SALDIRI TÜRLERİ VE AĞ GÜVENLİĞİ

Ankara Üniversitesi

Bölüm Tanıtımı

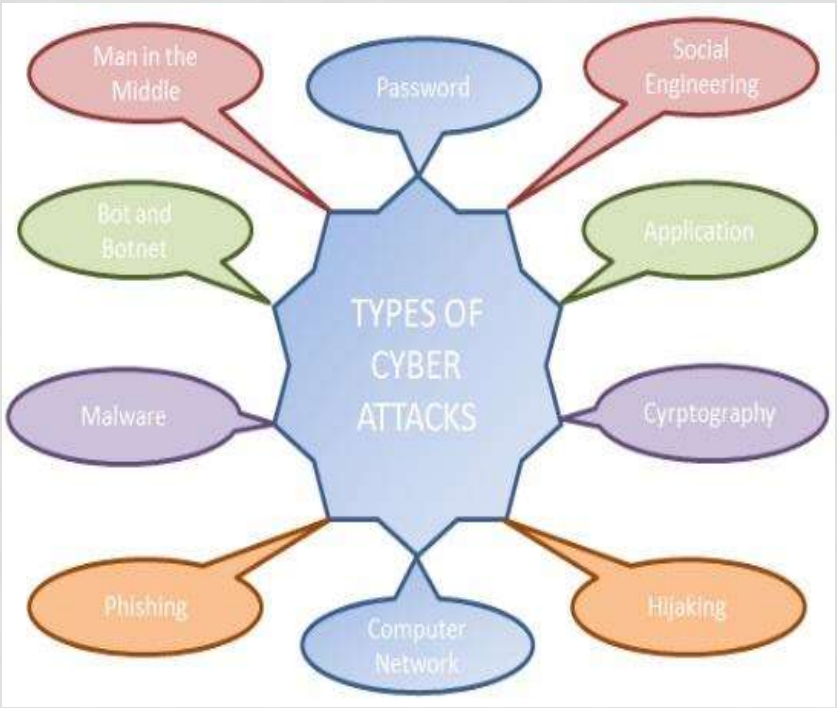
- Bu bölümde
  - saldırılar
  - Ağ güvenliği
  - Ağ katmanları ve bu katmanlara yönelik saldırı türleri

ayrıntılı olarak ele alınmıştır.

- Ayrıca her bir saldırı türü için öneriler, önlemler ve farkındalık konuları da tartışılacaktır.

Saldırı Türleri

- Yaygın saldırı türleri aşağıdaki şekilde verilmiştir:



Saldırı Türleri

- **Sosyal mühendislik:**

Birini bilgileri ifşa etmesi veya veri ağlarına erişmesi için kandırmanın bu yöntemi "sosyal mühendislik" olarak bilinir.

Çoğu siber saldırı gibi sosyal mühendislik de bir kişi veya kuruluşun güvenlik önlemlerini atlatmayı amaçlar.

Olası saldırıları önlemek için kişisel/özel bilgiler paylaşılmamalı, iletişime geçmek isteyenler sorgulanmalı, url/adres kontrolleri yapılmalı, güvenilir olmayan kaynaklardan kaçınılmalıdır.

Saldırı Türleri

- **Uygulama saldırıları:**

Saldırganlar genellikle uygulama katmanına bakarak ve kodda yazılı uygulama güvenlik açıklarını arayarak başlar.

Uygulama güvenlik açıkları, siber suçluların üretimdeki uygulamalardan yararlanma fırsatları yaratır.

Siber suçlular, koddaki güvenlik açıkları, eski sertifikalardan kaynaklanan güvenlik açıkları, kimlik doğrulama eksikliğinden kaynaklanan güvenlik açıkları gibi farklı yöntemlerden yararlanır.

Saldırı Türleri

- **Kriptografik saldırılar:**

Kriptografi, verileri yalnızca amaçlananların okuyup işleyebilmesi için belirli bir biçimde depolama ve iletme yöntemidir.

Kriptografik saldırı, kodda, şifrede, kriptografik protokolde veya anahtar yönetim şemasında bir zayıflık bularak bir kripto sistemini tehlikeye atma yöntemidir.

Saldırılar genellikle saldırgan tarafından gerçekleştirilen eyleme göre sınıflandırılır.

- Pasif bir saldırının temel amacı, bilgiye yetkisiz erişim elde etmektir .
- Aktif bir saldırı ise, bilgi üzerinde bazı işlemler gerçekleştirerek bilgiyi bir şekilde değiştirmeyi içerir.

Saldırı Türleri

- **Ele geçirme (hijacking) saldırıları:**

Ele geçirme saldırıları, saldırganın bilgisayar sistemlerinin, yazılım programlarının ve/veya ağ iletişimlerinin kontrolünü ele geçirdiği bir tür ağ güvenliği saldırısıdır.

Pek çok elel geçirme saldırısı türü vardır ve bunlar aşağıda listelenmiştir:

- tarayıcı kaçırma
- oturum çalma
- etki alanı ele geçirme
- pano ele geçirme
- alan adı sistemi (DNS) ele geçirme
- internet protokolünü (IP) ele geçirme
- sayfa ele geçirme

Saldırı Türleri

- **Bilgisayar Ağı Saldırıları (computer network attacks):**

Bilgisayar/bilgisayar ağının kontrolünü ele geçirmek için bilgisayarlardaki ve bilgisayar ağlarındaki bilgileri manipüle etme, bozma, reddetme, yok etme işlemidir.

CNA'lar ile sistemler kapatılabilir, veriler değiştirilebilir, kaynaklar botnet'ler için kötüye kullanılabilir veya bir sistemin bütünlüğünü veya kullanılabilirliğini tehlikeye atan diğer herhangi bir eylem gerçekleştirilebilir.

Saldırganlar yalnızca ağa erişim elde etmekle kalmaz, aynı zamanda keşif de yapar.

Saldırı Türleri

- **Kimlik Avı Saldırıları (Phishing Attacks):**

Oltalama "bilinen bir kaynaktan geliyormuş gibi görünen bir e-posta göndererek tüketicileri hedefleyen bir tür çevrimiçi dolandırıcılıktır".

Kurbanlardan telefon veya e-posta yoluyla zararlı bir bağlantıya veya eke tıklamalarını isteyerek, gizli bilgileri ifşa edecek şekilde manipüle eder.

Dikkat ve eğitim, kimlik avı saldırılarına yakalanmamanın anahtarıdır. Aynı zamanda, kimlik avı saldırılarından kaçınmak için web sitelerindeki pop-up'lara karşı dikkatli olmak ve URL'nin "https" ile başladığından ve adres çubuğunun yanında kapalı bir kilit simgesi olduğundan emin olmak önemlidir.

Saldırı Türleri

- **Kötü Amaçlı Yazılımlar (Malware Attacks):**

Kötü amaçlı yazılım, bilgisayar sistemlerine zarar vermek, bilgi çalmak veya kullanıcıları rahatsız etmek amacıyla tasarlanmış yazılımların genel adıdır.

Hemen hemen her programlama veya betik dilinde yazılabilir ve birçok farklı dosya türünde taşınabilir.

Kötü amaçlı yazılım, bulaştığı bilgisayar sistemini bilmeden uzun süre bilgi toplama ve casusluk yapabilir. Ayrıca girdiği sisteme zarar vermek veya sabote etmek için kullanılabilir.

Saldırı Türleri

- **Bot'lar ve Botnet'ler:**

Robot'un kısaltması olan "Bot", tekrarlayan, otomatik ve önceden tanımlanmış görevleri gerçekleştiren bir yazılım programıdır.

Müşteri hizmetleri veya arama motorlarını indeksleme gibi yararlı işlevleri yerine getirebilirler veya bir bilgisayar üzerinde tam kontrol elde etmek için kötü amaçlı yazılım biçiminde kullanılabilirler.

Kötü amaçlı yazılım botları, kullanıcı hesaplarına sızmak, iletişim bilgilerini taramak veya diğer kötü niyetli eylemleri gerçekleştirmek için programlanabilir/ele geçirilebilir.

Saldırı Türleri

- **Bot'lar ve Botnet'ler:**

Botnet kelimesi "robot" ve "network" kelimelerinin birleşiminden türetilmiştir.

Botnet, tekrarlayan görevleri ve hedefleri tamamlamak için diğer benzer makinelerle iletişim kuran, İnternet'e bağlı bir dizi bilgisayardır.

Bir botnet, saldırganın kontrolü altındadır ve onbinlerce hatta yüzbinlerce zombi bilgisayardan oluşan bir ağ olarak ifade edilebilir.

Saldırı Türleri

- **Şifre Saldırıları (password attack):**

Şifre saldırıları, siber saldırılarda en sık kullanılan saldırı türlerinden biridir.

Amaç, sosyal medya ağları, kullanılan teknolojiler veya kullanılan yazılımlar gibi parola gerektiren her türlü alanın parolalarını ele geçirerek kuruma veya kişilere zarar vermektir.

Örneğin sosyal medya hesaplarında kişinin tuttuğu takım, nereli olduğu, doğum tarihi, eşinin veya birlikte olduğu kişinin adı, ilişki yılları gibi pek çok bilgi bulunmaktadır. Bu bilgiler siber saldırganlar için çok önemlidir.

Saldırı Türleri

- **Ortadaki Adam Saldırıları (man-in-the-middle attack):**

Ortadaki adam saldırısı, kötü niyetli bir kişinin gizlice iki taraf arasındaki iletişime dahil olduğu en eski siber saldırı türüdür.

Saldırgan bunu, kendi bilgisayarı ile kurbanın bilgisayarı arasında gizli, sözde sahte bir bağlantı oluşturarak başarır.

Genellikle ortadaki adam saldırısının amacı kişisel verileri ele geçirmektir.

Ücretsiz Wi-Fi sağlayan alanlar bu saldırının gerçekleştirilebilmesi için en uygun alanlardır. WiFi alanlarındaki saldırganlar ağ trafiğini kendilerinin üzerinden geçmesi için yönlendirirler. Böylece o ağdaki kişilerin trafiği saldırgan üzerinden akmaya başlar.

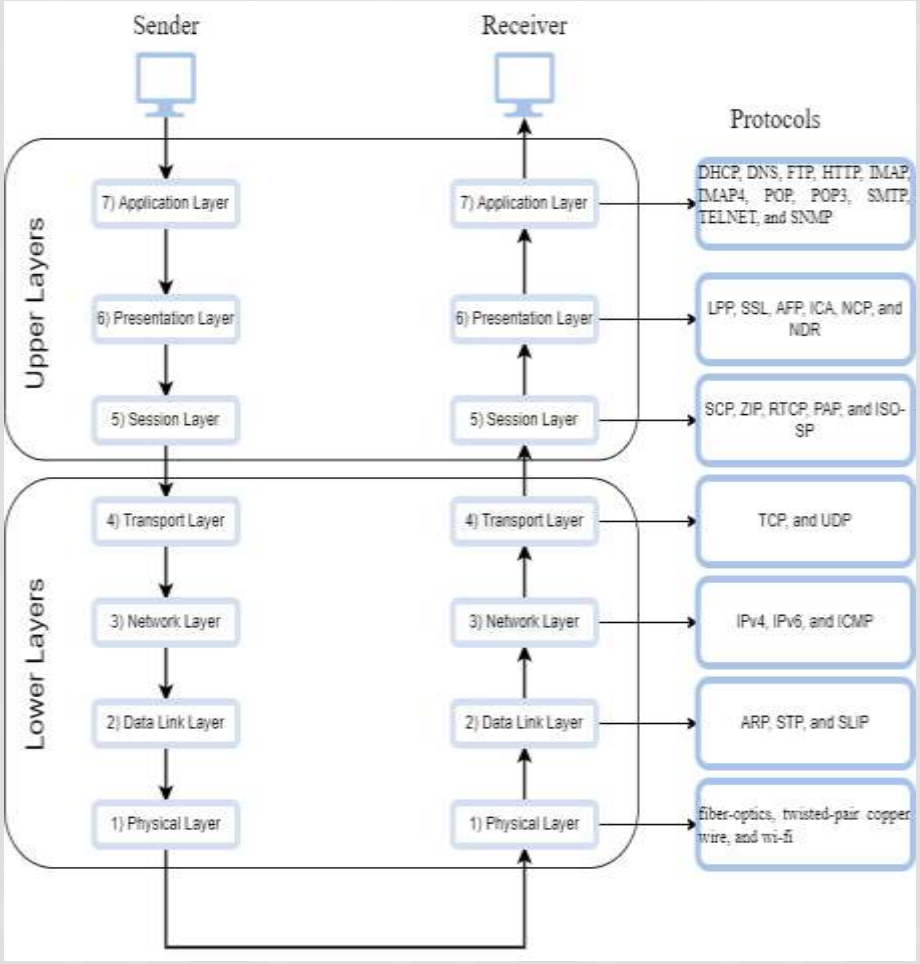
Saldırılara karşı önlemler

Bilgisayar tabanlı sistemleri bu tür tehdit, risk ve saldırılardan korumak veya önlemek için aşağıdaki işlemler yapılabilir:

- bilinmeyen bir kaynaktan program indirmeyin veya açmayın.
- güvenli olmayan e-postaları asla açmayın veya bunların eklerini çalıştırmayın.
- lisanslı işletim sistemleri ve yazılımları kullanma.
- Antivirus ve Antispyware kullanma.
- kişisel bir güvenlik duvarı kullanma.
- mümkün olduğunca şüpheli web sitelerini ziyaret etmekten kaçının.
- sanal makineler kullanmak
- güçlü parolalar kullanmak

Ağ güvenliği

- Temel olarak, OSI modeli iletişim sürecini yedi katmana ayırır. Katmanlar birbirinden bağımsızdır ve her katman görevleri bağımsız olarak yürütür.
- OSI modeli ayrıca iki kategoriye ayrılmıştır: Üst Katmanlar ve Alt Katmanlar.



OSI katmanları

1. Uygulama Katmanı

- Uygulama katmanı protokolleri, son kullanıcıların mesajları birbirlerine nasıl ilettikleri olarak tanımlanabilir. Temel olarak, bir uygulama katmanı, mesaj türlerini ve mesajları gönderme ve yanıtlama sürecine ilişkin kuralları tanımlar. Belirgin bir şekilde, uygulama katmanı, ağ protokollerinin ve ağ uygulamalarının yalnızca bir parçasıdır.
- Önemli uygulama katmanı protokollerinden bazıları:
  - Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP),
  - Alan Adı Sistemi (DNS),
  - Dosya Aktarım Protokolü (FTP),
  - Köprü Metni Aktarım Protokolü (HTTP),
  - İnternet Mesaj Erişim Protokolü (4) (IMAP ve IMAP4),
  - Postane Protokolü (POP ve POP3),
  - Basit Posta Aktarım Protokolü (SMTP),
  - TELetype NETwork (TELNET)
  - Basit Ağ Yönetimi Protokolü (SNMP).

OSI katmanları

1. Uygulama Katmanı Saldırıları

- DoS, DDoS, SMTP saldırısı, FTP sıçrama, güvensiz HTTP, Tarayıcı ele geçirme, Arabellek Taşması, Kötü Amaçlı Yazılım Saldırısı, Veri Saldırısı vb. dahil olmak üzere çok çeşitli uygulama katmanı saldırıları vardır.
- Son zamanlarda, uygulama katmanı DoS saldırıları çok popüler hale gelmiştir. En büyük uygulama katmanı DoS saldırıları 2019'da rapor edimiştir ve her üç ayda bir ikiye katlanmaya devam etmektedir.
- SMTP saldırısı, saldırganın müşterinin postasına yetkisiz erişim elde ettiği ve posta adreslerini gözlemlediği ve kötüye kullandığı bir tekniktir.
- FTP sıçrama saldırısı, saldırganın kurban makineyi kullanarak bağlantı noktalarına erişebilmesi açısından SMTP saldırısına benzer.
- Tarayıcı ele geçirme, saldırgan tarafından yetkisiz web tarayıcısı ayarlarını değiştirmek için kullanılan bir kötü amaçlı yazılım programıdır.
- Arabellek Taşması saldırısı, dosyalara zarar vermek ve özel bilgileri açığa çıkarmak için bir uygulamanın belleğinin üzerine yazmayı amaçlayan bir tekniktir.
- Güvenli olmayan HTTP, HTTP verilerinin şifrelenmediği anlamına gelir ve bu da onu saldırılara karşı savunmasız hale getirir.
- Saldırganlar, kurbana saldırmak için kötü amaçlı yazılım kullanır. En yaygın kötü amaçlı yazılım saldırıları, reklam yazılımları, virüsler, solucanlar, Truva atları, botlar ve fidye yazılımlarıdır.

OSI katmanları

2. Sunum Katmanı

- OSI modelinin altıncı katmanına Sunum Katmanı denir.
- Bu katman, son kullanıcılar arasında değiş tokuş edilen mesajlardaki alanlarla ve mesajların anlamlarıyla ilgilenir.
- Uygulama ile taşıma katmanı arasında bir köprüdür ve veri çevirisi, şifreleme-şifre çözme ve sıkıştırmadan sorumludur.
- Ayrıca uygulama katmanından gelen düz metin mesajını şifreler ve taşıma katmanından gelen şifreli verinin şifresini çözer.
- Kayba dayanıklı verilerdeki bit sayısını azaltmak için veri sıkıştırması gerçekleştirir.

OSI katmanları

2. Sunum Katmanı

- Sunum katmanı protokolleri:
  - Hafif Sunum Protokolü (LPP-Lightweight Presentation Protocol),
  - Güvenli Yuva Katmanı (SSL-Secure Socket Layer) protokolü
  - Apple Dosyalama Protokolü (AFP-Apple Filing Protocol)
  - Bağımsız Bilgi İşlem Mimarisi (ICA-Independent Computing Architecture)
  - NetWare Çekirdek Protokolü (NCP-NetWare Core Protocol)
  - Ağ Veri Temsili (NDR-Network Data Representation)
- Sunum Katmanı Saldırıları, bankacılık, çevrimiçi alışveriş vb. dahil olmak üzere web hizmetlerinin güvenliği için kullanılır.
- Sunum katmanı saldırıları, hatalı biçimlendirilmiş Güvenli Yuva Katmanı (SSL), SSL soyma ve Şifre Belirtimi Değiştir (CCS) manipülasyon saldırılarını içerir.

OSI katmanları

3. Oturum Katmanı

- Bu katman, Sunum Katmanı ile Aktarım Katmanı arasındaki verileri yönetir.
- Temel olarak, iki son kullanıcı uygulaması arasında iletişimi sağlamak, sistemlerin yarım veya tam çift yönlü iletişim modunda iletişim kurmasını sağlamak, yönetmek, kontrol noktaları ekleme sürecine izin vermek, iletişim oturumlarını yönetmek ve bilgileri senkronize etmekten sorumludur.

OSI katmanları

3. Oturum Katmanı

- Bu katmanda yaygın kullanılan RPC protokolü dışında diğer popüler oturum katmanı uygulamaları:
  - Oturum Kontrol Protokolü (SCP-Session Control Protocol)
  - Bölge Bilgi Protokolü (ZIP-Zone Information Protocol)
  - Gerçek Zamanlı Aktarım Kontrol Protokolü (RTCP-Real-time Transport Control Protocol)
  - Parola Doğrulama Protokolü (PAP-Password Authentication Protocol)
  - OSI oturum katmanı Protokolü (ISO-SP-OSI session layer Protocol)

OSI katmanları

3. Oturum Katmanı

- İki ana oturum katmanı saldırısı vardır: oturum ele geçirme ve oturum kimliğini çalma.
- Aynı saldırıları farklı şekillerde yapan hijacking saldırılarını aktif, pasif ve hybrid session hijacking olmak üzere üç gruba ayırıyoruz.
- Wireshark, T-SightS, Hunt ve Hamster and ferret gibi oturum ele geçirme işlemleri için kullanılan popüler araçlar vardır.
- Oturum kimliği çalma amaçları için üç popüler yol vardır. Koklama, Brute force ve komut dosyası oluşturma.

OSI katmanları

4. Taşıma Katmanı

- Son kullanıcılar arasında eksiksiz mesajların iletilmesinden ve bir hata oluşması durumunda verilerin onaylanmasından sorumludur.
- Gönderici tarafında, taşıma katmanı üst katmandan biçimlendirilmiş verileri alır ve segmentasyon yapar, gerekli akış/hata kontrollerini uygular, kaynak-hedef bağlantı noktası numaralarını veri başlığına ekler ve segmentlere ayrılmış verileri Ağ Katmanına iletir.
- Alıcı tarafında taşıma katmanı, parçalanmış veriyi birleştirir, port numarasına bakar ve veriyi ilgili uygulamalara iletir.

OSI katmanları

4. Taşıma Katmanı

- İletim Kontrol Protokolü (TCP) ve Kullanıcı Datagram Protokolü (UDP) bu katmandadır ve OSI modeli için çok önemli protokollerdir. UDP bağlantısız bir protokol iken, TCP hız yerine veri kalitesini ön planda tutan protokoldür.
- Özellikle, bu katmanda yaygın olarak görülen üç tür güvenlik tehdidi vardır: **TCP taşma saldırısı, UDP taşma saldırısı ve TCP sıra Tahmini saldırısı**. TCP flooding saldırısı, internetteki en yaygın saldırıdır. Gönderici ve alıcı bilgisayarlar arasında bir TCP bağlantısı kurulduğunda, gönderici, alıcının dinlemediğinden emin olduktan sonra alıcı bilgisayara TCP Reset (TCP RST) paketini gönderir.
- UDP flood saldırısı aynı zamanda kurban bilgisayarın performansını zayıflatmayı hedefleyen bir DDoS saldırısıdır.
- TCP sıra tahmini saldırısı, bir TCP bağlantısındaki paketleri tanımlamak için kullanılan sıra numarasını tahmin ederek kurban bilgisayara sahte paketler göndermenin bir yoludur.

OSI katmanları

5. Ağ Katmanı

- Ağ Katmanı, OSI modelindeki en karmaşık katmanlardan biridir. Bu katmanda kontrol ve veri düzlemleri olmak üzere iki düzlem vardır. Veri düzleminde, yönlendiriciye bir paket geldiğinde, uygun çıkış bağlantısına taşınması gerekir. Sunucular arası yönlendirme dahil olmak üzere kaynaktan hedefe paketin iletilmesinden sorumludur.
- Ağ Katmanındaki iyi bilinen protokoller, İnternet Protokolü sürüm 4 ve 6'yı (IPv4 ve IPv6) ve İnternet Kontrol Mesajı Protokolünü (ICMP) içerir.

OSI katmanları

5. Ağ Katmanı

- Yaygın ağ katmanı saldırıları, Smurf saldırıları, IP sızdırma saldırıları ve Hijacking Saldırılarıdır.
- Smurf saldırı, bir Dağıtılmış Hizmet Reddi (DDoS) saldırısı türüdür.
- IP sızdırma saldırısı, saldırganın sunucuya paket göndermek için güvenilir bir IP adresi kullandığı ve sunucunun saldırganın IP adresini belirleyemediği bir tekniktir.
- Ele geçirme saldırısı, bir sunucu-istemci oturumunu bozma ve ardından saldırgan ile sunucu arasında yeni bir oturum oluşturma yöntemidir.

OSI katmanları

6. Veri Bağlantı Katmanı

- Data Link katmanı, OSI modelinin ikinci katmanıdır. Protokoller bu katmandaki düğümler tarafından yürütülür.
- Bu katmanda pek çok protokol vardır, ancak yaygın olanları aşağıda verilmiştir:
  - Adres Çözümleme Protokolü (ARP-Address Resolution Protoco)
  - Yayılan Ağaç Protokolü (STP-Spanning Tree Protocol)
  - Seri Hat İnternet Protokolü (SLIP-Serial Line Internet Protocol)
- Veri Bağlantısı Katmanındaki yaygın saldırılardan bazıları MAC saldırıları, STP saldırıları ve ARP zehirlenmesi saldırılarıdır.

OSI katmanları

6. Veri Bağlantı Katmanı

- MAC Saldırıları, bir anahtarı, paketleri tüm bağlantı noktalarına iletmek için bir merkez gibi çalışmaya zorlar. Bu, anahtar tablosuna neden olur.
- STP saldırıları, Genişleyen Ağaç topolojisini değiştirmek için sahte BPDU mesajları kullanır. Sık topoloji değişiklikleri DoS saldırılarına neden olabilir.
- Ağ katmanında çalışmasına rağmen ARP zehirlenmesi Veri Bağlantısı Katmanında gerçekleştirilir. Yerel Alan Ağı üzerindeki cihazlar, girişlerin IP adresini ve ilgili MAC adresini bir önbellekte tutar. Bir saldırgan, sahte MAC ve IP adreslerinin kombinasyonunu duyurmak için internet üzerinden karşılıksız bir ARP paketi gönderdiğinde, cihazlar önbelleklerini günceller. Bu nedenle saldırgan, ağ geçidinin trafiğini anahtarı üzerinden akmaya zorlayarak trafiği izlemek için bu işlemi kullanabilir.

OSI katmanları

7. Fiziksel Katman

- OSI modelinin son katmanı Fiziksel Katmandır. Fiziksel katman çerçeve içindeki tüm çerçeveler yerine tek tek bitleri düğümler arasında taşımaktan sorumludur.
- Bu katmandaki protokoller, fiber optik, çift bükümlü bakır tel, wi-fi vb. bağlantıların malzemesine ve ortamına bağlıdır.
- Bazı yaygın Fiziksel Katman saldırıları, Telefon Dinleme, Karıştırma ve Kurcalamadır.

OSI katmanları

7. Fiziksel Katman

- Karıştırma saldırısı, bir karıştırma düğümünün ağ performansını düşürmek için iletilen paketlere müdahale ettiği bir saldırı türüdür.
- Telefon dinleme saldırısı, bir saldırganın üçüncü taraf bir kabloyu bağlantı kablolarına bağlaması anlamına gelir ve bu, saldırgana aktif ve pasif modda veri akışını gözlemleme ve analiz etme yeteneği verir.
- Kurcalama saldırısı, bir saldırganın bir sistemi veya bileşenlerini ve ağdaki verileri değiştirdiği yetkisiz bir eylemdir.

Kablosuz Ağ Saldırıları

- Kötü amaçlı ilişkilendirme, yaygın kablosuz ağ saldırılarından biridir. Bir saldırgan, bir şirketin erişim noktasını hedef alır ve kırılmış dizüstü bilgisayarının kablosuz ağ kartını meşru bir erişim noktası gibi gösterir. Bir kullanıcı bu erişim noktasına bağlandığında, saldırgan kullanıcının parolalarını çalabilir.
- Geçici ağlar, istemcilerin bir erişim noktası kullanmadan kablosuz olarak birbirine bağlandığı Eşler Arası (P2P) ağlardır. Bu tür bir ağ, önemli sayıda tehdide neden olabilecek yeterli korumaya sahip değildir. Bluetooth cihazları gibi geleneksel olmayan ağlar, zayıf güvenlik korumaları nedeniyle güvenlik risklerine neden olabilir.

Kablosuz Ağ Güvenliği Sağlama

- Şifreleme, kablosuz ağları korumanın en etkili yollarından biridir.
- Antivirüs, güvenlik duvarı ve casus yazılım önleme yazılımları kullanmak ve bunları sık sık güncellemek, kablosuz ağ koruması için önemlidir.
- Her bilgisayarın, ağa bağlandığında kullandığı kendi Medya Erişim Kontrolü (MAC) adresi vardır. Kablosuz yönlendiriciler, belirli MAC adreslerinin ağa erişmesine izin verecek şekilde ayarlanabilir.
- Kullanıcıları ağ güvenliğinin önemi konusunda eğitmek ve koruma yöntemlerinin kullanımını rutin hale getirmek.
- Anahtarların güvenliğini sağlamak, ağ güvenliği adına çok önemli bir tekniktir.
- Yönlendiriciler: Yönlendiricilerin güvenliğini sağlamak, kullanıcıları tehditlere karşı korumak için de önemli bir tekniktir.