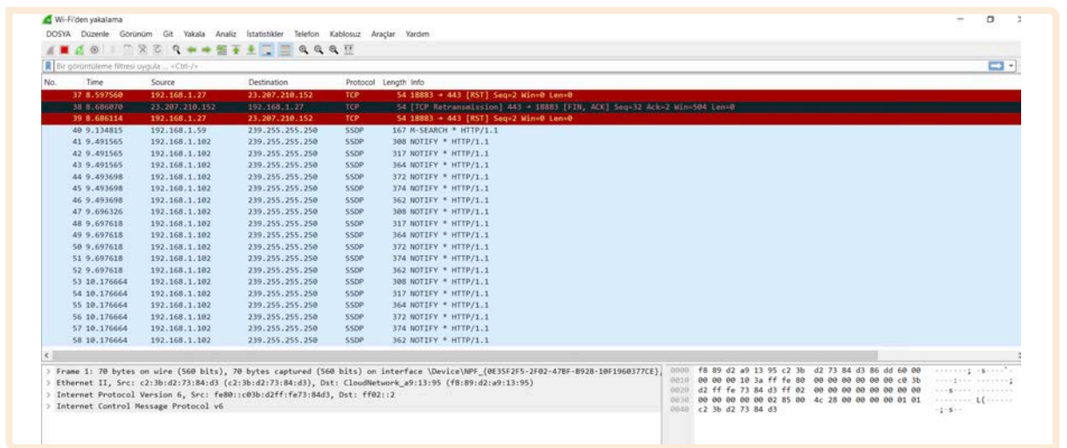
3.1.1. Wireshark

Wireshark, ağ trafiğini analiz etmek için kullanılan açık kaynak kodlu bir yazılımdır. Bu program, ağ üzerindeki veri paketlerini gerçek zamanlı olarak yakalayarak kullanıcıya ağ iletişiminin detaylı bir görüntüsünü sunar. Wireshark; ağ sorunlarını teşhis etmek, performans analizleri yapmak ve güvenlik açıklarını belirlemek için ideal bir araçtır. Bu aracın paketlerin içeriklerini detaylı bir şekilde inceleyebilme yeteneği sayesinde ağ üzerindeki veri akışını anlamak ve ağ yapılandırmalarında karşılaşılan sorunları çözmek mümkün hâle gelir. Bu özellikleriyle Wireshark hem ağ yöneticileri hem de güvenlik uzmanları için vazgeçilmez bir yardımcıdır (Görsel 3.2).



Görsel 3.2: Wireshark programının ana ekranı

Wireshark'ta filtreleme, büyük miktarda ağ trafiği arasından yalnızca belirli verileri veya olayları izlemek ve analiz etmek amacıyla kullanılır. Filtreleme özellikle karmaşık ağlar ve yoğun trafik altında çalışan sistemler için önemli bir işlevdir. Tüm ağ trafiğini incelemek yerine sadece ilgili spesifik veriyi görmeyi sağlar (Görsel 3.3).



Görsel 3.3: Wireshark ile paketlerin dinlenmesi ve filtrelenmesi

Wireshark ile filtrelemenin kullanım amaçları şunlardır:

Belirli Protokolleri İzleme: Wireshark'ta filtreleme yapılarak sadece belirli protokoller (HTTP, DNS, TCP, UDP) üzerinde akan trafik incelenebilir. Bu durum, bir ağ sorununu teşhis ederken veya belirli bir protokolün performansını değerlendirirken oldukça faydalıdır.

Kaynak ve Hedef IP Adreslerini İzleme: Filtreleme sayesinde belirli bir kaynak veya hedef IP adresinden gelen/verilen trafik gözlemlenebilir. Bu durum, belirli cihazlar arasındaki iletişimi incelemek veya bir saldırganın IP adresini tespit etmek için kullanışlıdır.

Port Bazlı Trafik Analizi: Ağ trafiği belirli portlar üzerinden süzülerek sadece web trafiği (Port 80 veya Port 443), e-posta trafiği (Port 25) vb. izlenebilir. Bu işlem, belirli servislerdeki sorunları tespit etme veya izinsiz erişim denemelerini yakalama konusunda yardımcı olabilir.

Şüpheli Trafiği Tespit Etme: Wireshark'ta filtreleme yapılarak şüpheli paketler veya saldırı girişimleri (ARP poisoning, SYN flooding) tespit edilebilir. Bu tür filtreler, ağ güvenliğini sağlamak için kritik öneme sahiptir.

Veri Hacmini Azaltma: Büyük ağlarda tüm trafiğin kaydedilmesi ve analiz edilmesi zor olabilir. Filtreleme, gereksiz verilerin ayıklanarak sadece ilgili trafiğin kaydedilmesine olanak tanır. Böylece analiz süreci hızlanır ve daha verimli hâle gelir.

Performans İzleme: Filtreleme kullanılarak belirli bir cihazın veya servisin ağ üzerindeki performansı izlenebilir ve veri aktarım hızları, gecikmeler veya paket kayıpları analiz edilebilir.

Wireshark ile yapılabilecek filtreleme işlemleri ve örnek kullanımlarından bazıları Tablo 3.1'de görülür.

Tablo 3.1: Örnek Filtre Kullanımları

FİLTRE	AÇIKLAMA
ip.addr == [IP Adresi]	Belirli bir IP adresinden gelen ve giden tüm trafiği gösterir. **Örnek:** ip.addr == 192.168.1.10
ip.src == [IP Adresi]	Belirli bir IP adresinden kaynaklanan trafiği gösterir. **Örnek:** ip.src == 192.168.1.10
ip.dst == [IP Adresi]	Belirli bir IP adresine yönelen trafiği gösterir. **Örnek:** ip.dst == 192.168.1.10
tcp.port == [Port Numarası]	Belirli bir TCP portunu kullanan trafiği gösterir. **Örnek:** tcp.port == 80 (HTTP trafiği)
udp.port == [Port Numarası]	Belirli bir UDP portunu kullanan trafiği gösterir. **Örnek:** udp.port == 53 (DNS trafiği)
tcp.flags.syn == 1 && tcp.flags.ack == 0	TCP bağlantı kurulum sürecindeki SYN paketlerini gösterir (SYN flood saldırılarını tespit etmek için).
tcp.flags.reset == 1	TCP bağlantılarında RESET (RST) bayrağını içeren paketleri gösterir.
http	HTTP protokolü üzerinden yapılan trafiği gösterir.
dns	DNS protokolü üzerinden yapılan trafiği gösterir.
frame.len > [Boyut]	Belirli bir uzunluktan büyük paketleri gösterir. **Örnek:** frame.len > 1000 (1000 bayttan büyük paketler)
icmp	ICMP protokolü üzerinden yapılan trafiği gösterir.

Filtreleme yapılırken kullanılan karşılaştırma ve mantıksal operatörlere ait örnekler Tablo 3.2'de görülür.

Tablo 3.2: Karşılaştırma ve Mantıksal Operatörlerin Örnek Kullanımları

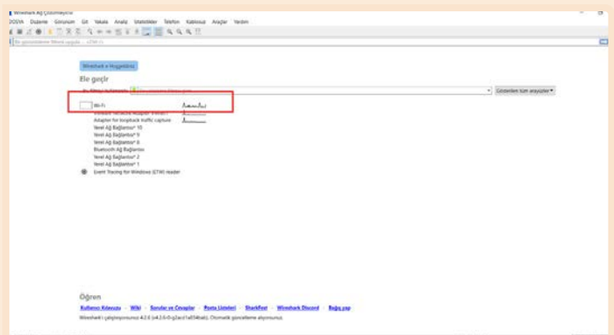
KARŞILAŞTIRMA VE MANTIKSAL OPERATÖRLER	ÖRNEK KULLANIM
== (eşitlik)	ip.src == 192.168.1.1 192.168.1.1 IP adresinden gelen trafiği filtreler.
!= (eşit değil)	ip.src != 192.168.1.1 192.168.1.1 IP adresinden gelmeyen trafiği filtreler.
> (büyük)	frame.len > 1000 1000 bayttan büyük olan paketleri filtreler.
< (küçük)	frame.len < 100 100 bayttan küçük olan paketleri filtreler.
>= (büyük veya eşit)	tcp.port >= 1024 1024 veya daha büyük port numaralarına sahip trafiği filtreler.
<= (küçük veya eşit)	tcp.port <= 80 80 veya daha küçük port numaralarına sahip trafiği filtreler.
&& (ve)	ip.src == 192.168.1.1 && tcp.port == 80 Kaynak IP adresi 192.168.1.1 olan VE 80 numaralı portu kullanan trafiği filtreler.
|| (mantıksal veya)	ip.src == 192.168.1.1 || ip.dst == 192.168.1.2 Kaynak IP adresi 192.168.1.1 olan VEYA hedef IP adresi 192.168.1.2 olan tüm trafiği filtreler.

1. UYGULAMA

İşlem adımlarına göre HTTP protokolünü kullanan bir web sitesine lokal ağınızdan yapılan oturum açma isteğini Wireshark programı ile dinleyiniz.

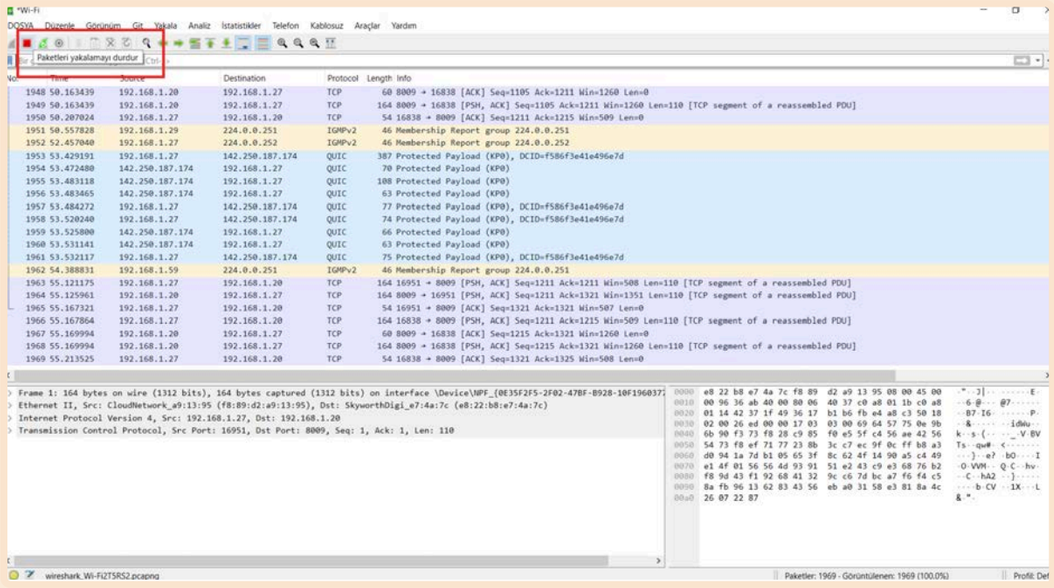
1. Adım: Wireshark programını açtıktan sonra Görsel 3.4'teki Wi-Fi seçeneğine çift tıklayınız.

NOT Bu aşamada Wireshark programı ile **Wi-Fi** ağını dinleme işlemi başlar.



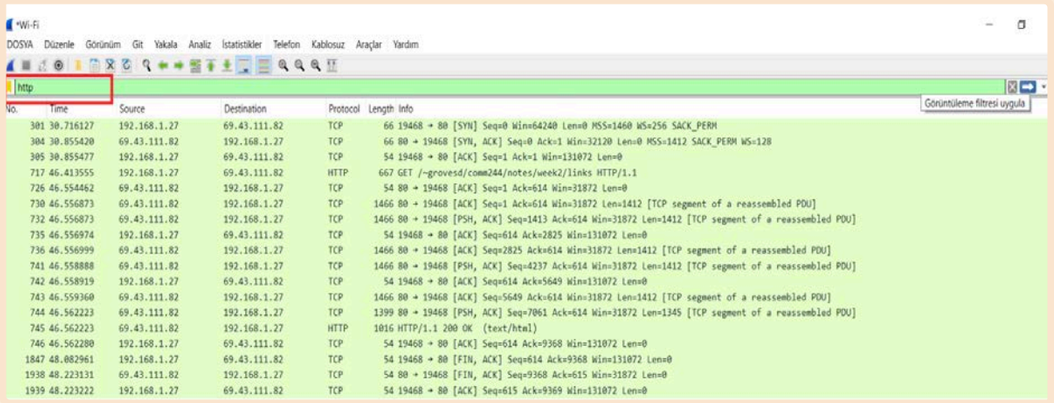
Görsel 3.4: Wireshark ile kablosuz ağ trafiğinin dinlenmesi

2. Adım: Ağ üzerinde HTTP protokolünü oluşturmak için herhangi bir web tarayıcısını açarak farklı web sitelerinde geziniz ve Görsel 3.5'teki **Stop Capture (Dinlemeyi Durdur)** düğmesine tıklayınız.



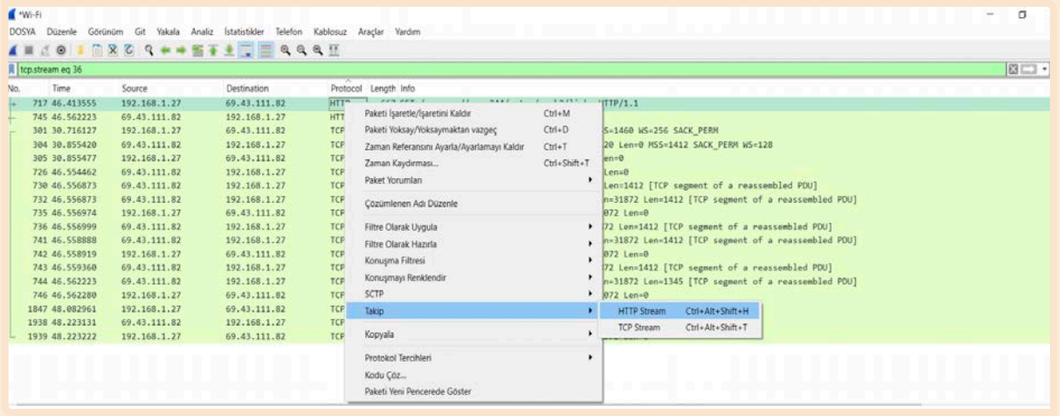
Görsel 3.5: Ağ trafiğini izlemenin durdurulması

3. Adım: HTTP trafiğini izlemek için filtreleme alanına **http** yazarak filtreleme işlemini uygulayınız (Görsel 3.6).



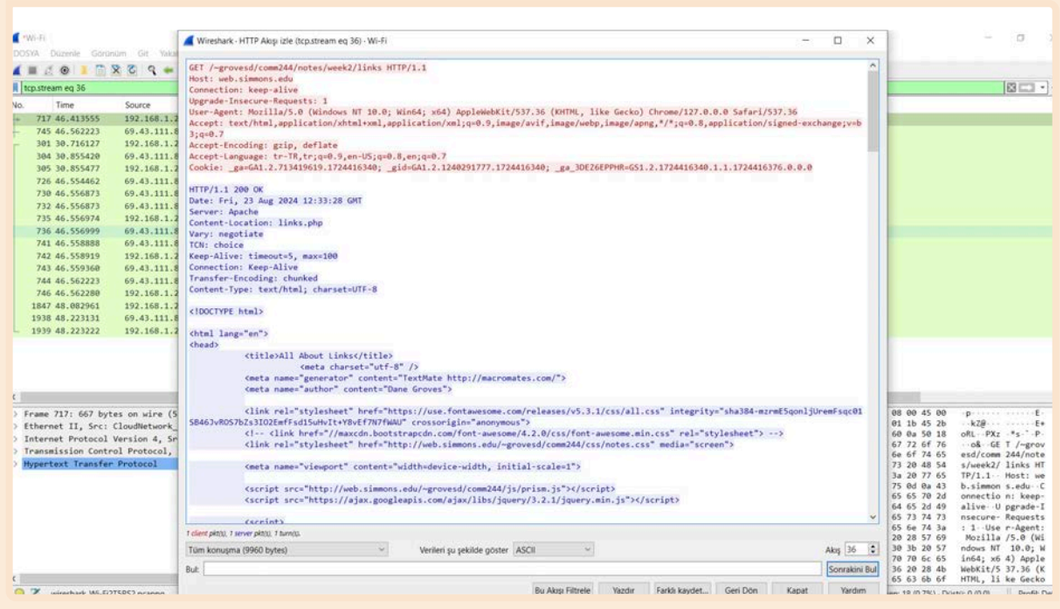
Görsel 3.6: HTTP trafiğinin filtrelenmesi

4. Adım: Görüntülemek istediğiniz HTTP protokolünün üzerine gelerek sağ tıklayınız. Görsel 3.7'deki gibi **Takip** ve **HTTP Stream** seçeneklerine tıklayınız.



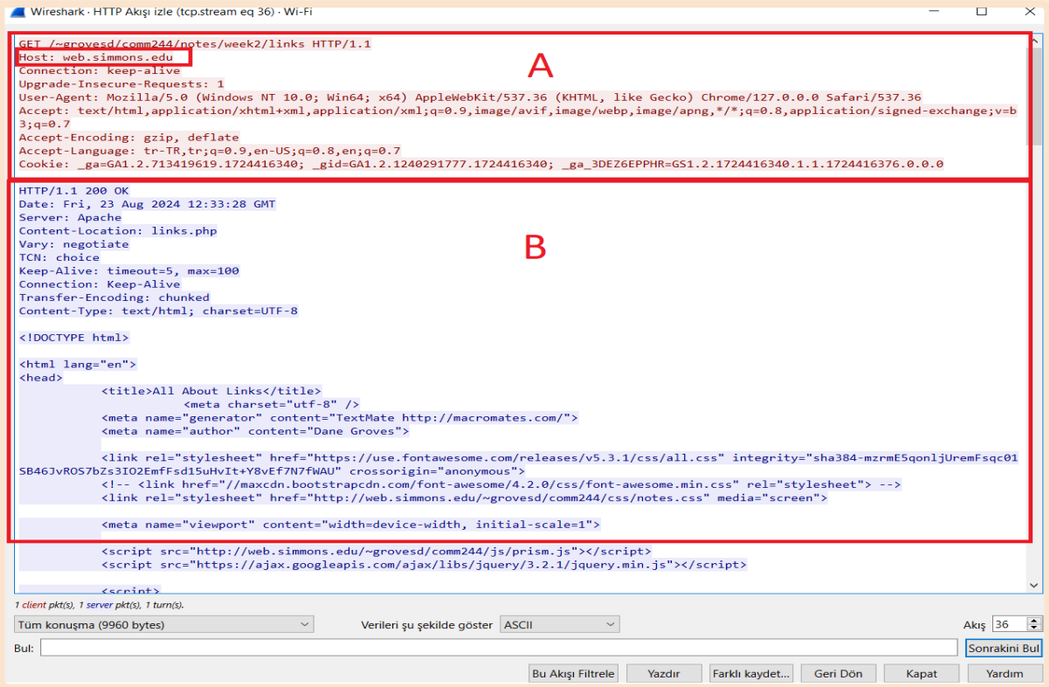
Görsel 3.7: HTTP protokolünün içeriğine ulaşılması

5. Adım: Görsel 3.8'deki gibi bir akış izleme sayfası oluşturmak amacıyla izlemek istediğiniz HTTP trafiğini seçiniz.



Görsel 3.8: İzlenen HTTP protokolü

6. Adım: Ağ dinlemesine takılan HTTP protokol içeriğinin Görsel 3.9'daki gibi oluştuğunu gözlemleyiniz.



Görsel 3.9: HTTP trafiğindeki bilgilerin toplanması

SIRA SİZDE

HTTPS protokolü kullanan web sitelerine giriniz ve Wireshark aracılığıyla HTTPS trafiğini filtreleyerek oluşan akışı inceleyiniz.

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız. Çalışmanızı bir ders saati içinde tamamlayınız.

KONTROL LİSTESİ

DEĞERLENDİRME ÖLÇÜTLERİ	EVET	HAYIR
Wireshark ile yerel ağı dinlemeye aldı.		
HTTPS protokolü kullanan sitelerde gezinti yaptı.		
Uygun filtreleme kullanarak HTTPS trafiğinin dinlenmesini ve görüntülenmesini analiz etti.		

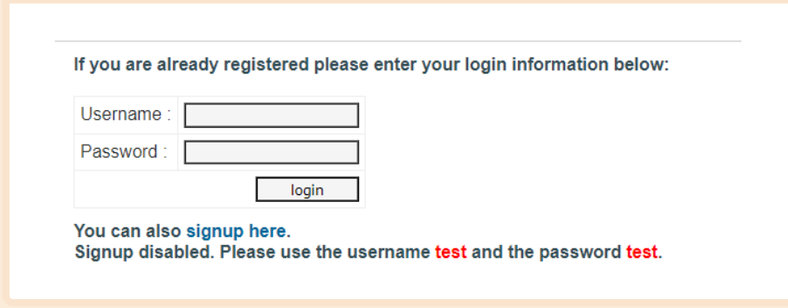
2. UYGULAMA

İşlem adımlarına göre HTTP protokolünü kullanan bir web sitesine giriş işlemi için gerekli oturum bilgilerini Wireshark programı ile ele geçiriniz.

1. Adım: Herhangi bir arama motoruna ait sitede **http login test** araması yapınız ve arama sonuçlarını gösteren listedeki sitelerden birine giriş yapınız.

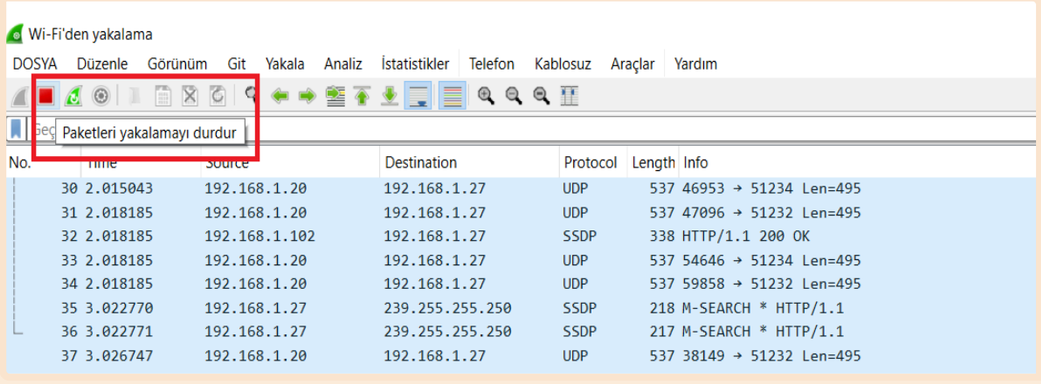
2. Adım: Wireshark uygulamasını açınız ve ağ dinleme işlemini birinci uygulamada gösterildiği gibi başlatınız.

3. Adım: Görsel 3.10'da görüldüğü gibi site üzerinde yer alan formdaki **Username** ve **Password** alanlarını doldurarak **login** düğmesine basınız (Username: medya ve Pasword: medya değerlerini giriniz.).



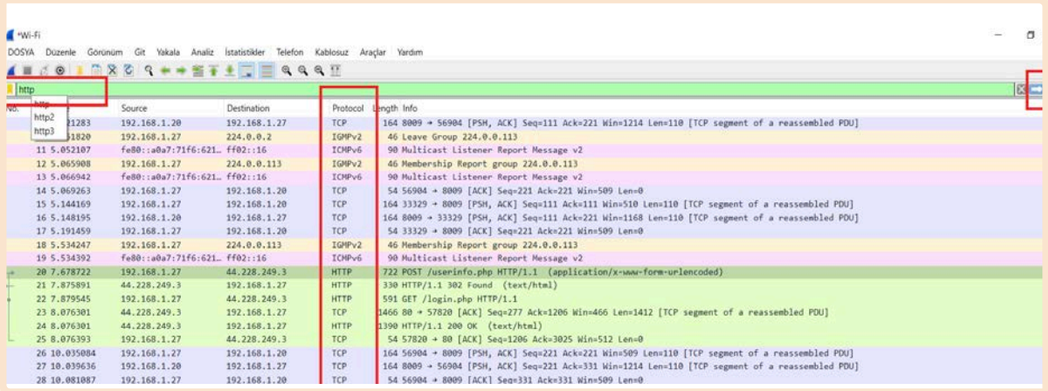
Görsel 3.10: Giriş ekranı

4. Adım: Wireshark programında **Paketleri yakalamayı durdur** düğmesine basınız (Görsel 3.11).



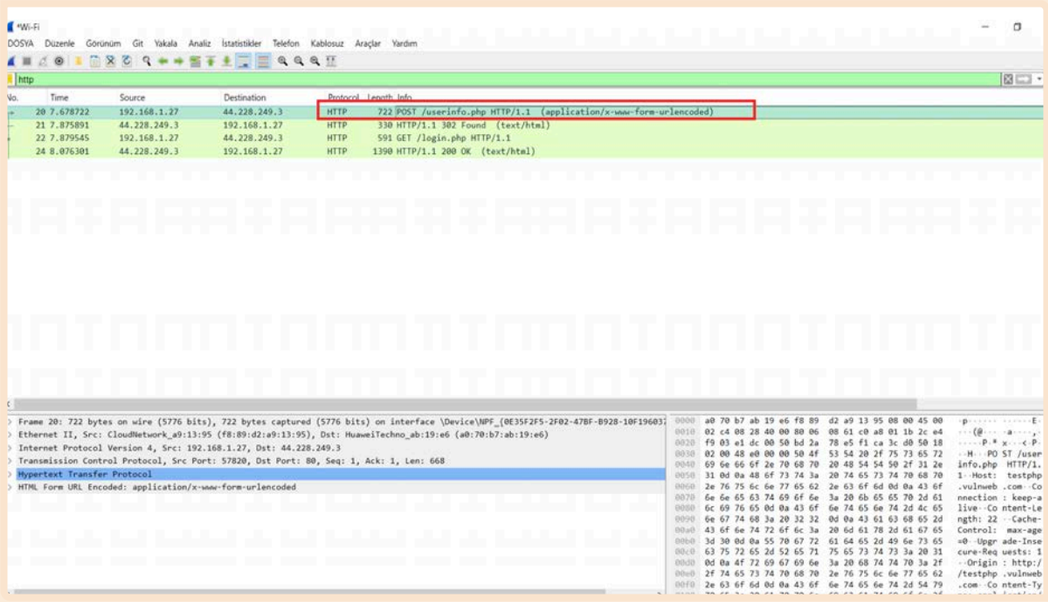
Görsel 3.11: Paketleri yakalamanın durdurulması

5. Adım: HTTP protokolü üzerinde yer alan oturum açma bilgilerine ulaşmak için protokol filtre alanına **http** yazarak filtre uygulayınız (Görsel 3.12).



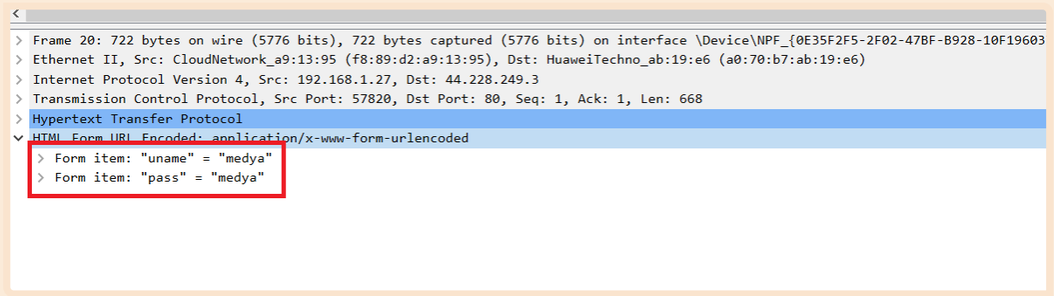
Görsel 3.12: Filtreleme işleminin yapılması

6. Adım: POST edilen userinfo.php sayfası üzerindeki forma girdiğiniz **uname = kullanıcıadı** ve **pass = parola** değerlerine ulaşınız (Görsel 3.13).



Görsel 3.13: Post bilgilerine erişim sağlanması

7. Adım: Kullanıcı adı ve parola bilgilerini görüntüleyiniz (Görsel 3.14).



Görsel 3.14: Kullanıcı adı ve parola bilgilerinin görüntülenmesi

3. UYGULAMA

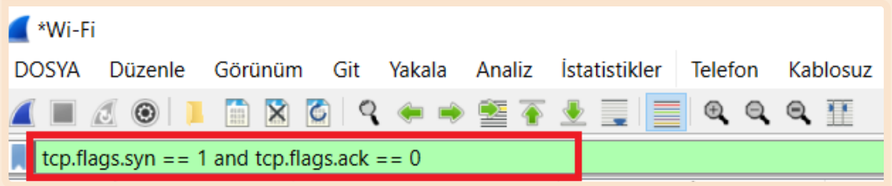
İşlem adımlarına göre Wireshark kullanarak sisteme yapılan SYN taramalarını tespit ediniz.

NOT İzinsiz giriş denemelerinde saldırganlar, açık portları tespit etmek için port taraması yaparlar.

1. Adım: İzinsiz girişlerin tespiti için birinci ve ikinci uygulamada olduğu gibi ağı Wireshark ile izlemeye aldıktan sonra paketlerin akışını durdurunuz.

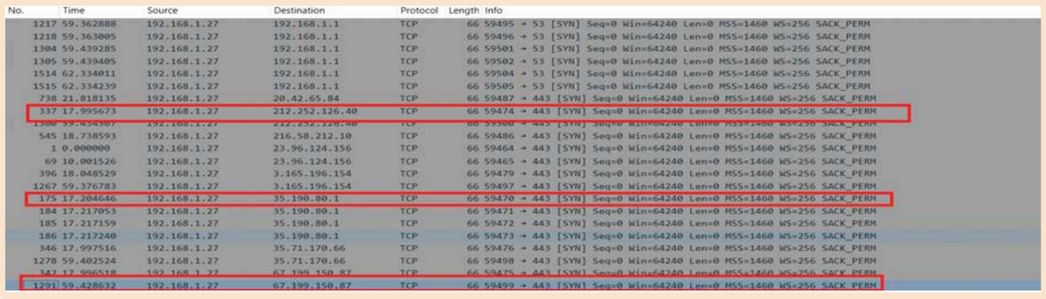
NOT SYN taraması, sisteminize açık portların tespiti için yapılan bir giriş işlemidir. Bu işlem, Nmap gibi aktif tarama yapan uygulamalar veya çeşitli çevrimiçi port tarama uygulamalarıyla yapılabilir.

2. Adım: SYN paketlerinin tespiti için filtreleme alanına Görsel 3.15'teki sorguyu yazınız.



Görsel 3.15: SYN taramalarının tespiti için gerekli sorgu

3. Adım: Yapılan sorgu sonucunda izinsiz girişleri görüntüleyiniz (Görsel 3.16).



Görsel 3.16: İzinsiz girişler

3.1.2. TCPDump

Ağ yönetimi ve güvenliği, ağ trafiğinin ayrıntılı bir şekilde izlenmesini ve analiz edilmesini gerektirir. **TCPDump;** ağ yönetimi ve güvenliğini sağlamak amacıyla geliştirilmiş, komut satırında çalışan ve Linux sistemlerde kurulu şekilde gelen ücretsiz bir araçtır. Bu araç, TCP/IP trafiğini yakalayarak ağ üzerinden geçen veri paketlerini incelemeyi ve analiz etmeyi sağlar. Ağ sorunlarını çözmek, güvenlik açıklarını tespit etmek ve ağ performansını artırmak için vazgeçilmez bir araç olarak hem ağ yöneticileri hem de siber güvenlik profesyonelleri tarafından yaygın olarak kullanılır. TCPDump, kullanıcıya trafiği filtreleme ve detaylı bir şekilde inceleme imkânı sunar. Kali Linux işletim sisteminde TCPDump komutlarını kullanmak için root (yönetici) yetkisine sahip olmak gerekir. TCPDump komutunun yaygın şekilde kullanılan parametreleri ve bu parametrelerin açıklamaları Tablo 3.3'te görülür.

Tablo 3.3: TCPDump Parametreleri ve Açıklamaları

PARAMETRE ADI	AÇIKLAMA
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 [Address Resolution Protocol (Adres Çözümleme Protokolü)] paketlerini listeler.
tcpdump -p	TCPDump ile yalnızca dinleme yapılan arabirime gelen paketleri yakalamak amacıyla seçici olmayan moddan çıkmayı sağlar.
tcpdump -e	Yakalanan paketlerin ikinci katman bilgilerini, bir başka deyişle MAC adreslerini elde etmeyi sağlar.
tcpdump -w "dosya ismi"	İstenilen paketleri bir dosya hâlinde kaydeder. Kaydedilen bu dosya, Wireshark vb. programlarla açılarak incelenebilir.
tcpdump -r "dosya ismi"	Dosya hâlinde olan bir paket listesini açar.

SIRA SİZDE

Kali Linux işletim sisteminde bulunan TCPDump uygulamasını kullanarak, eth0 arayüzü üzerindeki tüm trafiği dinleyip yakalayınız.

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız. Çalışmanızı bir ders saati içinde tamamlayınız.

KONTROL LİSTESİ

DEĞERLENDİRME ÖLÇÜTLERİ	EVET	HAYIR
Kali Linux işletim sistemi komut panelini açtı.		
TCPDump komutlarını kullanarak eth0 arayüzünü dinledi.		
Uygun parametreleri kullanarak dinlenen trafiği listeledi.		

3.1.3. Ettercap

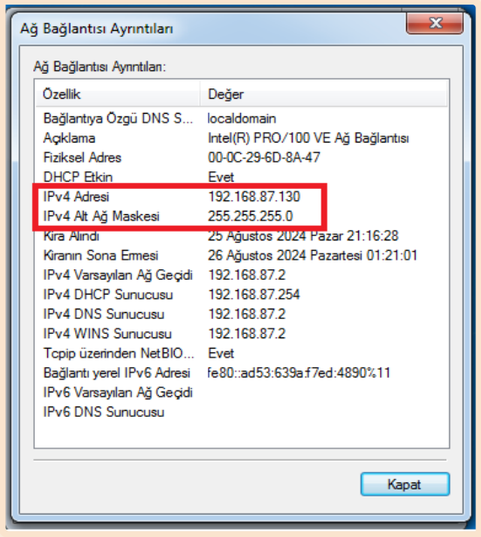
Ettercap, Ortadaki Adam [Man in the Middle (MitM)] saldırılarını gerçekleştirmek ve ağ trafiğini analiz etmek için kullanılan güçlü bir güvenlik ve ağ protokolü aracıdır. Hem grafiksel hem de komut satırı arayüzüne sahip Ettercap; ağ üzerinde dolaşan paketleri yakalayabilir, analiz edebilir ve değişikliğe uğratabilir. Bu yetenekleri sayesinde ağ güvenliği uzmanları, ağ üzerinde bulunan güvenlik açıklarını belirleyebilir ve bu açıkları kapatmak için gerekli önlemleri alabilir. Ettercap özellikle ARP poisoning, DNS poisoning, MAC flooding, HTTPS gibi çeşitli MitM saldırıları için kullanılabilir.

MitM; bir saldırganın iki taraf arasında geçen iletişime gizlice dâhil olarak veri alışverişini dinlemesi, manipüle etmesi veya yönlendirmesiyle gerçekleşen bir siber saldırı türüdür. İletişimlerinin güvenli olduğunu düşünen kurbanlar, araya giren bir saldırgan tarafından izlendiklerinin farkında olmazlar. Bu süreçte saldırgan; şifreler, oturum bilgileri, kişisel veriler gibi hassas bilgileri ele geçirebilir veya iletişimi değiştirerek yanlış bilgi aktarımı sağlayabilir. MitM saldırıları özellikle güvenli olmayan ağlarda, kamuya açık Wi-Fi ağlarında ve zayıf şifreleme yöntemleri kullanılan sistemlerde kullanıcılar için büyük bir risk teşkil eder.

4. UYGULAMA

İşlem adımlarına göre Kali Linux cihazınızda kurulu gelen **ettercap-graphical** uygulamasını kullanarak, lokal ağınızda bulunan Windows 7 işletim sistemli bir istemci cihazın ağ geçidiyle arasına girip istemci cihazın HTML site oturum bilgilerini ele geçiren uygulamayı yapınız.

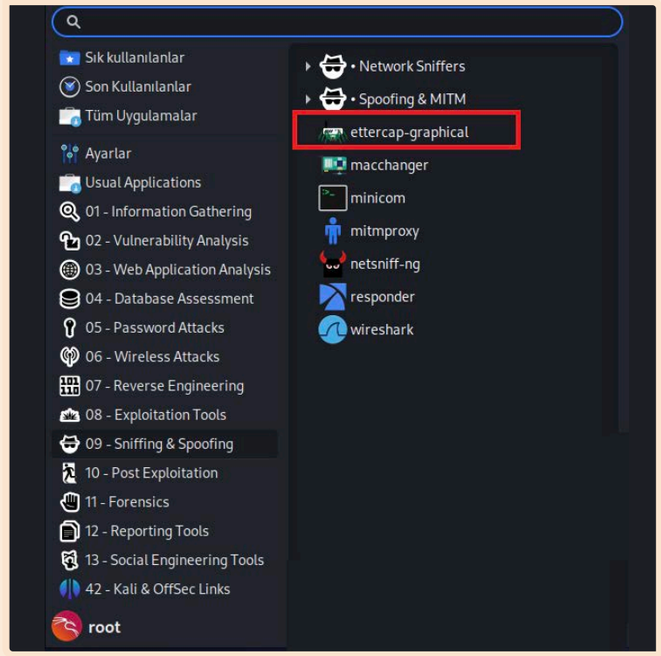
1. Adım: Windows 7 kurulu istemci bilgisayarı ile Kali Linux kurulu bilgisayarın aynı ağda olduğunu doğrulayınız (Görsel 3.17 ve Görsel 3.18).



Görsel 3.17: Windows 7 IP yapılandırması

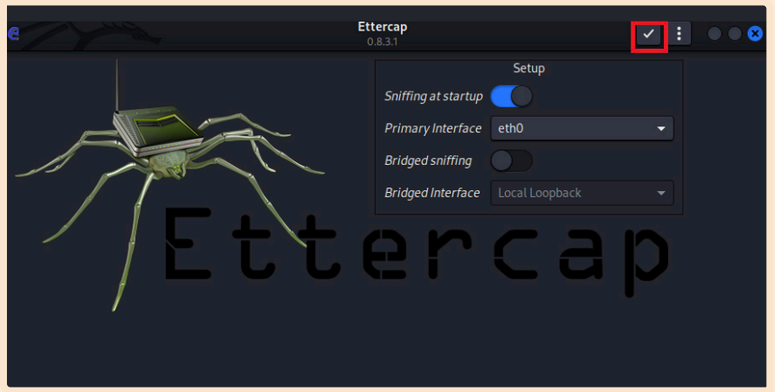
Görsel 3.18: Kali Linux IP yapılandırması

2. Adım: Kali Linux işletim sistemi yüklü cihazdan **Sniffing & Spoofing** araçları arasında kurulu gelen **ettercap-graphical** isimli uygulamayı açınız (Görsel 3.19).



Görsel 3.19: Kali Linux işletim sisteminde uygulamanın açılması

3. Adım: Görsel 3.20'deki ayarları kontrol edip belirtilen onay işaretine tıklayınız.



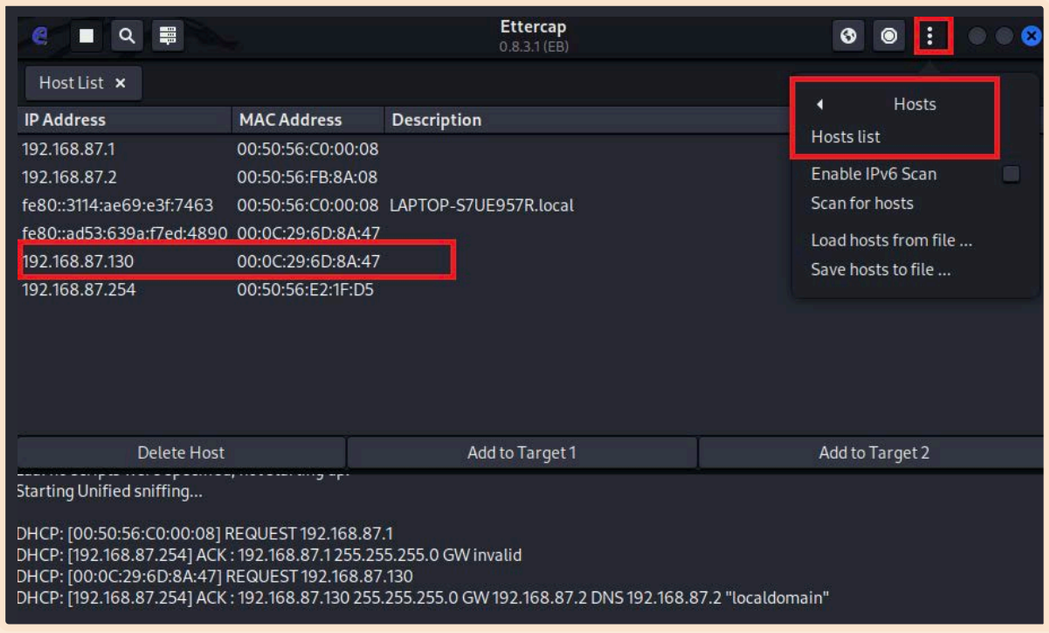
Görsel 3.20: Ettercap ile ağın izlenmesine onay verilmesi

4. Adım: Verilen onayın ardından lokal ağınızda bulunan diğer cihazları izleme işlemine başlayan Ettercap programının listelediği verileri gözlemleyiniz (Görsel 3.21).

Görsel 3.21: İzleme işleminin başlatılması

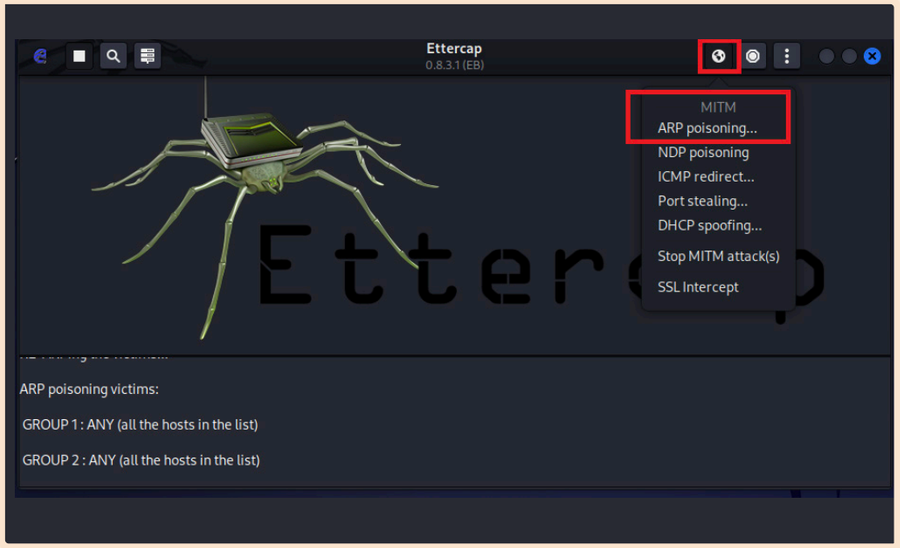
5. Adım: Görsel 3.22'de işaretlenmiş alana tıklayarak **host** listesini gözlemleyiniz.

NOT Host listesinde MitM saldırısının uygulanacağı yerel ağdaki istemci cihazın görüntülenmesi gereklidir.



Görsel 3.22: Host listesinin görüntülenmesi

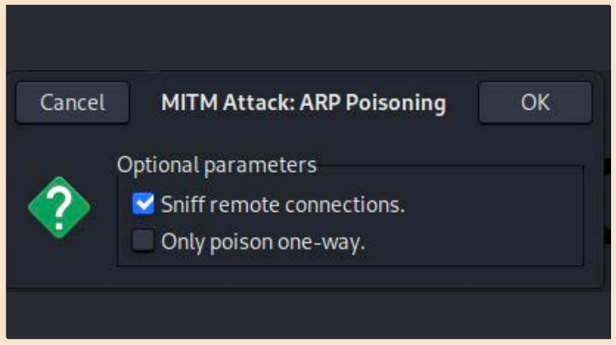
6. Adım: Görsel 3.23'te işaretlenen alandaki **ARP poisoning** seçeneğini tıklayarak saldırıyı başlatınız.



Görsel 3.23: MitM saldırısının başlatılması

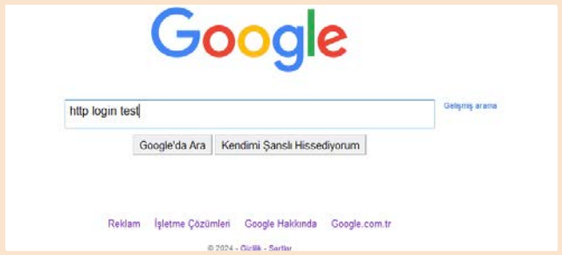
7. Adım: Gelen pencerede **Sniff remote connections**. alanının seçili olduğunu onaylayarak **OK** tuşuna basınız (Görsel 3.24).

NOT Bu adımda MitM saldırısı başlar. İstemci, HTML sitelerinde gezindiğinde oturum bilgileri Ettercap aracılığı ile Kali Linux kullanıcısına ulaşır.



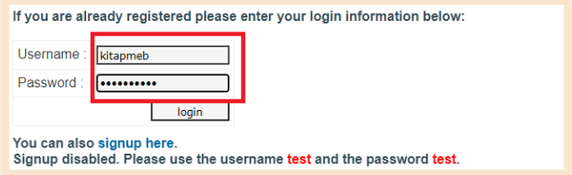
Görsel 3.24: Onay verilmesi

8. Adım: Windows kurulu istemci bilgisayarındaki arama motorlarından birini kullanarak **http login test** aramasını gerçekleştiriniz (Görsel 3.25) ve aramada çıkan sonuçlara göre login paneli testini yapmayı mümkün kılan bir HTML sitesine giriş yapınız.



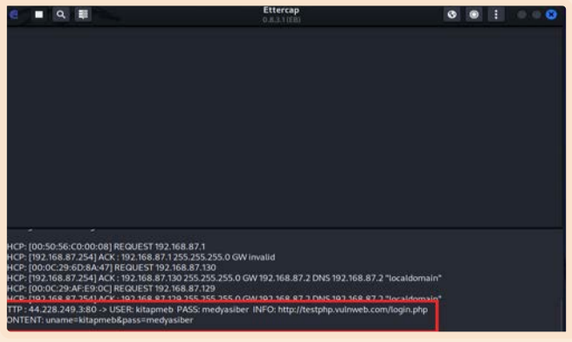
Görsel 3.25: Google arama ifadesi

9. Adım: Giriş yaptığınız test sitesine **Username: kitapmeb** ve **Password: medyasiber** ifadelerini girerek oturum açma isteği gönderiniz (Görsel 3.26).



Görsel 3.26: Oturum bilgilerinin girilmesi

10. Adım: Kali Linux işletim sistemi yüklü cihazınızdaki Ettercap uygulamasının panelini kontrol ederek oturum bilgilerini ele geçiriniz (Görsel 3.27).



Görsel 3.27: Oturum bilgilerinin Ettercap aracılığı ile elde edilmesi

3.1.4. Cain & Abel

Cain & Abel, Windows platformunda çalışan bir şifre kurtarma ve ağ güvenliği aracı olarak özellikle sniffing yetenekleriyle dikkat çeker. Bu yazılım; ağ trafiğini izleyerek şifrelenmemiş parolaları yakalama, VoIP görüşmelerini kaydetme, oturum bilgilerini elde etme gibi işlemleri gerçekleştirir. Sniffing yetenekleri sayesinde Cain & Abel, ağ üzerinde dolaşan veri paketlerini analiz eder ve potansiyel güvenlik açıklarını belirlemek için bu bilgileri kullanır. Bu özellikleriyle ağ güvenliği denetimlerinde ve sızma testlerinde önemli bir araç olarak yerini alır.

SIRA SİZDE

Cain & Abel yazılımını kullanarak yerel ağınızda bulunan başka bir cihazın HTML sitelerine oturum açma isteğini sniff ediniz. Sniffing işlemi sonucunda oturum açma bilgilerini ele geçiriniz.

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız. Çalışmanızı bir ders saati içinde tamamlayınız.

KONTROL LİSTESİ

DEĞERLENDİRME ÖLÇÜTLERİ	EVET	HAYIR
Cain & Abel yazılımını açtı.		
Yerel ağı dinlemeye aldı.		
HTTP protokolünü kullanan ve oturum açma paneli bulunan web sitesine giriş yaptı.		
Cain & Abel uygulamasıyla HTTP sitesinin oturum bilgilerini ele geçirdi.		

3.2. SINIFFING SALDIRILARININ TESPİTİ

Sniffing, bir saldırgan tarafından ağ üzerindeki veri trafiğinin izlenerek gizli bilgilerin ele geçirildiği saldırılardır. Bu saldırılar, güvenli olmayan veya şifrelenmemiş ağlarda gerçekleşir.

Sniffing saldırılarının türleri şunlardır:

Pasif Sniffing: Saldırgan, ağdaki veri trafiğini dinler ancak trafiğe müdahale etmez. Böylece saldırgan; kullanıcıların şifrelerini, e-postalarını veya diğer hassas bilgilerini kullanıcı fark etmeden ele geçirebilir.

Aktif Sniffing: Saldırgan, ağ trafiğine müdahale eder veya ağı manipüle eder. Örneğin saldırgan, ağ cihazlarını kandırarak (ARP spoofing gibi) verilerin kendi cihazına yönlendirilmesini sağlayabilir.

ARP Spoofing: Aktif sniffing saldırısının bir örneğidir. Saldırgan, ağdaki cihazlara sahte ARP mesajları göndererek trafiğin kendi cihazına yönlendirilmesini sağlar. Böylece saldırgan, iki cihaz arasındaki tüm veri trafiğini izleyebilir.

DNS Spoofing: Saldırgan, DNS (Domain Name System) sorgularını manipüle ederek kullanıcıları sahte bir web sitesine yönlendirebilir. Böylece kullanıcıların girdiği bilgiler (örneğin kullanıcı adı ve şifreler) saldırgan tarafından ele geçirilebilir.

MAC Flooding: Saldırgan, bir switchin MAC adres tablosunu sahte MAC adresleriyle doldurur. Switch bu tabloyu dolduramadığında hub gibi davranmaya başlar ve bu durum, saldırganın tüm ağ trafiğini dinlemesine olanak tanır.

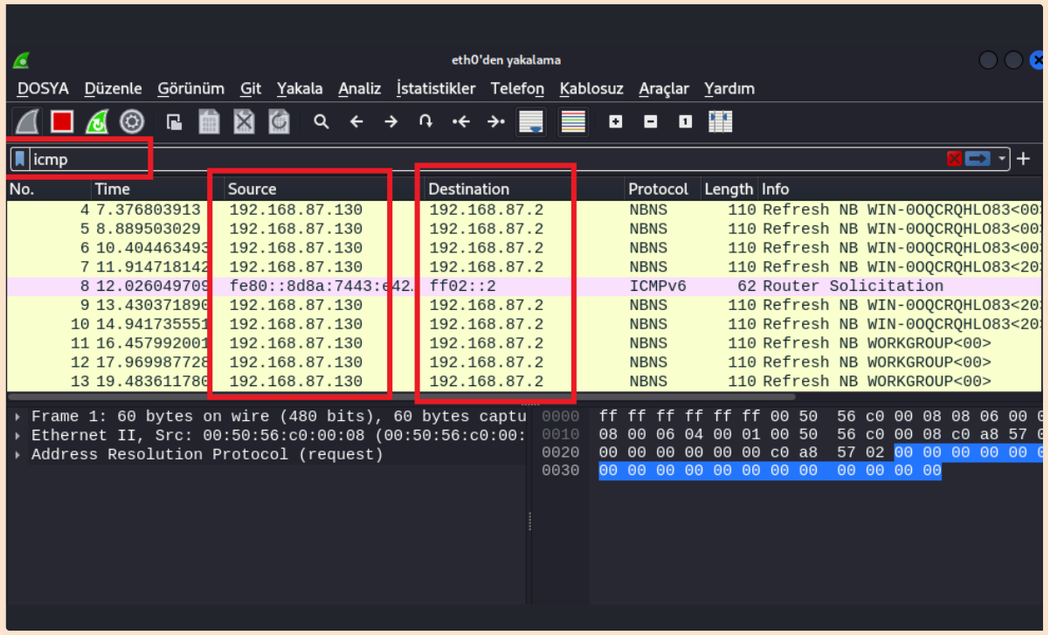
3.2.1. MAC Flooding Saldırısı

MAC flooding, MAC adres tablosunun aşırı yüklenmesi anlamına gelir. Ağdaki switch cihazları, yerel ağ iletişimini yönetmek için bir MAC adres tablosuna sahiptir. Switch cihazlarına ait bu tablolarının belirli bir kapasitesi vardır. Saldırgan, sürekli yeni MAC adresleri göndererek switchin MAC tablosunu doldurur ve cihazın işlevini yerine getirmesini engeller. Switch cihazı, bu saldırıya daha fazla dayanamayıp gelen paketleri belirli bir adrese değil tüm makinelere göndermeye başlar. Bu saldırı; switchi bir hub gibi davranmaya zorlar. Bu durum, ağ trafiğinin tüm portlara yönlendirilmesine ve saldırganın bu trafiği izleyerek gizli bilgilere erişmesine olanak tanır. Bu saldırı türü, MAC flooding saldırısı olarak adlandırılır. MAC flooding saldırısına karşı etkili bir savunma için switch üzerindeki port güvenliği ayarlarının doğru yapılandırılması çok önemlidir.

5. UYGULAMA

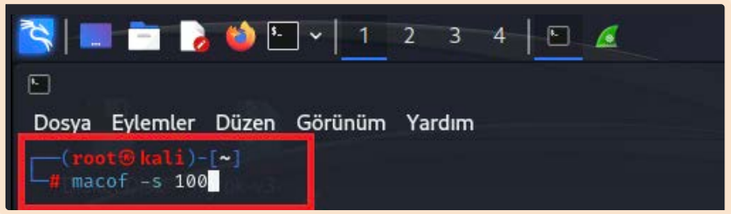
İşlem adımlarına göre Kali Linux işletim sistemi araçlarını kullanarak MAC flooding saldırısı gerçekleştiriniz ve bu saldırının analizini Wireshark programı ile yapınız.

1. Adım: Saldırıya başlamadan önce Wireshark programı ile **icmp** paketlerinin analizini yapınız ve analiz sonucunda gerçek MAC adres isteklerinin olduğunu doğrulayınız (Görsel 3.28).



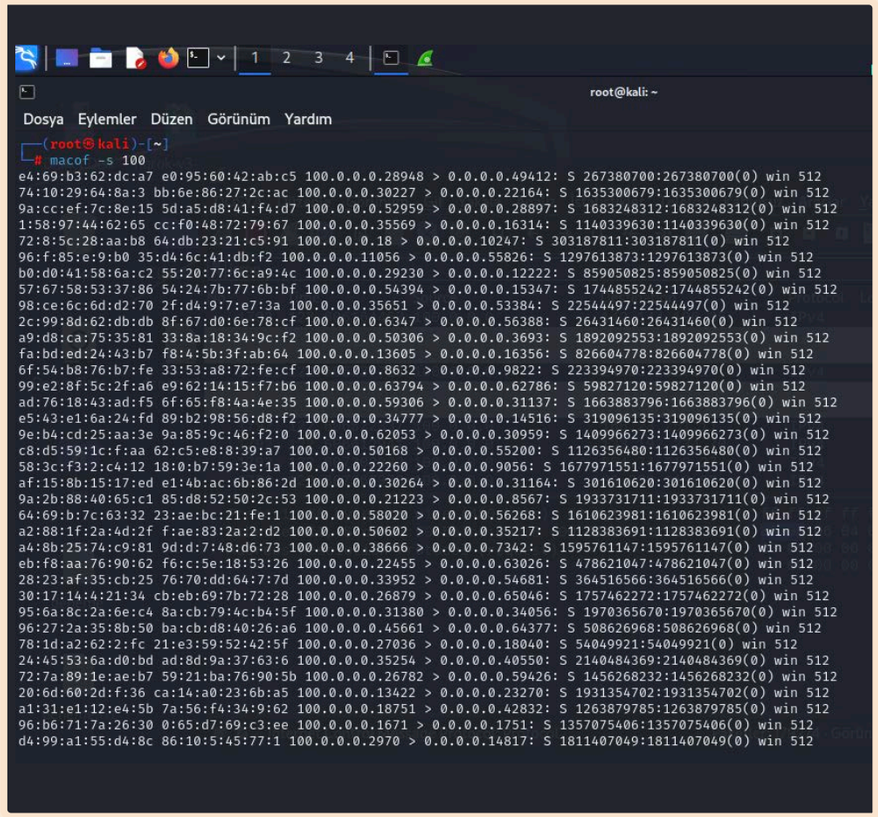
Görsel 3.28: Saldırı öncesi Wireshark ile icmp paketlerinin incelenmesi

2. Adım: 100 adet MAC flooding saldırısı yapmak için Görsel 3.29'daki gibi **macof -s 100** kodunu yazınız.



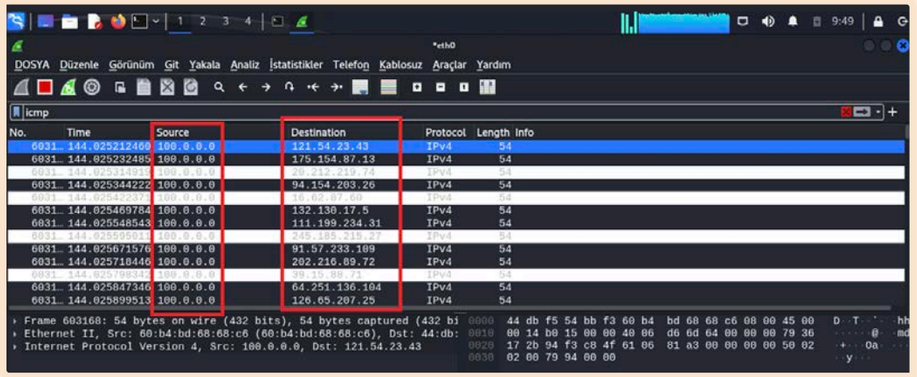
Görsel 3.29: MAC flooding saldırısının başlatılması

3. Adım: macof komutu ile başlayan saldırının sonucunda sahte MAC adresleri üretiminin başladığını doğrulayınız (Görsel 3.30).



Görsel 3.30: Saldırının başlangıcı ve sahte MAC adreslerinin üretimi

4. Adım: Saldırı sonrasında Wireshark ile tekrar **icmp** paketlerinin analizini yapınız ve sahte MAC adreslerinin üretildiğini görüntüleyiniz (Görsel 3.31).



Görsel 3.31: Wireshark ile saldırı analizi

5. Adım: Saldırı yapıldığını Wireshark programının **İstatistik** kısmından doğrulayınız (Görsel 3.32).

NOT Wireshark programındaki menü seçeneklerinden **İstatistik** ve **Konuşma** sekmesi tıklandığı zaman belirli bir süre içinde ağdaki paket sayısının anormal şekilde artması saldırının yapıldığını gösterir.

Görsel 3.32: Saldırı gerçekleştiğine dair Wireshark programının analiz istatistikleri

MAC flooding saldırısından korunmak için çeşitli stratejiler ve güvenlik önlemleri alınmalıdır. Öncelikle her bir switch portuna bağlanabilecek maksimum MAC adresi sayısını **Port Security** özelliğini kullanarak sınırlandırmak, saldırganların ağa sahte MAC adresleri göndererek tabloyu doldurmasını engeller. Ayrıca **Dynamic ARP Inspection** vb. teknolojiler, sahte ARP yanıtlarını engelleyerek saldırı girişimlerini tespit ve bloke eder. **VLAN'lar** kullanarak ağı segmentlere ayırmak, saldırının etkisini sınırlayabilir. Düzenli olarak **ağ trafiğini izlemek** ve **günlük analizleri** yapmak da saldırıların erken tespit edilmesine olanak tanır. Bu önlemler, ağ güvenliğini artırır ve MAC flooding gibi tehditlere karşı etkili bir savunma sağlar.

3.2.2. ARP Poisoning Saldırısı

ARP poisoning, bir saldırganın yerel ağda sahte ARP mesajları göndererek ağdaki cihazları yanlış yönlendirmesiyle gerçekleşen bir saldırıdır. Bu saldırıda saldırgan, hedef cihazların ARP tablolarını manipüle ederek kendi MAC adresini hedef cihazın IP adresiyle ilişkilendirir. Sonuç olarak ağ trafiği saldırganın cihazına yönlendirilir. Böylece saldırgan; bu trafiği izleyebilir, değiştirebilir veya engelleyebilir. ARP poisoning özellikle MitM saldırılarının gerçekleştirilmesinde yaygın olarak kullanılır ve ağ güvenliği açısından ciddi bir tehdit oluşturur. Ağ içinde taşınan paketler, saldırganın belirlediği bilgisayara gönderilir. Hedef bilgisayarın ulaşmak istediği HTTP paketindeki web sayfası yerine saldırganın belirlediği web sayfasının açılması sağlanır.

ARP poisoning saldırılarına karşı alınabilecek çeşitli güvenlik tedbirleri şunlardır:

Port Security: Switch portlarına bağlanabilecek cihazların sayısını ve MAC adreslerini sınırlandırarak güvenliği artırır. Bu özellik, belirli bir port üzerinden sadece izin verilen MAC adreslerinin geçmesine izin verir ve böylece saldırganların sahte MAC adresleriyle switchi yanıltmasını zorlaştırır. Ayrıca belirlenen limitlerin aşılması durumunda port güvenliğine yönelik ihlalleri bildirilir ve gerekli önlemleri otomatik olarak alır.

Dynamic ARP Inspection (DAI): ARP poisoning saldırılarını tespit edip engellemek için kullanılan bir switch güvenlik özelliğidir. DAI, ağda dolaşan ARP paketlerini izler ve yalnızca güvenilir kaynaklardan gelen ARP yanıtlarının geçerli olmasına izin verir. Bu güvenilirlik, DHCP snooping veya manuel olarak tanımlanan güvenilir portlar üzerinden sağlanır. DAI etkinleştirildiğinde switch, sahte ARP paketlerini tespit eder ve bu paketleri engelleyerek ağın güvenliğini sağlar.

DHCP Snooping: Switch üzerinde etkinleştirildiğinde yalnızca güvenilir DHCP sunucularından gelen IP adresi atamalarına izin verir. Bu işlem, saldırganların sahte DHCP sunucuları oluşturmasını ve sahte ARP tablosu bilgileriyle ağdaki cihazları yanıltmasını engeller. DHCP snooping aynı zamanda DAI ile entegre çalışarak sahte ARP girişimlerinin tespit edilmesine yardımcı olur.

Statik ARP Girdilerini Kullanmak: Ağda kritik cihazlar için statik ARP girdileri belirlemek, ARP poisoning saldırılarına karşı etkili bir savunma yöntemi olabilir. Statik ARP girdileri, belirli bir IP adresinin yalnızca belirli bir MAC adresine karşılık gelmesini sağlar ve bu eşlemenin manuel olarak değiştirilmesini engeller. Bu güvenlik tedbirinin büyük ağlarda yönetimi zor olabilir ve sadece kritik cihazlar için uygulanması önerilir.

ARP Tablolarını Düzenli Olarak İzlemek: Ağ yöneticileri, ARP tablolarını düzenli olarak izleyerek anormal değişiklikleri tespit edebilir. Örneğin ARP tablosundaki bir IP adresinin farklı bir MAC adresine yönlendirilmesi durumunda saldırının varlığından söz edilebilir. Bu tür anormallikler fark edildiğinde müdahale için gerekli adımlar atılabilir.

Segmentasyon ve VLAN Kullanmak: Ağın segmentlere ayrılması, ARP poisoning saldırılarının etkisini sınırlar. Saldırgan, yalnızca kendi bulunduğu VLAN'daki cihazları etkileyebildiği için bu işlem, saldırının yayılmasını önler ve zararı minimize eder.

VPN Kullanmak: Ağ trafiğini şifreleyerek ARP poisoning gibi saldırılara karşı ek bir koruma sağlar. VPN, saldırganların ağ trafiğini izlemesini ve manipüle etmesini zorlaştırır. Böylece ağdaki cihazlar arasında güvenli bir iletişim sağlar.

ÖLÇME VE DEĞERLENDİRME

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

1. ( ) Sniffer araçları, ağ yöneticilerinin performans analizi yapmasına ve güvenlik açıklarını tespit etmesine yardımcı olur.

2. ( ) Sniffer araçları yalnızca ağ üzerindeki veri paketlerini izlemek için kullanılır ve ağ performansını etkilemez.

3. ( ) Wireshark, ağ üzerindeki veri paketlerini analiz etmek için yalnızca belirli bir protokolün verilerini yakalar.

4. ( ) DHCP snooping sadece güvenilir DHCP sunucularından gelen IP adresi atamalarını kabul ederek sahte DHCP sunucularının ağa IP atamasını engeller.

5. ( ) Statik ARP girdileri kullanmak, büyük ağları kolayca yönetmeyi sağlar.

B) Aşağıdaki sorularda doğru cevabı işaretleyiniz.

6. Aşağıdaki işlemlerden hangisi Wireshark'ta filtreleme kullanılarak gerçekleştirilebilir?

A) Yazılım güncellemelerini otomatik olarak yüklemek.

B) Wireshark arayüzünün renk şemasını değiştirmek.

C) Belirli bir IP adresine ait trafiği gözlemlemek.

D) Wireshark'ın veri paketlerini otomatik olarak şifrelemek.

E) Wireshark'ın ağ performansını artırmak.

7. Aşağıdakilerden hangisi belirtilen IP adresine giden trafiği yakalamak için kullanılan TCPDump komutudur?

A) tcpdump -i eth0

B) tcpdump dst 192.168.10.1

C) tcpdump src 192.168.2.1

D) tcpdump port 80

E) tcpdump –v

8. Aşağıdakilerden hangisi Cain & Abel aracının ağ güvenlik denetimleri ve sızma testlerinde önemli rol oynayan özelliğidir?

A) Şifrelenmemiş parolaları yakalamak ve VoIP görüşmelerini kaydetmek.

B) Ağ trafiğini şifreleyerek güvenliği artırmak.

C) Yalnızca e-posta hesaplarını şifrelemek.

D) Güvenlik duvarlarını otomatik olarak kapatmak.

E) Sadece ağ üzerinde çalışan uygulamaları izlemek.

9. Aşağıdakilerden hangisi MAC flooding saldırısı sonucunda bir switch cihazında meydana gelebilecek davranış değişikliğidir?

A) Switch, ağ trafiğini sadece belirli bir IP adresine yönlendirir.

B) Switch, MAC adres tablosunu temizleyerek tekrar başlar.

C) Switch, tüm ağ trafiğini tüm portlara yayarak çalışır ve bu durum, saldırganın trafiği izleyebilmesine olanak tanır.

D) Switch, gelen paketleri hiç işlemeyip ağ trafiğini tamamen durdurur.

E) Switch, şifreleme algoritmaları kullanarak trafiği güvenli hâle getirir.

10. Aşağıdakilerden hangisi Ettercap programının ağ üzerindeki veri trafiğini dinleyerek manipüle etmesini sağlayan özelliğidir?

A) Ağ trafiğini şifrelemek ve şifre çözme işlemlerini gerçekleştirmek.

B) MAC adres tablosunu yönetmek ve saldırı anında port güvenliğini sağlamak.

C) İletişim için gerekli olan ağ yapılandırma parametrelerini otomatik olarak atamak.

D) Güvenlik açıklarını tespit etmek için ağ performansını izlemek.

E) MitM saldırıları için ARP spoofing ve DNS spoofing yapabilmek.

NOT

4. ÖĞRENME BİRİMİ

ŞİFRELEME TEKNİKLERİ

KONULAR

4.1. SİMETRİK ŞİFRELEME YÖNTEMLERİ
4.2. ASİMETRİK ŞİFRELEME YÖNTEMLERİ
4.3. STEGANOGRAFİ YÖNTEMLERİ

NELER ÖĞRENECEKSİNİZ?

- Şifreleme yöntemlerini sıralama
- Simetrik ve asimetrik şifreleme işlemlerini kullanma
- Hashing işlemini gerçekleştirme
- Steganografi yöntemlerini kullanma

ANAHTAR KAVRAMLAR

DES, Diffie-Hellman, hash, MD5, ortak anahtar, özel anahtar, private, public, RSA, salt, SHA, steganografi, şifre

HAZIRLIK ÇALIŞMALARI

1. Parola ve şifre kavramları arasında hangi farklılıklar bulunabilir? Düşüncelerinizi arkadaşlarınızla paylaşınız.
2. İnternetten indirilen bir dosyanın güvenilirliği ve bütünlüğü nasıl anlaşılır? Düşüncelerinizi arkadaşlarınızla tartışınız.

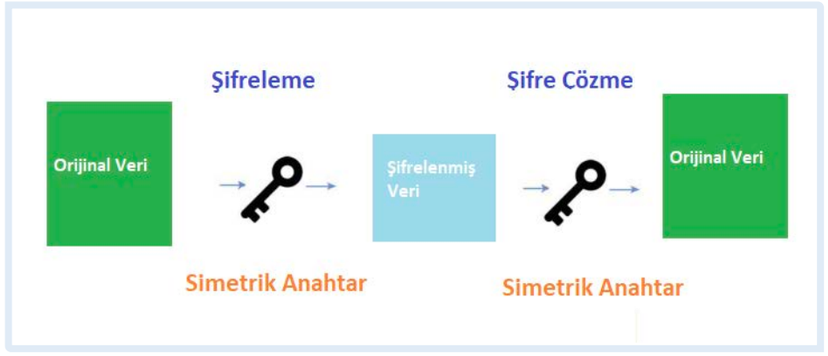
4.1. SİMETRİK ŞİFRELEME YÖNTEMLERİ

Şifreleme algoritmaları, dijital dünyanın görünmez koruyucuları olarak kabul edilir. Bilgi güvenliğinin en önemli unsurlarından biri olan bu algoritmalar, verileri karmaşık matematiksel süreçle şifreleyerek yetkisiz kişilerin ilgili bilgilere ulaşmasını engeller. Özellikle internetin yaygınlaşmasıyla birlikte şifreleme teknikleri hem bireysel hem de kurumsal veri güvenliğinin vazgeçilmez bir parçası hâline gelmiştir. Dijitalleşmenin hızla arttığı bu çağda verilerin gizliliğini ve bütünlüğünü sağlamak, şifreleme algoritmalarının doğru ve etkili bir şekilde kullanılmasına bağlıdır.

Ağ güvenliğinde önemli bir rol oynayan **şifreleme (encrypt)** işlemi, gönderilen verinin yalnızca yetkili alıcılar tarafından okunmasını sağlamak amacıyla gerçekleştirilir. **Şifrelenmiş veri (ciphertext),** ilgili veriyi yetkisiz erişimlerden koruyan bir dönüştürme sürecidir. Bu süreçte veriler, karmaşık matematiksel algoritmalar kullanılarak şifrelenir. Şifreli verinin tekrar orijinal hâle getirilmesine ise **şifre çözme (decrypt)** adı verilir. Şifreleme ve şifre çözme işlemleri hem gizli hem de açık anahtarlı sistemlerde uygulanabilir ve veri güvenliğinin sağlanmasında kritik öneme sahiptir.

Şifreleme algoritmaları, anahtar kullanma yöntemlerine göre gizli anahtarlı (simetrik) ve açık anahtarlı (asimetrik) şifreleme algoritmaları olmak üzere iki ana kategoriye ayrılır. Simetrik anahtarlama sisteminde hem şifreleme hem de şifre çözme işlemleri aynı anahtarla gerçekleştirilir.

Simetrik şifreleme, verilerin şifrelenmesi ve çözümlenmesi için tek bir gizli anahtarın kullanıldığı en temel şifreleme türüdür. Bu yöntem, şifreleme ve şifre çözme işlemleri için aynı anahtarı kullanan gizli anahtar algoritmalarına dayanır. Bu özellik, veri şifreleme sürecini daha basit ve verimli hâle getirir. Gizli anahtar şifreleme, yaygın olarak tercih edilen bir yöntemdir ancak bu algoritmalarda şifrelenmiş veri, alıcıya iletilirken gizli anahtarın da güvenli bir şekilde alıcıya ulaştırılması gereklidir. Simetrik şifreleme sistemleri, şifreleme ve şifre çözme işlemlerini son derece hızlı bir şekilde gerçekleştirme avantajına sahiptir. Görsel 4.1'de simetrik şifreleme yöntemine ait bir blok diyagramı görülür.



Görsel 4.1: Simetrik şifreleme blok diyagramı

Simetrik şifrelemenin avantajları şunlardır:

Hızlı İşlem: Simetrik şifreleme algoritmaları, veriyi şifrelerken ve verinin şifresini çözerken karmaşık matematiksel işlemlere ihtiyaç duymadığı için genellikle hızlı çalışır. Bu hız, büyük miktarda verinin şifrelenmesi gerektiğinde önemli bir avantaj sağlar.

Daha Az Hesaplama Gücü: Simetrik şifreleme algoritmaları genellikle daha az hesaplama gücü gerektirir. Bu durum, işlemci üzerindeki yükü azaltır ve enerji tüketimini düşürür. Özellikle mobil cihazlar, gömülü sistemler gibi sınırlı kaynaklara sahip cihazlarda faydalıdır.

Basitlik: Tek bir gizli anahtarın hem şifreleme hem de şifre çözme için kullanılması, algoritmanın uygulanmasını ve anlaşılmasını daha kolay hâle getirir.

Daha Az Depolama Gereksinimi: Sadece tek bir anahtarın saklanması gerektiği için simetrik şifreleme, asimetrik şifrelemeye göre daha az depolama alanı gerektirir.

Simetrik şifrelemenin dezavantajları şunlardır:

Anahtar Dağıtımı Zorluğu: Simetrik şifrelemenin en büyük dezavantajı, gizli anahtarın güvenli bir şekilde iletilmesini ve saklanmasını gerektirmesidir. Gizli anahtar, yetkisiz bir kişi tarafından ele geçirilirse tüm şifreleme sistemi tehlikeye girebilir.

Anahtar Yönetimi: Birden fazla kişiyle güvenli iletişim sağlanacaksa her kişiye ayrı bir gizli anahtar gerekeceği için gizli anahtarların yönetimi karmaşık hâle gelir. Bu durum, büyük ölçekli ağlarda zorluk yaratabilir.

Gizlilik Sorunu: Gizli anahtarın hem şifreleme hem de şifre çözme işlemleri için kullanılması, gizli anahtarın çalınması durumunda tüm şifreli bilgilerin tehlikeye girmesine neden olabilir. Bu durum, simetrik şifrelemeyi güvensiz kılabilir.

Anahtar Sayısı: Çok sayıda kullanıcı arasındaki iletişimde her iki kullanıcı arasında ayrı bir gizli anahtarın bulunması gerektiği için gerekli gizli anahtar sayısı hızla artar. Bu durum, yönetim ve güvenlik açısından zorluk yaratabilir.

4.1.1. DES (Data Encryption Standart) Veri Şifreleme

DES (Data Encryption Standard), 1970'lerin ortalarında IBM tarafından geliştirilen ve Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından 1977'de standart olarak kabul edilen bir simetrik şifreleme algoritmasıdır. DES, dünyada en yaygın kullanılan şifreleme algoritmalarından biridir. DES'in en önemli özelliklerinden biri, simetrik bir şifreleme algoritması olmasıdır. Bu durum, şifreleme ve şifre çözme işlemleri için aynı anahtarın kullanıldığı anlamına gelir. Bu özellik, DES hızlı ve verimli bir şifreleme yöntemi hâline getirirken anahtar yönetimi konusunda bazı zorluklar yaratır.

Anahtarın güvenli bir şekilde iletilmesi ve saklanması, sistemin güvenliği açısından kritik öneme sahiptir. Bu algoritma, şifrelenecek açık metni bloklara ayırır ve her bloku bağımsız olarak şifreler. Şifrelenmiş metni çözmek için aynı işlemi bu bloklar üzerinde tekrarlar. DES'in kullandığı bloklar 64 bit uzunluğundadır. Anahtar uzunluğunun kısa olması nedeniyle DES şifreleri brute force saldırılarıyla kırılabilir hâle gelir. Bu nedenle DES, zamanla yerini daha güçlü ve güvenli algoritmalara bırakır ancak veri şifrelemenin temel prensiplerini anlamak açısından önemli bir referanstır. Bu durumu aşmak amacıyla DES algoritmasının üç kez üst üste uygulanmasıyla elde edilen 3DES (Triple Data Encryption Standard) geliştirilir. Bu yöntem, DES'e kıyasla üç kat daha yavaş çalışır. Daha sonra AES'in (Advanced Encryption Standard) geliştirilmesiyle birlikte DES popülerliğini kaybeder.

DES, bit tabanlı (1 ve 0) bir şifreleme algoritması olarak çalışır. Bu algoritmada şifrelenecek mesaj 64 bitlik parçalara bölünür. Her bir 64 bitlik blok, 8 karaktere karşılık gelir (1 bayt, 8 bit olarak kabul edilir.). 64 bitlik mesaj, sağ ve sol olmak üzere iki parçaya ayrılır. 32 bitlik sağ kısım çaprazlanarak doğrudan çıkışın sol tarafına aktarılır. Aynı zamanda bu 32 bitlik sağ bölüm, anahtar üretici tarafından oluşturulan 48 bitlik bir anahtar ile F fonksiyonuna tabi tutulur ve sol kısımdan gelen 32 bitlik mesajla XOR işlemi uygulanır. Ortaya çıkan sonuç, çıkışın sağ tarafına aktarılır. Bu işlem, toplamda 16 kez tekrarlanır. Bu nedenle ilk aşamada doğrudan aktarılan 32 bitlik sağ kısım, bir sonraki adımda sol tarafa geçer ve F fonksiyonu ile XOR işlemine tabi tutulur. Bu sayede şifrelenmemiş hiçbir bit kalmaz ve tüm veri şifrelenir.

DES, uzun yıllar boyunca çeşitli sektörlerde veri güvenliğini sağlamak için kullanılmıştır. DES'in yaygın kullanıldığı sistemlere ve kullanım alanlarına dair bazı örnekler şunlardır:

1. Bankacılık ve Finans Sektörü

Ödeme Sistemleri: DES, kredi kartı işlemlerinde ve ATM ağlarında veri şifrelemesi için kullanılmıştır. Özellikle ATM'lerde müşteri PIN'leri ve diğer hassas verilerin güvenli bir şekilde iletilmesi amacıyla DES kullanımı yaygındır. Örneğin 1980'ler ve 1990'lar boyunca büyük ödeme sistemleri, DES'i ödeme ağlarında kullanmıştır.

SWIFT (Society for Worldwide Interbank Financial Telecommunication) Ağı: Bankalar, uluslararası para transferlerini güvenli hâle getirmek için DES'i şifreleme protokollerinin bir parçası olarak kullanmıştır. SWIFT ağı, dünya çapındaki bankalar arasında milyarlarca dolarlık işlemleri güvenli bir şekilde gerçekleştirmek için DES tabanlı şifreleme yöntemlerine dayanmıştır.

2. Telekomünikasyon

Telefon Şifreleme: DES, telekomünikasyon ağlarında sesli iletişimlerin şifrelenmesi amacıyla kullanılmıştır. Örneğin askerî haberleşmede ve hükümet iletişiminde hassas bilgilerin güvenliğini sağlamak için DES tabanlı şifreleme cihazları kullanılmıştır.

Uydu İletişimi: Uydu tabanlı iletişim sistemlerinde veri ve ses sinyallerinin güvenli bir şekilde iletilmesi amacıyla DES kullanılmıştır. Bu tür uygulamalarda DES şifreleme, uydu üzerinden gönderilen verilerin yetkisiz erişimlere karşı korunmasını sağlamıştır.

3. Hükümet ve Askerî Uygulamalar

Hükümet Sistemleri: ABD hükümeti tarafından bir dönem boyunca verilerin şifrelenmesi için DES kullanılmıştır. Özellikle veri aktarımı ve saklanması için DES tabanlı çözümler tercih edilmiştir.

Askerî İletişim: DES, askerî iletişimde de kullanılmıştır. Askerî alandaki bazı eski iletişim cihazları ve sistemleri, güvenliği sağlamak için DES tabanlı şifreleme yöntemlerini kullanmıştır.

4. Kurumsal Ağ Güvenliği

VPN (Virtual Private Network): 1990'lı yıllarda ve 2000'lerin başlarında bazı VPN sistemleri, veri trafiğini güvenli hâle getirmek için DES tabanlı şifreleme yöntemlerini kullanmıştır.

Dosya Şifreleme: Bazı kurumsal veri şifreleme yazılımları, dosyaların güvenliğini sağlamak için DES algoritmasını kullanmıştır. Örneğin eski veriyi arşivleme sistemlerinde dosyaların ve yedeklerin güvenli bir şekilde saklanması amacıyla DES kullanılmıştır.

5. Elektronik İmza ve Dijital Sertifikalar

Dijital İmza Sistemleri: DES, dijital imzaların ve sertifikaların oluşturulması ve doğrulanması sürecinde de kullanılmıştır. Bu durum, kurumlara ve hükümetlere ait belgelerinin bütünlüğünü ve gizliliğini sağlamak için tercih edilen bir yöntem olmuştur.

6. Kablosuz İletişim ve Disk Şifreleme

Kablosuz İletişim: Bazı eski kablosuz iletişim protokollerinde verilerin şifrelenmesi için DES kullanılmıştır. Bu durum, 2G gibi eski nesil cep telefonu şebekelerinde görülen bir uygulamadır.

Disk Şifreleme: Bazı eski sabit disk ve veri depolama sistemleri, verileri şifrelemek için DES algoritmasını kullanmıştır.

DES, medya sektöründe de belirli alanlarda kullanılmıştır. DES'in medya sektöründeki bazı kullanım alanları şunlardır:

1. Dijital İçerik Koruma

Kişisel ve Kurumsal Veri Güvenliği: Medya şirketleri tarafından dijital içeriklerin güvenliğini sağlamak için DES tabanlı şifreleme yöntemleri kullanılmıştır. Özellikle müzik, video ve diğer dijital medya içeriklerinin yetkisiz erişime karşı korunması amacıyla DES uygulamalarından yararlanılmıştır. Bu durum, medya dosyalarının şifrelenmesi ve güvenli bir şekilde saklanmasını içerir.

2. Kanal ve Yayın Şifrelemesi

Kanal Şifreleme: Kablolu veya uydu TV yayıncılığı gibi medya sektöründeki bazı eski sistemler, yayın verilerini şifrelemek için DES kullanmıştır. Bu durum özellikle içerik sağlayıcılarının, içeriklerini yetkisiz izleyicilerden korumayı amaçlayan bir yöntemdir.

Dijital Yayın Sistemleri: Medya şirketleri tarafından dijital yayın sistemlerinin güvenliğini sağlamak için DES tabanlı şifreleme yöntemleri kullanılmıştır. Bu durum, dijital TV sinyallerinin ve diğer medya içeriğinin şifrelenmesini içerir.

3. Güvenli İletişim

Medya Şirketleri Arası İletişim: Medya şirketleri tarafından güvenli veri iletimi ve iletişimi sağlamak amacıyla DES tabanlı şifreleme kullanılmıştır. Özellikle büyük medya projelerinde içerik değişimi ve iş birliği süreci için güvenli iletişim önemli bir gereksinimdir.

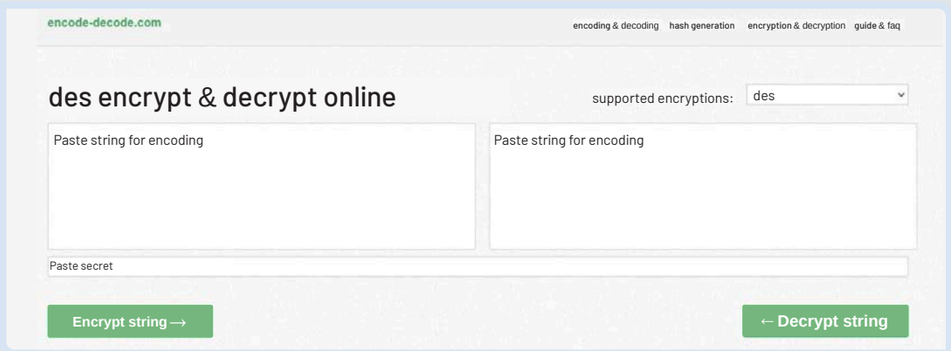
4. Arşivleme ve Saklama

Veri Arşivleme: Medya kuruluşları, büyük miktarda dijital içerik arşivlemesi yaparken bu verilerin güvenliğini sağlamak için DES tabanlı şifreleme yöntemlerini kullanmıştır. Bu durum, eski medya içeriklerini güvenli bir şekilde saklamayı ve yetkisiz erişimlerden korumayı hedeflemiştir.

1. UYGULAMA

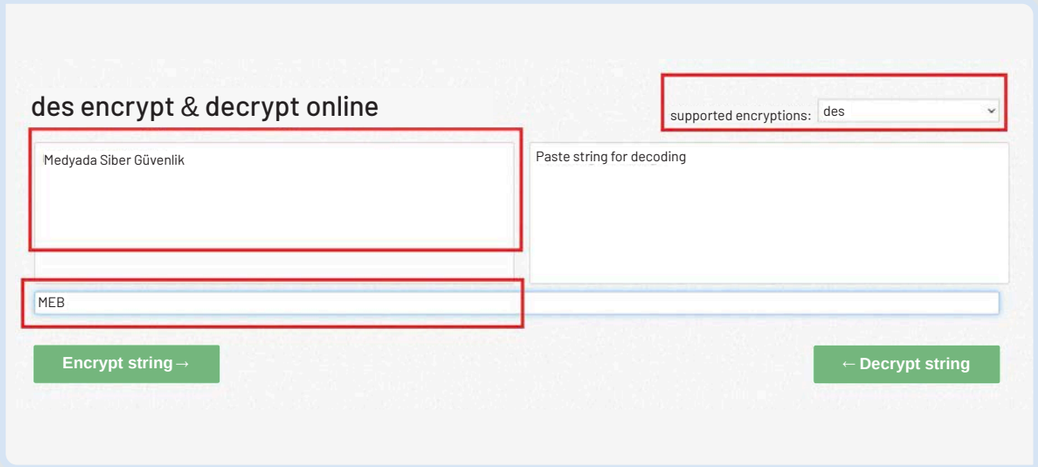
İşlem adımlarına göre online DES şifreleme araçlarını kullanarak istediğiniz bir metnin şifrelenmesini sağlayınız.

1. Adım: Web tarayıcısına **DES encode** yazıp, arama yaparak çevrimiçi bir araç bulunuz (Görsel 4.2).



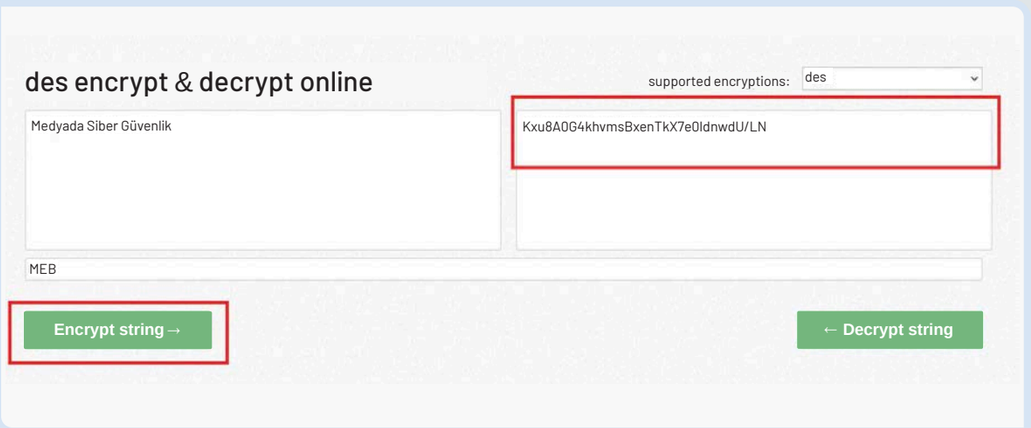
Görsel 4.2: DES şifreleme için kullanılacak çevrimiçi araç

2. Adım: Sol taraftaki işaretli alana şifrelemek istediğiniz metin için **Medyada Siber Güvenlik** ifadesini giriniz. Girdiğiniz metnin altında **Paste Secret** alanı bulunur. Bu alana **MEB** olarak belirlenen anahtar kelimeyi yazınız (Görsel 4.3).



Görsel 4.3: Şifrelenecek metnin ve anahtarın oluşturulması

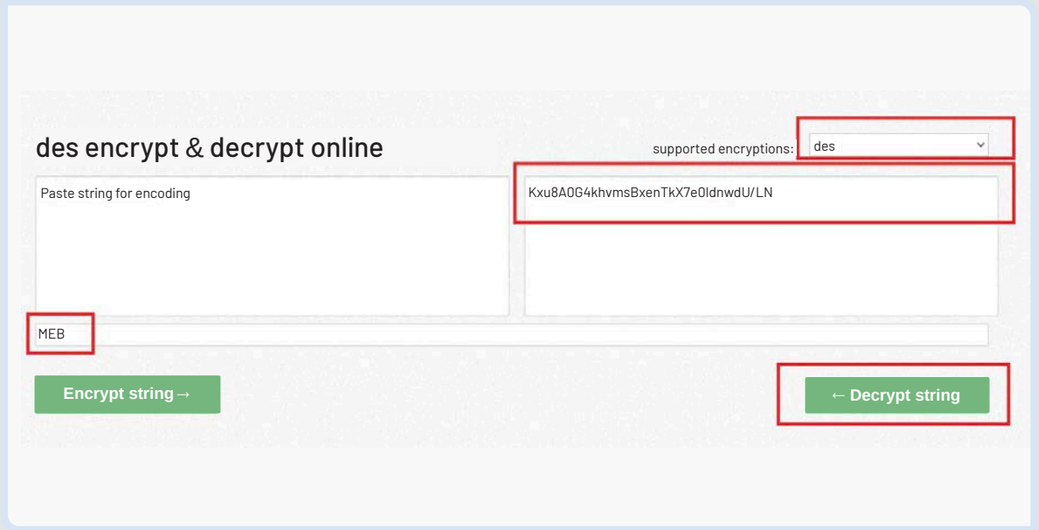
3. Adım: Bilgileri girdikten sonra şifrelenmiş metin için **Encrypt string** düğmesine basınız. Elde edilen şifrelenmiş metin, sağ taraftaki büyük metin kutusunda yazacaktır (Görsel 4.4).



Görsel 4.4: DES ile metnin şifrelenmesi

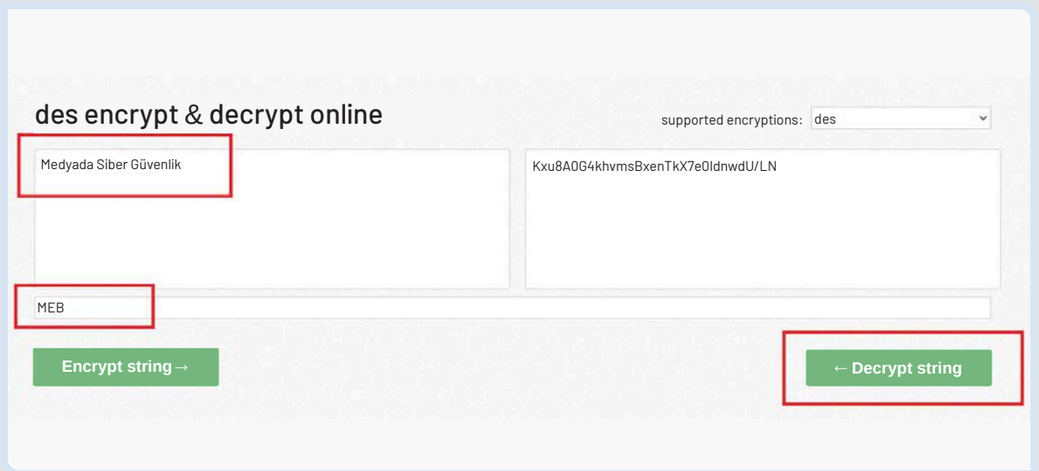
4. Adım: Elde edilen şifreler, açık metin (şifrelenmemiş metin) hâline de dönüştürülebilir. Bu işlem için Görsel 4.4'teki şifrelenmiş metni kopyalayınız.

5. Adım: Web sitesini tekrar açınız. Kopyalanan şifrelenmiş metni, sağ taraftaki metin kutusuna yapıştırınız. DES şifrelemede anahtar kelimenin değişmemesi gerektiği için **Paste Secret** alanına **MEB** yazarak sağ altta bulunan **Decrypt string** düğmesine basınız (Görsel 4.5).



Görsel 4.5: Şifrelenmiş verinin açık metne dönüştürülmesi

6. Adım: Açık metni (plaintext) veya şifrelenmemiş metni elde ediniz (Görsel 4.6).



Görsel 4.6: DES decrypt işlemi

Kullanılan bazı simetrik şifreleme yöntemleri şunlardır:

AES: Simetrik şifrelemenin en yaygın ve güvenli yöntemlerinden biridir. 2001 yılında NIST tarafından DES'in yerine geçmesi için standart olarak kabul edilmiştir. AES; 128, 192 ve 256 bit anahtar uzunlukları sunar ve güçlü güvenlik özellikleri ile bilinir.

3DES: DES'in üç kez arka arkaya uygulanması ile elde edilen bir şifreleme yöntemidir. Bu işlem, DES'in güvenliğini artırır ancak işlem süresi DES'e göre üç kat daha uzun olabilir.

Blowfish: Bruce Schneier tarafından geliştirilmiş bir simetrik şifreleme algoritmasıdır. 64 bitlik blok boyutunu ve değişken anahtar uzunluklarını destekler (32 bitten 448 bite kadar). Blowfish, en hızlı blok şifreleyici algoritmalardan biridir.

Twofish: Daha uzun anahtar uzunlukları (128, 192, 256 bit) ve 128 bit blok boyutu ile gelişmiş güvenlik sağlar. Blowfish'in bir evrimi olan Twofish, Bruce Schneier ve ekibi tarafından geliştirilmiştir.

RC4 (Rivest Cipher 4): Bir akış şifreleme algoritmasıdır ve çeşitli uzunlukta anahtarları destekler. RC4, veri akışını gerçek zamanlı olarak şifreleyip çözme yeteneğine sahiptir.

RC5 (Rivest Cipher 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

Çevrimiçi araçlar yardımıyla 3DES ve AES algoritmalarını şifre çözmek ve çözülen şifreyi tekrar açık metin hâline getirmek için kullanınız.

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız. Çalışmanızı bir ders saati içinde tamamlayınız.

KONTROL LİSTESİ

DEĞERLENDİRME ÖLÇÜTLERİ	EVET	HAYIR
Çevrimiçi 3DES ve AES şifreleme araçlarını buldu.		
Şifreleme işlemini gerçekleştirdi.		
Şifreleri tekrar açık metin hâline getirdi.		

4.1.2. Tek Yönlü Anahtarsız Şifreleme (Hash Fonksiyonları)

Hash fonksiyonları, değişken uzunluktaki verileri sabit uzunlukta ve benzersiz bir özet hâline getiren matematiksel algoritmalardır. Bu fonksiyonlar, girdinin boyutu ne olursa olsun aynı boyutta bir çıktı üretir ve aynı girdi, her zaman aynı hash değerini verir. Hash fonksiyonları genellikle veri bütünlüğünü sağlamak, parmak izi oluşturmak, şifreleme sistemlerinde doğrulama yapmak amacıyla kullanılır.

Tek yönlü anahtar şifrelemede orijinal verinin değiştirilmediğini alıcının hash fonksiyonlarıyla tespit etmesi hedeflenir. İyi bir hash algoritması, iki farklı girdiden aynı hash değerini üretmeyecek kadar karmaşık olmalıdır. Hash fonksiyonlarının en önemli özelliklerinden biri, küçük bir veri değişikliğinin tamamen farklı bir hash değeri üretmesidir. Bu sayede güvenilirlik ve doğruluk sağlanır. İki farklı değer için aynı hash kodu üretilirse bu durum hash çarpışması olarak bilinir. Hash algoritmasına şifrelenmesi istenen metin girilir ve hash fonksiyonuyla metin hashing işlemi yapılır. Elde edilen metin, hash değeridir. Hash algoritmaları, şifreleme algoritması içermez. SHA-256, MD5 gibi yaygın hash algoritmaları sıklıkla kullanılır.

Bir web uygulamasında kullanıcı parolalarının güvenliğini sağlamak için hash fonksiyonları kullanılır. Örneğin bir kullanıcının **Parola123** şeklinde basit bir parolası olduğu varsayılırsa bu parolayı doğrudan veri tabanına kaydetmek güvenlik riski oluşturur. Bunun yerine hash fonksiyonu kullanılarak parola şifrelenir ve parolanın şifrelenmiş hâli saklanır. Örneğin **Parola123** parolası, **SHA-256** algoritması kullanılarak şu şekilde hashlenir:

Girdi: Parola123
SHA-256 Hash Çıktısı:
ef92b778bafe771e89245b89ecbcf88f812fd563c9a9ba125b95d7e4b44f29b6

Hash fonksiyonunun önemli bir özelliği, girdinin küçük bir değişiklikle bile tamamen farklı bir çıktı üretmesidir. Kullanıcı, parolasını **Parola124** olarak girerse bu parola **SHA-256** algoritması kullanılarak şu şekilde hashlenir:

Girdi: Parola124
SHA-256 Hash Çıktısı:
ac8e3cefd729dfe9495cf22f183b16f0b0a235198e3cfb8b14b9cba920885fc9

Sadece bir karakter değişikliği hash sonucunu tamamen değiştirir. Böylece hash fonksiyonları, parolaların güvenli bir şekilde saklanmasını sağlar ve saldırganların parolaları tahmin etmesini zorlaştırır. Kullanıcıların şifrelerini düz metin belgesinde saklaması ciddi sorunlara yol açar. Belgeye erişmeyi başaran herhangi bir bilgisayar korsanı, korumasız şifrelerden oluşan değerli bir kaynak ele geçirir. 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 parola olur ve kullanıcının erişimine izin verilebilir.

MD5 (Message Digest Algorithm 5) Hash Fonksiyonu: 1991 yılında Ronald Rivest tarafından geliştirilen bir hash fonksiyonudur. Girdinin büyüklüğü ne olursa olsun 128 bit uzunluğunda bir hash değeri (özet) üretir ve genellikle veri bütünlüğünü sağlamak, parmak izi oluşturmak, dijital imzaları doğrulamak gibi alanlarda kullanılır. Girdideki en ufak bir değişiklik, çıktının tamamen değişmesine sebep olur. MD5 genellikle veri bütünlüğünü doğrulamak için bir sağlama toplamı olarak kullanılır.

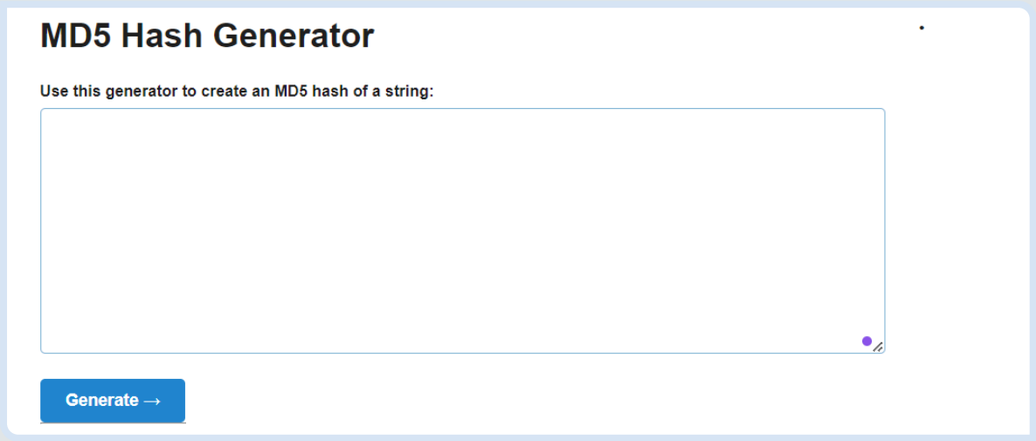
Bir verinin (dosyanın) doğru transfer edilip edilmediğinin veya değiştirilip değiştirilmediğinin kontrol edilmesi, MD5'in en fazla kullanıldığı yerlerden bazılarıdır. Bir dosya indirilirken dosyanın hash değeri de sağlanır ve dosyanın indirilmesinden sonra hash fonksiyonu çalıştırılarak orijinal hash değeriyle karşılaştırılır. Hash değerleri eşleşirse dosyanın bozulmadığı veya değiştirilmediği anlaşılır.

MD5 özellikle küçük veri bloklarının hızlı çalışmasıyla öne çıkmıştır ancak MD5'in çakışma problemleri, aynı hash değerinin farklı girdilerden elde edilebilmesi riskini doğurmuş ve bu durum, güvenlik açısından kritik uygulamalarda MD5'in yerini daha güvenli algoritmalara bırakmasına neden olmuştur. MD5 başlangıçta yaygın ve hızlı bir hash fonksiyonu olarak kullanılsa da bugün güvenli kabul edilmez. Onun yerine SHA-256 gibi daha güvenilir hash fonksiyonları tercih edilir.

2. UYGULAMA

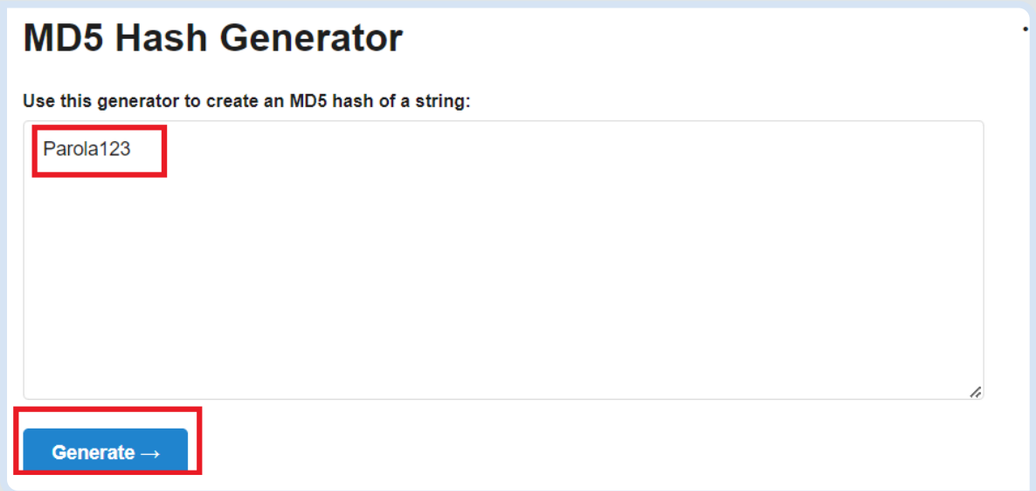
İşlem adımlarına göre online hashing hesaplama uygulamalarını kullanarak **Parola123** ve **Parola124** ifadelerinin hash değerlerini hesaplayınız.

1. Adım: Web tarayıcısına **MD5 Generator** yazarak çevrim içi bir hashing aracı bulunuz (Görsel 4.7).



Görsel 4.7: Hashing için kullanılacak çevrim içi araç

2. Adım: Metin kutusuna **Parola123** yazıp, **Generate** düğmesine basarak hashing işlemini yapınız (Görsel 4.8).

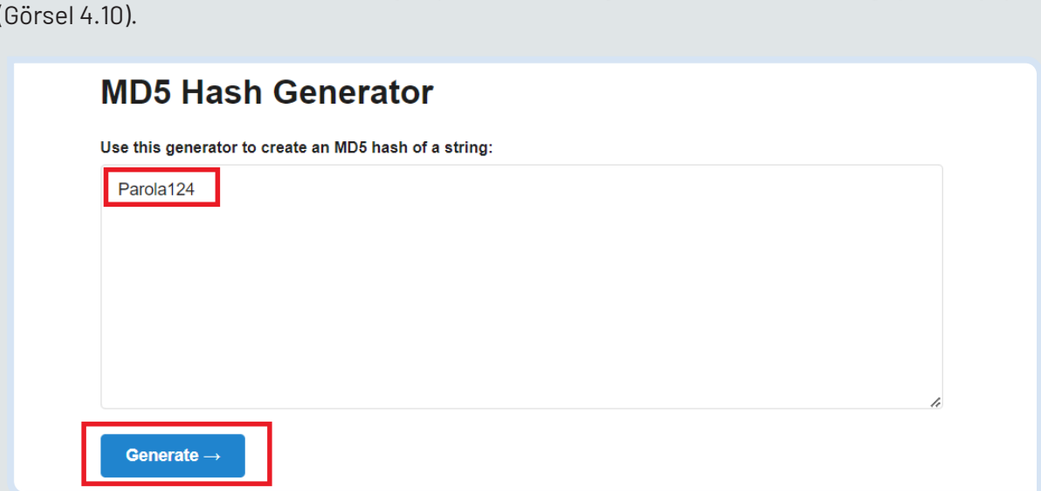


Görsel 4.8: Parola123 için hash değerinin üretilmesi

3. Adım: Üretilen hash değerini görüntüleyiniz (Görsel 4.9).

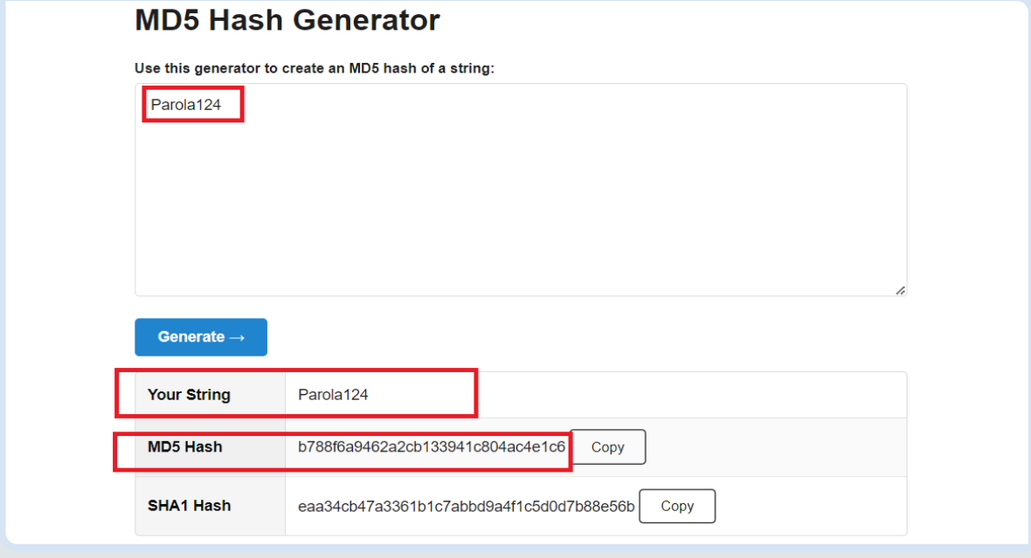
Görsel 4.9: Üretilen MD5 hash değeri

4. Adım: Metin kutusuna **Parola124** yazıp, **Generate** düğmesine basarak hashing işlemini yapınız (Görsel 4.10).



Görsel 4.10: Parola124 için hash değerinin üretilmesi

5. Adım: Üretilen hash değerini görüntüleyiniz (Görsel 4.11).



Görsel 4.11: Parola124 için hash değerinin üretilmesi

6. Adım: Parola123 ve **Parola124** arasında üretilen hash değerlerinin farkını inceleyiniz.

SHA-1 (Secure Hash Algorithm 1) Hash Fonksiyonu: 1995 yılında ABD Ulusal Güvenlik Ajansı (NSA) tarafından geliştirilmiş bir kriptografik hash fonksiyonudur. 160 bit uzunluğunda bir hash değeri üretir. Algoritmanın temel görevi, rastgele bilgileri sabit bir uzunluğa sahip değerlere dönüştürmektir. SHA-1, uzunluğu en fazla 264 bit olan mesajları girdi şeklinde kullanır ve 160 bitlik mesaj özeti üretir. Bu işlem sırasında ilk önce mesajı, 512 bitlik bloklara ayırır ve gerekirse son blok uzunluğunu 512 bite tamamlar. SHA-1 algoritması ile sadece şifreleme işlemi yapılır, şifre çözümleme işlemi yapılamaz.

Güvenliği artırmak amacıyla veriler, SHA-1 ve MD5 algoritmaları birbiri ardına kullanılarak şifrelenir. 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. SSL sertifika düzenleyicileri daha güvenilir olan SHA-256 kullanır. SHA-256'yı oldukça güvenli kılan özellikler şu şekilde sıralanabilir:

- İlk veriyi hash değerinden 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. Bu duruma **çığ etkisi** denir. Örneğin **Merhaba** kelimesinin SHA-256 hash kodu **7fdc9f4717c5fe66df286c700fab969b4d6209d03aa84624c5f8f58c17c9c058** iken **merhaba** kelimesinin SHA-256 hash kodu **4c6bcdd55f3153e1939669ab1ec039e4059174dc25abdfcb2f58868849b4d61b** olarak hesaplanır.

SIRA SİZDE

Çevrimiçi araçlar yardımıyla **Parola123** ve **Parola124** ifadelerinin SHA-256 hash değerini hesaplayınız.

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız. Çalışmanızı bir ders saati içinde tamamlayınız.

KONTROL LİSTESİ

DEĞERLENDİRME ÖLÇÜTLERİ	EVET	HAYIR
Çevrimiçi hashing araçlarını buldu.		
SHA-256 hash işlemini gerçekleştirdi.		
Hash değerlerini inceledi.		

Güvenli dosya alma ve gönderme işlemi sırasında **hashing** kullanarak dosya bütünlüğünü sağlamak mümkündür. Hash değerleri eşleştiğinde dosyanın güvenli şekilde alındığı alıcıya bildirilir. Hash değerleri uyuşmuyorsa dosyanın bozulduğu veya değiştirilmiş olabileceği bilgisi kullanıcıya iletilmelidir. Hashing işlemi şu şekilde gerçekleşir:

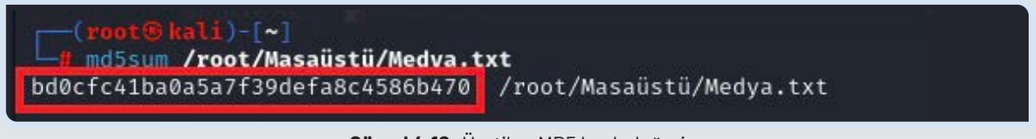
- Gönderen, dosyanın hash değerini hesaplar ve alıcıya dosyayla birlikte gönderir.
- Alıcı, dosyanın hash değerini yeniden hesaplar ve göndericiden gelen hash değeriyle karşılaştırır.
- Hash değerleri eşleşiyorsa dosya güvenli bir şekilde alınmış demektir.

Bu şekilde dosyanın transfer sırasında değiştirilip değiştirilmediği kolayca tespit edilir ve veri bütünlüğü sağlanır.

3. UYGULAMA

İşlem adımlarına göre **Medya.txt** isminde bir metin dosyası oluşturunuz ve içine **Medyada Siber Güvenlik** ifadesini yazarak hash değerini hesaplayınız. Ardından metin içeriğini değiştirerek hash değerini tekrar hesaplayınız ve dosyanın bütünlüğünü kontrol ediniz.

1. Adım: Kali Linux işletim sistemi komut satırına **md5sum** ve **dosya yolunu** yazarak hash değerini görüntüleyiniz (Görsel 4.12).



Görsel 4.12: Üretilen MD5 hash değeri

2. Adım: Medya.txt dosyasının içeriğini değiştirip, **md5sum** komutunu kullanarak tekrar hash değeri hesaplaması yapınız (Görsel 4.13).

```
┌──(root㉿kali)-[~]
└─# md5sum /root/Masaüstü/Medya.txt
30e3925476f5cc63b46a3abb1caaff75  /root/Masaüstü/Medya.txt
```

Görsel 4.13: İçerik değiştirilen MD5 hash değeri

3. Adım: İçerik değiştiğinde oluşan hash değeri farklılığını inceleyiniz (Görsel 4.14).

```
┌──(root㉿kali)-[~]
└─# md5sum /root/Masaüstü/Medya.txt
bd0cfc41ba0a5a7f39defa8c4586b470  /root/Masaüstü/Medya.txt

┌──(root㉿kali)-[~]
└─# md5sum /root/Masaüstü/Medya.txt
30e3925476f5cc63b46a3abb1caaff75  /root/Masaüstü/Medya.txt

┌──(root㉿kali)-[~]
└─# md5sum /root/Masaüstü/Medya.txt
bd0cfc41ba0a5a7f39defa8c4586b470  /root/Masaüstü/Medya.txt
```

Görsel 4.14: Hash değerlerinin değişimi

SIRA SİZDE

Bir metin dosyası hazırlayarak bu dosyanın hash değerini hesaplayınız. Ardından bu dosyayı arkadaşınıza e-posta olarak gönderiniz ve arkadaşınızın bunu güvenli bir şekilde aldığını teyit etmesini sağlayınız.

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız. Çalışmanızı bir ders saati içinde tamamlayınız.

KONTROL LİSTESİ

DEĞERLENDİRME ÖLÇÜTLERİ	EVET	HAYIR
Metin dosyasını oluşturdu ve bu dosyanın hash değerini hesapladı.		
Dosyayı e-posta olarak gönderdi.		
Gönderilen dosyanın hash değerini hesapladı.		
Gönderilen ve alınan dosyanın hash değerlerini karşılaştırdı.		
Dosyanın bütünlüğünü ve güvenliğini teyit etti.		

4.2. ASİMETRİK ŞİFRELEME YÖNTEMLERİ

Asimetrik şifreleme, şifreleme teknolojilerinde gizlilik ve güvenlik kavramlarını ön planda tutar. Simetrik şifreleme algoritmalarından farklı olarak asimetrik şifreleme algoritmaları, bir **genel anahtar (public key)** ve bir **özel anahtar (private key)** olmak üzere iki anahtar üzerinden çalışır (Görsel 4.15). Bu iki anahtar birbiriyle bağlantılıdır ancak her biri farklı işlevler için kullanılır. Açık anahtar, şifreleme işlemi için kullanılırken özel anahtar yalnızca şifreli veriyi çözmek amacıyla kullanılır. Bu sayede herhangi biri açık anahtarı kullanarak veriyi şifreleyebilir ancak sadece ilgili özel anahtara sahip olan kişi veya sistem bu veriyi çözebilir.

Görsel 4.15: Asimetrik şifreleme blok diyagramı

Asimetrik şifrelemenin en büyük avantajı, gizli anahtarın paylaşılma zorunluluğunu ortadan kaldırmasıdır. Açık anahtar herkesin erişimine açık olabilirken özel anahtar sadece alıcıda bulunduğu için yüksek güvenlik sağlar. Bu şifreleme yöntemi özellikle dijital imza ve güvenli veri alışverişi alanlarında yaygın olarak tercih edilir. Asimetrik şifreleme algoritmaları arasında en popüler olanı **RSA** algoritmasıdır. **Diffie-Hellman, DSA (Digital Signature Algorithm), Eliptik Eğri Şifreleme [Elliptic Curve Cryptography (ECC)]** gibi algoritmalar da kullanılır. Asimetrik algoritmalar, simetrik algoritmalara göre daha fazla hesaplama gücü gerektirdiği için genellikle daha yavaş çalışır ve bu nedenle küçük boyutlu verilerde veya anahtar değişimlerinde kullanılır.

4.2.1. RSA (Rivest-Shamir-Adleman) Şifreleme Tekniği

RSA algoritması, adını geliştiricileri olan Rivest, Shamir ve Adleman'ın baş harflerinden alır ve kriptografi dünyasında en yaygın kullanılan asimetrik şifreleme yöntemlerinden biridir. RSA'nın güvenilirliği, çok büyük asal sayıların çarpanlarına ayrılmasındaki hesaplama zorluğuna dayanır. Bu sayede algoritma oldukça yüksek bir güvenlik sunar ancak bu karmaşık matematiksel işlemler sebebiyle RSA, diğer şifreleme yöntemlerine kıyasla daha yavaş çalışabilir. Güvenilirliği sayesinde RSA; bankacılık, e-ticaret ve dijital imzalama işlemlerinde yaygın olarak kullanılır. RSA özellikle dijital imza ve kimlik doğrulama işlemlerinde sıkça tercih edilir. RSA, HTTPS bağlantıları gibi güvenli internet protokollerinin yanı sıra SSH gibi uzaktan erişim araçlarında kritik bir rol oynar. Her ne kadar güvenli bir algoritma olsa da zayıf anahtar yönetimi veya yanlış yapılandırmalar sonucu istismar edilebilecek zafiyetler içerebilir. Buna rağmen güçlü anahtar boyutları ve doğru kullanımla hâlâ en güvenilir şifreleme yöntemlerinden biri olarak kabul edilir.

RSA şifreleme yöntemi; anahtar oluşturma, şifreleme ve şifre çözme aşamalarından oluşan asimetrik bir algoritmadır. Bu yöntemde güvenli iletişimi sağlamak için bir ortak anahtar ve bir özel anahtar kullanılır. Ortak anahtar, mesajı şifrelemek için herkesin erişebileceği şekilde paylaşılırken özel anahtar sadece alıcıya özeldir ve şifrelenmiş mesajı çözmek için kullanılır.

RSA şifreleme yönteminde işlemler şu şekilde gerçekleşir:

1. Anahtar Oluşturma: RSA algoritmasında anahtarlar, büyük asal sayıların kullanımıyla oluşturulur. İlk adımda rastgele iki büyük asal sayı (p ve q) seçilir. Bu asal sayıların çarpımı, **n** olarak adlandırılır ve **n = p * q** formülüyle hesaplanır. Ardından Totient fonksiyonu kullanılarak **Φ (n) = (p-1)(q-1)** değeri bulunur. Bu işlem, RSA'nın güvenlik temeli olan önemli bir adımdır. Şifreleme işlemi için bir **e** sayısı seçilir. Bu sayı, **1 < e < Φ (n)** koşulunu sağlayacak şekilde ve **Φ (n)** ile aralarında asal olmalıdır. Bu **e** sayısı, sistemin ortak anahtarıdır. Özel anahtarı oluşturmak için **d** değeri hesaplanır. **d, e** ile ters modüler işlem sonucu bulunur ve bu sonuç, gizli anahtar olarak kullanılır.

2. Şifreleme: Anahtarlar oluşturulduktan sonra şifreleme işlemine geçilir. Mesajın ASCII karşılıkları bulunur ve mesaj, **mesaj^e mod n** formülüyle şifrelenir. Bu işlem, mesajın güvenli bir şekilde şifrelenmesini sağlar ve sadece ilgili özel anahtar tarafından çözülebilir. Örneğin **A** karakterinin ASCII değeri 41'dir. Bu nedenle şifreleme işleminde bu sayı kullanılır.

3. Şifre Çözme: Şifrelenmiş mesajı çözmek için özel anahtar kullanılır. Bu işlem, **şifrelenmiş mesaj^d mod n** formülüyle gerçekleştirilir. Bu aşamada mesaj, orijinal formuna geri dönüştürülür ve alıcı, mesajı deşifre ederek okuyabilir. RSA'nın temel güvenliği, büyük asal sayıların çarpanlarına ayrılmasının zorluğuna dayandığı için şifreleme işlemi oldukça güvenli kabul edilir. Bu adımlar sayesinde RSA, dijital imzalar ve güvenli veri iletiminde yaygın olarak kullanılır.

4.2.2. Diffie-Hellman Anahtar Değişimi

Diffie-Hellman anahtar değişimi, iki tarafın güvenli şekilde ortak bir gizli anahtar oluşturmasına olanak tanıyan asimetrik bir kriptografik algoritmadır. Bu yöntem özellikle güvenli iletişim sağlamak amacıyla açık kanallar üzerinden gizli anahtarın paylaşılmadan oluşturulmasını mümkün kılar. Diffie-Hellman algoritmasının temelinde matematiksel bir işlem süreci yatar ve bu süreç, iki tarafın kendine ait gizli anahtarı kullanarak ortak bir anahtar üretmesi ile sonuçlanır.

Bu işlemde taraflar birbirleriyle yalnızca açık anahtarlarını paylaşır. Taraflardan her biri, kendi gizli anahtarını kullanarak ortak anahtarı hesaplar. Bu hesaplama sürecinde kullanılan matematiksel prensip, **gab = gba** ifadesine dayanır. Başka bir deyişle her iki tarafın gizli anahtarı farklı olsa da üretilen ortak anahtar, her iki taraf için aynı olur. Bu ortak anahtar, daha sonra taraflar arasında şifreli veri iletişimini sağlamak için kullanılır.

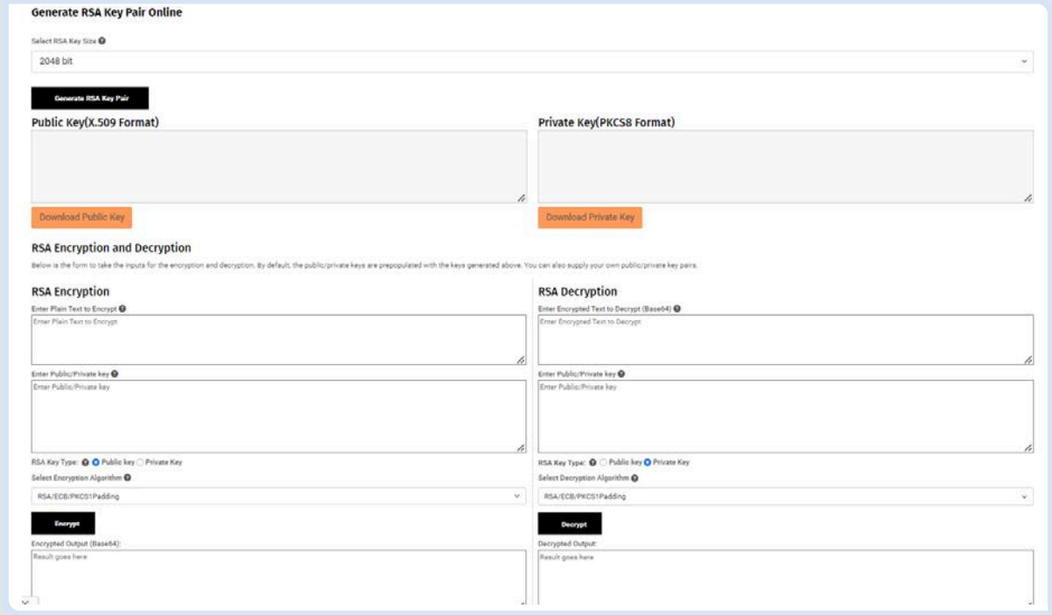
Diffie-Hellman algoritması özellikle başlangıçta iki taraf arasında güvenli bir iletişim kanalı oluşturmak amacıyla kullanılır. Bu yöntem tek başına veri şifrelemez sadece şifreleme için kullanılacak gizli anahtarın güvenli bir şekilde üretilmesini sağlar. Genel ağ üzerinden veri paylaşımında güvenliği sağlamak için yaygın bir şekilde kullanılan bu yöntem, gizli anahtar paylaşımı sırasında araya girme saldırılarına karşı etkili bir güvenlik sunar.

Diffie-Hellman anahtar değişimi, internet üzerindeki güvenli iletişimde kritik bir protokoldür. Özellikle sanal özel ağlar (VPN) kullanılarak yapılan veri iletiminde şifreleme işlemini güvenli hâle getirir. Ayrıca kripto para birimleri ve blockchain tabanlı uygulamalarda kullanıcıların anahtar paylaşımını güvenli bir şekilde gerçekleştirmelerini sağlar. Şifreli mesajlaşma platformları da kullanıcılar arasında güvenli bir iletişim sağlamak için bu yöntemi tercih eder. Sonuç olarak Diffie-Hellman anahtar değişimi, birçok dijital sistemde veri güvenliğini sağlamak amacıyla önemli bir işlevi yerine getirir.

4. UYGULAMA

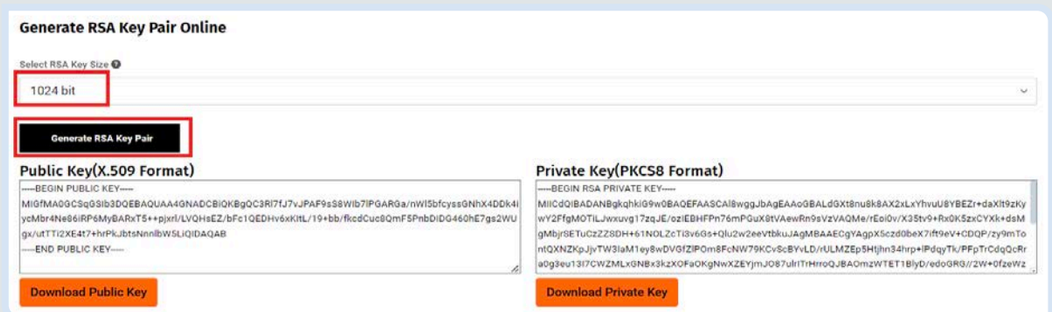
İşlem adımlarına göre online RSA şifreleme tekniği kullanan araçlarla anahtar değişimi uygulamasını gerçekleştiriniz.

1. Adım: Web tarayıcısına **Online rsa key generator** yazarak çevrimiçi bir RSA aracı bulunuz (Görsel 4.16).



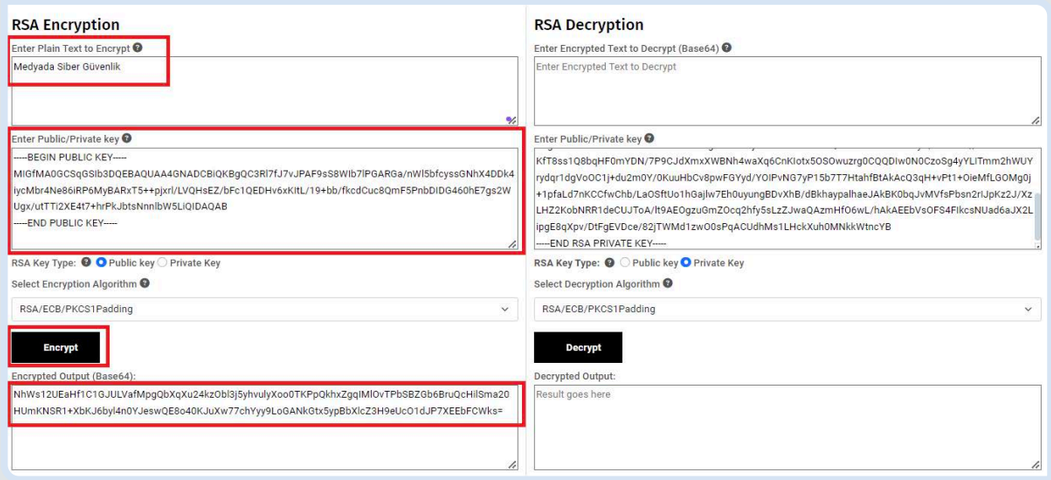
Görsel 4.16: RSA şifreleme için kullanılacak çevrimiçi araç

2. Adım: 1024 bitlik bir RSA anahtar çifti oluşturunuz ve sonrasında **Generate RSA Key Pair** düğmesine basarak genel ve özel anahtarı oluşturunuz (Görsel 4.17).



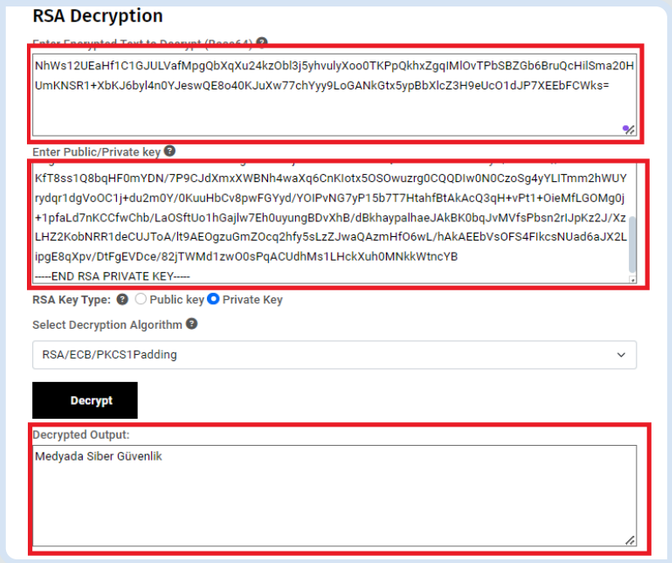
Görsel 4.17: Genel ve özel anahtarın oluşturulması

3. Adım: Şifrelenmesini istediğiniz metni giriniz ve ardından **encryp** düğmesine basınız. Üretilen genel anahtarı ve kriptolanmış bilgiyi görüntüleyiniz (Görsel 4.18).



Görsel 4.18: Verinin kriptolanması

4. Adım: Kriptolanmış veriyi kopyalayarak ilgili alana giriniz. Ardından **decrypt** düğmesine basarak verinin açık metin hâlini görüntüleyiniz. İşlem yapılırken özel anahtarın kullanıldığını doğrulayınız (Görsel 4.19).



Görsel 4.19: Decrypt işleminin sonucu

4.3. STEGANOGRAFİ YÖNTEMLERİ

Steganografi, kökeni Antik Yunan'a dayanan ve **gizli yazı** anlamına gelen bir yöntemdir. Siber güvenlik bağlamında steganografi, bilgileri görünmeyen biçimde saklayarak üçüncü şahısların iletilen gerçek mesajdan haberdar olmamasını sağlamak amacıyla kullanılır. Bu teknoloji, mesajların içinde gizli verilerin saklanmasını ve bu bilgilerin yalnızca yetkili kişiler tarafından anlaşılmasını sağlar. Örneğin "**M**ehmet **e**kmeği **d**oğru **y**erden **a**ldı." şeklindeki bir cümlede ilk harfler kullanılarak gizli bir mesaj oluşturulabilir. Bu metnin ilk harfleri **Medya** şeklinde sıralanabilir ve başka bir teknik, şifrelenmiş bir mesajın açığa çıkmasını sağlayabilir. Bir başka örnek ise kelimelerin belirli harflerini kullanarak gizli bir mesaj oluşturma yöntemidir. "**S**abah, t**i**lkileri am**b**arın **e**trafında a**r**ıyorlardı." cümlesinde sırasıyla kelimelerin 1, 2 ve 3. harfleri alınarak ve sonrasında tekrar 1, 2 ve 3. harfleri alınarak **Siber** gibi bir şifreleme gerçekleştirilebilir.

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 arkadaşlarınızla kendi belirleyeceğiniz 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

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız. Çalışmanızı bir ders saati içinde tamamlayınız.

KONTROL LİSTESİ

DEĞERLENDİRME ÖLÇÜTLERİ	EVET	HAYIR
Steganografi yapmak için bir metin hazırladı.		
Metni gizlemek için bir mantık oluşturdu.		
Şifrelenmiş metni elde etti.		
Sınıf arkadaşları ile takım çalışmasına uygun davrandı.		
Zamanı verimli kullandı.		

4.3.1. Resim İçine Resim Gizleme Tekniği

Dijital resimlerin gizli verileri barındırma yeteneğini anlamak için önce dijital resimlerin nasıl çalıştığını bilmek gerekir. Dijital resimler, her biri bir renk tonunu temsil eden piksellerden oluşur. Bu pikseller, belirli bir renk ve parlaklık seviyesindeki değerleri saklar ve genellikle bir matris şeklinde düzenlenir. Resimler genellikle kırmızı, yeşil ve mavi (RGB) renk modeline dayanarak oluşturulur. Bu modelde her bir piksel, her biri 8 bitlik üç renk kanalından oluşur ve bu da toplamda 24 bitlik renk derinliği sağlar. Her bir renk kanalı 0 ile 255 arasında değer alabilir. Bu durum, piksellere geniş

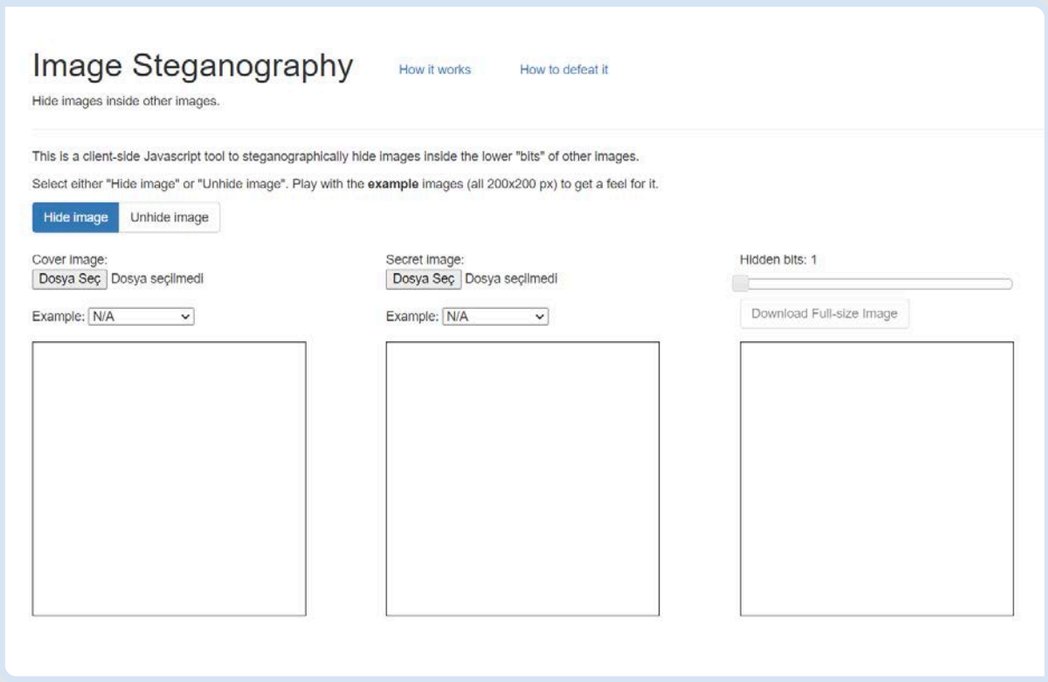
bir renk aralığı sunar. Örneğin bir pikselle temsil edilen renk, RGB modelinde belirli bir bit dizilimi ile ifade edilir. En soldaki bitler, renk değerinin en anlamlı kısımlarını belirlerken en sağdaki bitler, renk değişikliklerinde daha az etkili olur. Bu nedenle piksellerdeki en az anlamlı bitlerin değiştirilmesi, resmin genel görünümünde çok küçük değişiklikler yapar ve insan gözü bu değişiklikleri fark edemez. Bu özellik, steganografi tekniğinin temelini oluşturur. Başka bir deyişle bir resmi, diğer bir resmin içine gizlice yerleştirme yöntemini mümkün kılar.

Resim içine veri gizleme işlemi, birçok farklı teknikle gerçekleştirilebilir. Hem Linux hem de Windows işletim sistemi için geliştirilmiş çeşitli özel yazılımlar bu işlemi desteklerken internet üzerindeki çevrimiçi araçlar da kullanıcıların bu işlemleri kolayca yapabilmesine olanak sağlar. Steganografi teknikleri, dijital medya üzerinde veri gizlemede etkilidir. Bu teknikler sayesinde görünüşte zararsız bir resim, gizli bilgileri saklamak için kullanılabilir.

5. UYGULAMA

İşlem adımlarına göre çevrimiçi araçlar kullanarak resim içine resim gizleme işlemini gerçekleştiriniz.

1. Adım: Web tarayıcısına **image steganography** yazarak resim içine resim gizlemek için çevrimiçi araç bulunuz (Görsel 4.20).



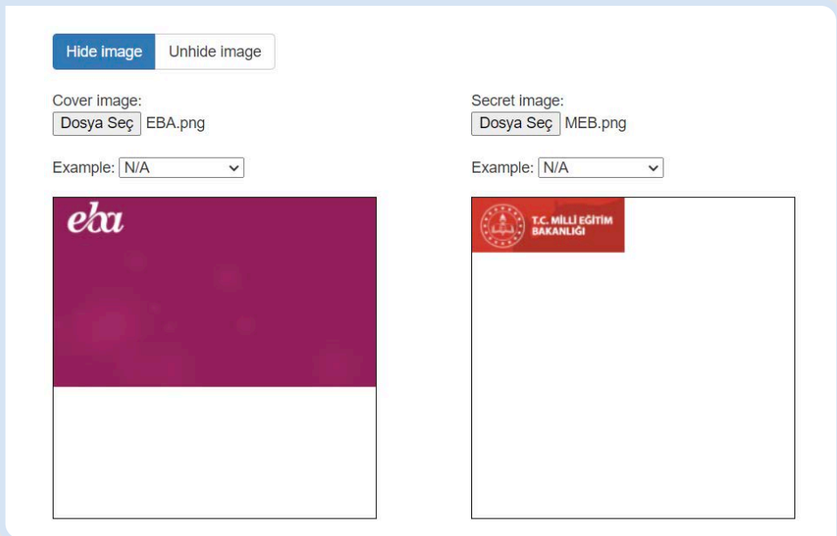
Görsel 4.20: Resim içine resim gizleme için kullanılacak çevrimiçi araç

2. Adım: Hide image düğmesine basınız. Bu özellik, resim gizlemek için kullanılır.

3. Adım: Cover image başlığı altındaki **Dosya Seç** düğmesine basınız ve ana resmi seçiniz. Seçilen resmin içine başka bir resim gizlenecektir (Görsel 4.21).

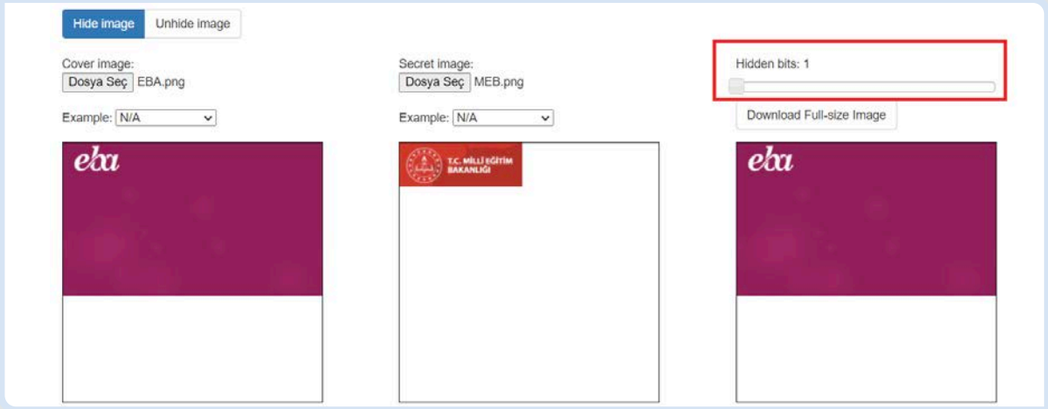
Görsel 4.21: Ana resmin seçilmesi

4. Adım: Secret image düğmesinin altındaki **Dosya Seç** butonuna basınız. Gizlemek istediğiniz resmi seçiniz (Görsel 4.22).



Görsel 4.22: Gizlenecek resmin seçilmesi

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 gizlemek mümkün olmayabilir. Bu nedenle **Hidden bits: 1** olarak seçiniz (Görsel 4.23).



Görsel 4.23: Hidden bits ayarı

6. Adım: Gizleme işlemi tamamlanınca hazırlanan resim dosyasını **Download Full-size Image** düğmesine basarak indiriniz.

SIRA SİZDE

Beşinci uygulamada indirdiğiniz resimde gizlenen resmi, aynı aracı kullanarak tekrar ortaya çıkarınız.

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız. Çalışmanızı bir ders saati içinde tamamlayınız.

KONTROL LİSTESİ

DEĞERLENDİRME ÖLÇÜTLERİ	EVET	HAYIR
Çevrimiçi aracı açtı.		
Unhide image seçeneğini seçti.		
Mesaj gizlenen resmi seçti.		
Mesaj gizlenen resmi ekledi.		
Hidden bitsleri değiştirerek gizlenen resmi ortaya çıkardı.		
Gizlenen resmi bilgisayara indirdi.		

4.3.2. Resim İçine Metin Gizleme Tekniği

Dijital resimler ve diğer multimedya materyaller, temelinde ikili sistem olan 1 ve 0'lar ile temsil edilir. Bu yapının bir avantajı, resimlerin içine neredeyse fark edilmeyecek şekilde veri gizlenebilmesidir. Bu tekniğin uygulanabilmesi için çeşitli yazılımlar ve araçlar mevcuttur. Linux tabanlı sistemlerde bu işlem için yaygın olarak kullanılan araçlardan biri **Steghide**'dir. Steghide, ses ve resim dosyalarının içine metin veya başka veri türlerini gizleyebilen güçlü bir steganografi aracıdır. Benzer şekilde Windows işletim sistemlerinde de benzer işlevleri görebilen çeşitli araçlar mevcuttur. Bu araçlar, kullanıcıların gizli mesajları veya verileri görsel dosyaların içine entegre etmelerini sağlar. Böylece veri aktarımını daha güvenli ve gizli hâle getirir. Metin gizleme tekniği sadece veri güvenliği için değil dijital sanat ve iletişimde yaratıcı bir ifade aracı olarak da kullanılır.

6. UYGULAMA

Linux işletim sisteminde masaüstüne bir resim ve resmin içine bir metin belgesi oluşturarak steghide aracı ile resim içine metin gizleme tekniğini uygulayınız.

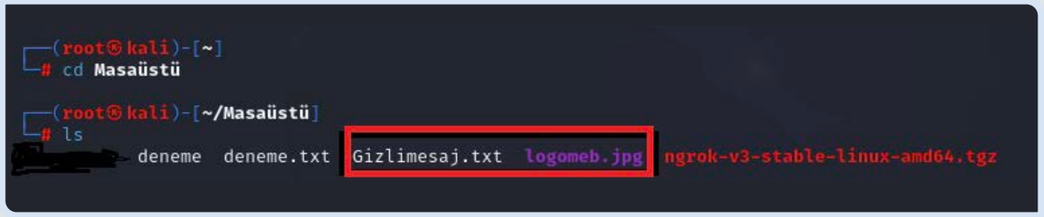
1. Adım: Sisteminizde **steghide** aracı yüklü değilse komut satırından **root** kullanıcısıyla **apt-get install steghide** komutunu yazarak yükleme işlemini gerçekleştiriniz (Görsel 4.24).

Görsel 4.24: Steghide aracının kurulumu

2. Adım: İşletim sisteminizde masaüstüne içine mesaj gizlenecek bir resim yükleyiniz. Bir metin dosyası oluşturarak içine gizli mesajınızı yazınız (Görsel 4.25).

Görsel 4.25: Resim içine metin gizleme tekniği için ilgili dosyaların oluşturulması

3. Adım: Oluşturduğunuz dosyaların Linux komut satırıyla masaüstünde listelenmesini sağlayınız (Görsel 4.26).



Görsel 4.26: Dosyaların listelenmesi

4. Adım: steghide embed –cf logomeb.jpg –ef Gizlimesaj.txt komutunu yazdıktan sonra parola girerek resim içine metin gizleme tekniğini uygulayınız. Örnekteki parola medya olarak oluşturulmuştur (Görsel 4.27).

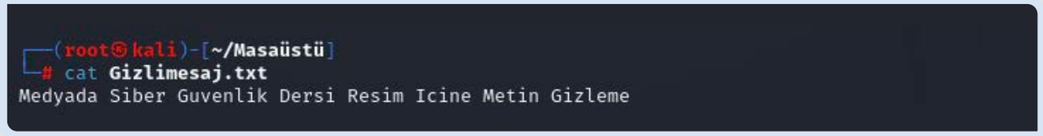
Görsel 4.27: Resim içine metin gizleme tekniğinin uygulanması

5. Adım: Resim içine metin gizleme tekniğini uyguladığınız resmi açarak resimde bir değişiklik olup olmadığını görüntüleyiniz.

6. Adım: steghide –extract –sf logomeb.jpg –p medya komutunu girerek resim içine metin gizleme tekniği uygulanan görselin içindeki **Gizlimesaj.txt** dosyasına ulaşım sağlayınız (Görsel 4.28).

Görsel 4.28: Gizli mesajın açılması

7. Adım: Metin dosyasının olduğu konumda cat **Gizlimesaj.txt** komutunu yazarak mesajın içeriğine ulaşınız (Görsel 4.29).



Görsel 4.29: Gizli mesajın görüntülenmesi

SIRA SİZDE

Altıncı uygulamadaki resim içine metin gizleme tekniğini, Windows işletim sistemini kullanarak tekrar uygulayınız.

DEĞERLENDİRME

Çalışmanız aşağıda yer alan kontrol listesi kullanılarak değerlendirilecektir. Çalışmanızı yaparken değerlendirme ölçütlerini dikkate alınız. Çalışmanızı bir ders saati içinde tamamlayınız.

KONTROL LİSTESİ

DEĞERLENDİRME ÖLÇÜTLERİ	EVET	HAYIR
Windows işletim sisteminde dosyaları hazırladı.		
Gerekli sıkıştırma işlemini yaptı.		
Komut satırı ile resim içine metin gizledi.		
Resim içine metin gizleme tekniği uygulanan görseldeki değişiklikleri inceledi.		
Gizli mesajı görüntülemek için komut satırından tekrar tersine işlem uyguladı.		
Gizli mesajı görüntüledi.		

ÖLÇME VE DEĞERLENDİRME

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

1. ( ) Simetrik şifreleme sistemlerinde hem şifreleme hem deşifre çözme işlemleri farklı anahtarlar kullanılarak gerçekleştirilir.

2. ( ) Genellikle hızlı çalışan simetrik şifreleme algoritmaları, az hesaplama gücü gerektirir.

3. ( ) Gizli veri saklama yöntemi olarak sadece metin dosyalarında kullanılan steganografi, diğer medya dosyalarında kullanılamaz.

4. ( ) Asimetrik anahtarlama sisteminde hem şifreleme hem de şifre çözme işlemleri aynı anahtar kullanılarak gerçekleştirilir.

5. ( ) Dijital imzaların doğrulanmasında kullanılan asimetrik anahtarlamada mesajın doğruluğunu kontrol etmek için açık anahtar gereklidir.

B) Aşağıdaki sorularda doğru cevabı işaretleyiniz.

6. Aşağıdakilerden hangisi simetrik şifrelemenin avantajlarını ve dezavantajlarını doğru bir şekilde tanımlar?

A) Simetrik şifreleme, veri şifreleme sürecini daha karmaşık ve verimsiz hâle getirir, bu nedenle büyük veri setleri için uygun değildir.

B) Simetrik şifreleme algoritmaları genellikle daha az hesaplama gücü gerektirir ve daha az depolama alanı kullanır ancak gizli anahtarın güvenli bir şekilde dağıtılması zor olabilir.

C) Simetrik şifreleme, şifreleme ve şifre çözme işlemi için her kullanıcıya ayrı bir anahtar kullanarak anahtar yönetimini kolaylaştırır.

D) Simetrik şifreleme, verileri şifrelemek için açık anahtarlar kullanır ve bu nedenle anahtar dağıtımı konusunda herhangi bir zorluk yaşanmaz.

E) Simetrik şifreleme algoritmaları, karmaşık matematiksel işlemler gerektirdiği için genellikle hızlı işlem yapamaz.

7. Aşağıdakilerden hangisi steganografi yöntemlerinin bir özelliğini doğru olarak tanımlar?

A) Steganografi, verileri şifreleyerek güvenliğini artırır ve sadece şifre çözme işlemi yapar.

B) Steganografi, verileri görünür hâle getirerek şifreli verileri açık bir şekilde saklar.

C) Steganografi, gizli verilerin mevcut veriler içinde saklanmasını sağlar ve yalnızca yetkili kişiler tarafından gizli verilere erişilmesini sağlar.

D) Steganografi yalnızca metin mesajlarını gizlemek için kullanılabilir, ses ve resim verileri üzerinde uygulanamaz.

E) Steganografi yöntemi, gizli verileri şifreleyerek ve metin dosyası içinde saklayarak bilgiyi herkesin erişebileceği şekilde sunar.

8. RSA algoritması ile ilgili aşağıdaki ifadelerden hangisi doğrudur?

A) Sadece şifreleme için kullanılabilir, bu algoritmayla şifre çözme işlemi mümkün değildir.

B) Algoritmanın güvenliği, büyük asal sayıların çarpanlarına ayrılmasındaki hesaplama zorluğuna dayanır.

C) Anahtarlar yalnızca bir kez oluşturulur ve tekrar kullanılmaz.

D) Yalnızca veri şifreleme işlemlerinde kullanılır ve dijital imzalama işlemlerinde kullanılmaz.

E) Şifreleme ve şifre çözme işlemleri aynı anahtar kullanılarak yapılır.

9. Aşağıdakilerden hangisi asimetrik şifrelemenin en büyük avantajıdır?

A) Açık anahtarın gizli kalmasını sağlar.

B) Şifreleme işlemlerini hızlandırır.

C) Gizli anahtarın paylaşılma zorunluluğunu ortadan kaldırır.

D) Şifreleme ve şifre çözme işlemlerini aynı anahtar ile gerçekleştirir.

E) Anahtarları yalnızca tek bir kez kullanır ve tekrar oluşturmaz.

10. Aşağıdakilerden hangisi Diffie-Hellman anahtar değişimi algoritmasının en büyük kısıtlamasıdır?

A) Anahtarlar yalnızca tek bir kez kullanılır.

B) Anahtarların gizli kalması gereklidir.

C) Veri şifrelemesi doğrudan gerçekleştirilir.

D) Anahtar paylaşımı sırasında araya girme saldırılarına karşı savunmasızdır.

E) Anahtarlar simetrik olarak şifrelenmiş şekilde paylaşılır.

NOT

CEVAP ANAHTARI

		1. ÖĞRENME BİRİMİ	2. ÖĞRENME BİRİMİ	3. ÖĞRENME BİRİMİ	4. ÖĞRENME BİRİMİ
1	DOĞRU-YANLIŞ	Y	Y	D	Y
2		D	D	Y	D
3		D	D	Y	Y
4		Y	D	D	Y
5		D	Y	Y	D
6	ÇOKTAN SEÇMELİ	C	D	C	B
7		B	A	B	C
8		A	A	A	B
9		E	E	C	C
10		D	D	E	D

GENEL AĞ KAYNAKÇASI VE GÖRSEL KAYNAKÇASI

Ders materyalinin genel ağ kaynakçası ve görsel kaynakçasına buradan ulaşılır. Karekoda ulaşılamaması durumunda aşağıdaki link kullanılabilir.

http://kitap.eba.gov.tr/karekod/Kaynak.php?KOD=4065

NOT

NOT