Ağ ve Bilişim Güvenliği

Öğr. Gör. Zafer SERİN

IP(INTERNET PROTOCOL) NEDİR?

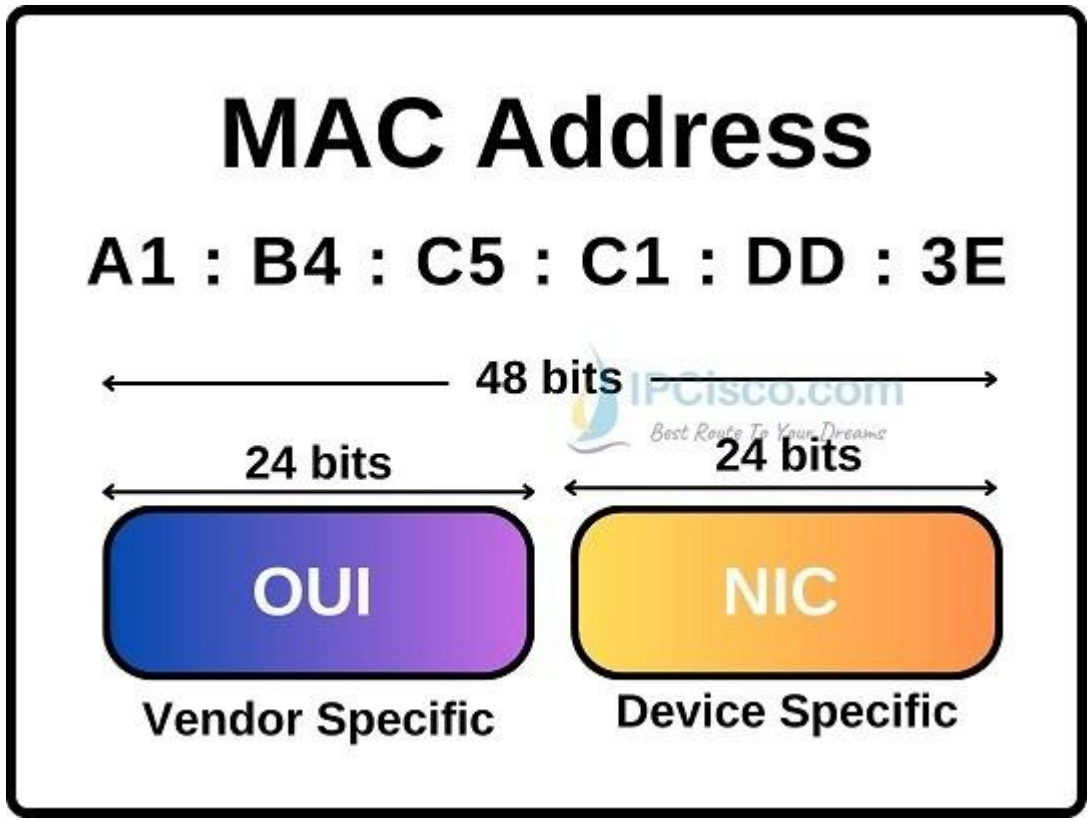
- IP (Internet Protokolü), internet ve diğer ağlar üzerinde cihazlar arasında veri iletişimi sağlamak için kullanılan temel bir protokoldür. IP, verilerin ağ üzerinden nasıl yönlendirileceğini ve teslim edileceğini tanımlayan kuralları belirler. IP, verileri paketlere böler ve bu paketleri hedefe ulaştırmak için gerekli yönlendirme bilgilerini ekler.
- **IP Adresi**: Her cihazın ağ üzerinde benzersiz bir tanımlayıcısıdır. IP adresi, genellikle dört bölümden oluşan bir sayı dizisidir (örneğin, 192.168.1.1).
- **IPv4 ve IPv6**: İki ana IP adresleme sürümü vardır. IPv4, 32 bitlik adresler kullanırken, IPv6, 128 bitlik adresler kullanarak daha fazla adresleme kapasitesi sunar.

IP(INTERNET PROTOCOL) NEDİR?

MAC(MEDIA ACCESS CONTROL) NEDİR?

- MAC (Media Access Control) adresi, ağ arabirim kartlarının (NIC - Network Interface Card) fiziksel olarak benzersiz tanımlayıcısıdır. Her ağ cihazı, üretici tarafından atanan ve cihazın donanımına sabit olarak bağlı olan bir MAC adresine sahiptir. MAC adresi, ağ üzerindeki cihazların birbirleriyle iletişim kurması için kullanılır ve 48 bittir.
- Her MAC adresi, dünya çapında benzersizdir. Bu, aynı ağda veya farklı ağlarda iki cihazın aynı MAC adresine sahip olmamasını sağlar.
- MAC adresi, genellikle 12 karakterlik bir hexadecimal (onaltılık) sayı dizisidir. Örneğin: 00:1A:2B:3C:4D:5E

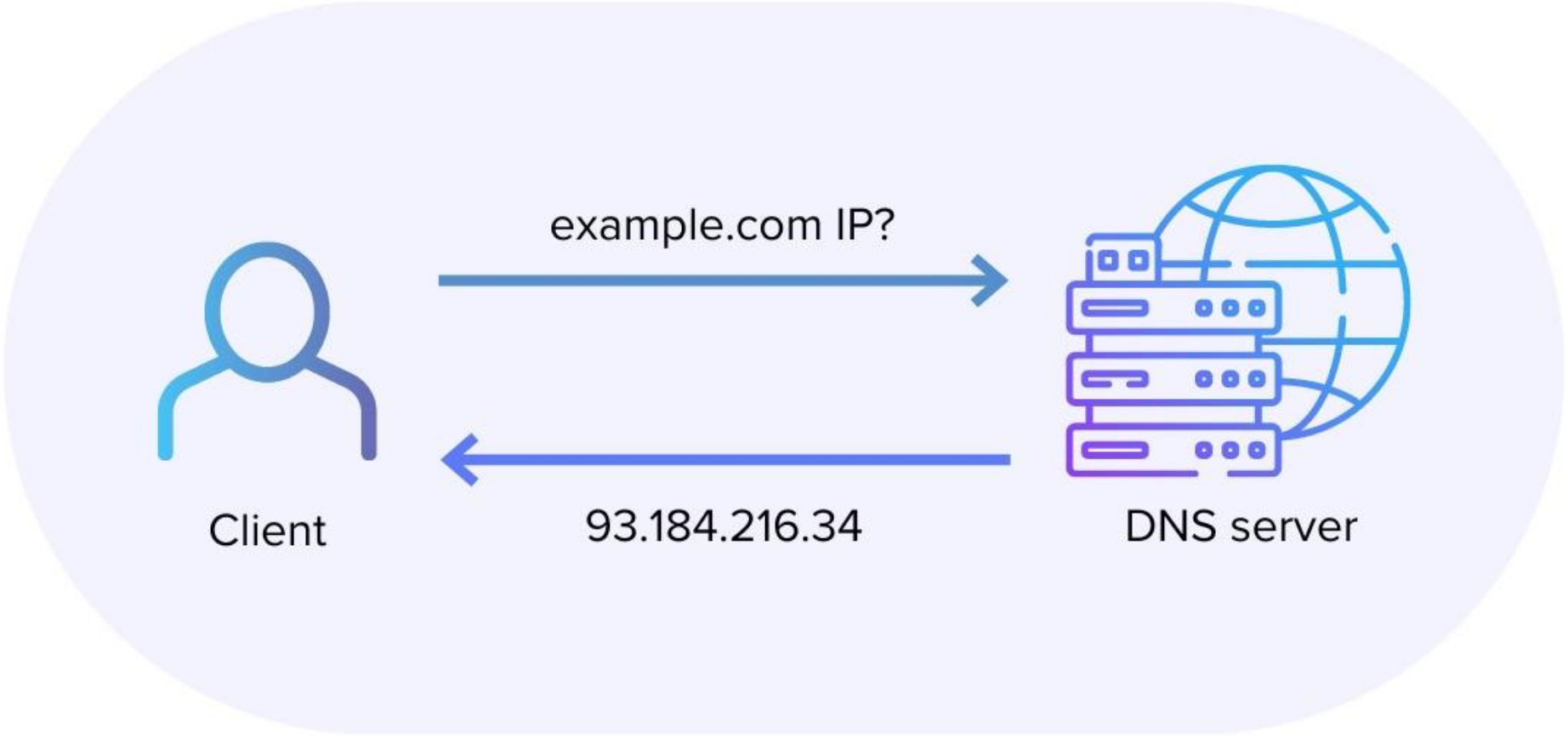
MAC(MEDIA ACCESS CONTROL) NEDİR?



DNS(DOMAIN NAME SYSTEM) NEDİR?

- DNS (Domain Name System), internet üzerindeki alan adlarını (örneğin, www.example.com) IP adreslerine (örneğin, 192.0.2.1) çeviren bir sistemdir. DNS, internetin "telefon rehberi" olarak düşünülebilir ve kullanıcıların alan adlarını hatırlamasını ve bu adlar aracılığıyla web sitelerine erişmesini sağlar.

DNS(DOMAIN NAME SYSTEM) NEDİR?



OSI(OPEN SYSTEM INTERCONNECTION) MODELİ

- OSI (Open Systems Interconnection) modeli, bilgisayar ağlarında farklı cihazların ve sistemlerin birbiriyle iletişim kurmasını sağlayan bir referans modelidir. Bu model, ağ iletişiminin yedi farklı katmana ayrıldığını öne sürer. Her katman, belirli bir işlevi yerine getirir ve diğer katmanlarla iletişim kurar. OSI modelinin katmanları şunlardır: Fiziksel Katman(Physical Layer), Veri Bağlantı Katmanı(Data Link Layere), Ağ Katmanı(Network Layer), Taşıma Katmanı(Transport Layer), Oturum Katmanı(Session Layer), Sunum Katmanı(Presentation Layer), Uygulama Katmanı(Application Layer)

1 - FİZİKSEL KATMAN

- **İşlevi**: Verilerin fiziksel ortam üzerinden iletilmesini sağlar. Bu katman, elektrik sinyalleri, ışık sinyalleri veya radyo dalgaları gibi fiziksel iletişim yöntemlerini kullanır.
- **Kullanım Alanı**: Kablo, fiber optik, antenler ve diğer fiziksel bağlantılar.

2 - VERİ BAĞLANTI KATMANI

- **İşlevi**: Fiziksel katman üzerinden alınan ham verileri çerçeveleme ve hata kontrolü sağlar. Bu katman, veri paketlerinin güvenli bir şekilde iletilmesini ve alınmasını sağlar.
- **Kullanım Alanı**: Ethernet, Wi-Fi, MAC adresleri.

3 - AĞ KATMANI

- **İşlevi**: Veri paketlerinin kaynaktan hedefe en uygun yoldan iletilmesini sağlar. Bu katman, yönlendirme ve adresleme işlevlerini yerine getirir.
- **Kullanım Alanı**: IP adresleri, yönlendiriciler, NAT (Network Address Translation).

4 - TAŞIMA KATMANI

- **İşlevi**: Uçtan uca veri iletimi sağlar ve veri akışının güvenilirliğini kontrol eder. Bu katman, hata kontrolü, akış kontrolü ve segmentasyon işlevlerini yerine getirir.
- **Kullanım Alanı**: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

5 - OTURUM KATMANI

- **İşlevi**: İki cihaz arasında oturum (session) kurulmasını, sürdürülmesini ve sonlandırılmasını sağlar. Bu katman, oturum yönetimi ve senkronizasyon işlevlerini yerine getirir.
- **Kullanım Alanı**: RPC (Remote Procedure Call), NetBIOS.

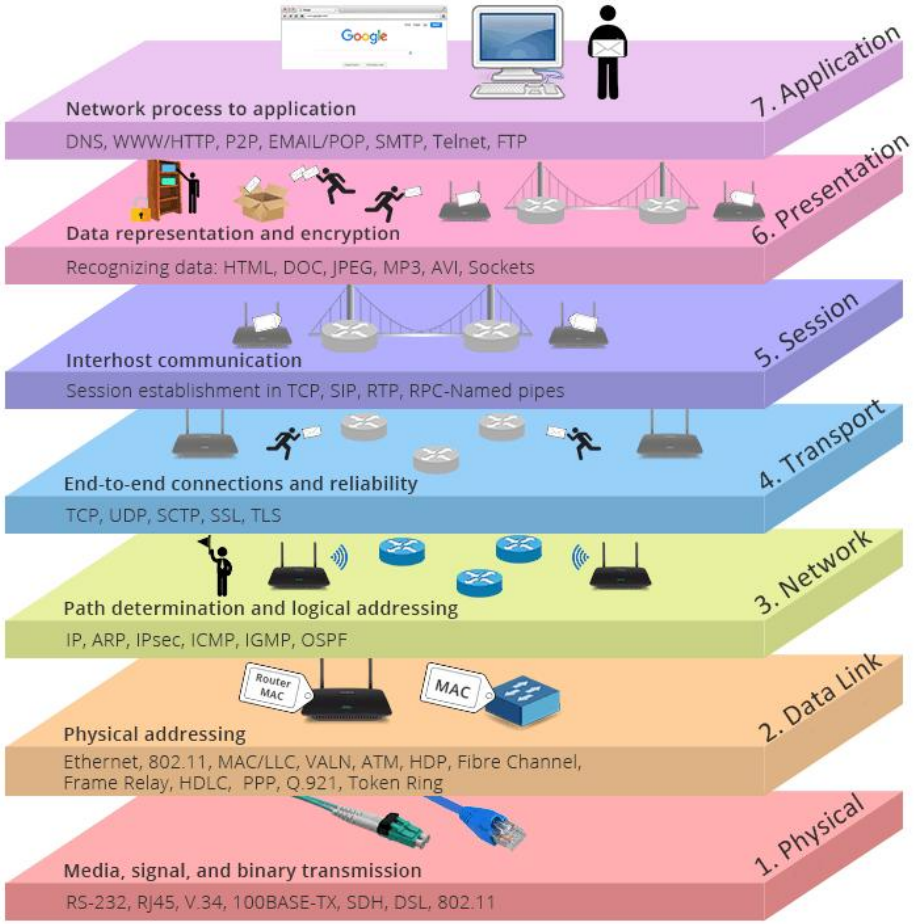
6 - SUNUM KATMANI

- **İşlevi**: Verilerin uygulama katmanından alınıp, ağa uygun bir biçime dönüştürülmesini sağlar. Bu katman, veri şifreleme, sıkıştırma ve karakter kodlaması gibi işlevleri yerine getirir.
- **Kullanım Alanı**: SSL/TLS, JPEG, MPEG.

7 - UYGULAMA KATMANI

- **İşlevi**: Son kullanıcıya doğrudan hizmet veren katmandır. Bu katman, e-posta, dosya aktarımı, web taraması gibi uygulamaların iletişimini sağlar.
- **Kullanım Alanı**: HTTP, FTP, SMTP, DNS.

OSI MODELİ


Google
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
7. Application
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
6. Presentation
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
5. Session
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
4. Transport
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
3. Network
Router MAC
MAC
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring
2. Data Link
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11
1. Physical

TCP ve UDP

- TCP (Transmission Control Protocol) ve UDP (User Datagram Protocol), ağ iletişiminde kullanılan iki temel protokoldür. Her ikisi de Taşıma Katmanı'nda (Transport Layer) çalışır ve veri iletimi için farklı yaklaşımlar sunar.

TCP ve UDP

Özellik	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Güvenilirlik	Yüksek (Hata kontrolü, akış kontrolü, yeniden iletim)	Düşük (Hata kontrolü yok, yeniden iletim yok)
Aktarım Hızı	Daha yavaş (Güvenilirlik için ekstra işlem gerektirir)	Daha hızlı (Ekstra işlem yok)
Paket Sırası	Sıralı iletim (Paketler belirli bir sırayla iletilir)	Sırasız iletim (Paketler rastgele sırada iletilir)
Kaynak Kullanımı	Daha fazla (Güvenilirlik için ekstra kaynak gerektirir)	Daha az (Ekstra kaynak gerektirmez)
Uygulama Örnekleri	HTTP, FTP, SMTP, SSH, Telnet	DNS, SNMP, VoIP, Oyunlar
Üst Düzey Protokoller	HTTP, FTP, SMTP, SSH, Telnet	DNS, SNMP, RTP, DHCP
Kullanım Senaryoları	Güvenilirlik ve doğruluk önemli olduğunda (örn. dosya aktarımı)	Hız ve düşük gecikme süresi önemli olduğunda (örn. gerçek zamanlı uygulamalar)

SİBER GÜVENLİK NEDİR?

- Siber, sadece internet değildir. Çok daha fazlasıdır.
- **Siber güvenlik ise** dijital ortamda bilginin ve verinin güvenliği için yapılan tüm çalışmalardır.
- Ağ yapısına bağlı sistemleri ve bu sistemlerle ilişkili verileri yetkisiz kullanım veya zararlardan korumak için sarf edilen sonsuz bir çabadır.

VERİ NEDİR?

- Veri, bilgisayarların işleyebileceği bir forma dönüştürülmüş gerçekler(sayılar, kelimeler, ölçümler, gözlemler, vb.) topluluğudur.

KİŞİSEL VERİLER NELERDİR?

- Çevrimdışı Kimliğiniz
- Çevrimiçi Kimliğiniz
- Tıbbi Kayıtlar(Hasta Kayıtları)
  - ✓ Fiziksel, zihinsel ve diğer kişisel bilgiler
  - ✓ Reçeteler
- İstihdam ve Finansal Kayıtlar
  - ✓ Gelir ve giderler
  - ✓ Vergi kayıtları – maaş çekleri, kredi kartı ekstreleri, kredi notu ve bankacılık ekstreleri

VERİLER NEREDE SAKLANIR?

- Tıbbi Kayıtlar
  - ✓ Hastane, doktor ofisi, sigorta şirketi
- Tüketim Bilgilerimiz
  - ✓ Mağaza sadakat kartları
- Kişisel Bilgilerimiz
  - ✓ Sosyal medya hesaplarımızda
- Tüketim Bilgilerimiz
  - ✓ Online alışveriş sitelerinde
- Bilgisayarlarımız ve Cep Telefonlarımız

BİLGİ GÜVENLİĞİ NEDİR?

- Bilgi güvenliği, bir organizasyonun veya bireyin hassas bilgilerini, verilerini ve bilgi kaynaklarını, yetkisiz erişim, değiştirme, ifşa veya zarar verme gibi tehditlere karşı koruma sürecidir.
- Bilgi güvenliği, bilgiyi gizli, bütünlüklü ve erişilebilir şekilde koruma amacını taşır. Bu kapsamda bilgi güvenliği, fiziksel güvenlik önlemlerini, teknik önlemleri ve insan kaynaklarına yönelik politikaları içerir.

BİLGİ GÜVENLİĞİNİN TEMEL HEDEFLERİ?

- **Gizlilik:** Hassas bilgilerin yetkisiz kişiler tarafından erişilmesini önlemek.
- **Bütünlük:** Bilgilerin değiştirilmesini veya bozulmasını engellemek.
- **Erişilebilirlik:** Yetkilendirilmiş kullanıcıların bilgilere güvenli bir şekilde erişimini sağlamak.
- **Süreklilik:** Bilgilerin sürekli olarak kullanılabilir ve erişilebilir olmasını sağlamak.
- **İzlenebilirlik:** Bilgiye kimin eriştiğini ve ne zaman eriştiğini izleyebilme yeteneği.

SİBER GÜVENLİK VE BİLGİ GÜVENLİĞİ

- **Bilgi Güvenliği Genel Bir Yaklaşım:** Bilgi güvenliği, organizasyonların genel olarak bilgi varlıklarını korumak için aldıkları önlemleri kapsar
- **Siber Güvenlik Özel Bir Alan:** Siber güvenlik, bilgi sistemlerini ve ağları korumak için alınan spesifik önlemleri ifade eder. Siber güvenlik, bilgi güvenliğinin bir parçasıdır ve bilgi sistemlerinin çevrimiçi tehditlere karşı korunmasına odaklanır.

SİBER GÜVENLİK VE BİLGİ GÜVENLİĞİ

- **Karşılıklı Bağımlılık:** Bilgi güvenliği ve siber güvenlik arasındaki ilişki karşılıklıdır. Siber güvenlik, organizasyonların bilgi güvenliğini sağlama çabalarının önemli bir bileşenidir. Bilgi güvenliği politika ve prosedürleri, siber güvenlik tedbirlerini içerirken, siber güvenlik önlemleri de bilgi güvenliğini destekler.

HACK VE HACKER NEDİR?

- **Hack:** Herhangi bir şeyi kullanım amacı dışında kullanmaktır.
- **Hacker ya da bilgisayar korsanı:** Bilgisini sorunların üstesinden gelmek için kullanan yetenekli bilgisayar uzmanı olarak tanımlanır. Hacker ismi, yetenekli bilgisayar uzmanı anlamına gelse de popüler kültürde teknik bilgisi ile bilgisayar sistemlerine girmek için hata veya istismar yöntemlerini kullanan zararlı kişi olarak kullanılır.

SİYAH ŞAPKALI HACKER(BLACK HAT HACKER)

- Amaçları kötüdür.
- Bilgisayar sistemlerine izinsiz erişmek, bilgileri çalmak veya zarar vermek gibi kötü niyetli eylemleri gerçekleştirirler.
- Saldırganlar, kişisel kazanç veya zarar verme amaçlarıyla hareket edebilirler.

BEYAZ ŞAPKALI HACKER(WHITE HAT HACKER)

- Amaçları iyidir.
- Bilgisayar sistemlerinin güvenliğini test etmek veya zafiyetleri tespit etmek için izin almış güvenlik uzmanlarıdır.
- Sorunları tespit edip düzeltme konusunda organizasyonlara yardımcı olurlar.

GRİ ŞAPKALI HACKER(GRAY HAT HACKER)

- Amaçları karmaşıktır ve genellikle belirsizdir.
- İzin almadan bilgisayar sistemlerini test edebilirler, ancak bu işlemi genelde kötü niyetli amaçlarla yapmazlar.
- Sistem zafiyetlerini tespit edip sahiplerine bildirebilirler, ancak izin almadan test yapma eğilimindedirler.

SOSYAL MÜHENDİSLER(SOCIAL ENGINEERS)

- Teknik bilgisayar becerileri yerine insanları manipüle etmeye odaklanan saldırganlardır.
- Kişisel bilgileri, kimlik bilgilerini veya giriş bilgilerini elde etmek için insanların güvenini kazanmaya çalışırlar.

SCRIPT KIDDIES

- Genellikle teknik bilgiye sahip olmayan veya sınırlı bilgiye sahip olan amatör saldırganlardır.
- Hazır yazılımları veya saldırı araçlarının kullanımına tam hakim olmadan basit saldırılar gerçekleştirirler.
- Genellikle popüler olmayan hedeflere yönelirler.

HACKER GRUPLARI(HACKTIVIST GROUPS)

- Belirli bir sosyal veya politik amaç için siber saldırılar gerçekleştiren gruplardır.
- Örnek olarak Anonymous gibi gruplar, çevrimiçi aktivizm veya sansür karşıtı eylemler için siber saldırılar düzenlerler.

SİBER GÜVENLİK UZMANLARI

- Siber güvenlik uzmanları, bilgisayar sistemlerinin ve ağlarının güvenliğini sağlamak için çalışan kişilerdir. Siber güvenlik uzmanları, siber tehditleri tanımlamak, önlemek ve azaltmak için çalışırlar. Bunların görevleri:
  - ✓ Siber tehditleri ve güvenlik açıklarını belirlemek
  - ✓ Güvenlik politikaları ve prosedürleri geliştirmek
  - ✓ Güvenlik sistemlerini ve uygulamalarını kurmak ve yönetmek
  - ✓ Siber saldırıları araştırmak ve yanıtlamak
  - ✓ Güvenlik eğitimi ve farkındalık sağlamak
- Bunlar kırmızı takım(red team) ve mavi takım(blue team) olarak ikiye ayrılırlar.

KIRMIZI TAKIM(RED TEAM)

- Kırmızı takım üyeleri, saldırganlar gibi düşünerek ve hareket ederek, kurumun güvenlik açıklarını ve zayıflıklarını belirlemeye çalışırlar.
- Kırmızı takım çalışmaları, bir kurumun siber güvenlik duruşunu geliştirmenin ve bir saldırı durumunda ne kadar hazırlıklı olduğunu belirlemenin etkili bir yoludur. Kırmızı takım amaçları:
  - ✓ Saldırganlardır
  - ✓ Kuruluşun savunmasını test ederler
  - ✓ Gerçek dünya siber saldırılarında kullanılan teknikleri kullanırlar
  - ✓ Açıklıkları ve zayıflıkları bulmayı amaçlarlar

MAVİ TAKIM(BLUE TEAM)

- Mavi takım üyeleri, bir kurumun siber güvenlik sistemlerini ve süreçlerini korumaktan sorumlu bir ekiptir. Mavi takım üyeleri, saldırganların saldırılarını tespit etmek, engellemek ve etkisini azaltmak için çalışırlar.
  - ✓ Savunmacılardır
  - ✓ Kuruluşun savunmasını korumaya çalışırlar
  - ✓ Güvenlik politikaları, prosedürleri ve tekniklerini kullanırlar
  - ✓ Saldırıları tespit etmek, engellemek ve yanıt vermeyi amaçlarlar

SİBER GÜVENLİK İÇİN ÖNEMLİ KAVRAMLAR

- Linux
- Python
- Network
- Şifreleme
- Yazılım Geliştirme
- Bulut Bilişim
- Donanım
- Adli Bilişim
- Sosyal Mühendislik

SİBER GÜVENLİK KAVRAMLARI

- **Siber Tehdit(Cyber Threat):** Bilgisayar sistemlerine veya dijital ortama zarar verme veya hassas bilgilere erişme amacıyla gerçekleştirilen herhangi bir potansiyel zararlı aktiviteyi ifade eder.
- **Siber Saldırı(Cyber Attack):** Bilgisayar sistemlerine veya dijital altyapılara yönelik saldırılar, siber tehditin gerçekleştirildiği eylemlerdir.
- **Güvenlik Duvarı(Firewall):** Ağ trafiğini izleyen ve izin verilen trafiği geçiren, izin verilmeyen trafiği engelleyen bir yapıdır. Güvenlik Duvarı yazılımsal veya donanımsal olabilir.

SİBER GÜVENLİK KAVRAMLARI

- **Parola(Password):** Bir kullanıcının bir sisteme veya uygulamaya erişmek için kullandığı bir dizi karakterdir. Parolalar genellikle harflerden, sayılardan ve sembollerden oluşur ve karmaşık ve tahmin edilmesi zor olmaları için tasarlanır.
- **Şifre(Cipher):** Bir parolanın şifrelenmiş halidir. Şifreleme, bir parolayı korumanın bir yoludur, çünkü şifrelenmemiş parolayı bilmeden şifreyi çözmek zordur.

SİBER GÜVENLİK KAVRAMLARI

- **Kodlayıcı(Encoder):** Bir metni başka bir metne dönüştüren bir programdır.
- **Kimlik Doğrulama(Authentication):** Kullanıcıların veya sistemlerin kimliklerini doğrulama sürecidir. Parola, biyometrik veriler veya iki faktörlü kimlik doğrulama bu kavrama örnek olarak verilebilir.
- **Yetkilendirme(Authorization):** Kimlik doğrulama sonrasında kullanıcılara veya sistemlere belirli kaynaklara erişim izni verilmesi sürecidir.

SİBER GÜVENLİK KAVRAMLARI

- **Güvenlik Güncellemeleri(Security Patch):** Yazılım veya işletim sistemlerindeki güvenlik açıklarını kapatmak için yayınlanan düzeltmelerdir. Bu güncellemeler, bilgisayarların güvenliğini artırmak için önemlidir.
- **Sosyal Mühendislik(Social Engineering):** Siber saldırganların insanları manipüle ederek hassas bilgilere veya sistemlere erişmeye çalıştığı bir saldırı taktiğidir. Örnekler arasında sahtekarlık, telefon dolandırıcılığı ve oltalama(phishing) yer alır.

SİBER GÜVENLİK KAVRAMLARI

- **Sosyal Mühendislik Testleri:** İnsanların güvenlik önlemlerini manipüle etmeye çalışan saldırılar veya testlerdir. Bu, sahtekarlık ve insanların duygusal tepkilerini kullanma stratejilerini içerebilir.
- **Veri Sızıntısı(Data Breach):** Hassas veya kişisel bilgilerin izinsiz bir şekilde sızdırılması veya çalınmasıdır. Bu, kullanıcıların gizliliğinin ihlal edilmesine neden olabilir.
- **Ağ Güvenliği(Network Security):** Bilgisayar ağlarını, ağ trafiğini ve verileri koruma amacıyla alınan önlemleri ifade eder.

SİBER GÜVENLİK KAVRAMLARI

- **Güvenlik Politikası(Security Policy):** Bir organizasyonun veya bireyin siber güvenlikle ilgili belirlediği kurallar, prosedürler ve yönergelerdir.
- **Güvenlik Bilinci(Security Awareness):** Kullanıcıların siber güvenlik risklerini ve önlemlerini anlama ve bu konuda eğitimli olma durumunu ifade eder.
- **Ofansif Güvenlik(Hacking):** Sistemlerin veya ağların güvenlik önlemlerini aşmayı amaçlayan siber saldırılar veya testler için kullanılan teknikler ve stratejiler.

SİBER GÜVENLİK KAVRAMLARI

- **Defansif Güvenlik(İyileştirme-Güçlendirme):** Bilgisayar sistemlerini ve ağları koruma amacıyla güvenlik önlemlerini geliştirme ve iyileştirme süreçleri.
- **Sızma Testi(Penetrasyon Testi/Penetration Test):** Bilgisayar sistemlerinin veya ağların güvenlik açıklarını ve zafiyetlerini belirlemek için yapılan kontrollü saldırı ve testler.

SİBER GÜVENLİK KAVRAMLARI

- **İç Ağ Sızma Testi(Internal Test):** Bir organizasyonun iç ağındaki güvenlik açıklarını ve riskleri değerlendirmek için gerçekleştirilen sızma testleri.
- **Dış Ağ Sızma Testi(External Test):** Bir organizasyonun dış ağındaki güvenlik açıklarını ve riskleri değerlendirmek için gerçekleştirilen sızma testleri.
- **Uygulamaya Yönelik Sızma Testleri(+Mobil):** Web uygulamaları veya mobil uygulamalar gibi yazılım uygulamalarının güvenlik açıklarını ve zafiyetlerini tespit etmek için yapılan testler.

SİBER GÜVENLİK KAVRAMLARI

- **Bilgi Toplama Yöntemleri(Pasif/Aktif):** Siber saldırganların veya güvenlik uzmanlarının hedef sistem veya organizasyon hakkında bilgi toplama işlemleri. Pasif bilgi toplama, kamu kaynaklarından veri toplamayı içerirken, aktif bilgi toplama, hedef sistemle doğrudan etkileşim gerektirebilir.
- **Sızma Testi Yöntemleri(Black Box-Gray Box-White Box):** Sızma testi sırasında test edilen sistem veya uygulamanın bilgilendirilme düzeyine göre kullanılan yaklaşımlar

SİBER GÜVENLİK KAVRAMLARI

- **Siyah Kutu(Black Box):** Önceden ilgili sistemle ilgili hiçbir bilgi olmadan yapılan testlere denir.
- **Beyaz Kutu(White Box):** Önceden ilgili sistemle ilgili bilgilerin tamamına sahip olarak yapılan testlere denir.
- **Gri Kutu(Gray Box):** Önceden ilgili sistemle ilgili bilgilerin bir kısmına sahip olarak yapılan testlere denir.
- **Zafiyet Taraması(Vulnerability Assessment):** Bilgisayar sistemlerinde ve ağlarda potansiyel güvenlik zafiyetlerini belirlemek ve sınıflandırmak için kullanılan bir süreç.

SİBER GÜVENLİK KAVRAMLARI

- **Sömürü(Exploit):** Güvenlik açığını veya zafiyetini kullanarak bir sisteme veya uygulamaya sızmayı veya kontrol etmeyi amaçlayan yazılım veya kod parçası.
- **Google Hacking(Google Dork):** Google gibi arama motoru ile hassas veya gizli bilgilere erişmeye çalışan siber saldırılar veya arama sorguları.
- **Siber Terör:** Siber alanlarda yasa dışı veya tehlikeli eylemleri teşvik eden veya gerçekleştiren bir grup veya bireyler tarafından gerçekleştirilen eylemleri tanımlayan bir terimdir. Siber terör, geleneksel terörizmin dijital ortamda gerçekleşen bir uzantısıdır.

SİBER GÜVENLİK KAVRAMLARI

- **Siber Suç:** Bilgisayarlar, ağlar ve dijital teknoloji kullanarak yasa dışı faaliyetlerde bulunma eylemidir. Bu faaliyetler genellikle finansal kazanç, veri çalma veya zarar verme amaçları taşır.