Aşağıda yer alan içerikler eğitim notlarıdır.

Düzenleyen:

Emre KÖSEOĞLU

İletişim:

https://www.linkedin.com/in/emre-k%C3%B6seo%C4%9Flu-b753661a3/

Table of Contents

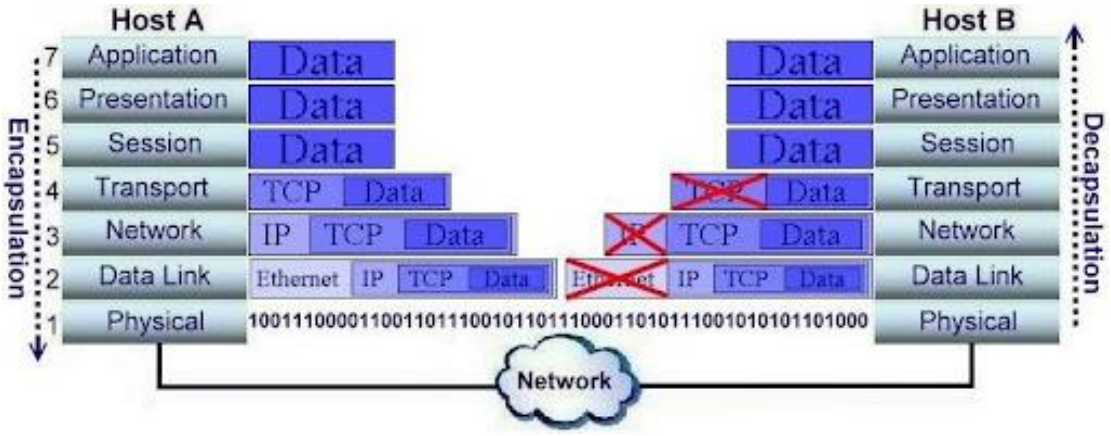
NETWORK GÜVENLİK TESTLERİ 3
OSI (Open Source Interconnection) Katmanları 3
Fiziksel Katman (Physical Layer) 4
Veri Bağlantı Katmanı (Data Link Layer) 4
Ağ Katmanı (Network Layer) 5
Nakil Katmanı (Transport Layer) 5

Sunum Katmanı (Presentation Layer) 8
Uygulama Katmanı (Application Layer) 8
Protokol Detayları 9
Domain Nedir? 11
DNS (Domain Name System) 12
DNS Kayıtları ve DNS Kayıt Tipleri 13
DNS Zone 13
Güvenlik Duvarı (Firewall) 17
WAF 17
IPS 17
IDS 17
IDS/IPS Topoloji 18
Network Scanning & Detection Evasion 19
Ağdaki Hostların Keşfi 19
TCP Taraması 19
SYN Taraması 20
UDP Taraması 20
Nmap (-sU) 20
XMass Taraması 20
İşletim Sistemi Tespiti 20
Servis ve Versiyon Tespiti 20
Zafiyet Taraması 20
Soket Bağlantı Türleri 20
BIND Shell Kavramı 20
Reverse Shell Kavramı 21
Tünelleme Teknikleri 22

NETWORK GÜVENLİK TESTLERİ

OSI (Open Source Interconnection) Katmanları

Sızma Testi, risk analizi zafiyet tarama gibi işlemler yapılırken ağ yapısının nasıl tasarlandığı, ağın nasıl çalıştığı, hangi ağ protokollerinin ağ üzerinde çalıştığının bilinmesi çok önemlidir. Bu bölümde temel network kavramları anlatılacak ağdaki cihazların görevleri hakkında bilgiler verilecek, ağ cihazlarında çalışan protokoller incelenecektir. Bu bölümde dinleyicinin ağ yapısı ve protokolleri hakkında ön bilgi sahibi olması amaçlanılmıştır.



Fiziksel Katman (Physical Layer)

Fiziksel katman 1 ve 0 sinyallerinin taşındığı katmandır. Bu katmanın görevi dijital sinyali taşımaktır. CAT5 kablo CAT6 kablo, fiber kablolar ve sinyali zayıfladığı anda sinyali yeniden güçlendirerek üreten tekrarlayıcılar bu katmanda çalışır. Ayrıca en ilkel ağ cihazlarından biri olan HUB cihazıda bu katmanda görev alır.

HUB cihazı, bir portundan aldığı veriyi diğer tüm portlarına ileterek, ağ içerisindeki iletişimi devam ettiren bir cihazdır.

Veri Bağlantı Katmanı (Data Link Layer)

Bu katman ağ içi iletişimi sağlar. Veri bağlantısı katmanı donanım katmanına erişmek ve kullanmak ile ilgili kuralları belirler. Veri bağlantısı katmanının büyük bir bölümü ağ kartı içinde gerçekleşir. Veri

bağlantısı katmanı ağ üzerindeki diğer bilgisayarları tanımlama, kablonun o anda kimin tarafından kullanıldığının tespiti ve fiziksel katmandan gelen verinin hatalara karşı kontrolü görevini yerine getirir.

Switchler, üzerinde bulunan MAC tablosuna göre frame'leri ilgili yere gönderir. MAC Tablosunda fiziksel portlar ve ilgili porta bağlı olan cihaz ya da cihazların MAC adresleri liste halinde bulunur.

```
Switch#show mac-address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

  10    0001.c7ad.e316    DYNAMIC      Fa0/24
  10    0002.4ab7.1701    DYNAMIC      Fa0/24
  11    0001.c7ad.e316    DYNAMIC      Fa0/24
  11    0002.4ab7.1701    DYNAMIC      Fa0/24
  12    0001.c7ad.e316    DYNAMIC      Fa0/24
  12    0002.4ab7.1701    DYNAMIC      Fa0/24
  12    000d.bd94.6b58    DYNAMIC      Fa0/1
  12    0060.3e5c.ba1d    DYNAMIC      Fa0/2
  12    00e0.f934.e3c4    DYNAMIC      Fa0/3
  13    0001.c7ad.e316    DYNAMIC      Fa0/24
  13    0002.4ab7.1701    DYNAMIC      Fa0/24
Switch#
```

(Mac Flood)

Ağ Katmanı (Network Layer)

Network katmanı networkler arası iletişimi sağlamakla görevlidir. Bu katmanda yönlendirme cihazı görev yapar. Bu cihazın görevi farklı ağları birbirine bağlamaktır. IP, ICMP ve ARP protokolleri bu katmanda görev yapar. ARP Protokolünün görevi IP adresinden MAC adres çözümlemesidir.

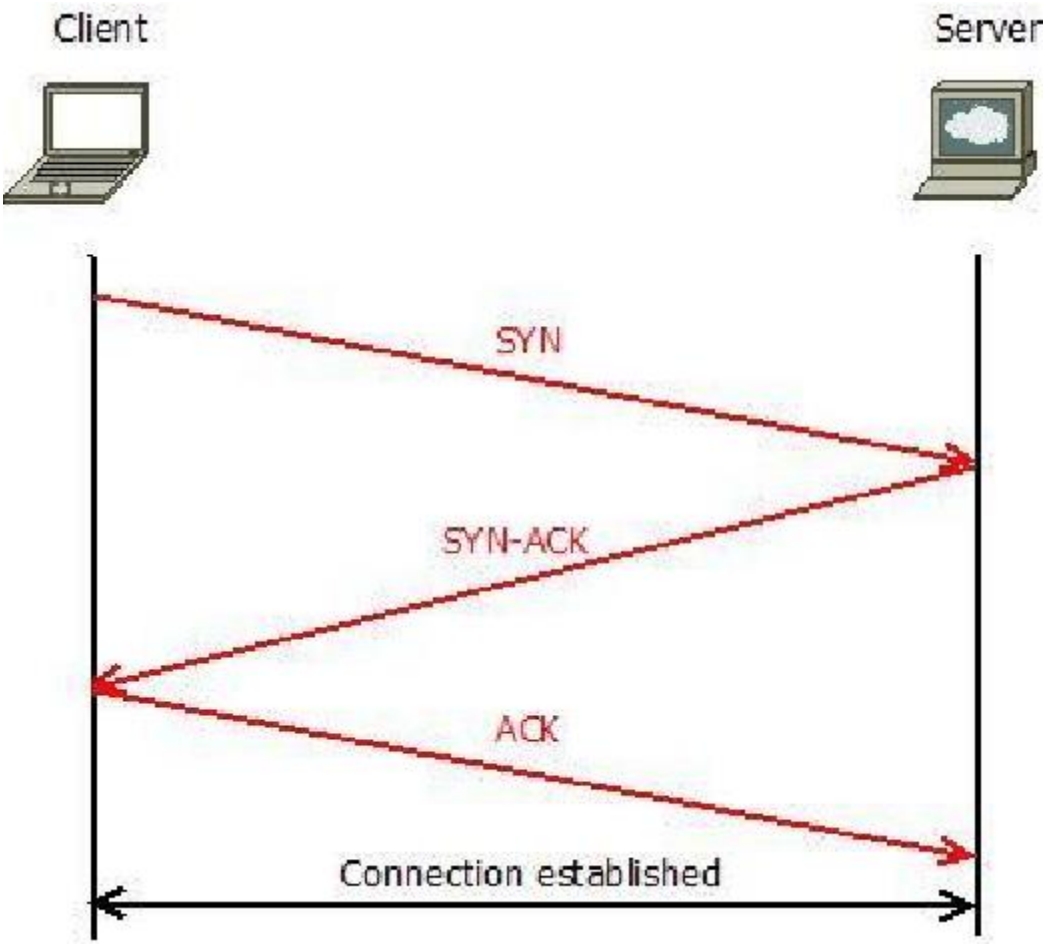
(ARP Poisoning)

Nakil Katmanı (Transport Layer)

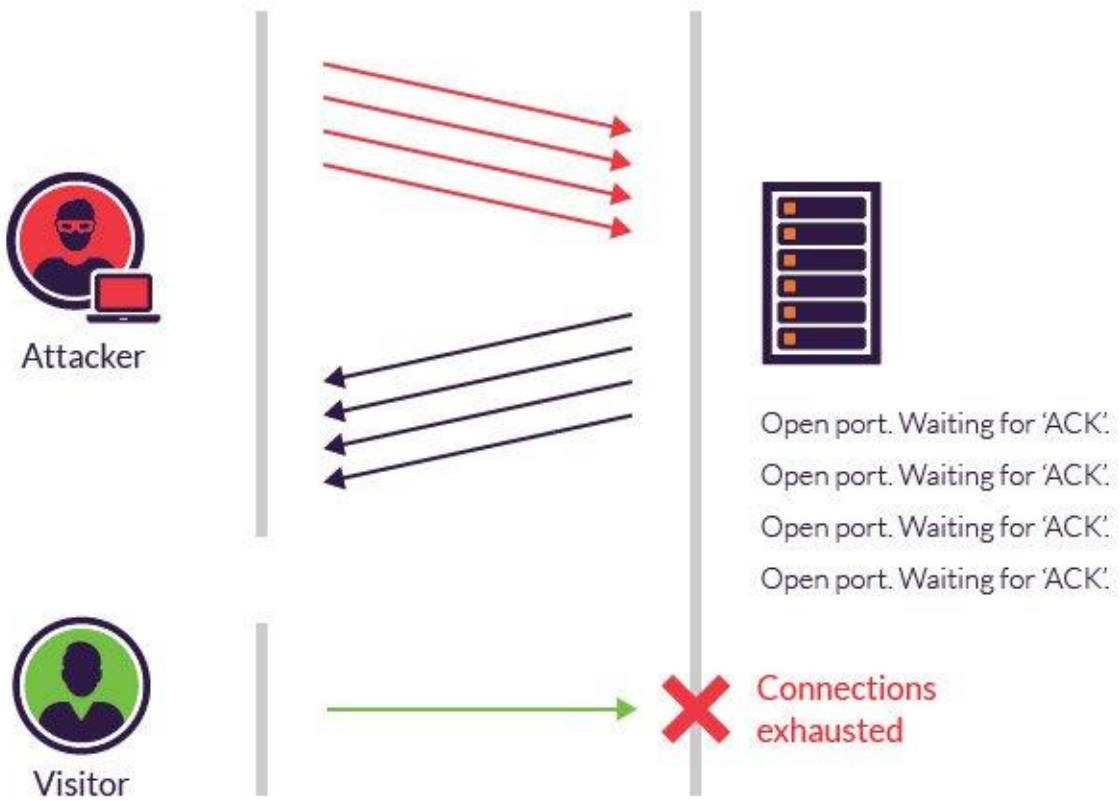
Uçtan uca iletişimi sağlayan katmandır. Port, network servislerinin bağlantı kurabilmesi için sistem üzerinde açılması gereken sanal iletişim noktalarıdır. TCP ve UDP bu katmanda çalışır. Bilgisayarınızda açık olan portları görüntülemek için windows kullanıyorsanız terminal açarak “ netstat -an” komutu, Linux kullanıyorsanız, “netstat -tuna” komutunu kullanabilirsiniz.

TCP (Transmission Control Procotol)

3’lü el sıkışma yöntemini kullanarak transfer edilen verinin karşı tarafa gidip gitmediğini, veri kaybı olup olmadığını kontrol eder.

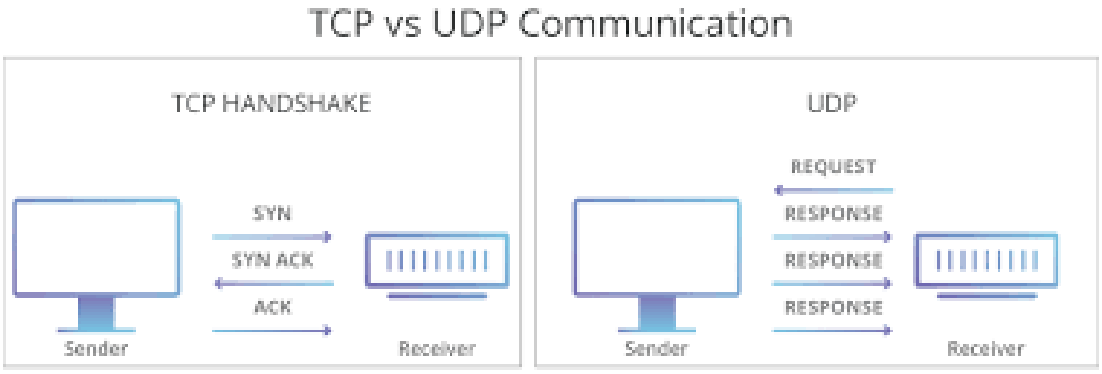


(SYN Flood)

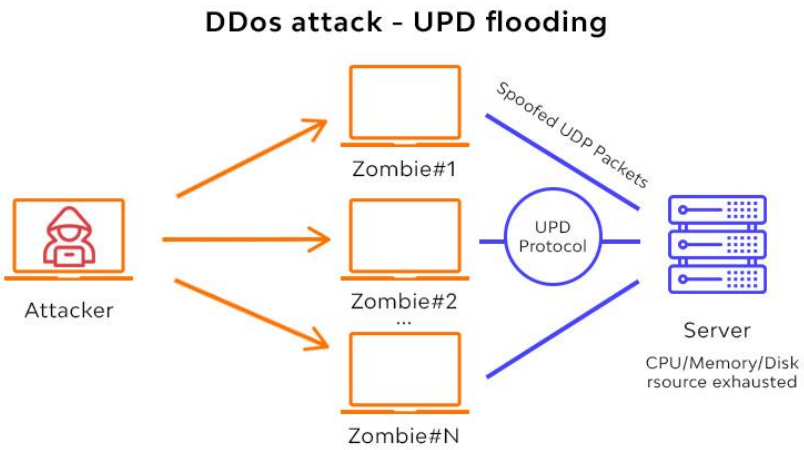


UDP (User Data Gram Protokol)

UDP Protokolünde herhangi bir onaylama mekanizması yoktur. Hızlı iletişim için gereken yerlerde kullanılır. VoIP, Stream vb.



(UDP Flood)



Oturum Katmanı (Session Layer)

İki bilgisayar arasında oturum açılması, devam ettirilmesini ve kapatılmasından sorumlu olan katmandır.

SMB (Dosya paylaşımları için kullanılır), NFS (Ağ Dosya Sistemi, ağda birden fazla bilgisayar üzerinde bulunan çeşitli dosyaların tek bilgisayardaymış gibi kullanılmasına olanak sağlayan protokol) bu katmanda çalışır.

(NTLM Relay Attack)

(SMB Exec)

Sunum Katmanı (Presentation Layer)

Verinin formatının belirlendiği katmandır. Veri sıkıştırma, şifreleme bu katmanda yapılır. Bu katman için ASCII kodlar ve jpeg örnek olarak verilebilir.

(Ransomware Attack)

Uygulama Katmanı (Application Layer)

Uygulamaların çalıştığı katmandır. HTTP,FTP,DNS,SNMP,TFTP,HTTPS,DHCP,SMTP,TELNET,SSH,RDP gibi protokoller bu katmanda çalışır.

Protokol Detayları

Bu başlıkta bazı önemli protokoller hakkında tanımlar yapılmış ve işlevleri kısaca özetlenmiştir. Önemli protokoller hakkında bilgi sahibi olunması amaçlanmıştır.

HTTP

HTTP (Hyper-Text Transfer Protocol), bir kaynaktan dağıtılan ve ortak kullanıma açık olan hiperortam bilgi sistemleri için uygulama seviyesinde bir iletişim kuralıdır. TCP 80. Portu kullanır.

HTTPS

HTTPS, HTTP Protokolünün şifreli halidir. TCP 443. Portu kullanır.

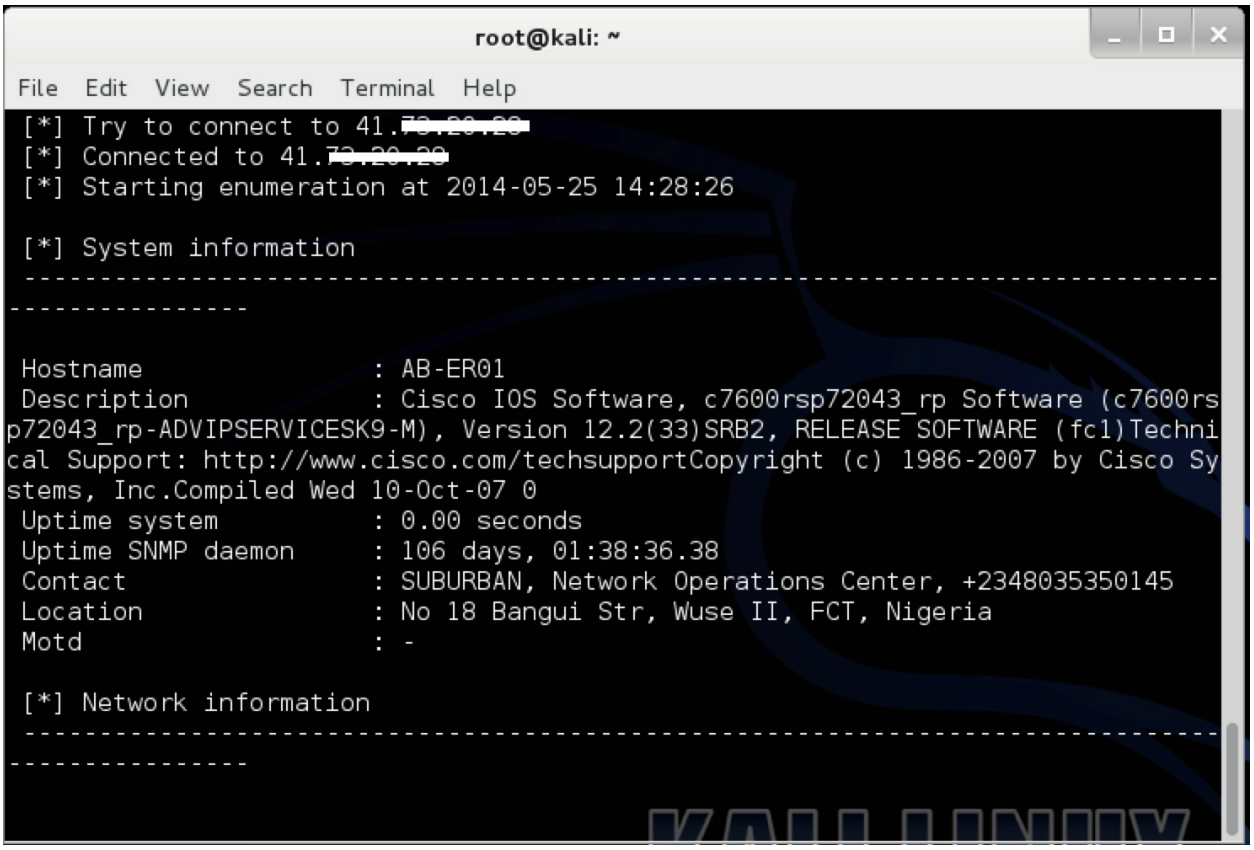
FTP

File Transfer protocol (dosya aktarım protokolü) dosyaların aktarımını sağlar. FTP 20 ve 21 numaralı TCP portlarını kullanır.

SNMP

Basit ağ yönetim protokolü (Simple Network Management Protocol) ağdaki cihazların durumunu kontrol eden ve bunları merkeze bildiren bir protokoldür. Ağ cihazları hakkında çeşitli bilgileri merkeze aktarır UDP 161. Portu kullanır.

(SNMP Enumeration)



SMTP

Simple Mail Transfer Protokol mail transferlerini sağlayan protokoldür. TCP 25. Portu kullanır. IMAP ve POP3 protokolleri de benzer işlevlere sahiptir.

SSH

Secure shell uzaktaki bir makineye bağlantı kurulmasını ve cihaz üzerinde komut çalıştırılmasını sağlayan protokoldür. Bağlantıyı şifreli kurarak Güvenlik sağlar. TCP 22. Portu kullanır.

Telnet

Uzaktaki bir makineye bağlantı kurulmasını ve cihaz üzerinde komut çalıştırılmasını sağlayan protokoldür. Veri iletişimi açık haldedir, şifresizdir. Güvenli değildir.

RDP

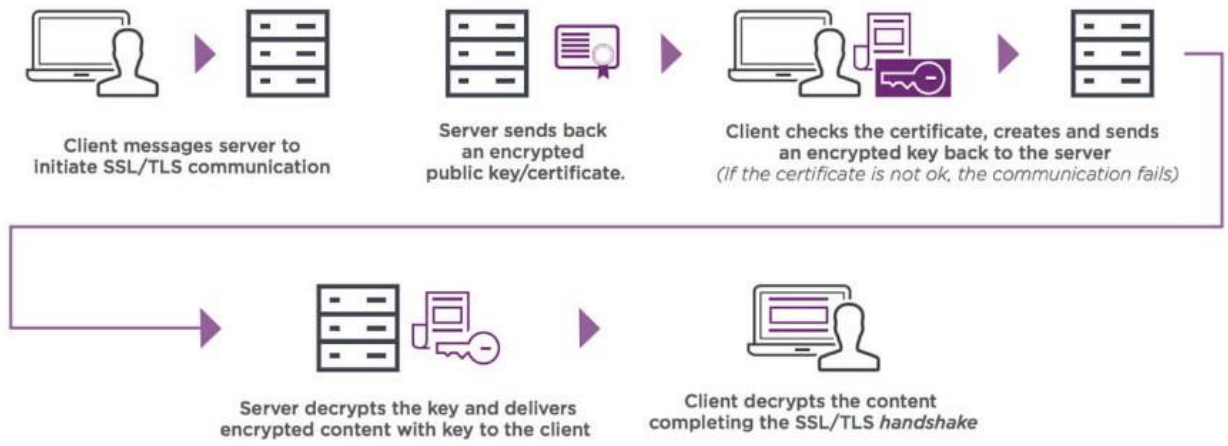
Remote Desktop Protocol, bir bilgisayarın masaüstünü uzaktan görüntülemeyi sağlar. Default olarak TCP 3389. Portu kullanır.

SQL

Struct Query Language, veri tabanı programlama dilidir. Veri tabanı sunucularına örnek olarak; MySQL ve MSSQL verilebilir. SQL sunucuları üzerinde veri tabanlarını tutarlar.

SSL

Secure Socket Layer, veri iletişiminin şifreli şekilde yapılması sağlanır. SSL sertifikaları sayesinde sitelerin adreslerinin doğruluğu kontrol edilir.



TFTP

Trivial File Transfer protocol, dosya aktarımı sağlayan bir protokoldür. UDP 69. Portu kullanır. Bağlantı için kullanıcı adı ve parola kullanılmaması ve verinin şifrelenmeden iletilmesinden dolayı TFTP ile yapılan dosya aktarımları kesinlikle güvensizdir.

Domain Nedir?

Domain, dilimizde alan adı olarak çevirilebilir. Alan adı internette yayınlanan bir web sitesinin ismidir. Örneğin; www.lostar.com.tr örneğindeki Lostar.com.tr bir alan adıdır. Alan adlarının sahip olduğu .com, .edu, .tr gibi uzantılar ise en üst seviye alan adıdır. (TLD: Top Level Domain Name). Örneğin, com ingilizce "commercial" kelimesinin kısaltmasıdır. Yani ticari siteleri ifade eden bir üst seviye alan adıdır.

DNS (Domain Name System)

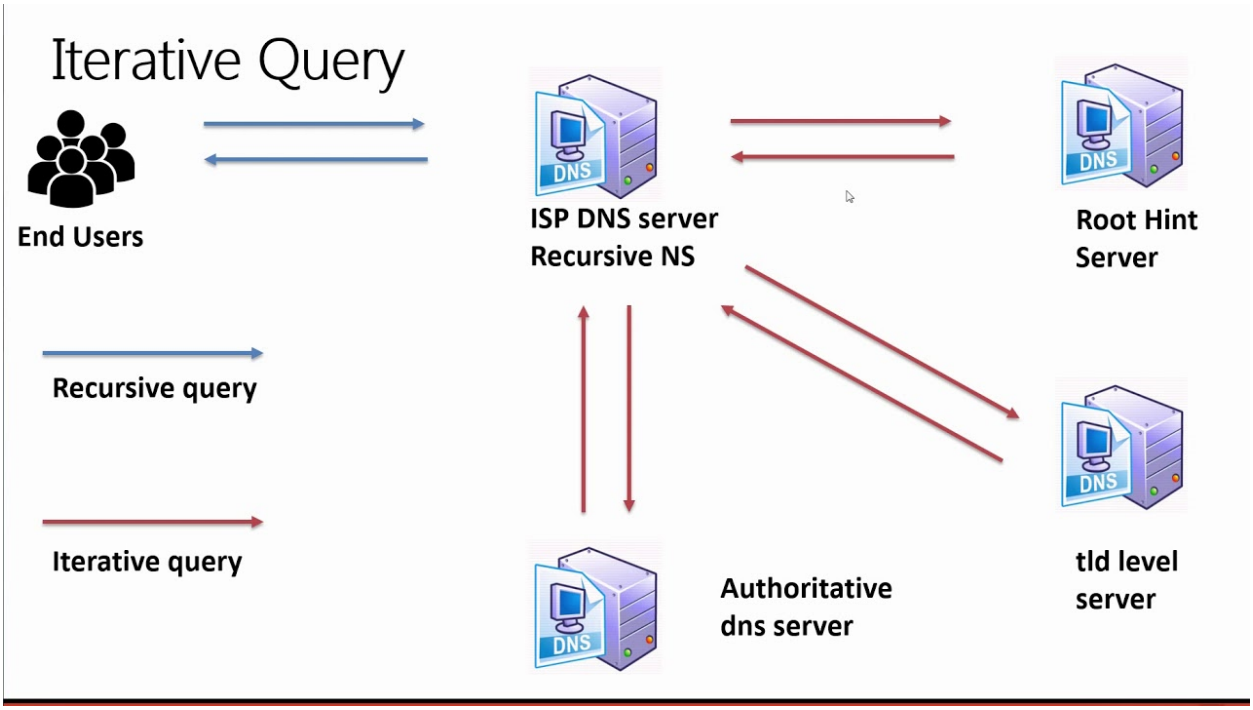
Internet üzerinde çalışan cihazların IP Adresleri ile işlem yaptıkları belirtilmişti. DNS etki alan sistemlerinden IP adresi çözümlemeye yarayan sistemdir.

Recursive Sorgular

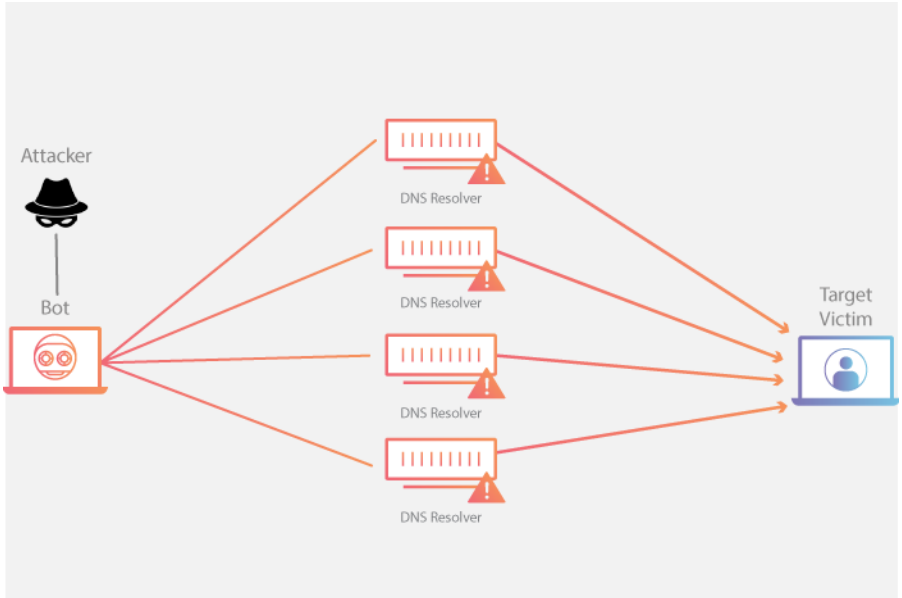
Recursive sorguda; Local DNS IP adresini bilmiyorsa diğer DNS'lerden cevabı öğrenerek cevabı verir. **Sorguya tam yanıt ya da hata mesajı döner.**

Iterative Sorgular

Iterative sorguda, genellikle DNS sunucularının birbirlerine yaptıkları no recursive sorgulardır.



(DNS Amplification)



DNS Kayıtları ve DNS Kayıt Tipleri

DNS sunucularının üzerlerinde bir takım kayıtlar tutarlar. Bu kayıtlar ve görevleri aşağıdaki tabloda verilmiştir.

DNS Kayıt Tipi	İşlevi
A	Alan adının IP adresini tutan kayıt.
MX	Alan adına ait mail sunucusunu gösteren kayıt.
NS	İlgili alan adından sorumlu dns sunucuyu gösteren kayıt.
TXT	DNS Sunucunun özelliklerini gösteren kayıt.
PTR	IP Adresine karşılık gelen alan adının tutulduğu kayıt.

DNS Zone

Bir DNS sunucu tarafından yönetilen etki alanına zone denir. Zone içerisinde ise kayıt bilgileri bulunur.

webadresim.xyz DNS Alanı Yönetimi

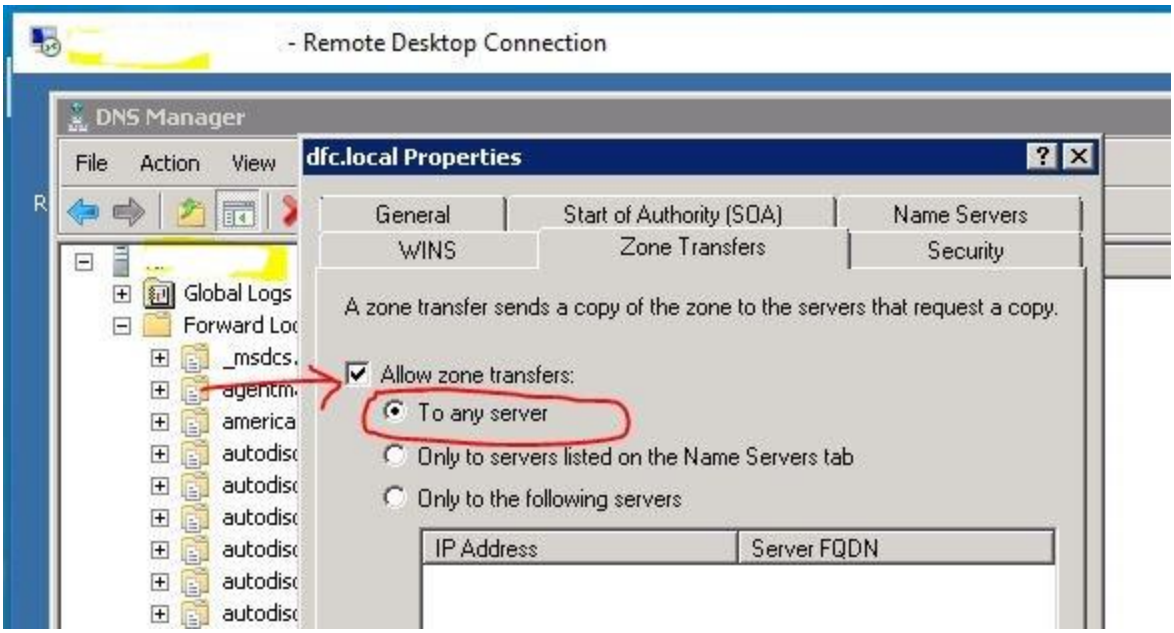
Name	Type	Value	İşlem
webadresim.xyz.	NS	p1.hosting.com.tr.	
webadresim.xyz.	NS	p2.hosting.com.tr.	
ftp	A	77.245.159.45	☐
mail	A	77.245.159.45	☐
pop	A	77.245.159.45	☐
smtp	A	77.245.159.45	☐
webadresim.xyz.	A	77.245.159.45	☐
www	A	77.245.159.45	☐
webadresim.xyz.	MX	10 mail	☐
webadresim.xyz.	TXT	"v=spf1 a mx ip4:77.245.159.45 ~all"	☐

Varsayılana Sıfırla | Sil

DNS Kaydı Ekle

Name	Type	Value	İşlem
mesela: ofis	A	mesela: 77.245.159.5	Kaydet
webadresim.xyz.	MX	10 ▾ mx1.hosting.com.tr.	Kaydet
cname.webadresim.xyz.	CNAME	mesela: ghs.google.com.	Kaydet
webadresim.xyz.	TXT	mesela: "v=spf1 a mx ip4:77.245.159.45 ~all"	Kaydet
mesela: fabrika	AAAA	mesela: FE80:1234:FCAB:0020:0A10:10DE:FCFC:F	Kaydet
Override TTL Value	TTL	○ 14400 ◉ Use Default	Kaydet

(DNS Zone Transferi)



Zone transfer konfügrasyonu doğru ayarlanmadıysa, 3. Şahıslar dns sunucusundaki tüm zone'a erişebilir.

BIND DNS Yapılandırması:

Sadece 192.168.0.3 IP adresi zone transfer izni vardır.

```
allow-transfer {192.168.0.3;};
```

Hiç bir istemci zone transferi yapamaz.

```
[important]allow-transfer {"none";};
```

Eğer hiç yapılandırma Yoksa default olarak bütün istemciler zone transfer işlemi yapabilir ve zone'a ulaşabilir.

```
; <<>> DiG 9.9.2-P1 <<>> @ns1.example.com example.com axfr
; (1 server found)
;; global options: +cmd
example.com.        3600    IN    SOA    ns1.example.com. hostmaster.example.com.
2009051396 1800 600 86400 3600
example.com.        3600    IN    A    1.1.1.201
example.com.        3600    IN    NS    ns1.example.com.
example.com.        3600    IN    NS    ns2.example.com.
example.com.        3600    IN    NS    nsp1.example.com.
example.com.        3600    IN    NS    nsp2.example.com.
example.com.        3600    IN    NS    ns4.example.com.
example.com.        3600    IN    MX    10 mail.example.com.
example.com.        3600    IN    TXT    “v=spf1 mx ptr ip4:1.1.1.1 +all”
mail.example.com.    3600    IN    A    1.1.1.1
ns1.example.com.    3600    IN    A    1.1.1.2
ns10.example.com.    3600    IN    A    213.139.193.2
ns2.example.com.    1200    IN    A    1.1.1.5
ns2.example.com.    1200    IN    AAAA    2002:5d5e:f903::5d5e:f903
ns20.example.com.    3600    IN    A    1.1.1.5
ns4.example.com.    3600    IN    A    1.1.1.22
nsp1.example.com.    3600    IN    A    1.1.1.3
nsp2.example.com.    3600    IN    A    123.123.123.123
webmail.example.com.    3600    IN    A    1.1.1.25
wiki.example.com.    3600    IN    A    1.1.1.4
wpad.example.com.    1200    IN    A    127.0.0.1
www.example.com.    3600    IN    A    1.1.1.201
example.com.        3600    IN    SOA    ns1.example.com. hostmaster.example.com.
2009051396 1800 600 86400 3600
;; Query time: 33 msec
;; SERVER: 1.1.1.2#53(1.1.1.2)
;; WHEN: Sun Jul 21 01:37:24 2013
;; XFR size: 23 records (messages 23, bytes 1308)
```

Güvenlik Duvarı (Firewall)

Güvenlik duvarı, üzerinde konumlandırılmış kurallara göre, gelen saldırı trafiğini engellemek üzere üretilmiş donanımsal, yazılımsal yapıdır. Katman 4 tabanlı çalışan Güvenlik duvarı sadece port bazlı engelleme yapabilirken, katman 7 seviyesinde çalışan Güvenlik duvarı uygulamaya yönelik denetim yaparlar.

WAF

Web Application Firewall, imzalarını web uygulamalarına göre yapılandırarak web temelli saldırıları engellemeye yönelik çalışırlar.

(SQL Injection)

https://testphp.vulnweb.com

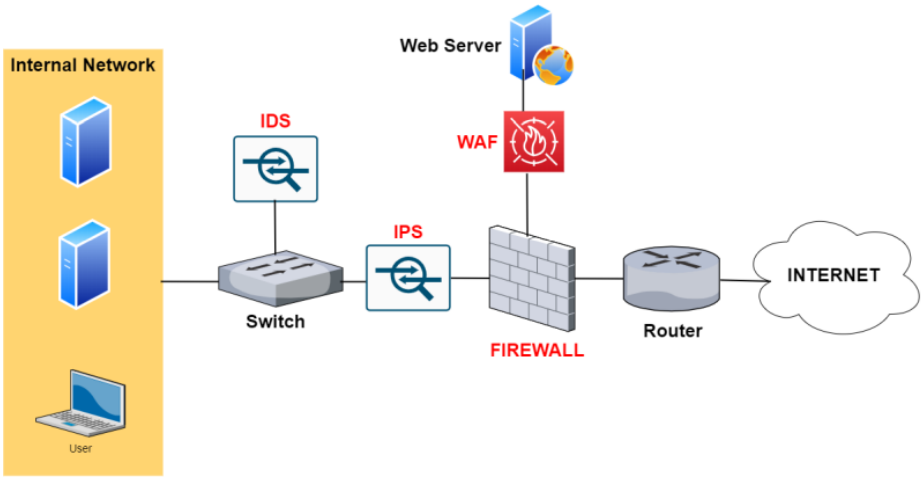
IPS

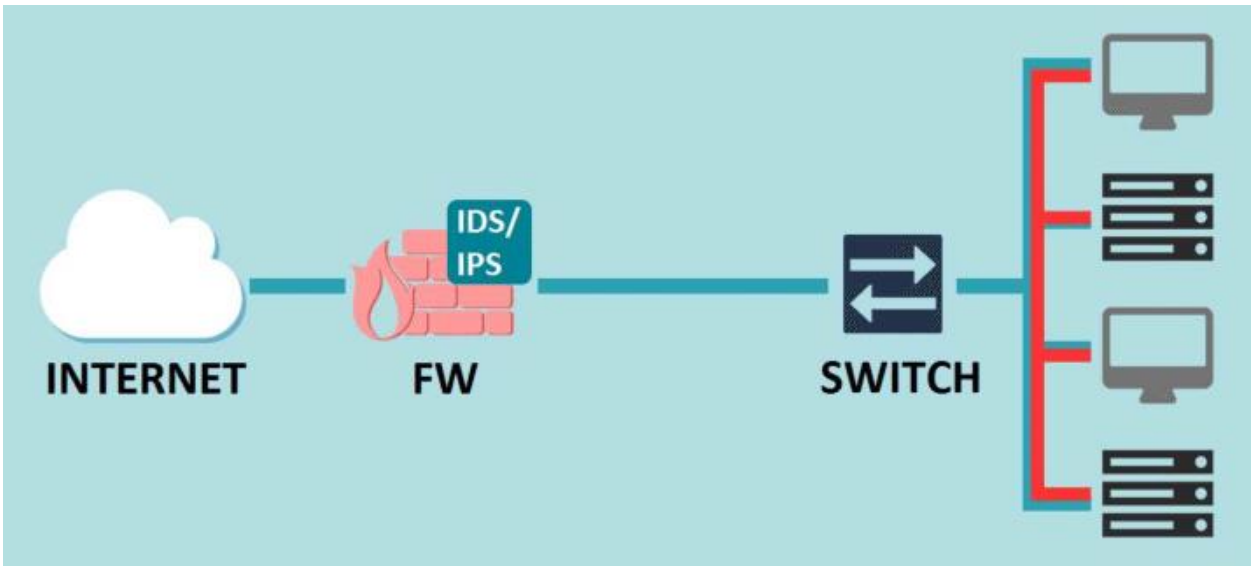
Katman 7 imzalar kullanarak uygulama seviyesinde gelen atakları analiz eder ve durdurur.

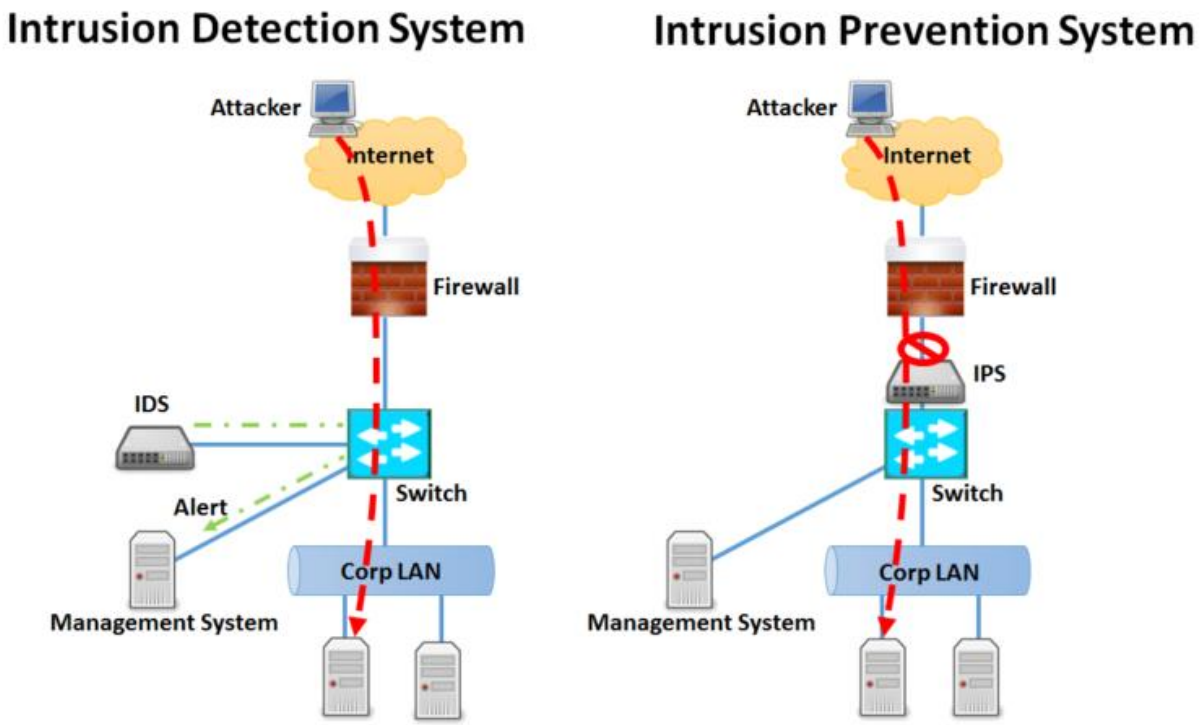
IDS

Intrusion Detection System, zararlı trafiği analiz eder ve LOG tutar.

IDS/IPS Topoloji







Network Scanning & Detection Evasion

Bilgi toplama safhasında, ağdaki bilgisayarların IP adresleri, ağın topolojisi, bilgisayarlar üzerindeki açık portların bulunması, bilgisayarlar üzerinde çalışan işletim sistemleri ve versiyonları, portlar üzerinde çalışan servislerin versiyonları, sistemler üzerindeki zafiyet taramaları yapılabilir.

Ağdaki Hostların Keşfi

Nmap (ICMP & ARP)

TCP Taraması

Nmap (-sT)

SYN Taraması

Nmap (-sS)

UDP Taraması

Nmap (-sU)

XMass Taraması

Hedef porta FIN,URG ve PUSH flagli paketler gönderilir. RST dönmemesi beklenir.

İşletim Sistemi Tespiti

Nmap (-O)

Servis ve Versiyon Tespiti

Nmap (-sV)

Zafiyet Taraması

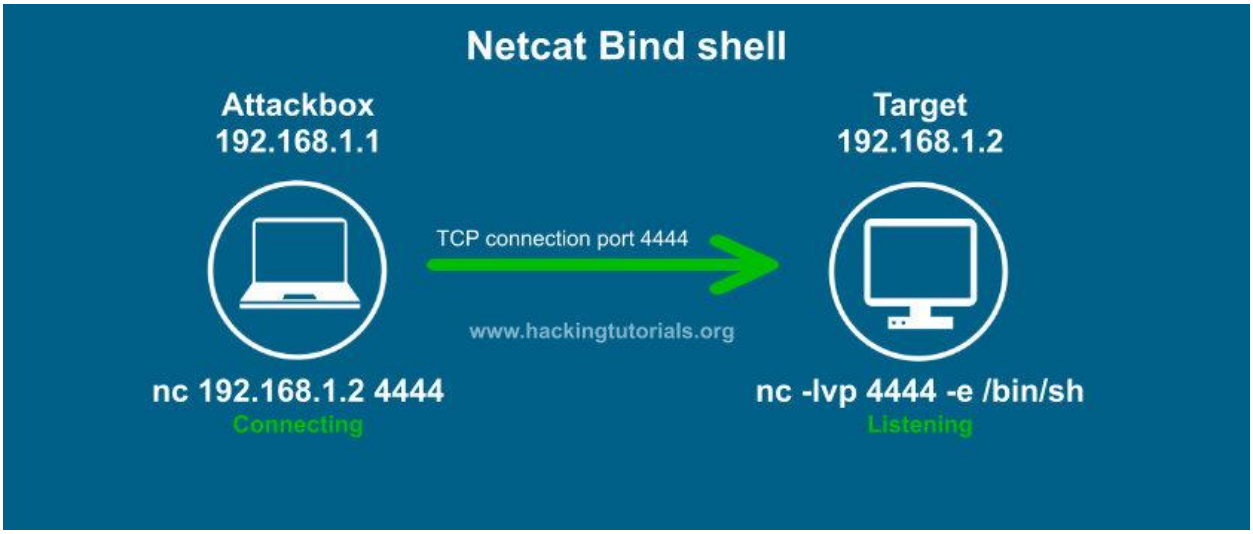
Nmap (--script)

Soket Bağlantı Türleri

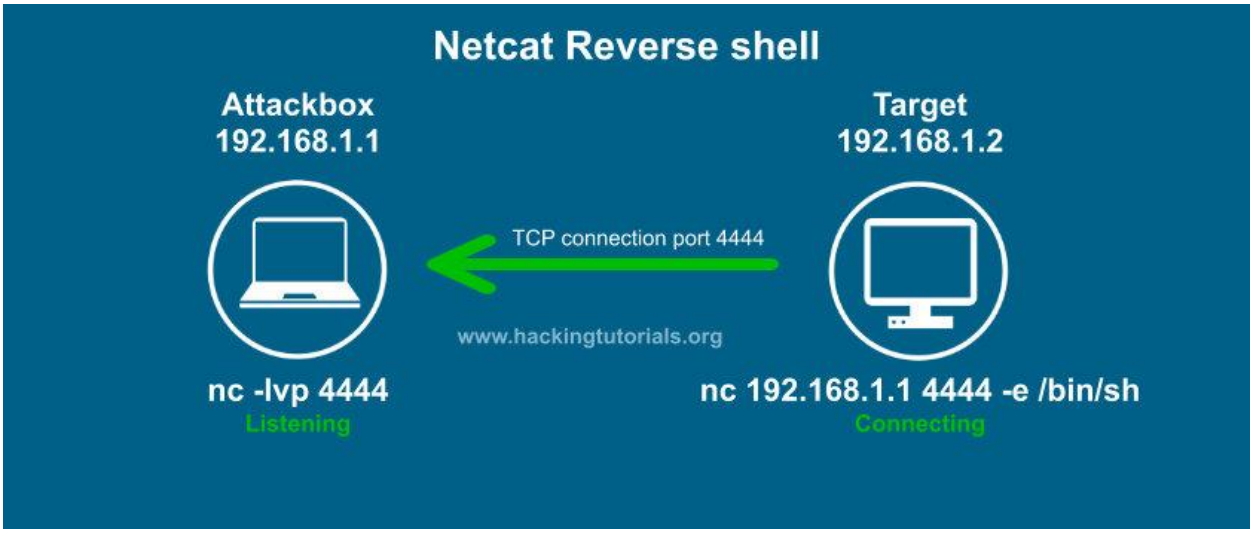
BIND Shell Kavramı

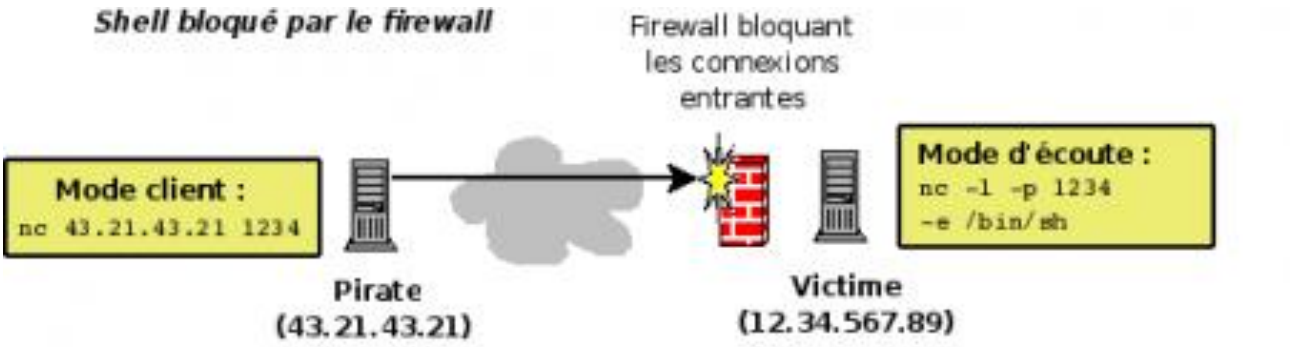
NC

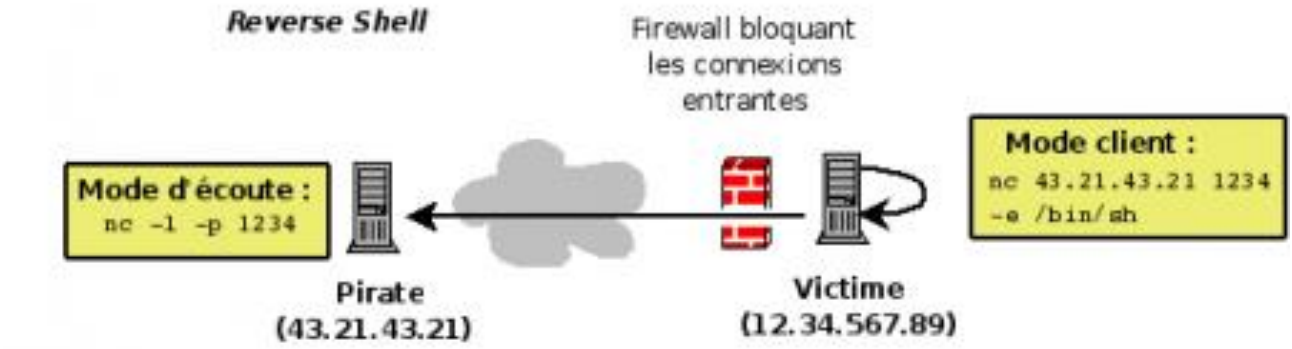
Netcat aracı ile ağdan veri göndermek, port tarama yapmak, tersine kanal açmak, uzaktan komut çalıştırmak, arka kapı bırakmak, dosya transfer etmek için kullanılan bir araçtır.



Reverse Shell Kavramı







(Wireshark)
(SBD)

Tünelleme Teknikleri

Bazı durumlarda dosya paylaşımları için gerekli ortamlar (web sunucu, TFTP, FTP vb.) kurulmuş olsa dahi güvenlik cihazları ağ trafiğini engellemektedir. Bu kimi zaman port bazlı kimi zaman imza bazlı yapılabilmektedir. Konfigürasyon hatalarından, personelin yeterli bilgi düzeyine sahip olmaması gibi nedenlerden ötürü tünelleme teknikleri kullanılarak Güvenlik cihazları atlatılabilmektedir. Güvenlik duvarı ve saldırı tespit sistemlerinin tünelleme yöntemleri ile test edilerek eğer tünelleme yapılabiliyorsa, tünellemenin yapıldığı zayıf noktalara katman 7 imzaları yazılarak bu tarz saldırılar engellenmelidir.

SSH Tunelleme

(ssh)

ICMP Tunelleme

(ptunnel-ng)