

Lab 3: Enumerating Hosts Using Wireshark, Windows, and Linux Commands

Objective:

1. Passive Scanning
2. Active Scanning with Commands
3. Active Scanning with tools

Takeaways:

1. Wireshark is a network protocol analyzer used for capturing and analyzing network traffic in real-time. It allows users to inspect data packets, understand network behavior, troubleshoot issues, and analyze security vulnerabilities.
2. The "route" command in computing is used to view and manipulate the IP routing table in an operating system. It allows users to display, add, delete, or modify entries in the routing table, which determines how network traffic is directed and forwarded between different networks or hosts.
3. The "net view" command is a Windows command-line utility used to display a list of available resources or shared folders on a network. It shows the names of computers or devices that are currently visible or accessible within the local network or domain.
4. 'nbtstat' is a Windows command-line utility used for troubleshooting and displaying NetBIOS over TCP/IP information, including NetBIOS name resolution statistics and cache on a local network.

5. `db_nmap` is a command used to conduct network scans using Nmap and store the scan results directly into the Metasploit database for further analysis, exploitation, or vulnerability assessment.

Challenges:

The screenshot displays a web browser window with two tabs. The active tab is titled "Ethical Hacking and Systems Defense" and shows a challenge page. The page content includes a terminal output snippet: `collisions:0 txqueuelen:0
RX bytes:1200 (1.1 KiB) TX bytes:1200 (1.1 KiB)`. Below this, a numbered instruction (9) states: "Notice the sample flag of 999018. Click on the Challenge icon and type the flag number into the answer box. This is just to show you how to capture Challenge Flags you will see throughout this lab." There are two buttons: "SAMPLE CHALLENGE" and "CHALLENGE #1". Below the buttons, a text box contains the number "123457". At the bottom of the challenge section are "Submit" and "Skip" buttons. The browser's address bar shows the URL: <https://lab.infoseclearning.com/course/WICWVYQVN/lab/RGYPGUWBCI#>. The second tab is titled "Console | Infosec Learning - Personal - Microsoft Edge" and shows a terminal window with the title "Internal Kali Scoring-sniff". The terminal output includes network statistics for two interfaces: `enp0s3` and `lo`. The `enp0s3` output shows: `TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1200 (1.1 KiB) TX bytes:1200 (1.1 KiB)`. The `lo` output shows: `Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr:::1::220 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
Flag:123457
TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:1200 (1.1 KiB) TX bytes:1200 (1.1 KiB)`. The terminal prompt is `root@kali:~#`. The browser's address bar for the second tab shows the URL: <https://lab.infoseclearning.com/console/3572181/3113>. The browser's taskbar at the bottom shows the time as 2:04 PM on 12/20/2023.

st-peters-blackboard - Search x Week 2-3- Scanning and 4- Enu... Enumerating Hosts Using Wiresh... ChatGPT

https://fab.infoseclearning.com/course/WICWEVYQVN/lab/RGYPGUWBCI

McAfee Security Dell Room GB 533-Fail... HomeworkKittyNet... untitled report Introduction to Cry...

Ethical Hacking and Systems Defense

Enumerating Hosts Using Wireshark, Windows, and Linux Commands

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

28 Get the information for below Challenge Flag by using the same techniques from the previous steps.

→ CHALLENGE #2

Get flag from the /etc/resolv.conf.backup2 file using the same technique.

334451

Submit Skip

29 Type the following command and press Enter, to set the DNS server.

← PREVIOUS NEXT →

55°F Light rain 2:15 PM 12/20/2023

Console | Infosec Learning - Personal - Microsoft Edge

https://fab.infoseclearning.com/console/3572181/3113

Internal Kali Scoring-sniff View Fullscreen Send Ctrl+Alt+Delete Reboot

```
root@kali2:~# ifconfig eth0 192.168.1.101 netmask 255.255.255.0
root@kali2:~# route add default gw 192.168.1.254
root@kali2:~# cp /etc/resolv.conf /etc/resolv.conf.backup1
root@kali2:~# cp /etc/resolv.conf /etc/resolv.conf.backup2
root@kali2:~# cat /etc/resolv.conf.backup1
# Generated by NetworkManager
search localdomain
nameserver 172.16.200.2
root@kali2:~# cat /etc/resolv.conf.backup2
# Generated by NetworkManager
search localdomain
nameserver 172.16.200.2
root@kali2:~#
```

st-peters-blackboard - Search x Week 2-3- Scanning and 4- Enu... Enumerating Hosts Using Wiresh... ChatGPT

https://fab.infoseclearning.com/course/WICWEVYQVN/lab/RGYPGUWBCI

McAfee Security Dell Room GB 533-Fail... HomeworkKittyNet... untitled report Introduction to Cry...

Ethical Hacking and Systems Defense

Enumerating Hosts Using Wireshark, Windows, and Linux Commands

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

31 Get the information for below Challenge Flag by using the same techniques from the previous steps.

→ CHALLENGE #3

Use the cat command to view the contents of the /etc/resolv.flag file. Type the Flag number displayed.

888999

Submit Skip

32 Type the following command and press Enter, to verify that the correct IPv4 address is listed for eth0.

```
root@kali2:~# ifconfig
```

← PREVIOUS NEXT →

55°F Light rain 2:36 PM 12/20/2023

Console | Infosec Learning - Personal - Microsoft Edge

https://fab.infoseclearning.com/console/3572296/3113

Internal Kali Scoring-sniff View Fullscreen Send Ctrl+Alt+Delete Reboot

```
root@kali2:~# ifconfig eth0 192.168.1.101 netmask 255.255.255.0
root@kali2:~# route add default gw 192.168.1.254
root@kali2:~# cat /etc/resolv.conf.backup1
# Generated by NetworkManager
search localdomain
nameserver 172.16.200.2
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
root@kali2:~#
```

st-peters-blackboard - Search x Week 2-3- Scanning and 4- Enu x Enumerating Hosts Using Wiresh... ChatGPT

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/RGYPGUWBCJ

McAfee Security Dell Room GB 533-Fail... HomeworklyNet... untitled report Introduction to Cy... Secur

Ethical Hacking and Systems Defense

Enumerating Hosts Using Wireshark, Windows, and Linux Commands

```
metasploitable server (Samba 3.0.20-Debian)

Share name      Type  Used as  Comment
-----
administrator   Disk             Home Directories
opt              Disk             oh noes!
tmp              Disk             oh noes!
The command completed successfully.
```

→ CHALLENGE #4

Use the net view command to view the machine named localhost on the network. Type the Flag5 number displayed.

571444

Submit Skip

→ CHALLENGE #5

NEXT →

55°F Light rain

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3572296/3115

Internal Windows 10 Scoring-1 View Fullscreen Send Ctrl+Alt+Delete Reboot

```
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             oh noes!
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             oh noes!
The command completed successfully.
```

2:45 PM 12/20/2023

st-peters-blackboard - Search x Week 2-3- Scanning and 4- Enu x Enumerating Hosts Using Wiresh... ChatGPT

https://lab.infoseclearning.com/course/WICWEVYQVN/lab/RGYPGUWBCJ

McAfee Security Dell Room GB 533-Fail... HomeworklyNet... untitled report Introduction to Cy... Secur

Ethical Hacking and Systems Defense

Enumerating Hosts Using Wireshark, Windows, and Linux Commands

```
opt              Disk             oh noes!
tmp              Disk             oh noes!
The command completed successfully.
```

✓ CHALLENGE #4

→ CHALLENGE #5

Use the net view command to view the machine named concord on the network. Type the Flag6 number displayed.

333459

Submit Skip

12 Attempt to enumerate the IP and MAC Address of the machine named server. Type the following command, then press Enter.

NEXT →

55°F Light rain

Console | Infosec Learning - Personal - Microsoft Edge

https://lab.infoseclearning.com/console/3572296/3115

Internal Windows 10 Scoring-1 View Fullscreen Send Ctrl+Alt+Delete Reboot

```
metasploitable server (Samba 3.0.20-debian)
Share name      Type  Used as  Comment
-----
administrator   Disk             Home Directories
opt              Disk             oh noes!
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             oh noes!
The command completed successfully.

C:\Windows\system32>
```

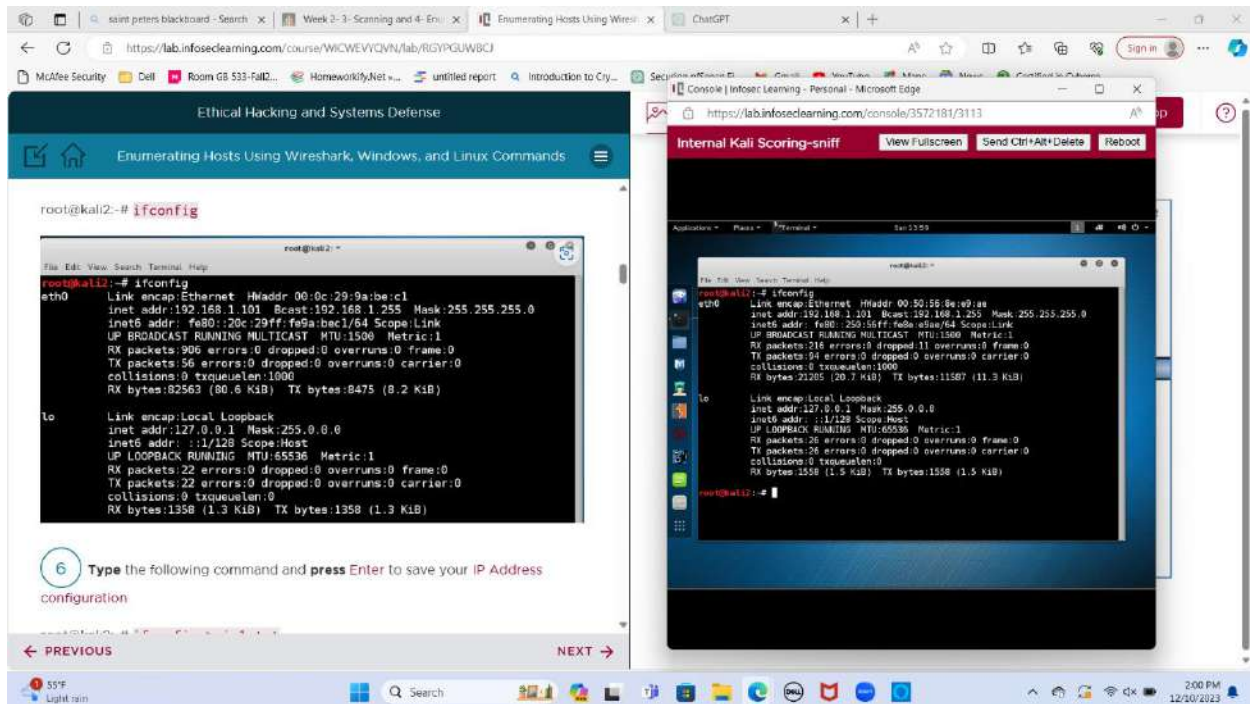
2:46 PM 12/20/2023

The flags are:

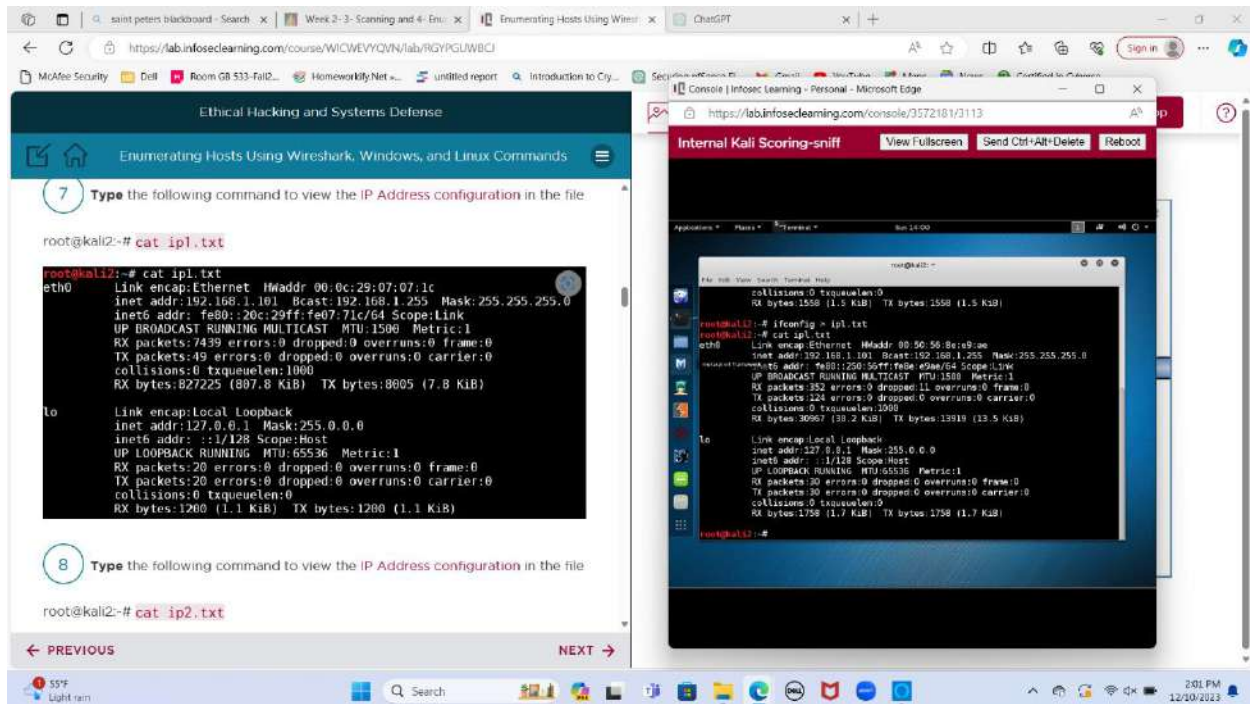
- Flag 1: 999818
- Flag 2: 123457
- Flag 3: 334451
- Flag 4: 888999
- Flag 5: 571444
- Flag 6: 333459

Screenshots:

Ip configuration



Ip address Configuration.



7 Type the following command to view the IP Address configuration in the file

```
root@kali2:~# cat ip1.txt
```

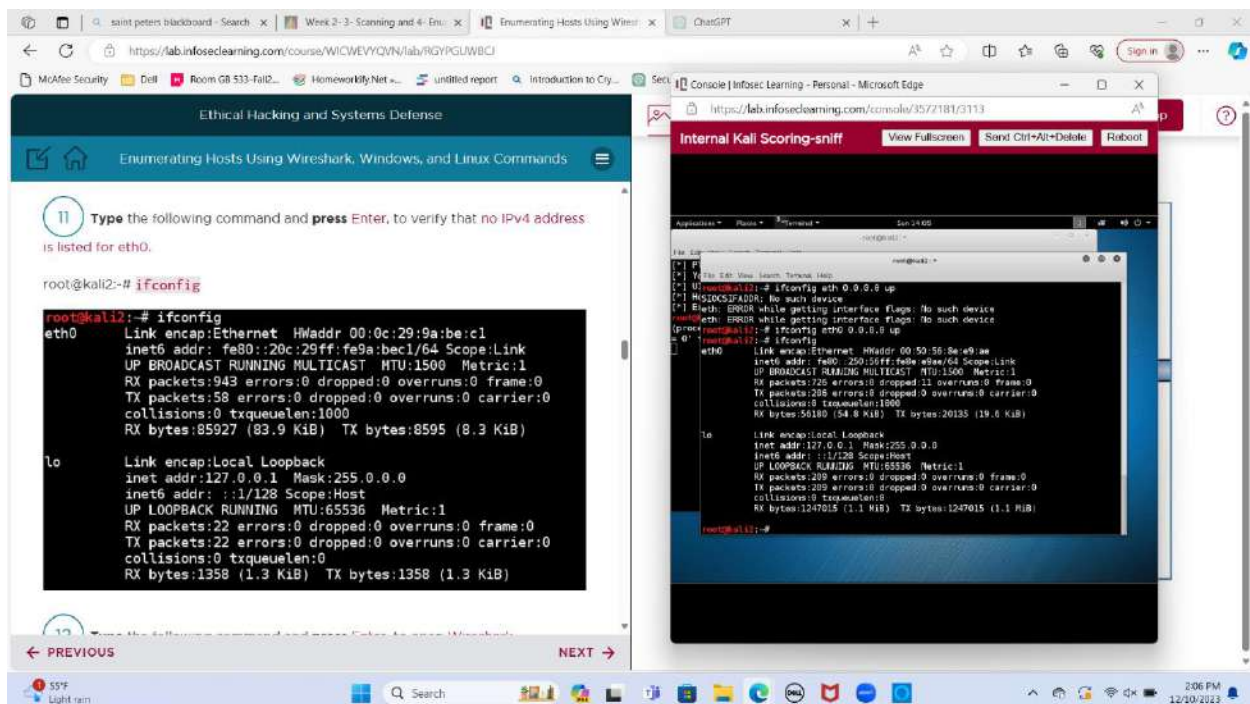
```
root@kali2:~# cat ip1.txt
eth0  Link encap:Ethernet  HWaddr 00:0c:29:07:07:1c
      inet addr: 192.168.1.101  Bcast: 192.168.1.255  Mask: 255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU: 1500  Metric: 1
      RX packets: 7439 errors: 0 dropped: 0 overruns: 0 frame: 0
      TX packets: 49 errors: 0 dropped: 0 overruns: 0 carrier: 0
      collisions: 0 txqueuelen: 1000
      RX bytes: 827225 (807.8 KiB)  TX bytes: 8805 (7.8 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: 20 errors: 0 dropped: 0 overruns: 0 frame: 0
      TX packets: 20 errors: 0 dropped: 0 overruns: 0 carrier: 0
      collisions: 0 txqueuelen: 0
      RX bytes: 1200 (1.1 KiB)  TX bytes: 1200 (1.1 KiB)
```

8 Type the following command to view the IP Address configuration in the file

```
root@kali2:~# cat ip2.txt
```

PREVIOUS NEXT



11 Type the following command and press Enter, to verify that no IPv4 address is listed for eth0.

```
root@kali2:~# ifconfig
```

```
root@kali2:~# ifconfig
eth0  Link encap:Ethernet  HWaddr 00:0c:29:9a:be:c1
      inet6 addr: fe80::20c:29ff:fe9a:bec1/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU: 1500  Metric: 1
      RX packets: 943 errors: 0 dropped: 0 overruns: 0 frame: 0
      TX packets: 58 errors: 0 dropped: 0 overruns: 0 carrier: 0
      collisions: 0 txqueuelen: 1000
      RX bytes: 85927 (83.9 KiB)  TX bytes: 8595 (8.3 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: 22 errors: 0 dropped: 0 overruns: 0 frame: 0
      TX packets: 22 errors: 0 dropped: 0 overruns: 0 carrier: 0
      collisions: 0 txqueuelen: 0
      RX bytes: 1358 (1.3 KiB)  TX bytes: 1358 (1.3 KiB)
```

12 Type the following command and press Enter, to see Wireshark

PREVIOUS NEXT

The image is a composite of two screenshots from a video tutorial. The left screenshot shows the Wireshark 'Capture Interfaces' window. The 'eth0' interface is selected, and the 'Start' button is highlighted. The right screenshot shows a web browser displaying the 'Internal Kali Scoring-sniff' application, which shows a list of captured packets.

[illegible]

Setting IP address, Subnet mask and Gateway

24 Type the following command and **press** Enter, to set the IP Address and Subnet Mask.

```
root@kali2:~# ifconfig eth0 192.168.1.101 netmask 255.255.255.0
```

25 Type the following command and **press** Enter, to set the gateway.

```
root@kali2:~# route add default gw 192.168.1.254
```

26 Type the following command to backup the current resolv.conf file.

```
root@kali2:~# cp /etc/resolv.conf /etc/resolv.conf.backup1
```

Internal Kali Scoring-sniff

```
root@kali2:~# ifconfig eth0 192.168.1.101 netmask 255.255.255.0
root@kali2:~# route add default gw 192.168.1.254
root@kali2:~# cp /etc/resolv.conf /etc/resolv.conf.backup1
cp: cannot stat '/etc/resolv.conf': No such file or directory
root@kali2:~# cat /etc/resolv.conf.backup1
# Generated by NetworkManager
search localdomain
nameserver 172.16.200.2
root@kali2:~#
```

Setting DNS Server

29 Type the following command and **press** Enter, to set the DNS server.

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

30 Type the following command to view the new /etc/resolv.conf file.

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

31 Get the information for below Challenge Flag by using the same techniques from the previous steps.

CHALLENGE #3

Internal Kali Scoring-sniff

```
root@kali2:~# ifconfig eth0 192.168.1.101 netmask 255.255.255.0
root@kali2:~# route add default gw 192.168.1.254
root@kali2:~# cp /etc/resolv.conf /etc/resolv.conf.backup1
cp: cannot stat '/etc/resolv.conf': No such file or directory
root@kali2:~# cat /etc/resolv.conf.backup1
# Generated by NetworkManager
search localdomain
nameserver 172.16.200.2
root@kali2:~# cat /etc/resolv.conf.backup2
# Generated by NetworkManager
search localdomain
nameserver 172.16.200.2
root@kali2:~# echo nameserver 192.168.1.10 > /etc/resolv.conf
root@kali2:~# cat /etc/resolv.conf
nameserver 192.168.1.10
root@kali2:~#
```


Attempt to enumerate machines.

The screenshot shows a web browser window with the URL <https://lab.infoseclearning.com/course/WICWEVYQVN/lab/RGYPLUWBCJ>. The page is titled "Ethical Hacking and Systems Defense" and "Enumerating Hosts Using Wireshark, Windows, and Linux Commands". It contains two numbered steps:

- 6 Attempt to enumerate machines.** Type the following command, then press Enter.
C:\Windows\system32>net view
- 7 Attempt to enumerate all of the domains.** Type the following command, then press Enter.
C:\Windows\system32>net view /domain

The terminal window on the right shows the output of the first command:

```
Microsoft Windows [version 10.0.17134.0]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net view

Server Name                Remark
-----
\\CONCORD
\\METASPLOITABLE metasploitable server (Samba 3.0.20-debian)
The command completed successfully.
```

Attempt to enumerate all the Domains.

The screenshot shows a web browser window with the URL <https://lab.infoseclearning.com/course/WICWEVYQVN/lab/RGYPLUWBCJ>. The page is titled "Ethical Hacking and Systems Defense" and "Enumerating Hosts Using Wireshark, Windows, and Linux Commands". It contains two numbered steps:

- 8 Attempt to enumerate all of the domains.** Type the following command, then press Enter.
C:\Windows\System32>net view /domain:campus
- 9 Attempt to enumerate all of the domains.** Type the following command, then press Enter.
C:\Windows\System32>net view /domain:workgroup

The terminal window on the right shows the output of the first command:

```
Microsoft Windows [version 10.0.17134.0]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\System32>net view /domain:campus

Server Name                Remark
-----
\\SERVER
The command completed successfully.
```

Windows taskbar and browser tabs are visible at the top. The browser address bar shows `https://lab.infoseclearning.com/course/WICWEVYQVN/lab/RGYPGUWBCJ`.

The main content area is titled "Enumerating Hosts Using Wireshark, Windows, and Linux Commands". It contains two numbered steps:

10 Attempt to enumerate the shares on the machine named **server**. **Type** the following command, then **press** Enter.

```
C:\Windows\System32>net view \\server
```

The output of the command is displayed in a terminal window:

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

Share name  Type  Used as  Comment
-----
NETLOGON    Disk   Logon server share
share       Disk   Logon server share
SYSVOL      Disk   Logon server share
The command completed successfully.
```

11 Attempt to enumerate the shares on the machine named **metasploitable**. **Type** the following command, then **press** Enter.

Navigation buttons "PREVIOUS" and "NEXT" are visible at the bottom of the content area.

The right sidebar shows a "Console | Infosec Learning - Personal - Microsoft Edge" window with the URL `https://lab.infoseclearning.com/console/3572296/3115`. It has a red header "Internal Windows 10 Scoring-1" and buttons "View Fullscreen", "Send Ctrl+Alt+Delete", and "Reboot". The console output shows the command `net view /domain:workgroup` being executed successfully, followed by `net view \\server` which also succeeds, displaying the same share list as in step 10.

Windows taskbar at the bottom shows the system clock as 2:42 PM on 12/20/2023.

Windows taskbar and browser tabs are visible at the top. The browser address bar shows `https://lab.infoseclearning.com/course/WICWEVYQVN/lab/RGYPGUWBCJ`.

The main content area is titled "Enumerating Hosts Using Wireshark, Windows, and Linux Commands". It contains one numbered step:

11 Attempt to enumerate the shares on the machine named **metasploitable**. **Type** the following command, then **press** Enter.

```
C:\Windows\System32>net view \\metasploitable
```

The output of the command is displayed in a terminal window:

```
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.
```

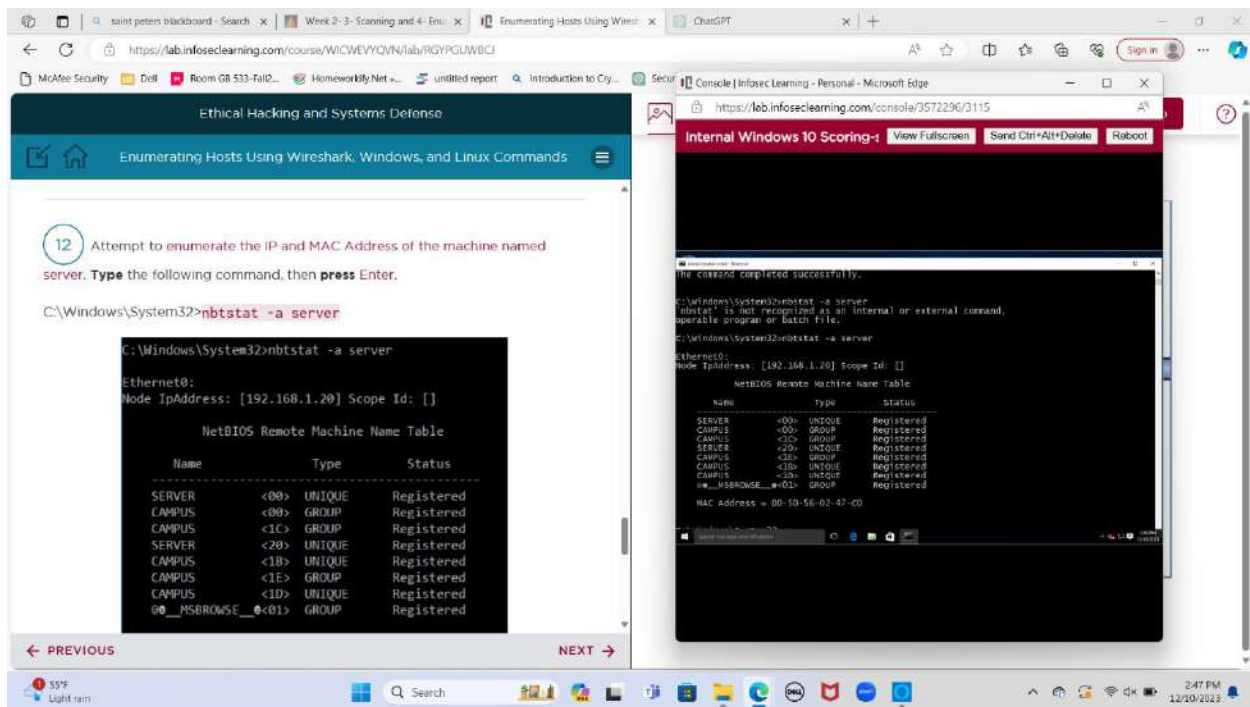
A red button labeled "CHALLENGE #4" is visible below the terminal output.

Navigation buttons "PREVIOUS" and "NEXT" are visible at the bottom of the content area.

The right sidebar shows a "Console | Infosec Learning - Personal - Microsoft Edge" window with the URL `https://lab.infoseclearning.com/console/3572296/3115`. It has a red header "Internal Windows 10 Scoring-1" and buttons "View Fullscreen", "Send Ctrl+Alt+Delete", and "Reboot". The console output shows the command `net view \\metasploitable` being executed successfully, displaying the share list from the previous screenshot.

Windows taskbar at the bottom shows the system clock as 2:44 PM on 12/20/2023.

Attempt to enumerate IP and MAC address.



12 Attempt to enumerate the IP and MAC Address of the machine named **server**. Type the following command, then press Enter.

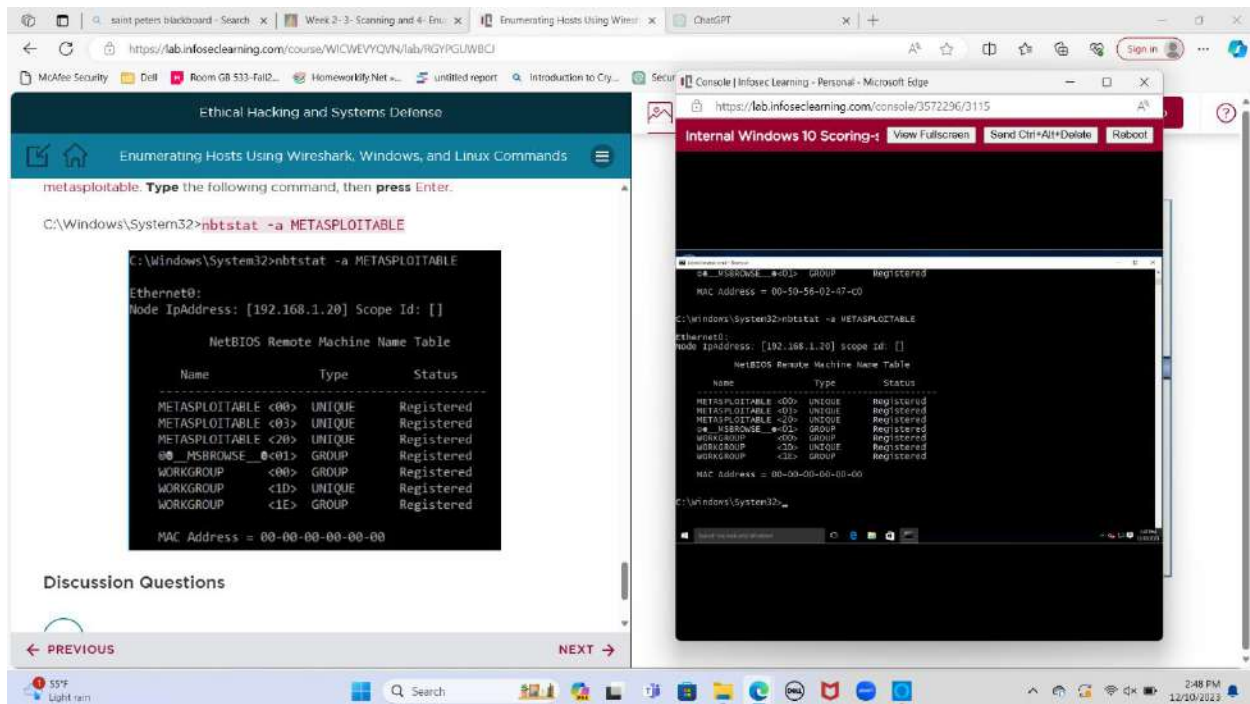
```
C:\Windows\System32>nbtstat -a server
```

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	<18> UNIQUE	Registered
CAMPUS	<1E> GROUP	Registered
CAMPUS	<1D> UNIQUE	Registered
00_MSBROWSE_0<01>	GROUP	Registered

MAC Address = 00-10-56-02-47-C0



metasploitable. Type the following command, then press Enter.

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

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

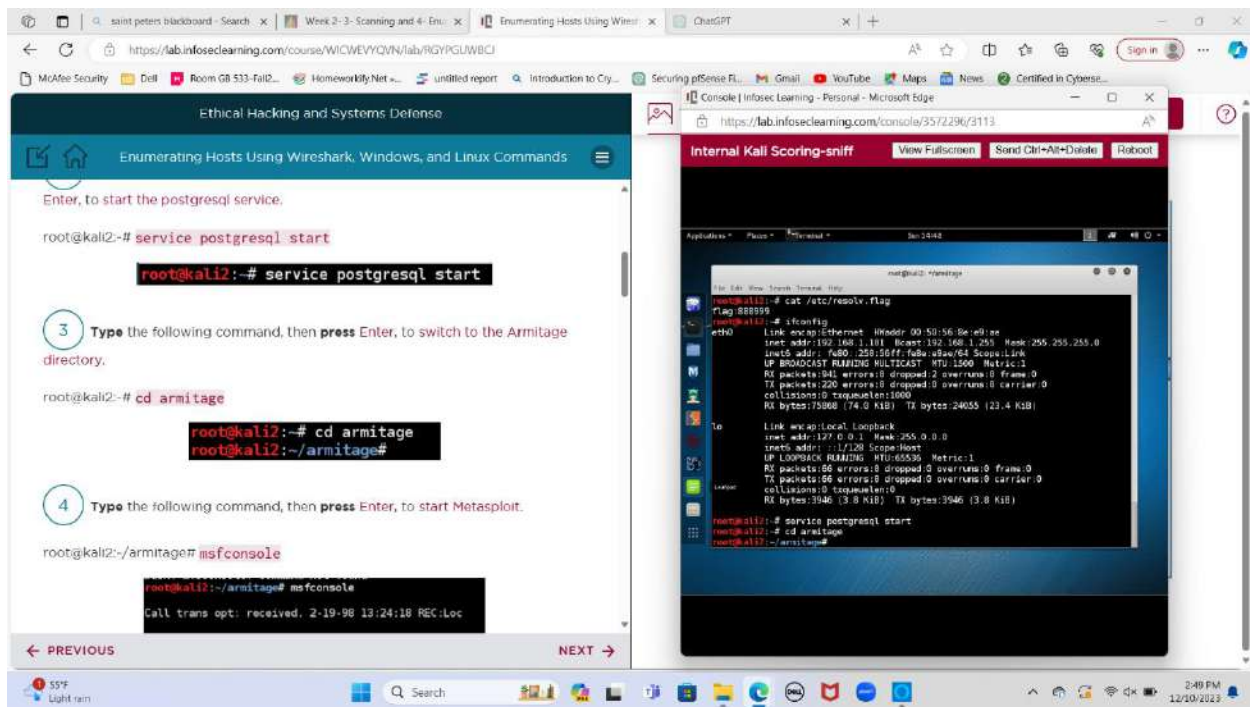
NetBIOS Remote Machine Name Table

Name	Type	Status
METASPLOITABLE	<00> UNIQUE	Registered
METASPLOITABLE	<03> UNIQUE	Registered
METASPLOITABLE	<20> UNIQUE	Registered
00_MSBROWSE_0<01>	GROUP	Registered
WORKGROUP	<00> GROUP	Registered
WORKGROUP	<1D> UNIQUE	Registered
WORKGROUP	<1E> GROUP	Registered

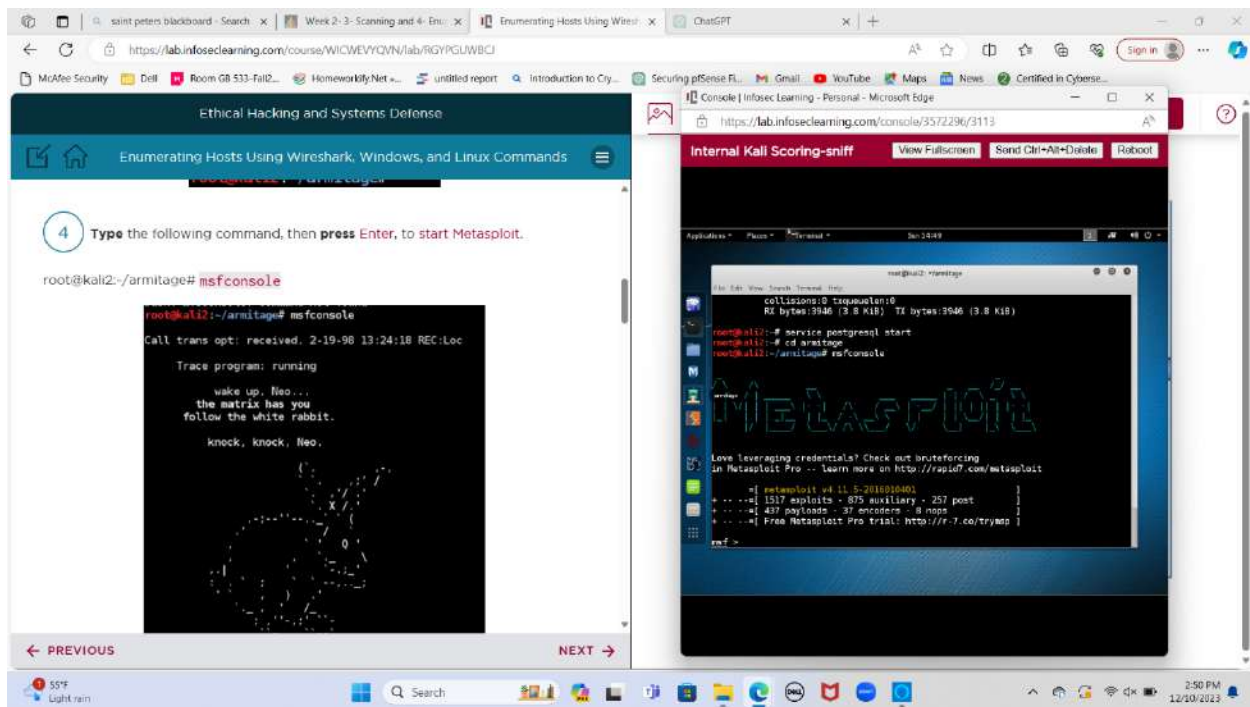
MAC Address = 00-00-00-00-00-00

Discussion Questions

Starting the postgresql service and switching to Armitage directory



Starting Metasploit



Scanning hosts

The screenshot shows a virtual machine environment with two main windows. The left window is titled "Enumerating Hosts Using Wireshark, Windows, and Linux Commands" and contains a terminal window. The terminal window shows the command `msf > db_nmap -T4 -A -v 192.168.1.*` and its output, which includes details about the scan progress and the discovery of 255 IP addresses. The right window is titled "Internal Kali Scoring-sniff" and shows a console window with the same Nmap scan output. The console window also displays the command `msf > db_nmap -T4 -A -v 192.168.1.*` and its output, which includes details about the scan progress and the discovery of 255 IP addresses.

5 Type the following command, then press Enter, to scan hosts.

```
msf > db_nmap -T4 -A -v 192.168.1.*
```

Note: This scan will take about 5 minutes to complete.

6 Notice Nmap: Nmap done will be displayed. The time of the scan and

The screenshot shows a virtual machine environment with two main windows. The left window is titled "Enumerating Hosts Using Wireshark, Windows, and Linux Commands" and contains a terminal window. The terminal window shows the command `msf > db_nmap -T4 -A -v 192.168.1.*` and its output, which includes details about the scan progress and the discovery of 255 IP addresses. The right window is titled "Internal Kali Scoring-sniff" and shows a console window with the same Nmap scan output. The console window also displays the command `msf > db_nmap -T4 -A -v 192.168.1.*` and its output, which includes details about the scan progress and the discovery of 255 IP addresses.

Note: This scan will take about 5 minutes to complete.

6 Notice Nmap: Nmap done will be displayed. The time of the scan and number of hosts up (6 including Kali 2) will also be displayed.

```
msf > db_nmap -T4 -A -v 192.168.1.*
```

7 Type the following command, then press Enter, to view all of the discovered hosts.

```
msf > hosts
```

Viewing all of the discovered hosts

The screenshot shows a virtual machine environment. On the left, a terminal window displays the output of the 'hosts' command in Metasploit. The output lists discovered hosts with their IP addresses, MAC addresses, names, operating systems, and purposes. On the right, a web browser window shows a page titled 'Internal Kali Scoring-sniff' with a 'View Fullscreen' button.

Terminal Output:

```
msf > hosts
```

address	mac	name	os_name	os_flavor	os_sp	purpose
192.168.1.10	00:50:56:9a:37:91		Windows 2008			server
192.168.1.20	00:50:56:9a:d7:a6		Windows Phone			device
192.168.1.30	00:50:56:9a:2b:40		Linux		2.6.X	server
192.168.1.254	00:50:56:9a:42:c8		embedded			device

Web Browser: Internal Kali Scoring-sniff. View Fullscreen. Send Ctrl+Alt+Delete. Reboot.

Starting Armitage

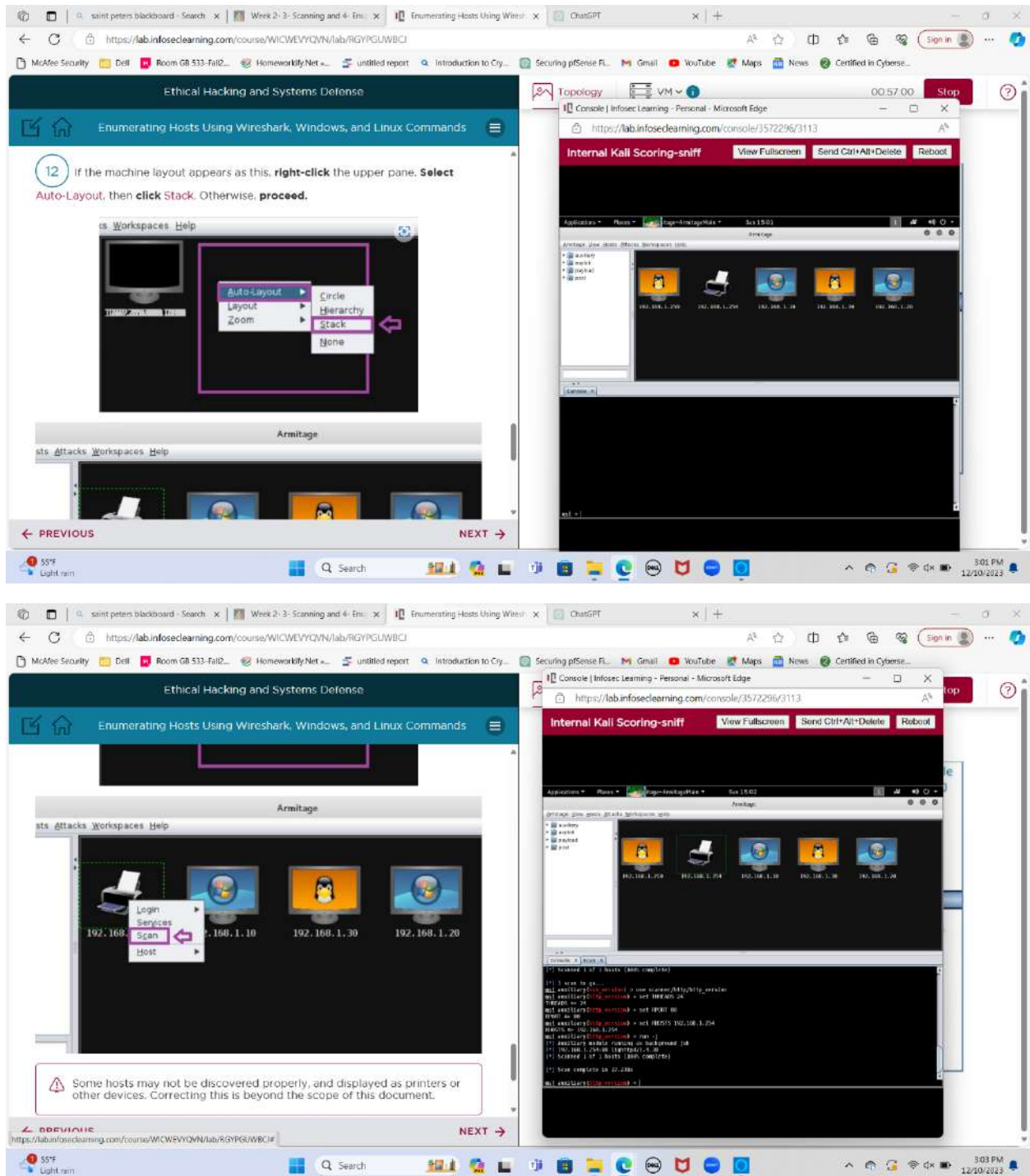
The screenshot shows a virtual machine environment. On the left, a terminal window displays the output of the 'armitage' command in Metasploit. The output shows the command being executed and the resulting output. On the right, a web browser window shows a page titled 'Internal Kali Scoring-sniff' with a 'View Fullscreen' button.

Terminal Output:

```
msf > ./armitage
```

Web Browser: Internal Kali Scoring-sniff. View Fullscreen. Send Ctrl+Alt+Delete. Reboot.

Machine Layout



This is the last screen before the end of this lab.