**TASK-2 - Evading IDS/Firewall with Fragmented Packets**

**Scenario**

A client suspects their Intrusion Detection System (IDS) is blocking legitimate scans. They want you to test the effectiveness of their IDS by performing a stealthy scan that avoids detection. The goal is to identify open ports without triggering alerts.

**Objectives**

* Perform a network scan while evading IDS/firewall detection.
* Use fragmented packets and timing techniques to avoid detection.
* Compare results with a standard scan.

**Instructions**

1. **Understand Evasion Techniques**: Research Nmap’s evasion options, such as packet fragmentation (-f), decoy scans (-D), and timing adjustments (-T). Understand how these techniques help bypass IDS.
2. **Perform a Standard Scan**: First, run a basic SYN scan (-sS) on the target IP to establish a baseline of open ports and services. Document the results.
3. **Perform a Stealth Scan**: Use fragmentation (-f) and slow timing (-T2) to evade detection. Compare the results with the standard scan. Note any differences in detected ports or services.
4. **Analyze IDS Logs**: If possible, review the IDS logs (or simulate this step) to confirm whether the stealth scan avoided detection. Document your findings.

**PRACTICE – RESULTS**

1. **Scenario**

A client suspects their Intrusion Detection System (IDS) is blocking legitimate scans. They want you to test the effectiveness of their IDS by performing a stealthy scan that avoids detection. The goal is to identify open ports without triggering alerts.

Objectives

Perform a network scan while evading IDS/firewall detection.

Use fragmented packets and timing techniques to avoid detection.

Compare results with a standard scan.

**Instructions**

Understand Evasion Techniques: Research Nmap’s evasion options, such as packet fragmentation (-f), decoy scans (-D), and timing adjustments (-T). Understand how these techniques help bypass IDS.

Perform a Standard Scan: First, run a basic SYN scan (-sS) on the target IP to establish a baseline of open ports and services. Document the results.

Perform a Stealth Scan: Use fragmentation (-f) and slow timing (-T2) to evade detection. Compare the results with the standard scan. Note any differences in detected ports or services.

**Analyze IDS Logs:** If possible, review the IDS logs (or simulate this step) to confirm whether the stealth scan avoided detection. Document your findings.

1. **NMAP T0, T1, T2, T3, T4**

**nmap -T1 192.168.0.170**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 22:47 +0530

Nmap scan report for 192.168.0.170

Host is up (0.00055s latency).

Not shown: 992 closed tcp ports (reset)

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

902/tcp open iss-realsecure

912/tcp open apex-mesh

2869/tcp open icslap

5357/tcp open wsdapi

8090/tcp open opsmessaging

**Nmap done: 1 IP address (1 host up) scanned in 16495.46 seconds**

**nmap -T2 192.168.0.170**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 21:38 +0530

Nmap scan report for 192.168.0.170

Host is up (0.00063s latency).

Not shown: 994 closed tcp ports (reset)

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

902/tcp open iss-realsecure

912/tcp open apex-mesh

5357/tcp open wsdapi

**Nmap done: 1 IP address (1 host up) scanned in 405.28 seconds**

**nmap -T3 192.168.0.170**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 21:39 +0530

Nmap scan report for 192.168.0.170

Host is up (0.000021s latency).

Not shown: 994 closed tcp ports (reset)

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

902/tcp open iss-realsecure

912/tcp open apex-mesh

5357/tcp open wsdapi

**Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds**

**nmap -T5 192.168.0.170**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 21:40 +0530

Nmap scan report for 192.168.0.170

Host is up (0.00013s latency).

Not shown: 994 closed tcp ports (reset)

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

902/tcp open iss-realsecure

912/tcp open apex-mesh

5357/tcp open wsdapi

**Nmap done: 1 IP address (1 host up) scanned in 0.87 seconds**

1. **nmap -A -T4 www.cloudstory.ind.in**

**$ nmap -A -T4 www.cloudstory.ind.in**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 23:11 +0530

NSOCK ERROR [49.7990s] poll\_loop(): nsock\_loop error 10022: An invalid argument was supplied.

NSE: Script Engine Scan Aborted.

An error was thrown by the engine: C:\Program Files (x86)\Nmap/nse\_main.lua:1078: a fatal error occurred in nsock\_loop

stack traceback:

[C]: in function 'nmap.socket.loop'

C:\Program Files (x86)\Nmap/nse\_main.lua:1078: in upvalue 'run'

C:\Program Files (x86)\Nmap/nse\_main.lua:1488: in function <C:\Program Files (x86)\Nmap/nse\_main.lua:1435>

[C]: in ?

**Nmap scan report for www.cloudstory.ind.in (65.254.80.15)**

**Host is up (0.020s latency).**

**rDNS record for 65.254.80.15: 65-254-80-15.webhostbox.net**

**Not shown: 919 filtered tcp ports (no-response), 10 filtered tcp ports (admin-prohibited), 60 closed tcp ports (reset)**

**PORT STATE SERVICE VERSION**

**22/tcp open ssh OpenSSH 8.0 (protocol 2.0)**

| ssh-hostkey:

| 3072 19:62:79:d8:cd:5a:c6:86:61:19:cf:b7:4c:42:08:da (RSA)

| 256 f7:81:86:d3:77:e3:50:44:32:40:9f:1b:11:ad:e3:b4 (ECDSA)

|\_ 256 ab:51:ae:09:e3:55:08:bd:3d:90:43:3c:be:fb:26:e2 (ED25519)

**53/tcp open domain PowerDNS Authoritative Server 4.9.5**

| dns-nsid:

| NSID: 65-254-80-15.cprapid.com (36352d3235342d38302d31352e637072617069642e636f6d)

| id.server: 65-254-80-15.cprapid.com

|\_ bind.version: PowerDNS Authoritative Server 4.9.5 (built May 12 2025 13:41:30 by root@bh-centos-8.dev.cpanel.net)

**80/tcp open http Apache httpd**

|\_http-server-header: Apache

|\_http-title: Cloudstory

**110/tcp open pop3 Dovecot pop3d**

|\_pop3-capabilities: TOP USER STLS SASL(PLAIN LOGIN) RESP-CODES CAPA PIPELINING AUTH-RESP-CODE UIDL

**143/tcp open imap Dovecot imapd**

|\_imap-capabilities: IMAP4rev1 post-login LOGIN-REFERRALS LITERAL+ NAMESPACE STARTTLS Pre-login SASL-IR capabilities ID AUTH=LOGINA0001 listed OK have more IDLE AUTH=PLAIN ENABLE

**443/tcp open ssl/http Apache httpd**

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

|\_http-server-header: Apache

|\_http-title: Cloudstory

**465/tcp open ssl/smtp Exim smtpd 4.98.2**

| ssl-cert: Subject: commonName=cloudstory.ind.in

| Subject Alternative Name: DNS:cloudstory.ind.in, DNS:cpanel.cloudstory.ind.in, DNS:cpcalendars.cloudstory.ind.in, DNS:cpcontacts.cloudstory.ind.in, DNS:mail.cloudstory.ind.in, DNS:webdisk.cloudstory.ind.in, DNS:www.cloudstory.ind.in

| Not valid before: 2025-06-22T22:28:47

|\_Not valid after: 2025-09-20T22:28:46

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

| smtp-commands: 65-254-80-15.cprapid.com Hello www.cloudstory.ind.in [49.207.202.153], SIZE 52428800, LIMITS MAILMAX=1000 RCPTMAX=50000, 8BITMIME, PIPELINING, PIPECONNECT, AUTH PLAIN LOGIN, HELP

|\_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP

**587/tcp open smtp Exim smtpd 4.98.2**

| smtp-commands: 65-254-80-15.cprapid.com Hello www.cloudstory.ind.in [49.207.202.153], SIZE 52428800, LIMITS MAILMAX=1000 RCPTMAX=50000, 8BITMIME, PIPELINING, PIPECONNECT, STARTTLS, HELP

|\_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP

**993/tcp open imaps?**

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

| ssl-cert: Subject: commonName=cloudstory.ind.in

| Subject Alternative Name: DNS:cloudstory.ind.in, DNS:cpanel.cloudstory.ind.in, DNS:cpcalendars.cloudstory.ind.in, DNS:cpcontacts.cloudstory.ind.in, DNS:mail.cloudstory.ind.in, DNS:webdisk.cloudstory.ind.in, DNS:www.cloudstory.ind.in

| Not valid before: 2025-06-22T22:28:47

|\_Not valid after: 2025-09-20T22:28:46

|\_imap-capabilities: IMAP4rev1 post-login LOGIN-REFERRALS LITERAL+ NAMESPACE have ENABLE SASL-IR capabilities ID AUTH=LOGINA0001 listed Pre-login more IDLE AUTH=PLAIN OK

**995/tcp open pop3s?**

| ssl-cert: Subject: commonName=cloudstory.ind.in

| Subject Alternative Name: DNS:cloudstory.ind.in, DNS:cpanel.cloudstory.ind.in, DNS:cpcalendars.cloudstory.ind.in, DNS:cpcontacts.cloudstory.ind.in, DNS:mail.cloudstory.ind.in, DNS:webdisk.cloudstory.ind.in, DNS:www.cloudstory.ind.in

| Not valid before: 2025-06-22T22:28:47

|\_Not valid after: 2025-09-20T22:28:46

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

|\_pop3-capabilities: TOP USER SASL(PLAIN LOGIN) RESP-CODES CAPA PIPELINING AUTH-RESP-CODE UIDL

**3306/tcp open mysql MariaDB 5.5.5-10.11.13**

| mysql-info:

| Protocol: 10

| Version: 5.5.5-10.11.13-MariaDB

| Thread ID: 4673

| Capabilities flags: 63486

| Some Capabilities: SupportsCompression, LongColumnFlag, Speaks41ProtocolNew, SupportsTransactions, ConnectWithDatabase, Speaks41ProtocolOld, DontAllowDatabaseTableColumn, IgnoreSigpipes, Support41Auth, ODBCClient, SupportsLoadDataLocal, IgnoreSpaceBeforeParenthesis, FoundRows, InteractiveClient, SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults

| Status: Autocommit

| Salt: ,~Y$Eo"WmBBaCls"H$z\

|\_ Auth Plugin Name: mysql\_native\_password

Aggressive OS guesses: Linux 3.4 (92%), Linux 4.15 (92%), Linux 4.19 - 5.15 (92%), Linux 3.11 - 4.9 (88%), Linux 3.2 - 3.8 (88%), Android TV OS 11 (Linux 4.19) (86%), IPFire 2.25 firewall (Linux 4.14) (86%), IPFire 2.27 (Linux 5.15 - 6.1) (86%), Linux 2.6.32 (86%), Linux 3.5 (86%)

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

Service Info: Host: 65-254-80-15.cprapid.com

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

1 4.00 ms 192.168.0.1

2 ... 30

NSOCK ERROR [49.8390s] poll\_loop(): nsock\_loop error 10022: An invalid argument was supplied.

NSE: Script Engine Scan Aborted.

An error was thrown by the engine: C:\Program Files (x86)\Nmap/nse\_main.lua:1078: a fatal error occurred in nsock\_loop

stack traceback:

[C]: in function 'nmap.socket.loop'

C:\Program Files (x86)\Nmap/nse\_main.lua:1078: in upvalue 'run'

C:\Program Files (x86)\Nmap/nse\_main.lua:1488: in function <C:\Program Files (x86)\Nmap/nse\_main.lua:1435>

[C]: in ?

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

**Nmap done: 1 IP address (1 host up) scanned in 49.84 seconds**

**Nmap Evasion Techniques - Basic Discovery (Baseline)**

**Packet Fragmentation (-f)**

* + 1. **nmap -sS -T3 -v 192.168.0.170 - This is your normal scan without evasion to compare later.**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 23:16 +0530

Initiating Parallel DNS resolution of 1 host. at 23:16

Completed Parallel DNS resolution of 1 host. at 23:16, 0.51s elapsed

Initiating SYN Stealth Scan at 23:16

Scanning 192.168.0.170 [1000 ports]

Discovered open port 139/tcp on 192.168.0.170

Discovered open port 445/tcp on 192.168.0.170

Discovered open port 135/tcp on 192.168.0.170

Discovered open port 912/tcp on 192.168.0.170

Discovered open port 5357/tcp on 192.168.0.170

Discovered open port 8090/tcp on 192.168.0.170

Discovered open port 902/tcp on 192.168.0.170

Completed SYN Stealth Scan at 23:16, 0.09s elapsed (1000 total ports)

Nmap scan report for 192.168.0.170

Host is up (0.00024s latency).

Not shown: 993 closed tcp ports (reset)

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

902/tcp open iss-realsecure

912/tcp open apex-mesh

5357/tcp open wsdapi

8090/tcp open opsmessaging

Read data files from: C:\Program Files (x86)\Nmap

Nmap done: 1 IP address (1 host up) scanned in 1.00 seconds

Raw packets sent: 1000 (44.000KB) | Rcvd: 2007 (84.308KB)

**Packet Fragmentation (-f)**

* + 1. **nmap -sS -f -v 192.168.65.131 - Sends fragmented packets to avoid detection by simple IDS.**

Warning: Packet fragmentation selected on a host other than Linux, OpenBSD, FreeBSD, or NetBSD. This may or may not work.

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 23:21 +0530

Initiating ARP Ping Scan at 23:21

Scanning 192.168.65.131 [1 port]

Completed ARP Ping Scan at 23:21, 0.06s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 23:21

Completed Parallel DNS resolution of 1 host. at 23:21, 0.50s elapsed

Initiating SYN Stealth Scan at 23:21

Scanning 192.168.65.131 [1000 ports]

Discovered open port 23/tcp on 192.168.65.131

Discovered open port 5900/tcp on 192.168.65.131

Discovered open port 22/tcp on 192.168.65.131

Discovered open port 139/tcp on 192.168.65.131

Discovered open port 3306/tcp on 192.168.65.131

Discovered open port 25/tcp on 192.168.65.131

Discovered open port 111/tcp on 192.168.65.131

Discovered open port 80/tcp on 192.168.65.131

Discovered open port 445/tcp on 192.168.65.131

Discovered open port 21/tcp on 192.168.65.131

Discovered open port 1099/tcp on 192.168.65.131

Discovered open port 6667/tcp on 192.168.65.131

Discovered open port 1524/tcp on 192.168.65.131

Discovered open port 514/tcp on 192.168.65.131

Discovered open port 6000/tcp on 192.168.65.131

Discovered open port 513/tcp on 192.168.65.131

Discovered open port 8009/tcp on 192.168.65.131

Discovered open port 5432/tcp on 192.168.65.131

Discovered open port 2121/tcp on 192.168.65.131

Discovered open port 2049/tcp on 192.168.65.131

Discovered open port 8180/tcp on 192.168.65.131

Discovered open port 512/tcp on 192.168.65.131

Completed SYN Stealth Scan at 23:21, 0.10s elapsed (1000 total ports)

Nmap scan report for 192.168.65.131

Host is up (0.0000020s latency).

Not shown: 978 closed tcp ports (reset)

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

23/tcp open telnet

25/tcp open smtp

80/tcp open http

111/tcp open rpcbind

139/tcp open netbios-ssn

445/tcp open microsoft-ds

512/tcp open exec

513/tcp open login

514/tcp open shell

1099/tcp open rmiregistry

1524/tcp open ingreslock

2049/tcp open nfs

2121/tcp open ccproxy-ftp

3306/tcp open mysql

5432/tcp open postgresql

5900/tcp open vnc

6000/tcp open X11

6667/tcp open irc

8009/tcp open ajp13

8180/tcp open unknown

MAC Address: 00:0C:29:90:CA:F0 (VMware)

Read data files from: C:\Program Files (x86)\Nmap

Nmap done: 1 IP address (1 host up) scanned in 1.03 seconds

**Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.116KB)**

* 1. **Decoy Scan (-D) - Your scan is hidden among 5 random decoy IPs**

**nmap -sS -D RND:5 192.168.65.131**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 23:33 +0530

Nmap scan report for 192.168.65.131

Host is up (0.00084s latency).

Not shown: 978 closed tcp ports (reset)

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

23/tcp open telnet

25/tcp open smtp

80/tcp open http

111/tcp open rpcbind

139/tcp open netbios-ssn

445/tcp open microsoft-ds

512/tcp open exec

513/tcp open login

514/tcp open shell

1099/tcp open rmiregistry

1524/tcp open ingreslock

2049/tcp open nfs

2121/tcp open ccproxy-ftp

3306/tcp open mysql

5432/tcp open postgresql

5900/tcp open vnc

6000/tcp open X11

6667/tcp open irc

8009/tcp open ajp13

8180/tcp open unknown

MAC Address: 00:0C:29:90:CA:F0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.86 seconds

**Spoof Source Port (--source-port)**

* + 1. **nmap -sS --source-port 53 192.168.65.131**

nmap -sS --source-port 53 192.168.65.131

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 23:35 +0530

Nmap scan report for 192.168.65.131

Host is up (0.00075s latency).

Not shown: 978 closed tcp ports (reset)

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

23/tcp open telnet

25/tcp open smtp

80/tcp open http

111/tcp open rpcbind

139/tcp open netbios-ssn

445/tcp open microsoft-ds

512/tcp open exec

513/tcp open login

514/tcp open shell

1099/tcp open rmiregistry

1524/tcp open ingreslock

2049/tcp open nfs

2121/tcp open ccproxy-ftp

3306/tcp open mysql

5432/tcp open postgresql

5900/tcp open vnc

6000/tcp open X11

6667/tcp open irc

8009/tcp open ajp13

8180/tcp open unknown

MAC Address: 00:0C:29:90:CA:F0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds

* 1. **MAC Address Spoofing (--spoof-mac)**
     1. **nmap -sS --spoof-mac Apple 192.168.65.131**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 23:38 +0530

Spoofing MAC address 00:03:93:82:B6:98 (Apple)

Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn

Nmap done: 1 IP address (0 hosts up) scanned in 6.26 seconds

* 1. **Combined Stealth Scan**
     1. **nmap -sS -f -T2 -D RND:10 --source-port 443 --spoof-mac Cisco 192.168.65.131**

Warning: Packet fragmentation selected on a host other than Linux, OpenBSD, FreeBSD, or NetBSD. This may or may not work.

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 23:40 +0530

Spoofing MAC address 00:00:0C:B7:30:BD (Cisco Systems)

Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn

Nmap done: 1 IP address (0 hosts up) scanned in 7.06 seconds

1. **Perform a Standard Scan: First, run a basic SYN scan (-sS) on the target IP to establish a baseline of open ports and services. Document the results.**
   1. **nmap -sS 192.168.65.131**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 23:48 +0530

Nmap scan report for 192.168.65.131

Host is up (0.00096s latency).

Not shown: 978 closed tcp ports (reset)

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

23/tcp open telnet

25/tcp open smtp

80/tcp open http

111/tcp open rpcbind

139/tcp open netbios-ssn

445/tcp open microsoft-ds

512/tcp open exec

513/tcp open login

514/tcp open shell

1099/tcp open rmiregistry

1524/tcp open ingreslock

2049/tcp open nfs

2121/tcp open ccproxy-ftp

3306/tcp open mysql

5432/tcp open postgresql

5900/tcp open vnc

6000/tcp open X11

6667/tcp open irc

8009/tcp open ajp13

8180/tcp open unknown

MAC Address: 00:0C:29:90:CA:F0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds

* 1. **nmap -sV 192.168.65.131**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 23:51 +0530

Nmap scan report for 192.168.65.131

Host is up (0.00094s latency).

Not shown: 978 closed tcp ports (reset)

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

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

111/tcp open rpcbind 2 (RPC #100000)

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 rexecd

513/tcp open login?

514/tcp open tcpwrapped

1099/tcp open java-rmi GNU Classpath grmiregistry

1524/tcp open bindshell Metasploitable root shell

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

2121/tcp open ftp ProFTPD 1.3.1

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

5900/tcp open vnc VNC (protocol 3.3)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

MAC Address: 00:0C:29:90:CA:F0 (VMware)

Service Info: Hosts: metasploitable.localdomain, 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 14.40 seconds

* 1. **nmap -A 192.168.65.131**

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 23:52 +0530

NSOCK ERROR [28.7630s] poll\_loop(): nsock\_loop error 10022: An invalid argument was supplied.

NSE: Script Engine Scan Aborted.

An error was thrown by the engine: C:\Program Files (x86)\Nmap/nse\_main.lua:1078: a fatal error occurred in nsock\_loop

stack traceback:

[C]: in function 'nmap.socket.loop'

C:\Program Files (x86)\Nmap/nse\_main.lua:1078: in upvalue 'run'

C:\Program Files (x86)\Nmap/nse\_main.lua:1488: in function <C:\Program Files (x86)\Nmap/nse\_main.lua:1435>

[C]: in ?

Nmap scan report for 192.168.65.131

Host is up (0.00067s latency).

Not shown: 978 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 192.168.65.1

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| vsFTPd 2.3.4 - secure, fast, stable

|\_End of status

|\_ftp-anon: Anonymous FTP login allowed (FTP code 230)

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

| ssh-hostkey:

| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)

|\_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

23/tcp open telnet Linux telnetd

25/tcp open smtp Postfix smtpd

|\_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN

|\_ssl-date: 2025-07-20T15:57:07+00:00; -2h26m12s from scanner time.

| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

| Not valid before: 2010-03-17T14:07:45

|\_Not valid after: 2010-04-16T14:07:45

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

|\_http-title: Metasploitable2 - Linux

|\_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

111/tcp open rpcbind 2 (RPC #100000)

|\_rpcinfo: ERROR: Script execution failed (use -d to debug)

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

512/tcp open exec netkit-rsh rexecd

513/tcp open login?

514/tcp open tcpwrapped

1099/tcp open java-rmi GNU Classpath grmiregistry

1524/tcp open bindshell Metasploitable root shell

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

2121/tcp open ftp ProFTPD 1.3.1

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

| mysql-info:

| Protocol: 10

| Version: 5.0.51a-3ubuntu5

| Thread ID: 10

| Capabilities flags: 43564

| Some Capabilities: SupportsTransactions, Support41Auth, Speaks41ProtocolNew, SwitchToSSLAfterHandshake, SupportsCompression, LongColumnFlag, ConnectWithDatabase

| Status: Autocommit

|\_ Salt: oKhK}Sg/N}MESR#T]Y%J

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

| Not valid before: 2010-03-17T14:07:45

|\_Not valid after: 2010-04-16T14:07:45

5900/tcp open vnc VNC (protocol 3.3)

| vnc-info:

| Protocol version: 3.3

| Security types:

|\_ VNC Authentication (2)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

| irc-info:

| users: 1

| servers: 1

| lusers: 1

| lservers: 0

| server: irc.Metasploitable.LAN

| version: Unreal3.2.8.1. irc.Metasploitable.LAN

| uptime: 0 days, 3:01:09

| source ident: nmap

| source host: 5080290D.B2C57017.FFFA6D49.IP

|\_ error: Closing Link: ypsazoiby[192.168.65.1] (Quit: ypsazoiby)

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

|\_ajp-methods: Failed to get a valid response for the OPTION request

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|\_http-favicon: Apache Tomcat

|\_http-server-header: Apache-Coyote/1.1

|\_http-title: Apache Tomcat/5.5

MAC Address: 00:0C:29:90:CA:F0 (VMware)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Network Distance: 1 hop

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Host script results:

| smb-security-mode:

| account\_used: guest

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

|\_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| Computer name: metasploitable

| NetBIOS computer name:

| Domain name: localdomain

| FQDN: metasploitable.localdomain

|\_ System time: 2025-07-20T11:56:53-04:00

|\_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE

HOP RTT ADDRESS

1 0.67 ms 192.168.65.131

NSOCK ERROR [28.7780s] poll\_loop(): nsock\_loop error 10022: An invalid argument was supplied.

NSE: Script Engine Scan Aborted.

An error was thrown by the engine: C:\Program Files (x86)\Nmap/nse\_main.lua:1078: a fatal error occurred in nsock\_loop

stack traceback:

[C]: in function 'nmap.socket.loop'

C:\Program Files (x86)\Nmap/nse\_main.lua:1078: in upvalue 'run'

C:\Program Files (x86)\Nmap/nse\_main.lua:1488: in function <C:\Program Files (x86)\Nmap/nse\_main.lua:1435>

[C]: in ?

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

Nmap done: 1 IP address (1 host up) scanned in 28.78 second

* 1. **nmap -f 192.168.65.131**

Warning: Packet fragmentation selected on a host other than Linux, OpenBSD, FreeBSD, or NetBSD. This may or may not work.

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-20 23:55 +0530

Nmap scan report for 192.168.65.131

Host is up (0.0000070s latency).

Not shown: 978 closed tcp ports (reset)

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

23/tcp open telnet

25/tcp open smtp

80/tcp open http

111/tcp open rpcbind

139/tcp open netbios-ssn

445/tcp open microsoft-ds

512/tcp open exec

513/tcp open login

514/tcp open shell

1099/tcp open rmiregistry

1524/tcp open ingreslock

2049/tcp open nfs

2121/tcp open ccproxy-ftp

3306/tcp open mysql

5432/tcp open postgresql

5900/tcp open vnc

6000/tcp open X11

6667/tcp open irc

8009/tcp open ajp13

8180/tcp open unknown

MAC Address: 00:0C:29:90:CA:F0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds

1. **Perform a Stealth Scan: Use fragmentation (-f) and slow timing (-T2) to evade detection. Compare the results with the standard scan. Note any differences in detected ports or services.**
   1. **nmap -sS -f -T2 192.168.65.130**

Warning: Packet fragmentation selected on a host other than Linux, OpenBSD, FreeBSD, or NetBSD. This may or may not work.

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-21 00:04 +0530

Nmap scan report for 192.168.65.130

Host is up (0.00059s latency).

All 1000 scanned ports on 192.168.65.130 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

**MAC Address: 00:0C:29:06:6B:CB (VMware)**

* 1. **Standard scan scans first 1000 ports, whereas nmap -sS ignores them.**

1. **Analyze IDS Logs: If possible, review the IDS logs (or simulate this step) to confirm whether the stealth scan avoided detection. Document your findings.**
   1. **REPORT**
   2. **WIFI LOGS**

netstat -a:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Active Internet connections (servers and established)

Proto Recv-Q Send-Q Local Address Foreign Address State

tcp 0 0 0.0.0.0:9000 0.0.0.0:\* LISTEN

tcp 0 0 192.168.0.1:80 0.0.0.0:\* LISTEN

tcp 0 0 0.0.0.0:52881 0.0.0.0:\* LISTEN

tcp 0 0 127.0.0.1:10002 0.0.0.0:\* LISTEN

tcp 0 0 127.0.0.1:10003 0.0.0.0:\* LISTEN

tcp 0 0 0.0.0.0:10004 0.0.0.0:\* LISTEN

tcp 0 0 0.0.0.0:7547 0.0.0.0:\* LISTEN

tcp 0 0 0.0.0.0:5500 0.0.0.0:\* LISTEN

tcp 0 0 192.168.0.1:80 192.168.0.170:17855 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17814 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17805 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17844 TIME\_WAIT

tcp 0 0 127.0.0.1:45826 127.0.0.1:10002 ESTABLISHED

tcp 0 0 192.168.0.1:80 192.168.0.170:17831 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17840 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17823 TIME\_WAIT

tcp 0 0 127.0.0.1:10003 127.0.0.1:39832 ESTABLISHED

tcp 0 0 192.168.0.1:80 192.168.0.170:17848 TIME\_WAIT

tcp 0 0 10.247.161.248:47024 8.211.36.117:11822 ESTABLISHED

tcp 0 0 192.168.0.1:80 192.168.0.170:17853 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17817 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17806 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17809 TIME\_WAIT

tcp 0 0 127.0.0.1:10002 127.0.0.1:45826 ESTABLISHED

tcp 0 0 192.168.0.1:80 192.168.0.170:17801 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17818 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17836 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17808 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17812 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17858 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17820 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17829 TIME\_WAIT

tcp 0 0 127.0.0.1:10004 127.0.0.1:60415 ESTABLISHED

tcp 0 0 192.168.0.1:80 192.168.0.170:17830 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17849 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17804 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17815 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17834 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17813 TIME\_WAIT

tcp 0 0 127.0.0.1:39832 127.0.0.1:10003 ESTABLISHED

tcp 0 0 192.168.0.1:80 192.168.0.170:17816 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17827 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17839 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17822 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17824 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17811 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17833 TIME\_WAIT

tcp 0 0 127.0.0.1:60415 127.0.0.1:10004 ESTABLISHED

tcp 0 0 192.168.0.1:80 192.168.0.170:17863 ESTABLISHED

tcp 0 0 192.168.0.1:80 192.168.0.170:17842 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17807 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17856 TIME\_WAIT

tcp 0 0 192.168.0.1:80 192.168.0.170:17802 TIME\_WAIT

tcp 0 0 :::80 :::\* LISTEN

udp 0 0 0.0.0.0:53 0.0.0.0:\*

udp 0 0 192.168.0.1:67 0.0.0.0:\*

udp 0 0 0.0.0.0:67 0.0.0.0:\*

udp 0 0 0.0.0.0:67 0.0.0.0:\*

udp 0 0 0.0.0.0:1900 0.0.0.0:\*

udp 0 0 0.0.0.0:1900 0.0.0.0:\*

udp 0 0 0.0.0.0:137 0.0.0.0:\*

udp 0 0 0.0.0.0:47255 0.0.0.0:\*

udp 0 0 192.168.0.1:48032 0.0.0.0:\*

udp 0 0 0.0.0.0:60618 0.0.0.0:\*

udp 0 0 0.0.0.0:5351 0.0.0.0:\*

udp 0 0 0.0.0.0:5353 0.0.0.0:\*

udp 0 0 192.168.0.1:39164 0.0.0.0:\*

udp 0 0 fe80::45f6:8be7:b99d:b96f:546 :::\*

udp 0 0 :::547 :::\*

udp 0 0 :::48716 :::\*

raw 0 0 0.0.0.0:255 0.0.0.0:\* 255

raw 0 0 ::%4512024:58 :::\* 58

Active UNIX domain sockets (servers and established)

Proto RefCnt Flags Type State I-Node Path

unix 2 [ ACC ] STREAM LISTENING 2658 /tmp/auto.socket

unix 2 [ ACC ] STREAM LISTENING 649 /var/pm\_socket

unix 2 [ ACC ] STREAM LISTENING 663 /var/cfm\_socket

unix 2 [ ACC ] STREAM LISTENING 668 /var/plog\_socket

unix 2 [ ACC ] STREAM LISTENING 1194 /var/nt\_socket

unix 2 [ ACC ] STREAM LISTENING 2027 /var/mw\_socket

unix 2 [ ACC ] STREAM LISTENING 1261 /var/wlan\_server\_socket

unix 2 [ ] DGRAM 2691

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

cat /proc/meminfo:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

MemTotal: 48756 kB

MemFree: 10996 kB

Buffers: 1388 kB

Cached: 13400 kB

SwapCached: 0 kB

Active: 9400 kB

Inactive: 5972 kB

Active(anon): 6076 kB

Inactive(anon): 0 kB

Active(file): 3324 kB

Inactive(file): 5972 kB

Unevictable: 5492 kB

Mlocked: 0 kB

SwapTotal: 0 kB

SwapFree: 0 kB

Dirty: 0 kB

Writeback: 0 kB

AnonPages: 6096 kB

Mapped: 4764 kB

Shmem: 0 kB

Slab: 6180 kB

SReclaimable: 1300 kB

SUnreclaim: 4880 kB

KernelStack: 504 kB

PageTables: 392 kB

NFS\_Unstable: 0 kB

Bounce: 0 kB

WritebackTmp: 0 kB

CommitLimit: 24376 kB

Committed\_AS: 32124 kB

VmallocTotal: 1048372 kB

VmallocUsed: 792 kB

VmallocChunk: 1046020 kB

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

cat /proc/slabinfo:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

cat /proc/interrupts:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

CPU0

2: 181 MIPS IRQ cascade

4: 9706075 MIPS eth0

5: 1852778 MIPS wlan0

6: 16570670 MIPS wlan1

7: 9017577 MIPS timer

17: 181 ICTL serial

24: 0 ICTL gpio cascade1

25: 0 ICTL gpio cascade2

ERR: 0

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

arp -a:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

? (192.168.0.170) at 14:85:7f:33:b7:a1 [ether] on br0

? (192.168.0.168) at 26:b7:9b:77:2a:a2 [ether] on br0

? (192.168.0.181) at 9e:e4:5b:91:5f:1c [ether] on br0

* 1. **REPORT – WIFI LOGS PROVIDES IP & PORT DETAILS WHEREAS nmap provides**

**netstat -a – Open and Active Network Connections**

* **Listening Ports:**
  + Port 80 (HTTP), 9000, 7547, 5500 are open.
  + Internal services: 127.0.0.1:10002, 10003, 10004 indicate local apps or management interfaces.
* **Active Connections**:
  + Many TIME\_WAIT states **to 192.168.0.170**, indicating repeated short-lived HTTP sessions (likely a user browsing).
  + One external connection: **10.247.161.248** → 8.211.36.117:11822, which might be a remote admin session or external data communication.

These logs help in identifying services running, unauthorized access, or suspicious activity over HTTP or other ports.

2. cat /proc/meminfo – Memory Usage Snapshot

* Total Memory: ~48MB (typical for embedded device).
* Free memory: ~11MB, low usage overall.
* No swap configured (common for flash storage devices).

Useful for debugging performance issues and resource exhaustion.

3. cat /proc/interrupts – Hardware Device Stats

* High interrupt counts on wlan0, wlan1, eth0: confirms active wireless and Ethernet interfaces.
* Timer and Serial IRQs also active.

Indicates that both Wi-Fi interfaces are heavily used (real client traffic).

4. arp -a – Active ARP Table

* Devices with IPs and MACs:
  + **192.168.0.170 → 14:85:7f:33:b7:a1**
  + **192.168.0.168 → 26:b7:9b:77:2a:a2**
  + **192.168.0.181 → 9e:e4:5b:91:5f:1c**

Can identify connected clients on the LAN/Wi-Fi and trace back to MACs.

🛠 **How This Compares with Nmap Scanning**

| **Feature** | **Wi-Fi Logs (Your Data)** | **Nmap Scan** |
| --- | --- | --- |
| Source | Generated by the router or access point | Generated by an external device scanning the network |
| Purpose | Monitors real-time system activity and connections | Probes systems to discover ports, services, and OS |
| Client Identification | ARP table and MACs provide direct device presence | Identifies live hosts via ping, ARP scan, or port activity |
| Port Visibility | Shows open/listening ports from the router’s view | Detects open ports from external network perspective |
| Service Detection | Implicit (e.g., port 80 = HTTP) | Explicit (e.g., Nmap can return Apache/2.4.7 on port 80) |
| Real-time Monitoring | Yes, dynamic data | Snapshot only (point-in-time scan) |
| Intrusion Detection Use | Can help correlate MAC/IP in security events | Helps find misconfigurations or exposed services |

🔐 **Security Relevance & Use Case**

* **From these logs:**
  + You can detect unusual external connections, such as outbound traffic to unknown IPs.
  + Use ARP/MAC mapping to trace unauthorized devices on Wi-Fi.
  + Validate which ports/services are unnecessarily exposed (e.g., port 7547 often abused via TR-069).
* **With Nmap:**
  + You’d simulate an attacker's view, showing which of the router's ports are accessible externally, or scan other devices on the same LAN (like .170, .168, etc.).

📌 Conclusion

Both Wi-Fi logs and Nmap serve critical roles:

* **Wi-Fi Logs = Internal monitoring & forensic insight**.
* **Nmap = External probing & vulnerability assessment**.

Together, they offer a complete picture for network diagnostics, penetration testing, or cybersecurity investigations.