Siber Saldırı (Atak) Çeşitleri

Tehdit, Saldır veya Siber Atak Ne demektir ?

- **Tehdit**, belirli durum, yetenek, veya olay olduğu anlarda güvenlik foksiyonunun yerine getirilmesini engelleyen potansiyel bir güvenlik bozucusu; **saldırı**, sistemin güvenlik servislerini etkisiz hale getirmeyi amaçlayan akıllı bir tehditten üretilen ani bir hücumdur.

- Başka bir tanımlama ise; bilgi sistemleri üzerinden; zarar vermek, sistemlerin işleyişini engellemek ya da bilgi çalmak için yapılan çalışmalara siber atak denilmektedir.

- Engelleme (DoS) ,Dinleme (Sniffing), Değiştirme/Aldatma (spoofing) ve yeniden oluşturma (Virus vs.) şeklinde 4 tip ana saldırı şekli vardır.

Atak Çeşitleri

- İçsel atak (Internal)
- Dışsal Atak (External)
- Pasif ataklar (Passive)
- Aktif ataklar (Aktive)
- Dağıtık atak (Distributed)
- Phishing atak (Phishing)
- Yakın atak (Close-in)
- Keşif Atakları
- Password atakları
- Kod atakları
- Sosyal Mühendislik ve Sosyal Ağ atakları

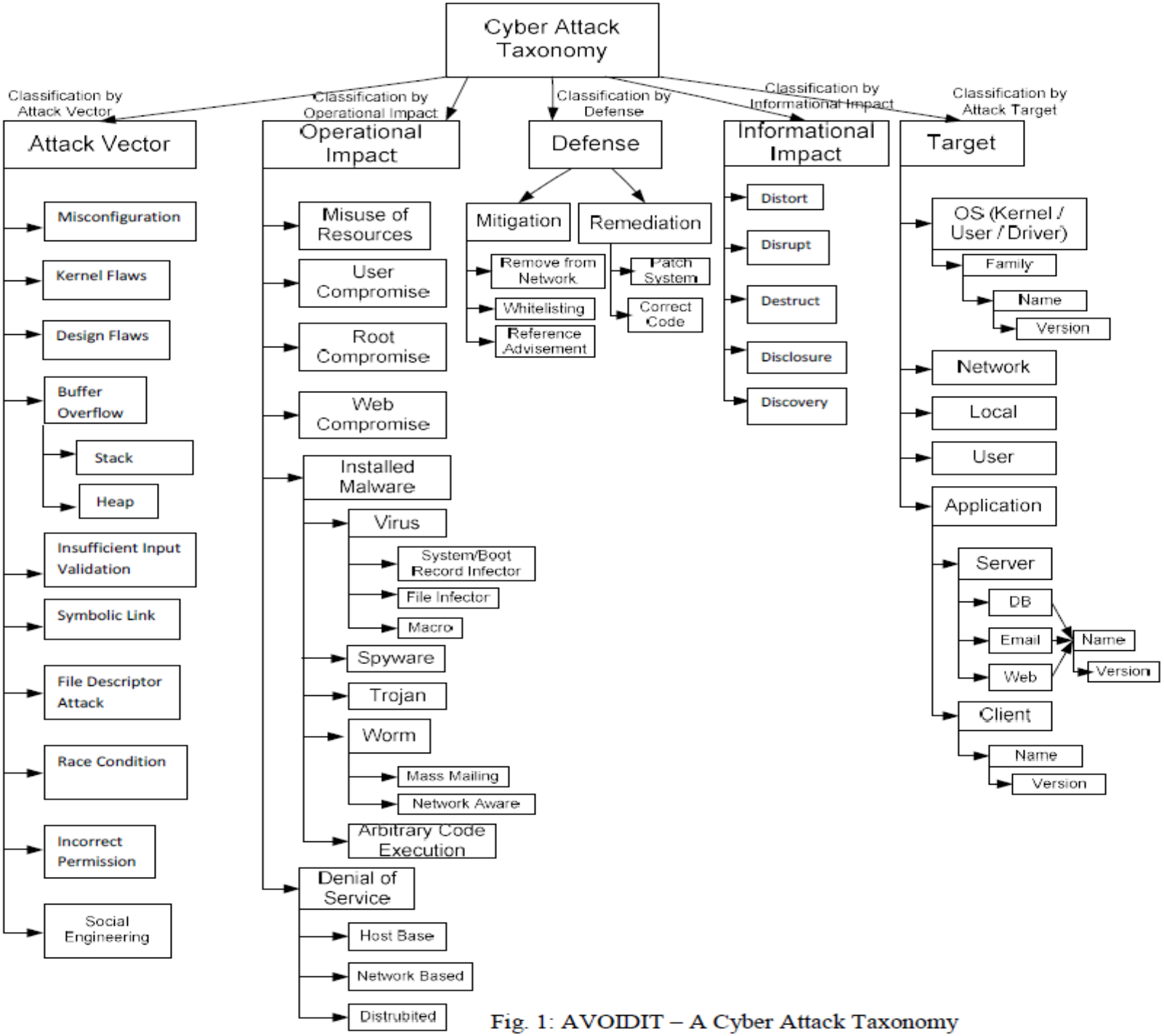


Fig. 1: AVOIDIT – A Cyber Attack Taxonomy

Atak Çeşitleri

Dışsal Atak (External Atak) :

- External saldırılar genellikle internet üzerinden veya LAN dışından yapılırlar.
- Bu tür saldırıların en önemli özelliği saldırgan hakkında çok fazla bir şey bilmiyor olmamızdır.
- Bu tür saldırılarda genellikle bir araç (malware) kullanılır.
- Bunun dışında saldırganları profesyonel ve amatör olarak da ayırmak mümkündür.
- Amatör saldırganların kullandığı yöntemlerden birisi sisteme müdahale edebilecekleri script'ler kullanmalarıdır. (Script kiddies)

Atak Çeşitleri

İçsel (İnternal) Atak

- External saldırganlara göre daha fazla zarar verirler.
- Özelliklere Bilgi sistemi varlıklara yakın olmaları hatta onları normal yollardan kullanmaları bu tür saldırıların en önemli özelliğidir.
- Yapılan güvenlik araştırmaları saldırıların çoğunun içerden ya da içerden kaynaklanan bilgi sızdırmalarıyla gerçekleştiğini göstermektedir.

Atak Çeşitleri

Pasif Atak:

- Pasif saldırılar, mesaj içeriğinin ifşa edilmesi ve ağ trafiğinin analiz edilmesidir.
- Veri içeriği değiştirilmediği için pasif saldırıları ortaya çıkartmak çok güçtür.
- Ana amaç "dinleme" ya da "bilgi toplama" dır.
- Şifrelenmemiş her türlü bilgi rahatlıkla okunabilir.

Atak Çeşitleri

Pasif Atak Çeşitleri:

- **Sniffing ve Eavesdropping**
- **Footprinting**
- **Backdoor (back doors)**
- **Fingerprinting**
- **….**

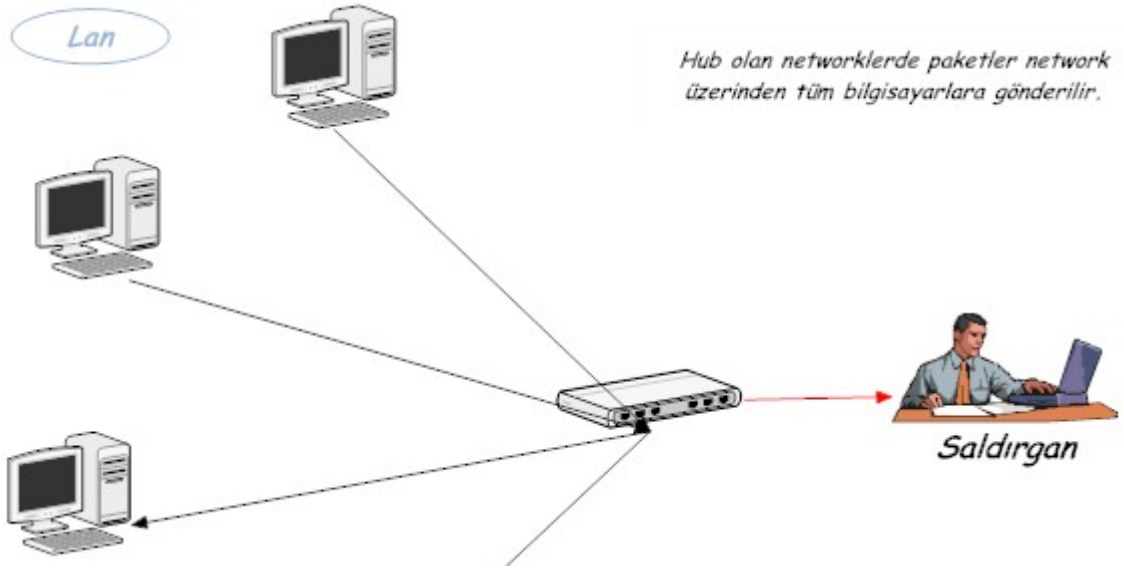
Paketlerin Monitör edilmesi (Paket Sniffing – paket koklama)

- Sniffing temel olarak verinin yolunu kesmek olarak tabir edilebilir.
- Sniffing ile networkdeki paketler yakalanabilir içeriği okunabilir.
- Sniffingin amacı ;
  Şifreleri (email, web, SMB , ftp, telnet,SQL) ,Email text'ini Transfer edilen dosyaları (e-mail,ftp, SMB) yakalamaktır.
- Sniffing metodu ikiye ayrılır ; Pasif Sniffing ve Aktif Sniffing.
- **Sniffing'e karşı zayıf protokoller:** Telnet, http, SMTP, NNTP, POP, FTP, IMAP, ..

Paketlerin Monitör edilmesi (Paket Sniffing – paket koklama)

Pasif Sniffing

- Hub olan sistemler için geçerlidir,Hub olan networklerde paketler tüm bilgisayarlara iletilir.
- Networkteki veri lan üzerinden tüm bilgisayarlara gönderildiği için sniff etmek kolaydır.



Paketlerin Monitör edilmesi (Paket Sniffing – paket koklama)

Aktif Sniffing

- Switch olan sistemler için geçerlidir. Switch MAC adreslerine bakar ve veriyi sadece alması gereken kişiye gönderir.
- Saldırgan switchi zehirlemeye (ARP Spoofing – Cache Posioning) çalışır , binlerce mac adresi gönderip swichin bir hub gibi davranmasına neden olur ve verinin tüm portlardan çıkmasını sağlar.

Sniffing ve Paket Sniffing Programları

- Tcpdump programı yaygın bir UNIX sniffing aracıdır.
- Bunun yanı sıra Solaris Snop vb araçlar vardır.
- WireShark ise grafik ortama sahip bir sniffing aracıdır.
- Diğer bir tür dinleme aracı da keylogger"lardır. Bu araçlar kullanıcının klavyesindeki basılan bütün tuşları kaydederler.
- Screenlogger ekrandaki verileri kaydetmek için kullanılır.
- MSN sniffer, Ethercap, Effetech (http sniffer) vs.

Diğer Pasif Atak Türleri

Footprinting

- Hedefin (şirketin) profilini çıkarmak. Atak öncesi adımlardan ilki:
- Web adresleri, server'lar vb. bilgilerin toplanması. Nslookup, tracert, vb araçlar.

1. Footprinting: Şirketin adı, adresi, vb ilk bilgileri.
2. Scanning: IP adresi, işlerim sistemi, vb bilgilerin elde edilmesi
3. Enumeration: Kullanıcı adlarını, bilgisayar adlarının elde edilmesi.

Diğer Pasif Atak Türleri

Backdoor (back doors)

- Bazen sistem yöneticileri İşletim sistemi ya da yazılım uygulamalarında sistemi izleme amaçlı bilinçli olarak bir açık kapı bırakırlar.
- Sonuçta yetkisiz kontrol işlemleri yapılabilmesidir.
  - Örnek proğramlar: Loki, NetCaz, Masters Paradise, NetBus, vb.

Fingerprinting

- Bir bilgisayar üzerindeki işletim sistemini belirlemek için kullanılır.
- Kullanılan tekniklerden birisi ICMP mesaj kotalarını kullanmaktır.
- Aynı zamanda Port scanning girişimi ile işletim sistemi ve host tanımlanmaya çalışılır.

Atak Çeşitleri

Aktif Atak:

- Aktif ataklar sisteme doğrudan zarar vermeyi, durdurmayı ya da bozmayı amaçlayan ataklardır.
- Atak yapan kişi (saldırgan) sistemi ya da servisi engellemeyi ya da kötüye kullanmayı amaçlar.
- Aktif ataklar genelde çabuk fark edilirler.
- Çünkü sistemi durdurur ya da bozarlar.
- Aktif Saldırılarda genellikle
  - saldırganın kimliğini gizlemesi(masquarade),
  - geri gönderme(replay),
  - Mesajın değiştirilmesi(modification of message) ve
  - servis durdurma(denial of service) amaçlanmaktadır.

Atak Çeşitleri

- Aktif Atak Türleri:

Aşağıdaki ana başlıklarda toplanabilir.

  - DoS Atak
  - Hijacking Atak
  - Spoof Atak
  - Buffer overflow
  - Exploit Atak

Aktif Atak Türleri

- **Denial-of-Services – DoS Atakları**
  - Çoğu DoS saldırısı network üzerinden yapılır.
  - Aynı zamanda lokal makine üzerinden de başlatılabilir.
  - Local olan DoS saldırıları genellikle daha kolay bulunur ve düzeltilebilir.
  - Örneğin bir "fork bomb" ise sürekli olarak tekrarlanan saldırılarla, oluşturulan işlemlerle sistem kaynaklarının tüketimi sağlanır.

Aktif Atak Türleri

DoS atakların amacı:

- Adından da anlaşılacağı üzere saldırılan bilgisayar veya çalışan servisi yavaşlatmak veya durdurmaktır.
- Yetkili kullanıcıların erişimini engellemek.
- Network'e sızmak, normal trafiği engellemek.
- LAN veya İnternette iki bilgisayar arasındaki trafiği engellemek.
- Şirket veya Kurumların önemli bilgilerini elde etmek ve onları kötü amaçlı kullanmak.
- Çeşitli Servisleri durdurmak ve sistemleri kullanılamaz hale getirmek (DNS, Web vs.).

Aktif Atak Türleri

DoS atak türleri:

- Smurf
- Buffer Overflow
- Ping of Death
- Teardrop
- SYN flood
- DNS Cache Posining

Aktif Atak Türleri

Çeşitli DoS atak Metodları:

- ICMP flood
- Smurf atak
- Ping flood
- Ping of death
- SYN flood
- Teardrop
- Peer-to-peer
- Permanent Denial-of-Service
- Banana
- Nuke
- Distributed atak (DDoS)
- Reflected atak
- Unintentional atak
- DoS flooding atak (emailler için)

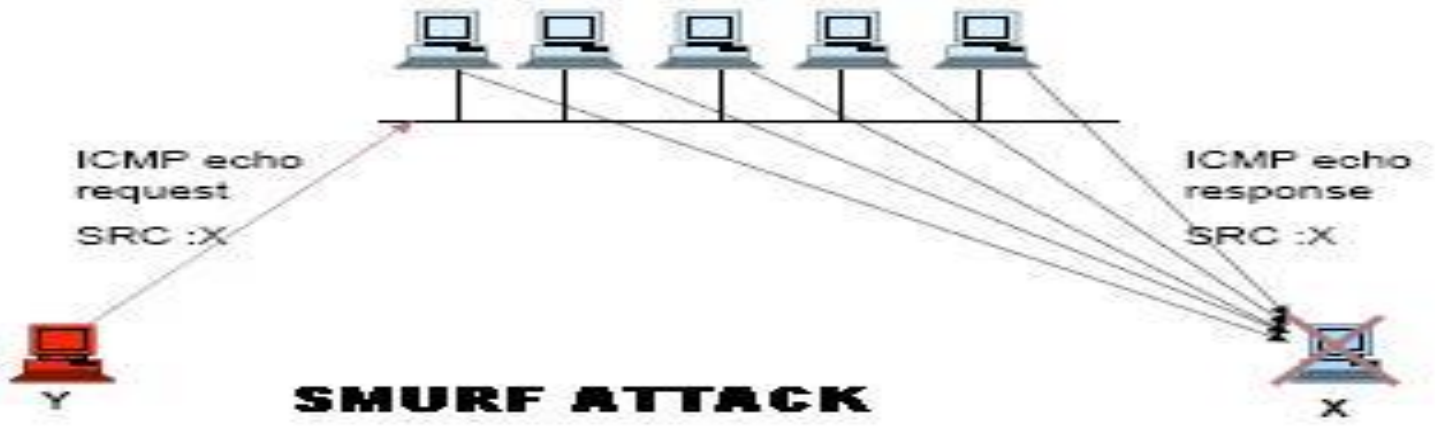
Aktif Atak Türleri

DoS Saldırı Türü:

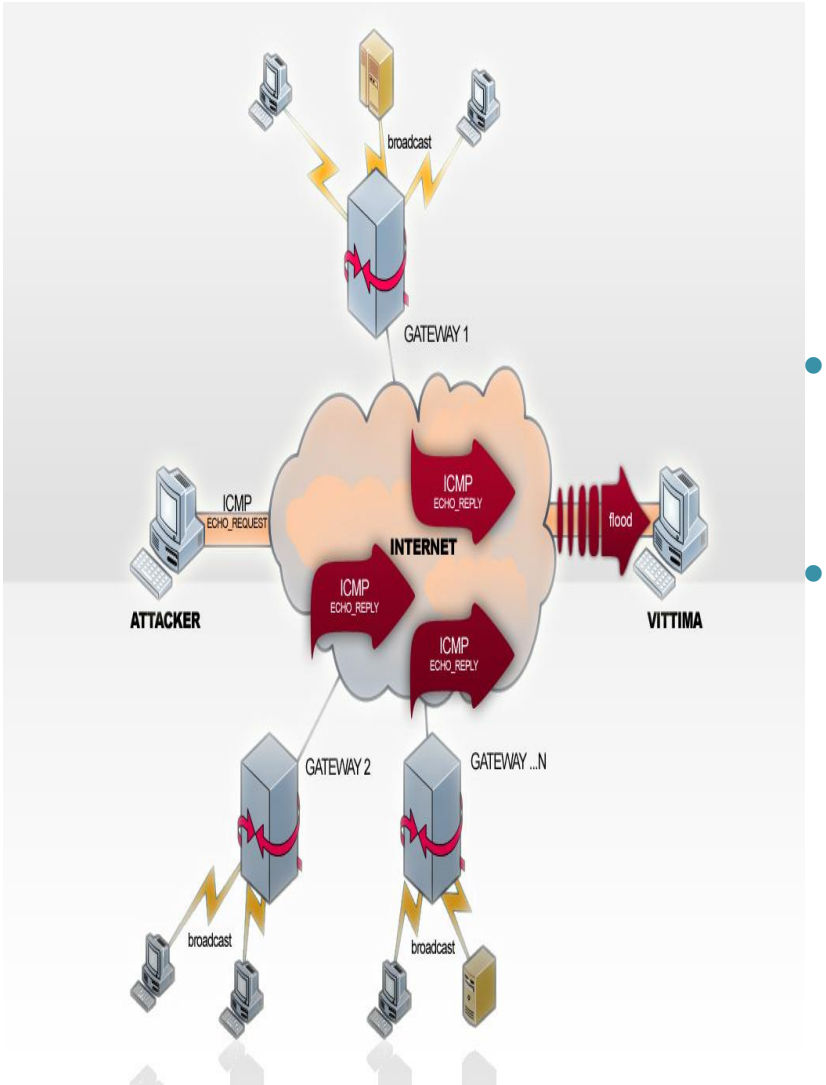
- **Smurf Saldırı;** ICMP (Internet Control Message Protocol)

Protokolüne ait özellikleri kötüye kullanan, band genişliğini hedef alan bir saldırı türüdür.

- İsmini saldırının yapıldığı programdan alır.
- Smurf saldırılarında IP ping paketinin işleyişinden yararlanılır.
- Çok sayıda reply paketi (yankı yanıt) ile hedefin gerçek trafiği alması engellenir.
- Bu tür ataklar "amplification attacks", "smurf attack" olarak da adlandırılır.



Aktif Atak Türleri



- Smurf ataklarında; kurban bilgisayarın IP adresinden network'ün broadcast adresine ICMP isteği (ping) gönderilir ve network üzerindeki bütün bilgisayarlardan kurban bilgisayara yanıt göndermesi sağlanır.
- Böylece ağda yavaşlama ve kurban bilgisayarın hizmet verememesi sağlanır.
- Aktif 100 bilgisayarın bulunduğu bir ağda 300kb/s ile smurf saldırısı yapılırsa ağabinecek yük yaklaşık olarak 3Mb/s olacaktır

Aktif Atak Türleri

DoS Atak Türleri:

Buffer Overflows;

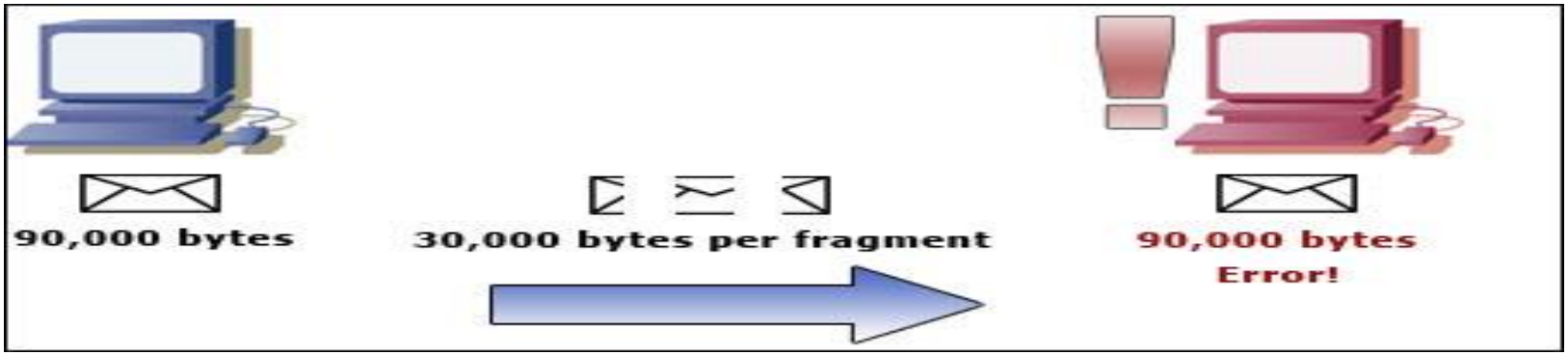
- Bilgisayar sistemlerinde kullanılan buffer'ların kapasitesinden çok veri gönderilerek sistemin bozulması ya da normalden fazla trafik oluşturarak iletişimin engellenmesidir.
- Saldırgan genellikle açıkları, buffer özelliklerini bilir ve ona göre sistemi zorlayacak bilgiler gönderir.
- Bu boyutu arttırılmış bir ping paketi olabilir.
- Buffer Overflow saldırısı yazılımların zayıf yönlerini kullanır.
- En Tipik "overflow attack"ları: Sasser wormdur.

Aktif Atak Türleri

Dos Saldırı Türleri:

Ping of Death

- Bu atağın amacı büyük boyutlu paket göndererek sistemi bozmaktır. Ayrıca IP paketleri taşıma sürecinde MTU (Maximum Transmission Unit) konfigürasyonu ile parçalara ayrılır. En bütük paket boyu The maximum size for a packet is 65,535 olması gerekirken birleştirilen paket daha büyük bir boyuta ulaşır. Sistem hata verir. PoD atağından amaç sistemi servis veremez hale getirmektir.



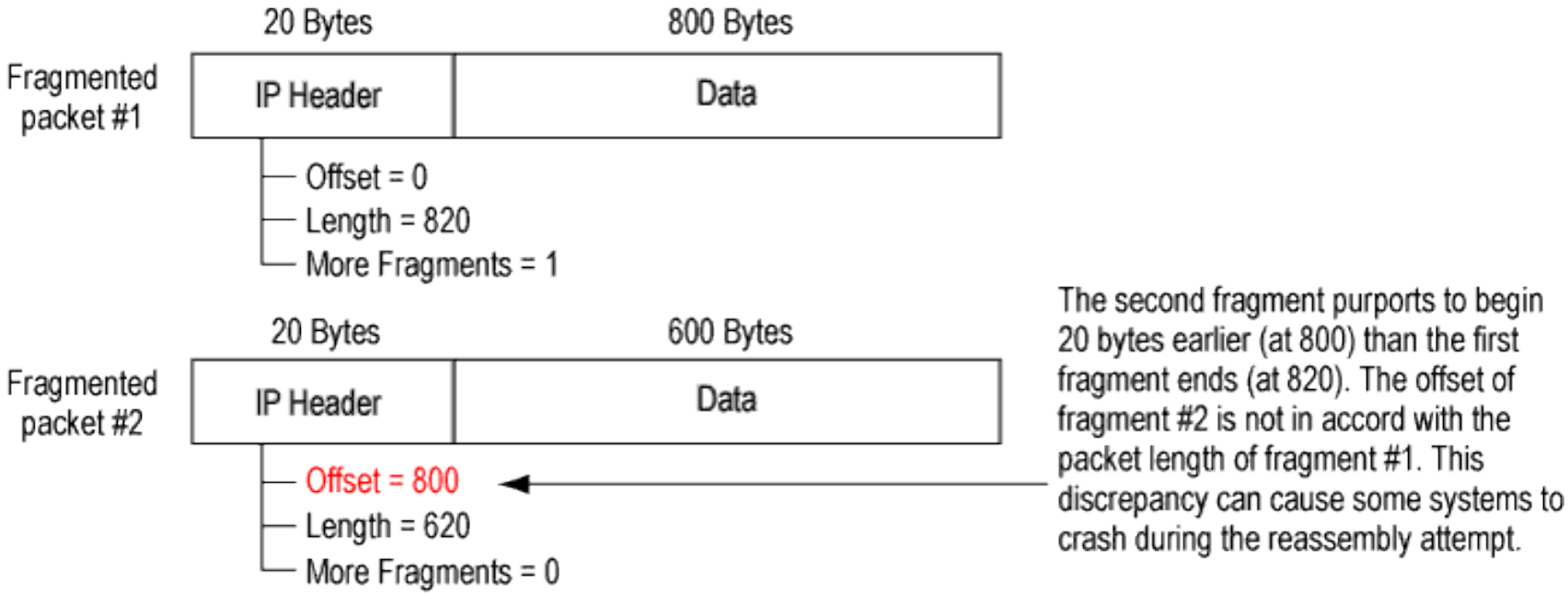
Aktif Atak Türleri

DoS atak Türleri:

Teardrop;

- Bu tür saldırılar büyük IP paketlerinin parçalara bölünmesi sistemini kullanır.
- Büyük MTU değerine sahip olan paket parçalanmış ve offset değeriyle hedef bilgisayara gönderilmiştir.
- Ancak Saldırgan paketlerin offset değerlerini karıştırarak (Bazen aynı değerler vererek) işletim sisteminin bu paketleri birleştirmesini yapamamasını sağlayarak sistemi çökertir.
- Overlapping, over-sized, payload paketler gönderilerek sistem bozulur.

Aktif Atak Türleri



Aktif Atak Türleri

DoS atak Türleri:

SYN Atağı / Syn Flood Atağı;

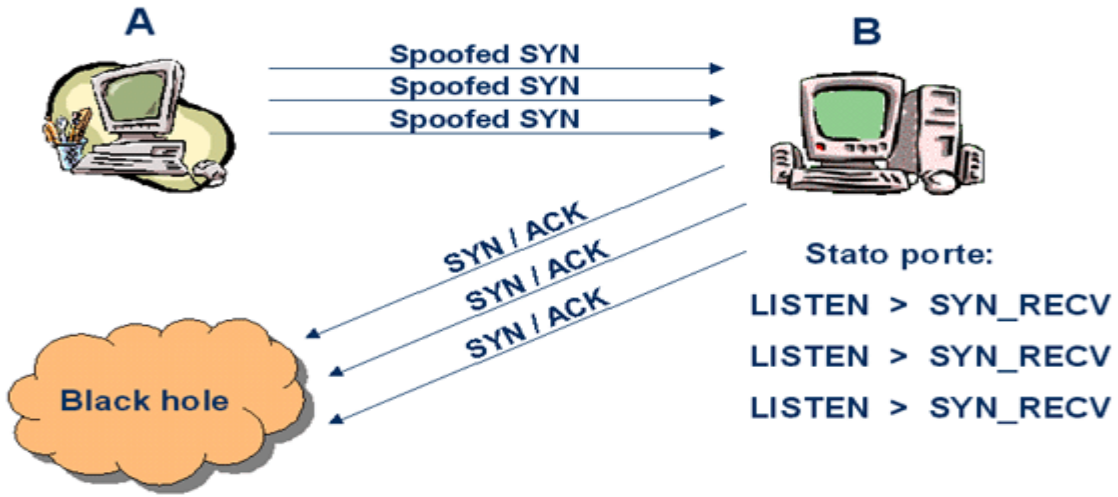
- TCP/IP protokolünün bir eksikliği üzerine kurulmuştur.
- Transmission Control Protocol (TCP) oturumunda iki hostun iletişim kurmasında kullanılan üç-yollu el sıkışmayı (the three-way handshaking) kullanır.
- Protokol basitçe şu şekilde çalışır.
  - İlk olarak SYN paketini gönderen hosta
  - SYN/ACK yanıtı verilir
  - ve kendisinden ACK yanıtı beklenir.

Aktif Atak Türleri

Dos Atak Türleri:

SYN Atağı / Syn Flood Atağı – Syn Bombardımanı;

- Syn Flood saldırısı yapmayı planlayan saldırgan yanıltılmış (spoofed/fake) IP adresini kaynak adresi olarak kullanarak çok sayıda SYN paketini kurban bilgisayara yollar.
- Kurban bilgisayar alının her SYN paketi için onay paketini (SYN-ACK) gelen IP adresine yollar.
- Adresin sahte olmasından dolayı kurban bir yanıt alamayacağından, SYN-ACK yanıtını sürekli göndermeye çalışılacak ve böylece hedef (kurban) bilgisayar meşgul edilmiş olacaktır.



Aktif Atak Türleri

Hijacking Ataklar:

- Client ile server arasındaki iletişimin arasına girmeyi, ve kullanıcının oturumunu ele geçirmeyi amaçlayan saldırılardır.
- TCP/IP nin güvenlik zafiyetleri üzerine kurulu olduğundan, "Replay" ve "Man in the middle" (MITM atak) teknikleri kullanılır.
- Bir "Man in the Middle" atağı saldırganın bir görüşmeyi kesmesi ya da araya girmesiyle yapılır.
- Araya giren saldırgan "eavesdropping" gibi dinleme işlemlerini yapabilir.

MITM atakları ayrıca şu adlarla da kullanılır:

- Bucket-brigade attack
- Fire brigade attacks
- Session hijacking
- TCP hijacking

Aktif Atak Türleri

TCP/IP Hijacking & Session Hijacking

- Saldırganın network üzerindeki bir hosta erişip onun üzerinden (spoofing) bir başka kurbana saldırmasıdır.
- Saldırgan iki kişi arasındaki güvenilir iletişimden yararlanır.
- TCP/IP hijacking ayrıca "active sniffing" olarak da adlandırılır.
- Ağ üzerindeki bir hosta erişen saldırgan onu bağlantısını mantıksal olarak keserek- aynı IP adresi ile başka bir bilgisayara bağlanır.
- Bir anlamda Session Hijacking içindeki bir adımdır.
- IP Spoofing ve MITM tekniklerini tamamen kullanır.
- Session hijacking ise Web-tabanlı uygulamaların oturumlarını ve cookie bilgilerini kullanarak yapılır.
- Hunt programı Telnet ve File Transfer Protocol (FTP) sessionları için hijack yapmada kullanılır.

Aktif Atak Türleri

Spoofing Atakları (Aldatma)

- Spoofing genel olarak saldırganın kendisine ait olmayan bir adresi ya da kimlik bilgilerini kullanılarak yaptığı ataktır.
- Örneğin; bir fake logon programı ile kullanıcının login bilgilerini alıp daha sonra onun hesaplarını kötüye kullanmak. Domain adını yanlış adreslere yönlendirmek ya da masquerading (başkasının yerine geçmek/impersonate) verilebilir.
- Spoofing işleminde saldırgan güvenilen bir IP adresine sahip olur ve ve onun bilgileriyle saldırır.
- Böylece hedef bilgisayar onun güvenilen bir kaynaktan geldiğini bildiği için anlaşılması en zor ataklardandır.

Aktif Atak Türleri

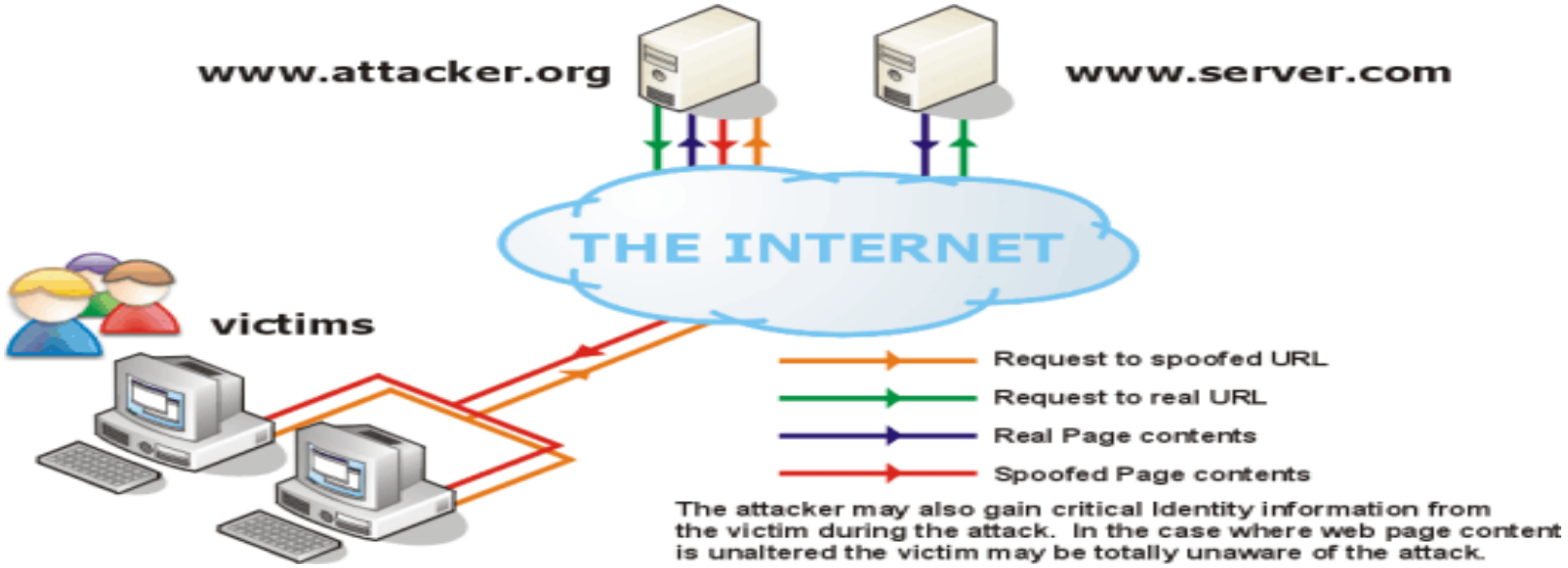
Spoofing Türleri:

IP Spoofing;

- Aldatma saldırısının genelde yapılan türü IP aldatmasıdır. Sahtecilik olarak çevirmek mümkündür.
- IP paketlerinin kaynak IP' sini değiştirmekle sağlanmaktadır.
- Böylece paketi alan hostun, paketin geldiği kaynak adresini bilmesini engellenmiş olur.
- Host gelen paketin saldırgandan değil de kullanıcıdan geldiğini sanır.
- IP adreslerine göre çalışan servisler üzerinde oldukça etkilidir.
- Sahte paketler üretme (fabrication) bu şekilde yapılabilmektedir.
- KOD, jolt, papasmurf gibi programlarla bu saldırı gerçeklenmektedir.

Aktif Atak Türleri

- IP Spoofing iki şekilde yapılır.
  - Proxy/Socks sunucularını kullanarak, veya IP paketlerini editleyerek.
  - Proxy/Socks sunucusu kullanmak basit bir yöntemdir.
  - Daha çok web/IRC bağlantılarında IPyi gizlemek için kullanılır.
  - IP paketlerini editleyerek yapılan IP Spoofing çok etkilidir ve genel olarak D.o.S saldırılarında veya session-hijacking yönteminde kullanılır.



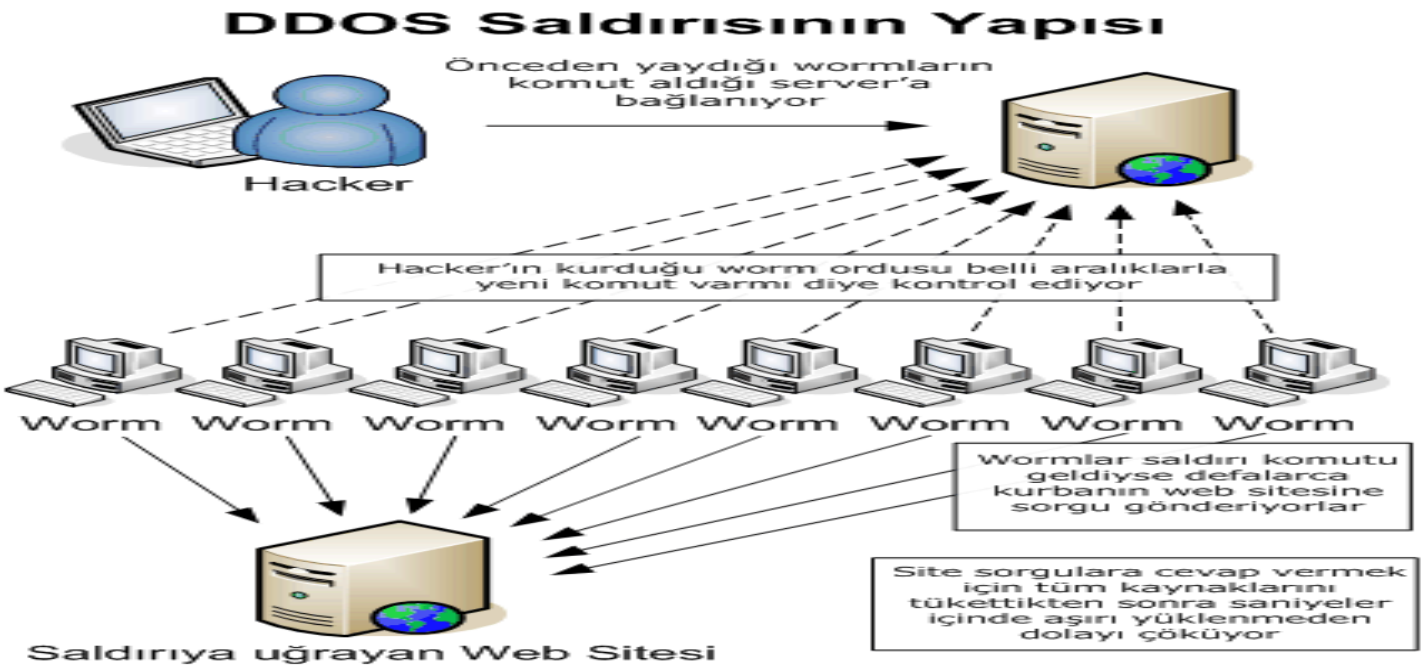
Aktif Atak Türleri

- Spoofing türleri:
- **E-mail Spoofing**
  - Güvenilen bir sahte e-mail adresi ile mail göndermek.
  - Ardından eklenen bir ek dosyası ile de hedefe saldırmak.
  - Spoofing, e-posta başlıklarının değiştirilmesi ile iletinin orijinal göndericisi yerine başka bir yerden ya da kurumdan geliyormuş gibi gösterme işlemidir.
- **Web Site Spoofing / Web Spoofing**
  - Saldırganın bilinen bir Web sitesi adresininin sahtesini kullanarak saldırı yapmasıdır.
  - Fake bir banka sitesi.

Aktif Atak Türleri

Distributed DoS atak:

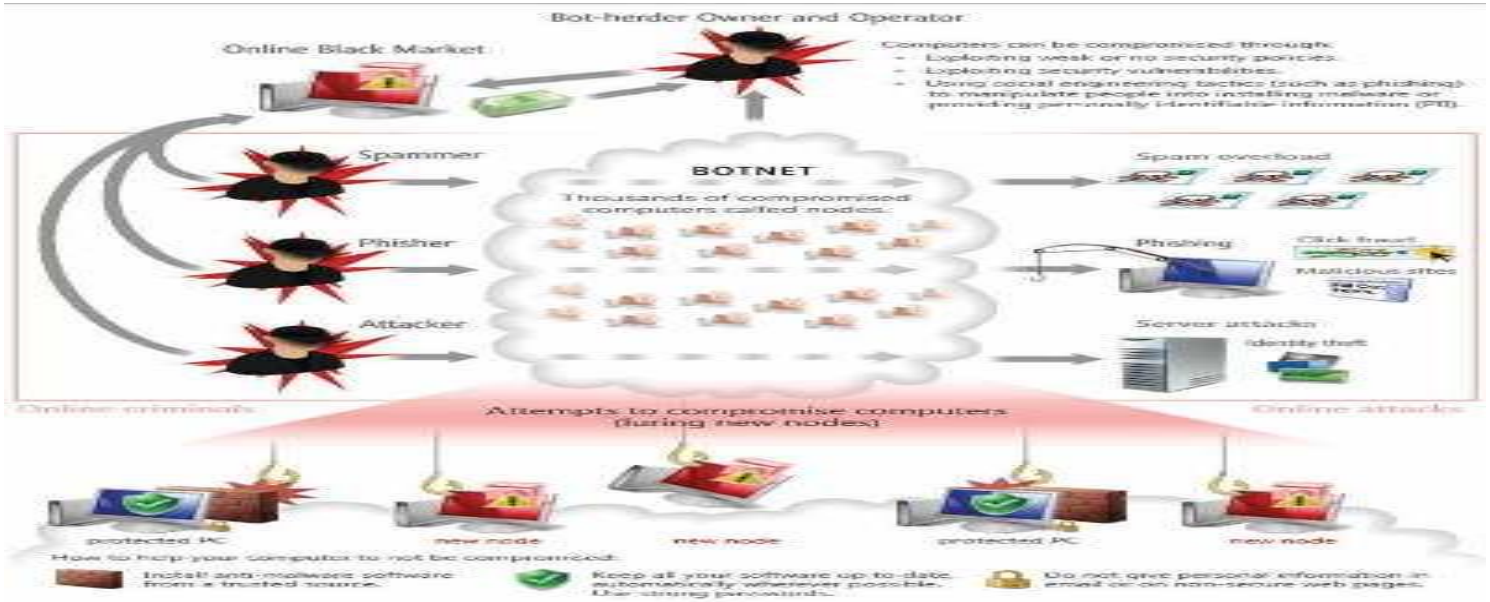
- DoS atağında saldırgan tek bir bilgisayar kullanarak saldırırken DDoS atakta saldırgan ele geçirmiş olduğu bilgisayarları kullanarak saldırmaya çalışır.
- Saldırgan tarafından ele geçirilmiş bilgisayarlara veya sistemlere zombi denir.
- Saldırgan farklı IP numaralarına sahip zombi bilgisayarları kullanarak aynı anda sistem kaynaklarını zorlar ve sonuçta sistem kilitlenir.
- 2011 yılında gerçekleştirilen DNS sunucularına yapılan saldırı bu tiptendir. 2009 yılında tiwiter da aynı saldıra maruz kalmış ve sisteme 1 gün ulaşılamamıştır.
- Ençok bilinen DDoS saldırıları MyDoom virüsü ve Stacheldraht ile gerçekleşmiştir.



Aktif Atak Türleri

DDoS atağı için zombi bilgisayar elde etmek veya BOTNET kurmak

- BOT Robot kavramının kısaltılmış hali olup saldırganlar tarafından ele geçirilmiş bilgisayarlara verilmiş addır.
- BOTNET ise aynı amaca hizmet eden BOT topluluğudur.
- Bir bilgissayarın BOT olabilmesi için bir şekilde Kötü amaçlı bir yazılım yüklenmesi gerekir.
- IRC programları aslında bu tip yazılımların bir türüdür.
- Bu tip programlar kullanılarak bilgisyara port açtırmaktan tutunda format bile attırılır.
- Sistemin tüm kontrolü saldırganın elinde olduğundan internet ortamında istediği sisteme veya bilgisayara saldırta bilir.



Aktif Saldırı Türleri

- **DNS Cache Poisoning**
- Cache poisoning, DNS poisoning ya da DNS cache poisoning olarak bilinir.
- DNS kayıtlarının bozularak kullanıcıları başka server'lara yönlendirilmesini sağlar.
- Bu sırada bir worm, spyware, Web browser hijacking programı ya da diğer bir kötü kod kullanıcının bilgisayarına indirilir.
- Cache poisoning, URL poisoning ile ilgilidir. URL poisoning işlemi "location poisoning" olarak da bilinir.
- Internet kullanıcılarının davranışları izlenir.

Phishing Atakları

- **Phishing**
  - E-mail ve Web site spoofing işleminin birleşimidir.
  - Kullanıcıya sahte bir mail gönderilerek kullanıcının sahte bir siteye çekilmesi amaçlanır.
  - Böylece kullanıcının yasal bir banka sitesine giriş için kullandığı bilgilerin sahte site yoluyla elde edilmesidir.
  - Çok gelişmiş türleri vardır.

- **Hoax Mail**
  - Internet üzerinden gönderilen ve genelde "fazla iyi" bir hikaye ile bilgi ya da para sızdırmayı amaçlayan çalışmalardır.
    - Örneğin; e-posta adresi toplamak veya markaları karalamak için oluşturulan yalan haber içeren e-postalar.

Keşif Atakları

- Ping komutu : İki uçbirim arasında fiziksel bağlantının varlığı ve IP protokolünün düzgün kurulup kurulmadığına yönelik test işlemidir. İki uçbirim arasında iletişimin varlığını sınar. Bir saldırgan bunu kurban ağın sınırlarını belirlemede ve ağı keşfetme aşamasında kullanabilir

- Port taraması : Erişilebilir uç sistemler keşfedildikten sonra saldırgan bu sistemlerde 4. katman düzeyinde(OSI) açık olan portları taramak suretiyle aktif olan servisleri öğrenebilir.

- Uygulama ve açık taraması : Uç sistemdeki bir işletim sistemi veya web sunucusu uygulaması olabileceği gibi router, gateway, firewall gibi cihazlardaki yazılımlar da olabilir. Saldırgan hedefteki sistemde çalışan yazılımları ve bunların açıklarını taramak suretiyle sistem hakkında daha detaylı bilgiye erişmiş olur.

Password Atakları

- Password atakları yaygın olarak yapılır. İki tür password atağı vardır:
  - Brute force
  - Dictionary-based atakları
- Password atakları online ya da offline olabilir.
- Online ataklarda password'ler sistemden doğrudan alınır.
- Offline ataklar daha zordur.
- Ancak network üzerinde bir işlem oluşturmazlar ve "lock out" sorunu olmaz.

Password Atakları

- **Brute Force Attacks**
  - Bir tür Password Cracking yöntemidir.
  - Password'ü tahmin etmek için deneme yapmayı içerir.
  - Brute force saldırıları belli araçlarla yapılır.
  - Bu araçlar olası karakter kombinasyonu deneyerek parolayı tahmin etmeyi sağlar.
  - Brut force ataklar, dictionary ataklarına göre daha uzun zaman alır.
- **Birthday Atak**
  - İnsanları aynı günde doğmuş olacakları varsayımından hareket ederek; MD5 içindeki keyleri bulmak için yapılan bir saldırıdır.
  - Birthday saldırısı bir tür brut force saldırısıdır. Bir şekilde hash fonksiyonunu kırıp password'leri bulmayı amaçlar.

Password Atakları

Dictionary-based Attacks

- Brut force benzeri bir saldırı işlemidir.
- Bir dictionary (sözlük) dosyası kullanılarak password'lerin tahmin edilmesidir.
- Sözlük terimi kelimelerden oluşan bir veritabanında gelir.
- Bu veri parolanın kırılmasına yardımcı olur. Dictionary saldırısından korunmak için "kolay tahmin edilemeyen" parolalar girilmesi gerekir.

Kod atakları

Zararlı Kod Atakları (Malicious Code Attacks)

- Kod atakları özel olarak yazılmış "zararlı" programlar aracılığıyla bilgisayarlara zarar vermeyi amaçlar.
- Genel olarak malware ya da spefisik olarak trojan horse, virus, spyware, rootkit olarak adlandırılan bu programlar farklı şekillerde bulaşırlar ve çoğalırlar.
  - **Kod atakları:**
    - Virüsler
    - Worm'lar
    - Trojan Horses
    - RootKits
    - Logic Bombs
    - Spyware ve Adware

Kod Atakları

Virüs

- Kendi kendine çalışmaz. Bir dosyaya bulaşır. Çalışabilir durumdadır. Dosyaları bozar. Dosyalara yapışır, onların üzerinden çalışır. Genellikle veri dosyalarını değiştirir, bozar. Mesajlar gösterir ya da işletim sisteminin fonksiyonlarını bozar.

  Virüs çeşitleri:

  - Parasitic: Executive dosyaları etkiler.
  - Bootstrap Sector: Boot sektörde yerleşir.
  - Multi-partite: Birden çok özelliğe sahip. Örneğin Parasitic ve Bootstrap.
  - Companion: Var olan bir programın aynı adı kopyasının oluşturur.
  - Link: İşletim sisteminin bir programını bulmasını/çalıştırmasını bozar.
  - Data File: Veri dosyalarını bozar.
  - Polymorphic: Sistemi bozan tipik virüsler. Mesajlar verir ya da dosyaları siler.
  - Stealth: Kendini gizler.
  - Retrovirus: Antivirüs yazılımlarını bypass etmeyi amaçlar.
  - Armored virüs: Tanımlanamayan virüsler.
  - Phage virüs: Programları ve veritabanları değiştirir.
  - Macro virüs: Ofis programlarını bozmaya yönelik.

Kod Atakları

Worm

- Kendi kendine çalışır ve kendini kopyalar.
- Virüsler gibi bir dosya üzerinden (host) hareket etmezler.
- Örneğin sistemi restart etmeyi sağlayan bir worm, genelde bellekte aktif kalan programlardır.

Bazı örnekler:

- Nimda ,SQL Slammer, Blaster, Morris ,Badtrans, Code Red

Trojan Horse

- Virüs gibi bir host dosya kullanmaz. Kendi başına bir programdır.
- Kopyalama ile çoğalmaz. Genelde server gibi çalışır.
- Sistemden dışarıya bilgi sızdırılır.
- Trojan'lar iletişim programı, e-mail ya da Web sayfaları olabilir.
- Manuel olarak yüklenebilir, e-mail ile gönderilebilir ya da bir programla birlikte gönderilebilir.

  Trojanlar aşağıdaki bilgileri elde etmek için kullanılırlar:

  - Kredi kartı bilgileri
  - Kullanıcı hesap bilgileri (logon name, password, vb)
  - Gizli dokümanlar

Kod Atakları

Rootkit

- Kendisini gizleyebilen bir tehlikeli yazılım türüdür. Adı, UNIX'te kullanılan root kullanıcısından gelir. İşletim sisteminin temel bileşenlerini bozmayı hedef alır. Mevcut işletim sistemini virtual machine yapmak, uzaktan kontrol programları yüklemek gibi işlemler yapılır.

Logic Bomb

- Bir tür virüs olan logical bomb'lar önceden belirlenmiş koşullara göre çalışırlar. Örneğin belli bir tarih ve zamanda aktive olmak gibi.

Spyware ve Adware

- Spyware programları yüklendiği bilgisayar üzerinde spy (ajan) görevini üstlenir. Özel bilgilerin alınması ve sistem fonksiyonlarının bozulması gibi işlevlere sahiptir. Özellikle Internet üzerinden gelir ve Browser üzerinde çalışır.

Sosyal Mühendislik

- İnsanları aldatarak ya da yanıltarak yapılan iletişim sonucunda bilgiler elde etmek ve onları saldırı amaçlı kullanmak ya da çeşitli saldırılarda kullanmak üzere bilgi hırsızlığı yapmak.
- "Sosyal mühendislik" olarak adlandırılan bu ataklar genellikle insan kaynaklıdır ve çeşitli iletişim teknikleriyle network güvenliğine ilişkin bilgileri elde etmeyi amaçlar.

  - Kişileri inandırma yoluyla istediğini yaptırma eylemidir.
  - Albenili e-posta ekleri, web hizmetleri. (too good to be true)
  - ISP görevlisi kılığında kullanıcının şifresini öğrenmek.
  - Banka personeli kılığında kişisel ve kredi kartı bilgilerini ele geçirmek.
  - Teknisyen kılığında kurumun içine fiziksel olarak sızmak...

Sosyal Mühendislik

Sosyal Mühendislik Yöntemleri

- Sahte senaryolar uydurmak (pretexting)
- Güvenilir bir kaynak olduğuna ikna etmek (phishing)
- Güvenilir bilgi karşılığında yardım, para, eşantiyon, hediye, … önermek
- Güven kazanarak bilgi edinmek.
- Çöp karıştırmak, eski donanımları kurcalamak
- Çöp karıştırmak -- Çöpe atılmış CD, disket, kağıt, ajanda, not, post-it, … gibi eşyaları incelemek
- Eski donanımları kurcalamak – Hurdaya çıkmış, ikinci el satış sitelerinde satışa sunulmuş, çöpe atılmış, kullanılmadığı için hibe edilmiş donanımın içeriğini incelemek

Günümüzde sık karşılaşılan ataklar

Günümüzde karşılaşılan atakları genel olarak şu şekilde sıralayabiliriz:

- Keşif (Pasif Atak)
- Başlıkta oynama ile paket parçalama işlemi (Aktif Atak)
- 3. veya ve 4. katman seviyesinde aldatma (3rd and 4th layer spoofing)
- ARP ve DHCP atakları (Aktif Atak)
- Yayınla saldırıya maruz bırakma (Broadcast amplification attacks-smurf)
- Paket gözleme (Sniffing – Pasif Atak)
- Uygulama katmanı saldırıları (Aktif Atak)
- Ortadaki adam saldırısı (Man in the middle)
- Paket seli (Flooding)
- Sosyal Ağ atakları
- Açık sistem Web atakları
- Finansal ve güvenlik kurumlarına yapılan Ddos Atakları
- ….

İletişim Protokolü Bazlı Saldırılar

- IP sahteciliği (IP spoofing)
- TCP dizi numarası saldırısı (TCP sequence number attack)
- ICMP atakları
- Ölümcül ping
- TCP SYN seli atağı (TCP SYN Flood Attack)
- IP parçalama saldırısı (IP Fragmentation Attack)
- Internet yönlendirme saldırısı (Internet Routing Attacks)
- UDP sahteciliği ve Dinleme (UDP Spoofing and Sniffing)
- UDP portunu servis dışı bırakma saldırısı (UDP Port Denial-of-Service Attack)
- Rasgele port taraması (Random port scanning)
- ARP saldırıları (ARP Attacks)
- Ortadaki adam saldırıları

IPv4 Zaafiyeti Saldırıları

- Out of Band Nuke,
- Land,
- Teardrop,
- Boink,
- Nestea,
- Brkill,
- ICMP Nuke,
- Jolt/Ssping,
- Smurf,
- Suffer3
- Vs…

İşletim Sistemine Yönelik Saldırılar

- UNIX, Linux ve MS Windows için ayrı ayrı geliştirilen ve işletim sistemi açıklarını kullanan yazılımsal saldırılardır.
- Bunlar işletim sistemi mimarisine göre özel tasarlanırlar.
  - Rootkitler
  - Exploitler
    - Windows Null Session Exploit
    - PHF Exploit
    - ASP Exploit
    - Sendmail Exploit
    - Vs….

Uygulama Katmanına Yönelik Saldırılar

- DNS,SMTP,MIME,NFS,NTP saldırıları
- Uzaktan giriş ile saldırılar (Hacking and Remote Login)
- Bilgi sızdıran saldırılar
- URL sahteciliği (URL Spoofing)
- CGI saldırıları
- X-Windows sistem saldırıları
- Kötü niyetli java ve AktiveX uygulamacıkları
- Sistem log seli (Güvelik duvarının Logunu doldurma yönünde yapılan saldırı)
- Program ve ağ üstündeki virüsler

Kaynaklar

- CERT 2010 Research Report
- http://www.comptechdoc.org/independent/security/recommendations/secattacks.html
- IPv4 / IPv6 Güvenlik Tehditleri ve Karşılaştırılması, A. Çakın, M.A. Aydın Emo Dergisihttp://www.emo.org.tr/ekler/e964cf77e41a4da_ek.pdf
- **A taxonomy of network and computer attacks,** S Hansman, R Hunt - Computers & Security, 2005 – Elsevie
- S Hansman, R Hunt - Retrieved March, 2003 - cosc.canterbury.ac.nz

,A taxonomy of network and computer attack methodologies.

- Simmons, C., Shiva , S., Dasgupta , D., and Wu, Q., "AVOIDIT: A

cyber attack taxonomy," , Technical Report: CS-09-003, University of Memphis, August 2009

- https://isc.sans.edu/presentations/SANSFIRE2008-Is_Troy_Burning_Vanhorenbeeck.pdf
- Yeni Nesil İnternet Protokolü'ne (IPv6) Geçişle Birlikte İnternet Saldırılarının Geleceğine Yönelik Beklentiler, Ali EFE, Akademik Bilişim 2006 - Denizli 2006