CSCI-6658-01

ETHICAL HACKING

Infoseclablearning Assignment-2

Enumerating Hosts Using Wireshark, Windows, and Linux Commands

Student Info:
Name : Akhila Parankusham
Student ID: 00810899
Email: apara7@unh.newhaven.edu

TABLE OF CONTENTS

Executive Summary

Highlights

Wireshark-Capturing Packets: Wireshark, a network protocol analyzer, empowers users to inspect and capture network packets. It serves as a lens into network traffic, revealing hidden details. In this lab, Wireshark is the tool of choice for capturing and scrutinizing packets to unveil machine IP addresses within the network.

ifconfig: "ifconfig" is a command tool in Linux that shows all the different ways your computer connects to networks. It's also a tool to make changes to how your computer talks to those networks.

Active Scanning: Passive scanning cannot be detected whereas active scanning is detected on a network. This lab is implemented by using two active scanning methods, one through the command line and another via graphical tools, all with the aim of uncovering valuable inventory information about networked machines.

net command (Windows): It helps you uncover critical network details like users, domains, shared resources, print jobs, and the roster of machines within the network.

nbtstat: It is a windows command-line tool. It is like a multilingual translator for network communication. It queries NetBIOS name resolution, which is like the network's linguistic backbone, helping different devices communicate efficiently over networks.

Metasploit: Metasploit is a toolbox for ethical hackers, included in Kali Linux. It is used in this lab to find devices on a specific network.

Armitage: Armitage is the user-friendly sidekick to Metasploit. It's a hacking tool that provides a visual interface, making it easier for investigators to explore potential targets and execute security tests on systems.

Objectives

This lab’s main goal is to use an Armitage to scan a network and also to use system commands like ifconfig, nmap, and Wireshark to list resources on a target system.

Lab Description Details

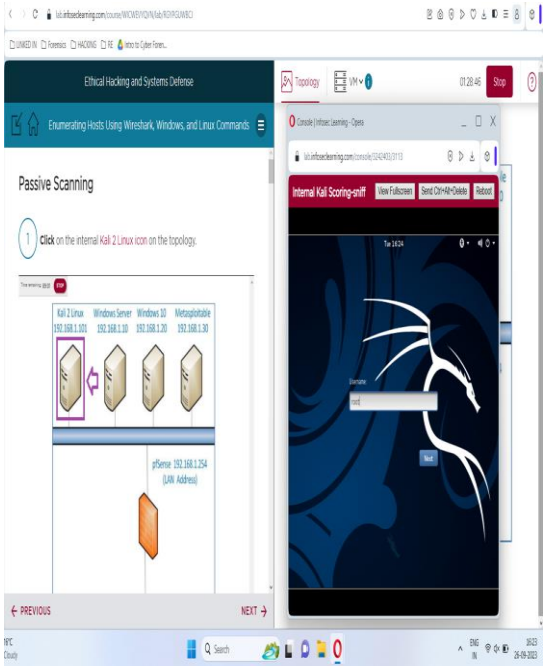
1. Lab Environment Setup: Creating a controlled network environment that resembles real-world configurations, using Metasploitable, Windows Server, Kali Linux, and Windows 10.
2. Passive Scanning with Wireshark: Configure IP addresses on Kali Linux, create network traffic, and use Wireshark to analyze it for insights.
3. Active Scanning Using Tools: Use 'db_nmap' in Metasploit to scan active hosts while automatically storing scan results for systematic tracking.
4. Active Scanning with Commands: Run thorough scans on the target hosts.

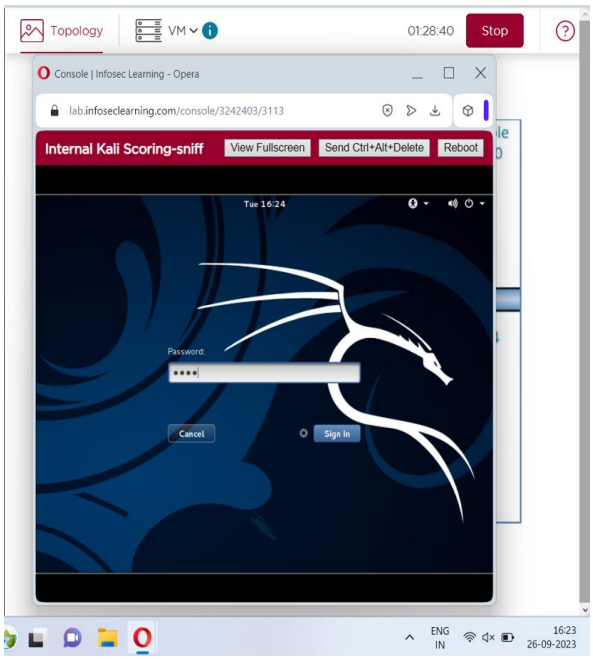
Supporting Evidence

Step 1: Log in to the Kali Linux. Enter the credentials.

Username: **root**

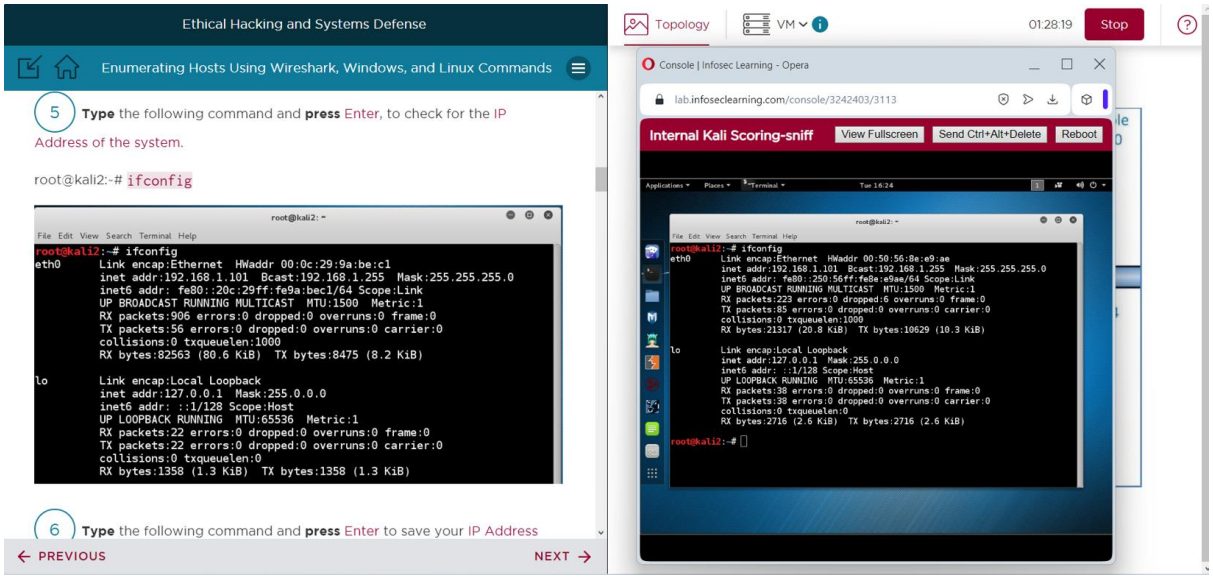
Password: **toor**





Step 2: Use ifconfig command to check the IP address of the system.

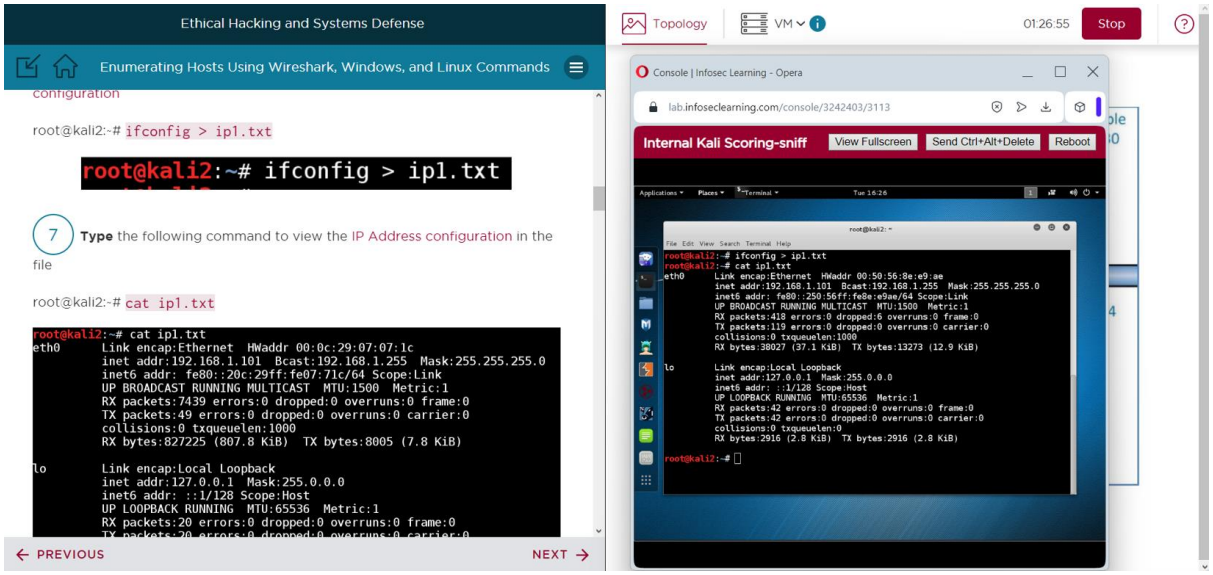
ifconfig



Step 3: Saving the IP address configuration and viewing it by using the following commands:

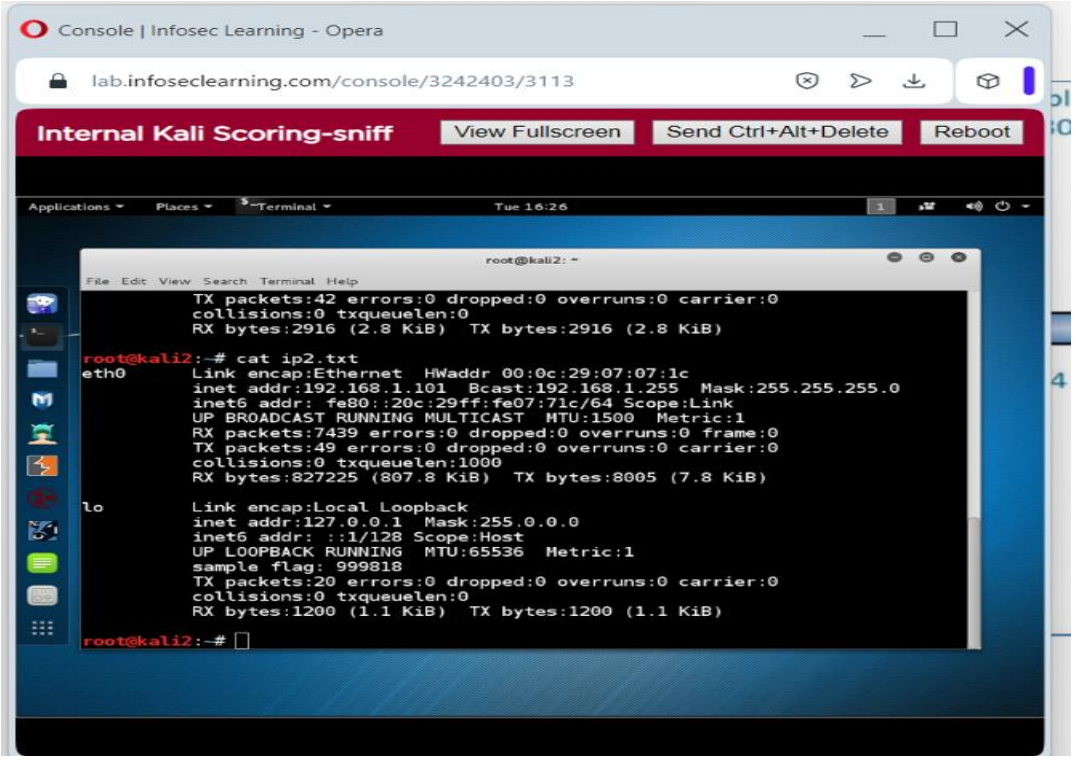
ifconfig > ip1.txt

cat ip1.txt

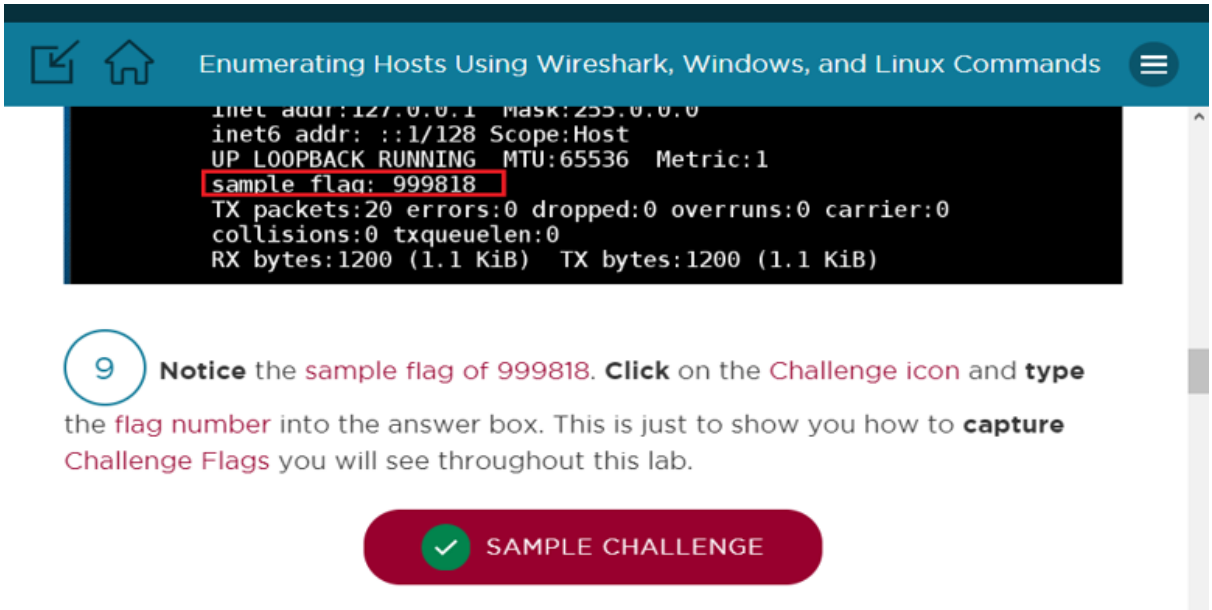


Step 4: View the IP address configuration of ip2.txt.

cat ip2.txt



Step 5: Complete the sample challenge by entering the flag details.



Step 6: We will make sure that the system doesn't have an IP address.

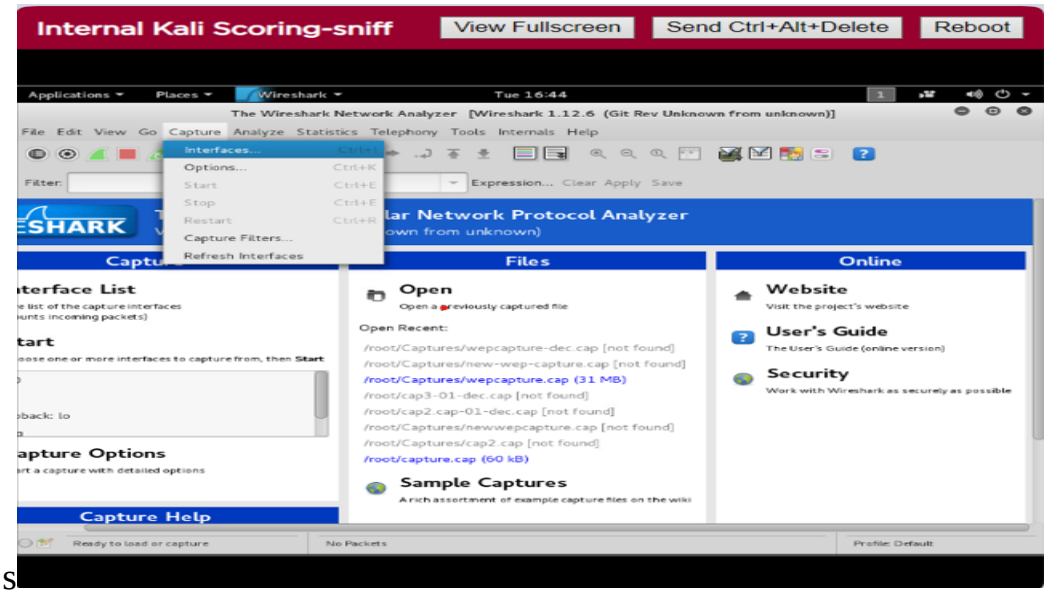
ifconfig eth0 0.0.0.0 up

Step 7: Verifying that no IPv4 address is listed for eth0.

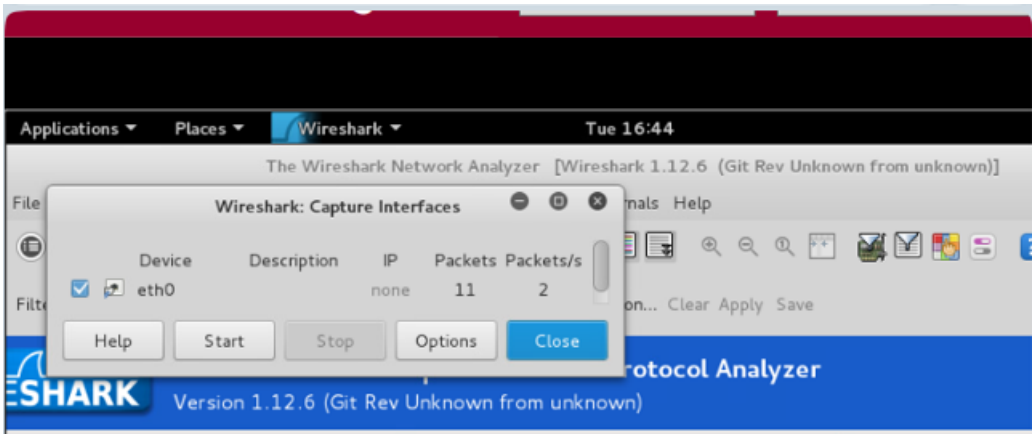
ifconfig

Step 8: Open Wireshark and capture the eth0 data by clicking the start button.

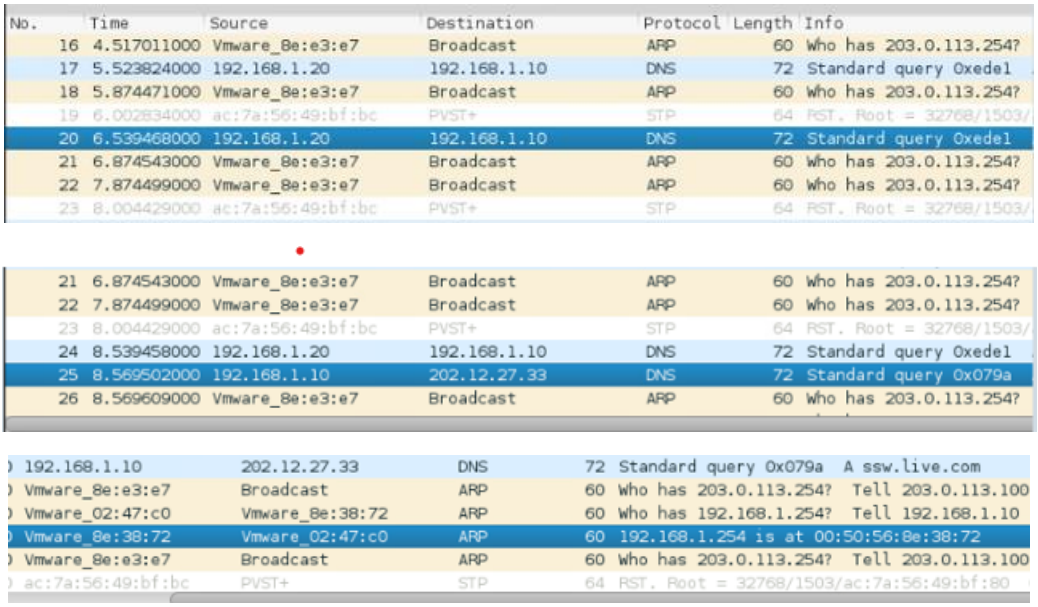
Wireshark>Click OK>Capture>Choose Interfaces>select eth0>start



s



Step 9: Capture the packets which consists of IP addresses 192.168.1.10, 192.168.1.20, and 192.168.1.254 from the traffic.

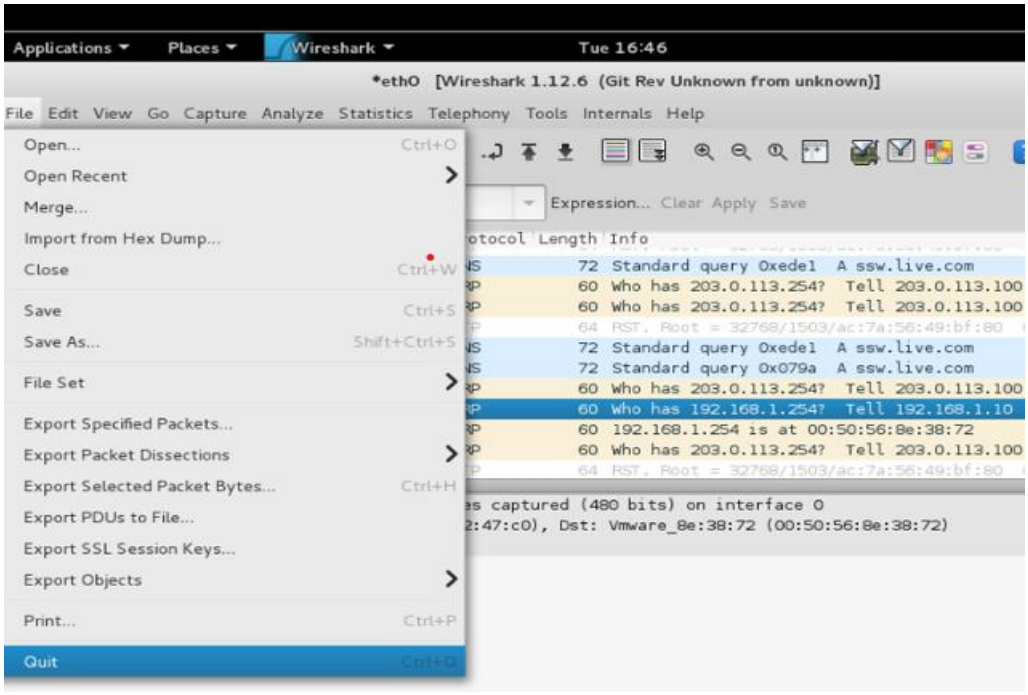


No.	Time	Source	Destination	Protocol	Length	Info
16	4.517011000	Vmware_8e:e3:e7	Broadcast	ARP	60	Who has 203.0.113.254?
17	5.523824000	192.168.1.20	192.168.1.10	DNS	72	Standard query 0xede1
18	5.874471000	Vmware_8e:e3:e7	Broadcast	ARP	60	Who has 203.0.113.254?
19	6.002834000	ac:7a:56:49:bf:bc	PVST+	STP	64	RST. Root = 32768/1503/
20	6.539468000	192.168.1.20	192.168.1.10	DNS	72	Standard query 0xede1
21	6.874543000	Vmware_8e:e3:e7	Broadcast	ARP	60	Who has 203.0.113.254?
22	7.874499000	Vmware_8e:e3:e7	Broadcast	ARP	60	Who has 203.0.113.254?
23	8.004429000	ac:7a:56:49:bf:bc	PVST+	STP	64	RST. Root = 32768/1503/

21	6.874543000	Vmware_8e:e3:e7	Broadcast	ARP	60	Who has 203.0.113.254?
22	7.874499000	Vmware_8e:e3:e7	Broadcast	ARP	60	Who has 203.0.113.254?
23	8.004429000	ac:7a:56:49:bf:bc	PVST+	STP	64	RST. Root = 32768/1503/
24	8.539458000	192.168.1.20	192.168.1.10	DNS	72	Standard query 0xede1
25	8.569502000	192.168.1.10	202.12.27.33	DNS	72	Standard query 0x079a
26	8.569609000	Vmware_8e:e3:e7	Broadcast	ARP	60	Who has 203.0.113.254?

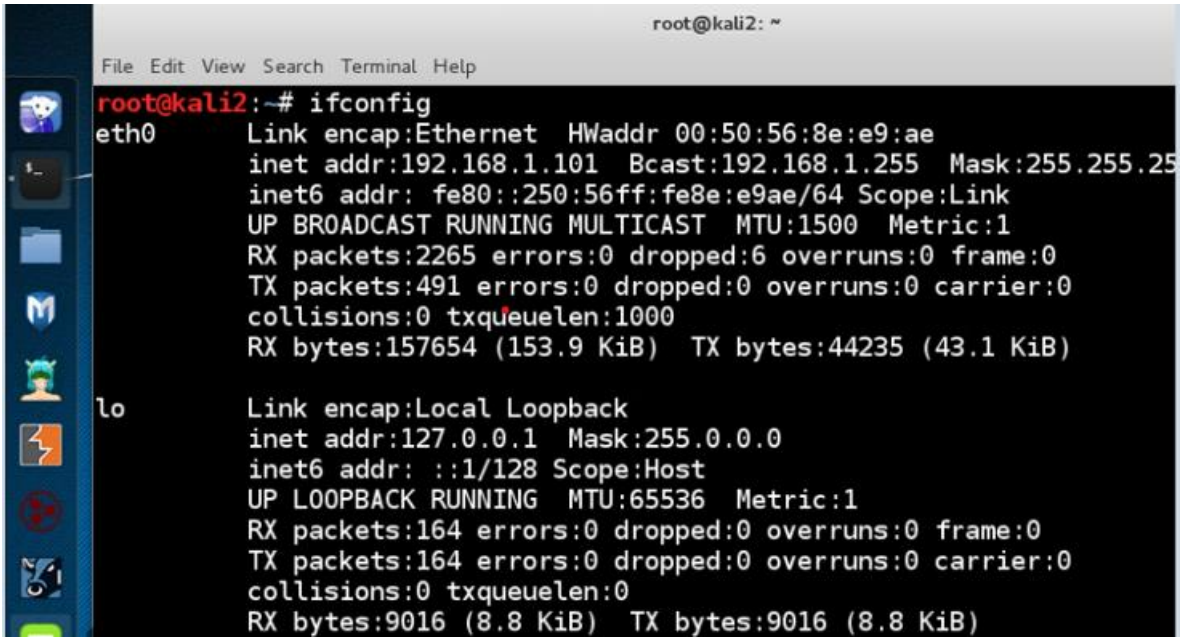
192.168.1.10	202.12.27.33	DNS	72	Standard query 0x079a	A ssw.live.com
Vmware_8e:e3:e7	Broadcast	ARP	60	Who has 203.0.113.254?	Tell 203.0.113.100
Vmware_02:47:c0	Vmware_8e:38:72	ARP	60	Who has 192.168.1.254?	Tell 192.168.1.10
Vmware_8e:38:72	Vmware_02:47:c0	ARP	60	192.168.1.254 is at 00:50:56:8e:38:72	
Vmware_8e:e3:e7	Broadcast	ARP	60	Who has 203.0.113.254?	Tell 203.0.113.100
ac:7a:56:49:bf:bc	PVST+	STP	64	RST. Root = 32768/1503/ac:7a:56:49:bf:80	

Step 10: Stop Wireshark and quit.



Step 11: Checking the IP address of the system.

ifconfig



Step 12: Setting the IP address and subnet mask.

ifconfig eth0 192.168.1.101 netmask 255.255.255.0

Step 13: Setting the gateway.

route add default gw 192.168.1.254

```
root@kali2:~# ifconfig eth0 192.168.1.101 netmask 255.255.255.0
root@kali2:~# route add default gw 192.168.1.254
SIOCADDRT: File exists
```

Step 14: We will backup the current resolv.conf file.

cp /etc/resolv.conf /etc/resolv.conf.backup1

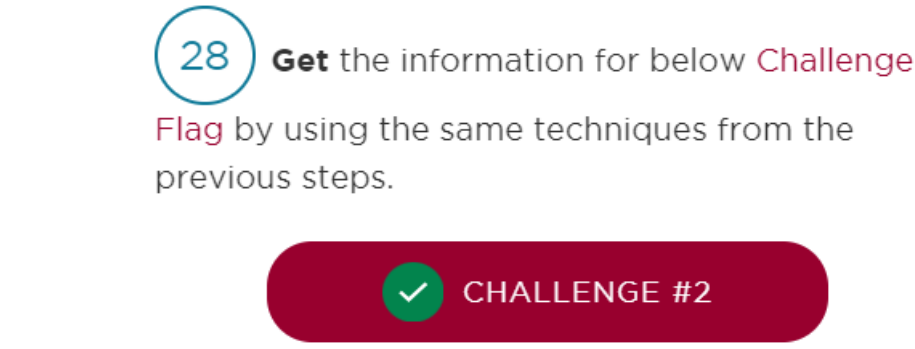
Step 15: Viewing the IP address configuration of the file.

cat /etc/resolv.conf.backup1

```
root@kali2:~# cp /etc/resolv.conf /etc/resolv.conf.backup1
root@kali2:~# cat /etc/resolv.conf.backup1
# Generated by NetworkManager
search localdomain
nameserver 172.16.200.2
```

Step 16: We will solve the challenge by repeating the two steps below

```
root@kali2:~# cat /etc/resolv.conf.backup2
# Generated by NetworkManager
search localdomain
nameserver 172.16.200.2
flag:334451
```



Step 17: Setting the DNS server and viewing the contents of the resolv file.

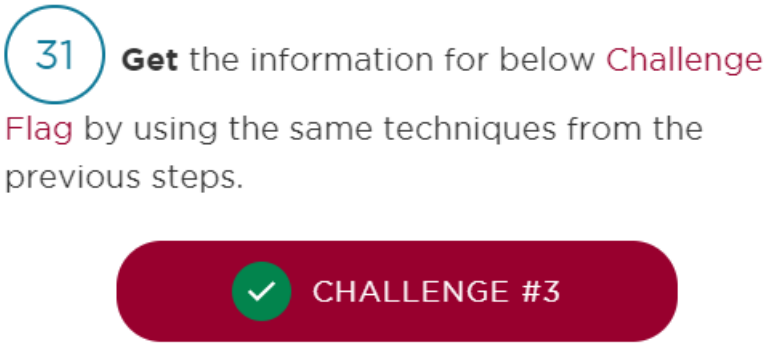
echo nameserver 192.168.1.10 > /etc/resolv.conf

cat /etc/resolv.conf

```
root@kali2:~# echo nameserver 192.168.1.10 > /etc/resolv.conf
root@kali2:~# cat /etc/resolv.conf
nameserver 192.168.1.10
```

Step 18: Solving the challenge by repeating the step 17.

```
root@kali2:~# echo nameserver 192.168.1.10 > /etc/resolv.conf
root@kali2:~# cat /etc/resolv.conf
nameserver 192.168.1.10
root@kali2:~# cat /etc/resolv.flag
flag:888999
```



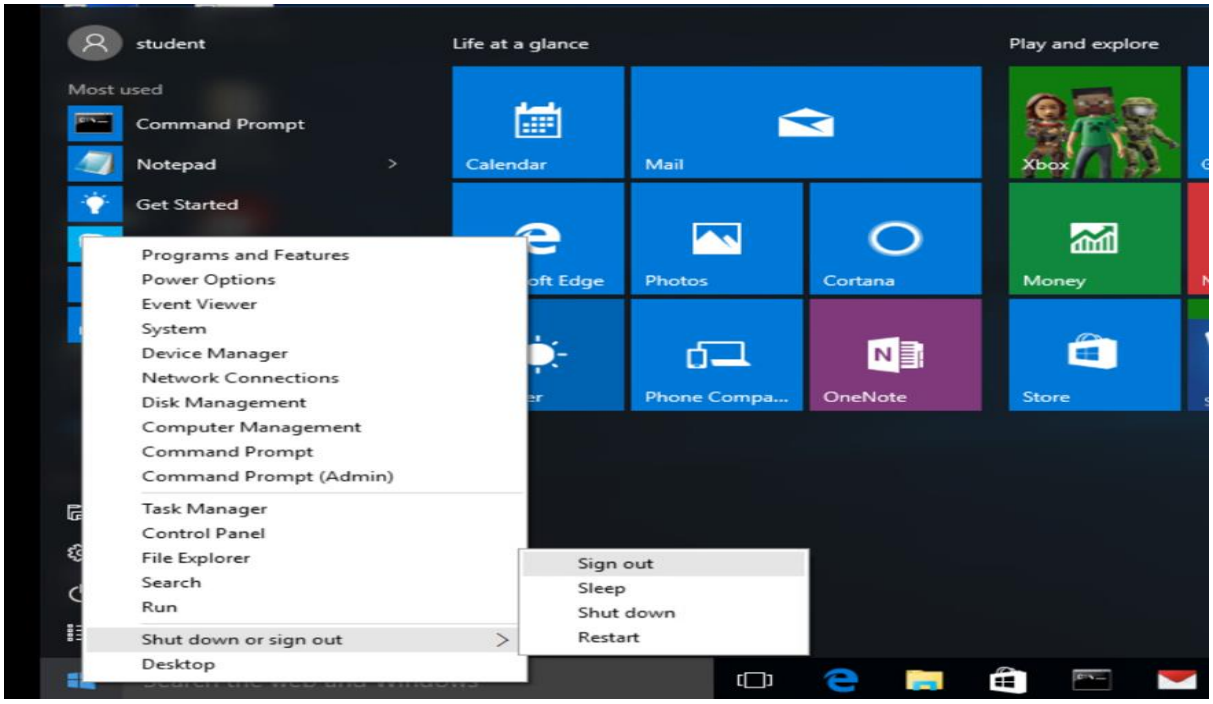
Step 19: Verifying that correct IPv4 address is listed for eth0.

ifconfig

```
root@kali2:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:8e:e9:ae
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe8e:e9ae/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2638 errors:0 dropped:6 overruns:0 frame:0
          TX packets:630 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:181984 (177.7 KiB)  TX bytes:55743 (54.4 KiB)

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:65536  Metric:1
          RX packets:186 errors:0 dropped:0 overruns:0 frame:0
          TX packets:186 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:10116 (9.8 KiB)  TX bytes:10116 (9.8 KiB)
```

Step 20: Click on the Desktop Windows key and select sign out.



Step 21: Click on the screen saver displaying the time.

>Select Administrator>Type Password(P@ssw0rd)

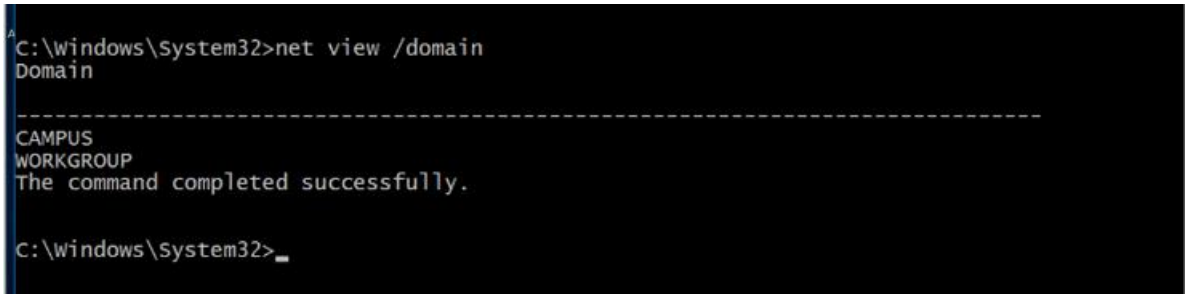
Step 22: Right-click on cmd-shortcut and run it as admin.

Step 23: Enumerating the machines.

>net view

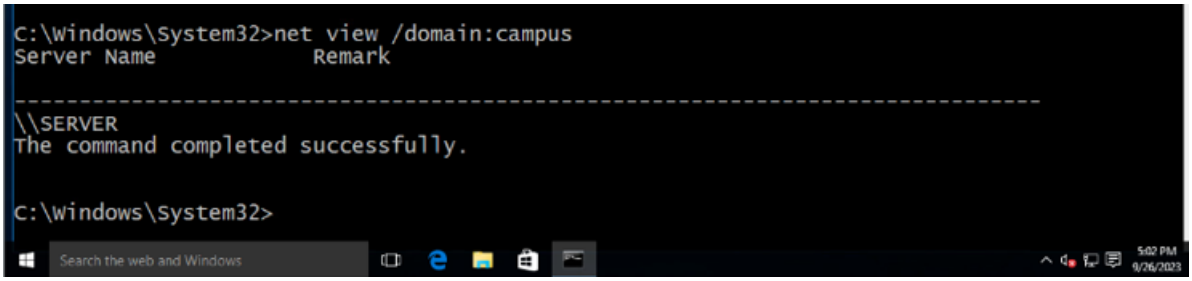
Step 24: Enumerating all the domains.

>net view /domain



Step 25: Enumerating all the domains of campus.

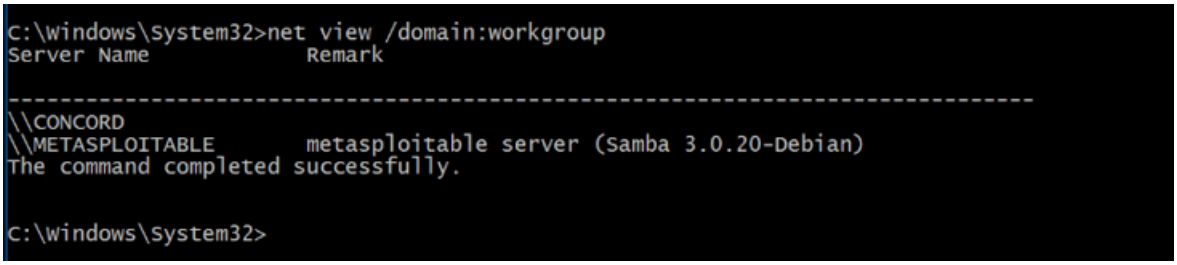
>net view /domain:campus



2

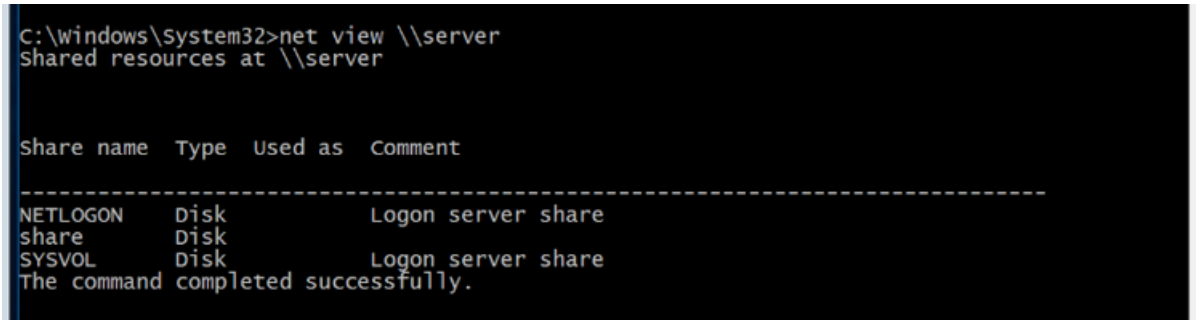
Step 26: Enumerating all the domains of the workgroup.

>net view /domain:workgroup



Step 27: Enumerating the shares on the server.

>net view \\server



Step 28: Enumerating the shares on metasploitable.

>net view \\metasploitable

```
C:\Windows\System32>net view \\metasploitable
Shared resources at \\metasploitable

metasploitable server (Samba 3.0.20-Debian)

Share name     Type  Used as  Comment

-------------------------------------------------------------------------------
administrator  Disk           Home Directories
opt            Disk
tmp            Disk           oh noes!
The command completed successfully.


C:\Windows\System32>
```

Step 29: Solving the challenges and capturing the flags.

```
Administrator: cmd - Shortcut
C:\Windows\System32>net view \\metasploitable
Shared resources at \\metasploitable

metasploitable server (Samba 3.0.20-Debian)

Share name     Type  Used as  Comment

-------------------------------------------------------------------------------
administrator  Disk           Home Directories
opt            Disk
tmp            Disk           oh noes!
The command completed successfully.


C:\Windows\System32>net view \\localhost
Shared resources at \\localhost


Share name  Type  Used as  Comment

-------------------------------------------------------------------------------
flag5       Disk           flag5:571444
flag6       Disk           flag6:333459
share       Disk
The command completed successfully.
```

Step 30: Enumerating the IP and MAC address of the server.

>nbtstat -a server

```
C:\Windows\System32>nbtstat -a server

Ethernet0:
Node IpAddress: [192.168.1.20] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    SERVER          <00>  UNIQUE      Registered
    CAMPUS          <00>  GROUP       Registered
    CAMPUS          <1C>  GROUP       Registered
    SERVER          <20>  UNIQUE      Registered
    CAMPUS          <1E>  GROUP       Registered
    CAMPUS          <1B>  UNIQUE      Registered
    CAMPUS          <1D>  UNIQUE      Registered
    ☺☻__MSBROWSE__☻<01>  GROUP       Registered

    MAC Address = 00-50-56-02-47-C0
```

Step 31: Enumerating the IP and MAC address of metasploitable.

>nbtstat -a METASPLOITABLE

```
C:\Windows\System32>nbtstat -a METASPLOITABLE

Ethernet0:
Node IpAddress: [192.168.1.20] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    METASPLOITABLE <00>  UNIQUE      Registered
    METASPLOITABLE <03>  UNIQUE      Registered
    METASPLOITABLE <20>  UNIQUE      Registered
    ☺☻__MSBROWSE__☻<01>  GROUP       Registered
    WORKGROUP       <00>  GROUP       Registered
    WORKGROUP       <1D>  UNIQUE      Registered
    WORKGROUP       <1E>  GROUP       Registered

    MAC Address = 00-00-00-00-00-00
```

Step 32: Open the terminal and start the postgresql service.

service postgresql start

```
root@kali2: ~
File  Edit  View  Search  Terminal  Help
root@kali2:~# service postgresql service
Usage: /etc/init.d/postgresql {start|stop|restart|reload|force-reload|status
ersion ..]
root@kali2:~#
```

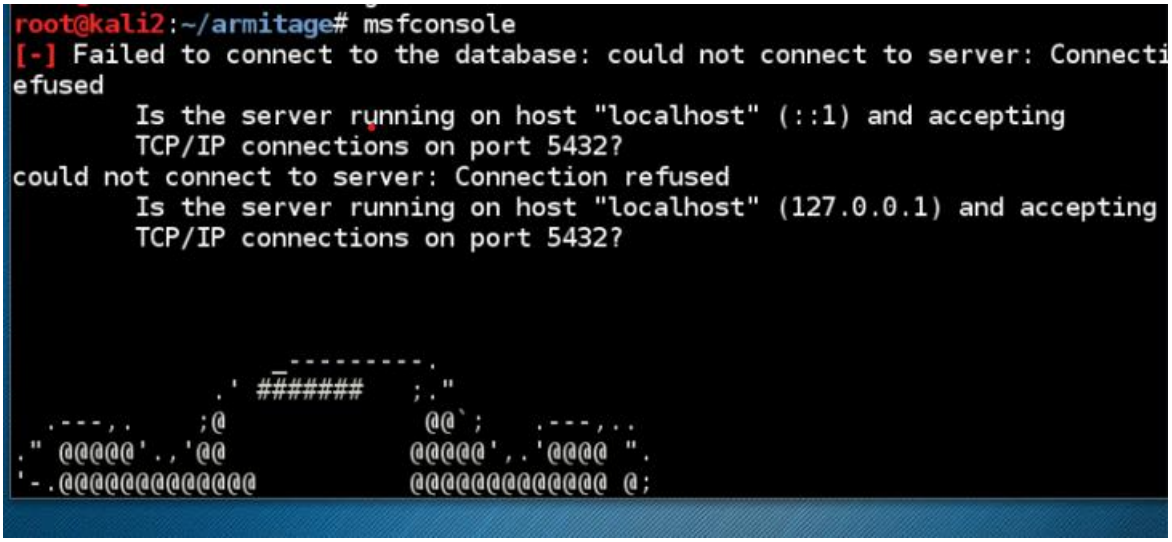
Step 33: Switch to the Armitage directory and start.

cd armitage

```
root@kali2:~# cd armitage
root@kali2:~/armitage#
```

Step 34: Start Metasploit.

#msfconsole



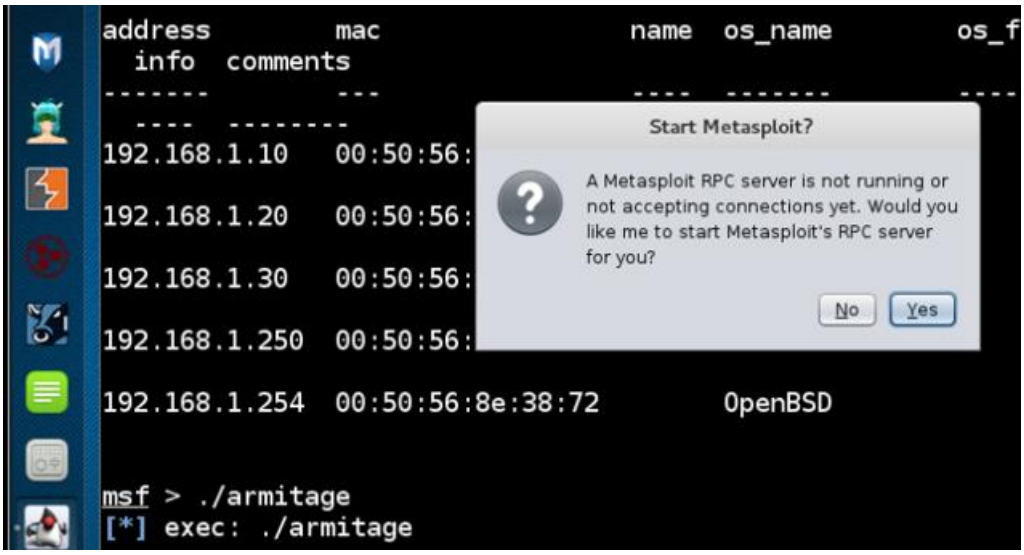
Step 35: Scan the hosts.

>db_nmap -T4 -A -v 192.168.1.*

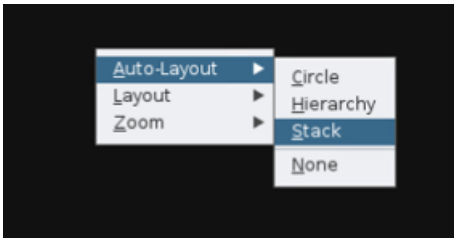
Step 36: Viewing all the discovered hosts.

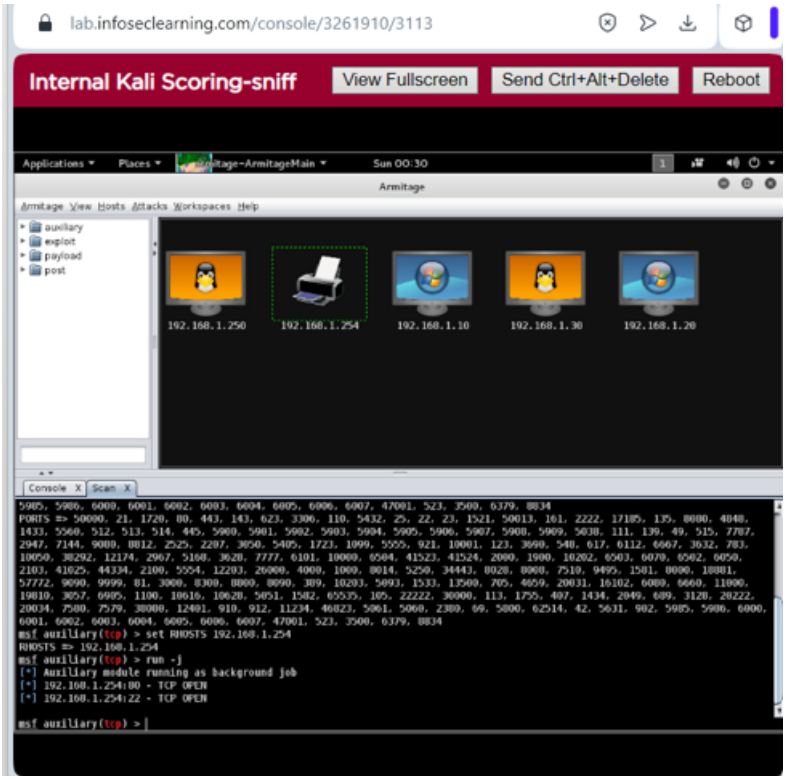
>hosts

Step 37: Start Armitage>Click to connect>Click yes



Step 38: Right-click on the upper pane>Select Auto-layout>Click Stack>Proceed.





Conclusion & Wrap-up

- In conclusion, this lab offered insightful knowledge in the field of system enumeration through the use of command-line and graphical tools in both Linux and Windows platforms. Tools like 'nmap,' 'net,' and 'nbtstat,' which represent active scanning techniques, were used to locate discoverable network resources, while Wireshark and Armitage, which represent passive scanning techniques, operated undetectedly.
- The crucial relevance of identifying and protecting items found throughout the enumeration process was learned through this exercise. Potential vulnerabilities, open ports, and service information were discovered by aggressively probing the network; if these issues were not fixed, attackers might use them to their advantage. Passive scanning also made it clear how

important it is to keep an eye on network traffic for suspicious activity, underscoring the necessity for strong security measures.

- Proactive network security is essential, with a focus on the need to protect and fix found vulnerabilities to avoid threats and maintain the integrity and confidentiality of crucial assets.