**EXPERIMENT 9: nmap**

**PORT SCANNING**

**c502@comp:~$ nmap -sP scanme.nmap.org google.com yahoo.in amazon.in**

Starting Nmap 7.01 ( https://nmap.org ) at 2019-04-05 11:31 IST

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.00037s latency).

Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

Nmap scan report for google.com (172.217.26.174)

Host is up (0.00056s latency).

Other addresses for google.com (not scanned): 2404:6800:4009:80d::200e

rDNS record for 172.217.26.174: maa03s22-in-f174.1e100.net

Nmap scan report for yahoo.in (124.108.115.101)

Host is up (0.00045s latency).

Other addresses for yahoo.in (not scanned): 74.6.136.151 106.10.248.151 98.136.103.24 212.82.100.151

rDNS record for 124.108.115.101: w2.src1.vip.tw1.yahoo.com

Nmap scan report for amazon.in (52.95.120.67)

Host is up (0.00044s latency).

Other addresses for amazon.in (not scanned): 52.95.116.115 54.239.33.92

Nmap done: 4 IP addresses (4 hosts up) scanned in 18.53 seconds

**OS FINGERPRINTING**

**c502@comp:~$ nmap -v -O scanme.nmap.org**

TCP/IP fingerprinting (for OS scan) requires root privileges.

QUITTING!

**c502@comp:~$ sudo nmap -v -O scanme.nmap.org**

[sudo] password for c502:

Starting Nmap 7.01 ( https://nmap.org ) at 2019-04-05 11:32 IST

Initiating Ping Scan at 11:32

Scanning scanme.nmap.org (45.33.32.156) [4 ports]

Completed Ping Scan at 11:32, 0.21s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 11:32

Completed Parallel DNS resolution of 1 host. at 11:32, 0.00s elapsed

Initiating SYN Stealth Scan at 11:32

Scanning scanme.nmap.org (45.33.32.156) [1000 ports]

Discovered open port 443/tcp on 45.33.32.156

Discovered open port 80/tcp on 45.33.32.156

Discovered open port 22/tcp on 45.33.32.156

Increasing send delay for 45.33.32.156 from 0 to 5 due to 19 out of 63 dropped probes since last increase.

Increasing send delay for 45.33.32.156 from 5 to 10 due to 11 out of 18 dropped probes since last increase.

Increasing send delay for 45.33.32.156 from 10 to 20 due to max\_successful\_tryno increase to 4

SYN Stealth Scan Timing: About 25.87% done; ETC: 11:34 (0:01:29 remaining)

Increasing send delay for 45.33.32.156 from 20 to 40 due to 11 out of 21 dropped probes since last increase.

SYN Stealth Scan Timing: About 31.13% done; ETC: 11:36 (0:02:15 remaining)

Increasing send delay for 45.33.32.156 from 40 to 80 due to 11 out of 23 dropped probes since last increase.

Increasing send delay for 45.33.32.156 from 80 to 160 due to 11 out of 28 dropped probes since last increase.

SYN Stealth Scan Timing: About 36.18% done; ETC: 11:36 (0:02:40 remaining)

Increasing send delay for 45.33.32.156 from 160 to 320 due to 11 out of 26 dropped probes since last increase.

SYN Stealth Scan Timing: About 38.62% done; ETC: 11:38 (0:03:12 remaining)

SYN Stealth Scan Timing: About 40.05% done; ETC: 11:39 (0:03:46 remaining)

Increasing send delay for 45.33.32.156 from 320 to 640 due to 11 out of 29 dropped probes since last increase.

SYN Stealth Scan Timing: About 41.13% done; ETC: 11:40 (0:04:19 remaining)

SYN Stealth Scan Timing: About 42.10% done; ETC: 11:41 (0:04:50 remaining)

SYN Stealth Scan Timing: About 42.90% done; ETC: 11:42 (0:05:21 remaining)

SYN Stealth Scan Timing: About 43.83% done; ETC: 11:43 (0:05:51 remaining)

SYN Stealth Scan Timing: About 44.77% done; ETC: 11:44 (0:06:22 remaining)

SYN Stealth Scan Timing: About 46.07% done; ETC: 11:45 (0:06:59 remaining)

SYN Stealth Scan Timing: About 47.67% done; ETC: 11:47 (0:07:39 remaining)

SYN Stealth Scan Timing: About 49.60% done; ETC: 11:49 (0:08:24 remaining)

SYN Stealth Scan Timing: About 53.22% done; ETC: 11:52 (0:09:15 remaining)

SYN Stealth Scan Timing: About 67.50% done; ETC: 12:02 (0:09:32 remaining)

SYN Stealth Scan Timing: About 76.13% done; ETC: 12:06 (0:08:03 remaining)

SYN Stealth Scan Timing: About 82.32% done; ETC: 12:08 (0:06:22 remaining)

SYN Stealth Scan Timing: About 87.93% done; ETC: 12:10 (0:04:33 remaining)

SYN Stealth Scan Timing: About 93.23% done; ETC: 12:12 (0:02:39 remaining)

SYN Stealth Scan Timing: About 97.42% done; ETC: 12:13 (0:01:02 remaining)

Completed SYN Stealth Scan at 12:14, 2481.64s elapsed (1000 total ports)

Initiating OS detection (try #1) against scanme.nmap.org (45.33.32.156)

adjust\_timeouts2: packet supposedly had rtt of -80733 microseconds. Ignoring time.

adjust\_timeouts2: packet supposedly had rtt of -80733 microseconds. Ignoring time.

adjust\_timeouts2: packet supposedly had rtt of -54664 microseconds. Ignoring time.

adjust\_timeouts2: packet supposedly had rtt of -54664 microseconds. Ignoring time.

Retrying OS detection (try #2) against scanme.nmap.org (45.33.32.156)

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.24s latency).

Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

Not shown: 882 filtered ports, 115 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

443/tcp open https

Device type: specialized|general purpose|router|WAP|storage-misc|VoIP adapter

Running (JUST GUESSING): AVtech embedded (94%), FreeBSD 6.X (91%), Linux 2.6.X|3.X|4.X (91%), Linksys embedded (90%), OpenBSD 4.X (90%), Apple embedded (88%), Netgear RAIDiator 4.X (88%), Cisco embedded (85%)

OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:linux:linux\_kernel:2.6 cpe:/o:openbsd:openbsd:4.0 cpe:/o:linux:linux\_kernel:3 cpe:/o:linux:linux\_kernel:4 cpe:/h:apple:airport\_extreme cpe:/o:netgear:raidiator:4.1.4 cpe:/h:cisco:unified\_call\_manager

Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (94%), FreeBSD 6.2-RELEASE (91%), Linux 2.6.18 - 2.6.22 (91%), Linksys BEFSR41 EtherFast router (90%), OpenBSD 4.0 (90%), Linux 2.6.18 (90%), OpenBSD 4.3 (90%), Linux 3.11 - 4.1 (89%), Apple AirPort Extreme WAP (88%), FreeBSD 6.3-RELEASE (88%)

No exact OS matches for host (test conditions non-ideal).

Read data files from: /usr/bin/../share/nmap

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 2493.65 seconds

Raw packets sent: 5976 (268.072KB) | Rcvd: 1038 (46.784KB)

c502@comp:~$

**TCP SCAN**

**c502@comp:~$ nmap -sT scanme.nmap.org**

Starting Nmap 7.01 ( https://nmap.org ) at 2019-04-05 11:49 IST

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.23s latency).

Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

Not shown: 882 filtered ports, 115 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 36.80 seconds

**UDP SCAN**

**c502@comp:~$ nmap -sU scanme.nmap.org**

You requested a scan type which requires root privileges.

QUITTING!

**c502@comp:~$ sudo nmap -sU scanme.nmap.org**

[sudo] password for c502:

Starting Nmap 7.01 ( https://nmap.org ) at 2019-04-05 11:50 IST

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.076s latency).

Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

Not shown: 987 open|filtered ports

PORT STATE SERVICE

53/udp closed domain

88/udp closed kerberos-sec

500/udp closed isakmp

2048/udp closed dls-monitor

2049/udp closed nfs

2160/udp closed apc-2160

2161/udp closed apc-2161

2222/udp closed msantipiracy

2343/udp closed nati-logos

2345/udp closed dbm

2362/udp closed digiman

4500/udp closed nat-t-ike

33459/udp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 36.03 seconds

**SCREENSHOTS**



