SİBER GÜVENLİĞE BÜTÜNCÜL BAKIŞ

İÇERİK

1- *SİBER GÜVENLİK NEDİR?*

Siber güvenlik, en basit tanımıyla, ülkelerin sınırlarının askerler tarafından korunmasına benzer şekilde, dijital sistemleri koruyan ekiplerin faaliyetidir. Bilgisayar sistemlerinin ve bu sistemlerde depolanan bilginin güvenliğini ifade eder. Bir başka deyişle, dijital bilgi ve sistemlerin yetkisiz kullanım veya erişime karşı korunması olarak tanımlanabilir.

Günümüzde bilginin büyük çoğunluğu bilgisayar ortamında üretilmekte ve saklanmaktadır. Bu durum, siber güvenliğin önemini artırmaktadır; zira iletişimden ticarete kadar pek çok hayati süreç dijitalleşmiştir. Bilginin kolayca erişilebilir olması, korunmasını daha kritik hale getirmektedir.

Gelişen dünyada iletişimin büyük bir kısmı dijital ortamdan sağlandığından ve çevrimiçi olarak erişilebilir olduğundan, siber güvenlik bu çevrimiçi sistemlerin bütünlüğünü, gizliliğini ve erişilebilirliğini korumak için vazgeçilmez bir gereklilik haline gelmiştir. Bu sayede hem bireysel hem de ulusal dijital varlıkların güvenliği sağlanmış olur.

2- *SİBER GÜVENLİKTE TEMEL TERİMLER EV KAVRAMLAR:*

- **Attack***:* Siber saldırı**,** bilgisayar kullanarak veri çalmaya veya bilgisayarlara ve ağlara yetkisiz erişim sağlamaya çalışma sürecidir. Siber saldırı, genellikle bir

saldırganın veri ihlali gerçekleştirmeden önce bireysel veya kurumsal bilgisayarlara veya ağlara yetkisiz erişim elde etmek için attığı ilk adımdır .

Gerçek hayattan örnekler:

Devlet Destekli Endüstriyel Sabotaj: Stuxnet (2010),

Kritik Altyapının Felç Edilmesi: Colonial Pipeline (2021),

Küresel Felç ve Yıkım: NotPetya (2017),

Büyük Veri İhlali: Yahoo (2013–2014),

Jeopolitik Saldırı: Estonya Siber Saldırıları (2007)

- **Ransomware**: Fidye yazılımı saldırıları, finansal olarak desteklenen bir kötü amaçlı yazılım saldırısı biçimidir. Saldırganlar, indirildiğinde belirli verileri ve dosyaları veya tüm bilgisayarları şifreleyen kötü amaçlı bir ek içeren mesajlar gönderir. Saldırgan daha sonra kurbandan fidye talep eder ve yalnızca ödeme yapıldığında verilere erişimi serbest bırakır veya geri yükler.

Gerçek hayattan örnekler:

WannaCry (2017),

NotPetya (2017),

Colonial Pipeline Saldırısı (2021),

Garmin Saldırısı (2020)

- **MFA/Multi-Factor Authentication:** Çok faktörlü kimlik doğrulama (MFA) , çevrimiçi hesap parolası ve parmak izi veya diğer biyometrik veriler gibi en az iki farklı kanıt türü gerektirerek bir kullanıcının kimliğini doğrulamanın bir yoludur . Çok faktörlü kimlik doğrulama, parolaların tek başına sunabileceği korumanın ötesinde ek koruma katmanları sağlar.

Gerçek hayattan örnekler:

Uber Saldırısı (2022) — MFA Fatigue,

Cisco Saldırısı (2022) — (Vishing),

Okta/MGM Resorts ve Caesars Entertainment Saldırıları (2023) — Servis Masası Manipülasyonu,

Adversary-in-the-Middle (AiTM) Saldırıları

- **Exploit:** Bir exploit, bir uygulama veya bilgisayar sistemindeki bir güvenlik açığını veya güvenlik açığını bulup bundan yararlanmak için tasarlanmış bir program veya kod parçasıdır. Genellikle kötü amaçlı yazılım yüklemek gibi kötü amaçlı amaçlar için kullanılır. Bir exploit, kötü amaçlı yazılımın kendisi değil, siber suçlular tarafından kötü amaçlı yazılım dağıtmak için kullanılan bir yöntemdir .

Gerçek hayattan örnekler:

WannaCry (2017),

SolarWinds Tedarik Zinciri Saldırısı (2020),

MOVEit Dosya Aktarımı Exploit'i (2023)

- **Firewall:** Firewall (güvenlik duvarı), ağ trafiğini kontrol ederek yetkisiz erişimleri engelleyen ve ağ güvenliğini sağlayan bir güvenlik sistemidir. Temel olarak, önceden tanımlanmış güvenlik kurallarına göre gelen ve giden tüm ağ trafiğini filtreler. Zararlı veya şüpheli trafiği tespit ederek engellerken, izin verilen trafiğin sorunsuz bir şekilde akmasını sağlar.

Firewall hizmeti sunan şirketler:

Fortinet, Palo Alto Networks, Check Point, Sophos, Forcepoint, SonicWall, WatchGuard

- **Phishing:** "Kimlik avı", genellikle kullanıcı adları, parolalar, kredi kartı numaraları, banka hesap bilgileri veya diğer önemli veriler gibi hassas bilgileri çalmak ve bu bilgileri kullanmak veya satmak amacıyla yapılan bir girişimi ifade eder. Cazip bir istekle güvenilir bir kaynak gibi görünen saldırgan, tıpkı bir balıkçının balık yakalamak için yem kullanması gibi, kurbanı kandırmak için onu kandırır.

Gerçek hayattan örnekler:

Demokratik Ulusal Komite (DNC) Olayı (2016),

RSA SecurID İhlali (2011),

Hedef (Target) Veri İhlali (2013),

İş E-postası Uzlaşması (Business Email Compromise — BEC) Örnekleri

- **Vulnerability:** Güvenlik açıkları, saldırganların bir sisteme erişmesine, kod çalıştırmasına, kötü amaçlı yazılım yüklemesine ve hassas verileri çalmak, yok etmek veya değiştirmek için dahili sistemlere erişmesine olanak tanır. Tespit edilmezse, saldırganlar tam erişim ayrıcalıklarına sahip süper kullanıcı veya sistem yöneticisi gibi davranabilir.

Gerçek hayattan örnekler:

Stuxnet (2010),

WannaCry (2017),

Equifax Veri İhlali (2017),

Log4j (“Log4Shell”) Zafiyeti (2021),

- **Encryption:** Şifreleme , veri ve bilgilerin güvenliğini sağlamak için kullanılan bir teknolojidir. Bu işlem, verilerin matematiksel bir algoritma kullanılarak şifrelenmesini ve yalnızca doğru şifreleme anahtarına sahip olan kişilerin erişebilmesini sağlar. Şifreleme, bilgisayar sistemleri, internet iletişimi, akıllı telefonlar ve diğer cihazlarda sıklıkla kullanılır.

Gerçek hayattan örnekler:

Heartbleed Zafiyeti (2014),

ROBOT Saldırısı (2017),

DigiNotar Saldırısı (2011),

WannaCry ve NotPetya (2017),

Colonial Pipeline Saldırısı (2021),

- **Payload:** Bilgisayar programlama açısından yük terimine baktığımızda, birçok uygulama ve sistem düzenli olarak çevrimiçi veri ve bilgi paylaşımında bulunur. Bu verinin her birimi hareket ettiğinde, iki temel parçaya sahiptir: başlık (veya üstbilgi tanımlayıcısı) ve yük (iletilen gerçek bilgi).

Başlık, kaynak ve hedef gibi ayrıntıları içerirken, yük, bir uygulamanın veya sistemin çalışması gereken gerçek mesajı taşır.

Örnek:

Press enter or click to view image in full size

```
{
   "data":{
      "message":"Merhaba dünya!"
   }
}
```

"*Merhaba, dünya!*" değeri yük, geri kalanı ise protokol yüküdür.

Görsel Linki

- **Malware:** Kötü amaçlı yazılım, kısaltmasıyla malware olarak da bilinen kötü amaçlı yazılım, siber suçlular tarafından veri çalmak ve bilgisayarlara ve bilgisayar sistemlerine zarar vermek veya yok etmek için geliştirilen her türlü müdahaleci yazılımı ifade eder. Yaygın kötü amaçlı yazılım örnekleri arasında virüsler, solucanlar, Truva atları, casus yazılımlar, reklam yazılımları ve fidye yazılımları bulunur.

Gerçek hayattan örnekler:

Stuxnet (2010) — Siber Silah,

Mirai (2016) — Botnet Yazılımı,

Emotet (2014-Halen Değişen) — Truva Atı ve Dağıtıcı,

- **Authorization:** *Yetkilendirme,* bir bilgisayar sisteminde kimlik doğrulama , bir kullanıcının iddia ettiği kişi olduğunu doğrulayan süreçtir. Temel olarak bir sistemdeki kullanıcının veya hizmetin, belirli bir kaynağa (dosya, veri, işlev, uygulama vb.) erişme veya belirli bir eylemi gerçekleştirme **iznine sahip olup olmadığını** kontrol etme mekanizmasıdır.

- **Authentication:** Kimlik doğrulaması, oturum açan kişinin gerçekten o kişi olduğunu, yani kimliğini doğrularken yetkilendirme, bu kişinin erişmeye çalıştıkları bilgilere erişim izni olduğunu doğrular.

Örneğin, insan kaynaklarından bir çalışanın bordro veya çalışan dosyaları gibi diğer birimlerdeki çalışanların göremedikleri dosyaların yer aldığı sistemlere erişim izni olabilir.

- **Patch Management:** Yama yönetimi, sistem yöneticisinin, işletim sistemi (OS), platform veya uygulama güncellemeleri üzerindeki kontrolüdür. İyileştirilebilecek veya düzeltilebilecek sistem özelliklerinin belirlenmesini, bu iyileştirmenin veya düzeltmenin oluşturulmasını, güncelleme paketinin yayınlanmasını ve bu güncellemelerin kurulumunun doğrulanmasını içerir. BT ekiplerinin hataları ortadan kaldırmasına, üretkenliği artırmasına ve bilinen açıklardan sızmalara hızla yanıt vermesine yardımcı olur. Yazılım güncellemeleri ve sistemin yeniden yapılandırılmasıyla birlikte düzeltme eki uygulama, güvenlik açığı yönetiminin önemli bir parçasıdır.

Siber dünyada büyük etkisi olan ve önemli yama örnekleri:

MS17–010,

OpenSSL 1.0.1g,

Log4j 2.15.0/2.16.0

- **Social Engineering:** Sosyal mühendislik, saldırganın istediği şekilde davranmanızı sağlayan psikolojik bir saldırı türüdür. İnsanların tanımadıkları biri için yapmayacakları şeyleri yapmalarını sağlama sanatıdır. Teknoloji kullanımından çok insanların hile ile kandırılarak bilgi elde edilmesidir.

Farklı sosyal mühendislik tekniklerini gösteren örnekler:

Kevin Mitnick'in Telefon Şirketlerini Kandırması (Rol Yapma — Impersonation),

CEO Dolandırıcılığı (Whaling / Hedefli Oltalama),

RSA SecurID Sızıntısı (Gizli Bilgi Çalma),

USB Bellek Yemleme (Baiting),

Sahte Teknik Destek (Vishing / Ters Sosyal Mühendislik),

- **Penetration Testing / Pentest:** Sızma testi (penetration testing), bir kurumun bilgi sistemlerindeki güvenlik açıklarını tespit etmek ve bu açıklardan faydalanılarak ne ölçüde zarar verilebileceğini ortaya koymak amacıyla gerçekleştirilen kontrollü siber saldırı simülasyonudur. Penetrasyon testi olarak da bilinen bu yöntem, siber güvenlik uzmanlarının gerçek bir siber saldırgan gibi davranarak ve onların tekniklerini taklit ederek sistemlerin dış tehditlere ne kadar dirençli olduğunu değerlendirmesini sağlar.

- **Zero-Day Vulnerability:** Sıfır gün açığı, bir uygulama veya işletim sisteminde keşfedilmemiş bir kusurdur; yazılım üreticisinin varlığından haberdar olmaması nedeniyle savunması veya yaması olmayan bir güvenlik açığıdır; etkili bir yanıt hazırlamak için "sıfır gün" süreleri vardır.

Gerçek hayattan örnekler:

Google Chrome ve iOS Zero-Click Saldırıları (2020-Günümüz),

Log4Shell (Apache Log4j) Zafiyet Zinciri (2021),

SolarWinds Tedarik Zinciri Saldırısı (2020),

- **Breach:** Güvenlik ihlali, bilgisayar verilerine, uygulamalara, ağlara veya cihazlara yetkisiz erişimle sonuçlanan herhangi bir olaydır. Bilgilere yetkisiz erişime neden olur. Genellikle, bir saldırganın güvenlik mekanizmalarını aşabildiği durumlarda ortaya çıkar.

- **Threat:** Siber tehdit avcılığı, bir kuruluşun ağı, uç noktaları ve verileri içinde bilinmeyen veya algılanmamış tehditleri proaktif olarak araması işlemidir.

- **Attack Surface:** *Saldırı yüzeyi,* yetkisiz bir kullanıcının bir sisteme erişip veri alabileceği tüm olası noktaların veya saldırı vektörlerinin sayısıdır**.** Saldırı yüzeyi ne kadar küçükse, korunması o kadar kolaydır.

- **Logging:** Log kaydı yani günlüğe kaydetme, olay veya bilgileri genellikle oldukları gibi kaydetme sürecini ifade eder. Bilgi işlemde log kaydı, bir bilgisayar sisteminde meydana gelen olaylar hakkındaki bilgileri bir günlük dosyasında depolamak anlamına gelir. Bu bilgiler, sistem hataları, kullanıcı eylemleri ve diğer verilerle ilgili ayrıntıları içerebilir.

- **Brute Force Attack:** Kaba kuvvet saldırısı, kapsamlı arama olarak da bilinir, doğru parola bulunana kadar hedeflenen parolanın olası kombinasyonlarını tahmin etmeye dayanan bir kriptografik saldırıdır.

- **Botnet:** Botnet (robot ağı) kötü amaçlı yazılımlarla enfekte olmuş ve bot çobanı olarak bilinen bir siber suçlu tarafından uzaktan kontrol edilen, bot adı verilen, ele geçirilmiş bilgisayar veya cihazlardan oluşan bir ağdır. Bu botlar, DDoS saldırıları, veri hırsızlığı ve spam dağıtımı gibi büyük ölçekli kötü amaçlı faaliyetler yürütmek için birlikte çalışır.

- **APT — Advanced Persistent Threat:** Gelişmiş kalıcı tehdit (APT), bir saldırganın hassas verileri uzun bir süre boyunca çalmak için bir ağda tespit edilemeyen bir varlık oluşturduğu karmaşık ve sürekli bir siber saldırıdır.

Gerçek hayattan örnekler:

Operation Aurora (2009),

SolarWinds Tedarik Zinciri Saldırısı (2020),

Lazarus Group'un Banka Soygunları (APT38),

Stuxnet (2010)

- **CIA — Confidentiality, Integrity, Availability:** CIA üçlüsü (Gizlilik, Bütünlük ve Erişilebilirlik), bilgi güvenliğinde temel bir kavramdır. Rehberimiz, CIA üçlüsünün üç temel unsurunu inceleyerek, hassas verilerin korunması ve bilgi sistemlerinin genel güvenliğinin sağlanmasındaki önemlerini açıklamaktadır.

3- TEHDİT TÜRLERİ

- **Fidye Yazılımı (Ransomware)**

Saldırı Yöntemi: Oltalama (Phishing) e-postaları, RDP zafiyetleri, yamasız sistemlere sızma, zararlı reklamlar (malvertising).

Savunma Prensibi: Düzenli ve İzole Yedekleme (Air-Gapped Backup): Yedekleri ağdan ayrı tutmak. Uç Nokta Algılama ve Yanıt (EDR): Şifreleme başlamadan davranışı tespit edip durdurmak.

- **Solucan (Worm)**

Saldırı Yöntemi: İşletim sistemindeki kritik güvenlik açıklarını (örneğin EternalBlue) kullanarak ağda otomatik ve hızla yayılma.

Savunma Prensibi: Ağ Bölümleme (Network Segmentation): Solucanın yatay hareketini kısıtlamak. Hızlı Yama Yönetimi (Patch Management): Kritik açıkları derhal kapatmak.

- **Truva Atı (Trojan) / Casus Yazılım (Spyware)**

Saldırı Yöntemi: Meşru görünen program indirmeleri, crackli yazılımlar, tuş vuruşu kaydı (keylogging) ile veri çalma.

Savunma Prensibi: Davranışsal Analiz ve AV**/**EDR**:** İmza tabanlı korumadan ziyade, şüpheli davranışları izlemek. Uygulama Kontrolü **(**Application Whitelisting**):** Yalnızca onaylı programların çalışmasına izin vermek.

- **Oltalama (Phishing)**

Saldırı Yöntemi: Sahte giriş sayfalarına (login page) yönlendirme, acil durum veya ödül temalı e-postalar.

Savunma Prensibi: Simülasyon ve Sürekli Eğitim: Çalışanları düzenli Phishing testlerine tabi tutmak. E-posta Ağ Geçidi Koruması: Zararlı ekleri ve linkleri filtrelemek.

- **Hedefli Oltalama (Spear Phishing / Whaling)**

Saldırı Yöntemi: CEO taklidi (BEC), kurbana özel, detaylı bilgilerle güven kazanma.

Savunma Prensibi: İletişim Prosedürleri**:** Büyük para transferi veya hassas bilgi paylaşımını daima ikincil bir kanal (telefonla doğrulama gibi) ile onaylama zorunluluğu.

- **Fiziksel Sosyal Mühendislik**

Saldırı Yöntemi: Rol yapma (Impersonation), Omuz Sörfü (Shoulder Surfing), Yakın Takip (Tailgating) ile izinsiz erişim.

Savunma Prensibi: Fiziksel Erişim Kontrolü: Kart okuyucular, kamera sistemleri. "Challenging" Kültürü: Tanınmayan kişilere kimlik sorma ve refakat etme.

- **Hizmet Reddi (DDoS/DoS)**

Saldırı Yöntemi: Botnet'ler aracılığıyla sunucuya yüksek hacimli trafik gönderme (Volumetrik) veya uygulama katmanında kaynak tüketme.

Savunma Prensibi: DDoS Azaltma Hizmetleri **(**DDoS Mitigation**):** Trafiği filtreden geçiren bulut tabanlı koruma. Hız Sınırlama **(**Rate Limiting**):** Belirli bir kaynaktan gelen istek sayısını kısıtlamak.

- **Ortadaki Adam (Man-in-the-Middle — MITM)**

Saldırı Yöntemi: Güvenli olmayan Wi-Fi ağlarında trafik dinleme, ARP Zehirlenmesi (ARP Spoofing) ile iletişimi kendi üzerine yönlendirme.

Savunma Prensibi: Zorunlu HTTPS**/**TLS**:** Tüm iletişimin şifreli olmasını sağlamak. HSTS **(**HTTP Strict Transport Security**):** Tarayıcıların her zaman şifreli bağlantı kullanmasını zorlamak.

- **DNS Zehirlenmesi (DNS Spoofing)**

Saldırı Yöntemi: DNS sunucusuna sahte kayıtlar enjekte ederek kullanıcıları yanlış (zararlı) IP adreslerine yönlendirme.

Savunma Prensibi: **D**NSSEC (DNS Security Extensions)**:** DNS kayıtlarının orijinalliğini kriptografik olarak doğrulamak.

- **SQL Enjeksiyonu (SQLi)**

Saldırı Yöntemi: Web formu alanlarına kötü amaçlı SQL komutları girerek veritabanı sorgularını manipüle etme.

Savunma Prensibi:Parametreli Sorgular (Prepared Statements): Girdinin veri olarak algılanmasını sağlamak, kod olarak değil.Girdi Doğrulama (Input Validation): Tüm kullanıcı girdilerini filtrelemek.

- **Siteler Arası Komut Dosyası Çalıştırma (XSS)**

Saldırı Yöntemi: Web sitesine zararlı istemci tarafı (client-side) betiği enjekte ederek diğer kullanıcıların tarayıcılarını ele geçirme.

Savunma Prensibi: Çıktı Kodlama **(**Output Encoding**):** Kullanıcı girdisini tarayıcıda çalışabilir kod yerine düz metin olarak göstermek. **İçerik** Güvenlik Politikası **(**CSP**):** Hangi kaynaklardan komut dosyası yüklenebileceğini kısıtlamak.

- **Yanlış Yapılandırma**

Saldırı Yöntemi: Varsayılan yönetici parolalarını kullanma, gereksiz hizmetleri açık bırakma, izinleri yanlış ayarlama.

Savunma Prensibi: Güvenlik Sertleşmesi (Security Hardening): Sistemleri kurduktan sonra gereksiz işlevleri kapatma. Sızma Testleri (Penetration Testing): Yapılandırma hatalarını düzenli olarak test etme.

- **Sıfır Gün Saldırısı (Zero-Day Attack)**

Saldırı Yöntemi: Yama yayınlanmadan önce bilinmeyen veya yeni keşfedilen bir yazılım açığını kullanma.

Savunma Prensibi: Sıfır Güven Mimarisi (Zero Trust): Ağ içinde dikey ve yatay hareketi sürekli doğrulama ile engellemek. Davranışsal Tespit: Açığı değil, açığın sisteme sızdıktan sonraki anormal davranışlarını tespit etmeye odaklanmak.

- **İçeriden Gelen Tehdit (Insider Threat)**

Saldırı Yöntemi: Mevcut veya eski çalışanların erişim yetkilerini kötüye kullanarak veri çalması veya sabotaj yapması.

Savunma Prensibi: Ayrıcalıklı Erişim Yönetimi (PAM): Yönetici hesaplarına erişimi sıkıca denetlemek. Kullanıcı Davranışı Analizi (UEBA): Çalışanların normal davranışlarının dışındaki hareketleri izlemek.

- **Tedarik Zinciri Saldırıları**

Saldırı Yöntemi: Güvenilir bir yazılımın veya hizmetin (örneğin SolarWinds) içine zararlı kod yerleştirme.

Savunma Prensibi: Tedarikçi Risk Yönetimi: Kullanılan tüm üçüncü taraf yazılımların ve hizmetlerin güvenlik süreçlerini denetlemek. Mikro
Bölümleme **(**Microsegmentation**):** Yazılımların ve hizmetlerin sadece ihtiyaç duydukları ağ kaynaklarına erişmesine izin vermek.

4- LİNUX'UN SİBER GÜVENLİKTEKİ ROLÜ VE DAĞITIMLARININ FARKLARI

Linux işletim sistemi, ağ güvenliğini artırır. Siber tehditlere karşı etkili savunma sağlar ve işletmelerin siber güvenlik stratejilerini destekler.

Linux işletim sistemi, ağ güvenliği yönetimi için benzersiz özellikler ve araçlar sunar. Bu özellikler, Linux'un ağ güvenliği yönetiminde tercih edilmesinin başlıca nedenleridir. Linux, gelişmiş güvenlik duvarı yapılandırmaları, karmaşık ağ yönlendirme yetenekleri ve güçlü izolasyon mekanizmaları sunar. Bu özellikler, işletmelerin ağlarını daha güvenli hale getirir ve siber tehditlere karşı etkili bir savunma sağlar.

Linux dağıtımları, bir linux dağıtımı, eksiksiz bir işletim sistemi oluşturmak için bir araya gelen temel ve isteğe bağlı bileşenlerin bir toplamıdır.

-Kali Linux:

Kali Linux (eski adıyla BackTrack Linux) *, kullanıcıların gelişmiş sızma testleri ve güvenlik denetimleri gerçekleştirmelerine olanak tanıyan* açık kaynaklı, Debian tabanlı bir Linux dağıtımıdır.

-Parrot OS:

Parrot Security (ParrotOS, Parrot), güvenlik uzmanları, geliştiriciler ve gizliliğe önem veren kişiler için tasarlanmış *Debian Stable* tabanlı, Özgür ve Açık Kaynaklı bir GNU/Linux dağıtımıdır.

-Black Arch :

BlackArch Linux, sızma testi uzmanları ve güvenlik araştırmacıları için Arch Linux tabanlı bir sızma testi dağıtımıdır.

Linux Dağıtım Farkları

İşletiim Sistemleri

Özellik	Kali Linux	Parrot OS	BlackArch
Temel Altyapı	**Debian** (Sebian'ın standart paket yöneticisi)	Kararlı güncellemeler alır, ancak Kali'ye göre daha güncellemeri	**Arch Linux** (Bağımsız)
Paket Yöneticisi	`apt` (Debian'ın yöneticisi)	`apt`	`pacmon` (Arch'ın paket yöneticisi)
Araç Sayısı	Yaklaşık **600** civarında, özenle seçilmiş ve bakımı yapılmış araç.	Kali'ye benzer sayıda araç, ek olaralı gizlilik günçlanna odaklanmıştır.	**2200'den Fazla araç:** En kapaamlı araç setine sahiptir.
Ana Odak Alanı	**Endiistri Standardı Sızma Testi** ve Dijital Adli Tıp. Profesyonel kullanımda en yaygınıdır.	**Sızma Testi, Anonimlik ve Gizlilik.** Günlük kullanım için de daha uygundur.	Sizma Testi, Hız ve **Ozelleştirme.**
Performans/Hafiflik	Orta seviye. Varsayılan masaüstü GNOME (biraz ağır olabilir), ancak hafif türevleri (Xfce) de vardır.	**Daha Hafif** olmasıyla bilinir. Varsayılan masaüstü MATE/KDE'dir ve kaynaklan daha verimii kullanır.	**Çok Hafif** ve hızlı. Kurulumu minimaldir, kullancıı istediği masaüstü ortamını kurabilir (Arch felsefesi).
Kurulum Zorluğu	**Kolay.** Grafik arayiizü ile basit kurulum.	**Kolay.** Grafik arayiizü ile basit kurulum.	**Zor/Orta.** Kurulumu Arch Linux'a benzer, komut

Yeni başlayanlara önerim Kali Linux veya Parrot OS ile başlamaları, ileri seviye kullanıcılar için ise BlackArch tavsiyemdir.

5- ARAÇ SETLERİ

- **Nmap**: Nmap, ağ tarama ve zafiyet tespiti için kullanılan açık kaynaklı bir araçtır. İsmini Network Mapper'in kısaltmasından almaktadır. Ağ yöneticileri nmap'i sistemlerinde hangi cihazların çalıştığını belirlemek, mevcut ana makineleri ve sundukları hizmetleri keşfetmek, açık bağlantı noktaları bulmak ve güvenlik risklerini taramak için kullanırlar.

Nmap sistem bağlantı noktalarına ham paketler göndererek bilgi toplar. Yanıtları dinler ve bağlantı noktalarının örneğin bir güvenlik duvarı tarafından açık, kapalı veya filtrelenmiş olup olmadığını belirler. Nmap üzerinde bulunan modüller sayesinde port taraması, servis keşfi, versiyon ve işletim sistemi tespiti gerçekleştirebilir.

- **Wireshark**: Wireshark ağ sorunlarını giderme, ağ çözümleme, yazılım veya iletişim protokolü geliştirme ve eğitim amacıyla kullanılmaktadır.

- **Burp Suite**: Burp Suite, bir web uygulaması güvenlik test aracıdır. Burp Suite, bir HTTP/HTTPS istemci-sunucu arasındaki tüm verileri, istek ve yanıt başlıklarını, gövde içeriğini ve diğer parametreleri izleyerek, analiz ederek ve değiştirerek inceleyebilir. Bu araç, güvenlik testi yapılan web uygulamalarında kullanılan pek çok saldırı yöntemini test etmek için kullanılabilir.

- **Metasploit**: Güvenlik açıkları hakkında veri sağlayan ve sızma testlerine yardımcı olan bir bilgisayar güvenliği projesidir . Metasploit'in önemli bir alt projesi, uzak hedef sistemlerde istismar kodu geliştirmek ve çalıştırmak için kullanılan bir araç olan açık kaynaklı Metasploit Çerçevesi'dir.

- **John the Ripper**: John the Ripper, çeşitli şifre kırma yöntemleri ve saldırılar kullanarak parolaları deneme ve çözme yeteneğine sahiptir.

- **Nessus:** Siber güvenlik dünyasında, en popüler zafiyet tarayıcılarından biridir. Nessus, ağdaki cihazları tarayarak olası güvenlik açıklarını tespit etmeye yönelik geliştirilmiş kapsamlı bir yazılımdır.

- **TCPdump**: TCPdump, ağ veri paketlerine erişim sağlayan bir ağ ve protokol analiz aracıdır. Siber güvenlik uzmanlarının araç setinin vazgeçilmez bir parçasıdır. Kullanıcı düzeyinde ağ veri paketlerine erişmek için taşınabilir, sistemden bağımsız bir arayüz sağlayan libpcap arayüzü temelinde oluşturulan TCPdump kılavuzu, ağ trafiği akışını yakalamak ve belirlemek için uyarlanabilir bir çözüm sunar.

- **Snort / Suricata:**

Suricata, saldırı tespit sistemi (IDS) ve saldırı önleme sistemi (IPS) olarak işlev görebilen açık kaynaklı bir tespit motorudur.

SNORT, gerçek zamanlı ağ trafiği analizi ve veri paketi kaydı sağlayan güçlü bir açık kaynaklı saldırı tespit sistemi (IDS) ve saldırı önleme sistemidir (IPS) . SNORT, potansiyel olarak kötü amaçlı etkinlikleri tespit etmek için anomali, protokol ve imza inceleme yöntemlerini birleştiren kural tabanlı bir dil kullanır.

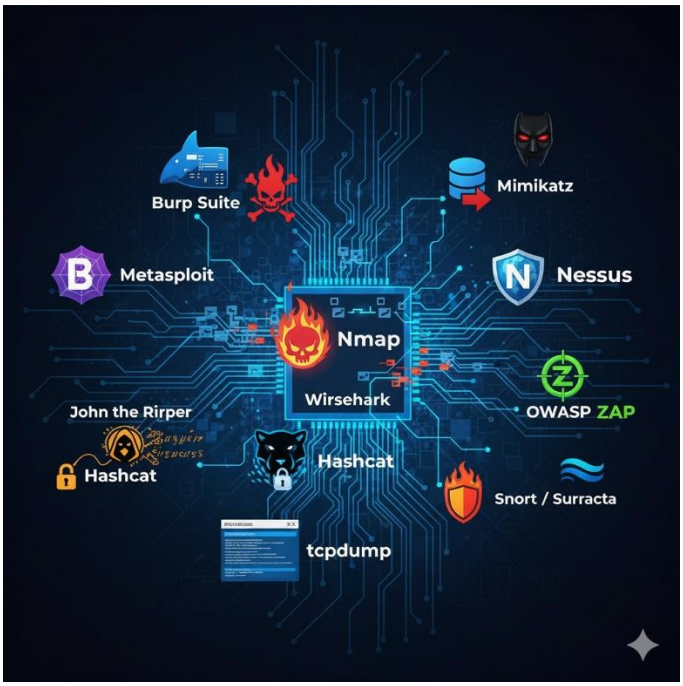
- **SQLmap**: Sqlmap, açık kaynak kodlu sql injection açıkları tespit ve istismar etme aracıdır. Kendisine sağlanan hedef web uygulamasının kullandığı veri tabanı sistemine gönderdiği çeşitli sorgular/komutlar ile sistem üzerindeki sql injection tipini tespit eder. Yine kendisine sağlanan parametrelere göre çeşitli bilgileri hedef veri tabanından alır.

- **Hashcat:** Hashat, kaba kuvvet saldırılarına, aracın tahmin ettiği veya uyguladığı parolaların karma değerleriyle yardımcı olan, özellikle hızlı, etkili ve çok yönlü bir saldırı aracıdır.

- **Mimikatz**: Mimikatz, kullanıcıların kimlik doğrulama bilgilerini görüntülemesine ve kaydetmesine olanak tanıyan açık kaynaklı bir uygulamadır. Araç seti, Windows'un mevcut sürümüyle çalışır ve güvenlik açıklarını değerlendirmeye yardımcı olmak için farklı ağ saldırılarından oluşan bir koleksiyon içerir.

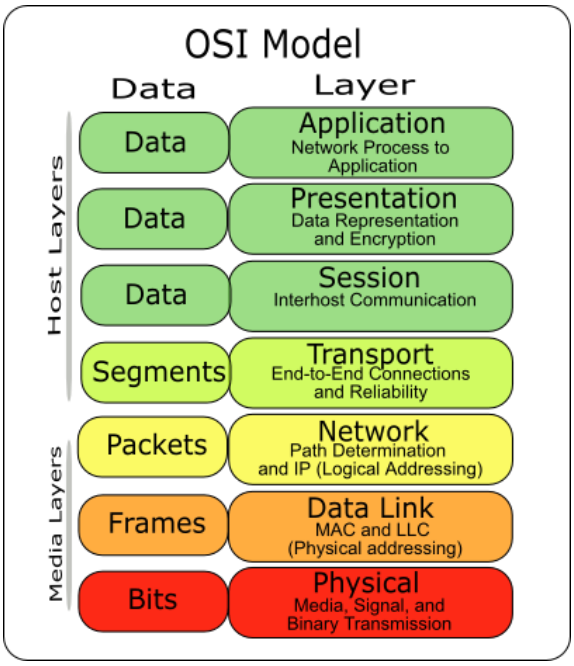
Saldırganlar genellikle kimlik bilgilerini çalmak ve ayrıcalıkları artırmak için Mimikatz'ı kullanır çünkü çoğu durumda uç nokta koruma yazılımları ve antivirüs sistemleri saldırıyı tespit etmez veya silmez. Bunun aksine, sızma testi uzmanları, ağlarınızdaki güvenlik açıklarını tespit edip bunlardan yararlanmak ve bunları gidermek için Mimikatz'ı kullanır.

Press enter or click to view image in full size



6- TEMEL AĞ YAPISI

- **OSI**: Açık Sistemler Ara Bağlantısı (OSI) modeli, ağ iletişimi işlevlerini yedi katmana bölen kavramsal bir çerçevedir. Çeşitli donanım ve yazılım teknolojilerinin coğrafi ve siyasi sınırlar arasında tutarlı bir şekilde çalışması gerektiğinden, ağ üzerinden veri göndermek karmaşıktır. OSI veri modeli, bilgisayar ağı için evrensel bir dil sağlar. Böylece çeşitli teknolojiler, standart protokolleri veya iletişim kurallarını kullanarak iletişim kurabilir.

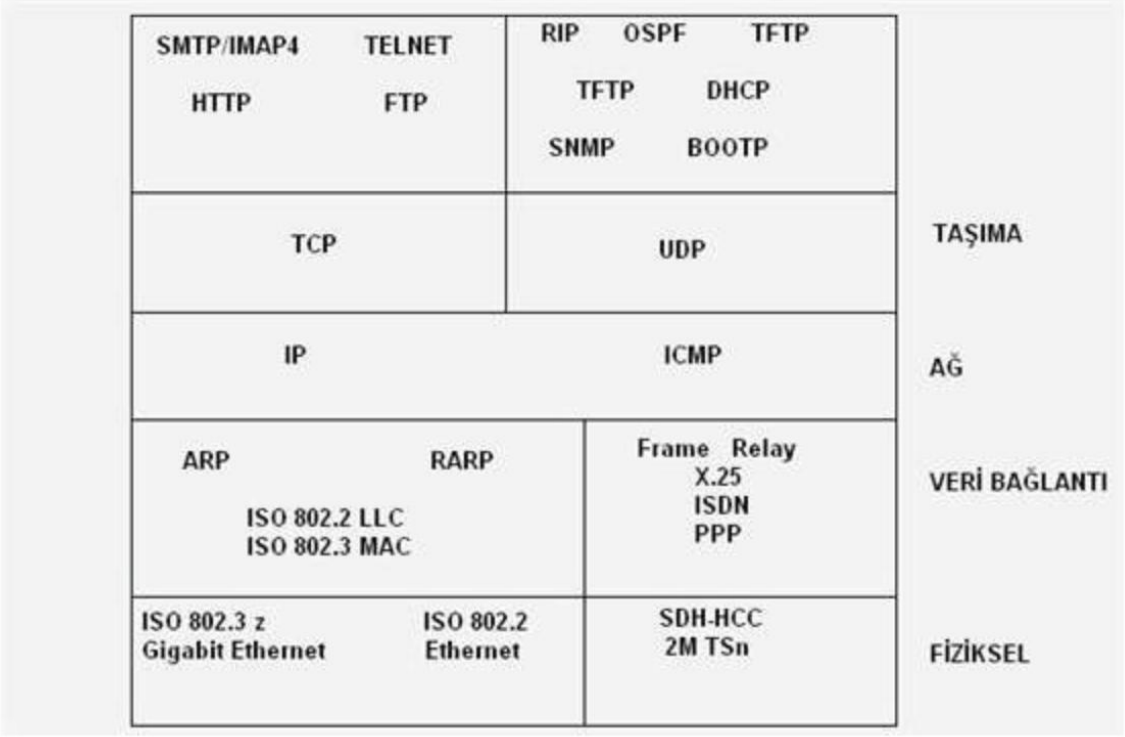


Görsel Linki

- **TCP/IP Modelleri:** İki veya daha fazla bilgisayarın birbiriyle haberleşmesi için belirli protokollere ihtiyaç vardır. TCP/IP, günümüzde en yaygın olarak kullanılan protokol takımıdır ve TCP/IP protokol yığınına (TCP/IP stack) gömülü, İnternette veri aktarımı için kullanılan 2 protokolü temsil eder; Transmission Control Protocol (TCP) ve Internet Protocol (IP).

TCP/IP'de, yollanan veriler katmanlara göre paketlenerek yollanır ve alıcıda bu paketler teker teker açılıp veri ulaştırılır. Her katmanda yollanan verinin türüne göre (e-posta, dosya aktarımı) belirli protokoller görev yapar. OSI referans modelindeki 7 katmana karşılık TCP/IP'de 4 katman mevcuttur; Application **(**Uygulama**),** Transport **(**Taşıma**),** Internet, Network Interface (Ağ Arayüzü).

Genel TCP/IP yapısı:



- **IP Adresleme:** Bir ağa bağlı olan her cihazın benzersiz bir IP adresine sahip olması gerekmektedir. Bu cihazlara IP adreslerinin tanımlanması işlemine IP adresleme denir. IP adreslerinin IPv4 ve IPv6 olmak üzere iki farklı versiyonu bulunmaktadır. İlk versiyon olan IPv4, 4,3 milyar benzersiz IP adresi oluşturulmasına imkân sağlar.

Bir **IPv4 adresi**, genellikle dört sekizlik (octet) olarak bilinen 8 bitlik dört gruptan oluşan, noktalarla ayrılmış 32-bitlik bir sayı dizisidir. Her bir sekizlik, 0 ile 255 arasında bir değere sahip olabilir.

IPv6 adresleri, 128 bit uzunluğunda olup, on altılık (heksadesimal) rakamlardan oluşan, iki nokta üst üste (:) ile ayrılmış sekiz gruptan oluşur.

- **Router:** Yönlendirici, iki veya daha fazla paket anahtarlamalı ağı veya alt ağı bağlayan bir cihazdır. İki temel işlevi yerine getirir: Veri paketlerini amaçlanan IP adreslerine ileterek bu ağlar arasındaki trafiği yönetmek ve birden fazla cihazın aynı internet bağlantısını kullanmasını sağlamak.

Birkaç yönlendirici türü vardır, ancak bunların çoğu LAN'lar (yerel alan ağları) ve WAN'lar (geniş alan ağları) arasında veri iletir. LAN, belirli bir coğrafi alanla sınırlandırılmış bir grup bağlı cihazdır. LAN genellikle tek bir yönlendirici gerektirir.

- **Switch: Ağ güvenlik anahtarı** yani **switch,** bir ağdaki birden fazla cihazı birbirine bağlayan ve bunlar arasında veri ileten bir cihazdır. Bir yerel alan ağı (LAN) oluşturmak için genellikle Ethernet ağlarında kullanılır.Switch, gelen veri paketlerini rastgele tüm cihazlara göndermek yerine, MAC adreslerini (cihazların fiziksel kimliği) kullanarak çalışır.

- **UDP:** User Datagram Protocol (UDP) yani Kullanıcı Datagram Protokolü anlamına gelir. Ana işlevi veri paketlerini bir ağ üzerinden iletmek olan bağlantısız bir internet protokolüdür. Güvenilir bir kullanıcı datagram protokolü bağlantısız bir protokoldür ve veri iletmeden önce bir oturum gerektirmez.

- **DNS:** DNS, tarayıcınıza girdiğiniz etki alanını, bilgisayar tarafından okunabilir bir IP'ye çeviren bir tür telefon rehberidir. Web tarayıcıları, Internet Protokolu (IP) adresleri aracılığıyla etkileşim kurarlar. Açılımı "Domain Name System" olan DNS de alan adlarını IP adreslerine çevirir, böylece tarayıcılar internet kaynaklarına erişebilir.

- **DHCP:** Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP), kuruluşunuzun ağındaki her ana bilgisayara İnternet Protokolü (IP) adreslerini dinamik olarak atamak için kullanılır. Bu DHCP anlamında, bir ana bilgisayar, bir ağa erişim sağlayan herhangi bir cihazı ifade edebilir. Masaüstü bilgisayarlar, dizüstü

bilgisayarlar, ince istemciler ve kişisel cihazlar bunlara örnek olarak verilebilir. DHCP, tüm bu cihazlara bir IP adresi atanmasını sağlar.

- **HTTP:** "Hyper Text Transfer Protocol" olan bu kavram dilimizde "Üstün Metin Transfer Protokolü" olarak biliniyor. İnternet kullanıcıları bunu aktif olarak kullanmasa da otomatik olarak arama çubuğu bu protokolü koyar.

Web sayfalarının görüntülenmesini sağlayan protokoldür. HTTP, kullanıcının bilgisayarı ve sunucu(server) arasındaki veri alışverişinin kurallarını belirler. Bu protokolü kullanmak için tarayıcı kullanılır.

Google Chrome, Mozilla Firefox, Internet Explorer bu web tarayıcılarından bazılarıdır. Bu tarayıcılar yardımı ile herhangi bir internet sitesine girmek için adres çubuğuna sitenin adresini yazdığınız vakit HTTP ile sunucuya bir istek gönderilir ve sunucu bu isteğe cevap verdiği vakit internet sitesinin verileri size gelir. Yani internet sitesine girmiş olursunuz.

- **HTTPS:** "Secure Hyper Text Transfer Protocol" olsa da dilimizde "Güvenli Metin Aktarma Protokolü" olarak biliniyor. Temelde iki protokol de aynı işi yapsa da HTTPS'de güvenlik öne çıkar. HTTP protokolüne SSL sertifikası eklenerek oluşur.

HTTP, herhangi bir siteye bağlanmak istediğiniz zaman isteğinizi alıp, sunucuya iletir ve siteye girişinizi sağlar. HTTPS de aynı işlevi görür. Farkı ise HTTPS protokolü ile bir siteye bağlandığınız zaman güvenlik önlemleri daha ağırdır ve bilgileriniz asla başkaları tarafından okunamaz.

- **ARP:** ARP (Address Resolution Protocol) yani Adres Çözümleme Protokolü, OSI modelindeki ağ katmanının en önemli protokollerinden biridir ve sistemin IP adresine verilen MAC (Media Access Control) adresini bulmaya yardımcı olur.

Bir cihaz aynı ağdaki başka bir cihaza veri göndermek istediğinde, hedef IP adresi için zaten bir eşlemeye sahip olup olmadığını görmek için önce ARP önbelleğini kontrol eder. Eşleme önbellekte yoksa, cihaz, hedef IP adresine karşılık gelen MAC adresini soran ağa bir ARP istek yayını gönderir.

- **SMPT:** SMTP, Basit Posta Aktarım Protokolü anlamına gelir. İnternet üzerinden e-posta mesajları göndermek ve almak için kullanılan bir iletişim protokolüdür. Posta sunucuları ve diğer mesaj aktarım aracıları (MTA'lar); posta mesajları göndermek, almak ve aktarmak için SMTP'yi kullanır.

- **POP3/IMAP:**

IMAP, bulunduğunuz her yerden ve her cihazdan e-postanıza erişmenizi sağlar. IMAP kullanarak e-postanızı okuduğunuzda, aslında e-postayı bilgisayarınıza indirmiş veya depolamış olmazsınız; e-postayı e-posta hizmetinden okuyor olursunuz. Sonuç olarak, e-postanızı dünyanın herhangi bir yerindeki farklı cihazlardan kontrol edebilirsiniz: telefonunuz, bir bilgisayar, bir arkadaşınızın bilgisayarı.

IMAP yalnızca üzerine tıkladığınız iletiyi indirir ve ekler otomatik olarak indirilmez. Bu şekilde, iletilerinizi POP yönteminden çok daha hızlı bir şekilde denetleyebilirsiniz.

POP, e-posta hizmetinizle iletişim kurarak ve tüm yeni iletilerinizi oradan indirerek çalışır. Bunlar PC veya Mac bilgisayarınıza indirildikten sonra e-posta hizmetinden silinir. Bu da, indirildikten sonra e-postaya yalnızca aynı bilgisayar kullanılarak erişilebileceği anlamına gelir. E-postanıza farklı bir cihazdan erişmeye çalışırsanız, daha önce indirilmiş olan iletiler size sağlanmaz.

- **FTP/SFTP:** FTP, veri ve kontrol için şifrelenmemiş iki farklı kanal kullanırken, SFTP aracılığıyla aktarılan veriler küçük paketlere bölünür ve veri ve kontrol için yalnızca bir iletişim kanalı kullanır. Bu iki ağ protokolü arasındaki kanal kullanımındaki fark, güvenlik açısından önemlidir.

- **SSH:** Bir kullanıcının cihazı ile uzaktaki bir makine (genellikle bir sunucu) arasında bağlantı kurar. Bağlantıdan geçen verileri şifrelemek için kullanır.

- **TELNET:** Telnet, yerel ağ içinde uzak bir bilgisayara doğrudan bağlıymışsın gibi oturum açmanızı ve uzak bir bilgisayarı kullanmanızı sağlayan bir protokoldür.

Fiziksel olarak önünde olduğunuz sistem (genellikle bir kişisel bilgisayar) Telnet istemcisidir. Telnet sunucusu, istemcinin bağlı olduğu uzak bilgisayardır. TCP/IP, Telnet istemcisini ve sunucusunu destekler.

En önemli Telnet işlevlerinden biri, Telnet istemcisi ile sunucu arasındaki veri akımlarının iletimini kararlaştırabilme yeteneğidir. Bu tip bir anlaşma, istemcinin ya da sunucunun bir isteği başlatmasını ya da yerine getirmesini sağlar.

- **VLAN:** Sanal Yerel Alan Ağı (VLAN) teknolojisi, fiziksel bir LAN'ı mantıksal olarak birden fazla yayın alanına böler ve her birine VLAN adı verilir.

Her VLAN ayrı bir yayın alanı işlevi görür ve aynı VLAN'daki cihazlar birbirleriyle doğrudan iletişim kurabilirken, farklı VLAN'lardaki cihazlar iletişim kuramaz. Sonuç olarak, yayın paketleri tek bir VLAN içinde sınırlandırılır.

- **SSL/TLS:** Bir istemci ile sunucu arasındaki, özellikle web tarayıcıları ve web siteleri/uygulamaları arasındaki iletişimleri şifreler.

SSL (Güvenli Yuva Katmanı) şifrelemesi ve daha modern ve güvenli alternatifi olan TLS (Aktarım Katmanı Güvenliği) şifrelemesi, internet veya bilgisayar ağı üzerinden gönderilen verileri korur. Bu, saldırganların (ve İnternet Servis Sağlayıcılarının) iki düğüm (genellikle bir kullanıcının web tarayıcısı ve bir web/uygulama sunucusu) arasında paylaşılan verileri görüntülemesini veya değiştirmesini engeller.

Görsel Linki

7- AĞ GÜVENLİK UNSURLARI

- **NAT**: Ağ Adresi Çevirisi (Network Address Translation), özel IP adreslerini genel IP adreslerine çevirerek internete çıkış yapılmasını sağlayan ağ protokolüdür. NAT IP adreslerinin çevrilmesiyle birlikte ağ güvenliğini ve adres tasarrufunu sağlamaktır. IPv4 adreslerinin sınırlı olduğu için ağlar arasında geçiş zorlaşır. NAT bu zorluğu

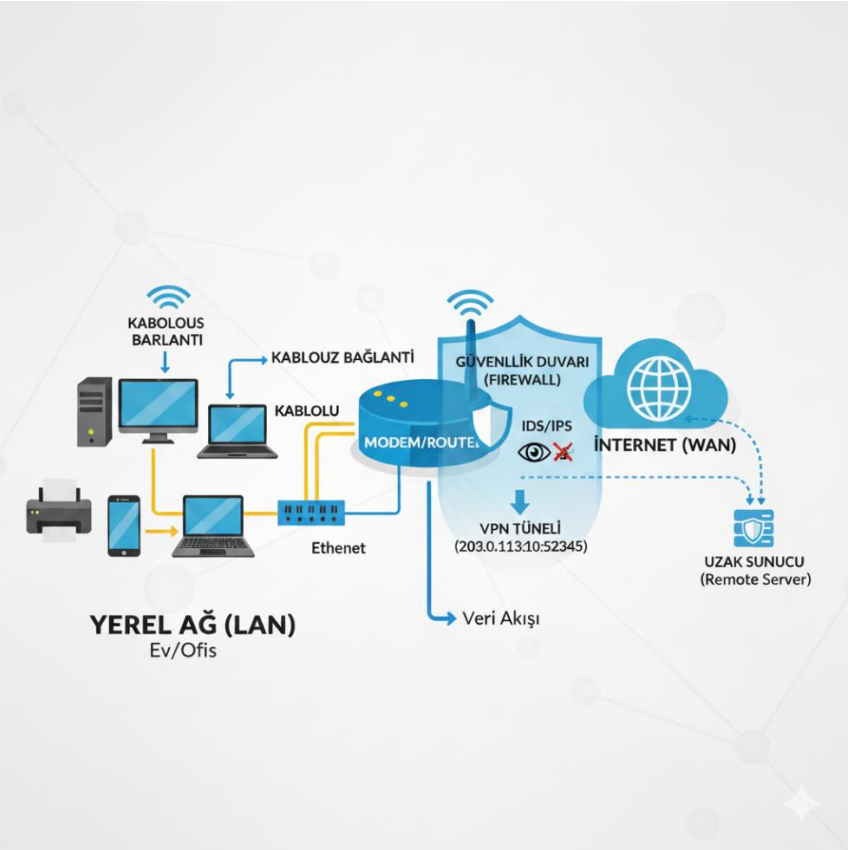
kolaylığa çeviren temel çözümlerden biri haline gelmiştir. NAT, bir yönlendirici (router) ya da güvenlik duvarı (firewall) üzerinde çalışır, iç ağdaki IP adreslerini dış dünyaya karşı gizler.

- **VPN**: Sanal Özel Ağ (virtual private network), uzaktan erişim yoluyla farklı ağlara bağlanmayı sağlayan bir internet teknolojisidir. VPN, sanal bir ağ uzantısı oluşturarak, ağa bağlanan cihazların fiziksel olarak bağlıymış gibi veri alışverişinde bulunmasına olanak tanır
- **FİREWALL**: Güvenlik duvarı (firewall), iç ve dış trafiği denetlememizi sağlayan bir cihazdır. Bu duvar sayesinde bilgisayarımızdaki yazılımlar bizim iznimiz dışında bilgi vermez. Yani bilgisayardan internete doğru bilgi alışverişinin iznimiz dışına çıkmasını engellenmiş olur.

- **IDS/IPS:**

IPS (**I**ntrusion **P**revention **S**ystem), bir çeşit siber saldırı önleme sistemidir. Genel olarak güvenlik duvarının arkasında oluşturulan bu önleme sistemi, tehlikeli ve güvenilir içerikleri analiz edip ayırt etmek üzerine kurulmuş bir katman sayesinde gerçekleştirilir. TCP sisteminde veri alışverişinin katmanlar halinde gerçekleştiğini biliyoruz. Bu katmanlar içinde veriler paketler halinde taşınırlar. Bu sistem üzerinde oluşturulan bir güvenlik katmanı olan IPS, trafik üzerindeki paketleri analiz eder, kaynak ve hedef arasındaki iletişimi sürekli olarak kontrol eder. Anormal durumlar tespit etmesi halinde iletişimi ve veri akışını keser, bağlantıyı sıfırlar ve ağ yöneticisine saldırı hakkında uyarı gönderir.

IDS (**I**ntrusion **D**etection **S**ystem) saldırı tespit sistemi olarak adlandırılan temelde ve bir ağı izleyip güvenlik açıkları ve saldırıları tespit etmek üzere kurgulanmış yazılım veya donanım şeklinde çalışan siber güvenlik sistemidir. IPS sistemi ile kombine bir şekilde veya ayrı olacak şekilde kurgulanabilir. Her iki sistemde güvenlik duvarının arkasında kurgulanmaktadır.



8- SİBER GÜVENLİK TEST SÜREÇLERİ

Test Süreci — Penetrasyon Testinin Beş Aşaması

- **Keşif (4–6 gün)**: Bu aşamada, test uzmanı hedef sistem hakkında ağ topolojisi, işletim sistemleri ve uygulamalar, kullanıcı hesapları ve diğer ilgili bilgiler de dahil olmak üzere mümkün olduğunca fazla bilgi toplar.

Aktif ve pasif keşif vardır. Pasif keşif, halihazırda kamuya açık kaynaklardan bilgi toplarken, aktif keşif, bilgi edinmek için hedef sistemle doğrudan etkileşim kurmayı içerir. Genellikle, hedefin güvenlik açıklarının tam bir resmini oluşturmak için her iki yöntem de gereklidir.

- **Tarama (2–3 gün)**: Bu aşamasında, test uzmanı açık portları belirlemek ve hedef sistemdeki ağ trafiğini kontrol etmek için çeşitli araçlar kullanır. Açık portlar saldırganlar için potansiyel giriş noktaları olduğundan, sızma test uzmanlarının bir sonraki sızma testi aşaması için mümkün olduğunca çok açık port belirlemesi gerekir.

- **Güvenlik Açığı Değerlendirmesi (1–3 gün)**: Bu aşamada , test uzmanının keşif ve tarama aşamalarında toplanan tüm verileri kullanarak potansiyel güvenlik açıklarını tespit edip bunlardan yararlanılıp yararlanılamayacağını belirlediği güvenlik açığı değerlendirmesidir.

- **Sömürü (1–2 gün)**: Bu sızma testi aşamasında, sızma testi uzmanı hedef sisteme erişmeye ve tespit edilen güvenlik açıklarından yararlanmaya çalışır; bu işlem genellikle Metasploit gibi bir araç kullanarak gerçek dünya saldırılarını simüle eder.

Bu, hedef sisteme erişimin güvenlik kısıtlamalarını aşmayı gerektirmesi nedeniyle, belki de en hassas sızma testi aşamasıdır.

- **Raporlama (2–4 gün)**: İstismar aşaması tamamlandıktan sonra, test uzmanı, sızma testinin bulgularını belgeleyen bir rapor hazırlar. Bu son sızma testi aşamasında oluşturulan rapor, sistemde bulunan herhangi bir güvenlik açığını gidermek ve kuruluşun güvenlik duruşunu iyileştirmek için kullanılabilir.

Bir sızma testi raporu oluşturmak, güvenlik açıklarının açıkça belgelenmesini ve kuruluşun güvenlik risklerini giderebilmesi için bağlamına oturtulmasını gerektirir.

9- VERİ GÜVENLİĞİ VE GİZLİLİK KAVRAMI

Veri gizliliği, kişisel veya önemli bilgileri kimlerin görebileceğini yönetmek ve bu bilgilerin doğru şekilde ele alındığından emin olmakla ilgilidir.

Veri güvenliği, bilgilerin bu bilgilere sahip olmaması gereken kişilerden korunması, sızıntıların durdurulması veya zararın önlenmesi anlamına gelir.

10-OLAY MÜDAHALE

Olay müdahalesi (Incident response-IR), bir kuruluşun siber güvenlik tehditlerini ve ihlallerini tespit etmek ve bunlara müdahale etmek için kullandığı süreçleri ve sistemleri ifade eder. Olay müdahale'nin amacı, kuruluş içindeki saldırıları tespit etmek, araştırmak ve kontrol altına almaktır. Olay müdahale faaliyetlerinden edinilen dersler, aynı zamanda, kuruluşun genel güvenlik duruşunu güçlendirerek, alt düzey önleme ve azaltma stratejilerini bilgilendirmek için de kullanılır.

Olay Müdahale Planı altı aşamadan oluşur.

11 -ÖNERİLEN İÇERİKLER

[1] [2] [3] [4] [5] [6]

KAYNAKÇA

[1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [50] [51] [52] [53] [54] [55] [56] [57] [58] [59] [60] [61] [62] [63] [64] [65] [66]