

Ağ Keşif Çalışmaları

Bilgi Güvenliği AKADEMİSİ

Bölüm Amacı

- Hedef sistemler hakkında ağ üzerinden edinilebilecek bilgileri toplama.
- Aktif bilgi toplama çeşididir.

Bölüm içeriği

- Taramanın/Keşif Tanımı
- Amaçları
- Çeşitleri
- Tarama/Keşif Teknikleri
- Tarama/Keşif Araçları
- İşletim Sistemi Belirleme
- Taramaya karşı Önlem Alma

Ağ Keşfi Neden Önemlidir?

- Aktif cihazların tespiti
- Çalışan servislerin belirlenmesi
- Cihazlar üzerindeki işletim sistemlerinin belirlenmesi
- Ağ haritasının çıkarılması
 - Router-Firewall-IPS-WAF-Host ...
- Ağ haritası keşfi ve basit bir açıklığın interneti durdurması(!)

Host/Port Tarama

- Saldırganın ilk yapacağı işlemlerden
- Tarama sonucunda
 - Aktif IP adresleri
 - Aktif servisler
 - İşletim sistemleri
 - Genel ağ haritası
 - Firewall, router vs
- Tarama Çeşitleri
 - Host/Ag Tarama
 - Port tarama
 - Versiyon belirleme
 - İşletim sistemi belirleme
 - Zayıflık tarama

Tarama Çeşitleri

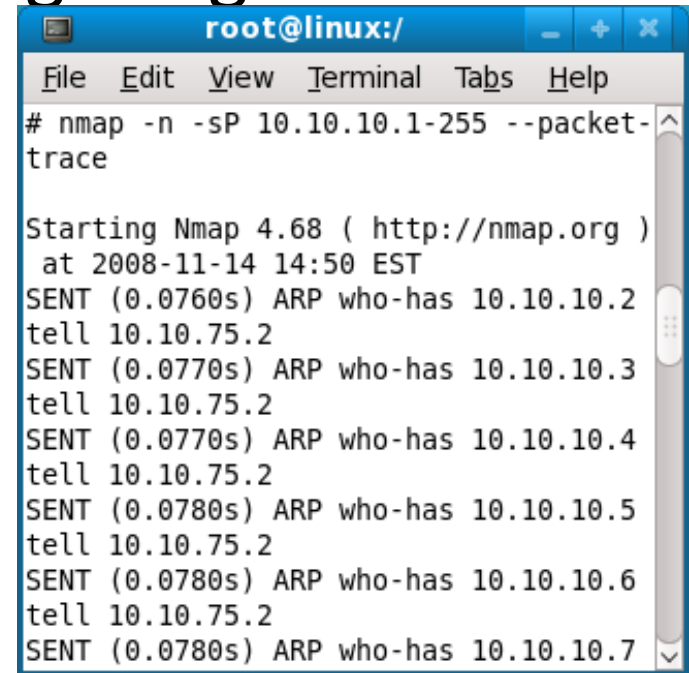
- Host/ağ tarama
 - Belli bir host ya da networkün ip seviyesinden taranması
- Port tarama
 - Belirli bir IP/Ag için çalışan servislerin belirlenmesi
- Ağ haritalama
 - Ağda bulunan aktif cihazların ve konfigürasyonlarının (FW kuralları) belirlenmesi
- İşletim sistemi belirleme
- Zayıflık tarama
 - Aktif bulunan cihazların güvenlik açısından uzaktan incelenmesi

Aktif Sistemlerin Belirlenmesi(Ping)

- ICMP Tarama(klasik ping aracı ile)
- TCP Ping Kavramı
- UDP Ping Kavramı
- ARP Ping

Aktif Sistemlerin Belirlenmesi:ARP Scan

- Sadece yerel ağlar için geçerli bir tarama türüdür.
- Yerel ağda bir makinenin diğerine ulaşabilmesi için ARP sorgusuna cevap alabilmesi gerekir.
- Nmap hedef sistem için arp sorgusu gönderir
- Cevap olumlu ise sistemin ayakta olduğunu
- Cevap olumsuz ise sistemin down durumda olduğunu belirler



```
root@linux:/  
File Edit View Terminal Tabs Help  
# nmap -n -sP 10.10.10.1-255 --packet-trace  
  
Starting Nmap 4.68 ( http://nmap.org )  
at 2008-11-14 14:50 EST  
SENT (0.0760s) ARP who-has 10.10.10.2  
tell 10.10.75.2  
SENT (0.0770s) ARP who-has 10.10.10.3  
tell 10.10.75.2  
SENT (0.0770s) ARP who-has 10.10.10.4  
tell 10.10.75.2  
SENT (0.0780s) ARP who-has 10.10.10.5  
tell 10.10.75.2  
SENT (0.0780s) ARP who-has 10.10.10.6  
tell 10.10.75.2  
SENT (0.0780s) ARP who-has 10.10.10.7
```


Aktif Sistemlerin Belirlenmesi-ICMP

- Sistemlerin icmp paketlerini kabul ettiği düşünülerek yapılır
- İcmp echo-request, reply paketleride dayanır.
- Ping aracı kullanılabilir
 - Daha hızlı taramalar için fping, nmap vs
- Günümüzde geçerliliği yoktur.

Ping Sweep

- Belirlenen bir ağa paralel ICMP paketleri gönderilmesi ve bunların döndüğü cevaba göre aktif sistemlerin belirlenmesi.
- Sistem ayaktaysa kendine gelen echo-request paketlerine echo-reply ile cevap verir.

Port Tarama

- Port Kavramı
 - TCP Portları
 - UDP Portları
 - ICMP/IP için port tarama(?)
- Port Tarama Mantığı
 - RFC'e göre portların durumu
 - UDP için
 - TCP için

En İlkel Host/Port Tarama Aracı

- For a in ... ;ping or netcat, telnet

```
root@home-labs: ~  
root@home-labs:~# for a in {1..25};do echo -e 192.168.2.$a; ping 192.168.2.$a -c 1|grep received;done  
192.168.2.1  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
192.168.2.2  
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms  
192.168.2.3  
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms  
192.168.2.4  
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms  
192.168.2.5  
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms  
192.168.2.6
```

```
root@home-labs: ~  
root@home-labs:~# telnet mail02.lifeoverip.net 25  
Trying 91.93.119.80...  
Connected to mail02.lifeoverip.net.  
Escape character is '^]'.  
220 mail.sistembil.com ESMTP
```

Host/Port Tarama Araçları

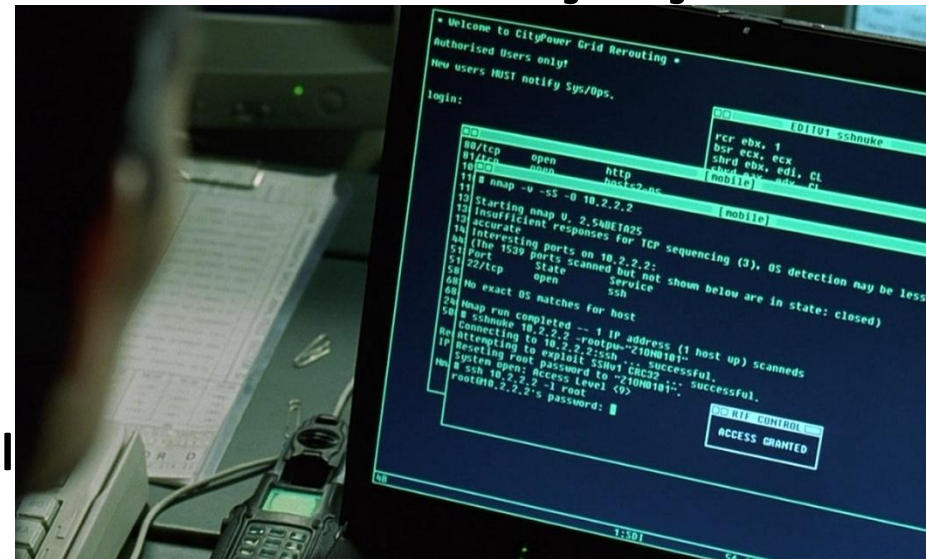
- Scapy, hping, nmap, Nessus
- Angry Ip scan
- Foundstone superscan
- Netcat
- fping



Bölüm-2:Nmap Ağ Keşif Aracı

Nmap

- Gelişmiş özelliklere sahip port tarama ve zaafiyet bulma aracı
- <http://www.insecure.org/nmap> adresinden edinilebilir
- Fyodor Tarafından '98 yılından geliştirilmeye başlandı
- Yaygın kullanılan tüm işletim sistemlerinde çalışır.
- Bilinen, bilinmeyen tüm port tarama tiplerini destekler
- Komut satırı ve grafik arabirimden çalışma modları



Temel Nmap Kullanımı

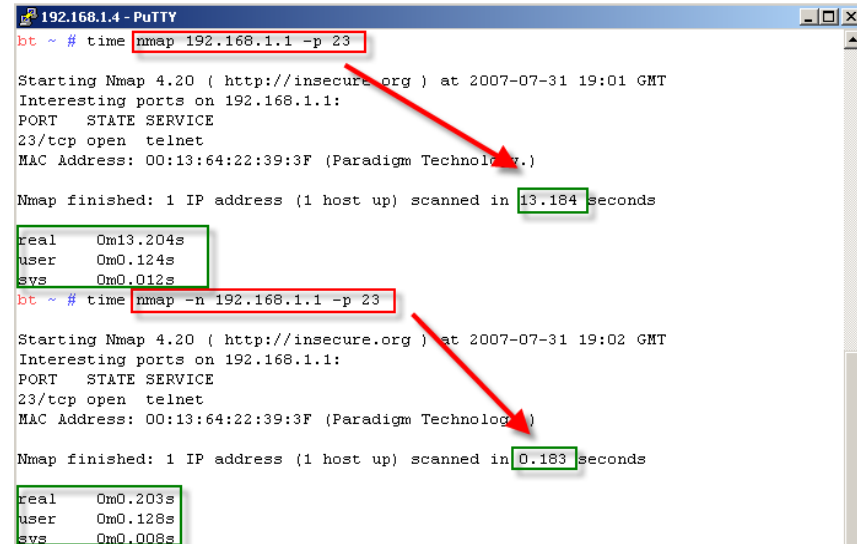
- Nmap'in çalışması için gerekli minimal koşullar
 - Taranacak Hedef Belirtme
 - Yetkili kullanıcı hesabı

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>nmap 192.168.2.1
Starting Nmap 4.76 ( http://nmap.org ) at 2009-04-04 17:02 GTB Daylight Time
Interesting ports on RI (192.168.2.1):
Not shown: 995 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
1050/tcp  open  java-or-OTGfileshare
MAC Address: 00:1A:2A:A7:22:5C (Arcadyan Technology)
Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
C:\Documents and Settings\A
```

Default port listesine göre tarama yapar.

Nmap Tarama Adımları

- Nmap'in her tarama öncesi izlediği yol
 - **1) Verilen hedef host ismi is IP karşılığını bulur, IP ise reverse dns sorgusu ile isim karşılığını bulmaya çalışır. Reverse sorgulama gerekli değil ise -n parametresi ile iptal edilebilir.**
 - Bunun farkını nmap'in tarama sonuçlarından görebilir ya da daha hassas bir sonuç verecek olan UNIX time komutu ile rahatlıkla ölçebiliriz.



```
192.168.1.4 - PuTTY
bt ~ # time nmap 192.168.1.1 -p 23

Starting Nmap 4.20 ( http://insecure.org ) at 2007-07-31 19:01 GMT
Interesting ports on 192.168.1.1:
PORT      STATE SERVICE
23/tcp    open  telnet
MAC Address: 00:13:64:22:39:3F (Paradigm Technology)

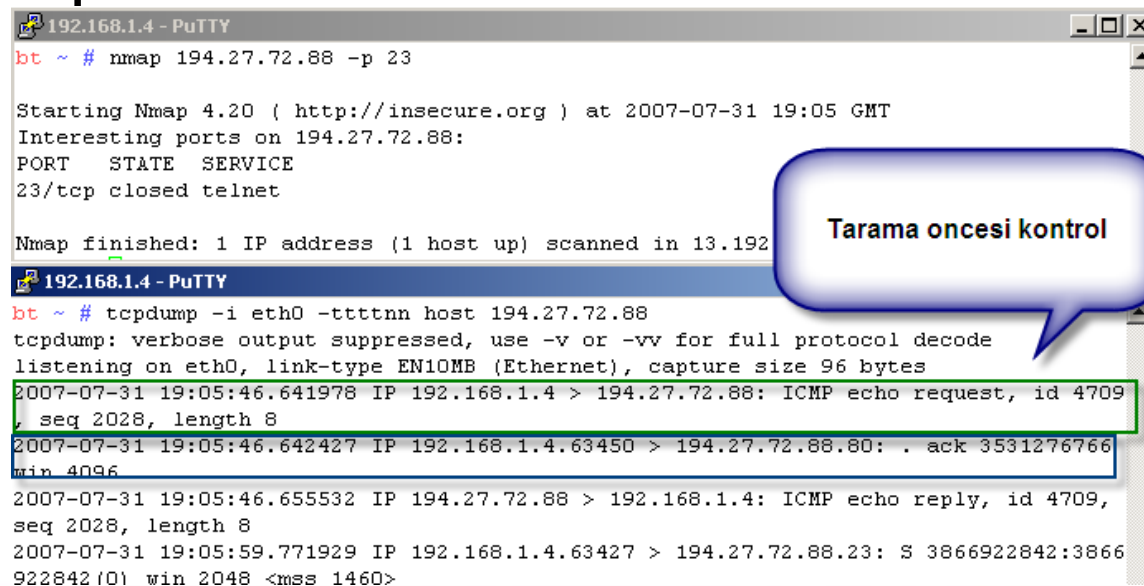
Nmap finished: 1 IP address (1 host up) scanned in 13.184 seconds
real    0m13.204s
user    0m0.124s
sys     0m0.012s
bt ~ # time nmap -n 192.168.1.1 -p 23

Starting Nmap 4.20 ( http://insecure.org ) at 2007-07-31 19:02 GMT
Interesting ports on 192.168.1.1:
PORT      STATE SERVICE
23/tcp    open  telnet
MAC Address: 00:13:64:22:39:3F (Paradigm Technology)

Nmap finished: 1 IP address (1 host up) scanned in 0.183 seconds
real    0m0.203s
user    0m0.128s
sys     0m0.008s
```

Nmap Tarama Adımları-II

- Hedef sistemi taramadan ayakta mı diye kontrol eder.
- Öntanımlı olarak bunu icmp paketleri ve hedef sistemin 80 TCP portuna SYN, ACK bayraklı paket göndererek yapar. Bu işlem nmap'e -PN parametresi verilerek iptal edilebilir.



```
192.168.1.4 - PuTTY
bt ~ # nmap 194.27.72.88 -p 23

Starting Nmap 4.20 ( http://insecure.org ) at 2007-07-31 19:05 GMT
Interesting ports on 194.27.72.88:
PORT      STATE SERVICE
23/tcp    closed telnet

Nmap finished: 1 IP address (1 host up) scanned in 13.192s

192.168.1.4 - PuTTY
bt ~ # tcpdump -i eth0 -ttttnn host 194.27.72.88
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
2007-07-31 19:05:46.641978 IP 192.168.1.4 > 194.27.72.88: ICMP echo request, id 4709
, seq 2028, length 8
2007-07-31 19:05:46.642427 IP 192.168.1.4.63450 > 194.27.72.88.80: . ack 3531276766
win 4096
2007-07-31 19:05:46.655532 IP 194.27.72.88 > 192.168.1.4: ICMP echo reply, id 4709,
seq 2028, length 8
2007-07-31 19:05:59.771929 IP 192.168.1.4.63427 > 194.27.72.88.23: S 3866922842:3866
922842(0) win 2048 <mss 1460>
```

Tarama öncesi kontrol

Nmap ile Port Tarama Çeşitleri

- Nmap 15 farklı tarama çeşidini destekler
- Ek olarak kendi tarama türlerinizi(TCP bayrakları ile) oluşturmanıza da fırsat verir.

Nmap Scan	Command Syntax	Requires Privileged Access	Identifies TCP Ports	Identifies UDP Ports
TCP SYN Scan	-sS	YES	YES	NO
TCP connect() Scan	-sT	NO	YES	NO
FIN Scan	-sF	YES	YES	NO
Xmas Tree Scan	-sX	YES	YES	NO
Null Scan	-sN	YES	YES	NO
Ping Scan	-sP	NO	NO	NO
Version Detection	-sV	NO	NO	NO
UDP Scan	-sU	YES	NO	YES
IP Protocol Scan	-sO	YES	NO	NO
ACK Scan	-sA	YES	YES	NO
Window Scan	-sW	YES	YES	NO
RPC Scan	-sR	NO	NO	NO
List Scan	-sL	NO	NO	NO
Idlescan	-sI	YES	YES	NO
FTP Bounce Attack	-b	NO	YES	NO

Nmap ile Host Keşfi

- IP/ICMP Ping
 - Nmap -sP
- TCP SYN/ACK Syn Ping
 - Nmap -PS -p 80
- UDP ping
- Yerel ağlar için ARP scan özelliği
 - Nmap -PR
 - Yerel ağlar için default

Nmap ile TCP Port Taramaları

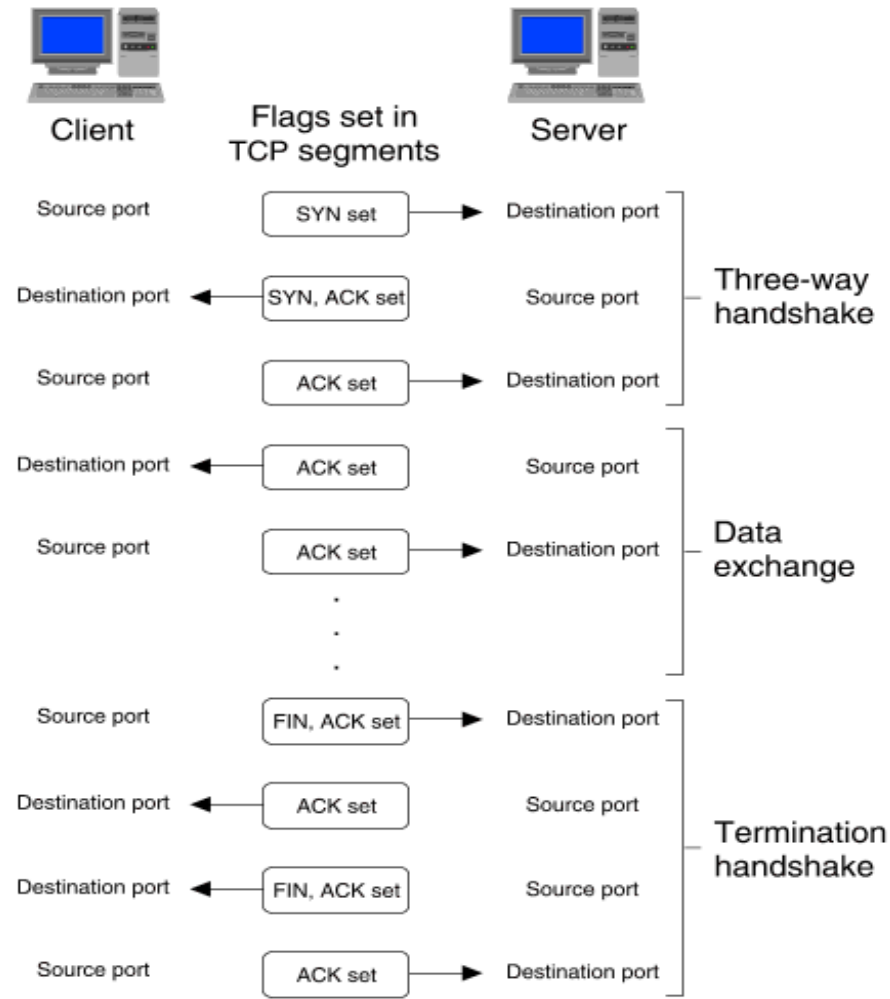
- TCP port taramaları TCP başlığında bulunan bayrak bilgilerine(Control Flags/Communication Flgags) göre yapılır.
- Güvenilir sonuç verir
- Hedef sistemin
 - İşletim sistemi
 - Uptime süresi
 - TCP Seq numara tahmin durumuBilgileri tcp taramalarda elde edilebilir...

Source Port				Destination Port				
Sequence Number								
Acknowledgment Number								
Data Offset	Reserved	URG	ACK	PSH	RST	SYN	FIN	Window
Checksum				Urgent Pointer				
Options				Padding				

TCP Bayrakları -Hatırlatma

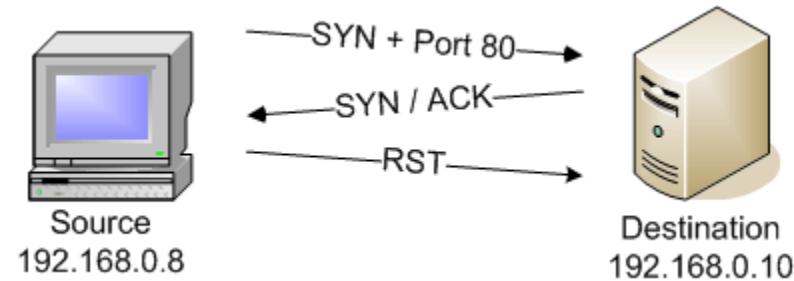
- **Synchronize** - also called "SYN"
 - Used to initiate a connection between hosts.
- **Acknowledgement** - also called "ACK"
 - Used in establishing a connection between hosts
- **Push** - "PSH"
 - Instructs receiving system to send all buffered data immediately
- **Urgent** - "URG"
 - States that the data contained in the packet should be processed immediately
- **Finish** - also called "FIN"
 - Tells remote system that there will be no more transmissions
- **Reset** - also called "RST"
 - Also used to reset a connection.

TCP Oturum Kurulumu/Bitirimi

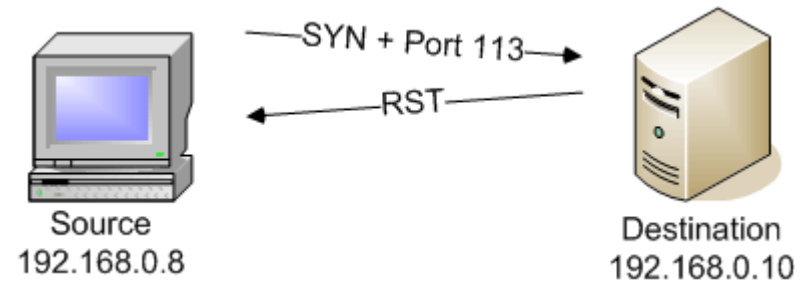


TCP SYN Scan(-sS)

- Hedef sisteme SYN bayraklı TCP paketi gönderilir ve cevap beklenir. Cevap için üç seçenek vardır:
- **SYN/ACK** Portun açık olduğunu belirtir. Nmap bu cevabı aldıktan sonra RST ile bağlantıyı sonlandırır (RST paketini Nmap değil, OS gönderir)



- **RST** Hedef sistem RST cevabı döndürürse portun kapalı olduğuna karar verilir.



- **Cevap Gelmeme Durumu** : Bu durumda Hedef sistemin önünde bir güvenlik duvarı vardır ve paketleri DROP/DENY edecek şekilde ayarlanmıştır yani kapalı port için RST cevabı göndermez. Filtered durumu.

TCP Syn Scan Uygulaması

- Nmap -P0 -sS ...
- Taramaları tcpdump ile izleme
- Taramaları -packet_trace ile izleme

Tarama Detaylarını İzleme

- Nmap port tarama yaparken tcpdump ile gelen-giden paketler incelenerek taramaya ait detay bilgi edinilebilir(--packet_trace seçeneği)
 - Tarama neden uzun sürüyor?
 - Neden istediğim sonuçları bulamıyor
 - Arada başka router/firewall mu paketleri engelliyor?
 - ...

```
root@bt:~# nmap -p 22 localhost --packet_trace
Starting Nmap 5.00 ( http://nmap.org ) at 2010-03-12 15:44 EST
SENT (0.0660s) TCP 127.0.0.1:62497 > 127.0.0.1:22 S ttl=54 id=669 iplen=44 seq=33549
RCVD (0.0660s) TCP 127.0.0.1:62497 > 127.0.0.1:22 S ttl=54 id=669 iplen=44 seq=33549
RCVD (0.0660s) TCP 127.0.0.1:22 > 127.0.0.1:62497 SA ttl=64 id=0 iplen=44 seq=146380
Interesting ports on localhost (127.0.0.1):
PORT      STATE SERVICE
22/tcp    open  ssh
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

TCP Connect Scan(-sT)

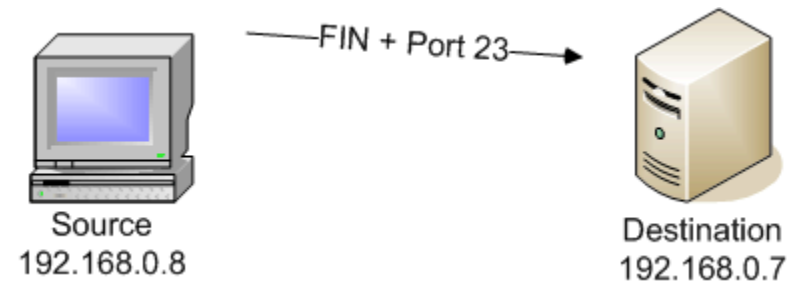
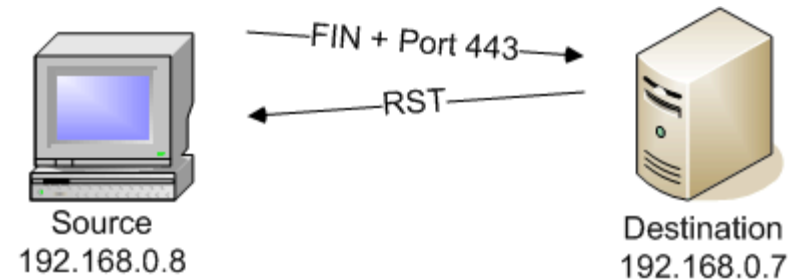
- Bu tarama tipi klasik TCP oturumu kurmaya çalışır
- İşletim sistemi metodları kullanılarak yapılan bu tarama tipi için herhangi bir ek hak gerekmez
- Sistem üzerindeki her kullanıcı bu tarama tipini kullanabilir.
- Bu tarama tipinin dezavantajı çoğu güvenlik sistemi tarafından loglanmasıdır.*

Nmap TCP Connect Scan Uygulaması

- Nmap -P0 -sT ...

TCP FIN Scan(-sF)

- Hedef sisteme FIN bayraklı TCP paketleri gönderilerek;
- Kapalı portları için RST bayraklı paket beklenir.



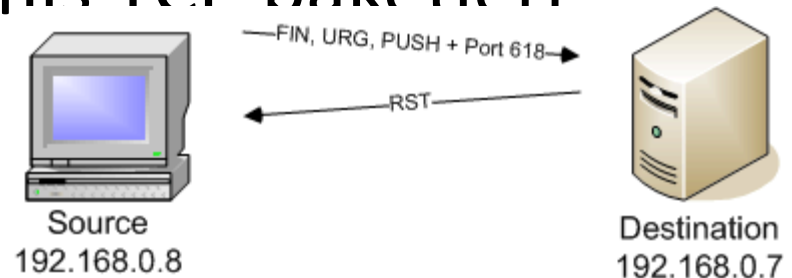
- Açık olan portlar bu tarama tipine cevap dönmez

TCP Null Scan(-sN)

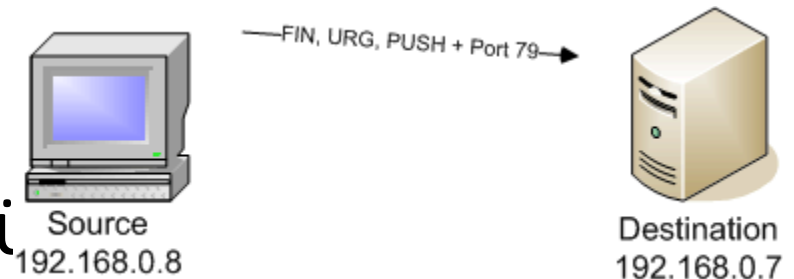
- Hedef TCP portuna herhangi bir bayrak set edilmemiş TCP paketleri gönderilir.
 - Yine kapalı portlar için RST bayraklı TCP paketi beklenir.
 - Açık portlar için herhangi bir cevap dönmemesi beklenir.

XMAS Scan(-sX)

- XMAS tarama tipi hedef sisteme FIN, URG ve PUSH bayrakları set edilmiş TCP paketleri gönderilir:



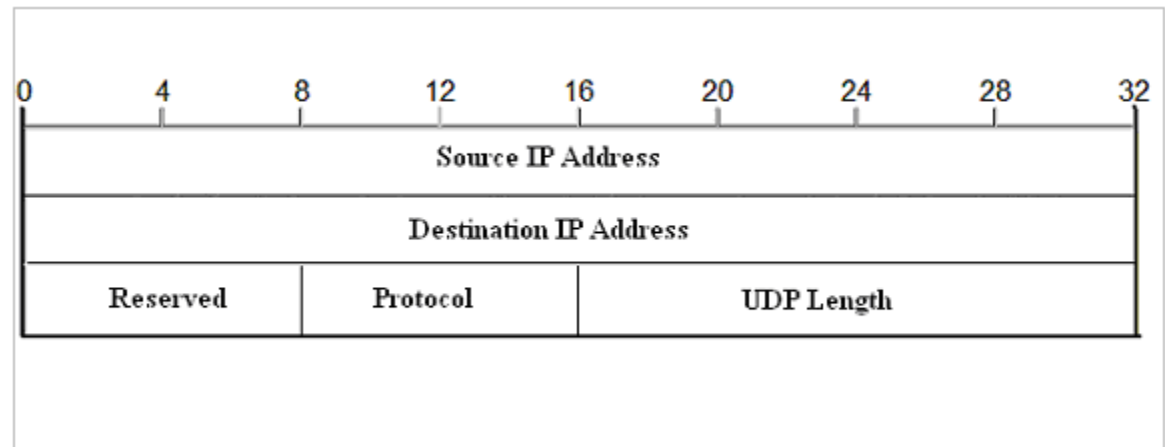
- Kapalı portlar için RST



- Açık portlar için cevap dön

Nmap ile UDP Port Taramaları

- UDP'de TCP benzeri hata kontrolü yoktur.
- Hata kontrolü alt protokol ICMP tarafından gerçekleştirilir.
- UDP port taramalarında başlık bilgilerindeki port alanı kullanılır



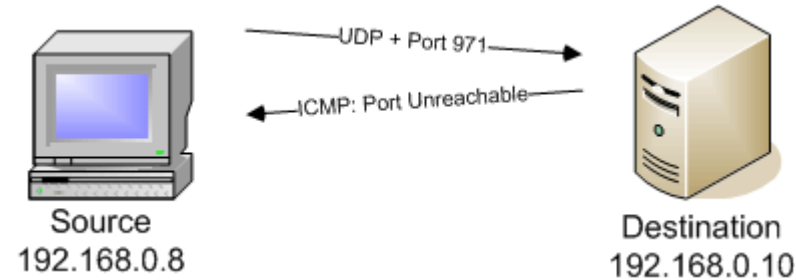
Nmap ile UDP Port Taramaları-II

- Nmap de UDP taramaları için `-sU` parametresi kullanılır.
- UDP tarama türü TCP'ye göre biraz daha basit ama daha az güvenilirdir.
- UDP Taramalarda Versiyon taraması yapılmazsa sonuçlar güvenilir olmayacaktır.
 - Taranacak UDP portlara uygun protokol bilgisi içeren veri koyulması gerekir
 - `#nmap -sU -sV` şeklinde tarama yapılmalıdır

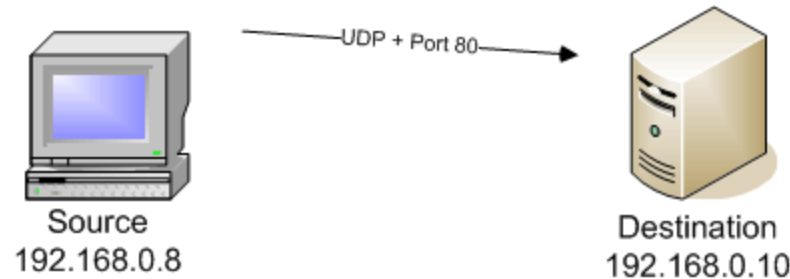
Nmap ile UDP Port Taramaları-III

- RFC'ye göre

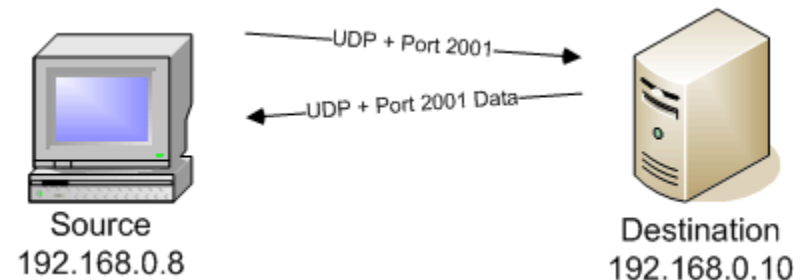
- Kapalı Portlar için: (ICMP Port Unreachable paketi)



- Açık Portlar için:
Cevap dönülmez

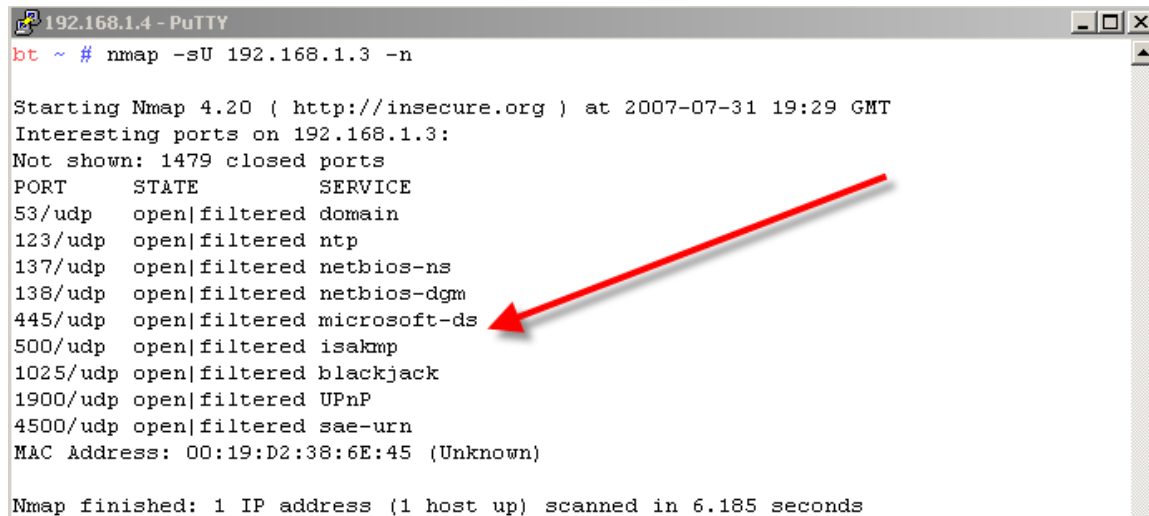


- Ya da ilgili porta istek yapan uygulamaya cevap dönülür (DNS istek ve Cevapları)



UDP Taramalarında Sıkıntı

- Tarama yapılan host'un göndereceği ICMP mesajları filtrelenmiş ise bazı tarama programları o UDP portunu açık olarak gösterecektir.
- Nmap cevap dönmeyen icmp mesajlarından o portun açık ya da filtrelenmiş olduğunu söyler.



```
192.168.1.4 - PuTTY
bt ~ # nmap -sU 192.168.1.3 -n

Starting Nmap 4.20 ( http://insecure.org ) at 2007-07-31 19:29 GMT
Interesting ports on 192.168.1.3:
Not shown: 1479 closed ports
PORT      STATE      SERVICE
53/udp    open|filtered domain
123/udp   open|filtered ntp
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
445/udp   open|filtered microsoft-ds
500/udp   open|filtered isakmp
1025/udp  open|filtered blackjack
1900/udp  open|filtered UPnP
4500/udp  open|filtered sae-urn
MAC Address: 00:19:D2:38:6E:45 (Unknown)

Nmap finished: 1 IP address (1 host up) scanned in 6.185 seconds
```

UDP Tarama Uygulaması

```
root@bt:~# nmap localhost -sU -sV --top-ports 100

Starting Nmap 5.00 ( http://nmap.org ) at 2010-03-12 15:12
Interesting ports on localhost (127.0.0.1):
Not shown: 98 closed ports
PORT      STATE      SERVICE VERSION
68/udp    open|filtered dhcpcd
514/udp   open|filtered syslog

Service detection performed. Please report any incorrect results.
Nmap done: 1 IP address (1 host up) scanned in 56.38 seconds
root@bt:~#
```

Versiyon Belirleme

- Klasik port taramalarda amaç portun durumunu öğrenme
 - Port 80 Open | Closed
- Versiyon belirlemede amaç: ilgili port üzerinde çalışan uygulamayı belirleme
 - Port 80
 - HTTP
 - Apache
 - » 1.3.27 version
- Daha sağlıklı sonuçlar almak için kullanılır
 - UDP taramalar için vazgeçilmez
- Nmap versiyon belirleme konusunda en iyi araçlardan.

Versiyon Tarama Örnekleri

- TCP Servisleri için
- UDP servisleri için

İşletim Sistemi Belirleme



İşletim Sistemi Belirleme-Nmap

- Hedef sisteme çeşitli paketler göndererek sonuçlarını bir veritabanı ile karşılaştırılır
- Sağlıklı sonuç için bir açık bir kapalı port gerekir.

```
[root@netdos1 ~]# nmap -O hackme.lifeoverip.net

Starting Nmap 5.00 ( http://nmap.org ) at 2010-03-12 21:32 EET
sendto in send_ip_packet: sendto(4, packet, 44, 0, 91.93.119.77, 16) => Operation n
Offending packet: TCP 212.88.220.212:47933 > 91.93.119.77:80 S ttl=55 id=30424 iplen=40
Interesting ports on host-91-93-119-77.teletelekom.com (91.93.119.77):
Not shown: 995 closed ports
PORT      STATE      SERVICE
22/tcp    filtered  ssh
23/tcp    open       telnet
80/tcp    open       http
443/tcp   open       https
3306/tcp  open       mysql
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.26
Network Distance: 6 hops

OS detection performed. Please report any incorrect results at http://nmap.org/subm
Nmap done: 1 IP address (1 host up) scanned in 325.43 seconds
```


İşletim Sistemi Belirleyememe

- Nmap bir açık bir kapalı port bulamazsa işletim sistemi belirleyemez
- İşletim sistemini belirleyemediği durumlarda genellikle tarama yapan sistemin bilgilerini ekrana basar

```
Increasing ports on www.cdnkci.com.tr (212.252.160.123).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE  
80/tcp    open  http  
443/tcp   open  https  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose  
Running (JUST GUESSING) : FreeBSD 6.X (85%)  
Aggressive OS guesses: FreeBSD 6.2-RELEASE (85%)  
No exact OS matches for host (test conditions non-ideal).
```

Tarama Opsiyonlarını Birleştirme

- Tarama seçeneklerini unutanlar için ideal tarama tipi
- Nmap -A localhost
- -A= -sV -sC -O -

```
root@home-labs:~  
root@home-labs:~# nmap -A mail02.lifeoverip.net  
Starting Nmap 4.85BETA7 ( http://nmap.org ) at 2009-04-16 14:15 EDT  
Interesting ports on mail02.lifeoverip.net (91.93.119.80):  
Not shown: 990 closed ports  
PORT      STATE SERVICE      VERSION  
22/tcp    open  ssh          OpenSSH 5.1p1 (FreeBSD 20080901; protocol 2.0)  
|_ ssh-hostkey: 1024 e2:28:d8:ae:48:b9:e4:9e:89:c7:99:29:bc:10:a8:49 (DSA)  
23/tcp    filtered telnet  
25/tcp    open  smtp         Access Remote PC smtpd  
|_ smtp-commands: EHLO mail.sistenbil.com, AUTH LOGIN CRAM-MD5 PLAIN, AUTH=LOGIN CRAM-MD5 PLAIN, PIPELINING, 8BITMIME  
|_ HELP qmail home page: http://pobox.com/~djb/qmail.html  
80/tcp    open  http         Apache httpd 2.2.9 ((FreeBSD))  
|_ html-title: Webmail Service - Giriş  
|_ Requested resource was http://mail02.lifeoverip.net/src/login.php  
110/tcp   open  pop3         qmail pop3d  
|_ pop3-capabilities: capa APOP  
143/tcp   open  imap         Dovecot imapd (SASL enabled)  
161/tcp   filtered snmp  
587/tcp   open  smtp         Access Remote PC smtpd  
|_ smtp-commands: EHLO mail.sistenbil.com, AUTH LOGIN CRAM-MD5 PLAIN, AUTH=LOGIN CRAM-MD5 PLAIN, PIPELINING, 8BITMIME  
|_ HELP qmail home page: http://pobox.com/~djb/qmail.html  
1720/tcp  filtered H.323/Q.931  
3306/tcp  filtered mysql  
Device type: general purpose|firewall|router|WAP  
Running (JUST GUESSING) : FreeBSD 7.X|6.X (95%), m0n0wall FreeBSD (90%), Juniper JUNOS 9.X (88%), Apple embedded (86%), Apple Mac OS X 10.4.X (85%)  
Aggressive OS guesses: FreeBSD 7.0-RELEASE (95%), FreeBSD 7.1-PRERELEASE (91%), m0n0wall 1.3b11 - 1.3b15 FreeBSD-based firewall (90%), FreeBSD 7.0-STABLE (89%), FreeBSD 7.0-RC1 (88%), FreeBSD 6.2-RELEASE (88%), Juniper Networks JUNOS 9.0R2.10 (88%), Apple Airport Extreme WAP v7.3.2 (86%), Apple Mac OS X 10.4.10 (Tiger) (Darwin 8.10.0, PowerPC) (85%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 9 hops  
Service Info: Host: mail.sistenbil.com; OSs: FreeBSD, Windows  
  
TRACEROUTE (using port 8080/tcp)  
HOP RTT ADDRESS  
1 1.01 RT (192.168.2.1)  
2 12.13 ds1.static85961861.ttnet.net.tr (85.96.186.1)  
3 ...  
4 11.75 81.212.31.153  
5 11.03 81.212.25.173  
6 12.56 gayrettepe_t2_1-gayt1_2_.turktelekom.com.tr (81.212.28.122)  
7 239.31 gayrettepe_t3_2-gayrettepe_t2_1.turktelekom.com.tr (212.156.110.18)  
8 11.64 195.175.51.218  
9 25.24 84.51.1.98  
10 12.53 mail02.lifeoverip.net (91.93.119.80)  
  
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 70.08 seconds
```

Sık Kullanılan Portları Tarama

- Bir IP Adresi için
 - TCP ve UDP protokollerinin her biri için 65535 port olasılığı var.
 - Tüm portları taramak zaman kaybı olur.
 - Nmap soc projesi:-top 10, top 100, top 1000 port değerleri

<i>TCP</i>	<i>UDP</i>
1. 80	1. 137
2. 23	2. 161
3. 22	3. 1434
4. 443	4. 123
5. 3389	5. 138
6. 445	6. 445
7. 139	7. 135/
8. 21	8. 67
9. 135	9. 139
10. 25	10. 53

Top 10 Portun Taranması

- Taramalarda bu özelliği kullanmak için
–top-ports 10 ya da –top-ports 1000 parametreleri kullanılabilir.

```
root@bt:~# nmap localhost -sT --top-ports 10
Starting Nmap 5.00 ( http://nmap.org ) at 2010-03-12 15:39 EST
Interesting ports on localhost (127.0.0.1):
PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    open  ssh
23/tcp    closed telnet
25/tcp    closed smtp
80/tcp    open  http
110/tcp   closed pop3
139/tcp   closed netbios-ssn
443/tcp   closed https
445/tcp   closed microsoft-ds
3389/tcp  closed ms-term-serv
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

Tarama Sonuçlarının Sebebi(--reason)

UDP Taraması için Sonuç Değerleri

```
root@bt:~# nmap -p 22,68,514 -sU -sV --reason localhost
Starting Nmap 5.00 ( http://nmap.org ) at 2010-03-12 15:41
Interesting ports on localhost (127.0.0.1):
PORT      STATE      SERVICE    REASON      VERSION
22/udp    closed     ssh        port-unreach
68/udp    open|filtered dhcpd      no-response
514/udp    open|filtered syslog     no-response

Service detection performed. Please report any incorrect r
```

TCP Taraması için Sonuç Değerleri

```
root@bt:~# nmap -p 22,23 -sT --reason localhost
Starting Nmap 5.00 ( http://nmap.org ) at 2010-03-12
Interesting ports on localhost (127.0.0.1):
PORT      STATE      SERVICE    REASON
22/tcp    open       ssh        syn-ack
23/tcp    closed     telnet     conn-refused

Nmap done: 1 IP address (1 host up) scanned in 0.07 s
```

Nmap ile Traceroute

- Nmap bir port üzerinde TCP ya da UDP protokolünü kullanarak traceroute yapabilir.
- Klasik traceroute programları UDP ve ICMP kullanır.
 - UDP kullananlarda hedef port numarası değiştirme seçeneği yoktur ve genellikle traceroute tarafından kullanılan yüksek numaralı UDP portları kapalıdır
- Nmap ile hem UDP hem de TCP üzerinden trace çıktısı alınabilir
- Nmap traceroute özelliği istenilen UDP, TCP portuna seçilerek yapılabilir

Nmap Traceroute Örnek

```
root@bt:~# traceroute www.microsoft.com
traceroute to www.microsoft.com (207.46.19.190), 30 hops
 1 192.168.1.1 (192.168.1.1) 0.716 ms 1.027 ms 1.174 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
```

Klasik traceroute aracı

Nmap
traceroute

```
[root@mail ~]# nmap -p 80 www.microsoft.com --traceroute -PN
Starting Nmap 4.68 ( http://nmap.org ) at 2010-03-12 22:42 EET
Interesting ports on wwwco1vip.microsoft.com (65.55.21.250):
 80/tcp open  http

CEROUTE (using port 80/tcp)
  RTT  ADDRESS
 1  0.66  router.lifeoverip.net (91.93.119.65)
 2  2.00  84.51.1.153
 3  5.20  static.turktelekom.com.tr (212.156.145.117)
 4  3.36  gayrettepe-t2-2-besiktas-t3-1.turktelekom.com.tr (212.156.
 5  2.67  gayt1-2-gayrettepe-t2-2.turktelekom.com.tr (212.156.252.19
 6  3.19  acb-t1-2-gayt1-2-x.turktelekom.com.tr (81.212.25.18)
 7  4.99  static.turktelekom.com.tr (212.156.118.214)
 8  62.52  amsterdam-1--acb-t2-1.turktelekom.com.tr (212.156.102.9)
 9  64.24  146.82.55.17
10 150.22  MSN-HOTMAIL.TenGigabitEthernet4-2.ar6.NYC1.gblx.net (64.21
11 311.02  wwwco1vip.microsoft.com (65.55.21.250)
```

Nmap Taramalarını Karşılaştırma

- Aynı hedefe yapılan iki taramanın sonuçlarını karşılaştırmak için kullanılır.
- Host sayısı yüksek ağlarda envanter çalışması

```
root@home-labs:~# nmap localhost -oX test1
```

```
Starting Nmap 4.85BETA7 ( http://nmap.org ) at 2009-04-16 14:22 EDT
Warning: Hostname localhost resolves to 2 IPs. Using 127.0.0.1.
Interesting ports on localhost (127.0.0.1):
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
5432/tcp   open  postgresql
```

```
root@home-labs:~# nmap localhost -oX test2
```

```
Starting Nmap 4.85BETA7 ( http://nmap.org ) at 2009-04-16 14:23 EDT
Warning: Hostname localhost resolves to 2 IPs. Using 127.0.0.1.
Interesting ports on localhost (127.0.0.1):
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3306/tcp   open  mysql
5432/tcp   open  postgresql
```

```
root@home-labs:~# ndiff --text test1 test2
```

```
Thu Apr 16 14:22:10 2009 -> Thu Apr 16 14:23:04 2009
localhost (127.0.0.1):
  -80/tcp closed
  +80/tcp open http
  -3306/tcp closed
  +3306/tcp open mysql
```


Bölüm-X:Nmap Scripting Engine

Zayıflık Tarama Aracı Olarak Nmap

- NSE(Nmap Script Engine) desteğiyle birlikte Nmap port taramanın ötesinde çeşitli güvenlik zayıflıklarını tarayabilir hale geldi.
- NSE çeşitli LUA scriptlerinden oluşur ve isteyen herkes tarafından geliştirilebilir.
- NSE ile ilgili Nmap parametreleri
 - *SCRIPT SCAN:*
 - *-sC: equivalent to `-script=safe,intrusive`*
 - *`-script=<Lua scripts>`: `<Lua scripts>` is a comma separated list of directories, script-files or script-categories*
 - *`-script-args=<n1=v1,[n2=v2,...]>`: provide arguments to scripts*
 - *`-script-trace`: Show all data sent and received*
 - *`-script-updatedb`: Update the script database.*

Temel NSE Kullanımı

- NSE'i test etmek için en basitinden -sC parametresi kullanılabilir.

```
# nmap -P0 -sC -p 21,22,23,25,80,3306 mail.lifeoverip.net

Starting Nmap 4.60 ( http://nmap.org ) at 2009-01-12 20:47 GMT
Interesting ports on mail.lifeoverip.net (80.93.212.86):
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    closed telnet
25/tcp    open  smtp
| SMTP: Responded to EHLO command
| mail.sistembil.com
| AUTH LOGIN CRAM-MD5 PLAIN
| AUTH=LOGIN CRAM-MD5 PLAIN
| PIPELINING
| 250 8BITMIME
| Responded to HELP command
| _qmail home page: http://pobox.com/~djb/qmail.html
80/tcp    open  http
| _ HTML title: 302 Found
3306/tcp  open  mysql
| MySQL Server Information: MySQL Error detected!
| Error Code was: 1130
| _ Host '85.96.187.185' is not allowed to connect to this MySQL server
Nmap done: 1 IP address (1 host up) scanned in 6.237 seconds
```

NSE ve Versiyon Tarama

- NSE kullanırken `-sV` parametresini kullanmak sonuçların daha güvenilir olmasını sağlar
 - Farklı bir portta çalışan uygulamayı ancak versiyon belirleme yaparak ortaya çıkarabiliriz.

99.Portta çalışan
SSH

```
root@bt:~# nmap localhost -p 99 -sC

Starting Nmap 5.00 ( http://nmap.org ) at 2010-03-12 15:18 EST
Interesting ports on localhost (127.0.0.1):
PORT      STATE SERVICE
99/tcp    open  metagram

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
root@bt:~#
```

99.Portta Çalışan
SSH

```
root@bt:~# nmap localhost -p 99 -sV -sC

Starting Nmap 5.00 ( http://nmap.org ) at 2010-03-12 15:17 EST
Interesting ports on localhost (127.0.0.1):
PORT      STATE SERVICE VERSION
99/tcp    open  ssh      OpenSSH 5.1p1 Debian 3ubuntu1 (protocol 2.0)
|_ ssh-hostkey: 1024 dc:b3:e2:09:8b:2a:84:1b:42:cb:1f:2a:14:76:66:45
|_ 2048 23:10:41:2f:62:c6:a5:30:3d:a6:6d:e9:a6:81:83:1a (RSA)
Service Info: OS: Linux
```

Örnek NSE Kullanımları

Anonim ftp destekleyen sistemlerin bulunması

```
# nmap -P0 -p 21 --script anonFTP.nse ftp.linux.org.tr
```

```
Starting Nmap 4.60 ( http://nmap.org ) at 2009-01-12 20:55 GMT  
Interesting ports on ftp.linux.org.tr (193.140.100.100):  
PORT STATE SERVICE  
21/tcp open ftp  
|_ Anonymous FTP: FTP: Anonymous login allowed  
Nmap done: 1 IP address (1 host up) scanned in 0.152 seconds
```

Hedef sistemin SSLV2 desteklediğini öğrenmek

```
# nmap -P0 -p 443 --script SSLv2-support blog.lifeoverip.net
```

```
Starting Nmap 4.60 ( http://nmap.org ) at 2009-01-12 20:57 GMT  
Interesting ports on mail.lifeoverip.net (80.93.212.86):  
PORT STATE SERVICE  
443/tcp open https  
| SSLv2: server still supports SSLv2  
| SSL2_DES_192_EDE3_CBC_WITH_MD5  
| SSL2_RC2_CBC_128_CBC_WITH_MD5  
| SSL2_RC4_128_WITH_MD5  
| SSL2_RC4_64_WITH_MD5  
| SSL2_DES_64_CBC_WITH_MD5  
| SSL2_RC2_CBC_128_CBC_WITH_MD5  
|_ SSL2_RC4_128_EXPORT40_WITH_MD5  
Nmap done: 1 IP address (1 host up) scanned in 0.114 seconds
```

Nmap NSE ile DNS Cache Poisoning Testi

- Dns cache poisoning açıklığını test etmek için hedef sistemde iki değer kontrol edilir:
 - Birincisi dns sorgulamalarında kaynak portun değiştirilmesi.
 - İkincisi dns sorgularındaki TXID değerinin yeteri kadar random/rastgele olmasının kontrolü.
- Kaynak port rastgeleliği testi
 - **# nmap -P0 -sU -p 53 --script dns-random-srcport 100.100.100.2 -vv**
- Txid üreticinin tahmin edilebilirlik testi
 - **nmap -P0 -sU -p 53 --script dns-random-txid 100.100.100.2 -vv**
- Her iki testi de tek bir Nmap taraması ile gerçekleştirmek için scriptler arasına “,” koyulması yeterli olacaktır.

Nmap NSE ile Conficker Wormu Tespit Etme

- MS08-067, Windows RPC vulnerability
- Nmap **smb-check-vulns.nse** scripti
- Kullanımı:

```
nmap --script smb-check-vulns.nse -p445 <host>
```

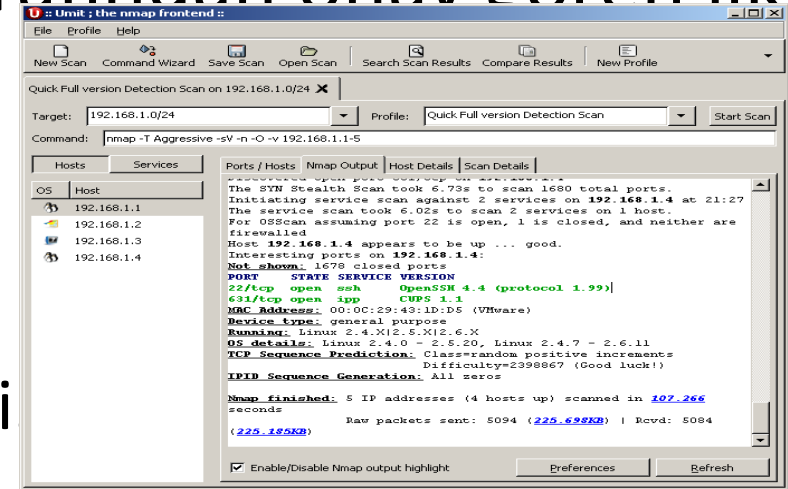
```
nmap -sU -sS --script smb-check-vulns.nse -p U:137,T:139 <host>
```
- Örnek Çıktı:
Host script results:
| smb-check-vulns:
| MS08-067: FIXED
| Conficker: Likely INFECTED
|_ regsvc DoS: VULNERABLE

Tarama Sonuçlarının Raporlanması

- Tarama çıktılarının dosyaya yazdırılması
- Raporlama Çeşitleri XML, HTML
- Kolay parse edilebilir formatta çıktı üretme
- Veritabanına aktarma

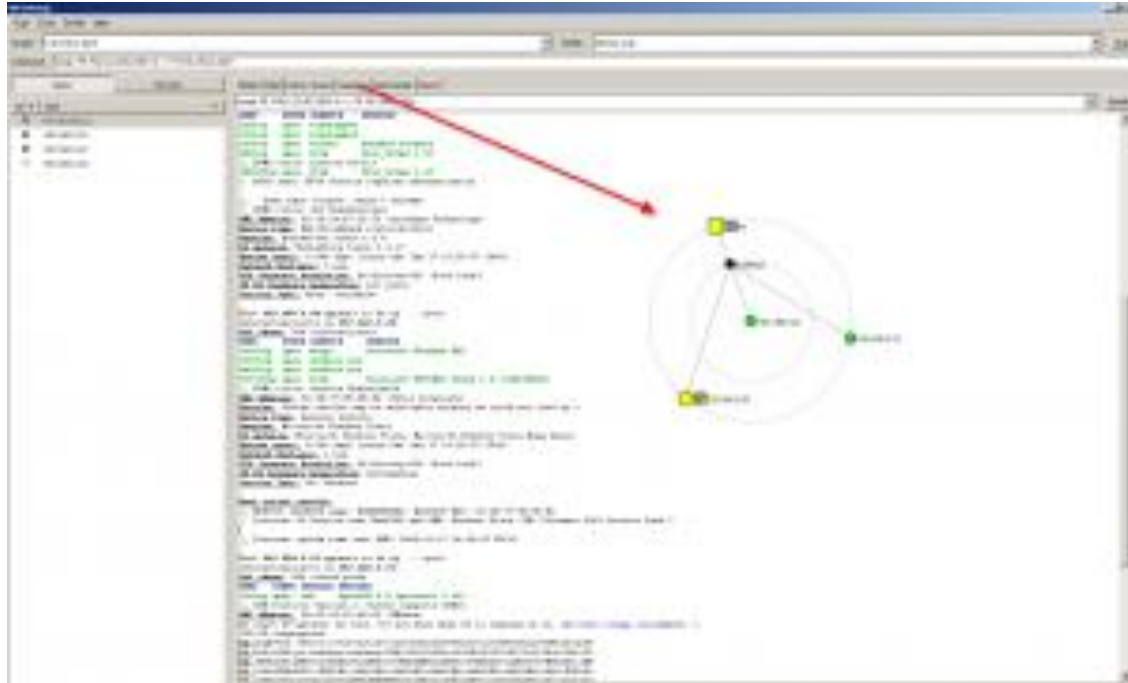
Nmap Grafik Arabirim Kullanımı

- Nmap komut satırı düşünülerek yazılmış bir uygulamadır.
- Ara ara grafik arabirimi denemeleri yapılmış fakat genel kullanıma sahip bir arabirim üzerinde anlaşılamadı.
- Nmap yazarı ve komuniti tarafından onay gören ilk deneme:Umit
- Google SOC Projesi
- Nmap 4.5 ile birlikte
 - Zenmap olarak isim değiştirdi



Nmap Grafik Arabirimi:Zenmap

- Nmap 4.5 sürümü ile birlikte artık **resmi** bir Grafik arabirimine sahip olmuştur.
- Komut satırından kullanılan tüm özellikler ve daha fazlası Zenmap ile birlikte gelmektedir.



Port Taramaları ve IDS Sistemleri

- Eğer IDS/IPS sistemi düzgün yapılandırıldıysa port taramalarını kolaylıkla yakalayacaktır.

Hping ile Port Tarama

```
#hping -FUP -n -p 22 192.168.1.4 -c 2

HPING 192.168.1.4 (eth0 192.168.1.4): FPU set, 40 headers + 0 data bytes

--- 192.168.1.4 hping statistic ---

2 packets tramitted, 0 packets received, 100% packet loss
```

Tarama Esnasında Snort(IDS)'e düşen Loglar

```
# tail -f /var/log/snort/alert
**U*P**F Seq: 0x5DDA5952 Ack: 0x3220A1A8 Win: 0x200 TcpLen: 20 UrgPtr: 0x0
[Xref => http://www.whitehats.com/info/IDS30]

[**] [1:1228:7] SCAN nmap XMAS [**]
[Classification: Attempted Information Leak] [Priority: 2]

07/12-20:41:07.953181 192.168.1.5:2165 -> 192.168.1.4:22
TCP TTL:64 TOS:0x0 ID:47151 IpLen:20 DgmLen:40
**U*P**F Seq: 0x6C47BC04 Ack: 0x736BEDAF Win: 0x200 TcpLen: 20 UrgPtr: 0x0
[Xref => http://www.whitehats.com/info/IDS30]
```

Syncookie ve Port Tarama-I

- Syncookie=Syn flood ddos saldırılarını engelleme amaçlı geliştirilmiş teknoloji
- Synproxy=synflood ddos saldırılarını engelleme amaçlı geliştirilmiş, syncookie benzeri fakat daha esnek bir teknoloji
- Syncookie arkasında koruma altına aldığı sistemlerdeki portların durumuna bakmaksızın gelen her SYN paketi için SYN/ACK cevabı döner
- Synproxy ile sadece belirli sistemlerin belirli portlarına synproxy özelliği eklenebilir

Syncookie ve Port Tarama-II

- Bu tip sistemlere yapılacak taramalarda tüm portlar açık gözükcektir.

Bu şekilde korunmuş sistemlere yönelik başarılı TCP taramaları gerçekleştirmek için 3'lü el sıkışmayı tamamlayan ve sonrasında ek paketler gönderen tarama tiplerini denemek gerekir. —sV gibi.

```
root@bt:~# nmap www.example.com-p80-100 -reason
```

```
Starting Nmap 5.00 ( http://nmap.org ) at 2010-02-14 12:09 EST  
Warning: Hostname www.example.com resolves to 5 IPs. Using 95.0.11.13.
```

PORT	STATE	SERVICE	REASON
80/tcp	open	http	syn-ack
81/tcp	open	hosts2-ns	syn-ack
82/tcp	open	xfer	syn-ack
83/tcp	open	mit-ml-dev	syn-ack
84/tcp	open	ctf	syn-ack
85/tcp	open	mit-ml-dev	syn-ack
86/tcp	open	mfcobol	syn-ack
87/tcp	open	priv-term-l	syn-ack
88/tcp	open	kerberos-sec	syn-ack
89/tcp	open	su-mit-tg	syn-ack
90/tcp	open	dnsix	syn-ack
91/tcp	open	mit-dov	syn-ack
92/tcp	open	npp	syn-ack
93/tcp	open	dcp	syn-ack
94/tcp	open	objcall	syn-ack
95/tcp	open	supdup	syn-ack
96/tcp	open	dixie	syn-ack
97/tcp	open	swift-rvf	syn-ack
98/tcp	open	linuxconf	syn-ack
99/tcp	open	metagram	syn-ack
100/tcp	open	newacct	syn-ack

```
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

Syncookie ve Port Tarama-III

- Versiyon belirleme taraması yapılırsa açık olan portlar rahatlıkla belirlenebilir.



#nmap -sV

```
root@bt:~# nmap www.example.com-PN -sV -top-ports 10
```

```
Starting Nmap 5.00 ( http://nmap.org ) at 2010-02-14 12:52 EST
```

```
Interesting ports on 11.22.33.44(11.22.33.44):
```

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

21/tcp	filtered	ftp	
--------	----------	-----	--

22/tcp	filtered	ssh	
--------	----------	-----	--

23/tcp	filtered	telnet	
--------	----------	--------	--

25/tcp	filtered	smtp	
--------	----------	------	--

80/tcp	open	http	Microsoft IIS webserver 7.0
--------	------	------	-----------------------------

110/tcp	filtered	pop3	
---------	----------	------	--

139/tcp	filtered	netbios-ssn	
---------	----------	-------------	--

443/tcp	filtered	https	
---------	----------	-------	--

445/tcp	filtered	microsoft-ds	
---------	----------	--------------	--

3389/tcp	filtered	ms-term-serv	
----------	----------	--------------	--

```
Service Info: OS: Windows
```

```
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 10.32 seconds
```

Nmap ile Performans Testleri

- Ağ ve güvenlik cihazlarının paket işleme kapasitesini test etme
 - Pps=packet per second
 - Fragmented paketleri geçirme
 - Badchecksum paketleri geçirme
- Nmap ile tarama yaparken saniyede şu kadar paket gönder diyebiliriz
- Bu özellik rate-limiting(saniyede belirli sayıdan fazla paket gönderen iplerin bloklanması)yapan sistemleri atlatma için de kullanılabilir
- --min-rate, --max-rate

Nmap --min-rate, --max-rate

- Saniyede 30.000 paket
65535 portu taraması
toplamda 2.7 saniye
sürmekte...

```
# time nmap --min-rate 30000 --max-rate 30000 localhost -vvv -PN  
-p1-65535
```

```
Starting Nmap 4.90RC2 ( http://nmap.org ) at 2009-12-26 11:56 EST  
Warning: Hostname localhost resolves to 2 IPs. Using 127.0.0.1.  
Initiating SYN Stealth Scan at 11:56  
Scanning localhost (127.0.0.1) [65535 ports]  
Completed SYN Stealth Scan at 11:56, 2.59s elapsed (65535 total ports)  
Host localhost (127.0.0.1) is up (0.0000080s latency).  
Scanned at 2009-12-26 11:56:26 EST for 3s  
Interesting ports on localhost (127.0.0.1):  
Not shown: 65525 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
587/tcp    open  submission  
953/tcp    open  rmdc  
5432/tcp  open  postgresql  
8118/tcp  open  privoxy  
9050/tcp  open  tor-socks  
  
Read data files from: /usr/local/share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 2.71 seconds  
Raw packets sent: 65555 (2.884MB) | Rcvd: 131083 (5.506MB)  
  
real    0m2.720s  
user    0m0.476s  
sys     0m0.948s
```

**saniyede 30.000
paket**