

## 03 - Tarama

### BGM 553 - Sızma Testleri ve Güvenlik Denetlemeleri-I

Bilgi Güvenliği Mühendisliği  
Yüksek Lisans Programı

**Dr. Ferhat Özgür Çatak**  
ozgur.catak@tubitak.gov.tr

İstanbul Şehir Üniversitesi  
2017 - Güz

## İçindekiler

1 Tarama

- Giriş
  - Keşif Türleri
  - Pasif Keşif
  - Aktif Keşif
  - Ping Sweep
  - Angry IP Scanner
  - TCP Flag Tipleri
  - Nmap
- Nmap Taraması
- Nmap Ping Taraması

- Nmap Port Taraması

### 3 Servis, Versiyon ve OS Tespiti

- Servis ve Versiyon Tespiti
- Girdi - Çıktı Yönetimi

#### 4 NMAP Betik Taraması

- Betik Taraması

5 Zamanlama, IPS/IDS Atlatma

- Zamanlama
- IPS/IDS Atlatma

## 6 Büyük Ağların Taranması

- Büyük Ağlarda Tarama

# İçindekiler

1

## Tarama

- Giriş
- Keşif Türleri
- Pasif Keşif
- Aktif Keşif
- Ping Sweep
- Angry IP Scanner
- TCP Flag Tipleri
- Nmap

2

## Nmap Taraması

- Nmap Ping Taraması

3

## Nmap Port Taraması

- Servis, Versiyon ve OS Tespiti
- Servis ve Versiyon Tespiti
- Girdi - Çıktı Yönetimi

4

## NMAP Betik Taraması

- Betik Taraması

5

## Zamanlama, IPS/IDS Atlatma

- Zamanlama
- IPS/IDS Atlatma

6

## Büyük Ağların Taranması

- Büyük Ağlarda Tarama

# Tarama I

# Tarama

- ▶ Pentest planlamasında yerel ağın tespit edilmesi önem taşımaktadır.
- ▶ Ağı ele geçirmek isteyen saldırgan, ağ üzerinde yer alan IP adresleri ve sistemler üzerinde yer alan servisler hakkında bilgi sahibi değildir.
- ▶ **Tarama:** Ağ üzerinde bulunan çalışır halde ve yanıt veren sistemlerin bulunması işlemi.
- ▶ Tarama araçları kullanılarak hedef bilgisayarın IP bilgisi, işletim sistemi ve üzerinde çalışan servisler gibi bilgilere ulaşabiliriz.
- ▶ Bu faz iki aşamaya ayrılmaktadır:
  - ▶ network scanning
  - ▶ port scanning
- ▶ IP adreslerini taramak için birçok araç bulunmaktadır.
  - ▶ Angry IP Scanner
  - ▶ Nmap - Zenmap





# Tarama IV

## 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.

## 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, tracert





**Şekil: Pasif keşif aracı: ARP**

# Aktif Keşif

## Aktif Keşif

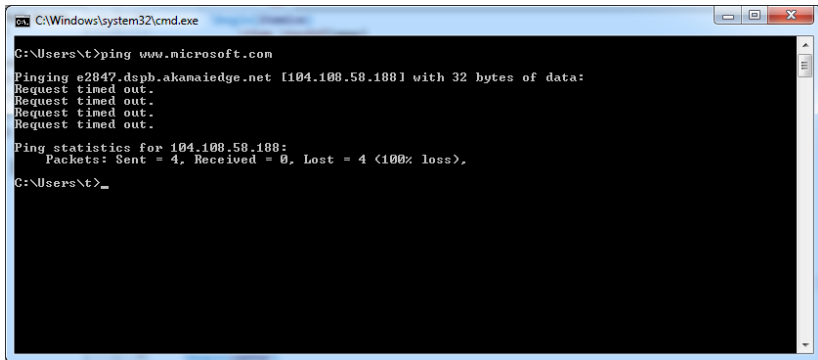
- ▶ Saldırgan aktif olarak ağa paketler gönderir.
  - ▶ Angry IP
  - ▶ nmap
  - ▶ hping
  - ▶ Scapy
  - ▶ nessus
- ▶ Bu eğitim kapsamında kullanılacak olan araç: **nmap**

# 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

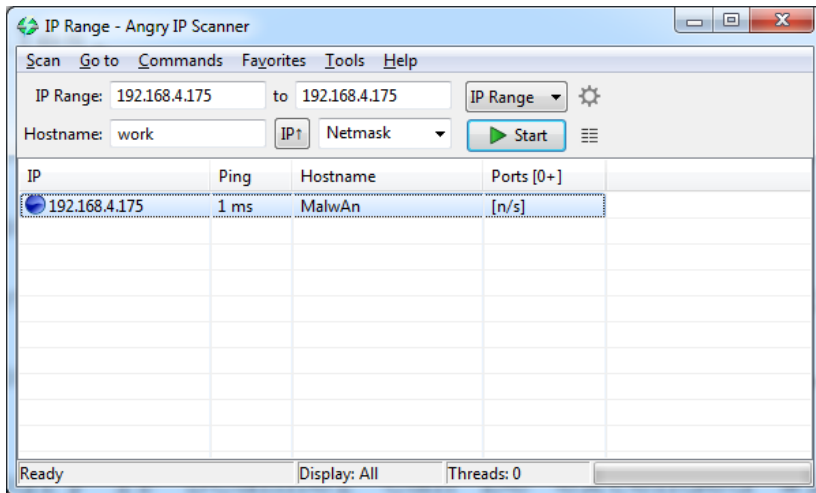
- ping'e karşılık uzak sistem kapalı, cevap vermiyor veya ping bloklandı.

# Angry IP Scanner I

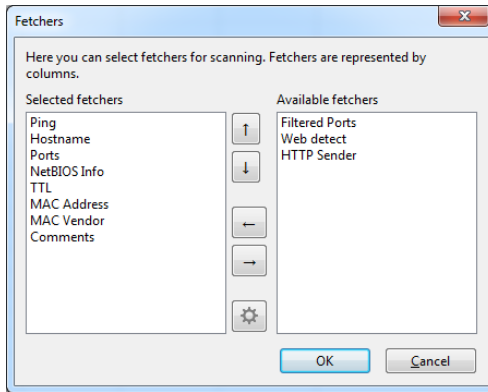
## Angry IP Scanner

- ▶ 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 yazılabilir.
- ▶ Multi-thread. Her bir IP adresi için ayrı thread oluşturularak hızlı bir şekilde sonuç alınabilmektedir.

# Angry IP Scanner II

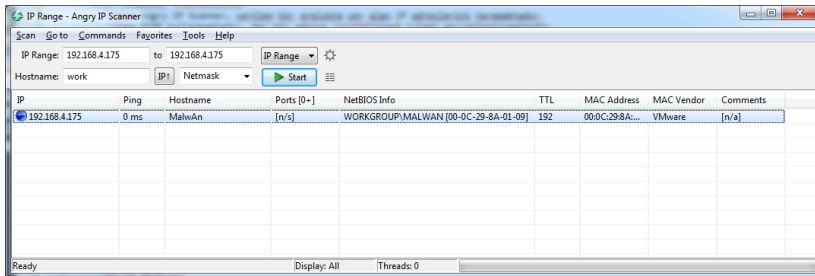


# Angry IP Scanner III





# Angry IP Scanner IV



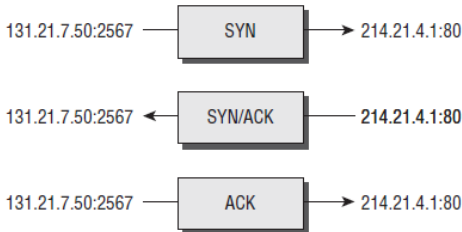
# TCP Flag Tipleri I

## 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
- ▶ port scanning
- ▶ service identification
- ▶ IP address detection
- ▶ operating system detection
- ▶ 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</b> , <b>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 edinmektir. 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 yazılabilir.
- ▶ 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 oluşturması sebebiyle Root/Administrator yetkileri ister.

## Uygulama

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

# İçindekiler

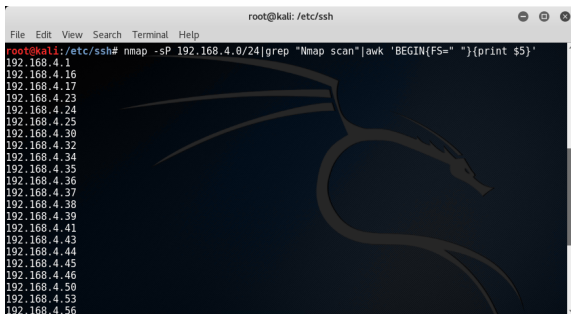
- 1 Tarama
  - Giriş
  - Keşif Türleri
  - Pasif Keşif
  - Aktif Keşif
  - Ping Sweep
  - Angry IP Scanner
  - TCP Flag Tipleri
  - Nmap
- 2 Nmap Taraması
  - Nmap Ping Taraması
  - Nmap Port Taraması
- 3 Servis, Versiyon ve OS Tespiti
  - Servis ve Versiyon Tespiti
  - Girdi - Çıktı Yönetimi
- 4 NMAP Betik Taraması
  - Betik Taraması
- 5 Zamanlama, IPS/IDS Atlatma
  - Zamanlama
  - IPS/IDS Atlatma
- 6 Büyük Ağların Taranması
  - 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.



```
root@kali: /etc/ssh
File Edit View Search Terminal Help
root@kali: /etc/ssh# nmap -sP 192.168.4.0/24 | grep "Nmap scan" | awk "BEGIN{FS=" "}{print $5}"
192.168.4.1
192.168.4.16
192.168.4.17
192.168.4.23
192.168.4.24
192.168.4.25
192.168.4.30
192.168.4.32
192.168.4.34
192.168.4.35
192.168.4.36
192.168.4.37
192.168.4.38
192.168.4.39
192.168.4.41
192.168.4.43
192.168.4.44
192.168.4.45
192.168.4.46
192.168.4.50
192.168.4.53
192.168.4.56
```

Şekil: Nmap ping taraması

# Nmap SYN Taraması

```

root@kali: /etc/ssh
File Edit View Search Terminal Help
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

\*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.4.16

No.	Time	Source	Destination	Protocol	Length	Info
38	7.610409104	192.168.4.33	192.168.4.16	TCP	58	64354→3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
39	7.611000967	192.168.4.16	192.168.4.33	TCP	60	3306→64354 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
L 40	7.611014345	192.168.4.33	192.168.4.16	TCP	54	64354→3306 [RST] Seq=1 Win=0 Len=0

Frame 40: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0

Ethernet II, Src: CadmusCo\_ef:6f:fe (08:00:27:ef:6f:fe), Dst: HewlettP\_4c:24:2e (48:0f:cf:4c:24:2e)

Internet Protocol Version 4, Src: 192.168.4.33, Dst: 192.168.4.16

Transmission Control Protocol, Src Port: 64354, Dst Port: 3306, Seq: 1, Len: 0

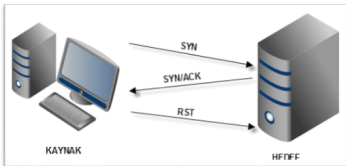
```

0000  48 0f cf 4c 24 2e 08 00  27 ef 6f fe 08 00 45 00  H..L$....'.o...E.
0010  00 28 bc b5 40 00 40 00  f4 98 c0 a8 04 21 c0 a8  ..(..@. ....
0020  04 10 fb 62 0c ea 55 1c  12 a9 00 00 00 00 50 04  ...b..U. ....P.
0030  00 00 b6 4c 00 00

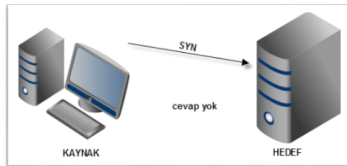
```

Şekil: wireshark paket filtreleme

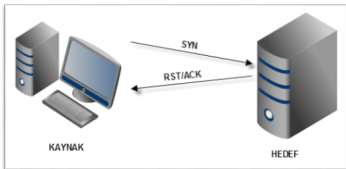
# SYN Taraması



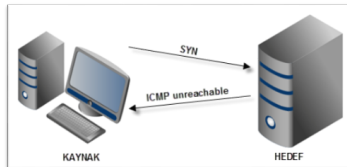
Şekil: OPEN



Şekil: FILTERED



Şekil: CLOSED



Şekil: FILTERED

# 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 filtrelemiş
- Port açık veya kapalı olabilir

# Port Taraması

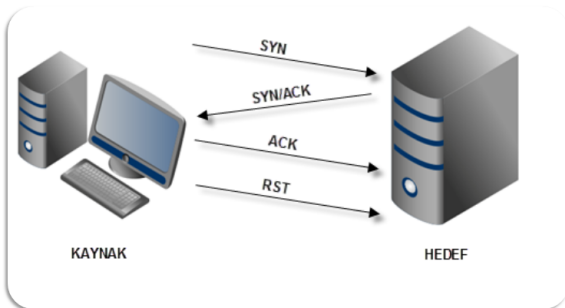
- ▶ En sık kullanılan 1000 port
- ▶ -p80,443,445-447
- ▶ -sU -sT -p U:53,T:21-25,80
- ▶ --top-ports 10
- ▶ -F Scan 100 most common ports (Fast)
- ▶ Tüm portlar: -p1-65535

```
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

The image shows the Wireshark network protocol analyzer interface. At the top, the packet capture filter is set to `ip.addr == 192.168.4.35`. Below the filter, a list of captured packets is displayed. The selected packet is a TCP SYN packet (No. 38) from source IP 10.49884.1031 to destination IP 192.168.4.35. The packet details show a SYN flag and a sequence number of 49832.

No.	Time	Source	Destination	Protocol	Length	Info
38	10.49884.1031	192.168.4.33	192.168.4.35	TCP	58	49832→3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
41	10.499186908	192.168.4.35	192.168.4.33	TCP	60	3389→49832 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=
42	10.499204787	192.168.4.33	192.168.4.35	TCP	54	49832→3389 [RST] Seq=1 Win=0 Len=0

**Şekil: SYN taraması**

The image shows the Wireshark network protocol analyzer interface. At the top, the title bar indicates the current capture file is 'eth0'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with icons for various functions like opening files, saving, and zooming. The packet capture filter is set to 'ip.addr == 192.168.4.35'. The packet list pane shows four captured packets, all of which are TCP segments from 192.168.4.35 to 192.168.4.35. The selected packet (No. 9) is a RST (Reset) segment with Seq=1, Ack=1, Win=29312, and Len=0. The packet details pane on the right shows the structure of this RST segment, including the SYN, ACK, RST, and Seq=1 fields.

No.	Time	Source	Destination	Protocol	Length	Info
6	1.108642913	192.168.4.33	192.168.4.35	TCP	74	35224→3389 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_
7	1.108762151	192.168.4.35	192.168.4.33	TCP	74	3389→35224 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=
8	1.108779942	192.168.4.33	192.168.4.35	TCP	66	35224→3389 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=39
9	1.108852243	192.168.4.33	192.168.4.35	TCP	66	35224→3389 [RST, ACK] Seq=1 Ack=1 Win=29312 Len=0 TS

**Şekil: TCP taraması**

# TCP Taraması III

## SYN Taraması

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

## 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 I

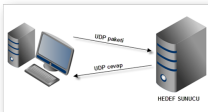
- ▶ `nmap -sU 192.168.4.35`
- ▶ **Uzun zaman alır:** UDP taramasında hedef sistemden geriye bir cevap gelmesi garantisi bulunmadığından zaman aşırımları (timeouts) beklenir.
- ▶ **Boş UDP paketi gönderir:** Boş pakete UDP protokolü ile çalışan bir servisin herhangi bir cevap dönmeme ihtimali yüksektir.
- ▶ 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 II

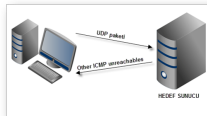
```
root@kali: /etc/ssh
File Edit View Search Terminal Help
root@kali:/etc/ssh# nmap -sU 192.168.4.35 --top-ports 10
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-10-11 13:31 EEST
Nmap scan report for 192.168.4.35
Host is up (0.00018s latency).
PORT      STATE SERVICE
53/udp    open|filtered domain*
67/udp    open|filtered dhcpc
123/udp   open|filtered ntp
135/udp   open|filtered msrpc
137/udp   open      netbios-ns
138/udp   open|filtered netbios-dgm
161/udp   open|filtered snmp
445/udp   open|filtered microsoft-ds
631/udp   open|filtered ipp
1434/udp  open|filtered ms-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#
```

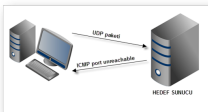
# UDP Taraması I



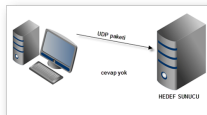
Şekil: OPEN



Şekil: FILTERED



Şekil: CLOSED



Şekil: OPEN—FILTERED

## UDP Taraması II

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.

# İçindekiler

- 1 Tarama
  - Giriş
  - Keşif Türleri
  - Pasif Keşif
  - Aktif Keşif
  - Ping Sweep
  - Angry IP Scanner
  - TCP Flag Tipleri
  - Nmap
- 2 Nmap Taraması
  - Nmap Ping Taraması
- 3 Servis, Versiyon ve OS Tespiti
  - Servis ve Versiyon Tespiti
  - Girdi - Çıktı Yönetimi
- 4 NMAP Betik Taraması
  - Betik Taraması
- 5 Zamanlama, IPS/IDS Atlatma
  - Zamanlama
  - IPS/IDS Atlatma
- 6 Büyük Ağların Taranması
  - Büyük Ağlarda Tarama

# Servis ve Versiyon Tespiti I

## Port üzerinde çalışan servisin tespiti

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

## nmap-service-probes veritabanı

- ▶ Dinleyen servise çeşitli paketler göndererek davranışına göre uygulamanın versiyonunu 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, ...)



## Servis ve Versiyon Tespiti III

```
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    dhcp
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

## Girdi 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

# İçindekiler

- 1 Tarama
  - Giriş
  - Keşif Türleri
  - Pasif Keşif
  - Aktif Keşif
  - Ping Sweep
  - Angry IP Scanner
  - TCP Flag Tipleri
  - Nmap
- 2 Nmap Taraması
  - Nmap Ping Taraması
- 3 Servis, Versiyon ve OS Tespiti
  - Servis ve Versiyon Tespiti
  - Girdi - Çıktı Yönetimi
- 4 NMAP Betik Taraması
  - Betik Taraması
- 5 Zamanlama, IPS/IDS Atlatma
  - Zamanlama
  - IPS/IDS Atlatma
- 6 Büyük Ağların Taranması
  - 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 sistemde 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 sistemde 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 çalıştırmak

- ▶ `nmap -sS -p23 10.0.0.1 --script telnet-brute`
- ▶ `nmap -sU -p53 10.0.0.1 --script "dns-*.nmap.org"`

# 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 ozgurcatac$ 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 ozgurcatac$
```

# 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: MACB00KAIR-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
  - Keşif Türleri
  - Pasif Keşif
  - Aktif Keşif
  - Ping Sweep
  - Angry IP Scanner
  - TCP Flag Tipleri
  - Nmap
- 2 Nmap Taraması
  - Nmap Ping Taraması
- 3 Servis, Versiyon ve OS Tespiti
  - Servis ve Versiyon Tespiti
  - Girdi - Çıktı Yönetimi
- 4 NMAP Betik Taraması
  - Betik Taraması
- 5 Zamanlama, IPS/IDS Atlatma
  - Zamanlama
  - IPS/IDS Atlatma
- 6 Büyük Ağların Taranması
  - 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 türüdür. 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 aşımaları beklenmeyeceğinden bazı servisler için yanlış sonuçlar da dönme ihtimali vardır.



# 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
  - Keşif Türleri
  - Pasif Keşif
  - Aktif Keşif
  - Ping Sweep
  - Angry IP Scanner
  - TCP Flag Tipleri
  - Nmap
- ## 2 Nmap Taraması
- Nmap Ping Taraması

3

## • Nmap Port Taraması

## 3 Servis, Versiyon ve OS Tespiti

- Servis ve Versiyon Tespiti
- Girdi - Çıktı Yönetimi

4

## 4 NMAP Betik Taraması

- Betik Taraması

5

## 5 Zamanlama, IPS/IDS Atlatma

- Zamanlama
- IPS/IDS Atlatma

6

## 6 Büyük Ağların Taranması

- Büyük Ağlarda Tarama



# Büyük Ağlarda Tarama I

## Büyük ağların küçük ağlara bölünmesi

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