

Table of Contents

Nmap Scans.....	1
Null.....	1
Xmas.....	3
ACK.....	4
Version Scan.....	5
Extra Scan.....	7

Nmap Scans

Null

Nmap -sN -p80 192.168.56.102

Flags set = None

Protocol = TCP

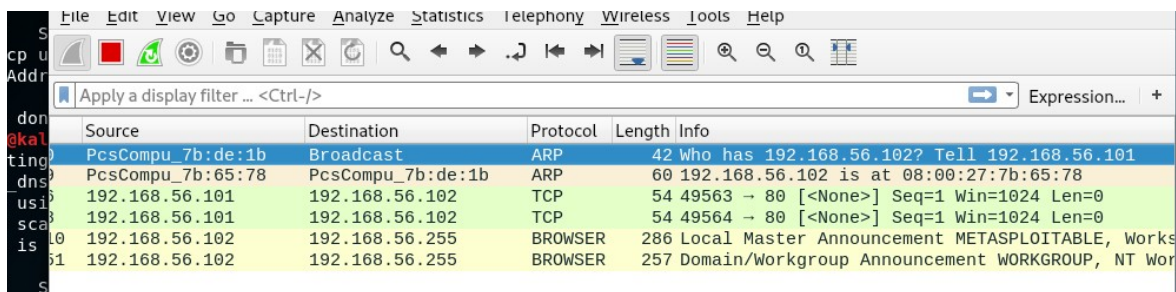
Source IP = 192.168.56.101

Dest IP = 192.168.56.102

Port 80

```
root@kali:~# nmap -sN -p80 192.168.56.102
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-26 01:28 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00030s latency).
PORT      STATE SERVICE
80/tcp    open|filtered http
MAC Address: 08:00:27:7B:65:78 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

The header does not have any flags set, the response of the scan was open|filtered



The image shows a Wireshark packet capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A display filter bar shows 'Apply a display filter ... <Ctrl-/>'. The packet list pane on the left shows several packets, with the first three selected. The packet details pane on the right shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol.

No.	Source	Destination	Protocol	Length	Info
1	PcsCompu_7b:de:1b	Broadcast	ARP	42	Who has 192.168.56.102? Tell 192.168.56.101
2	PcsCompu_7b:65:78	PcsCompu_7b:de:1b	ARP	60	192.168.56.102 is at 08:00:27:7b:65:78
3	192.168.56.101	192.168.56.102	TCP	54	49563 → 80 [<None>] Seq=1 Win=1024 Len=0
4	192.168.56.101	192.168.56.102	TCP	54	49564 → 80 [<None>] Seq=1 Win=1024 Len=0
5	192.168.56.102	192.168.56.255	BROWSER	286	Local Master Announcement METASPLOITABLE, Works
6	192.168.56.102	192.168.56.255	BROWSER	257	Domain/Workgroup Announcement WORKGROUP, NT Wor

Xmas

Nmap -sX -p80 192.168.56.102

Flags set FIN PSH URG

Protocol = TCP

Source IP = 192.168.56.101

Dest IP = 192.168.56.102

Port 80

```
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
root@kali:~# nmap -sX -p80 192.168.56.102
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-26 01:26 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00042s latency).
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:7B:65:78 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```

Got no response back so that means the port is open.

sing --system-dns or specify valid servers with --dns-servers

*eth0

Source	Destination	Protocol	Length	Info
PcsCompu_7b:de:1b	Broadcast	ARP	42	Who has 192.168.56.102? Tell 192.168.56.101
PcsCompu_7b:65:78	PcsCompu_7b:de:1b	ARP	60	192.168.56.102 is at 08:00:27:7b:65:78
192.168.56.101	192.168.56.102	TCP	54	63801 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0
192.168.56.101	192.168.56.102	TCP	54	63802 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0

ACK

Nmap -sA -p80 192.168.56.102

Flag set ACK

Protocol = TCP

Source IP = 192.168.56.101

Dest IP = 192.168.56.102

Port 80

```
root@kali:~# nmap -sA -p80 192.168.56.102
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-26 01:40 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00035s latency).
Total Length: 40
PORT      STATE SERVICE
80/tcp    unfiltered http
MAC Address: 08:00:27:7B:65:78 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

Got back a reset which means the port is not filtered by a firewall

Source	Destination	Protocol	Length	Info
fe80::94c1:59bf:618...	ff02::c	UDP	718	55543 → 3702 Len=656
fe80::94c1:59bf:618...	ff02::c	UDP	718	55543 → 3702 Len=656
192.168.56.1	239.255.255.250	UDP	698	55542 → 3702 Len=656
192.168.56.1	239.255.255.250	UDP	698	55542 → 3702 Len=656
fe80::94c1:59bf:618...	ff02::c	UDP	718	55543 → 3702 Len=656
fe80::94c1:59bf:618...	ff02::c	UDP	718	55543 → 3702 Len=656
192.168.56.1	239.255.255.250	UDP	698	55542 → 3702 Len=656
PcsCompu_7b:de:1b	Broadcast	ARP	42	Who has 192.168.56.102? Tell 192.168.56.101
PcsCompu_7b:65:78	PcsCompu_7b:de:1b	ARP	60	192.168.56.102 is at 08:00:27:7b:65:78
192.168.56.101	192.168.56.102	TCP	54	39383 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=6
192.168.56.102	192.168.56.101	TCP	60	80 → 39383 [RST] Seq=1 Win=0 Len=0

Frame 1: 698 bytes on wire (5584 bits), 698 bytes captured (5584 bits) on interface 0

Ethernet II, Src: 0a:00:27:00:00:0c (0a:00:27:00:00:0c), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)

Internet Protocol Version 4, Src: 192.168.56.1, Dst: 239.255.255.250

User Datagram Protocol, Src Port: 55542, Dst Port: 3702

Data (656 bytes)

Version Scan

`nmap -sV --version-intensity 2 192.168.56.102`

Flags set FIN ACK

Protocol = TCP

Source IP = 192.168.56.101

Dest IP = 192.168.56.102

Ports Open = 21 22 23 25 53 80 111 139 445 512 513 514 1099 1524 2049 2121 3306 5432 5900 6000 6667 8009 8180

```
root@kali: /usr/share/theharvester/discovery
File Edit View Search Terminal Help
p://hackers.org/weird/rfi-locations.dat) or from http://osvdb.org/
^Croot@kali:/usr/share/theharvester/discovery# ^C
root@kali:/usr/share/theharvester/discovery# nmap -sV --version-intensity 2 192.168.56.102
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-31 02:20 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00018s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rshd
513/tcp   open  login?       Netkit rshd
514/tcp   open  shell        Netkit rshd
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  rpcbind      ProFTPD 1.3.1
2121/tcp  open  ftp          MySQL 5.0.51a-3ubuntu5
3306/tcp  open  mysql        PostgreSQL DB 8.3.0 - 8.3.7
5432/tcp  open  postgresql   VNC (protocol 3.3)
5900/tcp  open  vnc          (access denied)
6000/tcp  open  X11          UnrealIRCd
6667/tcp  open  irc          Apache Jserv (Protocol v1.3)
8009/tcp  open  ajp13        Apache Tomcat/Coyote JSP engine 1.1
8180/tcp  open  http         MAC Address: 08:00:27:7B:65:78 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
root@kali:/usr/share/theharvester/discovery#
```


Places Wireshark Thu 02:35

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
2320	11.609999311	192.168.56.102	192.168.56.101	TCP	66	8009 → 41726 [ACK] Seq=1 Ack=6
2321	11.611488686	192.168.56.102	192.168.56.101	AJP13	71	1033:RSP:CPONG
2322	11.611514934	192.168.56.101	192.168.56.102	TCP	66	41726 → 8009 [ACK] Seq=6 Ack=6
2323	11.611812379	192.168.56.101	192.168.56.102	TCP	66	41726 → 8009 [FIN, ACK] Seq=6 A
2324	11.612563308	192.168.56.102	192.168.56.101	TCP	66	8009 → 41726 [FIN, ACK] Seq=6 A
2325	11.612605960	192.168.56.101	192.168.56.102	TCP	66	41726 → 8009 [ACK] Seq=7 Ack=7

Frame 2323: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Ethernet II, Src: PcsCompu_7b:de:1b (08:00:27:7b:de:1b), Dst: PcsCompu_7b:65:78 (08:00:27:7b:65:78)

Internet Protocol Version 4, Src: 192.168.56.101, Dst: 192.168.56.102

Transmission Control Protocol, Src Port: 41726, Dst Port: 8009, Seq: 6, Ack: 6, Len: 0

Source Port: 41726

Destination Port: 8009

[Stream index: 1033]

[TCP Segment Len: 0]

Sequence number: 6 (relative sequence number)

[Next sequence number: 6 (relative sequence number)]

Acknowledgment number: 6 (relative ack number)

1000 = Header Length: 32 bytes (8)

Flags: 0x011 (FIN, ACK)

Window size value: 229

0010 00 34 d4 07 40 00 40 06 74 a0 c0 a8 38 65 c0 a8 4 .@.t...8e .

0020 38 66 a2 fe 1f 49 44 d5 64 86 bf 08 18 1b 80 11 8f...ID. d.....

Extra Scan

SYN

Nmap -sS -p80 192.168.56.102

```
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
root@kali:~# nmap -sS -p80 192.168.56.102
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-26 01:44 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.00042s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:7B:65:78 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
root@kali:~#
```

Apply a display filter ... <Ctrl-/> ➡ Expression... +

Time	Source	Destination	Protocol	Length	Info
0.639568506	PcsCompu_7b:de:1b	Broadcast	ARP	42	Who has 192.168.56.102? Tell 192.168.56.1
0.639972043	PcsCompu_7b:65:78	PcsCompu_7b:de:1b	ARP	60	192.168.56.102 is at 08:00:27:7b:65:78
0.731642414	192.168.56.101	192.168.56.102	TCP	58	56583 → 80 [SYN] Seq=0 Win=1024
0.732383821	192.168.56.102	192.168.56.101	TCP	60	80 → 56583 [SYN, ACK] Seq=0 Ack=56583
0.732457755	192.168.56.101	192.168.56.102	TCP	54	56583 → 80 [RST] Seq=1 Win=0 Len=0
0.983189293	192.168.56.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1

▶ Frame 1: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface 0
▶ Ethernet II, Src: 0a:00:27:00:00:0c (0a:00:27:00:00:0c), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
▶ Internet Protocol Version 4, Src: 192.168.56.1, Dst: 239.255.255.250
▶ User Datagram Protocol, Src Port: 59519, Dst Port: 1900
▶ Simple Service Discovery Protocol

0000	01 00 5e 7f ff fa 0a 00 27 00 00 0c 08 00 45 00	..A.....E.
0010	00 c9 20 90 00 00 01 11 af f0 c0 a8 38 01 ef ff	8...
0020	ff fa e8 7f 07 6c 00 b5 e4 a5 4d 2d 53 45 41 52	l...M-SEAR
0030	43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48	CH * HTTP/1.1..H
0040	4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35	OST: 239.255.255
0050	2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20	.250:1900..MAN:
0060	22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d	"ssdp:discover".
0070	0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a	.MX: 1..ST: urn:

wireshark_eth0_20190124190136_Jybmej.pcapng Packets: 9 · Displayed: 9 (100.0%) Profile: Default