

BGA

BİLGİ GÜVENLİĞİ
AKADEMİSİ

www.bga.com.tr

Nmap Kullanım Kitapçığı

[Nmap El Kitabı]

Gökay Bekşen
gbeksen@bga.com.tr

[Bu kitapçık de fakto ağ keşif aracı Nmap'in son sürümünde bulunan özelliklerin detaylı kullanımını içermektedir.]

İçerik

Nmap.....	4
Nmap Çalışma Prensipleri	4
Nmap Hedef Belirtme Özelliği	6
Yetki Yükseltme	7
Sunucuları/İstemcileri Keşfetme	7
Tarama	8
Portların Taramalara Verebileceği Cevaplar	8
Tarama Türleri	9
TCP Syn Scan	9
TCP Connect Scan	11
FIN Scan	13
XMas Tree Scan.....	14
Null Scan.....	16
Ping Scan	17
Version Detection	18
UDP Scan	20
IP Protocol Scan	22
ACK Scan.....	24
Window Scan	26
RPC Scan	28
List Scan	31
IdleScan	31
FTP Bounce Scan	33
Nmap Ping Seçenekleri	34
ICMP Echo Request ve TCP ACK Ping	34
ICMP Echo Request Ping	34
TCP ACK Ping :.....	34
TCP SYN Ping :.....	35
UDP Ping.....	35
ICMP Timestamp Ping	35
ICMP Address Mask Ping.....	36
Don't Ping Before Scanning	36

Require Reverse DNS	36
Disable Reverse DNS	36
Ping Scan (Disable Port Scan)	37
Treat all hosts as online.....	37
OS İzi Belirleme.....	37
Os İzi Belirleme Seçenekleri.....	38
Nmap Script Motoru (Nmap Scripting Engine – NSE)	38
NSE Seçenekleri	40
Güvenlik Ürünleri ve Nmap	40
Fragmentation	40
Spoofing	40
Packet Manipulating	42

Nmap

Nmap, bilgisayar ağıları uzmanı Gordon Lyon (Fyodor) tarafından C/C++ ve Python programlama dilleri kullanılarak geliştirilmiş bir güvenlik tarayıcısıdır. Taranan ağın haritasını çıkarabilir ve ağ makinalarında çalışan servislerin durumlarını, işletim sistemlerini, portların durumlarını gözlemleyebilir.

Nmap kullanarak ağa bağlı herhangi bir bilgisayarın işletim sistemi, çalışan fiziksel aygıt tipleri, çalışma süresi, yazılımların hangi servisleri kullandığı, yazılımların sürüm numaraları, bilgisayarın ateşduvarına sahip olup olmadığı, ağ kartının üreticisinin adı gibi bilgiler öğrenilebilmektedir.

Nmap tamamen özgür GPL (General Public Licence) lisanslı yazılımdır ve istendiği takdirde sitesinin ilgili bölümünden kaynak kodu indirilebilmektedir.

Nmap kullanım alanları :

- Herhangi bir ağ hazırlanırken gerekli ayarların test edilmesinde.
- Ağ envanteri tutulması, haritalaması, bakımında ve yönetiminde.
- Bilinmeyen yeni sunucuları tanımlayarak, güvenlik denetimlerinin yapılması.

Nmap Çalışma Prensipleri

Nmap çok güçlü bir uygulama olmasına rağmen, yeni başlayanlar için anlaşılması zordur. Nmap yaklaşık 15 farklı tarama yöntemine ve her tarama için yaklaşık 20 farklı seçeneğe (çıktı seçenekleri dahil) sahiptir. Nmap tarama süreci ile ilgili bilgiler aşağıda belirtilmiştir :

1. Taranılacak olan hedef makinanın ismi girilirse, Nmap öncelikle DNS lookup işlemi yapar. Bu aslında bir Nmap fonksiyonu değil, ancak DNS sorguları network trafiğinde gözüktüğünden beri, her durum loglanır. Bu yüzden isim ile tarama yapmadan önce bunun bilinmesinde fayda vardır. Eğer isim yerine IP girilirse, DNS lookup işlemi yapılmayacaktır. DNS lookup işleminin iptal edilmesinin bir yolu bulunmuyor, sadece Nmapin üzerinde bulunduğu makinanın host veya lmhost dosyalarının içinde IP – DNS eşleşmesi varsa DNS lookup yapılmaz.
2. Nmap hedef makinaı “ping”ler. Ancak bu bilinen ICMP ping işlemi değildir. Nmap farklı bir ping işlemi kullanır. Bu işlem hakkında bilgi ilerleyen bölümlerde verilecektir. Eğer ping işlemini iptal edilmek isteniyorsa –P0 seçeneği kullanılmalıdır.
3. Eğer hedef makinanın IP adresi belirtildiyse, Nmap reverse DNS lookup yaparak IP – Hostname eşleşmesi yapar. Bu 1. Adımda gerçekleştirilen olayın tersidir.

Bu işlem, ilk adımda DNS lookup yapılmasına rağmen gereksiz gözükebilir. Ancak IP-Hostname sonuçları ile Hostname-IP sonuçları farklı çıkabilir. Bir örnek ile açıklanması gerekirse;

Hedef makina ismi www.microsoft.com olarak belirtilirse, DNS lookup sonucu gelecek olan IP 207.46.19.30 olacaktır. Ancak 207.46.19.30, hedef makina IP si olarak belirtilirse DNS lookup sonucu gelecek olan hostname www.microsoft.com.nsadc.net olacaktır. Eğer reverse lookup işleminin kullanılmaması istenirse -n seçeneği kullanılmalıdır.

4. Nmap taramayı gerçekleştirir. Tarama bittikten sonra, bu dört adımlık süreç sona erer.

Aşağıda Nmap ile taramanın bir örneği verilmiştir :

#nmap -A -T4 192.168.1.2

Nmap scan report for 192.168.1.2

Host is up (0.00052s latency).

Not shown: 995 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 5.2 (protocol 2.0)

| ssh-hostkey: 1024 1a:bc:f6:0b:63:02:ef:72:dc:df:4b:60:fd:28:3d:f3 (DSA)

|_ 2048 72:b1:d5:a1:0e:bd:27:63:e7:ff:83:09:65:af:dc:06 (RSA)

53/tcp open domain dnsmasq 2.48

80/tcp open http Apache httpd 2.2.13 ((Fedora))

| http-methods: Potentially risky methods: TRACE

|_ See http://nmap.org/nsedoc/scripts/http-methods.html

|_html-title: Test Page for the Apache HTTP Server on Fedora

111/tcp open rpcbind

2049/tcp open nfs 2-4 (rpc #100003)

MAC Address: 00:0C:29:D7:D3:65 (VMware)

No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/).

TCP/IP fingerprint:

OS:SCAN(V=5.30BETA1%D=8/1%OT=22%CT=1%CU=31136%PV=Y%DS=1%DC=D%G=Y%M=000C29%T

OS:M=4C55943F%P=i686-pc-linux-gnu)SEQ(SP=C2%GCD=1%ISR=C4%TI=Z%CI=Z%II=I%TS=

OS:A)SEQ(SP=C2%GCD=2%ISR=C4%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M5B4ST11NW6%O2=M5B4S

OS:T11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O5=M5B4ST11NW6%O6=M5B4ST11)WIN

(W1=

OS:16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=Y%DF=Y%T=40%W=16D0

%O=

OS:M5B4NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%

OS:DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M5B4ST11NW6%RD=0%Q=)T4(R=Y%DF=Y%T=40%

W=

OS:0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)

T

OS:6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S

+

OS:%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK

OS:=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

TRACEROUTE

HOP RTT ADDRESS

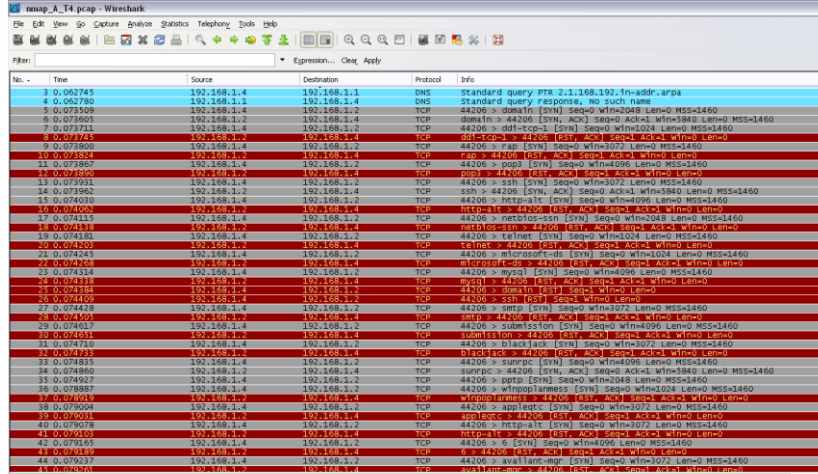
1 0.51 ms 192.168.1.2

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 19.18 seconds

Komutta yer alan özelliklerin açıklamaları aşağıdaki gibidir :

- -A, OS ve versiyon bulma, script taraması ve traceroute özelliğini çalıştırır.
- -T4, daha hızlı bir şekilde tarama yapar (T0 - T5 arası seçim yapılabilir).



Nmap Hedef Belirtme Özelliği

Nmap taramalarında hedef belirlemek için birçok farklı özellik kullanılabilir. Hedef belirtilirken, DNS ismi, IP, Subnet gibi seçenekler kullanılabileceği gibi farklı özelliklerde kullanılabilir.

Hedef belirtme özellikleri :

- -iL <dosya_ismi> : Hostların veya networklerin belirtildiği dosyadan bilgileri alarak tarama yapar.
- -iR <host sayısı>: Rastgele hedef seçer. Host sayısı ile kaç hedefin taranılması istenildiği belirtilir.
- - -exclude <host1[,host2][,host3],...> : Taranılması istenilmeyen hostların veya networklerin belirtilmesi için kullanılır.
- - -excludefile <exclude_file> : Taranılması istenilmeyen hostların veya networklerin bir dosya içerisinde alınarak hedefler belirtilir.

Hedef belirtme seçenekleri :

- 192.168.1.10
- 192.168.1.10/24 :192.168.1.0 – 192.168.1.255 aralığında bulunan subneti tarar.
- 192.168.1-2.* : 192.168.1.0 – 192.168.2.255 aralığındaki herşeyi tarar.
- 192.168.1,2,0-255 : 192.168.1.0 – 192.168.2.255 aralığındaki herşeyi tarar.
- *.*.1.5 : 1.0.1.5 – 255.255.1.5 aralığındaki herşeyi tarar.
- nmap -sV -iL hosts.txt : Taranılacak olan hostları, hosts.txt dosyasından alır
- nmap -p 443 -iR 10 : HTTPS servisini kullanan rastgele 10 tane hostu bulmak için kullanılır.

- `nmap -sP - - exclude web.xyz.com,dns.xyz.com,mail.xyz.com 192.168.1.0/24` : 192.168.1.0 - 192.168.1.255 subnetinde belirtilen adresler dışındaki herşeyi tarar.
- `nmap - -excludefile riskli.txt 192.168.0.0/16` : 192.168.0.0 – 192.168.255.255 subnetinde belirtilen dosyadaki adresler dışındaki herşeyi tarar.

Yetki Yükseltme

Nmap seçeneklerinin hepsi ve işletim sistemi kontrollerini gerçekleştiren yapıları bypass etmek için özelleştirilmiş “raw” paketler, sadece yüksek yetkilere sahip kullanıcıların taramalarında bulunabilir. Unix,Linux için root, Windows için Administrator olmak gerekir.

Sunucuları/İstemcileri Keşfetme

Organizasyon içerisindeki hostları bulmak için çok önemli bir yöntemdir. Keşfetme işlemi için birçok seçenek kullanılabilir. En basit yolu bir ping scan gerçekleştirmektir : (Ping Scan hakkında detaylı bilgi Tarama bölümünde mevcuttur.)

#nmap -sP 192.168.2.0/24

Host 192.168.2.1 appears to be up.

Host 192.168.2.3 appears to be up.

Host 192.168.2.4 appears to be up.

Nmap done: 256 IP addresses (3 hosts up) scanned in 1.281 seconds

Ping scan belirtilen hedef veya hedeflerin 80. portuna ICMP echo request ve TCP ACK (root veya Administrator değilse SYN) paketleri gönderir. Hedef veya hedeflerden dönen tepkilere göre bilgiler çıkartılır. Hedef/hedefler Nmap ile aynı yerel ağda bulunuyorsa, Nmap hedef/hedeflerin MAC adreslerini ve ilgili üreticiye ait bilgileri (OUI) sunar. Bunun sebebi, Nmap varsayılan olarak ARP taraması, -PR, yapar. Bu özelliği iptal etmek için- -send-ip seçeneği kullanılabilir. Ping scan portları taramaz yada başka tarama tekniklerini gerçekleştirmez. Ping scan network envanteri vb. işlemler için idealdir.

Keşfetme işlemleri için bazı seçenekler aşağıda sunulmuştur :

- `-sL`: List Scan – Hedefleri ve DNS isimlerinin bir listesini çıkarır.
- `-sn`: Ping Scan - Port scan seçeneğini iptal eder.
- `-Pn`: Host discovery yapılmaz, bütün hostlar ayakta gözüktür.
- `-n/-R`: Asla DNS Çözümlemesi yapılmaz/Herzaman DNS çözümlemesi yapılır [varsayılan: bazen]
- `--dns-servers <serv1[,serv2],...>`: Özel DNS serverları belirtmek için kullanılır.
- `--system-dns`: OS e ait DNS çözümleyici kullanılır.
- `--traceroute`: Traceroute özelliğini aktif hale getirir. TCP Connect ve Idle Scan dışındaki tarama türleri ile yapılmaz.

- -p : port veya port aralıklarını belirtmek için kullanılır. -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
- -F: Fast mode, varsayılan taramalarda belirlenen portlardan biraz daha azı kullanılır.
- -r: Portları sırayla tarar. Rastgele tarama kullanılmaz.
- --top-ports <sayı>: <sayı> ile belirtilen ortak portları taranır.
- p--port-ratio <oran>: Belirtilen <oran> üzerinden ortak portlar taranır.
- - -randomize_hosts, -rH : Listede belirtilen taranılacak hostları rastgele bir şekilde seçer.
- - -source_port, -g : Taramayı yapacak olan makinanın kaynak portunu belirlemek amacıyla kullanılır.
- -S <IP> : Kaynak IP yi belirlemek amacıyla kullanılır.
- -e : Network arayüzünü belirlemek amacıyla kullanılır.

Tarama

Nmap herhangi bir client veya serverı birçok farklı şekilde tarama yeteneğine sahiptir. Nmapin asıl gücü farklı tarama tekniklerinden gelir. Protokol bazlı (Tcp, Udp vb.) tarayabileceğiniz gibi, belirli aralıklardaki ipler, subnetler ve üzerlerinde çalışan port ve servisleride taranabilir.

Portların Taramalara Verebileceği Cevaplar

Tarama sonuçlarında ortaya çıkabilecek port durumları aşağıdaki gibidir :

- Open : Portlar açık ve aktif olarak TCP veya UDP bağlantısı kabul eder.
- Closed : Portlar kapalı ancak erişilebilir. Üzerlerinde dinlenen aktif bir bağlantı yoktur.
- Filtered : Dönen tepkiler bir paket filtreleme mekanizması tarafından engellenir. Nmap portun açık olduğuna karar veremez.
- Unfiltered : portlar erişilebilir ancak Nmap portların açık veya kapalı olduğuna karar Pveremez. (Sadece ACK scan için)
- Open|filtered : Nmap portların açık veya filtrelenmiş olduğuna karar veremez. (UDP, IP Proto, FIN, Null, Xmas Scan için)
- Closed|filtered : Nmap portların kapalı yada filtreli olduğuna karar veremez. (Sadece Idle Scan için)

Taramalar esnasında Nmapin performansının düşmemesi ve çıktıların daha düzenli olmasıyla amacıyla -v yada -vv seçenekleri kullanılabilir. Bu seçenekler vasıtasıyla Nmap bize sunacağı çıktıları limitler. -vv kullanılırsa, Nmap'e ait istatistikler görülmez ve en sade çıktı alınır.

Tarama Türleri

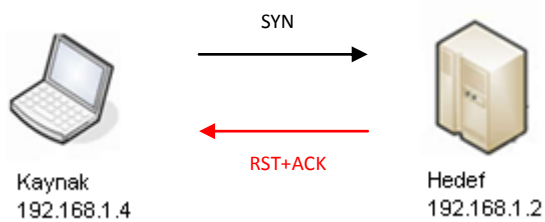
Varolan tarama türleri aşağıdaki resimde belirtilmiştir. Tarama türlerinde bulunan TCP bayrakları eğer elle eklenmek istenirse aşağıdaki komut kullanılmalıdır :

nmap -sS <TCP_Bayrağı> [Hedef_IP]

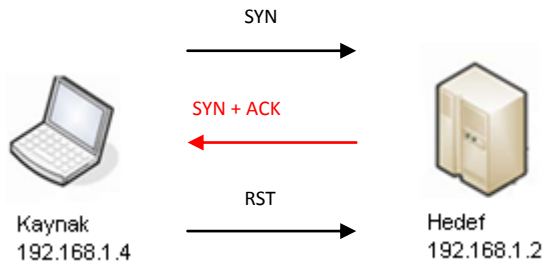
Nmap Scan	Command Syntax	Requires Privileged Access	Identifies TCP Ports	Identifies UDP Ports
TCP SYN Scan	-sS	YES	YES	NO
TCP connect() Scan	-sT	NO	YES	NO
FIN Scan	-sF	YES	YES	NO
Xmas Tree Scan	-sX	YES	YES	NO
Null Scan	-sN	YES	YES	NO
Ping Scan	-sP	NO	NO	NO
Version Detection	-sV	NO	NO	NO
UDP Scan	-sU	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

TCP Syn Scan

Kaynak makinanın hedef makinaya TCP SYN bayraklı paket göndererek başlattığı bu tarama türünde, tarama esnasında muhtemelen portların çoğu kapalı olacaktır. Kapalı olduğu durumlarda hedef makina RST + ACK bayraklı paket döndürür :



Açık olduğu durumda SYN + ACK bayraklı paket dönecektir. Kaynak makinada RST bayraklı paket göndererek bağlantıyı koparır ve böylelikle üçlü el sıkışma tamamlanmaz.



Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır :

nmap -sS -v [Hedef_IP]

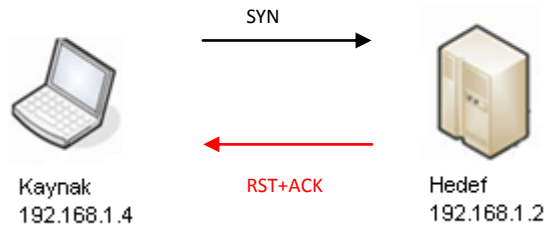
#nmap -sS -v 192.168.1.2

```
at 2010-08-01 18:37 EEST
Initiating ARP Ping Scan at 18:37
Scanning 192.168.1.2 [1 port]
Completed ARP Ping Scan at 18:37, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:37
Completed Parallel DNS resolution of 1 host. at 18:37, 0.02s elapsed
Initiating SYN Stealth Scan at 18:37
Scanning 192.168.1.2 [1000 ports]
Discovered open port 22/tcp on 192.168.1.2
Discovered open port 111/tcp on 192.168.1.2
Discovered open port 53/tcp on 192.168.1.2
Discovered open port 80/tcp on 192.168.1.2
Discovered open port 2049/tcp on 192.168.1.2
Completed SYN Stealth Scan at 18:37, 1.15s elapsed (1000 total ports)
Nmap scan report for 192.168.1.2
Host is up (0.00097s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
2049/tcp  open  nfs
MAC Address: 00:0C:29:D7:D3:65 (VMware)
Read data files from: /usr/local/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
Raw packets sent: 1006 (44.248KB) | Rcvd: 1001 (40.048KB)
```

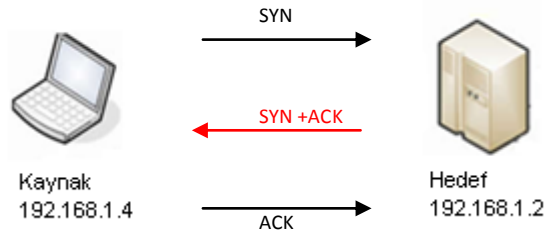
nmap_SYN.pcap - Wireshark					
File Edit View Go Capture Analyze Statistics Telephony Tools Help					
Filter: tcp Expression... Clear Apply					
No.	Time	Source	Destination	Protocol	Info
5	0.069578	192.168.1.4	192.168.1.2	TCP	52584 > blackjack [SYN] Seq=0 Win=4096 Len=0 MSS=1460
6	0.069644	192.168.1.2	192.168.1.4	TCP	blackjack > 52584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	0.069755	192.168.1.4	192.168.1.2	TCP	52584 > ssh [SYN] Seq=0 Win=4096 Len=0 MSS=1460
8	0.069798	192.168.1.2	192.168.1.4	TCP	ssh > 52584 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
9	0.069875	192.168.1.4	192.168.1.2	TCP	52584 > telnet [SYN] Seq=0 Win=4096 Len=0 MSS=1460
10	0.069920	192.168.1.2	192.168.1.4	TCP	telnet > 52584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	0.069945	192.168.1.4	192.168.1.2	TCP	52584 > https [SYN] Seq=0 Win=3072 Len=0 MSS=1460
12	0.069967	192.168.1.2	192.168.1.4	TCP	https > 52584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	0.070008	192.168.1.4	192.168.1.2	TCP	52584 > sunrpc [SYN] Seq=0 Win=2048 Len=0 MSS=1460
14	0.070034	192.168.1.2	192.168.1.4	TCP	sunrpc > 52584 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
15	0.070095	192.168.1.4	192.168.1.2	TCP	52584 > rtsp [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	0.070117	192.168.1.2	192.168.1.4	TCP	rtsp > 52584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17	0.070163	192.168.1.4	192.168.1.2	TCP	52584 > ms-wbt-server [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	0.070184	192.168.1.2	192.168.1.4	TCP	ms-wbt-server > 52584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	0.070225	192.168.1.4	192.168.1.2	TCP	52584 > ftp [SYN] Seq=0 Win=2048 Len=0 MSS=1460
20	0.070248	192.168.1.2	192.168.1.4	TCP	ftp > 52584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	0.070290	192.168.1.4	192.168.1.2	TCP	52584 > epmap [SYN] Seq=0 Win=2048 Len=0 MSS=1460
22	0.070312	192.168.1.2	192.168.1.4	TCP	epmap > 52584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	0.070352	192.168.1.4	192.168.1.2	TCP	52584 > pop3s [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	0.070372	192.168.1.2	192.168.1.4	TCP	pop3s > 52584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	0.070415	192.168.1.4	192.168.1.2	TCP	52584 > ssh [RST] Seq=1 Win=0 Len=0
26	0.070529	192.168.1.4	192.168.1.2	TCP	52584 > sunrpc [RST] Seq=1 Win=0 Len=0
27	0.070547	192.168.1.4	192.168.1.2	TCP	52584 > h323hostcall [SYN] Seq=0 Win=4096 Len=0 MSS=1460
28	0.070565	192.168.1.2	192.168.1.4	TCP	h323hostcall > 52584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29	0.070641	192.168.1.4	192.168.1.2	TCP	52584 > domain [SYN] Seq=0 Win=4096 Len=0 MSS=1460
30	0.070670	192.168.1.2	192.168.1.4	TCP	domain > 52584 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
31	0.070730	192.168.1.4	192.168.1.2	TCP	52584 > rap [SYN] Seq=0 Win=1024 Len=0 MSS=1460
32	0.070753	192.168.1.2	192.168.1.4	TCP	rap > 52584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	0.070793	192.168.1.4	192.168.1.2	TCP	52584 > http [SYN] Seq=0 Win=1024 Len=0 MSS=1460
34	0.070822	192.168.1.2	192.168.1.4	TCP	http > 52584 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
35	0.070881	192.168.1.4	192.168.1.2	TCP	52584 > microsoft-ds [SYN] Seq=0 Win=3072 Len=0 MSS=1460
36	0.072158	192.168.1.4	192.168.1.2	TCP	52584 > wherehoo [SYN] Seq=0 Win=4096 Len=0 MSS=1460
37	0.072181	192.168.1.2	192.168.1.4	TCP	wherehoo > 52584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38	0.072232	192.168.1.4	192.168.1.2	TCP	52584 > smpnamerex [SYN] Seq=0 Win=2048 Len=0 MSS=1460
39	0.072250	192.168.1.2	192.168.1.4	TCP	smpnamerex > 52584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40	0.072289	192.168.1.4	192.168.1.2	TCP	52584 > pds [SYN] Seq=0 Win=2048 Len=0 MSS=1460
41	0.072307	192.168.1.2	192.168.1.4	TCP	pds > 52584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42	0.072346	192.168.1.4	192.168.1.2	TCP	52584 > dandy-tester [SYN] Seq=0 Win=1024 Len=0 MSS=1460
43	0.072363	192.168.1.2	192.168.1.4	TCP	dandy-tester > 52584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
44	0.072401	192.168.1.4	192.168.1.2	TCP	52584 > 44176 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
45	0.072417	192.168.1.2	192.168.1.4	TCP	44176 > 52584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
46	0.072455	192.168.1.4	192.168.1.2	TCP	52584 > 32778 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
47	0.072471	192.168.1.2	192.168.1.4	TCP	32778 > 52584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

TCP Connect Scan

Kaynak makinanın gerçekleştireceği TCP Connect Scan, kapalı portlara yapıldığı zaman dönecek cevaplar TCP SYN Scan gibi olacaktır, RST + ACK bayraklı paket dönecektir :



Ancak açık olduğu durumlarda TCP SYN Scan tersine, hedef makinanın göndereceği SYN + ACK bayraklı paketi, kaynak makina ACK bayraklı paket göndererek cevaplar ve üçlü el sıkışmayı tamamlar:



Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır :

nmap -sT -v [Hedef_IP]

#nmap -sT -v 192.168.1.2

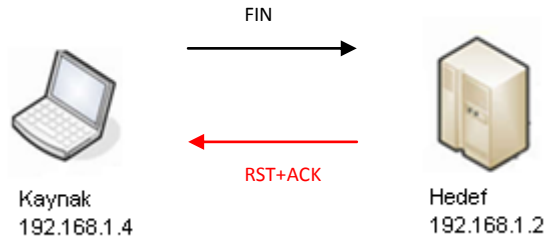
```
at 2010-08-01 18:38 EEST
Initiating ARP Ping Scan at 18:38
Scanning 192.168.1.2 [1 port]
Completed ARP Ping Scan at 18:38, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:38
Completed Parallel DNS resolution of 1 host. at 18:38, 0.02s elapsed
Initiating Connect Scan at 18:38
Scanning 192.168.1.2 [1000 ports]
Discovered open port 111/tcp on 192.168.1.2
Discovered open port 80/tcp on 192.168.1.2
Discovered open port 53/tcp on 192.168.1.2
Discovered open port 22/tcp on 192.168.1.2
Discovered open port 2049/tcp on 192.168.1.2
Completed Connect Scan at 18:38, 1.11s elapsed (1000 total ports)
Nmap scan report for 192.168.1.2
Host is up (0.0041s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
2049/tcp  open  nfs
MAC Address: 00:0C:29:D7:D3:65 (VMware)
Read data files from: /usr/local/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.27 seconds
Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
```

nmap_TcpConnect.pcap - Wireshark					
File Edit View Go Capture Analyze Statistics Telephony Tools Help					
Filter: tcp Expression... Clear Apply					
No.	Time	Source	Destination	Protocol	Info
5	0.048472	192.168.1.4	192.168.1.2	TCP	51229 > http-alt [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367818 TSER=0 WS=6
6	0.048628	192.168.1.2	192.168.1.4	TCP	http-alt > 51229 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	0.048953	192.168.1.4	192.168.1.2	TCP	57551 > pptp [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367818 TSER=0 WS=6
8	0.048979	192.168.1.2	192.168.1.4	TCP	pptp > 57551 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
9	0.049024	192.168.1.4	192.168.1.2	TCP	36761 > rtsp [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367818 TSER=0 WS=6
10	0.049074	192.168.1.2	192.168.1.4	TCP	rtsp > 36761 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	0.049150	192.168.1.4	192.168.1.2	TCP	48966 > h323hostcall [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367818 TSER=0 WS=6
12	0.049183	192.168.1.2	192.168.1.4	TCP	h323hostcall > 48966 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	0.049253	192.168.1.4	192.168.1.2	TCP	34784 > imap [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367818 TSER=0 WS=6
14	0.049298	192.168.1.2	192.168.1.4	TCP	imap > 34784 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	0.049362	192.168.1.4	192.168.1.2	TCP	41729 > mysql [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367818 TSER=0 WS=6
16	0.049394	192.168.1.2	192.168.1.4	TCP	mysql > 41729 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17	0.049514	192.168.1.4	192.168.1.2	TCP	53546 > sunrpc [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367818 TSER=0 WS=6
18	0.049578	192.168.1.2	192.168.1.4	TCP	sunrpc > 53546 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=6118730 TSER=0 WS=6
19	0.049683	192.168.1.4	192.168.1.2	TCP	57162 > ddt-tcp-1 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367818 TSER=0 WS=6
20	0.049719	192.168.1.2	192.168.1.4	TCP	ddt-tcp-1 > 57162 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	0.049863	192.168.1.4	192.168.1.2	TCP	34231 > microsoft-ds [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367818 TSER=0 WS=6
22	0.049890	192.168.1.2	192.168.1.4	TCP	microsoft-ds > 34231 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	0.049939	192.168.1.4	192.168.1.2	TCP	33919 > ident [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367818 TSER=0 WS=6
24	0.049970	192.168.1.2	192.168.1.4	TCP	ident > 33919 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	0.050031	192.168.1.4	192.168.1.2	TCP	32962 > https [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367818 TSER=0 WS=6
26	0.050102	192.168.1.2	192.168.1.4	TCP	https > 32962 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	0.050174	192.168.1.4	192.168.1.2	TCP	53470 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367818 TSER=0 WS=6
28	0.050219	192.168.1.2	192.168.1.4	TCP	http > 53470 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=6118730 TSER=0 WS=6
29	0.050293	192.168.1.4	192.168.1.2	TCP	40314 > netbios-ssn [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367818 TSER=0 WS=6
30	0.050326	192.168.1.2	192.168.1.4	TCP	netbios-ssn > 40314 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31	0.050389	192.168.1.4	192.168.1.2	TCP	51366 > smux [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367818 TSER=0 WS=6
32	0.050421	192.168.1.2	192.168.1.4	TCP	smux > 51366 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	0.050484	192.168.1.4	192.168.1.2	TCP	55792 > submission [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367818 TSER=0 WS=6
34	0.050533	192.168.1.2	192.168.1.4	TCP	submission > 55792 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
35	0.050611	192.168.1.4	192.168.1.2	TCP	60063 > ms-wbt-server [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367818 TSER=0 WS=6
36	0.050636	192.168.1.2	192.168.1.4	TCP	ms-wbt-server > 60063 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37	0.050680	192.168.1.2	192.168.1.4	TCP	newak > 55127 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
38	0.051223	192.168.1.4	192.168.1.2	TCP	40308 > 8290 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367819 TSER=0 WS=6
39	0.051327	192.168.1.2	192.168.1.4	TCP	8290 > 40308 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
40	0.051410	192.168.1.4	192.168.1.2	TCP	45714 > 60020 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367819 TSER=0 WS=6
41	0.051610	192.168.1.2	192.168.1.4	TCP	60020 > 45714 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42	0.051668	192.168.1.4	192.168.1.2	TCP	34932 > nucleus-sand [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367819 TSER=0 WS=6
43	0.051720	192.168.1.2	192.168.1.4	TCP	nucleus-sand > 34932 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
44	0.051782	192.168.1.4	192.168.1.2	TCP	51856 > cnrprotocol [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367819 TSER=0 WS=6
45	0.051881	192.168.1.2	192.168.1.4	TCP	cnrprotocol > 51856 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
46	0.051988	192.168.1.4	192.168.1.2	TCP	34479 > dxspider [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=3367819 TSER=0 WS=6
47	0.0519916	192.168.1.2	192.168.1.4	TCP	dxspider > 34479 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

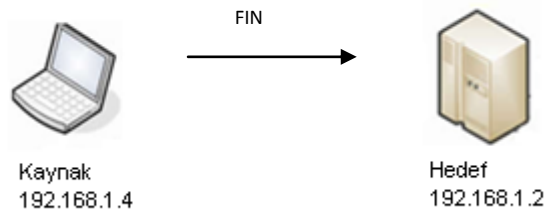
FIN Scan

FIN Scan ilişkin “saklı” framerer olağandışıdır çünkü hedef makinaya ilk TCP el sıkışması olmadan gönderilirler.

Kaynak makinanın göndereceği FIN bayraklı paket, hedef makinanın kapalı bir portuna gelirse hedef makina RST + ACK bayraklı paket döndürecek tir :



Eğer port açık olursa hedef makinadan herhangi bir tepki dönmeyecektir :



Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır :

nmap -sF -v [Hedef_IP]

#nmap -sF -v 192.168.1.2

at 2010-08-01 18:39 EEST

Initiating ARP Ping Scan at 18:39

Scanning 192.168.1.2 [1 port]

Completed ARP Ping Scan at 18:39, 0.02s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 18:39

Completed Parallel DNS resolution of 1 host. at 18:39, 0.02s elapsed

Initiating FIN Scan at 18:39

Scanning 192.168.1.2 [1000 ports]

Completed FIN Scan at 18:39, 4.35s elapsed (1000 total ports)

Nmap scan report for 192.168.1.2

Host is up (0.00085s latency).

Not shown: 995 closed ports

PORT STATE SERVICE

22/tcp open|filtered ssh

53/tcp open|filtered domain

80/tcp open|filtered http

111/tcp open|filtered rpcbind

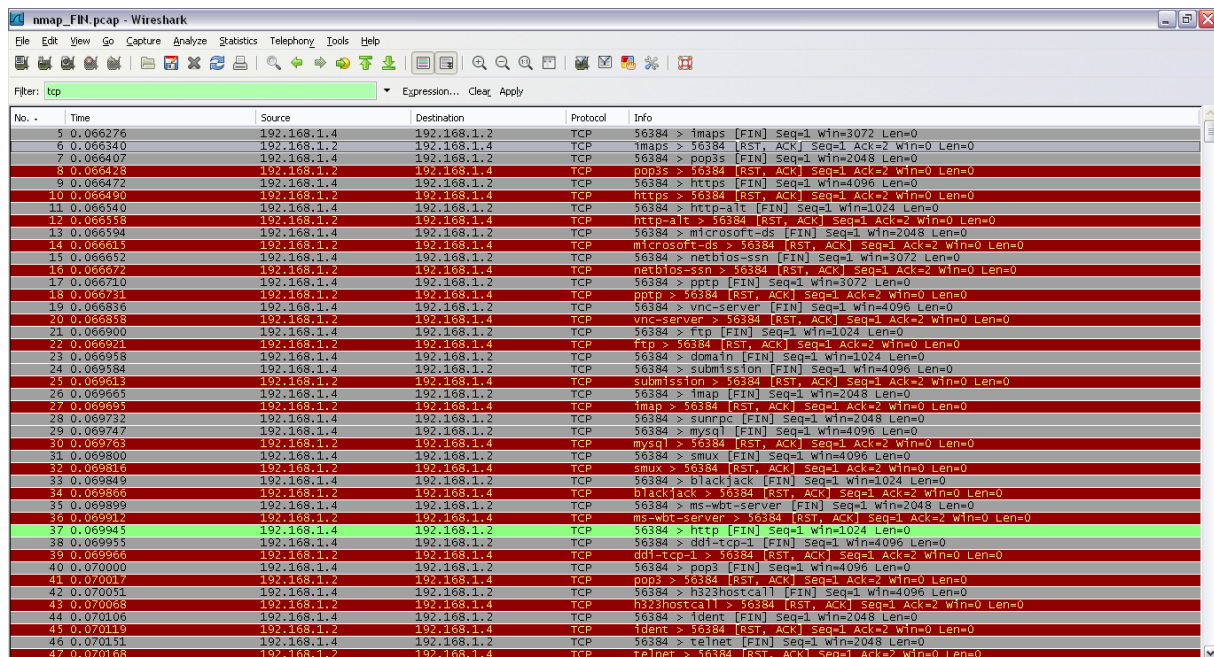
2049/tcp open|filtered nfs

MAC Address: 00:0C:29:D7:D3:65 (VMware)

Read data files from: /usr/local/share/nmap

Nmap done: 1 IP address (1 host up) scanned in 4.56 seconds

Raw packets sent: 1075 (42.988KB) | Rcvd: 997 (39.868KB)

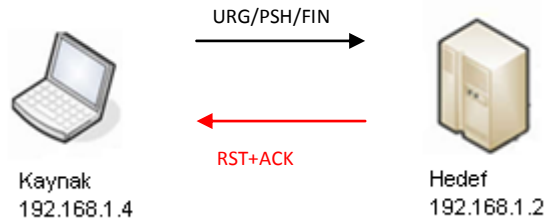


No.	Time	Source	Destination	Protocol	Info
5	0.066276	192.168.1.4	192.168.1.2	TCP	56384 > 1maps [FIN] Seq=1 win=3072 Len=0
6	0.066340	192.168.1.2	192.168.1.4	TCP	1maps > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
7	0.066407	192.168.1.4	192.168.1.2	TCP	56384 > pop35 [FIN] Seq=1 win=2048 Len=0
8	0.066478	192.168.1.2	192.168.1.4	TCP	pop35 > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
9	0.066472	192.168.1.4	192.168.1.2	TCP	56384 > https [FIN] Seq=1 win=4096 Len=0
10	0.066500	192.168.1.2	192.168.1.4	TCP	https > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
11	0.066540	192.168.1.4	192.168.1.2	TCP	56384 > http-alt [FIN] Seq=1 win=1024 Len=0
12	0.066558	192.168.1.2	192.168.1.4	TCP	http-alt > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
13	0.066594	192.168.1.4	192.168.1.2	TCP	56384 > microsoft-ds [FIN] Seq=1 win=2048 Len=0
14	0.066615	192.168.1.2	192.168.1.4	TCP	microsoft-ds > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
15	0.066652	192.168.1.4	192.168.1.2	TCP	56384 > netbios-ssn [FIN] Seq=1 win=3072 Len=0
16	0.066692	192.168.1.2	192.168.1.4	TCP	netbios-ssn > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
17	0.066710	192.168.1.4	192.168.1.2	TCP	56384 > pptp [FIN] Seq=1 win=3072 Len=0
18	0.066731	192.168.1.2	192.168.1.4	TCP	pptp > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
19	0.066836	192.168.1.4	192.168.1.2	TCP	56384 > vnc-server [FIN] Seq=1 win=4096 Len=0
20	0.066898	192.168.1.2	192.168.1.4	TCP	vnc-server > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
21	0.066900	192.168.1.4	192.168.1.2	TCP	56384 > ftp [FIN] Seq=1 win=1024 Len=0
22	0.066921	192.168.1.2	192.168.1.4	TCP	ftp > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
23	0.066958	192.168.1.4	192.168.1.2	TCP	56384 > domain [FIN] Seq=1 win=1024 Len=0
24	0.066984	192.168.1.4	192.168.1.2	TCP	56384 > submission [FIN] Seq=1 win=4096 Len=0
25	0.066983	192.168.1.2	192.168.1.4	TCP	submission > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
26	0.066965	192.168.1.4	192.168.1.2	TCP	56384 > imap [FIN] Seq=1 win=2048 Len=0
27	0.066995	192.168.1.2	192.168.1.4	TCP	imap > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
28	0.069732	192.168.1.4	192.168.1.2	TCP	56384 > sunrpc [FIN] Seq=1 win=2048 Len=0
29	0.069747	192.168.1.4	192.168.1.2	TCP	56384 > mysql [FIN] Seq=1 win=4096 Len=0
30	0.069763	192.168.1.2	192.168.1.4	TCP	mysql > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
31	0.069800	192.168.1.4	192.168.1.2	TCP	56384 > smux [FIN] Seq=1 win=4096 Len=0
32	0.069816	192.168.1.2	192.168.1.4	TCP	smux > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
33	0.069849	192.168.1.4	192.168.1.2	TCP	56384 > blackjack [FIN] Seq=1 win=1024 Len=0
34	0.069866	192.168.1.2	192.168.1.4	TCP	blackjack > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
35	0.069899	192.168.1.4	192.168.1.2	TCP	56384 > ms-wbt-server [FIN] Seq=1 win=2048 Len=0
36	0.069912	192.168.1.2	192.168.1.4	TCP	ms-wbt-server > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
37	0.069945	192.168.1.4	192.168.1.2	TCP	56384 > http [FIN] Seq=1 win=1024 Len=0
38	0.069955	192.168.1.4	192.168.1.2	TCP	56384 > ddi-tcp-1 [FIN] Seq=1 win=4096 Len=0
39	0.069966	192.168.1.2	192.168.1.4	TCP	ddi-tcp-1 > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
40	0.070000	192.168.1.4	192.168.1.2	TCP	56384 > pop3 [FIN] Seq=1 win=4096 Len=0
41	0.070017	192.168.1.2	192.168.1.4	TCP	pop3 > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
42	0.070051	192.168.1.4	192.168.1.2	TCP	56384 > h323hostcall [FIN] Seq=1 win=4096 Len=0
43	0.070068	192.168.1.2	192.168.1.4	TCP	h323hostcall > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
44	0.070106	192.168.1.4	192.168.1.2	TCP	56384 > ident [FIN] Seq=1 win=2048 Len=0
45	0.070119	192.168.1.2	192.168.1.4	TCP	ident > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0
46	0.070151	192.168.1.4	192.168.1.2	TCP	56384 > telnet [FIN] Seq=1 win=2048 Len=0
47	0.070165	192.168.1.2	192.168.1.4	TCP	telnet > 56384 [RST, ACK] Seq=1 Ack=2 win=0 Len=0

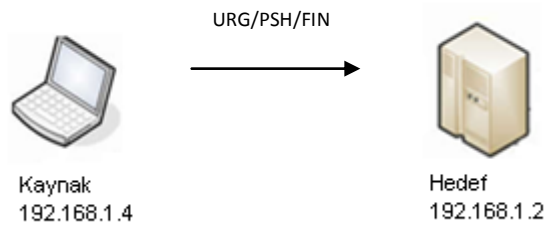
XMas Tree Scan

Kaynak makinanın TCP frame içine URG, PSH ve FIN bayraklarını set edeceği paket hedef makinaya gönderilir. Hedef makinanın döndüreceği cevaplar FIN Scan ile aynıdır.

Kaynak makinanın göndereceği URG,PSH ve FIN bayraklı paket, hedef makinanın kapalı bir portuna gelirse hedef makina RST + ACK bayraklı paket döndürecektir :



Eğer port açık olursa hedef makinadan herhangi bir tepki dönmeyecektir :



Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır :

nmap -sX -v [Hedef_IP]

#nmap -sX -v 192.168.1.2

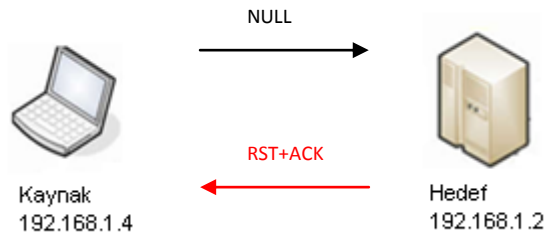
```
at 2010-08-01 18:40 EEST
Initiating ARP Ping Scan at 18:40
Scanning 192.168.1.2 [1 port]
Completed ARP Ping Scan at 18:40, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:40
Completed Parallel DNS resolution of 1 host. at 18:40, 0.02s elapsed
Initiating XMAS Scan at 18:40
Scanning 192.168.1.2 [1000 ports]
Completed XMAS Scan at 18:40, 2.63s elapsed (1000 total ports)
Nmap scan report for 192.168.1.2
Host is up (0.0040s latency).
Not shown: 995 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
53/tcp    open|filtered domain
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
2049/tcp   open|filtered nfs
MAC Address: 00:0C:29:D7:D3:65 (VMware)
Read data files from: /usr/local/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.85 seconds
Raw packets sent: 1061 (42.428KB) | Rcvd: 997 (39.868KB)
```

nmap_XMas.pcap - Wireshark					
File Edit View Go Capture Analyze Statistics Telephony Tools Help					
Filter: tcp Expression... Clear Apply					
No. -	Time	Source	Destination	Protocol	Info
5	0.070428	192.168.1.4	192.168.1.2	TCP	41906 > http [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
6	0.070479	192.168.1.4	192.168.1.2	TCP	41906 > h323hostcall [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
7	0.070535	192.168.1.2	192.168.1.4	TCP	h323hostcall > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
8	0.070638	192.168.1.4	192.168.1.2	TCP	41906 > ssh [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
9	0.070659	192.168.1.4	192.168.1.2	TCP	41906 > ms-wbt-server [FIN, PSH, URG] Seq=1 Win=2048 Urg=0 Len=0
10	0.070670	192.168.1.2	192.168.1.4	TCP	ms-wbt-server > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
11	0.070736	192.168.1.4	192.168.1.2	TCP	41906 > microsoft-ds [FIN, PSH, URG] Seq=1 Win=2048 Urg=0 Len=0
12	0.070766	192.168.1.2	192.168.1.4	TCP	microsoft-ds > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
13	0.070821	192.168.1.4	192.168.1.2	TCP	41906 > submission [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
14	0.070843	192.168.1.2	192.168.1.4	TCP	submission > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
15	0.070898	192.168.1.4	192.168.1.2	TCP	41906 > rtsp [FIN, PSH, URG] Seq=1 Win=4096 Urg=0 Len=0
16	0.070919	192.168.1.2	192.168.1.4	TCP	rtsp > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
17	0.070972	192.168.1.4	192.168.1.2	TCP	41906 > gmap [FIN, PSH, URG] Seq=1 Win=4096 Urg=0 Len=0
18	0.071002	192.168.1.2	192.168.1.4	TCP	gmap > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
19	0.071058	192.168.1.4	192.168.1.2	TCP	41906 > rap [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
20	0.071079	192.168.1.2	192.168.1.4	TCP	rap > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
21	0.071132	192.168.1.4	192.168.1.2	TCP	41906 > imap [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
22	0.071161	192.168.1.2	192.168.1.4	TCP	imap > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
23	0.072124	192.168.1.4	192.168.1.2	TCP	41906 > blackjack [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
24	0.074260	192.168.1.2	192.168.1.4	TCP	blackjack > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
25	0.074340	192.168.1.4	192.168.1.2	TCP	41906 > ddi-tcp-1 [FIN, PSH, URG] Seq=1 Win=2048 Urg=0 Len=0
26	0.074372	192.168.1.2	192.168.1.4	TCP	ddi-tcp-1 > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
27	0.074429	192.168.1.4	192.168.1.2	TCP	41906 > pop3 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
28	0.074457	192.168.1.2	192.168.1.4	TCP	pop3 > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
29	0.074513	192.168.1.4	192.168.1.2	TCP	41906 > ftp [FIN, PSH, URG] Seq=1 Win=2048 Urg=0 Len=0
30	0.074543	192.168.1.2	192.168.1.4	TCP	ftp > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
31	0.074599	192.168.1.4	192.168.1.2	TCP	41906 > vnc-server [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
32	0.074627	192.168.1.2	192.168.1.4	TCP	vnc-server > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
33	0.074682	192.168.1.4	192.168.1.2	TCP	41906 > pop3s [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
34	0.074708	192.168.1.2	192.168.1.4	TCP	pop3s > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
35	0.074757	192.168.1.4	192.168.1.2	TCP	41906 > sunrpc [FIN, PSH, URG] Seq=1 Win=4096 Urg=0 Len=0
36	0.074775	192.168.1.2	192.168.1.2	TCP	41906 > domain [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
37	0.074788	192.168.1.4	192.168.1.2	TCP	41906 > mysql [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
38	0.074818	192.168.1.2	192.168.1.4	TCP	mysql > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
39	0.074868	192.168.1.4	192.168.1.2	TCP	41906 > smtp [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
40	0.074890	192.168.1.2	192.168.1.4	TCP	smtp > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
41	0.074952	192.168.1.4	192.168.1.2	TCP	41906 > ident [FIN, PSH, URG] Seq=1 Win=2048 Urg=0 Len=0
42	0.074980	192.168.1.2	192.168.1.2	TCP	ident > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
43	0.075113	192.168.1.4	192.168.1.2	TCP	41906 > imaps [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
44	0.075147	192.168.1.2	192.168.1.4	TCP	imaps > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
45	0.075214	192.168.1.4	192.168.1.2	TCP	41906 > pptp [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0
46	0.075244	192.168.1.2	192.168.1.2	TCP	pptp > 41906 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
47	0.075300	192.168.1.4	192.168.1.2	TCP	41906 > netbios-ssn [FIN, PSH, URG] Seq=1 Win=3072 Urg=0 Len=0

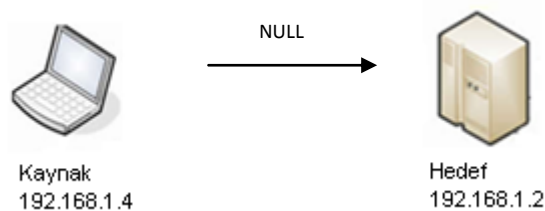
Null Scan

Hiçbir bayrağın bulunmayacağı bu tarama türü, gerçek hayatta karşımıza çıkmayan bir durumdur. kaynak makinanın göndereceği bayraksız paketler karşısında hedef makinanın vereceği tepkiler FIN Scan ile aynıdır.

Kaynak makinanın göndereceği bayraksız paket, hedef makinanın kapalı bir portuna gelirse hedef makina RST + ACK bayraklı paket döndürecek tir :



Eğer port açık olursa hedef makinadan herhangi bir tepki dönmeyecektir :



Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır :

nmap -sN -v [Hedef_IP]

#nmap -sN -v 192.168.1.2

at 2010-08-01 18:41 EEST

Initiating ARP Ping Scan at 18:41

Scanning 192.168.1.2 [1 port]

Completed ARP Ping Scan at 18:41, 0.02s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 18:41

Completed Parallel DNS resolution of 1 host. at 18:41, 0.02s elapsed

Initiating NULL Scan at 18:41

Scanning 192.168.1.2 [1000 ports]

Completed NULL Scan at 18:41, 21.07s elapsed (1000 total ports)

Nmap scan report for 192.168.1.2

Host is up (0.00028s latency).

All 1000 scanned ports on 192.168.1.2 are open|filtered

MAC Address: 00:0C:29:D7:D3:65 (VMware)

Read data files from: /usr/local/share/nmap

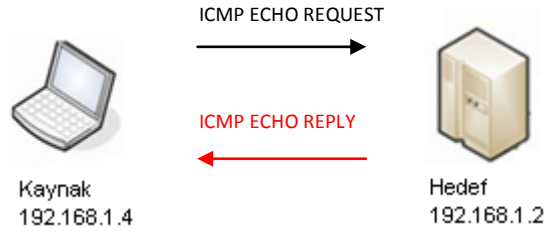
Nmap done: 1 IP address (1 host up) scanned in 21.29 seconds

Raw packets sent: 2001 (80.028KB) | Rcvd: 1991 (79.628KB)

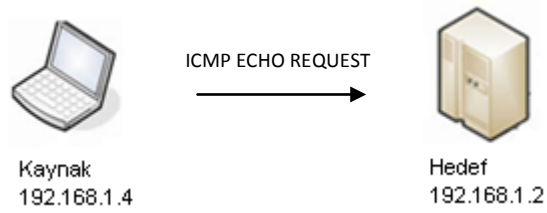
nmap_NULL.pcap - Wireshark					
File Edit View Go Capture Analyze Statistics Telephony Tools Help					
Filter: tcp					
No. -	Time	Source	Destination	Protocol	Info
5	0.066559	192.168.1.4	192.168.1.2	TCP	58015 > submission [<None>] Seq=1 win=1024 Len=0
6	0.066614	192.168.1.2	192.168.1.4	TCP	submission > 58015 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
7	0.066978	192.168.1.4	192.168.1.2	TCP	58015 > microsoft-ds [<None>] Seq=1 win=3072 Len=0
8	0.067012	192.168.1.2	192.168.1.4	TCP	microsoft-ds > 58015 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
9	0.067352	192.168.1.4	192.168.1.2	TCP	58015 > pptp [<None>] Seq=1 win=2048 Len=0
10	0.067355	192.168.1.2	192.168.1.4	TCP	pptp > 58015 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
11	0.067735	192.168.1.4	192.168.1.2	TCP	58015 > h323hostcall [<None>] Seq=1 win=1024 Len=0
12	0.067758	192.168.1.2	192.168.1.4	TCP	h323hostcall > 58015 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
13	0.068034	192.168.1.4	192.168.1.2	TCP	58015 > rap [<None>] Seq=1 win=4096 Len=0
14	0.068038	192.168.1.2	192.168.1.4	TCP	rap > 58015 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
15	0.068338	192.168.1.4	192.168.1.2	TCP	58015 > sunrpc [<None>] Seq=1 win=2048 Len=0
16	0.068507	192.168.1.4	192.168.1.2	TCP	58015 > smux [<None>] Seq=1 win=1024 Len=0
17	0.068540	192.168.1.2	192.168.1.4	TCP	smux > 58015 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
18	0.068879	192.168.1.4	192.168.1.2	TCP	58015 > ssh [<None>] Seq=1 win=2048 Len=0
19	0.069047	192.168.1.4	192.168.1.2	TCP	58015 > http-alt [<None>] Seq=1 win=2048 Len=0
20	0.069074	192.168.1.2	192.168.1.4	TCP	http-alt > 58015 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
21	0.069362	192.168.1.4	192.168.1.2	TCP	58015 > vnc-server [<None>] Seq=1 win=2048 Len=0
22	0.069385	192.168.1.2	192.168.1.4	TCP	vnc-server > 58015 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
23	1.167387	192.168.1.4	192.168.1.2	TCP	58016 > vnc-server [<None>] Seq=1 win=3072 Len=0
24	1.167435	192.168.1.2	192.168.1.4	TCP	vnc-server > 58016 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
25	1.167606	192.168.1.4	192.168.1.2	TCP	58016 > http-alt [<None>] Seq=1 win=2048 Len=0
26	1.167636	192.168.1.2	192.168.1.4	TCP	http-alt > 58016 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
27	1.167706	192.168.1.4	192.168.1.2	TCP	58016 > ssh [<None>] Seq=1 win=1096 Len=0
28	1.167728	192.168.1.4	192.168.1.2	TCP	58016 > smux [<None>] Seq=1 win=2048 Len=0
29	1.167758	192.168.1.2	192.168.1.4	TCP	smux > 58016 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
30	1.167829	192.168.1.4	192.168.1.2	TCP	58016 > sunrpc [<None>] Seq=1 win=3072 Len=0
31	1.167850	192.168.1.4	192.168.1.2	TCP	58016 > rap [<None>] Seq=1 win=3072 Len=0
32	1.167894	192.168.1.2	192.168.1.4	TCP	rap > 58016 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
33	1.167936	192.168.1.4	192.168.1.2	TCP	58016 > h323hostcall [<None>] Seq=1 win=3072 Len=0
34	1.167961	192.168.1.2	192.168.1.4	TCP	h323hostcall > 58016 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
35	1.168025	192.168.1.4	192.168.1.2	TCP	58016 > pptp [<None>] Seq=1 win=3072 Len=0
36	1.168045	192.168.1.2	192.168.1.4	TCP	pptp > 58016 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
37	1.168112	192.168.1.4	192.168.1.2	TCP	58016 > microsoft-ds [<None>] Seq=1 win=1024 Len=0
38	1.168136	192.168.1.2	192.168.1.4	TCP	microsoft-ds > 58016 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
39	1.168201	192.168.1.4	192.168.1.2	TCP	58016 > submission [<None>] Seq=1 win=3072 Len=0
40	1.168226	192.168.1.2	192.168.1.4	TCP	submission > 58016 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
41	1.267433	192.168.1.4	192.168.1.2	TCP	58015 > pop3s [<None>] Seq=1 win=2048 Len=0
42	1.267470	192.168.1.2	192.168.1.4	TCP	pop3s > 58015 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
43	1.267613	192.168.1.4	192.168.1.2	TCP	58015 > pop3 [<None>] Seq=1 win=2048 Len=0
44	1.267645	192.168.1.2	192.168.1.4	TCP	pop3 > 58015 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
45	1.267714	192.168.1.4	192.168.1.2	TCP	58015 > dtl-tcp-1 [<None>] Seq=1 win=2048 Len=0
46	1.267740	192.168.1.2	192.168.1.4	TCP	dtl-tcp-1 > 58015 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
47	1.267806	192.168.1.4	192.168.1.2	TCP	58015 > imap [<None>] Seq=1 win=3072 Len=0

Ping Scan

Kaynak makinanın hedef makinaya tek bir ICMP Echo istek paketi göndereceği bu tarama türünde, IP adresi erişilebilir ve ICMP filtreleme bulunmadığı sürece, hedef makina ICMP Echo cevabı döndürecektir :



Eğer hedef makina erişilebilir değilse veya paket filtreleyici ICMP paketlerini filtreliyorsa, hedef makinadan herhangi bir cevap dönmeyecektir :



Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır :

nmap -sP -v [Hedef_IP]

#nmap -sP -v 192.168.1.2

at 2010-08-01 18:42 EEST

Initiating ARP Ping Scan at 18:42

Scanning 192.168.1.2 [1 port]

Completed ARP Ping Scan at 18:42, 0.03s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 18:42

Completed Parallel DNS resolution of 1 host. at 18:42, 0.16s elapsed

Nmap scan report for 192.168.1.2

Host is up (0.00040s latency).

MAC Address: 00:0C:29:D7:D3:65 (VMware)

Read data files from: /usr/local/share/nmap

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

Raw packets sent: 1 (28B) | Rcvd: 1 (28B)

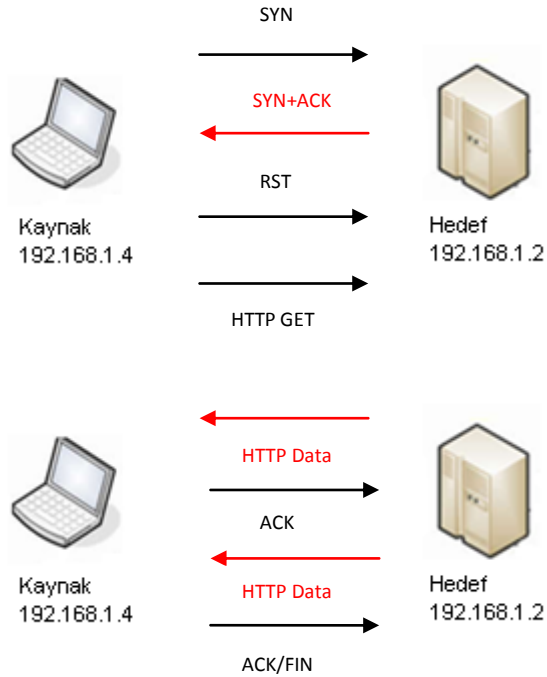
Version Detection

Version Detection, bütün portların bilgilerini bulabilecek herhangi bir tarama türü ile beraber çalışır.

Eğer herhangi bir tarama türü belirtilmezse yetkili kullanıcılar (root, admin) için TCP SYN, yetkisiz kullanıcılar için TCP Connect Scan çalıştırılır.

Eğer açık port bulunursa, Version Detection Scan hedef makina üzerinde araştırma sürecini başlatır. Hedef makinanın uygulamalarıyla direkt olarak iletişime geçerek elde edebileceği kadar bilgiyi almaya çalışır.

Başlangıçta varsayılan olarak TCP SYN Scan yapıldığı ve cevaplarının döndüğünü kabul edersek, 80. Port üzerinde çalışan HTTP hakkında bilgi toplayacak olan Version Detection Scan gerçekleştireceği tarama işlemleri aşağıdaki gibidir :



Farklı port ve uygulamalarda işlem farklı olacaktır.

Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır :

nmap -sV -v [Hedef_IP]

#nmap -sV -v 192.168.1.2

at 2010-08-01 18:43 EEST

NSE: Loaded 6 scripts for scanning.

Initiating ARP Ping Scan at 18:43

Scanning 192.168.1.2 [1 port]

Completed ARP Ping Scan at 18:43, 0.02s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 18:43

Completed Parallel DNS resolution of 1 host. at 18:43, 13.00s elapsed

Initiating SYN Stealth Scan at 18:43

Scanning 192.168.1.2 [1000 ports]

Discovered open port 80/tcp on 192.168.1.2

Discovered open port 22/tcp on 192.168.1.2

Discovered open port 53/tcp on 192.168.1.2

Discovered open port 111/tcp on 192.168.1.2

Discovered open port 2049/tcp on 192.168.1.2

Completed SYN Stealth Scan at 18:43, 2.32s elapsed (1000 total ports)

Initiating Service scan at 18:43

Scanning 5 services on 192.168.1.2

Completed Service scan at 18:43, 6.02s elapsed (5 services on 1 host)

Initiating RPCGrind Scan against 192.168.1.2 at 18:43

Completed RPCGrind Scan against 192.168.1.2 at 18:43, 0.01s elapsed (2 ports)

NSE: Script scanning 192.168.1.2.

NSE: Script Scanning completed.

Nmap scan report for 192.168.1.2

Host is up (0.0017s latency).

Not shown: 995 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 5.2 (protocol 2.0)

53/tcp open domain dnsmasq 2.48

80/tcp open http Apache httpd 2.2.13 ((Fedora))

111/tcp open rpcbind

2049/tcp open nfs 2-4 (rpc #100003)

MAC Address: 00:0C:29:D7:D3:65 (VMware)

Read data files from: /usr/local/share/nmap

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

Nmap done: 1 IP address (1 host up) scanned in 21.67 seconds

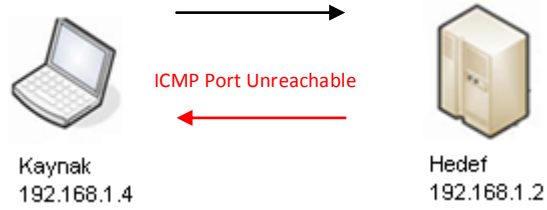
Raw packets sent: 1066 (46.888KB) | Rcvd: 1001 (40.048KB)

nmap_Version.pcap - Wireshark						
File Edit View Go Capture Analyze Statistics Telephony Tools Help						
Filter: tcp						
No. .	Time	Source	Destination	Protocol	Info	
14	13.043848	192.168.1.4	192.168.1.2	TCP	37315 > h323hostcall [SYN] Seq=0 Win=3072 Len=0 MSS=1460	
15	13.044002	192.168.1.2	192.168.1.4	TCP	h323hostcall > 37315 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
16	13.044209	192.168.1.4	192.168.1.2	TCP	37315 > http [SYN] Seq=0 Win=2048 Len=0 MSS=1460	
17	13.044312	192.168.1.2	192.168.1.4	TCP	http > 37315 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460	
18	13.044562	192.168.1.4	192.168.1.2	TCP	37315 > ftp [SYN] Seq=0 Win=3072 Len=0 MSS=1460	
19	13.044618	192.168.1.2	192.168.1.4	TCP	ftp > 37315 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
20	13.044765	192.168.1.4	192.168.1.2	TCP	37315 > http-alt [SYN] Seq=0 Win=2048 Len=0 MSS=1460	
21	13.044834	192.168.1.2	192.168.1.4	TCP	http-alt > 37315 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
22	13.044965	192.168.1.4	192.168.1.2	TCP	37315 > mysql [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
23	13.045023	192.168.1.2	192.168.1.4	TCP	mysql > 37315 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
24	13.045158	192.168.1.4	192.168.1.2	TCP	37315 > rap [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
25	13.045221	192.168.1.2	192.168.1.4	TCP	rap > 37315 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
26	13.045367	192.168.1.4	192.168.1.2	TCP	37315 > rtsp [SYN] Seq=0 Win=2048 Len=0 MSS=1460	
27	13.045421	192.168.1.2	192.168.1.4	TCP	rtsp > 37315 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
28	13.045604	192.168.1.4	192.168.1.2	TCP	37315 > dd1-tcp-1 [SYN] Seq=0 Win=3072 Len=0 MSS=1460	
29	13.045660	192.168.1.2	192.168.1.4	TCP	dd1-tcp-1 > 37315 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
30	13.045841	192.168.1.4	192.168.1.2	TCP	37315 > ssh [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
31	13.045934	192.168.1.2	192.168.1.4	TCP	ssh > 37315 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460	
32	13.046154	192.168.1.4	192.168.1.2	TCP	37315 > vnc-server [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
33	13.046202	192.168.1.2	192.168.1.4	TCP	vnc-server > 37315 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
34	13.046344	192.168.1.4	192.168.1.2	TCP	37315 > http [RST] Seq=1 Win=0 Len=0	
35	13.046993	192.168.1.4	192.168.1.2	TCP	37315 > ssh [RST] Seq=1 Win=0 Len=0	
36	13.047021	192.168.1.4	192.168.1.2	TCP	37315 > https [SYN] Seq=0 Win=3072 Len=0 MSS=1460	
37	13.047039	192.168.1.2	192.168.1.4	TCP	https > 37315 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
38	13.047198	192.168.1.4	192.168.1.2	TCP	37315 > ident [SYN] Seq=0 Win=2048 Len=0 MSS=1460	
39	13.047224	192.168.1.2	192.168.1.4	TCP	ident > 37315 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
40	13.047377	192.168.1.4	192.168.1.2	TCP	37315 > domain [SYN] Seq=0 Win=3072 Len=0 MSS=1460	
41	13.047433	192.168.1.2	192.168.1.4	TCP	domain > 37315 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460	
42	13.047772	192.168.1.4	192.168.1.2	TCP	37315 > netbios-ssn [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
43	13.047804	192.168.1.2	192.168.1.4	TCP	netbios-ssn > 37315 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
44	13.047960	192.168.1.4	192.168.1.2	TCP	37315 > blackjack [SYN] Seq=0 Win=4096 Len=0 MSS=1460	
45	13.068608	192.168.1.4	192.168.1.2	TCP	37315 > invokator [SYN] Seq=0 Win=3072 Len=0 MSS=1460	
46	13.068650	192.168.1.2	192.168.1.4	TCP	invokator > 37315 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
47	13.068698	192.168.1.4	192.168.1.2	TCP	37315 > 1906 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
48	13.068728	192.168.1.2	192.168.1.4	TCP	1906 > 37315 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
49	13.068754	192.168.1.4	192.168.1.2	TCP	37315 > avsecuremgmt [SYN] Seq=0 Win=2048 Len=0 MSS=1460	
50	13.068799	192.168.1.2	192.168.1.4	TCP	avsecuremgmt > 37315 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
51	13.068866	192.168.1.4	192.168.1.2	TCP	37315 > 61900 [SYN] Seq=0 Win=4096 Len=0 MSS=1460	
52	13.068919	192.168.1.2	192.168.1.4	TCP	61900 > 37315 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
53	13.068945	192.168.1.4	192.168.1.2	TCP	37315 > 57797 [SYN] Seq=0 Win=4096 Len=0 MSS=1460	
54	13.068970	192.168.1.2	192.168.1.4	TCP	57797 > 37315 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	
55	13.068995	192.168.1.4	192.168.1.2	TCP	37315 > berknet [SYN] Seq=0 Win=2048 Len=0 MSS=1460	
56	13.069010	192.168.1.2	192.168.1.4	TCP	berknet > 37315 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	

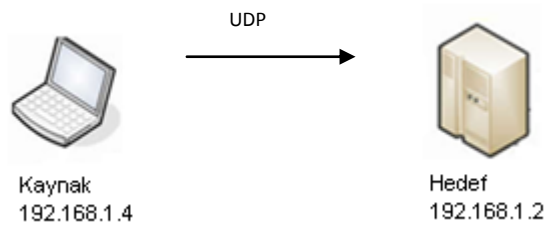
UDP Scan

Kaynak makinenin göndereceği UDP paketine ICMP Port Unreachable cevabı döndüren hedef makina kapalı kabul edilecektir. :

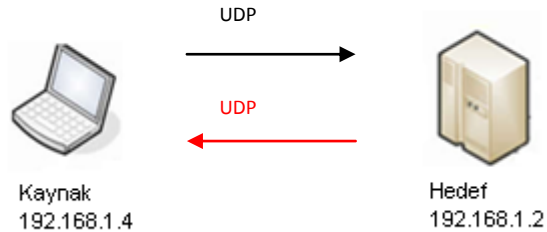
UDP



Herhangi bir tepki döndürmeyen hedef makina open | filtered (Bknz: Portların Taramalara Verebileceği Cevaplar) kabul edilecektir :



UDP paketiyle cevap döndüren hedef makinaya ait port açık kabul edilecektir :



Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır :

nmap -sU -v [Hedef_IP]

#nmap -sU -v 192.168.1.2

at 2010-08-01 18:44 EEST

Initiating ARP Ping Scan at 18:44

Scanning 192.168.1.2 [1 port]

Completed ARP Ping Scan at 18:44, 0.02s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 18:44

Completed Parallel DNS resolution of 1 host. at 18:44, 13.00s elapsed

Initiating UDP Scan at 18:44

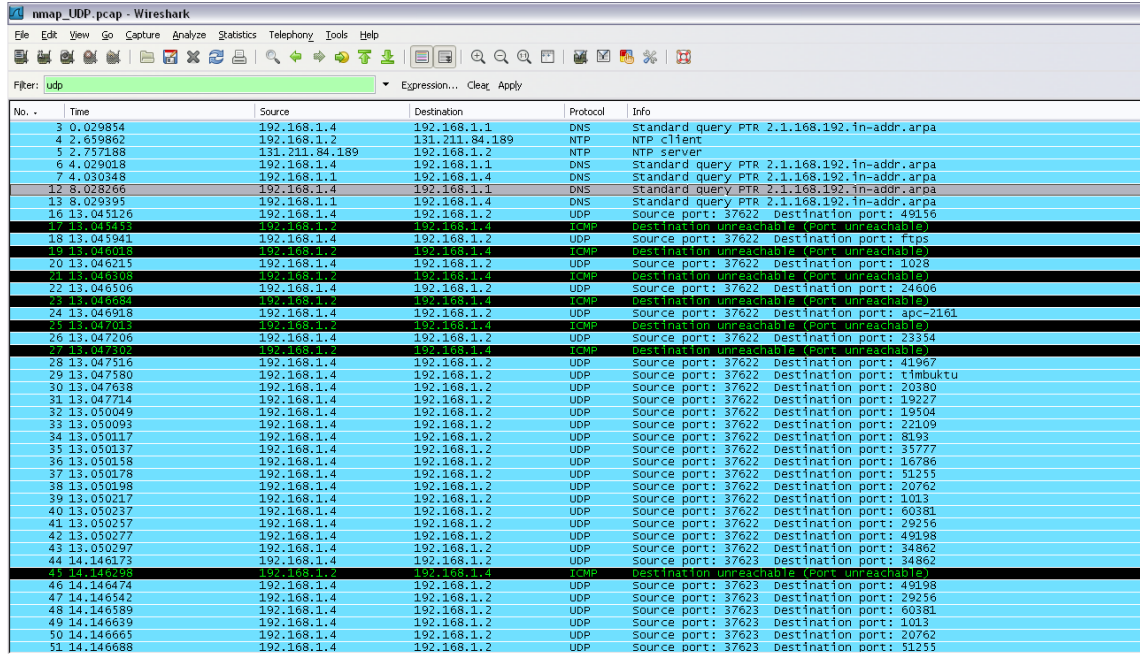
Scanning 192.168.1.2 [1000 ports]

Increasing send delay for 192.168.1.2 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.1.2 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.1.2 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.1.2 from 200 to 400 due to 11 out of 11 dropped probes since last increase.

Increasing send delay for 192.168.1.2 from 400 to 800 due to 11 out of 11 dropped probes since last increase.

UDP Scan Timing: About 4.88% done; ETC: 18:55 (0:10:05 remaining)

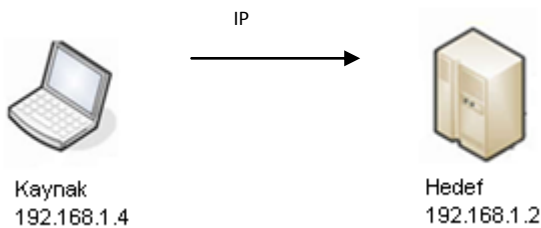
[3]+ Stopped nmap -sU -v 192.168.1.2



No.	Time	Source	Destination	Protocol	Info
3	0.029854	192.168.1.4	192.168.1.1	DNS	Standard query PTR 2.1.168.192.in-addr.arpa
4	2.659862	192.168.1.2	131.211.84.189	NTP	NTP client
5	2.757188	131.211.84.189	192.168.1.2	NTP	NTP server
6	4.029018	192.168.1.4	192.168.1.1	DNS	Standard query PTR 2.1.168.192.in-addr.arpa
7	4.030348	192.168.1.1	192.168.1.4	DNS	Standard query PTR 2.1.168.192.in-addr.arpa
12	8.028266	192.168.1.4	192.168.1.1	DNS	Standard query PTR 2.1.168.192.in-addr.arpa
13	8.029395	192.168.1.1	192.168.1.4	DNS	Standard query PTR 2.1.168.192.in-addr.arpa
16	13.045126	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 49156
17	13.045145	192.168.1.2	192.168.1.4	ICMP	Destination unreachable (Port unreachable)
18	13.045941	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 1028
19	13.046018	192.168.1.2	192.168.1.4	ICMP	Destination unreachable (Port unreachable)
20	13.046215	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 24506
21	13.046306	192.168.1.2	192.168.1.4	ICMP	Destination unreachable (Port unreachable)
22	13.046506	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 19227
23	13.046694	192.168.1.2	192.168.1.4	ICMP	Destination unreachable (Port unreachable)
24	13.046918	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 19504
25	13.047038	192.168.1.2	192.168.1.4	ICMP	Destination unreachable (Port unreachable)
26	13.047206	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 20762
27	13.047302	192.168.1.2	192.168.1.4	ICMP	Destination unreachable (Port unreachable)
28	13.047516	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 51255
29	13.047580	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 20762
30	13.047638	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 1013
31	13.047714	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 20762
32	13.050049	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 20762
33	13.050093	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 20762
34	13.050117	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 20762
35	13.050137	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 20762
36	13.050158	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 20762
37	13.050178	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 20762
38	13.050198	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 20762
39	13.050217	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 20762
40	13.050237	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 20762
41	13.050257	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 20762
42	13.050277	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 20762
43	13.050297	192.168.1.4	192.168.1.2	UDP	Source port: 37622 Destination port: 20762
44	14.146173	192.168.1.4	192.168.1.2	UDP	Source port: 37623 Destination port: 20762
45	14.146298	192.168.1.2	192.168.1.4	ICMP	Destination unreachable (Port unreachable)
46	14.146474	192.168.1.4	192.168.1.2	UDP	Source port: 37623 Destination port: 20762
47	14.146542	192.168.1.4	192.168.1.2	UDP	Source port: 37623 Destination port: 20762
48	14.146589	192.168.1.4	192.168.1.2	UDP	Source port: 37623 Destination port: 20762
49	14.146639	192.168.1.4	192.168.1.2	UDP	Source port: 37623 Destination port: 20762
50	14.146665	192.168.1.4	192.168.1.2	UDP	Source port: 37623 Destination port: 20762
51	14.146688	192.168.1.4	192.168.1.2	UDP	Source port: 37623 Destination port: 20762

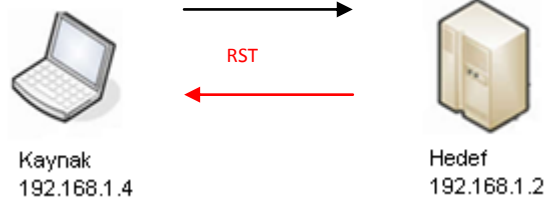
IP Protocol Scan

IP paketleriyle gerçekleştirilen bu taramada, erişilemeyen bir IP taramaya cevap vermeyecektir:



Erişilebilen bir IP ise protokol tipine mahsus olacak şekilde RST bayraklı paket döndürecekler :

IP



Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır :

nmap -sO -v [Hedef_IP]

#nmap -sO -v 192.168.1.2

at 2010-08-01 18:46 EEST

Initiating ARP Ping Scan at 18:46

Scanning 192.168.1.2 [1 port]

Completed ARP Ping Scan at 18:46, 0.02s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 18:46

Completed Parallel DNS resolution of 1 host. at 18:46, 0.14s elapsed

Initiating IPProto Scan at 18:46

Scanning 192.168.1.2 [256 ports]

Discovered open port 6/tcp on 192.168.1.2

Discovered open port 1/tcp on 192.168.1.2

Increasing send delay for 192.168.1.2 from 0 to 5 due to max_successful_tryno increase to 4

Increasing send delay for 192.168.1.2 from 5 to 10 due to max_successful_tryno increase to 5

Increasing send delay for 192.168.1.2 from 10 to 20 due to max_successful_tryno increase to 6

Increasing send delay for 192.168.1.2 from 20 to 40 due to max_successful_tryno increase to 7

Increasing send delay for 192.168.1.2 from 40 to 80 due to max_successful_tryno increase to 8

Increasing send delay for 192.168.1.2 from 80 to 160 due to max_successful_tryno increase to 9

Increasing send delay for 192.168.1.2 from 160 to 320 due to 11 out of 11 dropped probes since last increase.

IPProto Scan Timing: About 18.89% done; ETC: 18:48 (0:02:13 remaining)

Increasing send delay for 192.168.1.2 from 320 to 640 due to 11 out of 14 dropped probes since last increase.

Increasing send delay for 192.168.1.2 from 640 to 1000 due to 11 out of 23 dropped probes since last increase.

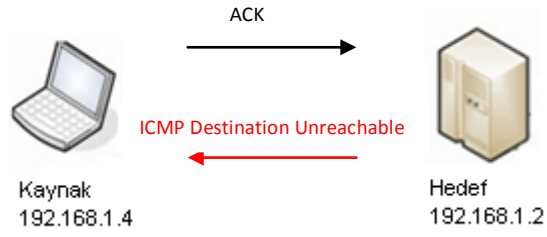
IPProto Scan Timing: About 32.00% done; ETC: 18:49 (0:02:29 remaining)

[4]+ Stopped nmap -sO -v 192.168.1.2

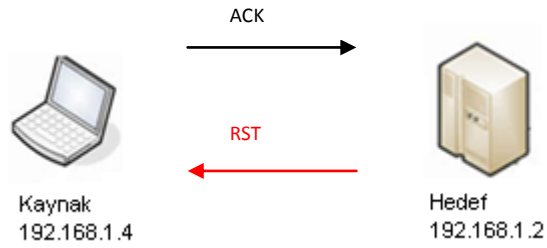
No.	Time	Source	Destination	Protocol	Info
5	0.182962	192.168.1.4	192.168.1.2	IP	Unknown (0x92)
6	0.183155	192.168.1.2	192.168.1.4	ICMP	Destination unreachable (Protocol unreachable)
7	0.183349	192.168.1.4	192.168.1.2	IP	TATP (0x75)
8	0.183546	192.168.1.2	192.168.1.4	ICMP	Destination unreachable (Protocol unreachable)
9	0.183695	192.168.1.4	192.168.1.2	IP	Unknown (0x9e)
10	0.183742	192.168.1.2	192.168.1.4	ICMP	Destination unreachable (Protocol unreachable)
11	0.183830	192.168.1.4	192.168.1.2	IP	IDRP (0x2d)
12	0.183909	192.168.1.2	192.168.1.4	ICMP	Destination unreachable (Protocol unreachable)
13	0.183994	192.168.1.4	192.168.1.2	IP	SM (0x7a)
14	0.184041	192.168.1.2	192.168.1.4	ICMP	Destination unreachable (Protocol unreachable)
15	0.184138	192.168.1.4	192.168.1.2	IP	Unknown (0xf3)
16	0.184195	192.168.1.2	192.168.1.4	ICMP	Destination unreachable (Protocol unreachable)
17	0.184295	192.168.1.4	192.168.1.2	IPv6	[Malformed Packet]
18	0.184346	192.168.1.4	192.168.1.2	IP	QNX (0x6a)
19	0.184394	192.168.1.4	192.168.1.2	IP	Multiplex (0x12)
20	0.184423	192.168.1.4	192.168.1.2	IP	Packet Video (0x4b)
21	0.187344	192.168.1.4	192.168.1.2	IP	Unknown (0x9d)
22	0.187390	192.168.1.4	192.168.1.2	IP	Unknown (0xd1)
23	0.187419	192.168.1.4	192.168.1.2	IP	Unknown (0xe1)
24	0.187444	192.168.1.4	192.168.1.2	IP	Interdomain routing (0x23)
25	0.187469	192.168.1.4	192.168.1.2	ICMP	Echo (ping) request
26	0.187522	192.168.1.2	192.168.1.4	ICMP	Echo (ping) reply
27	0.187637	192.168.1.4	192.168.1.2	IP	AX.25 Frames (0x5d)
28	0.187687	192.168.1.4	192.168.1.2	IP	Unknown (0xba)
29	0.187716	192.168.1.4	192.168.1.2	IP	Compaq Peer (0x6e)
30	0.187741	192.168.1.4	192.168.1.2	IP	Unknown (0xed)
31	0.187766	192.168.1.4	192.168.1.2	IP	SCPS (0x69)
32	0.187817	192.168.1.4	192.168.1.2	TCP	54194 > 54194 [ACK] Seq=1 Ack=1 Win=3072 Len=0
33	0.187830	192.168.1.2	192.168.1.4	TCP	54194 > 54194 [RST] Seq=1 Win=0 Len=0
34	0.187957	192.168.1.4	192.168.1.2	IPComp	[Malformed Packet]
35	0.190712	192.168.1.4	192.168.1.2	IP	Unknown (0x95)
36	0.190750	192.168.1.4	192.168.1.2	IP	GGP (0x03)
37	0.190790	192.168.1.4	192.168.1.2	IP	Dynamic source routing (0x30)
38	0.190812	192.168.1.4	192.168.1.2	IP	Unknown (0xef)
39	1.284220	192.168.1.4	192.168.1.2	IP	Unknown (0xef)
40	1.284297	192.168.1.2	192.168.1.4	ICMP	Destination unreachable (Protocol unreachable)
41	1.284417	192.168.1.4	192.168.1.2	IP	Dynamic source routing (0x30)
42	1.284453	192.168.1.4	192.168.1.2	IP	GGP (0x03)
43	1.284473	192.168.1.4	192.168.1.2	IP	Unknown (0x95)
44	1.284492	192.168.1.4	192.168.1.2	IPComp	[Malformed Packet]
45	1.284510	192.168.1.4	192.168.1.2	IP	SCPS (0x69)
46	1.284529	192.168.1.4	192.168.1.2	IP	Unknown (0xed)
47	1.284547	192.168.1.4	192.168.1.2	IP	Compaq Peer (0x6e)

ACK Scan

Kaynak makinanın hedef makinaya TCP ACK bayraklı paket göndereceği bu tarama türünde, hedef makina tarafından ICMP Destination Unreachable mesajı dönerse yada herhangi bir tepki oluşmazsa port “filtered” olarak kabul edilir :



Eğer hedef makina RST bayraklı paket döndürürse port “unfiltered” kabul edilir :



Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır :

nmap -sA -v [Hedef_IP]

#nmap -sA -v 192.168.1.2 -p80

at 2010-08-01 18:51 EEST

Initiating ARP Ping Scan at 18:51

Scanning 192.168.1.2 [1 port]

Completed ARP Ping Scan at 18:51, 0.02s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 18:51

Completed Parallel DNS resolution of 1 host. at 18:51, 0.02s elapsed

Initiating ACK Scan at 18:51

Scanning 192.168.1.2 [1 port]

Completed ACK Scan at 18:51, 0.03s elapsed (1 total ports)

Nmap scan report for 192.168.1.2

Host is up (0.0014s latency).

PORT STATE SERVICE

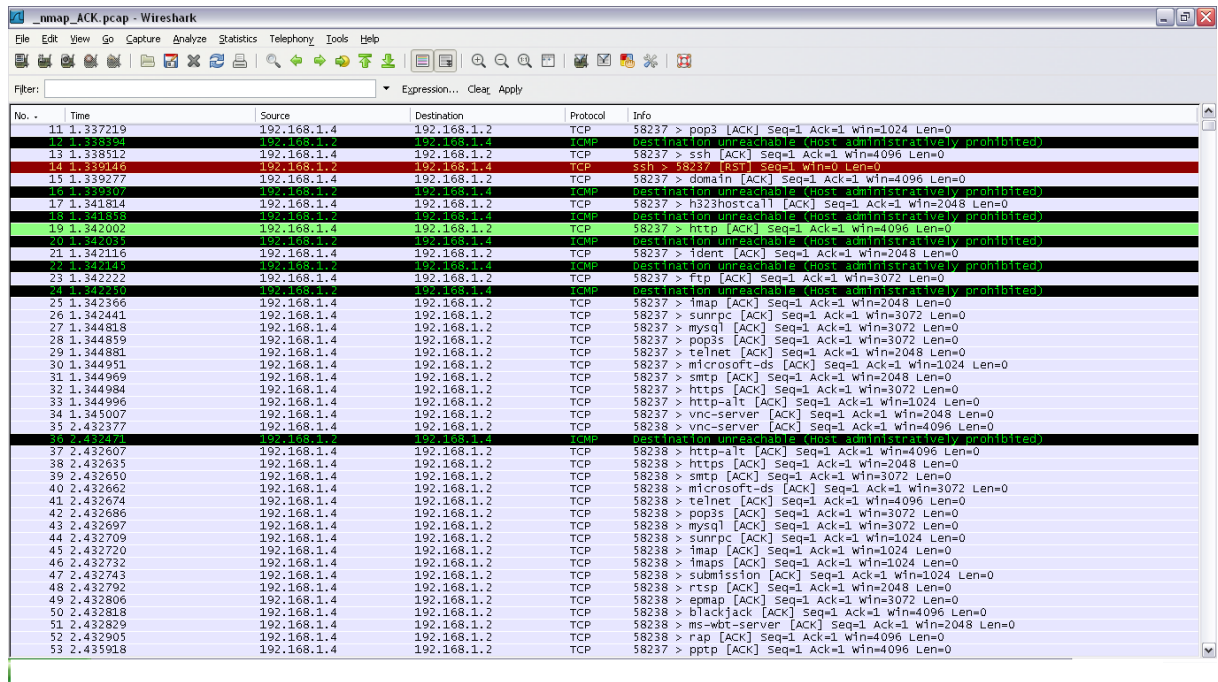
80/tcp unfiltered http

MAC Address: 00:0C:29:D7:D3:65 (VMware)

Read data files from: /usr/local/share/nmap

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

Raw packets sent: 2 (68B) | Rcvd: 2 (68B)



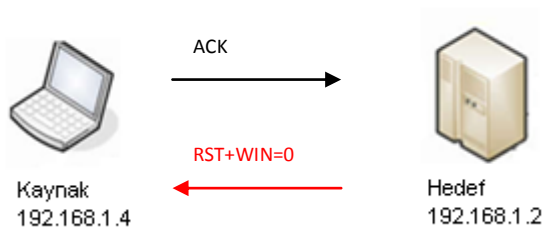
No.	Time	Source	Destination	Protocol	Info
11	1.337219	192.168.1.4	192.168.1.2	TCP	58237 > pop3 [ACK] Seq=1 Ack=1 Win=1024 Len=0
12	1.338354	192.168.1.2	192.168.1.4	ICMP	destination unreachable (host administratively prohibited)
13	1.338512	192.168.1.4	192.168.1.2	TCP	58237 > ssh [ACK] Seq=1 Ack=1 Win=4096 Len=0
14	1.339116	192.168.1.2	192.168.1.4	TCP	58237 > 3389 [ACK] Seq=1 Ack=1 Win=1024 Len=0
15	1.339277	192.168.1.4	192.168.1.2	TCP	58237 > domain [ACK] Seq=1 Ack=1 Win=4096 Len=0
16	1.339307	192.168.1.2	192.168.1.4	ICMP	destination unreachable (host administratively prohibited)
17	1.341814	192.168.1.4	192.168.1.2	TCP	58237 > h323hostcall [ACK] Seq=1 Ack=1 Win=2048 Len=0
18	1.342436	192.168.1.2	192.168.1.4	ICMP	destination unreachable (host administratively prohibited)
19	1.342002	192.168.1.4	192.168.1.2	TCP	58237 > http [ACK] Seq=1 Ack=1 Win=4096 Len=0
20	1.342035	192.168.1.2	192.168.1.4	ICMP	destination unreachable (host administratively prohibited)
21	1.342116	192.168.1.4	192.168.1.2	TCP	58237 > ident [ACK] Seq=1 Ack=1 Win=2048 Len=0
22	1.342145	192.168.1.2	192.168.1.4	ICMP	destination unreachable (host administratively prohibited)
23	1.342222	192.168.1.4	192.168.1.2	TCP	58237 > ftp [ACK] Seq=1 Ack=1 Win=3072 Len=0
24	1.342230	192.168.1.2	192.168.1.4	ICMP	destination unreachable (host administratively prohibited)
25	1.342366	192.168.1.4	192.168.1.2	TCP	58237 > imap [ACK] Seq=1 Ack=1 Win=2048 Len=0
26	1.342441	192.168.1.4	192.168.1.2	TCP	58237 > sunrpc [ACK] Seq=1 Ack=1 Win=3072 Len=0
27	1.344818	192.168.1.4	192.168.1.2	TCP	58237 > mysql [ACK] Seq=1 Ack=1 Win=3072 Len=0
28	1.344859	192.168.1.4	192.168.1.2	TCP	58237 > pop3s [ACK] Seq=1 Ack=1 Win=3072 Len=0
29	1.344881	192.168.1.4	192.168.1.2	TCP	58237 > telnet [ACK] Seq=1 Ack=1 Win=2048 Len=0
30	1.344951	192.168.1.4	192.168.1.2	TCP	58237 > microsoft-ds [ACK] Seq=1 Ack=1 Win=1024 Len=0
31	1.344969	192.168.1.4	192.168.1.2	TCP	58237 > smtp [ACK] Seq=1 Ack=1 Win=2048 Len=0
32	1.344984	192.168.1.4	192.168.1.2	TCP	58237 > https [ACK] Seq=1 Ack=1 Win=3072 Len=0
33	1.344996	192.168.1.4	192.168.1.2	TCP	58237 > http-alt [ACK] Seq=1 Ack=1 Win=1024 Len=0
34	1.345007	192.168.1.4	192.168.1.2	TCP	58237 > vnc-server [ACK] Seq=1 Ack=1 Win=2048 Len=0
35	2.432377	192.168.1.4	192.168.1.2	TCP	58238 > vnc-server [ACK] Seq=1 Ack=1 Win=4096 Len=0
36	2.432414	192.168.1.2	192.168.1.4	ICMP	destination unreachable (host administratively prohibited)
37	2.432607	192.168.1.4	192.168.1.2	TCP	58238 > http-alt [ACK] Seq=1 Ack=1 Win=4096 Len=0
38	2.432635	192.168.1.4	192.168.1.2	TCP	58238 > https [ACK] Seq=1 Ack=1 Win=2048 Len=0
39	2.432650	192.168.1.4	192.168.1.2	TCP	58238 > smtp [ACK] Seq=1 Ack=1 Win=3072 Len=0
40	2.432662	192.168.1.4	192.168.1.2	TCP	58238 > microsoft-ds [ACK] Seq=1 Ack=1 Win=3072 Len=0
41	2.432674	192.168.1.4	192.168.1.2	TCP	58238 > telnet [ACK] Seq=1 Ack=1 Win=4096 Len=0
42	2.432686	192.168.1.4	192.168.1.2	TCP	58238 > pop3s [ACK] Seq=1 Ack=1 Win=3072 Len=0
43	2.432697	192.168.1.4	192.168.1.2	TCP	58238 > mysql [ACK] Seq=1 Ack=1 Win=3072 Len=0
44	2.432709	192.168.1.4	192.168.1.2	TCP	58238 > sunrpc [ACK] Seq=1 Ack=1 Win=1024 Len=0
45	2.432720	192.168.1.4	192.168.1.2	TCP	58238 > imap [ACK] Seq=1 Ack=1 Win=1024 Len=0
46	2.432732	192.168.1.4	192.168.1.2	TCP	58238 > imaps [ACK] Seq=1 Ack=1 Win=1024 Len=0
47	2.432743	192.168.1.4	192.168.1.2	TCP	58238 > submission [ACK] Seq=1 Ack=1 Win=1024 Len=0
48	2.432792	192.168.1.4	192.168.1.2	TCP	58238 > rtsp [ACK] Seq=1 Ack=1 Win=2048 Len=0
49	2.432806	192.168.1.4	192.168.1.2	TCP	58238 > gmap [ACK] Seq=1 Ack=1 Win=3072 Len=0
50	2.432818	192.168.1.4	192.168.1.2	TCP	58238 > blackjack [ACK] Seq=1 Ack=1 Win=4096 Len=0
51	2.432829	192.168.1.4	192.168.1.2	TCP	58238 > ms-wbt-server [ACK] Seq=1 Ack=1 Win=2048 Len=0
52	2.432905	192.168.1.4	192.168.1.2	TCP	58238 > rap [ACK] Seq=1 Ack=1 Win=4096 Len=0
53	2.432918	192.168.1.4	192.168.1.2	TCP	58238 > pptp [ACK] Seq=1 Ack=1 Win=4096 Len=0

Window Scan

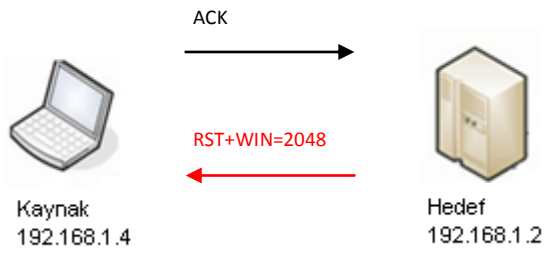
-Window Scan, ACK Scan türüne benzer ancak bir önemli farkı vardır. Window Scan portların açık olma durumlarını yani “open” durumlarını gösterebilir. Bu taramanın ismi TCP Windowing işleminden

gelmektedir. Bazı TCP yığınları, RST bayraklı paketlere cevap döndüreceği zaman, kendilerine mahsus window boyutları sağlarlar.

Hedef makinaya ait kapalı bir porttan dönen RST frame ait window boyutu sıfırdır (0) :



Hedef makinaya ait açık bir porttan dönen RST frame ait window boyutu sıfırdan farklı olur :



Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır :

nmap -sW -v [Hedef_IP]

#nmap -sW -v 192.168.1.2

at 2010-08-01 18:52 EEST

Initiating ARP Ping Scan at 18:52

Scanning 192.168.1.2 [1 port]

Completed ARP Ping Scan at 18:52, 0.02s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 18:52

Completed Parallel DNS resolution of 1 host. at 18:52, 0.02s elapsed

Initiating Window Scan at 18:52

Scanning 192.168.1.2 [1000 ports]

Completed Window Scan at 18:52, 2.27s elapsed (1000 total ports)

Nmap scan report for 192.168.1.2

Host is up (0.0011s latency).

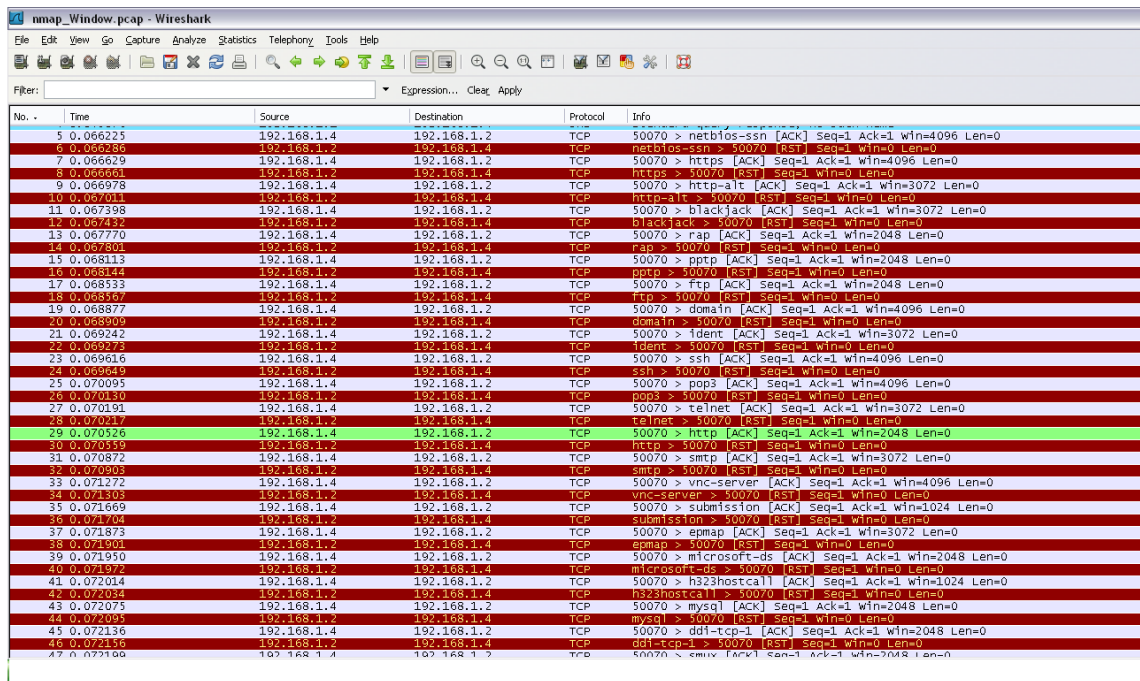
All 1000 scanned ports on 192.168.1.2 are closed

MAC Address: 00:0C:29:D7:D3:65 (VMware)

Read data files from: /usr/local/share/nmap

Nmap done: 1 IP address (1 host up) scanned in 2.46 seconds

Raw packets sent: 1062 (42.468KB) | Rcvd: 1001 (40.028KB)

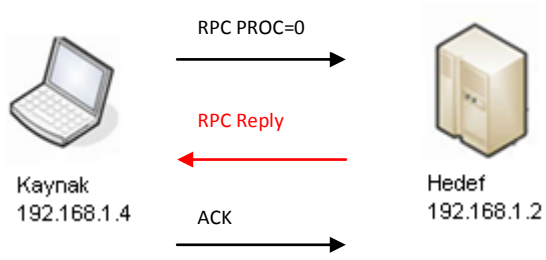
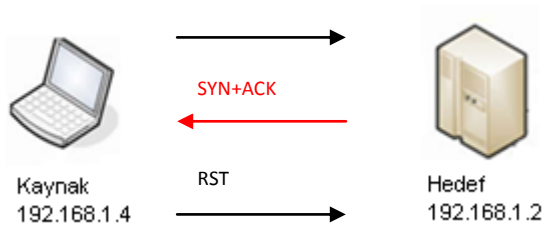


No. ·	Time	Source	Destination	Protocol	Info
5	0.066225	192.168.1.4	192.168.1.2	TCP	50070 > netbios-ssn [ACK] Seq=1 Ack=1 win=4096 Len=0
6	0.066286	192.168.1.2	192.168.1.4	TCP	netbios-ssn > 50070 [RST] Seq=1 win=0 Len=0
7	0.066629	192.168.1.4	192.168.1.2	TCP	50070 > https [ACK] Seq=1 Ack=1 win=4096 Len=0
8	0.066965	192.168.1.2	192.168.1.4	TCP	https > 50070 [RST] Seq=1 win=0 Len=0
9	0.066978	192.168.1.4	192.168.1.2	TCP	50070 > http-alt [ACK] Seq=1 Ack=1 win=3072 Len=0
10	0.067011	192.168.1.2	192.168.1.4	TCP	http-alt > 50070 [RST] Seq=1 win=0 Len=0
11	0.067398	192.168.1.4	192.168.1.2	TCP	50070 > blackjack [ACK] Seq=1 Ack=1 win=3072 Len=0
12	0.067435	192.168.1.2	192.168.1.4	TCP	blackjack > 50070 [RST] Seq=1 win=0 Len=0
13	0.067770	192.168.1.4	192.168.1.2	TCP	50070 > rap [ACK] Seq=1 Ack=1 win=2048 Len=0
14	0.067801	192.168.1.2	192.168.1.4	TCP	rap > 50070 [RST] Seq=1 win=0 Len=0
15	0.068113	192.168.1.4	192.168.1.2	TCP	50070 > pptp [ACK] Seq=1 Ack=1 win=2048 Len=0
16	0.068144	192.168.1.2	192.168.1.4	TCP	pptp > 50070 [RST] Seq=1 win=0 Len=0
17	0.068333	192.168.1.4	192.168.1.2	TCP	50070 > ftp [ACK] Seq=1 Ack=1 win=2048 Len=0
18	0.068567	192.168.1.2	192.168.1.4	TCP	ftp > 50070 [RST] Seq=1 win=0 Len=0
19	0.068877	192.168.1.4	192.168.1.2	TCP	50070 > domain [ACK] Seq=1 Ack=1 win=4096 Len=0
20	0.068909	192.168.1.2	192.168.1.4	TCP	domain > 50070 [RST] Seq=1 win=0 Len=0
21	0.069242	192.168.1.4	192.168.1.2	TCP	50070 > ident [ACK] Seq=1 Ack=1 win=3072 Len=0
22	0.069273	192.168.1.2	192.168.1.4	TCP	ident > 50070 [RST] Seq=1 win=0 Len=0
23	0.069616	192.168.1.4	192.168.1.2	TCP	50070 > ssh [ACK] Seq=1 Ack=1 win=4096 Len=0
24	0.069649	192.168.1.2	192.168.1.4	TCP	ssh > 50070 [RST] Seq=1 win=0 Len=0
25	0.070095	192.168.1.4	192.168.1.2	TCP	50070 > pop3 [ACK] Seq=1 Ack=1 win=4096 Len=0
26	0.070180	192.168.1.2	192.168.1.4	TCP	pop3 > 50070 [RST] Seq=1 win=0 Len=0
27	0.070191	192.168.1.4	192.168.1.2	TCP	50070 > telnet [ACK] Seq=1 Ack=1 win=3072 Len=0
28	0.070217	192.168.1.2	192.168.1.4	TCP	telnet > 50070 [RST] Seq=1 win=0 Len=0
29	0.070526	192.168.1.4	192.168.1.2	TCP	50070 > http [ACK] Seq=1 Ack=1 win=2048 Len=0
30	0.070589	192.168.1.2	192.168.1.4	TCP	http > 50070 [RST] Seq=1 win=0 Len=0
31	0.070772	192.168.1.4	192.168.1.2	TCP	50070 > smtp [ACK] Seq=1 Ack=1 win=3072 Len=0
32	0.070903	192.168.1.2	192.168.1.4	TCP	smtp > 50070 [RST] Seq=1 win=0 Len=0
33	0.071272	192.168.1.4	192.168.1.2	TCP	50070 > vnc-server [ACK] Seq=1 Ack=1 win=4096 Len=0
34	0.071505	192.168.1.2	192.168.1.4	TCP	vnc-server > 50070 [RST] Seq=1 win=0 Len=0
35	0.071669	192.168.1.4	192.168.1.2	TCP	50070 > submission [ACK] Seq=1 Ack=1 win=1024 Len=0
36	0.071704	192.168.1.2	192.168.1.4	TCP	submission > 50070 [RST] Seq=1 win=0 Len=0
37	0.071873	192.168.1.4	192.168.1.2	TCP	50070 > epmap [ACK] Seq=1 Ack=1 win=3072 Len=0
38	0.071905	192.168.1.2	192.168.1.4	TCP	epmap > 50070 [RST] Seq=1 win=0 Len=0
39	0.071950	192.168.1.4	192.168.1.2	TCP	50070 > microsoft-ds [ACK] Seq=1 Ack=1 win=1024 Len=0
40	0.071972	192.168.1.2	192.168.1.4	TCP	microsoft-ds > 50070 [RST] Seq=1 win=0 Len=0
41	0.072014	192.168.1.4	192.168.1.2	TCP	50070 > h323hostcall [ACK] Seq=1 Ack=1 win=1024 Len=0
42	0.072034	192.168.1.2	192.168.1.4	TCP	h323hostcall > 50070 [RST] Seq=1 win=0 Len=0
43	0.072075	192.168.1.4	192.168.1.2	TCP	50070 > mysql [ACK] Seq=1 Ack=1 win=2048 Len=0
44	0.072095	192.168.1.2	192.168.1.4	TCP	mysql > 50070 [RST] Seq=1 win=0 Len=0
45	0.072136	192.168.1.4	192.168.1.2	TCP	50070 > dd1-tcp-1 [ACK] Seq=1 Ack=1 win=2048 Len=0
46	0.072156	192.168.1.2	192.168.1.4	TCP	dd1-tcp-1 > 50070 [RST] Seq=1 win=0 Len=0
47	0.072180	192.168.1.4	192.168.1.2	TCP	50070 > smux [ACK] Seq=1 Ack=1 win=2048 Len=0

RPC Scan

RPC Scan, hedef makina üzerinde kořan RPC uygulamalarını keřfeder. Bařka bir tarama t r  ile a ık portlar keřfedildikten sonra,RPC Scan hedef makinanın a ık portlarına RPC null g ndererek, eēē

alışan bir RPC uygulaması varsa, RPC uygulamasını harekete geçirir.RPC Scan, Version Detection Scan işlemi esnasında otomatik olarak alıştırılır :



Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır :

nmap -sR -v [Hedef_IP]

#nmap -sR -v 192.168.1.2

```
at 2010-08-01 18:53 EEST
Initiating ARP Ping Scan at 18:53
Scanning 192.168.1.2 [1 port]
Completed ARP Ping Scan at 18:53, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:53
Completed Parallel DNS resolution of 1 host. at 18:53, 0.02s elapsed
Initiating SYN Stealth Scan at 18:53
Scanning 192.168.1.2 [1000 ports]
Discovered open port 111/tcp on 192.168.1.2
Discovered open port 80/tcp on 192.168.1.2
Discovered open port 53/tcp on 192.168.1.2
Discovered open port 22/tcp on 192.168.1.2
Discovered open port 2049/tcp on 192.168.1.2
Completed SYN Stealth Scan at 18:53, 2.28s elapsed (1000 total ports)
Initiating RPCGrind Scan against 192.168.1.2 at 18:53
Completed RPCGrind Scan against 192.168.1.2 at 18:53, 0.36s elapsed (5 ports)
Nmap scan report for 192.168.1.2
Host is up (0.0012s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH_5.3p1 Debian-5ubuntu1
53/tcp    open  domain       BIND 9.3.4-Debian
80/tcp    open  http         Apache/2.2.8-2.2.8-2ubuntu1
111/tcp   open  rpcbind      rpcbind (v2-4)
2049/tcp  open  nfs (nfs V2-4) 2-4 (rpc #100003)
MAC Address: 00:0C:29:D7:D3:65 (VMware)
Read data files from: /usr/local/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.84 seconds
Raw packets sent: 1098 (48.296KB) | Rcvd: 1001 (40.048KB)
```

nmap_rpc.pcap - Wireshark					
File Edit View Go Capture Analyze Statistics Telephony Tools Help					
Filter: Expression... Clear Apply					
No. ·	Time	Source	Destination	Protocol	Info
5	0.080469	192.168.1.2	192.168.1.2	TCP	45941 > smux [SYN] Seq=0 win=4096 Len=0 MSS=1460
6	0.080541	192.168.1.2	192.168.1.4	TCP	smux > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
7	0.080625	192.168.1.4	192.168.1.2	TCP	45941 > dd1-tcp-1 [SYN] Seq=0 win=4096 Len=0 MSS=1460
8	0.080654	192.168.1.2	192.168.1.4	TCP	dd1-tcp-1 > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
9	0.080710	192.168.1.4	192.168.1.2	TCP	45941 > submission [SYN] Seq=0 win=2048 Len=0 MSS=1460
10	0.080738	192.168.1.2	192.168.1.4	TCP	submission > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
11	0.080794	192.168.1.4	192.168.1.2	TCP	45941 > http-alt [SYN] Seq=0 win=2048 Len=0 MSS=1460
12	0.080820	192.168.1.2	192.168.1.4	TCP	http-alt > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
13	0.080875	192.168.1.4	192.168.1.2	TCP	45941 > gmap [SYN] Seq=0 win=4096 Len=0 MSS=1460
14	0.080911	192.168.1.2	192.168.1.4	TCP	gmap > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
15	0.080965	192.168.1.4	192.168.1.2	TCP	45941 > imap [SYN] Seq=0 win=2048 Len=0 MSS=1460
16	0.080992	192.168.1.2	192.168.1.4	TCP	imap > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
17	0.081048	192.168.1.4	192.168.1.2	TCP	45941 > sunrpc [SYN] Seq=0 win=3072 Len=0 MSS=1460
18	0.081101	192.168.1.2	192.168.1.4	TCP	sunrpc > 45941 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460
19	0.081282	192.168.1.4	192.168.1.2	TCP	45941 > telnet [SYN] Seq=0 win=3072 Len=0 MSS=1460
20	0.081312	192.168.1.2	192.168.1.4	TCP	telnet > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
21	0.081374	192.168.1.4	192.168.1.2	TCP	45941 > h323hostcall [SYN] Seq=0 win=1024 Len=0 MSS=1460
22	0.081401	192.168.1.2	192.168.1.4	TCP	h323hostcall > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
23	0.081456	192.168.1.4	192.168.1.2	TCP	45941 > microsoft-ds [SYN] Seq=0 win=2048 Len=0 MSS=1460
24	0.081484	192.168.1.2	192.168.1.4	TCP	microsoft-ds > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
25	0.081546	192.168.1.4	192.168.1.2	TCP	45941 > sunrpc [RST] Seq=1 win=0 Len=0
26	0.082407	192.168.1.4	192.168.1.2	TCP	45941 > pop3s [SYN] Seq=0 win=4096 Len=0 MSS=1460
27	0.082442	192.168.1.2	192.168.1.4	TCP	pop3s > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
28	0.082512	192.168.1.4	192.168.1.2	TCP	45941 > http [SYN] Seq=0 win=3072 Len=0 MSS=1460
29	0.082559	192.168.1.2	192.168.1.4	TCP	http > 45941 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460
30	0.082607	192.168.1.4	192.168.1.2	TCP	45941 > netbios-ssn [SYN] Seq=0 win=2048 Len=0 MSS=1460
31	0.082670	192.168.1.2	192.168.1.4	TCP	netbios-ssn > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
32	0.082842	192.168.1.4	192.168.1.2	TCP	45941 > imaps [SYN] Seq=0 win=1024 Len=0 MSS=1460
33	0.082868	192.168.1.2	192.168.1.4	TCP	imaps > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
34	0.082921	192.168.1.4	192.168.1.2	TCP	45941 > mysql [SYN] Seq=0 win=2048 Len=0 MSS=1460
35	0.082946	192.168.1.2	192.168.1.4	TCP	mysql > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
36	0.082998	192.168.1.4	192.168.1.2	TCP	45941 > https [SYN] Seq=0 win=1024 Len=0 MSS=1460
37	0.083023	192.168.1.2	192.168.1.4	TCP	https > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
38	0.083077	192.168.1.4	192.168.1.2	TCP	45941 > pop3 [SYN] Seq=0 win=1024 Len=0 MSS=1460
39	0.083104	192.168.1.2	192.168.1.4	TCP	pop3 > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
40	0.083157	192.168.1.4	192.168.1.2	TCP	45941 > ftp [SYN] Seq=0 win=2048 Len=0 MSS=1460
41	0.083183	192.168.1.2	192.168.1.4	TCP	ftp > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
42	0.083241	192.168.1.4	192.168.1.2	TCP	45941 > nap [RST] Seq=0 win=4096 Len=0 MSS=1460
43	0.083266	192.168.1.2	192.168.1.4	TCP	nap > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
44	0.083320	192.168.1.4	192.168.1.2	TCP	45941 > smtp [SYN] Seq=0 win=4096 Len=0 MSS=1460
45	0.083346	192.168.1.2	192.168.1.4	TCP	smtp > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
46	0.083400	192.168.1.4	192.168.1.2	TCP	45941 > blackjack [SYN] Seq=0 win=2048 Len=0 MSS=1460
47	0.083435	192.168.1.2	192.168.1.4	TCP	blackjack > 45941 [RST, ACK] Seq=1 Ack=1 win=0 Len=0

List Scan

Bu tarama türü gerçek bir tarama değildir. Sadece Nmapin sorun çözme ve test yeteneklerini aktif kılar. Taranacak olan aktif makinaların İplerini sıralar. Eğer reverse DNS çözümlemesi iptal edilmişse List Scan network üzerinde tamamen sessizdir. Herhangi bir paket almaz veya göndermez. Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır :

nmap -sL -v [Hedef_IP]

nmap -sL -v 192.168.1.2

Initiating Parallel DNS resolution of 1 host. at 18:54

Completed Parallel DNS resolution of 1 host. at 18:54, 0.02s elapsed

Nmap scan report for 192.168.1.2

Nmap done: 1 IP address (0 hosts up) scanned in 0.02 seconds

IdleScan

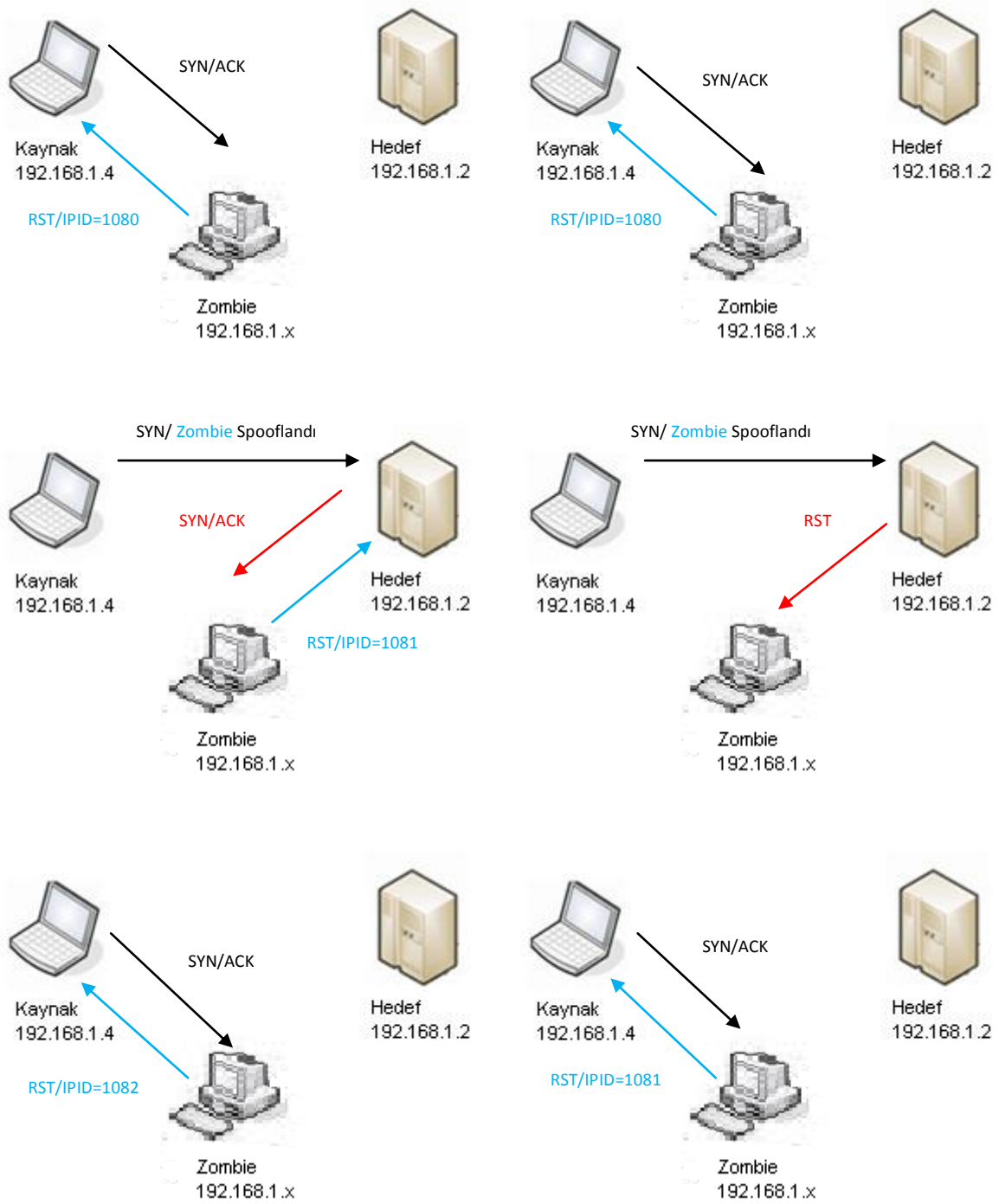
Kaynak makinanın hedef makinaryı tarama esnasında aktif olarak rol almadığı bir türdür. Kaynak makina “**zombie**” olarak nitelendirilen makinalar üzerinden hedef makinaryı tarayarak bilgi toplar :

HEDEFİN PORTU AÇIKSA



HEDEFİN PORTU KAPALIYSA





Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır :

nmap -sl -v [Zombie_IP] [Hedef_IP]

FTP Bounce Scan

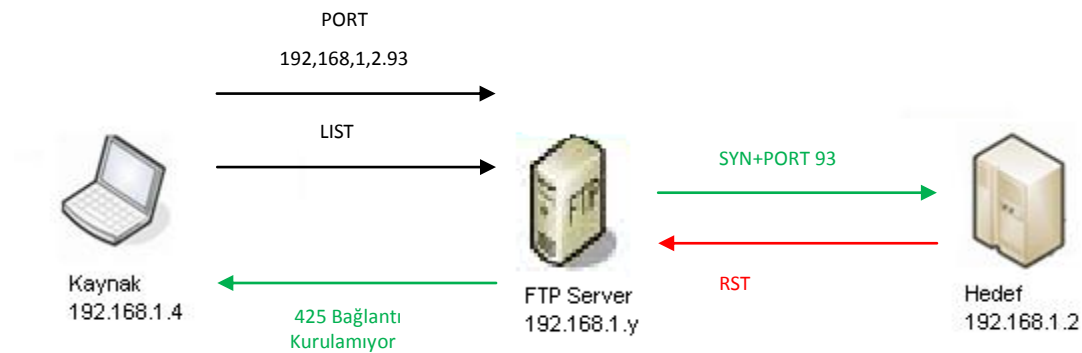
FTP Bounce Scan, FTP Serverlerinin pasif olarak çalışması ile gerçekleştirilir. Pasif moddaki FTPde, komut bağlantıları ile veriler tamamen ayrıdır. FTP Serverlar dışarıya veri bağlantıları kurduğu için FW ile uyumlu çalışması gerekir. Bunun dışında, herhangi bir kullanıcı bir veriyi tamamen farklı bir hedefe gönderebilir.

Nmapin taramayı gerçekleştirebilmesi için, aradaki adam olacak olan FTP Serverla bağlantı kurması gerekir. Bağlantı kurulduktan sonra Nmap verileri taranacak olan hedef IP ve porta yönlendirir.

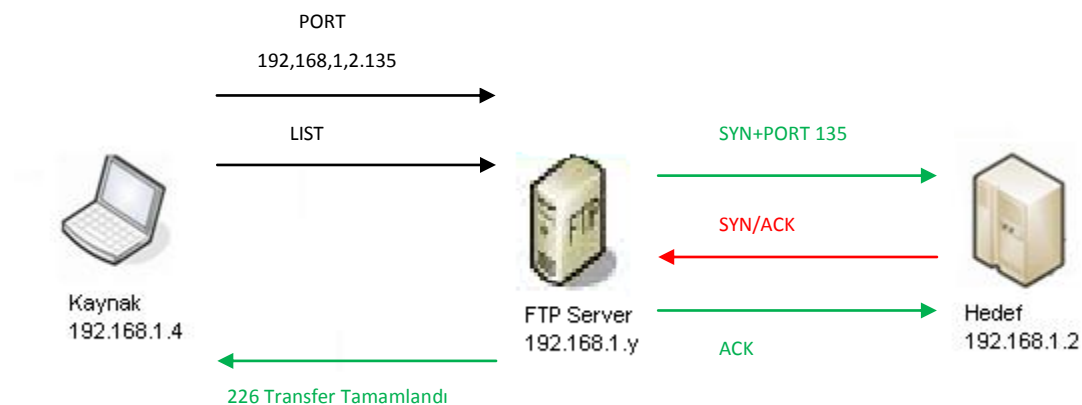
Yönlendirme işleminden sonra FTP üzerinde taramayı gerçekleştirebilmek için öncelikle PORT komutu, daha sonra verileri aktarabilmek için LIST komutu çalıştırılır.

Kapalı portta bağlantı sağlanamazken, açık portta sağlanır :

HEDEF KAPALI DURUMDA



HEDEF AÇIK DURUMDA



Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır :

```
nmap -b -v [user@ftpserver] [Hedef_IP]
```

Nmap Ping Seçenekleri

Nmap taramaya başlamadan önce hedef makinayı mutlaka pingler. Ping işlemi, ICMP Echo isteği ve ardından 80. Porta TCP ACK bayraklı paketin gönderilmesinden oluşur. Eğer hedef makina ping işlemine cevap vermezse, Nmap diğer hedefe geçer. Eğer başka hedef yoksa tarama biter.

Network dünyasında bilinen ping işlemi, ICMP Echo isteği gönderilir ve ICMP Echo cevabı döndürülerek gerçekleşir. Ancak Nmapin ping işlemi biraz daha kendine özgüdür. Nmap dünyasındaki ping hedef makinanın cevap döndürebileceği herhangi bir istek olarak nitelendirilebilir.

ICMP Echo Request ve TCP ACK Ping

Kaynak makina hedef makinaya aynı anda ICMP Echo isteği ve TCP ACK bayraklı paket gönderir ve aşağıdakilerin dönmesi bekler :

- TCP RST
- ICMP Echo Reply

Bu seçeneği çalıştırmak için aşağıdaki komut kullanılmalıdır :

nmap -PB [Hedef_IP]

ICMP Echo Request Ping

Kaynak makina hedef makinaya ICMP Echo isteği gönderir. Eğer herhangi bir cevap dönmezse makina kapalıdır veya “filtered” olarak kabul edilir.

Bu seçeneği çalıştırmak için aşağıdaki komut kullanılmalıdır :

nmap -PE [Hedef_IP]

TCP ACK Ping

Kaynak makinanın hedef makinaya göndereceği TCP ACK bayraklı pakete gelen cevap RST bayraklı paket olursa hedef makina açıktır. Herhangi bir cevap dönmezse makina kapalıdır. TCP ACK ping ile TCP ACK Scan sonuçları birbirine benzer çıkabilir.

Bu seçeneği çalıştırabilmek için aşağıdaki komut kullanılmalıdır :

nmap -PA [Hedef_IP]

TCP SYN Ping

TCP SYN Scan ile benzerlik taşıyan bu seçenekte, kaynak makina hedef makinaya TCP SYN bayraklı paket gönderir. Eğer hedef makina açıksa SYN + ACK bayraklı paket, kapalıysa RST bayraklı paket döndürecek.

Bu seçeneği çalıştırabilmek için aşağıdaki komut kullanılmalıdır :

nmap -PS [Hedef_IP]

UDP Ping

Kaynak makinanın hedef makinaya tek bir UDP paketi göndereceği bu seçenekte, eğer hedef makina açıksa ICMP Port Unreachable mesajı geri dönecektir.

Eğer herhangi bir cevap dönmezse hedef makina erişilebilir değildir denilebilir, ancak çoğu UDP uygulamaları herhangi bir cevap döndürmediğinden, bu sonuç doğru olmayabilir. Bu yüzden kapalı olduğu bilinen bir porta bu işlem uygulanarak test edilmelidir.

Bu seçeneği çalıştırabilmek için aşağıdaki komut kullanılmalıdır :

nmap -PU [Hedef_IP]

ICMP Timestamp Ping

Bu seçenek diğer ICMP bazlı işlemlere benzer. Kaynak makina hedef makinaya ICMP Get Timestamp isteği gönderir. Eğer ICMP Sent Timestamp mesajı dönerse hedef makina açıktır.

Eğer hedef makina kapalıysa ping düşer ve işlem yapılmaz.

Bu seçeneği çalıştırabilmek için aşağıdaki komut kullanılmalıdır :

nmap -PP [Hedef_IP]

ICMP Address Mask Ping

Kaynak makina hedef makinaya ICMP Address Mask isteği gönderir. Eğer hedef makina açıksa ICMP Address Mask cevabı döndürür.

Eğer hedef makina kapalıysa yada ICMP mesajlarına cevap vermiyorsa ping düşer.

Bu seçeneği çalıştırabilmek için aşağıdaki komut kullanılmalıdır :

nmap -PM [Hedef_IP]

Don't Ping Before Scanning

Bu seçenekler Nmap taramalardan önceki “ping” işlemini gerçekleştirmez ve direkt tarama işlemini gerçekleştirir. Yinede reverse DNS sorgusu aktif halde bulunur.

Bu seçeneği çalıştırabilmek için aşağıdaki komut kullanılmalıdır :

nmap -PO [Hedef_IP]

Require Reverse DNS

Reverse DNS işlemi, ping işleminden sonra scan işleminden önce varsayılan olarak Nmap tarafından gerçekleştirilir. Eğer IP-Hostname eşleşmesi gerekli ve önemliyse bu seçenek kullanılabilir. Tarama tipine bakılmaksızın çalışmaktadır.

Bu seçeneği çalıştırabilmek için aşağıdaki komut kullanılmalıdır :

nmap -R [Hedef_IP]

Disable Reverse DNS

Bu seçenekle, Nmap IP-Hostname eşleşmesi sürecini gerçekleştirmez ve direkt olarak tarama işlemine geçer. Bu şekilde daha fazla zaman kazanılır.

Bu seçeneği çalıştırabilmek için aşağıdaki komut kullanılmalıdır :

nmap -n [Hedef_IP]

Ping Scan (Disable Port Scan)

Bu seçenek ile Nmap sadece ping işlemi gerçekleştirir ve hedef makinanın açık olup olmadığını bildirir. Tarama işlemi gerçekleştirilmez.

Bu seçeneği çalıştırmak için aşağıdaki komut kullanılmalıdır :

nmap -sn [Hedef_IP]

Treat all hosts as online

Bu seçenek ile filtered olarak görülen bütün portlar open konumunda ele alınacaktır.

Bu seçeneği çalıştırmak için aşağıdaki komut kullanılmalıdır :

nmap -Pn [Hedef_IP]

OS İzi Belirleme

OS izi belirleme işlemi başlamadan önce, Nmap sırasıyla ping ve scan işlemlerini gerçekleştirir. Nmap tarama esnasında hedef makinanın portlarını open, closed, filtered olarak kategorize eder.

Bu işlem OS izi belirlemede çok önemlidir çünkü sorgular esnasında hem kapalı hemde açık portlar ele alınarak bir sonuç belirlenir.

Açık ve kapalı portlar belirlendikten sonra, OS izi belirleme işlemine geçilir. Bu işlem OS araştırması, TCP el sıkışma serileri ile devam eder. El sıkışma serileri ile TCP uptime, TCP sequence ve IPID tahminleri gerçekleştirilir.

Gönderilen herhangi bayraklı paketlere verilen cevaplar, ttl değerleri ve yukarıda bahsedilen seçenekler sonucunda Nmap OS izi ile ilgili bir tahminde bulunacaktır.

Bu seçeneği çalıştırmak için aşağıdaki komut kullanılmalıdır :

nmap -O [Hedef_IP]

```
#nmap -O 192.168.1.2
at 2010-08-01 20:01 EEST
Nmap scan report for 192.168.1.2
Host is up (0.0020s latency).
```

Not shown: 995 closed ports

PORT STATE SERVICE

22/tcp open ssh

53/tcp open domain

80/tcp open http

111/tcp open rpcbind

2049/tcp open nfs

MAC Address: 00:0C:29:D7:D3:65 (VMware)

Device type: general purpose

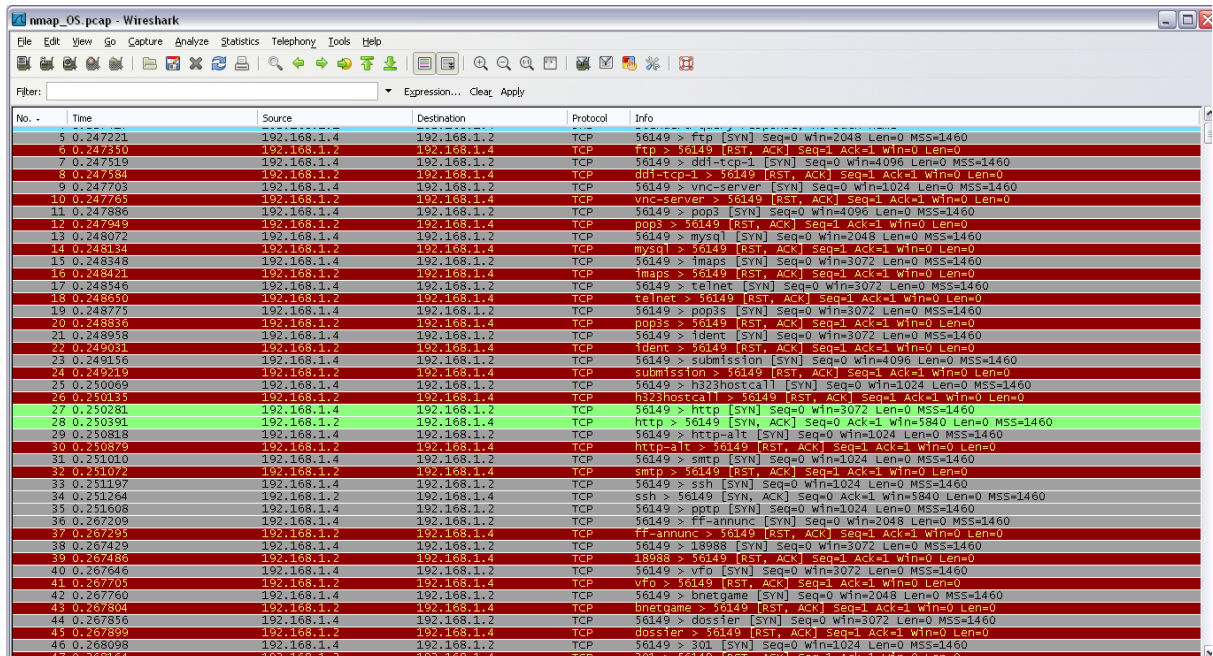
Running: Linux 2.6.X

OS details: Linux 2.6.24 - 2.6.31

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at <http://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds



No.	Time	Source	Destination	Protocol	Info
5	0.247221	192.168.1.4	192.168.1.2	TCP	56149 > ftp [SYN] Seq=0 win=2048 Len=0 MSS=1460
6	0.247430	192.168.1.2	192.168.1.4	TCP	4400 > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
7	0.247519	192.168.1.4	192.168.1.2	TCP	56149 > ddi-tcp-1 [SYN] Seq=0 win=4096 Len=0 MSS=1460
8	0.247584	192.168.1.2	192.168.1.4	TCP	ddi-tcp-1 > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
9	0.247703	192.168.1.4	192.168.1.2	TCP	56149 > vnc-server [SYN] Seq=0 win=1024 Len=0 MSS=1460
10	0.247725	192.168.1.2	192.168.1.4	TCP	vnc-server > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
11	0.247886	192.168.1.4	192.168.1.2	TCP	56149 > pop3 [SYN] Seq=0 win=4096 Len=0 MSS=1460
12	0.247949	192.168.1.2	192.168.1.4	TCP	pop3 > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
13	0.248072	192.168.1.4	192.168.1.2	TCP	56149 > mysql [SYN] Seq=0 win=2048 Len=0 MSS=1460
14	0.248164	192.168.1.2	192.168.1.4	TCP	mysql > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
15	0.248348	192.168.1.4	192.168.1.2	TCP	56149 > imap [SYN] Seq=0 win=3072 Len=0 MSS=1460
16	0.248421	192.168.1.2	192.168.1.4	TCP	imap > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
17	0.248546	192.168.1.4	192.168.1.2	TCP	56149 > telnet [SYN] Seq=0 win=3072 Len=0 MSS=1460
18	0.248550	192.168.1.2	192.168.1.4	TCP	telnet > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
19	0.248775	192.168.1.4	192.168.1.2	TCP	56149 > pop3s [SYN] Seq=0 win=3072 Len=0 MSS=1460
20	0.248836	192.168.1.2	192.168.1.4	TCP	pop3s > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
21	0.248958	192.168.1.4	192.168.1.2	TCP	56149 > ident [SYN] Seq=0 win=3072 Len=0 MSS=1460
22	0.249091	192.168.1.2	192.168.1.4	TCP	ident > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
23	0.249156	192.168.1.4	192.168.1.2	TCP	56149 > submission [SYN] Seq=0 win=1096 Len=0 MSS=1460
24	0.249419	192.168.1.2	192.168.1.4	TCP	submission > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
25	0.250069	192.168.1.4	192.168.1.2	TCP	56149 > h323hostcall [SYN] Seq=0 win=1024 Len=0 MSS=1460
26	0.250135	192.168.1.2	192.168.1.4	TCP	h323hostcall > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
27	0.250281	192.168.1.4	192.168.1.2	TCP	56149 > http [SYN] Seq=0 win=3072 Len=0 MSS=1460
28	0.250391	192.168.1.2	192.168.1.4	TCP	http > 56149 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460
29	0.250818	192.168.1.4	192.168.1.2	TCP	56149 > http-alt [SYN] Seq=0 win=1024 Len=0 MSS=1460
30	0.250879	192.168.1.2	192.168.1.4	TCP	http-alt > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
31	0.251010	192.168.1.4	192.168.1.2	TCP	56149 > smtp [SYN] Seq=0 win=1024 Len=0 MSS=1460
32	0.251072	192.168.1.2	192.168.1.4	TCP	smtp > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
33	0.251197	192.168.1.4	192.168.1.2	TCP	56149 > ssh [SYN] Seq=0 win=1024 Len=0 MSS=1460
34	0.251264	192.168.1.2	192.168.1.4	TCP	ssh > 56149 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS=1460
35	0.251608	192.168.1.4	192.168.1.2	TCP	56149 > pptp [SYN] Seq=0 win=1024 Len=0 MSS=1460
36	0.267209	192.168.1.2	192.168.1.4	TCP	56149 > ff-annunc [SYN] Seq=0 win=2048 Len=0 MSS=1460
37	0.267405	192.168.1.2	192.168.1.4	TCP	ff-annunc > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
38	0.267429	192.168.1.4	192.168.1.2	TCP	56149 > 18988 [SYN] Seq=0 win=3072 Len=0 MSS=1460
39	0.267486	192.168.1.2	192.168.1.4	TCP	18988 > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
40	0.267646	192.168.1.4	192.168.1.2	TCP	56149 > vrf [SYN] Seq=0 win=3072 Len=0 MSS=1460
41	0.267695	192.168.1.2	192.168.1.4	TCP	vrf > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
42	0.267760	192.168.1.4	192.168.1.2	TCP	56149 > bnetgame [SYN] Seq=0 win=2048 Len=0 MSS=1460
43	0.267804	192.168.1.2	192.168.1.4	TCP	bnetgame > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
44	0.267856	192.168.1.4	192.168.1.2	TCP	56149 > dossier [SYN] Seq=0 win=3072 Len=0 MSS=1460
45	0.267899	192.168.1.2	192.168.1.4	TCP	dossier > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0
46	0.268098	192.168.1.4	192.168.1.2	TCP	56149 > 301 [SYN] Seq=0 win=1024 Len=0 MSS=1460
47	0.268164	192.168.1.2	192.168.1.4	TCP	301 > 56149 [RST, ACK] Seq=1 Ack=1 win=0 Len=0

Os İzi Belirleme Seçenekleri

- --osscan-limit : En az bir açık ve bir kapalı portu bulunan hedeflerin OS izini belirlemeye çalışır.
- --osscan-guess : Daha agresif bir şekilde belirleme yapar.
- --max-retries <sayı> : Belirtilen <sayı> miktarında OS izi belirleme denemesi yapar.

Nmap Script Motoru (Nmap Scripting Engine – NSE)

NSE, varolan Nmap yeteneklerini geliştirmek ve Nmap dahilindeki formatlarla çıktı alabilmek için kullanılan bir yapıdır. NSE scriptlerinin içerdiği bazı örnekler aşağıdaki gibidir :

- Geliştirilmiş Ağ Keşfi : Whois lookup istekleri ve ek protokol sorguları gerçekleştirir. Ayrıca erişilebilir network paylaşımları gibi dinlenen servislerden bilgi toplamak amacıyla istemci gibi davranır.
- Geliştirilmiş Versiyon Keşfi : Karmaşık versiyon araştırmaları yapar ve servislere brute force saldırısı düzenler.
- Zafiyet Keşfi : Özel zafiyetlerin kontrolü amacıyla araştırma yapar.
- Zararlı Yazılım Keşfi : Virus, worm ve trojan gibi zararlı yazılımların bulunması amacıyla araştırmalar yapar.
- Zafiyeti Kullanmak : Bulunan zafiyetleri kullanmak amacıyla scriptleri çalıştırır.

Varsayılan olarak, Version Scanning (-sV) versiyon kategorisinde bulunan bütün NSE scriptlerini çalıştırır. -A özelliği ise, -sC (güvenli veizinsiz giriş kategorileri) seçeneğini çalıştırır.

NSE scriptleri Lua script dilinde yazılır ve .nse uzantısına sahiptir ve Nmap ana dizinin altında **“scripts”** dizininde saklanırlar. Bununla birlikte **“script.db”** Nmap ana dizinin altında bulunur ve bütün scriptleri kategorileriyle (Güvenli, Zorla Giriş, Zararlı Yazılım,Arka Kapı, Versiyon, Keşif, Zafiyet) saklar. NSE, scripti çalıştırmadan önce hedefteki makinanın, Nmap çıktılarına dayanarak, gerekli kriterleri karşılayıp karşılamadığını araştırır. Bu araştırmadan sonra scriptin çalışmasına karar verir.

NSE kullanmanın en çabuk yolu aşağıdaki gibidir :

nmap -sC 192.168.1.0/24

Yukarıdaki seçenek vasıtasıyla NSE bütün Güvenli ve Zorla Giriş scriptlerinin çalıştıracaktır. Eğer daha özel bir scriptin çalıştırılması istenirse - - script seçeneği kullanılarak istenilen bir kategoriye ait scriptler çalıştırılabilir :

nmap --script=vulnerability 192.168.1.34

Sadece tek bir script çalıştırılmak istenirse aşağıdaki seçenek kullanılmalıdır :

nmap --script=promiscuous.nse 192.168.1.0/24

Belirli bir dizinin altındaki scriptleri çalıştırmak istenirse aşağıdaki seçenek kullanılmalıdır :

nmap --script=/my-scripts 192.168.1.0/24

Bütün scriptlerin çalışması istenirse aşağıdaki seçenek kullanılmalıdır :

nmap --script=all 192.168.1.55

NSE Seçenekleri

- **--script-args=<n1=v1[,n2=v2,...]>** : Varolan script değerlerinin yerine belirlenen yeni değerler atanır.
- **--script-trace** : Scripte ait bütün iç ve dış iletişimin çıktısını gösterir.
- **--script-updatedb** : Scriptlerin bulunduğu veritabanını günceller.

Güvenlik Ürünleri ve Nmap

Nmap, taranılacak olan hedeflerin önünde bulunan güvenlik ürünlerinin kısıtlaması nedeniyle, istenilen şekilde tam olarak çalışamayabilir. Günümüzdeki güvenlik ürünleri Nmap ve taramalarını rahatlıkla yakalayabiliyor. Ancak Nmap kendi bünyesinde bulunan bazı seçenekler vasıtasıyla bu güvenlik ürünlerini atlatabilir. Fragmentasyon, spoofing ve packet manipulating seçenekleri vasıtasıyla Nmap güvenlik ürünlerini atlatıp, taramalarını daha rahat bir şekilde gerçekleştirebilir.

Fragmentation

Nmap ile fragmentasyon yapılmak istenirse, **-f**, **-f -f** veya **-mtu** seçenekleri kullanılmalıdır. Eğer parçalanmak istenilen paketin maksimum boyutu, IP başlık bilgisinden sonra, 8 byte olması isteniyorsa aşağıdaki komut kullanılmalıdır :

nmap -f [Hedef_IP]

Eğer parçalanmak istenilen paketin maksimum boyutu, IP başlık bilgisinden sonra, 16 byte olması isteniyorsa aşağıdaki komut kullanılmalıdır :

nmap -f -f [Hedef_IP]

Eğer parçalanmak istenilen paketin maksimum boyutu, IP başlık bilgisinden sonra, el ile girilerek belirlenmek isteniyorsa aşağıdaki komut kullanılmalıdır :

nmap - - mtu <Sayı> [Hedef_IP]

Spoofing

Fragmantasyon seçeneğinin güvenlik ürünleri tarafından yüksek oranla yakalanması yüzünden diğer bir atlatma türü olan spoofing tercih edilebilir. Nmap Decoy Scan (-D), tercih edilen Nmap taramasının bir makinadan değil, belirtilecek olan makinalardan da yapılıyormuş gibi göstererek yakalanma riskini düşürür. Belirtilecek olan makinaların IP leri taramanın yapılacağı ortamla uyumlu olması çok önemlidir. Private IP kullanılan LAN ortamın Reel IP ile tarama yapılması pek akıllıca olmayacaktır. Eğer IP ler belirtilmezse Nmap rastgele olarak IP ler seçecektir. Ancak bu IP lerin Reel IP olma olasılığı var ve yukarıda bahsedilen durumun aynısı oluşabilir. Spoofing işleminin yapılması için kullanılması gereken komut aşağıdaki gibidir :

nmap -D < [Spooflanan_IP] > [Hedef_IP]

Eğer geleneksel spoof yöntemi kullanılmak istenirse aşağıdaki komut kullanılmalıdır. Ancak geleneksel yöntemle gönderilen paketlerin cevapları taramanın yapıldığı makineye geri dönmeyecektir. Aynı zamanda bu yöntemi Nmapin ethernet kart arayüzünün IP adresini bulamadığı durumlarda -e parametresi ile beraber kullanarak IP adresi atanabilir. Buradaki -e parametresi interface ismini belirtir.

nmap -S <[Spooflanan_IP]> [Hedef_IP]

nmap -S <[Spooflanan_IP]> -e [interface] [Hedef_IP]

Diğer bir spoofing yöntemi ise MAC adresleri. Nmap paketlerinin içerisinde farklı MAC adresleri bulunması sağlanabilir. Bütün bir MAC adresi girilebileceği gibi bir vendor ismi veya vendor prefixi de girilebilir. Eğer () şeklinde yazılırsa Nmap MAC adresini kendisi belirler. MAC spoofing için aşağıdaki komutlar kullanılmalıdır :

nmap --spoof-mac 11:22:33:44:55:66 192.168.1.0/24

nmap --spoof-mac 000D93 192.168.1.0/24

nmap --spoof-mac D-Link 192.168.1.0/24

Son olarak kaynak port için spoofing kullanılabilir. Bu işlem için aşağıdaki komut kullanılmalıdır :

nmap -g 53 192.168.1.0/24

nmap --source-port 53 192.168.1.0/24

Packet Manipulating

Güvenlik ürünlerini atlatmak için, Nmap çok fazla sayıda packet manipulating özelliği barındırır. Aşağıda bu özellikler ve açıklamaları bulunmaktadır :

- --data-length <sayı> : Paket boyutunun olacağı uzunluğu <sayı> belirtir.
- --ip-options <R|T|U|S [IP IP2...] | L [IP IP2 ...] > yada --ip-options <hex string> : Paketler içerisindeki IP özelliklerini belirtir.
- --ttl <değer> :
- --randomize-hosts : Listede belirtilen taranılacak hostları rastgele bir şekilde seçer.
- --badsum : Yanlış checksuma sahip TCP veya UDP paketleri gönderir.