# **LAB #2 NMAP- NETWORK SCANNING**

#### **STEP #1** **SCANNING A SINGLE HOST USING -sS HALF OPEN TCP SCAN**

**Target: Seclists.org or 50.116.1.184**

## **Command:** Sudo nmap -sS seclists.org

## $ sudo nmap -sS seclists.org

## Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-01 00:56 EDT

## Nmap scan report for seclists.org (50.116.1.184)

## Host is up (0.072s latency).

## Other addresses for seclists.org (not scanned): 2600:3c01:e000:3e6::6d4e:7061

## rDNS record for 50.116.1.184: ack.nmap.org

## Not shown: 994 filtered tcp ports (no-response)

## PORT STATE SERVICE

## 22/tcp open ssh

## 70/tcp closed gopher

## 80/tcp open http

## 113/tcp closed ident

## 443/tcp open https

## 31337/tcp closed Elite

## **Command:** Sudo nmap –sS 50.116.1.184

## ─$ sudo nmap -sS 50.116.1.184

## Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-01 01:01 EDT

## Nmap scan report for ack.nmap.org (50.116.1.184)

## Host is up (0.072s latency).

## Not shown: 994 filtered tcp ports (no-response)

## PORT STATE SERVICE

## 22/tcp open ssh

## 70/tcp closed gopher

## 80/tcp open http

## 113/tcp closed ident

## 443/tcp open https

## 31337/tcp closed Elite

**Results:**

* The scan was performed using the SYN scan method (-sS), which is a stealth scanning technique that does not complete the TCP handshake.
* The scan identified that ports 22 (SSH), 80 (HTTP), and 443 (HTTPS) are open, which indicates that the target host is running services associated with these ports.
* Ports 70 (Gopher), 113 (Ident), and 31337 (Elite) are closed, suggesting that these services are not active or are explicitly turned off.
* A large number of TCP ports (994) were filtered, meaning that Nmap did not receive a response for these ports, possibly due to a firewall or network security device blocking access

#### **STEP #2: SCANNING A SINGLE HOST USING -sT FULL OPEN SCAN**

**Target: Seclists.org or 50.116.1.184**

## **Command:** Sudo nmap -sT seclists.org

## ─$ sudo nmap -sT seclists.org

## Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-01 01:32 EDT

## Nmap scan report for seclists.org (50.116.1.184)

## Host is up (0.073s latency).

## Other addresses for seclists.org (not scanned): 2600:3c01:e000:3e6::6d4e:7061

## rDNS record for 50.116.1.184: ack.nmap.org

## Not shown: 994 filtered tcp ports (no-response)

## PORT STATE SERVICE

## 22/tcp open ssh

## 70/tcp closed gopher

## 80/tcp open http

## 113/tcp closed ident

## 443/tcp open https

## 31337/tcp closed Elite

## **Command:** Sudo nmap -sT 50.116.1.184

## ─$ sudo nmap -sT 50.116.1.184

## Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-01 01:35 EDT

## Nmap scan report for ack.nmap.org (50.116.1.184)

## Host is up (0.070s latency).

## Not shown: 994 filtered tcp ports (no-response)

## PORT STATE SERVICE

## 22/tcp open ssh

## 70/tcp closed gopher

## 80/tcp open http

## 113/tcp closed ident

## 443/tcp open https

## 31337/tcp closed Elite

**Results:**

* The scan was performed using the TCP connect scan method (-sT), which completes the TCP handshake to determine port status.
* The scan identified that ports 22 (SSH), 80 (HTTP), and 443 (HTTPS) are open, indicating that these services are actively listening on the target host.
* Ports 70 (Gopher), 113 (Ident), and 31337 (Elite) are closed, suggesting these services are not active or have been disabled.
* A significant number of TCP ports (994) were filtered, meaning that Nmap did not receive a response from these ports, potentially due to firewall rules or network security devices.

## **STEP #3: SCANNING MULTIPLE HOSTS USING A FULL TCP SCAN**

## **Command:** Sudo nmap -sT seclists.org hackertarget.com

## sudo nmap -sT seclists.org hackertarget.com

## Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-01 01:47 EDT

## Nmap scan report for seclists.org (50.116.1.184)

## Host is up (0.072s latency).

## Other addresses for seclists.org (not scanned): 2600:3c01:e000:3e6::6d4e:7061

## rDNS record for 50.116.1.184: ack.nmap.org

## Not shown: 994 filtered tcp ports (no-response)

## PORT STATE SERVICE

## 22/tcp open ssh

## 70/tcp closed gopher

## 80/tcp open http

## 113/tcp closed ident

## 443/tcp open https

## 31337/tcp closed Elite

## Nmap scan report for hackertarget.com (172.67.72.147)

## Host is up (0.015s latency).

## Other addresses for hackertarget.com (not scanned): 104.26.9.237 104.26.8.237 2606:4700:20::681a:8ed 2606:4700:20::ac43:4893 2606:4700:20::681a:9ed

## Not shown: 996 filtered tcp ports (no-response)

## PORT STATE SERVICE

## 80/tcp open http

## 443/tcp open https

## 8080/tcp open http-proxy

## 8443/tcp open https-alt

## **Command:** Sudo nmap -sT 50.116.1.184 104.26.9.237

## ─$ sudo nmap -sT 50.116.1.184 104.26.9.237

## Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-01 01:47 EDT

## Nmap scan report for ack.nmap.org (50.116.1.184)

## Host is up (0.072s latency).

## Not shown: 994 filtered tcp ports (no-response)

## PORT STATE SERVICE

## 22/tcp open ssh

## 70/tcp closed gopher

## 80/tcp open http

## 113/tcp closed ident

## 443/tcp open https

## 31337/tcp closed Elite

## Nmap scan report for 104.26.9.237

## Host is up (0.015s latency).

## Not shown: 996 filtered tcp ports (no-response)

## PORT STATE SERVICE

## 80/tcp open http

## 443/tcp open https

## 8080/tcp open http-proxy

## 8443/tcp open https-alt

**Results:**

* The scans were performed using the TCP connect scan method (-sT), which involves completing the TCP handshake to determine port status.
* seclists.org: Identified as having open ports for SSH (22), HTTP (80), and HTTPS (443). Ports for Gopher (70), Ident (113), and Elite (31337) are closed. A significant number of ports (994) are filtered.
* hackertarget.com: Identified as having open ports for HTTP (80), HTTPS (443), HTTP-Proxy (8080), and HTTPS-Alt (8443). A large number of ports (996) are filtered

#### **STEP #4: SCAN A RANGE OF ADDRESSES USING NMAP**

**Command:** Sudo nmap –sT 104.26.9.237-255

sudo nmap -sT 104.26.9.237-255

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-02 17:53 EDT

Nmap scan report for 104.26.9.237

Host is up (0.016s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.238

Host is up (0.017s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.239

Host is up (0.015s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.240

Host is up (0.017s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.241

Host is up (0.015s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.242

Host is up (0.017s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.243

Host is up (0.017s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.244

Host is up (0.016s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.245

Host is up (0.015s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.246

Host is up (0.018s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.247

Host is up (0.016s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.248

Host is up (0.017s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.249

Host is up (0.016s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.250

Host is up (0.014s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.251

Host is up (0.015s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.252

Host is up (0.016s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.253

Host is up (0.015s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.254

Host is up (0.015s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Nmap scan report for 104.26.9.255

Host is up (0.015s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

8080/tcp open http-proxy

8443/tcp open https-alt

Results:

* The Nmap scan of the IP range 104.26.9.237 to 104.26.9.255 reveals that all 19 hosts are active, with low latency indicating efficient network performance.
* Each host has ports 80 (HTTP), 443 (HTTPS), 8080 (HTTP-Proxy), and 8443 (HTTPS-Alt) open, suggesting a standardized configuration for web and secure services, potentially indicative of a managed web infrastructure.
* The presence of 996 filtered ports on each host points to robust network security measures, such as firewalls or intrusion prevention systems, which protects these ports from unauthorized access. Top of Form

#### **STEP #5: SCAN A TARGET USING NMAP AGGRESSIVE SCAN –A**

**Command:** Sudo nmap –A 104.26.9.237

**Raw Data**:

─$ sudo nmap -A 104.26.9.237

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-08 00:03 EDT

Nmap scan report for 104.26.9.237

Host is up (0.014s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

80/tcp open http Cloudflare http proxy

|\_http-server-header: cloudflare

|\_http-title: Site doesn't have a title (text/plain; charset=UTF-8).

443/tcp open ssl/https cloudflare

|\_http-server-header: cloudflare

|\_http-title: 400 The plain HTTP request was sent to HTTPS port

8080/tcp open http Cloudflare http proxy

|\_http-title: Site doesn't have a title (text/plain; charset=UTF-8).

|\_http-server-header: cloudflare

8443/tcp open ssl/https-alt cloudflare

|\_http-server-header: cloudflare

|\_http-title: 400 The plain HTTP request was sent to HTTPS port

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Crestron XPanel control system (89%), ASUS RT-N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%), Linux 3.16 (87%), Linux 3.2 (87%), HP P2000 G3 NAS device (87%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (86%), Android 4.1 - 6.0 (Linux 3.4 - 3.14) (86%), Android 5.0 - 6.0.1 (Linux 3.4) (86%), Android 5.0 - 7.0 (Linux 3.4 - 3.10) (86%)

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

Network Distance: 9 hops

TRACEROUTE (using port 443/tcp)

HOP RTT ADDRESS

1 5.70 ms 192.168.2.1

2 ... 3

4 15.48 ms 64.230.53.50

5 17.03 ms 142.124.127.213

6 13.38 ms 142.124.127.39

7 16.65 ms 108.162.239.32

8 16.64 ms 108.162.239.4

9 14.65 ms 104.26.9.237

Results:

* The Nmap aggressive scan of IP address 104.26.9.237, performed on 2024-08-08, shows that the host is up with a latency of 0.014 seconds.
* The scan identifies four open ports: 80 (HTTP), 443 (HTTPS), 8080 (HTTP), and 8443 (HTTPS-Alt), all associated with Cloudflare, indicating the presence of Cloudflare's proxy services across these ports.
* For each open port, the server responds with a Cloudflare HTTP header and, for ports 443 and 8443, reports a "400 The plain HTTP request was sent to HTTPS port" error.
* The scan’s OS detection yielded several possible but unreliable guesses, such as Crestron XPanel control system, various Linux versions, and Android devices, due to inadequate test conditions.
* The network distance to the host is determined to be 9 hops, with traceroute revealing the path through multiple IP addresses, including 108.162.239.32 and 108.162.239.4, before reaching the target.

**Command:** Sudo nmap –A 50.116.1.184

**Raw Data**:

─$ sudo nmap -A 50.116.1.184

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-08 00:03 EDT

Nmap scan report for ack.nmap.org (50.116.1.184)

Host is up (0.070s latency).

Not shown: 994 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.4 (protocol 2.0)

| ssh-hostkey:

| 2048 48:e0:c6:cd:14:00:00:db:b6:b0:3d:f2:0a:2a:3b:6d (RSA)

| 256 88:2b:29:00:d0:c7:81:ac:dd:f4:90:42:d2:aa:f0:5b (ECDSA)

|\_ 256 64:d6:39:35:04:76:1c:ba:17:f3:fd:4f:1f:b3:71:61 (ED25519)

70/tcp closed gopher

80/tcp open http Apache httpd 2.4.6

|\_http-server-header: Apache/2.4.6 (CentOS)

|\_http-title: 403 Forbidden

113/tcp closed ident

443/tcp open ssl/http Apache httpd 2.4.6

|\_http-server-header: Apache/2.4.6 (CentOS)

|\_http-title: Did not follow redirect to https://nmap.org/

|\_ssl-date: TLS randomness does not represent time

| ssl-cert: Subject: commonName=insecure.com

| Subject Alternative Name: DNS:insecure.com, DNS:insecure.org, DNS:issues.nmap.org, DNS:issues.npcap.org, DNS:nmap.com, DNS:nmap.net, DNS:nmap.org, DNS:npcap.com, DNS:npcap.org, DNS:seclists.com, DNS:seclists.net, DNS:seclists.org, DNS:sectools.com, DNS:sectools.net, DNS:sectools.org, DNS:secwiki.com, DNS:secwiki.net, DNS:secwiki.org, DNS:svn.nmap.org, DNS:www.nmap.org

| Not valid before: 2024-06-11T09:03:25

|\_Not valid after: 2024-09-09T09:03:24

31337/tcp closed Elite

Device type: broadband router|storage-misc|general purpose|WAP|media device

Running (JUST GUESSING): Linux 3.X|2.6.X|5.X|4.X (90%), HP embedded (89%), Ubiquiti embedded (88%), Ubiquiti AirOS 5.X (88%)

OS CPE: cpe:/o:linux:linux\_kernel:3 cpe:/h:hp:p2000\_g3 cpe:/o:linux:linux\_kernel:2.6.32 cpe:/h:ubnt:airmax\_nanostation cpe:/o:linux:linux\_kernel:5.0 cpe:/o:ubnt:airos:5.5.9 cpe:/o:linux:linux\_kernel:4.2 cpe:/o:linux:linux\_kernel:2.6

Aggressive OS guesses: OpenWrt 12.09-rc1 Attitude Adjustment (Linux 3.3 - 3.7) (90%), HP P2000 G3 NAS device (89%), Linux 2.6.32 (88%), Linux 2.6.32 - 3.1 (88%), Ubiquiti AirMax NanoStation WAP (Linux 2.6.32) (88%), Linux 3.7 (88%), Linux 5.0 (88%), Linux 5.0 - 5.4 (88%), Linux 5.1 (88%), Ubiquiti AirOS 5.5.9 (88%)

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

Network Distance: 17 hops

Service Info: Host: issues.nmap.org

TRACEROUTE (using port 31337/tcp)

HOP RTT ADDRESS

1 10.31 ms 192.168.2.1

2 ... 3

4 31.74 ms 64.230.53.52

5 ...

6 31.22 ms 64.230.79.73

7 ... 8

9 26.77 ms 4.7.196.42

10 28.46 ms ae12.r02.ord01.icn.netarch.akamai.com (23.207.231.36)

11 70.94 ms ae16.r02.sjc01.icn.netarch.akamai.com (23.193.113.29)

12 74.52 ms ae2.r12.sjc01.ien.netarch.akamai.com (23.207.232.41)

13 69.61 ms a23-203-158-51.deploy.static.akamaitechnologies.com (23.203.158.51)

14 69.56 ms 10.203.32.4

15 ...

16 67.50 ms 10.203.8.6

17 70.00 ms ack.nmap.org (50.116.1.184)

Results:

* The aggressive Nmap scan of IP address 50.116.1.184, identified as ack.nmap.org, shows that the host is responsive with a latency of 0.070 seconds.
* The scan reveals open ports for SSH (22/tcp), running OpenSSH 7.4, and HTTP (80/tcp) and HTTPS (443/tcp), both served by Apache httpd 2.4.6 on CentOS.
* The HTTPS service displays an SSL certificate with a common name of insecure.com and multiple DNS entries, valid from June 11, 2024, to September 9, 2024. Ports 70/tcp (gopher), 113/tcp (ident), and 31337/tcp (Elite) are closed.
* The scan includes an OS fingerprinting that suggests possible operating systems and devices, including various Linux versions and Ubiquiti devices, but no exact match was found.
* The network path to the host traverses 17 hops, with traceroute results showing a route through several Akamai and other network nodes before reaching the destination