

## 03 - Tarama

### BGM 531 - Sızma Testleri ve Güvenlik Denetlemeleri

Bilgi Güvenliği Mühendisliği  
Yüksek Lisans Programı

**Dr. Ferhat Özgür Çatak**  
[ozgur.catak@tubitak.gov.tr](mailto:ozgur.catak@tubitak.gov.tr)

İstanbul Şehir Üniversitesi  
2018 - Güz

# İçindekiler

## 1 Tarama

- Giriş

## 2 Network Tracing

- IPv4 Başlığı ve TTL Alanı
- Keşif Türleri
- Pasif Keşif
- Aktif Keşif
- Ping Sweep
- Angry IP Scanner
- TCP Flag Tipleri
- Nmap

## 3 Nmap Taraması

- Nmap Ping Taraması
- Nmap Port Taraması

## • Nmap Kullanılabilirlik Özellikleri

## • Uygulama

## 4 Servis, Versiyon ve OS Tespiti

- İşletim Sistemi Tespiti
- Servis ve Versiyon Tespiti
- Girdi - Çıktı Yönetimi
- Uygulama

## 5 NMAP Betik Taraması

- Betik Taraması

## 6 Zamanlama, IPS/IDS Atlatma

- Zamanlama
- IPS/IDS Atlatma

## 7 Tarama İpuçları

- IP Adresi Kullanarak Tarama
- Büyük Ağlarda Tarama

# İçindekiler

1

## Tarama

- Giriş

2

## Network Tracing

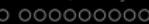
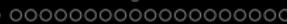
- IPv4 Başlığı ve TTL Alanı
- Keşif Türleri
- Pasif Keşif
- Aktif Keşif
- Ping Sweep
- Angry IP Scanner
- TCP Flag Tipleri
- Nmap

3

## Nmap Taraması

- Nmap Ping Taraması
- Nmap Port Taraması

- Nmap Kullanılabilirlik Özellikleri
- Uygulama
- Servis, Versiyon ve OS Tespiti
- İşletim Sistemi Tespiti
- Servis ve Versiyon Tespiti
- Girdi - Çıktı Yönetimi
- Uygulama
- NMAP Betik Taraması
- Betik Taraması
- Zamanlama, IPS/IDS Atlatma
- Zamanlama
- IPS/IDS Atlatma
- Tarama İpuçları
- IP Adresi Kullanarak Tarama
- Büyük Ağlarda Tarama



# Tarama I

## Taramanın amaçları

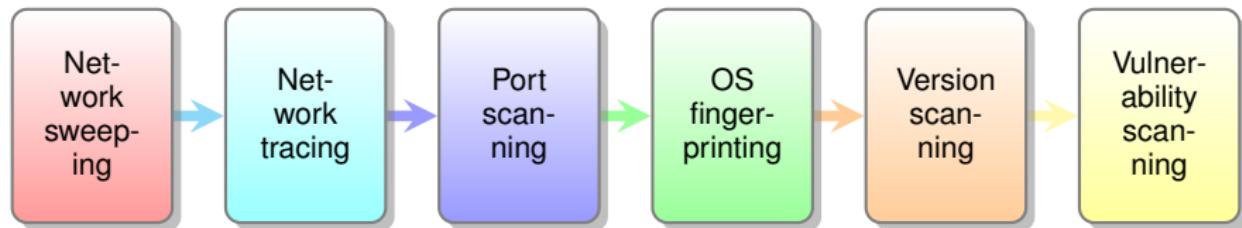
- ▶ **Genel hedef:** Hedef ortam hakkında daha fazla bilgi edinme ve hedef ortamla etkileşime girerek açıklıklar bulunması.
  - ▶ Ağ içinde yer alan hosts, firewalls, routers gibi bileşenlerin ağ adreslerinin belirlenmesi
  - ▶ Hedef ortamın ağ topolojisinin elde edilmesi
  - ▶ Keşfedilen bilgisayarların işletim sistemi türlerini belirleme
  - ▶ Hedef ortamda bulunan açık portların ve ağ hizmetlerinin belirlenmesi
  - ▶ Potansiyel zayıflık listesinin belirlenmesi
  - ▶ *Bunları, ana makine veya hizmete zarar verme riskini en aza indirecek şekilde yapılması.*



Tarama II

### Tarama Tipleri

- ▶ **Network sweeping:** Hedef ağdaki IP adreslerindeki canlı sistemleri tanımlamak için bir dizi paketin gönderimi
  - ▶ **Network tracing:** Ağ topolojisinin belirlenmesi ve bir harita çizimi
  - ▶ **Port scanning:** Hedef sisteme yer alan açık TCP ve UDP portlarının belirlenmesi
  - ▶ **OS fingerprinting:** Ağ davranışına göre hedef işletim sistemi türünü belirleme
  - ▶ **Version scanning:** Açık TCP ve UDP bağlantı noktalarının çalıştırıldığı hizmetlerin ve protokollerin sürümünü belirleme
  - ▶ **Vulnerability scanning:** Hedef ortamındaki olası güvenlik açıklarının (yanlış yapılandırmalar, unpatched services vb.) Bir listesini belirleme





Tarama V

### Ağ Tarama (Network Scanning)

- ▶ Ağ içerisinde yer alan aktif olarak çalışan sunucuların tespit edilmesi.
  - ▶ **Zafiyet Taraması (Vulnerability Scanning):** Ağ üzerinde yer alan bilgisayarlarda bilinen zafiyetlerin tespit edilmesi işlemi.

# İçindekiler

- 1 Tarama
  - Giriş

## 2 Network Tracing

- IPv4 Başlığı ve TTL Alanı
- Keşif Türleri
- Pasif Keşif
- Aktif Keşif
- Ping Sweep
- Angry IP Scanner
- TCP Flag Tipleri
- Nmap

## 3 Nmap Taraması

- Nmap Ping Taraması
- Nmap Port Taraması

## ● Nmap Kullanılabilirlik Özellikleri

- Uygulama

## 4 Servis, Versiyon ve OS Tespiti

- İşletim Sistemi Tespiti
- Servis ve Versiyon Tespiti
- Girdi - Çıktı Yönetimi
- Uygulama

## 5 NMAP Betik Taraması

- Betik Taraması

## 6 Zamanlama, IPS/IDS Atlatma

- Zamanlama
- IPS/IDS Atlatma

## 7 Tarama İpuçları

- IP Adresi Kullanarak Tarama
- Büyük Ağlarda Tarama

oooooooooooo●●oooooooooooooooooooo

oooooooooooooooooooo

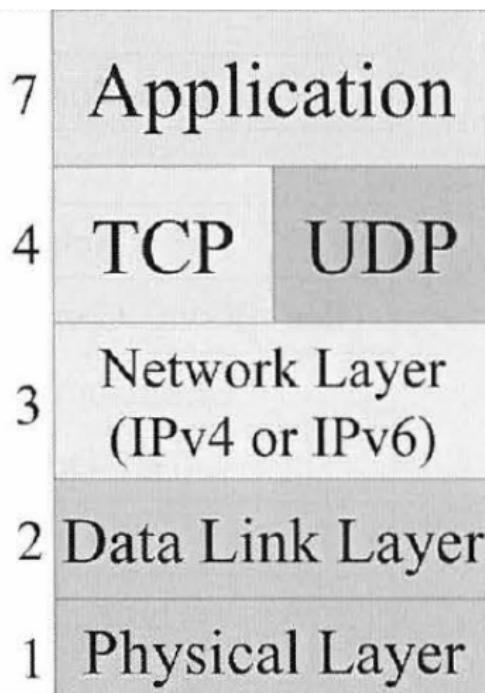
oooooooooooo

oooooooooooo

oooo

## IPv4 Başlığı ve TTL Alanı I

- ▶ Internet üzerinde yer alan servisler TCP veya UDP şeklindedir.
- ▶ Farklı özellikleri vardır. Bu sebeple taramayı etkilemektedir.
- ▶ **TCP:** Connection-oriented, tries to preserve sequence, retransmits lost packets
- ▶ **UDP:** Connectionless, no attempt made for reliable delivery



oooooooooooo●●oooooooooooooooooooo

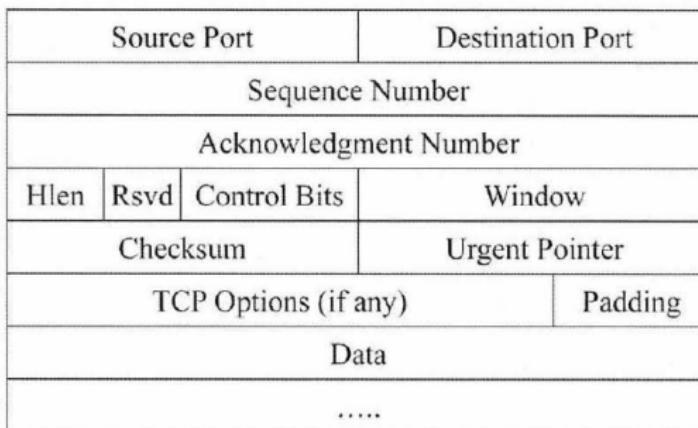
oooooooooooooooooooooooooooo

oooooooooooo

oooooooooooo

oooo

## IPv4 Başlığı ve TTL Alanı II



**Şekil:** TCP Başlığı

- ▶ *Source Port, Destination Port:* each is 16-bits in length.
- ▶ The TCP Control Bits, which are incredibly important for tracking the state of a given TCP connection.

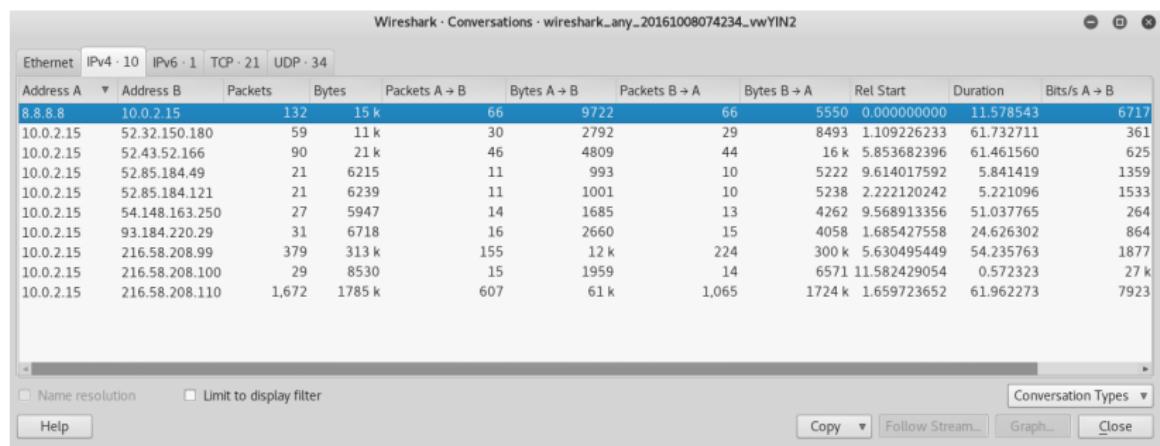
# Keşif Türleri

## Keşif Türleri

- ▶ **Pasif Keşif:** Ağ altyapısına ve sunuculara bir paket gönderimi yoktur. Ağ trafiği dinlenerek yapılır.
  - ▶ Ağın dinlenmesi
    - ▶ Tcpdump
    - ▶ Wireshark
  - ▶ ARP tablosu
- ▶ **Aktif Keşif:** Hedef sunucuların tespiti için paket gönderilir.
  - ▶ Nmap
  - ▶ Hping
  - ▶ Scapy
  - ▶ Ping, traceroute

# WireShark

- ▶ Ağ trafiğini dinlemek için kullanılan araç.
- ▶ Trafiği dinleme ve kaydetme özelliklerine sahip.
- ▶ Filtreleme ve inceleme



**Şekil:** Pasif keşif aracı: Wireshark

## ARP Tablosu

- Aynı ağ içinde bulunan diğer bilgisayarlara ait IP, mac adresi bilgileri bulunmaktadır.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# arp -a
gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on eth0
root@kali:~# arp
Address          HWtype  HWaddress           Flags Mask   Iface
gateway          ether    52:54:00:12:35:02 C        eth0
root@kali:~#
```

Şekil: Pasif keşif aracı: ARP

# Aktif Keşif

## Aktif Keşif

- ▶ Saldırgan aktif olarak ağa paketler gönderir.
  - ▶ Angry IP
  - ▶ nmap
  - ▶ hping
  - ▶ Scapy
  - ▶ nessus
- ▶ Bu eğitim kapsamında kullanılacak olan araç: **nmap**

# Ping Sweep I

## Ping Sweep

- ▶ IP adres bloğu üzerinde *ping sweep* işlemi ile canlı sistemlerin bulunması.
- ▶ Ağ üzerinde yer alan bilgisayarlardan ping cevabı alınması durumunda çalışır olduğu kabul edilir.
- ▶ Internet Control Message Protocol (ICMP) taramasında denilmektedir.
- ▶ *ping* komutu ICMP protokolu kullanır.
- ▶ **Internet Control Message Protocol:** Hataları raporlamak için kullanılan, kontrol amaçlı bir protokoldür. Bu şekilde normal kullanımının yanında, uzak sistem hakkında bilgi toplamak için sıkça kullanıldığından çok önemlidir.

## Ping Sweep II

```
C:\Windows\system32\cmd.exe
C:\Users\t>ping www.microsoft.com
Pinging e2847.dspb.akamaiedge.net [104.108.58.188] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 104.108.58.188:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\t>_
```

Şekil: Windows ping komutu

- ping'e karşılık uzak sistem kapalı, cevap vermiyor veya ping bloklandı.

# Angry IP Scanner I

## Angry IP Scanner

- ▶ Angry IP Scanner, verilen bir aralıkta yer alan IP adreslerini taramaktadır.
- ▶ ICMP kullanmaktadır. Her bir adrese **ping** işlemi gerçekleştirmektedir.
- ▶ NetBIOS bilgisini elde edebilir (computer name, workgroup name, and currently logged in Windows user)
- ▶ Tarama sonuçları CSV, TXT, XML gibi formatlarda kayıt altına alınabilmektedir.
- ▶ Temel ağ arama aracıdır.
- ▶ Plugin geliştirilebilir. Java dili ile uygulama yazılabılır.
- ▶ Multi-thread. Her bir IP adresi için ayrı thread oluşturularak hızlı bir şekilde sonuç alınabilmektedir.

oooooooooooo●●●●oooooooooooooooooooo

oooooooooooooooooooooooooooo

oooooooooooo

oooooooooooo

oooo

# Angry IP Scanner II

IP Range - Angry IP Scanner

Scan Go to Commands Favorites Tools Help

IP Range: 192.168.4.175 to 192.168.4.175 IP Range ▾

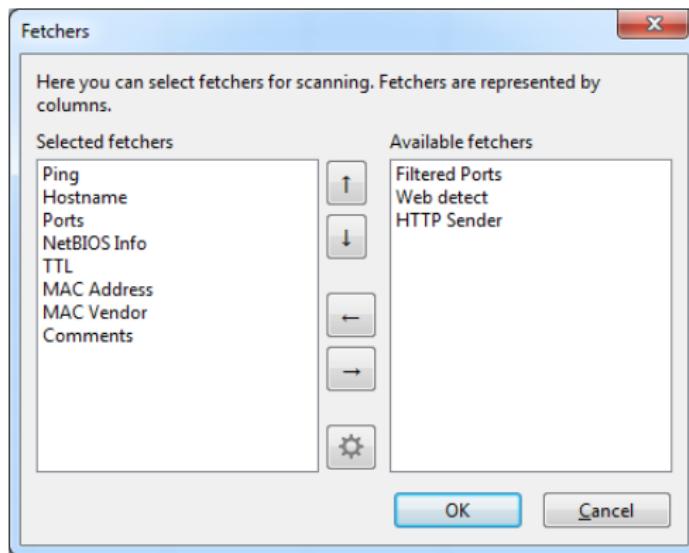
Hostname: work IP↑ Netmask ▾

IP	Ping	Hostname	Ports [0+]
192.168.4.175	1 ms	MalwAn	[n/s]

Ready Display: All Threads: 0



Angry IP Scanner III



oooooooooooo●●●●oooooooooooooooooooooooooooo

# Angry IP Scanner IV

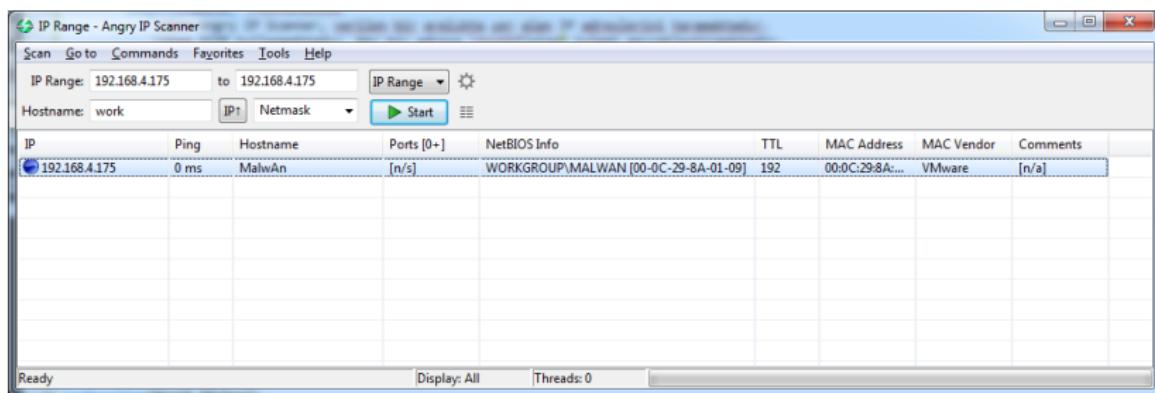
IP Range - Angry IP Scanner

Scan Go to Commands Favorites Tools Help

IP Range: 192.168.4.175 to 192.168.4.175 IP Range Hostname: work IP! Netmask Start

IP	Ping	Hostname	Ports [0+]	NetBIOS Info	TTL	MAC Address	MAC Vendor	Comments
192.168.4.175	0 ms	Malwan	[n/s]	WORKGROUP\MALWAN [00-0C-29-8A-01-09]	192	00:0C:29:8A:...	VMware	[n/a]

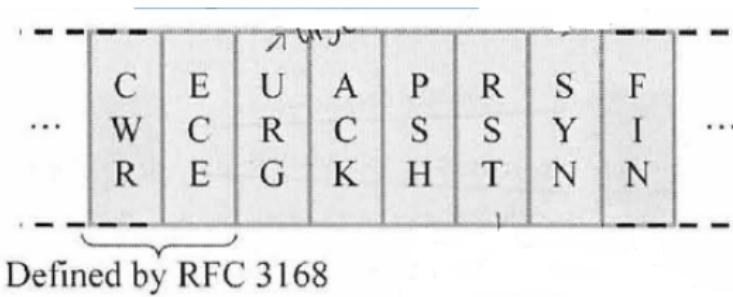
Ready Display: All Threads: 0



# TCP Flag Tipleri I

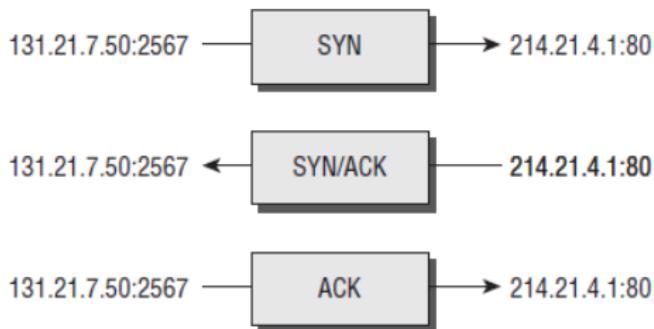
## TCP Flags

- ▶ **SYN** Synchronize. Initiates a connection between hosts.
- ▶ **ACK** Acknowledge. Established connection between hosts.
- ▶ **PSH** Push. System is forwarding buffered data.
- ▶ **URG** Urgent. Data in packets must be processed quickly.
- ▶ **FIN** Finish. No more transmissions.
- ▶ **RST** Reset. Resets the connection.



## TCP Flag Tipleri II

- ▶ *TCP three-way handshake* kullanılarak TCP taramaları yapılır. İki bilgisayar arasında başarılı bağlantı için three-way handshake yapılır.
  - ▶ Gönderici (Sender), SYN bit'i set edilmiş bir TCP paketi gönderir.
  - ▶ Alıcı (Receiver), SYN ve ACK bitleri set edilmiş TCP paketi gönderir.
  - ▶ Gönderici, ACK bit'i set edilmiş son bir TCP paketi gönderir.



**Şekil:** TCP three-way handshake

# Nmap I

## Nmap

Nmap, açık kaynak kodlu ağ keşif ve tarama aracıdır.

<http://www.nmap.org>

- ▶ Ping sweeps
- ▶ IP address detection
- ▶ port scanning
- ▶ operating system detection
- ▶ service identification
- ▶ Unix, Linux, Windows

## Nmap uygulamaları

- ▶ **Zenmap:** Nmap kullanıcı arayüzü
- ▶ **Ndiff:** Tarama sonuçlarını kıyaslama aracı. 2 Farklı nmap XML çıktısı arasında bulunan farklar
- ▶ **Nping:** Paket üreticisi ve gelen cevabın analizi aracı
- ▶ **Ncrack:** Kaba kuvvet saldırısı aracı

# Nmap II

Table: NMap tarama türleri

NMap Tarama	Açıklama
TCP connect	Hedef sistemle TCP bağlantısı. Doğruluğu yüksek fakat en farkedilir tarama. Açık portlar SYN/ACK, kapalı portlar RST/ACK
XMAS tree scan	XMAS-tree paketleri ile TCP servislerin kontrol edilmesidir. <b>PSH, URG</b> ve <b>FIN</b> . RFC793'e göre kapalı bir porta standart dışı paket gönderiminde cevap olarak <b>RST</b> gelir. Saldırgan kapalı portları bulmaya çalışmaktadır.
SYN stealth scan	<i>half-open</i> tarama. SYN paketi gönderilir, SYN-ACK bilgisi sunucudan alınır.
Null scan	Firewall tarafından algılanmama ihtimali olan, bütün flag'lerin kapalı olduğu tarama. Sadece Unix sistemlerde çalışır. Firewall üzerinde sadece belirli flaglere göre kural olması durumunda buradan geçme ihtimali vardır. Kapalı portlar için <b>RST</b> gelir.
ACK scan	Port'a gelen cevap unreachable olması durumunda filtered olarak kabul edilir. Amaç portların açık kapalı olması değil, firewall kuralları veya ACL (Access Control List) hakkında bilgi edinmektedir. Filtre olmayan sistemde <i>open</i> ve <i>closed</i> portlar için <b>RST</b> gelecektir. Bu durumda sisteme erişim vardır (Engel yok).

## Nmap III

## Nmap Parametreleri

- ▶ **-sT TCP connect scan**
  - ▶ **-sS SYN scan**
  - ▶ **-sF FIN scan**
  - ▶ **-sX XMAS tree scan**
  - ▶ **-sN Null scan**
  - ▶ **-sP Ping scan**
  - ▶ **-sU UDP scan**
  - ▶ **-sO Protocol scan**
  - ▶ **-sA ACK scan**
  - ▶ **-sW Windows scan**
  - ▶ **-sR RPC scan**
  - ▶ **-sL List/DNS scan**
  - ▶ **-sI Idle scan**
  - ▶ **-Po Don't ping**
  - ▶ **-PT TCP ping**
  - ▶ **-PS SYN ping**
  - ▶ **-PI ICMP ping**
  - ▶ **-PB TCP and ICMP ping**
  - ▶ **-PB ICMP timestamp**
  - ▶ **-PM ICMP netmask**
  - ▶ **-oN Normal output**
  - ▶ **-oX XML output**
  - ▶ **-oG Greppable output**
  - ▶ **-oA All output**
  - ▶ **-T Paranoid Serial scan; 300 sec between scans**
  - ▶ **-T Sneaky Serial scan; 15 sec between scans**
  - ▶ **-T Polite Serial scan; .4 sec between scans**
  - ▶ **-T Normal Parallel scan**
  - ▶ **-T Aggressive Parallel scan, 300 sec timeout, and 1.25 sec/probe**
  - ▶ **-T Insane Parallel scan, 75 sec timeout, and .3 sec/probe**

# Nmap IV

## Özellikleri

- ▶ NSE (Nmap scripting engine) kullanarak scriptler kullanılabilir veya yazılabılır.
- ▶ Wildcards destekler. 192.168.1.0/24. Üç octet iptal edilmiş - 192.168.1.1 - 192.168.1.255
- ▶ Ping dışında diğer tarama tipleri için özel paketler oluşturulması sebebiyle Root/Administrator yetkileri ister.

## Uygulama

- ▶ Nmap SYN taraması
- ▶ Açık Kapalı port cevapları
- ▶ Wireshark üzerinde izleme

# İçindekiler

1

- Tarama
  - Giriş

2

- Network Tracing
  - IPv4 Başlığı ve TTL Alanı
  - Keşif Türleri
  - Pasif Keşif
  - Aktif Keşif
  - Ping Sweep
  - Angry IP Scanner
  - TCP Flag Tipleri
  - Nmap

3

- Nmap Taraması
  - Nmap Ping Taraması
  - Nmap Port Taraması

- Nmap Kullanılabilirlik Özellikleri
- Uygulama

4

- Servis, Versiyon ve OS Tespiti
  - İşletim Sistemi Tespiti
  - Servis ve Versiyon Tespiti
  - Girdi - Çıktı Yönetimi
  - Uygulama

5

- NMAP Betik Taraması
  - Betik Taraması

6

- Zamanlama, IPS/IDS Atlatma
  - Zamanlama
  - IPS/IDS Atlatma

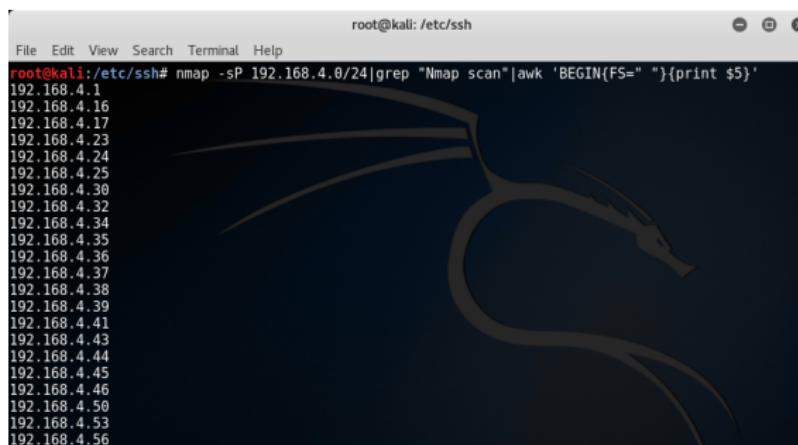
7

- Tarama İpuçları
  - IP Adresi Kullanarak Tarama
  - Büyük Ağlarda Tarama

# Nmap Ping Taraması

Açık sunucuların tespit edilmesi için yapılmaktadır.

- ▶ *nmap -sP 192.168.4.0/24* (ping scan)
  - ▶ ICMP echo request
  - ▶ TCP 443 portuna SYN
  - ▶ TCP 80 portuna ACK
  - ▶ ICMP timestamp request
- ▶ "-PN" parametresi kullanılırsa sunucu keşfi gerçekleşmez.



The screenshot shows a terminal window titled "root@kali: /etc/ssh". The command entered is "nmap -sP 192.168.4.0/24|grep "Nmap scan"|awk 'BEGIN{FS= " "}{print \$5}'". The output lists 56 IP addresses from 192.168.4.1 to 192.168.4.56, each preceded by a short horizontal line.

```
root@kali: /etc/ssh# nmap -sP 192.168.4.0/24|grep "Nmap scan"|awk 'BEGIN{FS= " "}{print $5}'\n192.168.4.1\n192.168.4.16\n192.168.4.17\n192.168.4.23\n192.168.4.24\n192.168.4.25\n192.168.4.30\n192.168.4.32\n192.168.4.34\n192.168.4.35\n192.168.4.36\n192.168.4.37\n192.168.4.38\n192.168.4.39\n192.168.4.41\n192.168.4.43\n192.168.4.44\n192.168.4.45\n192.168.4.46\n192.168.4.50\n192.168.4.53\n192.168.4.56
```

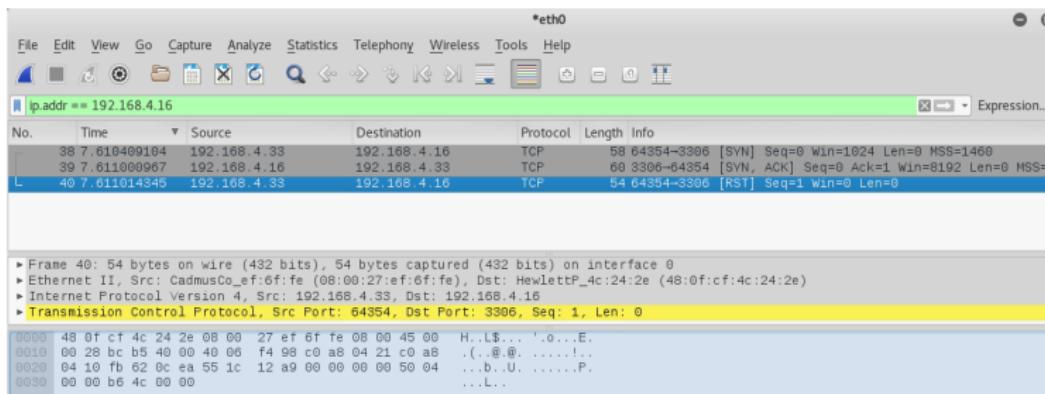
**Şekil:** Nmap ping taraması

# Nmap SYN Taraması

```

root@kali:/etc/ssh# nmap -sS 192.168.4.16 -p3306
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-10-10 14:25 EEST
Nmap scan report for 192.168.4.16
Host is up (0.00054s latency).
PORT      STATE SERVICE
3306/tcp  open  mysql
MAC Address: 48:0F:CF:4C:24:2E (Hewlett Packard)
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
root@kali:/etc/ssh#
  
```

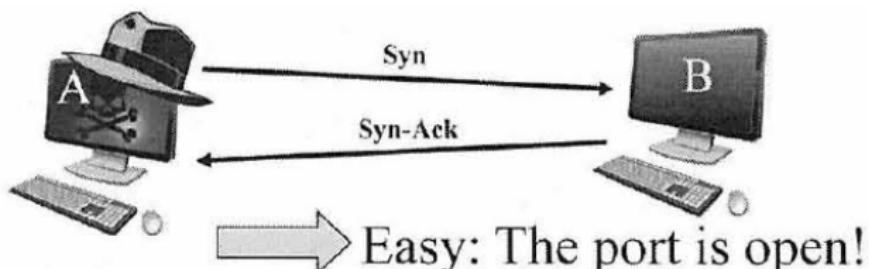
**Şekil:** Nmap port taraması



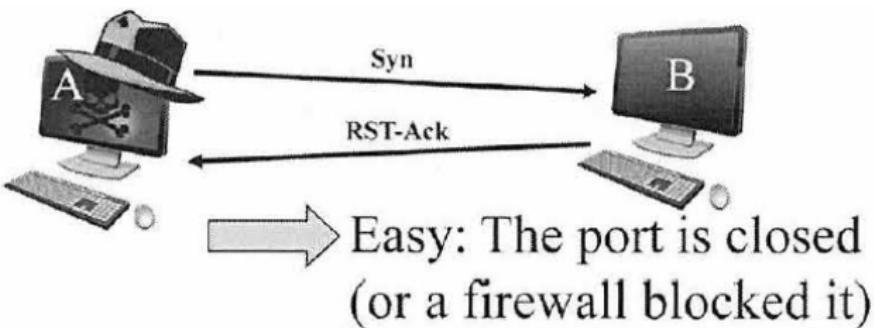
**Şekil:** wireshark paket filtreleme

# SYN Taraması I

Case T1:  
SYN in  
SYN-Ack back

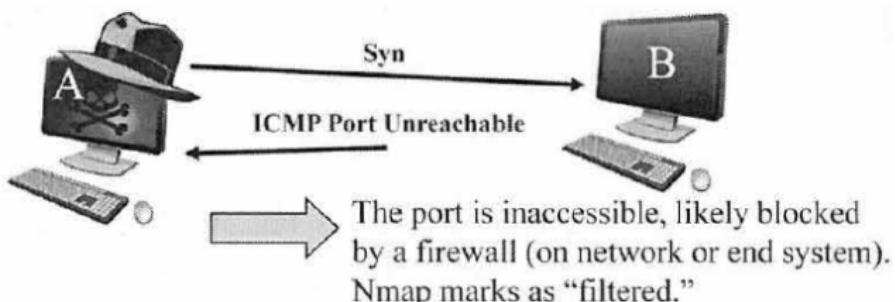


Case T2:  
SYN in  
RST-Ack back

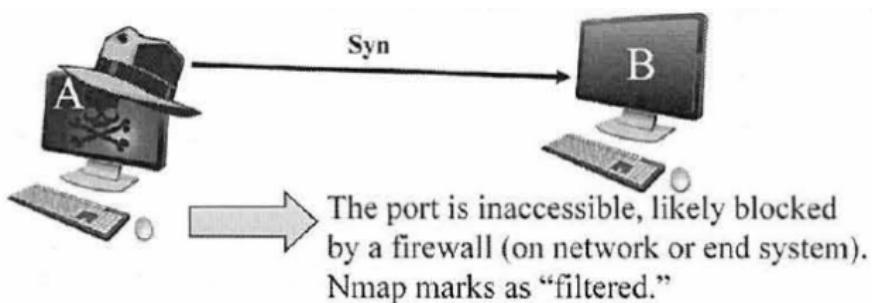


## SYN Taraması II

Case T3:  
SYN in  
ICMP Port  
Unreachable back



Case T4:  
SYN in  
Nothing back



oooooooooooooooooooooooo

oooooooo●oooooooooooo

oooooooooooo

oooooooooooo

oooo

# Port Durumları

## ▶ open

- ▶ Porta erişim var.
- ▶ Bir servis dinliyor.

## ▶ closed

- ▶ Porta erişim var.
- ▶ Güvenlik duvarı trafiği filtrelemiyor
- ▶ Port üzerinde dinleyen bir servis yok

- ▶ Örnek: Sunucu RST içeren paket dönmüş

## ▶ filtered

- ▶ Cevap alınamamış
- ▶ Güvenlik duvarı trafiği filtrelemiştir
- ▶ Port açık veya kapalı olabilir

oooooooooooooooooooooooooooo ●oooooooooooooooooooo oooooooo

## Port Taraması

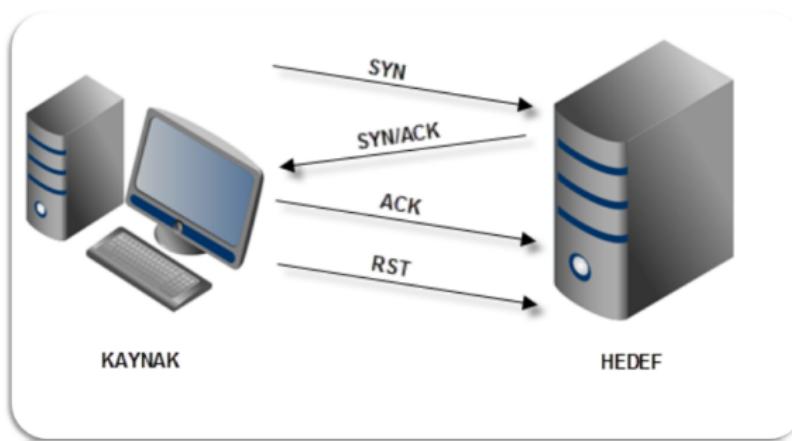
- ▶ En sık kullanılan 1000 port
- ▶ -p80,443,445-447
- ▶ -sU -sT -p U:53,T:21-25,80
- ▶ --top-ports 10
- ▶ -F Scan 100 most common ports (Fast)
- ▶ Tüm portlar: -p1-65535

```
root@kali:/etc/ssh
File Edit View Search Terminal Help
root@kali:/etc/ssh# nmap -sS --reason 192.168.4.35 --top-ports 10
[...]
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-10-11 09:33 EEST
Nmap scan report for 192.168.4.35
Host is up, received arp-response (0.00022s latency).
PORT      STATE     SERVICE      REASON
21/tcp    filtered  ftp          no-response
22/tcp    filtered  ssh          no-response
23/tcp    filtered  telnet      no-response
25/tcp    filtered  smtp         no-response
80/tcp    filtered  http         no-response
110/tcp   filtered  pop3        no-response
139/tcp   filtered  netbios-ssn no-response
443/tcp   filtered  https       no-response
445/tcp   filtered  microsoft-ds no-response
3389/tcp  open       ms-wbt-server syn-ack ttl 128
MAC Address: E8:39:35:34:E6:44 (Hewlett Packard)

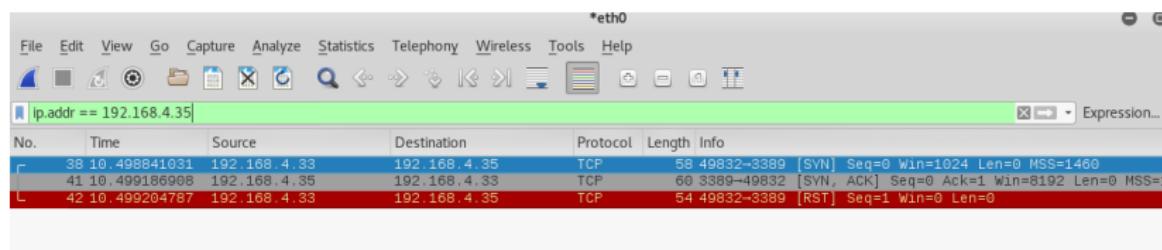
Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
root@kali:/etc/ssh#
```

# TCP Taraması I

► nmap -sT 192.168.4.35 -n -p80

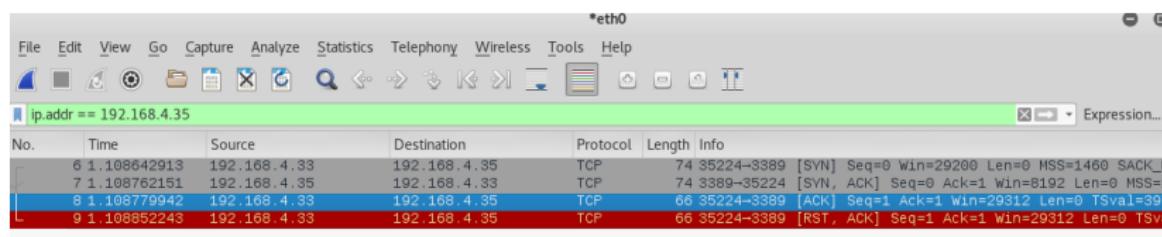


TCP Taraması II



### **Şekil:** SYN taraması

# TCP Taraması III



**Şekil:** TCP taraması

# TCP Taraması IV

## SYN Taraması

- ▶ 3'lü el sıkışma tamamlanmaz
- ▶ SYN+ACK gelirse RST ile bağlantı kapatılır
- ▶ Sunucuda kayıt tutulmaz
- ▶ Root hakkı gerektirir
  - ▶ Paketlere müdahale gereklili

## TCP Taraması

- ▶ 3'lü el sıkışma tamamlanır
- ▶ SYN+ACK gelirse ACK ile bağlantı tamamlanır
- ▶ Sunucuda bağlantıya ilişkin kayıt tutulur
- ▶ İşletim sistemi TCP connect() metodu kullanır, root hakkı gerektirmez

UDP Taraması |

Source Port	Destination Port
UDP Message Length	UDP Checksum
Data	
.....	

### **Şekil: UDP Header**

- ▶ There are no Control Bits in UDP, nor is there a sense of the "status" of a "connection."
  - ▶ nmap -sU 192.168.4.35

oooooooooooo

oooooooooooooooooooo

oooooooooooo●●●○○○○○○

oooooooooooo

oooooooooooo

oooo

## UDP Taraması II

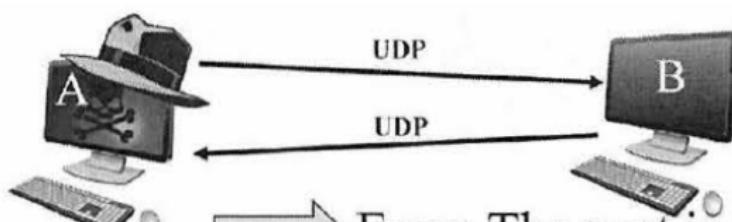
- ▶ **Uzun zaman alır:** UDP taramasında hedef sisteminde geriye bir cevap gelmesi garantisini bulunmadığından zaman aşımıları (timeouts) beklenir.
- ▶ **Boş UDP paketi gönderir:** Boş pakete UDP protokolü ile çalışan bir servisin herhangi bir cevap dönmeme ihtimali yüksektir.
- ▶ UDP protokolü ile çalışan en sık rastlanan uygulamalar ve port numaraları şu şekildedir: DNS (53), TFTP (69), DHCP (67-68), NTP (123), SNMP (161-162)

UDP Taraması III

```
File Edit View Search Terminal Help
root@kali: /etc/ssh# nmap -sU 192.168.4.35 --top-ports 10
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-10-11 13:31 EEST
Nmap scan report for 192.168.4.35
Host is up (0.00018s latency).
PORT      STATE      SERVICE      VERSION
53/udp    open|filtered domain      /etc/ssh/authorized_keys
67/udp    open|filtered dhcps      user's ~/ghosts and ~/sheets files
123/udp   open|filteredntp
135/udp   open|filteredmsrpc
137/udp   open       netbios-ns
138/udp   open|filterednetbios-dgm
161/udp   open|filteredsnmp
445/udp   open|filteredmicrosoft-ds
631/udp   open|filteredipp
1434/udp  open|filteredms-sql-m
MAC Address: E8:39:35:34:E6:44 (Hewlett Packard)
Nmap done: 1 IP address (1 host up) scanned in 1.25 seconds
root@kali: /etc/ssh# make sure SSH service always restarts on reboot in Kali Linux
```

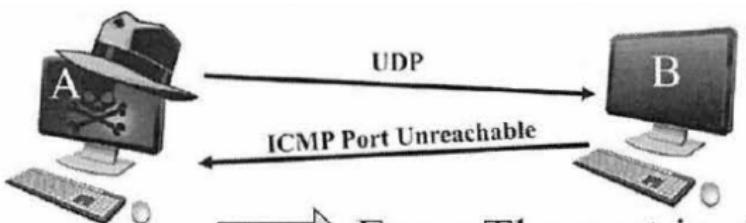
# UDP Taraması I

Case U1:  
UDP in  
UDP back



Easy: The port is open!

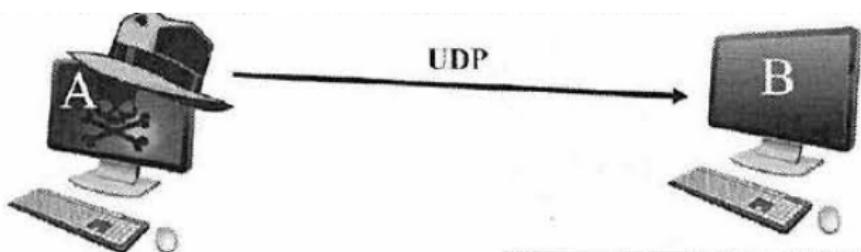
Case U2:  
UDP in  
ICMP Port  
Unreachable back



Easy: The port is closed  
(or a firewall blocked it)

## UDP Taraması II

Case U3:  
UDP in  
Nothing back



### The port is inaccessible

- ▶ Port is closed
- ▶ Firewall is blocking inbound UDP probe packet
- ▶ Firewall is blocking outbound response
- ▶ Port is open, but it was looking for specific data in UDP payload. Without the data, no response was sent

oooooooooooooooooooooooooooooooooooo●●●○○○oooooooo

## UDP Taraması III

UDP taraması port durumları:

- ▶ **open**: UDP servisi herhangi bir cevap döner. Bu durumda dinleyen bir servis olduğu anlaşılır.
- ▶ **closed**: UDP servisi “ICMP port unreachable” cevabı döner. Bu durumda porta erişimde bir güvenlik duvarının engellemesi olmadığı ancak dinleyen bir UDP servisi olmadığı anlaşılır.
- ▶ **filtered**: UDP servisi “ICMP port unreachable” haricinde “ICMP unreachable” mesajlarından birini döner. Bu durumda porta erişimde bir güvenlik duvarının engellemesi olduğu anlaşılır.
- ▶ **open—filtered**: UDP servisinden bir cevap gelmez. Bu durumda orada dinleyen bir servis olup olmadığı veya porta erişimde bir güvenlik duvarının engellemesi olup olmadığı hakkında bilgi sahibi olamayız.

## Nmap Kullanılabilirlik Özellikleri I

### --packet-trace

- ▶ Her bir paket için detaylı bilgiler sunmaktadır.
  - ▶ Nmap calls to the OS
  - ▶ SENT/ RCVD
  - ▶ Protocol (TCP/UDP)
  - ▶ Source IP:Port and Dest IP:Port
  - ▶ Control Bits

```
# map -Pn -sS 10.10.0.1 -p1-1024 --packet-trace
```

- ▶ **-Pn**: Indicates that we don't want to ping the target system; we just want to scan it.
- ▶ **-sS**: Indicates that we want a SYN scan (also known as a Stealth Scan or a Half-Open Scan).
- ▶ **-p1-1024**: Tells Nmap to scan ports 1 through 1024 only
- ▶ **--packet-trace**: Makes Nmap display the status and packet summary information.

## Nmap Kullanılabilirlik Özellikleri II

### Custom Control Bits in Scans

- ▶ İstenilen Control Bits ile bayrak oluşturmak için kullanılmaktadır  
--scanflags [URG|ACK|PSH|RST|SYN|FIN|ECE|CWR|ALL|NONE]
  - ▶ Kontrol Bitlerine ilişkin üç harfli referansı herhangi bir sırada (veya ALL veya NONE) ekleyin.
  - ▶ Örnek: 10.10.10.10'da TCP portuna bir SYN, bir PSH, bir ACK paketi göndermek için aşağıdakileri çalıştırabilirsiniz:  
`nmap --scanflags SYNPSHACK -p 445 10.10.10.10`

# Uygulama

## Uygulama

### ► ARP taraması:

```
nmap -n -sP 10.10.10.1-255 --packet-trace
```

- ▶ -n: Nmap should not resolve domain names
- ▶ -d: debug

### ► tcpdump uygulaması:

```
tcpdump -nn host 10.10.10.50
```

- ▶ to show traffic associated with host 10.10.10.50 (not resolving names).
- ▶ nmap -n -sT 10.10.10.50
- ▶ nmap -n -sT 10.10.10.50 -p1-65535

# İçindekiler

1

- Tarama
  - Giriş

2

- Network Tracing
  - IPv4 Başlığı ve TTL Alanı
  - Keşif Türleri
  - Pasif Keşif
  - Aktif Keşif
  - Ping Sweep
  - Angry IP Scanner
  - TCP Flag Tipleri
  - Nmap

3

- Nmap Taraması
  - Nmap Ping Taraması
  - Nmap Port Taraması

- Nmap Kullanılabilirlik Özellikleri
- Uygulama

4

- Servis, Versiyon ve OS Tespiti
  - İşletim Sistemi Tespiti
  - Servis ve Versiyon Tespiti
  - Girdi - Çıktı Yönetimi
  - Uygulama

5

- NMAP Betik Taraması
  - Betik Taraması

6

- Zamanlama, IPS/IDS Atlatma
  - Zamanlama
  - IPS/IDS Atlatma

7

- Tarama İpuçları
  - IP Adresi Kullanarak Tarama
  - Büyük Ağlarda Tarama

İsletim Sistemi Tespiti |

### Nmap Active OS Fingerprinting

Nmap Aktif İşletim Sistemi Parmak İzi

- ▶ Nmap, çeşitli paket türlerini göndererek ve yanıtını ölçerek hedeflerin işletim sistemini belirlemeye çalışmaktadır.
  - ▶ Farklı sistemler, uzaktan tetikleyememiz ve ölçebildiğimiz farklı protokol davranışlarına sahiptir.
  - ▶ Nmap'ın yeni sürümleri, yıllardır Nmap'te bulunan ilk nesil OS parmak izi kapasitesini değiştirdi.
    - ▶ Farklı işletim sistemleri için çoğunlukla olağandışı Kontrol Bit ayarları ile ilişkilendirilen bir hedefde dokuz farklı test gerçekleştirir
    - ▶ Modern Nmap sürümlerinde yalnızca ikinci nesil OS parmak izi işlevi bulunmaktadır
  - ▶ İkinci nesil kapasitete ek testler bulunmaktadır.
  - ▶ -O seçeneği (ve -O2) ikinci nesil yöntemi kullanır



Windows



Mac OSX



Linux

İsletim Sistemi Tespitı II

## Nmap Active OS Fingerprinting

## Tests Included in Nmap Second Gen OS Fingerprinting

- ▶ 30'dan fazla farklı yöntem bulunmaktadır:
    - ▶ TCP ISN greatest common denominator (GCD)
    - ▶ TCP ISN counter rate (ISR)
    - ▶ TCP IP ID sequence generation algorithm (TI)
    - ▶ ICMP IP ID sequence generation algorithm (II)
    - ▶ Shared IP ID sequence boolean (SS)
    - ▶ TCP timestamp option algorithm (TS)
    - ▶ TCP initial window size (W, WI - W6)
    - ▶ IP don't fragment bit (DF)
    - ▶ IP initial Time-To-Live guess (TG)
    - ▶ Explicit congestion notification (CC)



# Servis ve Versiyon Tespiti I

## Port üzerinde çalışan servisin tespiti

- ▶ Uygulama belirli port üzerinde çalışmak zorunda değil.
- ▶ Örnek TCP/443 portunda SSH çalışabilir.



# Servis ve Versiyon Tespiti II

## nmap-service-probes veritabanı

- ▶ Dinleyen servise çeşitli paketler göndererek davranışına göre uygulamanın versyonunu tespit etmeye çalışır.
- ▶ Uygulama protokolü (Örnek: FTP, SSH, Telnet, ...)
- ▶ Uygulama adı (Örnek: ISC BIND, Apache httpd, ...)
- ▶ Versiyon numarası
- ▶ Sunucu adı
- ▶ Cihaz türü (yazıcı, yönlendirici, ...)
- ▶ İşletim sistemi ailesi (Windows, Linux, ...)
- ▶ Version scan invoked with `-sV`
  - ▶ Or use `-A` for OS fingerprinting, version scan, script scan with default scripts, and traceroute (`-A = -O + -sV + -sC + --traceroute`)
  - ▶ For each listening port discovered during the port scan, Nmap

# Servis ve Versiyon Tespiti III

nmap -sS 192.168.4.54 --top-ports 10 -sV

```
root@kali:/etc/ssh# nmap -sS 192.168.4.54 --top-ports 10 -sV
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-10-11 14:05 EEST
Nmap scan report for 192.168.4.54 (ali Linux)
Host is up (0.00055s latency).

PORT      STATE SERVICE          VERSION
21/tcp    closed  ftp              /var/ssh/authorized_keys
22/tcp    open   ssh              OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
23/tcp    closed  telnet
25/tcp    closed  smtp
80/tcp    open   http             Apache httpd 2.4.7 ((Ubuntu))
110/tcp   closed  pop3
139/tcp   open   netbios-ssn     Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp   open   ssl/http        VMware VirtualCenter Web service
445/tcp   open   netbios-ssn     Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3389/tcp  closed  ms-wbt-server
MAC Address: FC:15:B4:E9:87:1C (Hewlett Packard)
Service Info: Host: COMPUTER-HP-ELITEBOOK-8470P; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.53 seconds
root@kali:/etc/ssh# [root@kali ~]# rc.d -f ssh enable 2 3 4 5
```



# Servis ve Versiyon Tespiti IV

nmap -sU 192.168.4.54 --top-ports 10 -sV

root@kali: /etc/ssh

```
File Edit View Search Terminal Help
root@kali:/etc/ssh# nmap -sU 192.168.4.54 --top-ports 10 -sV
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-10-13 13:36 EEST
Nmap scan report for 192.168.4.54
Host is up (0.00059s latency).
PORT      STATE     SERVICE      VERSION
53/udp    closed    domain
67/udp    closed    dhcps
123/udp   closed    ntp
135/udp   closed    msrpc
137/udp   open      netbios-ns  Samba nmbd netbios-ns (workgroup: WORKGROUP)
138/udp   open|filtered netbios-dgm
161/udp   closed    snmp
445/udp   closed    microsoft-ds
631/udp   open|filtered ipp
1434/udp  closed    ms-sql-m
MAC Address: FC:15:B4:E9:87:1C (Hewlett Packard)
Service Info: Host: COMPUTER-HP-ELI

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 91.25 seconds
root@kali:/etc/ssh#
```

## Girdi - Çıktı Yönetimi

- ▶ **-iL** ip\_listesi.txt
- ▶ 192.168.1-255.0-255: 192.168.1.0 adresinden 192.168.255.255 IP adresine kadar olan tüm IP adreslerini kapsar
- ▶ 192.168.1.0/24 10.0.0.0/16
- ▶ 192.168.1-255.1-10,254

## Çıktı Yönetimi

- ▶ **-oN**: Normal (Okunabilir)
- ▶ **-oG**: Grepable (Parsing)
- ▶ **-oX**: XML (Veritabanına atmak için)
- ▶ **-oA**: Tüm formatlarda

# Uygulama

## Uygulama

- ▶ run tcpdump so that it sniffs all packets going between your machine and the target network of 10.10.10
  - tcpdump -nn host [YourLinuxIPAddr] and net 10.0.2
  - ▶ Use OS fingerprinting.
  - ▶ Perform a TCP connect scan (the three-way handshake for each open port).
  - ▶ Scan target ports 1 through 1024.
  - ▶ Scan the target network 10.0.2.1-255.
  - ▶ -A: all
- ▶ nmap -n -O -sT -p1-1024 10.10.10.1-255
- ▶ locate nmap-service-probes

# İçindekiler

1

- Tarama
  - Giriş

2

- Network Tracing
  - IPv4 Başlığı ve TTL Alanı
  - Keşif Türleri
  - Pasif Keşif
  - Aktif Keşif
  - Ping Sweep
  - Angry IP Scanner
  - TCP Flag Tipleri
  - Nmap

3

- Nmap Taraması
  - Nmap Ping Taraması
  - Nmap Port Taraması

- Nmap Kullanılabilirlik Özellikleri

- Uygulama

4

- Servis, Versiyon ve OS Tespiti
  - İşletim Sistemi Tespiti
  - Servis ve Versiyon Tespiti
  - Girdi - Çıktı Yönetimi
  - Uygulama

5

- NMAP Betik Taraması
  - Betik Taraması

6

- Zamanlama, IPS/IDS Atlatma
  - Zamanlama
  - IPS/IDS Atlatma

7

- Tarama İpuçları
  - IP Adresi Kullanarak Tarama
  - Büyük Ağlarda Tarama

## Betik Taraması I

## Nmap Scripting Engine

- ▶ Lua programlama dili
  - ▶ Ağ keşfi
  - ▶ Gelişmiş servis tespiti
  - ▶ Zafiyet tespiti
  - ▶ Arka kapı tespiti
  - ▶ Zafiyet sömürme

# Betik Taraması II

## Betik Taraması

- ▶ Aktif hale getirmek için `-sC` veya `--script` kullanılır.

## Kategoriler

- ▶ **auth**: Yetkilendirme atlatma betikleri
- ▶ **brute**: Kaba kuvvet ile yetkilendirme atlatma betikleri
- ▶ **default**: Betik taraması aktif edildiğinde varsayılan betikler
- ▶ **dos**: Servis dışı bırakabilecek açıklıkları test eden betikler, genellikle servis dışı bırakma ile sonlanır
- ▶ **exploit**: Bazı zafiyetleri sömürmek için geliştirilmiş betikler
- ▶ **intrusive**: Güvenli kategorisine girmeyen, servis dışı bırakma ile sonuçlanabilen, sistem kaynaklarını fazla kullanan veya hedef sistem tarafından saldırgan olarak tanımlanacak aktiviteler gerçekleştiren betikler (örneğin kaba kuvvet betikleri)
- ▶ **malware**: Hedef sisteme belirli bir kötücül yazılımın veya arka kapının olup olmadığını test eden betikler
- ▶ **safe**: intrusive kategorisine girmeyen, servis dışı bırakma ile sonuçlanmayacak, sistem kaynaklarını aşırı tüketmeyecek veya hedef sistem tarafından saldırgan olarak tanımlanmayacak aktiviteler gerçekleştiren betikler
- ▶ **version**: Gelişmiş versiyon tespiti gerçekleştiren betikler
- ▶ **vuln**: Hedef sisteme belirli bir zafiyetin olup olmadığını test eden betikler

Betik Taraması III

#### Betik veritabanının güncellenmesi

- nmap --script-updatedb

## Betik aramak

- ▶ locate \*.nse — grep telnet
  - ▶ find / -name "\*.nse" — grep telnet

## Betik çalışırmak

- ▶ nmap -sS -p23 10.0.0.1 --script telnet-brute
  - ▶ nmap -sU -p53 10.0.0.1 --script "dns-\*\*"

## Betik Taraması IV

--script-help

```
Ozgur-MacBook-Pro:makale2 ozgurcatak$ nmap --script-help telnet-brute

Starting Nmap 7.12 ( https://nmap.org ) at 2016-10-16 15:20 EEST
telnet-brute
Categories: brute intrusive
https://nmap.org/nsedoc/scripts/telnet-brute.html
  Performs brute-force password auditing against telnet servers.
Ozgur-MacBook-Pro:makale2 ozgurcatak$ █
```

Betik Taraması V

#### Betik Taraması - Versiyon Tespiti İlişkisi

- ▶ Betik Taraması versiyon tespiti yapılmazsa sadece varsayılan portlara uygulanır

```
Ozgur-MacBook-Pro:makale2 ozgurcatak$ nmap -script telnet-* 192.168.2.1 -Pn -n -p23 -sV
Starting Nmap 7.12 ( https://nmap.org ) at 2016-10-16 15:34 EEST
Nmap scan report for 192.168.2.1
Host is up (0.0037s latency).
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  ZTE router telnetd
| telnet-brute:
[]  Accounts: No valid accounts found
|_ Statistics: Performed 13 guesses in 10 seconds, average tps: 1
|_ ERROR: Password prompt encountered
| telnet-encryption:
|_ Telnet server does not support encryption
Service Info: Device: broadband router

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
Ozgur-MacBook-Pro:makale2 ozgurcatak$
```

## Betik Taraması VI

## Sık kullanılan betikler

- ▶ \*-brute.nse
  - ▶ \*-info.nse
  - ▶ dns-recursion
  - ▶ dns-zone-transfer
  - ▶ http-slowloris-check
  - ▶ ms-sql-info
  - ▶ ms-sql-dump-hashes
  - ▶ nbstat
  - ▶ smb-check-vulns
  - ▶ smb-enum-users
  - ▶ smb-enum-shares



## Betik Taraması VII

### Sık kullanılan betikler - \*.brute.nse

- ▶ ftp-brute
- ▶ ftp-anon
- ▶ ms-sql-brute
- ▶ mysql-brute
- ▶ oracle-sid-brute
- ▶ snmp-brute
- ▶ telnet-brute
- ▶ vmauthd-brute
- ▶ vnc-brute

## Betik Taraması VIII

### nbstat

```
Last login: Sun Oct 16 15:49:28 on ttys000
[Ozgur-MacBook-Pro:~ ozgurcatak$ nmap --script-help nbstat

Starting Nmap 7.12 ( https://nmap.org ) at 2016-10-16 15:49 EEST

nbstat
Categories: default discovery safe
https://nmap.org/nsedoc/scripts/nbstat.html
Attempts to retrieve the target's NetBIOS names and MAC address.

By default, the script displays the name of the computer and the logged-in
user; if the verbosity is turned up, it displays all names the system thinks it
owns.

Ozgur-MacBook-Pro:~ ozgurcatak$ █
```

# Betik Taraması IX

## nbstat

```
[Ozgur-MacBook-Pro:makale2 ozgurcatak$ nmap --script nbstat 192.168.2.6 -Pn -n -p135,139,445 ]  
  
Starting Nmap 7.12 ( https://nmap.org ) at 2016-10-16 15:46 EEST  
Nmap scan report for 192.168.2.6  
Host is up (0.19s latency).  
PORT      STATE    SERVICE  
135/tcp    closed   msrpc  
139/tcp    closed   netbios-ssn  
445/tcp    open     microsoft-ds  
  
Host script results:  
|_nbstat: NetBIOS name: MACBOOKAIR-A398, NetBIOS user: <unknown>, NetBIOS MAC: c8:69:cd:8c:a3:  
98 (Apple)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds  
Ozgur-MacBook-Pro:makale2 ozgurcatak$ █
```

# İçindekiler

1

- Tarama
  - Giriş

2

- Network Tracing
  - IPv4 Başlığı ve TTL Alanı
  - Keşif Türleri
  - Pasif Keşif
  - Aktif Keşif
  - Ping Sweep
  - Angry IP Scanner
  - TCP Flag Tipleri
  - Nmap

3

- Nmap Taraması
  - Nmap Ping Taraması
  - Nmap Port Taraması

- Nmap Kullanılabilirlik Özellikleri

- Uygulama

4

- Servis, Versiyon ve OS Tespiti
  - İşletim Sistemi Tespiti
  - Servis ve Versiyon Tespiti
  - Girdi - Çıktı Yönetimi
  - Uygulama

5

- NMAP Betik Taraması
  - Betik Taraması

6

- Zamanlama, IPS/IDS Atlatma
  - Zamanlama
  - IPS/IDS Atlatma

7

- Tarama İpuçları
  - IP Adresi Kullanarak Tarama
  - Büyük Ağlarda Tarama

# Zamanlama I

## Zamanlama

- ▶ Tarama doğruluğu ve etkinliği açısından önemlidir.
- ▶ Dışardan yapılan taramalarda IPS/IDS'den kaçmak için yavaş taramalar.
- ▶ İçeriden yapılan taramalarda hızlı tarama tercih edilir.

## Parametreler

- ▶ **-T0 (paranoid):** En yavaş tarama türündür. Paralel tarama kapalıdır ve gönderilen her bir paket arasında 5 dk süre geçer.
- ▶ **-T1 (sneaky):** Paralel tarama kapalıdır ve gönderilen her bir paket arasında 15 sn süre geçer.
- ▶ **-T2 (polite):** Paralel tarama kapalıdır ve gönderilen her bir paket arasında 0.4 sn süre geçer.
- ▶ **-T3 (normal):** Nmap varsayılan tarama hızıdır. Belirli bir hız seçeneği sunulmadığında kullanılır. Paralel tarama ilk kez bu parametre ile başlar. Nmap hızını taramanın durumuna göre ayarlar.
- ▶ **-T4 (aggressive):** Varsayılan taramaya göre daha hızlıdır.
- ▶ **-T5 (insane):** En hızlı tarama seçeneğidir. Ağ trafiğinin dolmasına ve hizmet kesintilerine neden olabilir. Ayrıca zaman aşırıları beklenmeyeceğinden bazı servisler için yanlış sonuçlar da dönme ihtimali vardır.

Zamanlama II

--max-retries 2

- ▶ Nmap cevap alamadığı portlar için tekrardan istekte gönderir.
  - ▶ Bu parametre ile kaç kez tekrar paket gönderileceği belirtilebilir

```
--host-timeout 30
```

- ▶ Bir sunucuda taramanın en çok süreceğini süre belirtilebilmektedir.

#### Paralel Taramanın Kapatılması

- ▶ **-T0, -T1, -T2:** Paralel tarama bu parametreler kullanıldığında kapalıdır.
  - ▶ **--scan-delay 1:** Gönderilen her bir paket arasına 1 sn süre koyar.
  - ▶ **--max-parallelism 1:** Aynı anda bir sunucuya tek bir paket gönderilmesini sağlar.
  - ▶ **--max-hostgroup 1:** Paralel taramayı tamamen kapatmaz, tek bir anda tek bir sunucuya tarama gerçekleştirilmesini sağlar.

# IPS/IDS Atlatma

## ► Zamanlama

- ▶ Paketler arası süreyi uzat
- ▶ Paralel taramayı kapat

## ► Fragmentation

- ▶ -f

## ► Kaynak Portu

- ▶ --source-port
- ▶ Kaynak portu 80 olan bir bağlantı daha güvenilir olabilir

## ► Tarama sırasını karıştırma

- ▶ --randomize-hosts
- ▶ Sıra ile taramayı engeller

## ► IP Sahteciliği

- ▶ Gönderilen paket geri dönmez
- ▶ UDP trafiği için mantıklı

## ► Güvenlik duvarı ve IPS/IDS tespiti

- ▶ TTL
- ▶ --badsum

# İçindekiler

1

- Tarama
  - Giriş

2

- Network Tracing
  - IPv4 Başlığı ve TTL Alanı
  - Keşif Türleri
  - Pasif Keşif
  - Aktif Keşif
  - Ping Sweep
  - Angry IP Scanner
  - TCP Flag Tipleri
  - Nmap

3

- Nmap Taraması
  - Nmap Ping Taraması
  - Nmap Port Taraması

- Nmap Kullanılabilirlik Özellikleri

- Uygulama

4

- Servis, Versiyon ve OS Tespiti
  - İşletim Sistemi Tespiti
  - Servis ve Versiyon Tespiti
  - Girdi - Çıktı Yönetimi
  - Uygulama

5

- NMAP Betik Taraması
  - Betik Taraması

6

- Zamanlama, IPS/IDS Atlatma
  - Zamanlama
  - IPS/IDS Atlatma

7

- Tarama İpuçları
  - IP Adresi Kullanarak Tarama
  - Büyük Ağlarda Tarama

# IP Adresi Kullanarak Tarama

## IP Adresi Kullanarak Tarama

- ▶ Sistemleri tararken (ve istismar ederken), genellikle sistem adlarını değil, hedef IP adreslerini veya adres aralıklarını kullanmak için tarama araçlarını yapılandırırız.
  - ▶ Örneğin, www.target.tgt yerine 10.10.10.10
  - ▶ İsmey dayalı olarak saldırırsanız, test gerçekleştirken, round robin DNS, hedef sistemi değiştirebilir
  - ▶ Hatalı sonuçlara neden olabilir
    - ▶ İki farklı adrese yapılan port taramasında sonuçlar hatalara neden olacaktır
    - ▶ Hizmetin sömürülmesi sırasında farklı bir makineye bağlanılabilir
  - ▶ Tek bir IP adresinin bile birden çok fiziksel (veya sanal) hedefte dengeli olarak yüklediğini kabul edilmelidir.

# Büyük Ağlarda Tarama I

## Büyük ağların küçük ağlara bölünmesi

- ▶ Taramaların belirli bir düzen içerisinde gerçekleşmesi açısından taramaların daha küçük alt ağlara gerçekleştirilmesi önerilir.
- ▶ Örnekleme kümesi alınabilir.

## IP keşfi için ping taraması kullanımı

- ▶ Taramalardan önce ping taraması gerçekleştirilerek IP adresleri tespit edilebilir.
- ▶ Tespit edilen bu IP adresleri diğer sızma testi tekniklerinde kullanılmak adına hazır olmuş olur.

## İsim Çözümleme yapılmaması

- ▶ Nmap taradığı IP adreslerinin sunucu isimlerini tespit etmek için DNS sunucuya reverse kayıtları sorgulayabilir.
- ▶ Bu işlem yavaş olmaktadır. –n parametresi ile isim çözme kapatılabilir.

## Büyük Ağlarda Tarama II

### Hızlı tarama seçeneklerinin kullanılması

- ▶ -T4—5
- ▶ --max-retries
- ▶ --host-timeout
- ▶ Paket kaybı yaşanabilir (timeouts)
- ▶ Servis dışı kalma