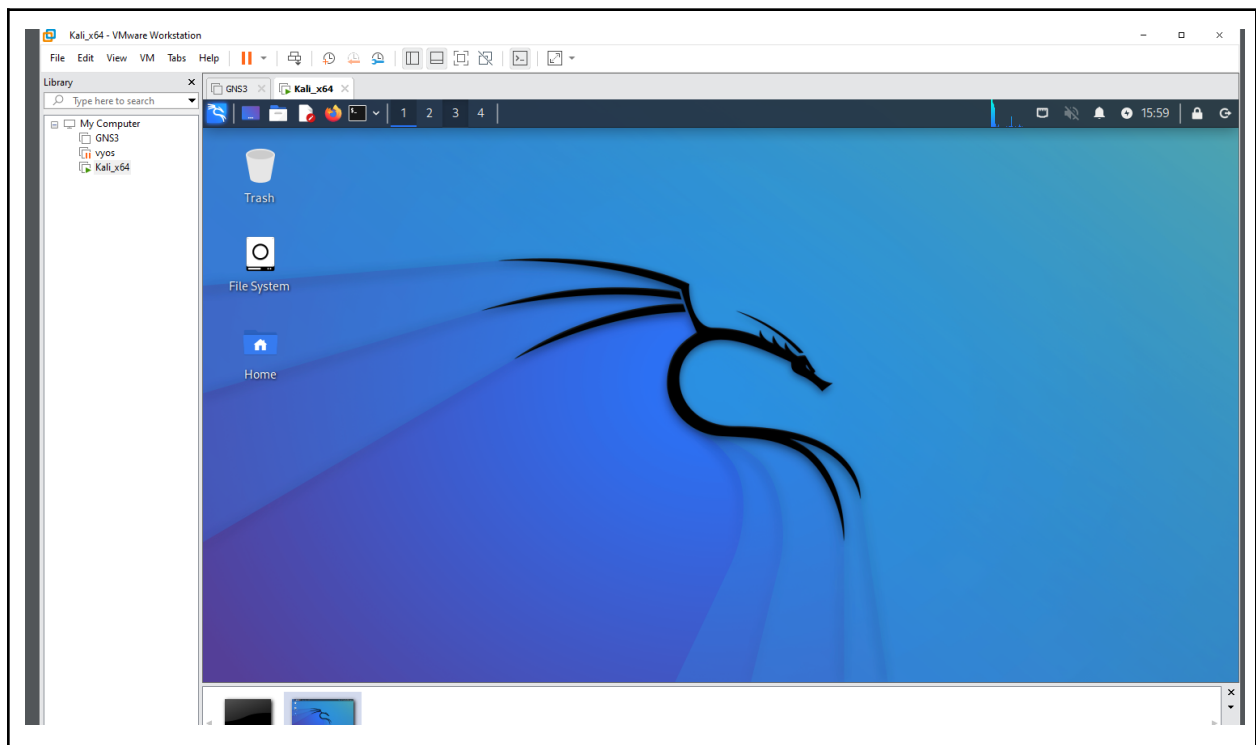


Mubariz Saeed  
CSF 432 - Lab#10  
Fall 2021

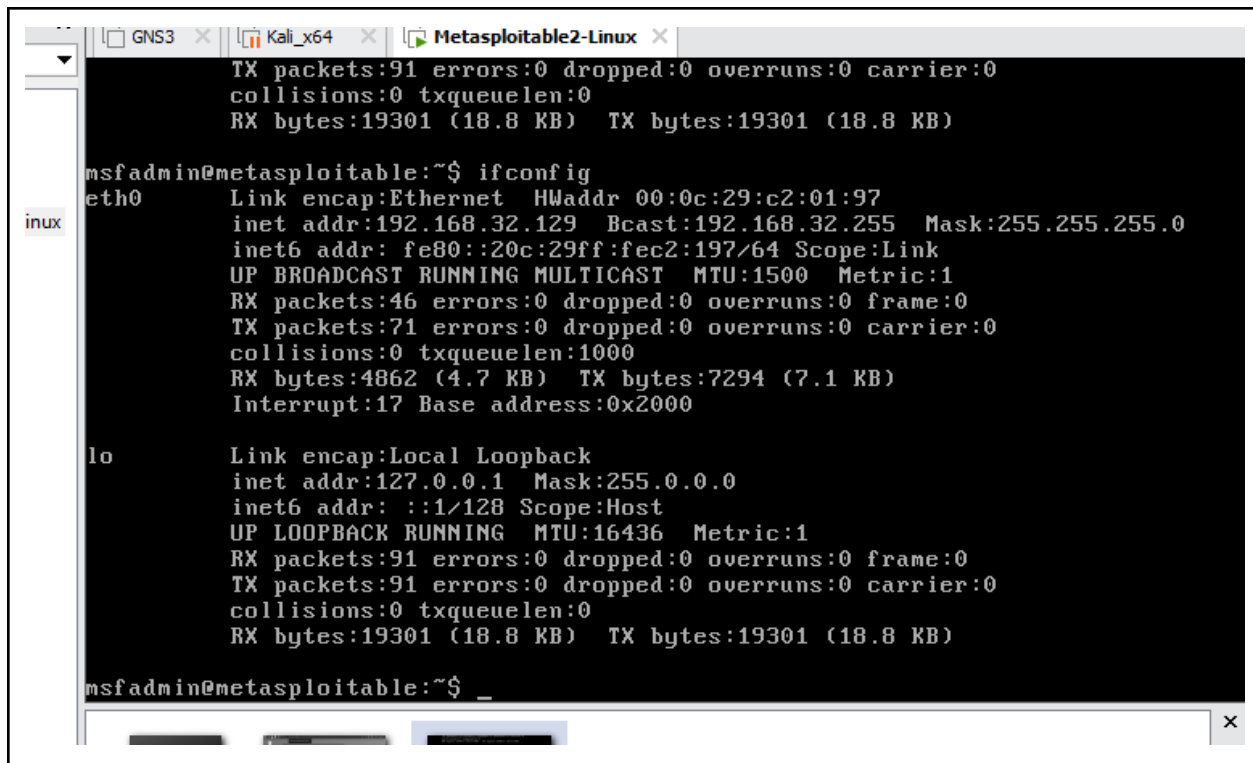
# Lab 10: Scanning with nmap and Netcat

## Part 1: Workstation Setup

!/? Question 1 - Submit a screenshot of your Kali terminal.



!/? Question 2 - Submit a screenshot of your ifconfig results.

A screenshot of a terminal window titled 'Metasploitable2-Linux'. The terminal shows the output of the 'ifconfig' command for the 'eth0' and 'lo' interfaces. The 'eth0' interface has an IPv4 address of 192.168.32.129. The prompt is 'msfadmin@metasploitable:~\$'.

```
TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c2:01:97
          inet addr:192.168.32.129  Bcast:192.168.32.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec2:197/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:46 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4862 (4.7 KB)  TX bytes:7294 (7.1 KB)
          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:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ _
```

!/? Question 3 - What is the IPv4 address assigned to your metasploitable VM?

192.168.32.129

## Part 2: Scanning with nmap

!/? Question 4 - Submit a screenshot of your scan results.

Target: 192.168.32.129 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.32.129

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

nmap -T4 -A -v 192.168.32.129

Starting Nmap 7.93 ( <https://nmap.org> ) at 2022-11-20 17:11 Pacific Standard Time  
NSOCK ERROR [0.2320s] ssl\_init\_helper(): OpenSSL legacy provider failed to load.

**NSE:** Loaded 155 scripts for scanning.

**NSE:** Script Pre-scanning.

Initiating NSE at 17:11

Completed NSE at 17:11, 0.00s elapsed

Initiating NSE at 17:11

Completed NSE at 17:11, 0.00s elapsed

Initiating NSE at 17:11

Completed NSE at 17:11, 0.00s elapsed

Initiating ARP Ping Scan at 17:11

Scanning 192.168.32.129 [1 port]

Completed ARP Ping Scan at 17:11, 0.03s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 17:11

Completed Parallel DNS resolution of 1 host. at 17:11, 0.01s elapsed

Initiating SYN Stealth Scan at 17:11

Scanning 192.168.32.129 [1000 ports]

Discovered open port 445/tcp on 192.168.32.129

Discovered open port 25/tcp on 192.168.32.129

Discovered open port 21/tcp on 192.168.32.129

Discovered open port 5900/tcp on 192.168.32.129

Discovered open port 23/tcp on 192.168.32.129

Discovered open port 139/tcp on 192.168.32.129

Discovered open port 3306/tcp on 192.168.32.129

Discovered open port 22/tcp on 192.168.32.129

Discovered open port 111/tcp on 192.168.32.129

Discovered open port 80/tcp on 192.168.32.129

Discovered open port 8009/tcp on 192.168.32.129

Discovered open port 514/tcp on 192.168.32.129

Discovered open port 6000/tcp on 192.168.32.129

Discovered open port 5432/tcp on 192.168.32.129

Discovered open port 2121/tcp on 192.168.32.129

Discovered open port 513/tcp on 192.168.32.129

Discovered open port 512/tcp on 192.168.32.129

Discovered open port 6667/tcp on 192.168.32.129

Discovered open port 1099/tcp on 192.168.32.129

Discovered open port 1524/tcp on 192.168.32.129

Discovered open port 2049/tcp on 192.168.32.129

Discovered open port 8180/tcp on 192.168.32.129

Completed SYN Stealth Scan at 17:11, 0.05s elapsed (1000 total ports)

Initiating Service scan at 17:11

Scanning 22 services on 192.168.32.129

Completed Service scan at 17:11, 11.08s elapsed (22 services on 1 host)

Initiating OS detection (try #1) against 192.168.32.129

**NSE:** Script scanning 192.168.32.129.

Initiating NSE at 17:11

**NSE:** [ftp-bounce] PORT response: 500 Illegal PORT command.

```
mubarizsaeed@csf432student:~$ nmap -T4 -Pn 192.168.32.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-20 20:12 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try
-Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.04 seconds

(mubarizsaeed@csf432student)-[~]
$ nmap -T4 -Pn 192.168.32.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 00:17 EST
Stats: 0:01:15 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 74.00% done; ETC: 00:18 (0:00:26 remaining)
Nmap scan report for 192.168.32.129
Host is up.
All 1000 scanned ports on 192.168.32.129 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 101.30 seconds

(mubarizsaeed@csf432student)-[~]
$ nmap -T4 -Pn 192.168.32.129
```

Wanted to see the actual ports so i download nmap

## Part 3: Immersive Labs

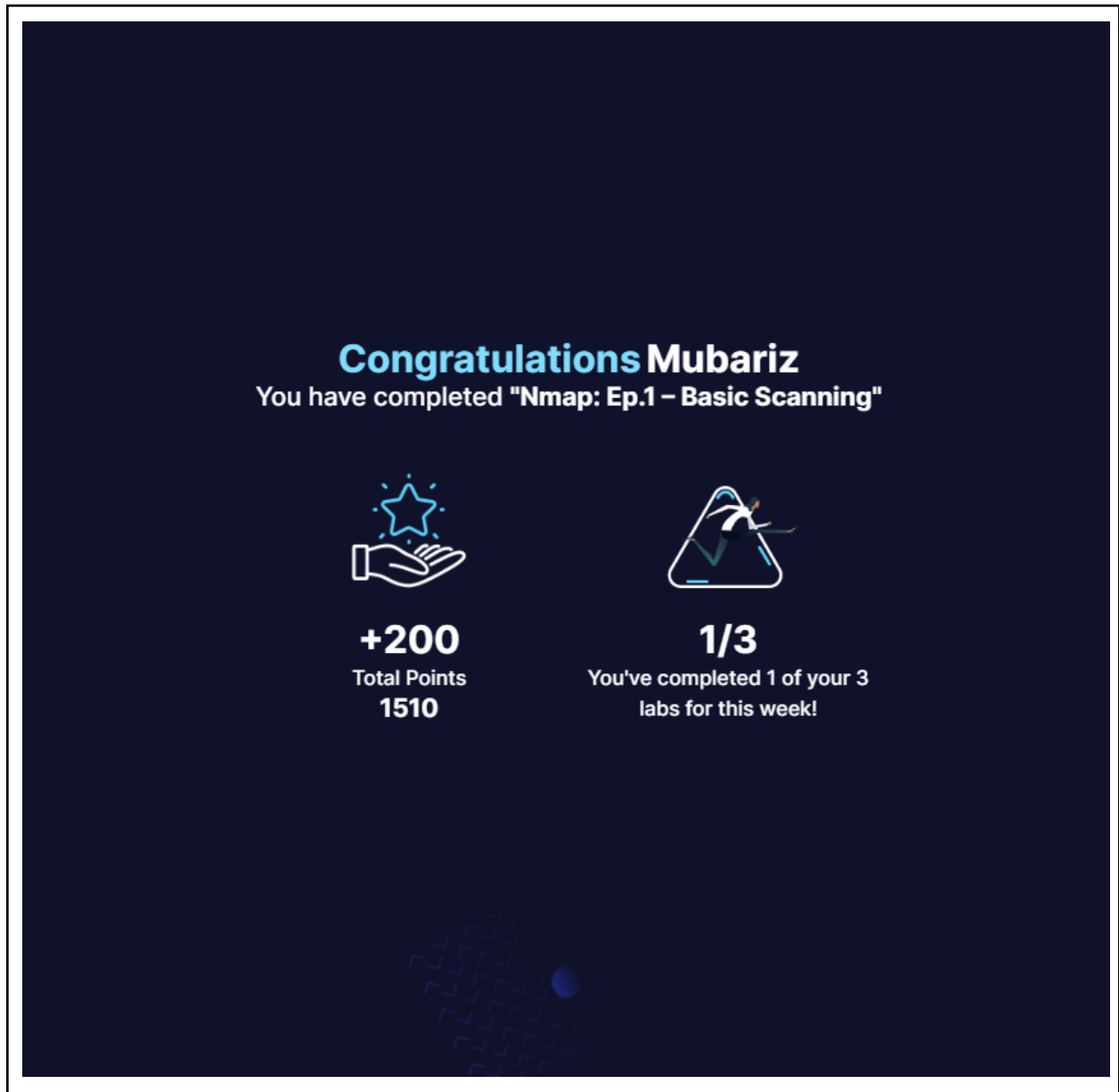
### Network Scanning

**!?** Question 5 - Submit a screenshot of your badge demonstrating the completion of this immersive lab module.



## Nmap: Episode 1 – Basic Scanning

**!?** Question 6 - Submit a screenshot of your badge demonstrating the completion of this immersive lab module.



## Netcat

**!?** Question 7 - Submit a screenshot of your badge demonstrating the completion of this immersive lab module.



## Banner Grabbing

**!?** Question 8 - Submit a screenshot of your badge demonstrating the completion of this immersive lab module.

**Congratulations Mubariz**  
You have completed "Banner Grabbing"



**+100**  
Total Points  
**1610**



**2/3**  
You've completed 2 of your 3  
labs for this week!

## Part 5: Submission

Convert your network document into a .PDF and upload a single `lastname_lab10.pdf` file to Brightspace through the attachment uploads option.