

CIT 485 ADVANCED CYBERSECURITY-

Lab2: Enumeration tools

The purpose of this lab is:

After completing this lab, you will have further knowledge of:

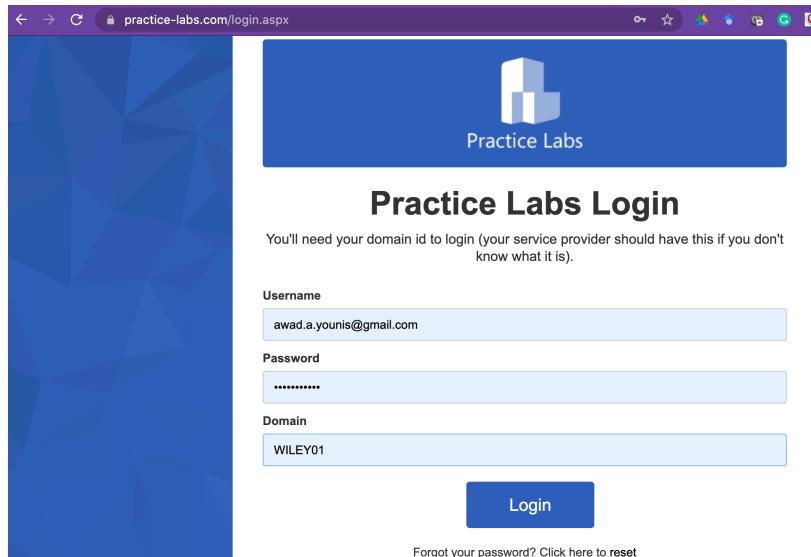
- Use Nmap
- Use the Hping Command
- Understand Active vs. Passive Enumeration
- Use the Responder

LAB INSTRUCTIONS:

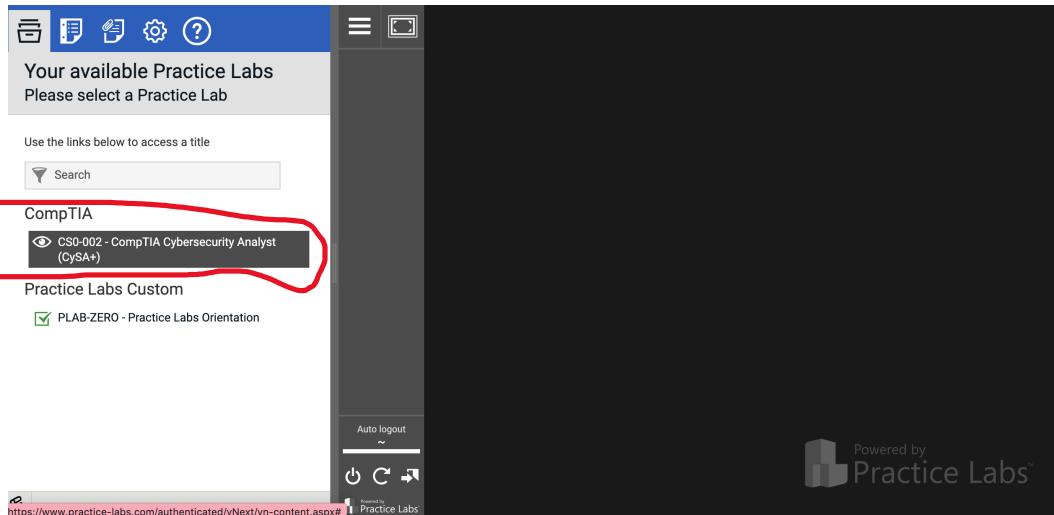
We assume you have completed lab0 and have created and activated your practice labs account. If you have not done that yet, please refer to lab0 instructions in Canvas, Week1, Lab0 section.

Lab2: Enumeration tools

- Enter your credentials and the domain name at: www.practice-labs.com/login.aspx



- On the “your available practice labs”, select CS0-002- CompTIA Cybersecurity Analyst



- From the lab guide, select Enumeration

The screenshot shows a modal dialog titled "Select your Lab Guide". The left side shows a list of lab guides for "Interconnecting Cisco Networking Devices Part 1": "Configure and verify initial switch configuration", "Configuring VLAN and Trunks", "Configure and verify initial router configurations", "Configure and verify routing configurations for static and default routes", and "Configure and verify interVLAN routing using a router on a stick". The "Configure and verify initial switch configuration" item has a blue circle with the number 1 above it. The right side of the dialog contains descriptive text about the lab guides and their objectives. At the bottom, there are checkboxes for "Don't show again." and "Close". A "Powered by Practice Labs" logo is at the bottom right.

- When the lab module's exercise opens, click Start

The screenshot shows a modal dialog titled "Navigating to different Exercises". It displays a list of exercises for "Configure and verify initial switch configuration": "Introduction", "Lab Topology", "Exercise 1 - Enumeration", "Exercise 2 - Leveraging the Gathered Information", and "Review". The "Exercise 1 - Enumeration" item has a blue circle with the number 1 above it. The right side of the dialog contains notes about selecting exercises and linear ordering. At the bottom, there are checkboxes for "Don't show again." and "Close". A "Powered by Practice Labs" logo is at the bottom right.

- Follow instruction and make sure you understand and go through all the provided information.

Powering on the devices

Step 1

To power devices on there are two options available. Either click the power on all icon, which will start all off devices. Or you can individually power on devices by hovering over the device icon and selecting power on.

Step 2

The devices are now powering on, please understand these are real devices and may take up to 5 minutes to connect. The device icon will reflect its progress as it loads.

Step 3

Once the device has powered on a console will appear. all

LAB SUBMISSION

Please make sure to do all the exercises.

1) Active Reconnaissance

- Place the output screenshot of the following command here: **(if you get the message the host is down then start that host/vm up)**
nmap 192.168.0.1

The screenshot shows a Kali Linux desktop environment with several terminal windows open. The main terminal window is titled 'root@PLABKALLI01: ~' and displays the output of an Nmap scan. The command run was 'nmap 192.168.0.1'. The output shows the host is up and various open ports, including domain, kerberos-sec, msrpc, netbios-ssn, ldap, microsoft-ds, kpasswd5, http-rpc-epmap, ldapssl, globalcatLDAP, globalcatLDAPssl, and ms-wbt-server. The MAC address of the host is listed as 00:15:5D:CC:D5:02 (Microsoft). The scan completed in 17.31 seconds.

```
File Edit View Search Terminal Help
root@PLABKALLI01:~# nmap 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-18 23:30 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0010s latency).
Not shown: 988 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
MAC Address: 00:15:5D:CC:D5:02 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 17.31 seconds
root@PLABKALLI01:~#
```

nmap 192.168.0.0/24,

The screenshot shows a terminal window titled "root@PLABKALLI01:~". The window displays the output of an Nmap scan. The first section shows the scan report for host 192.168.0.7, which is up with 0 latency. It lists open ports 80/tcp (http), 443/tcp (https), and 514/tcp (shell). The MAC address is 00:15:5D:CC:D5:06 (Microsoft). The second section shows the scan report for host PLABKALLI01 (192.168.0.3), which is also up with 0 latency. It lists open ports 22/tcp (ssh), 80/tcp (http), 443/tcp (https), and 514/tcp (shell). The MAC address is 00:15:5D:CC:D5:06 (Microsoft). The final message indicates that the scan completed in 28.08 seconds, scanning 256 IP addresses across 7 hosts.

```
File Edit View Search Terminal Help
80/tcp open http
443/tcp open https
514/tcp open shell
MAC Address: 00:15:5D:CC:D5:06 (Microsoft)

Nmap scan report for 192.168.0.7
Host is up (0.0014s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
514/tcp   open  shell
MAC Address: 00:15:5D:CC:D5:06 (Microsoft)

Nmap scan report for PLABKALLI01 (192.168.0.3)
Host is up (0.000015s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind

Nmap done: 256 IP addresses (7 hosts up) scanned in 28.08 seconds
root@PLABKALLI01:~#
```

nmap 192.168.0.1-10

The screenshot shows a Kali Linux desktop environment with several virtual machines listed in the top bar: PLABDC01, PLABDM01, PLABKALI01, PLABWIN10, and PLABALMA. The active terminal window is titled 'root@PLABKALLI01: ~'. The terminal displays the following Nmap scan output:

```
File Edit View Search Terminal Help
80/tcp open http
443/tcp open https
514/tcp open shell
MAC Address: 00:15:5D:CC:D5:06 (Microsoft)

Nmap scan report for 192.168.0.7
Host is up (0.0014s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
514/tcp   open  shell
MAC Address: 00:15:5D:CC:D5:06 (Microsoft)

Nmap scan report for PLABKALLI01 (192.168.0.3)
Host is up (0.000015s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind

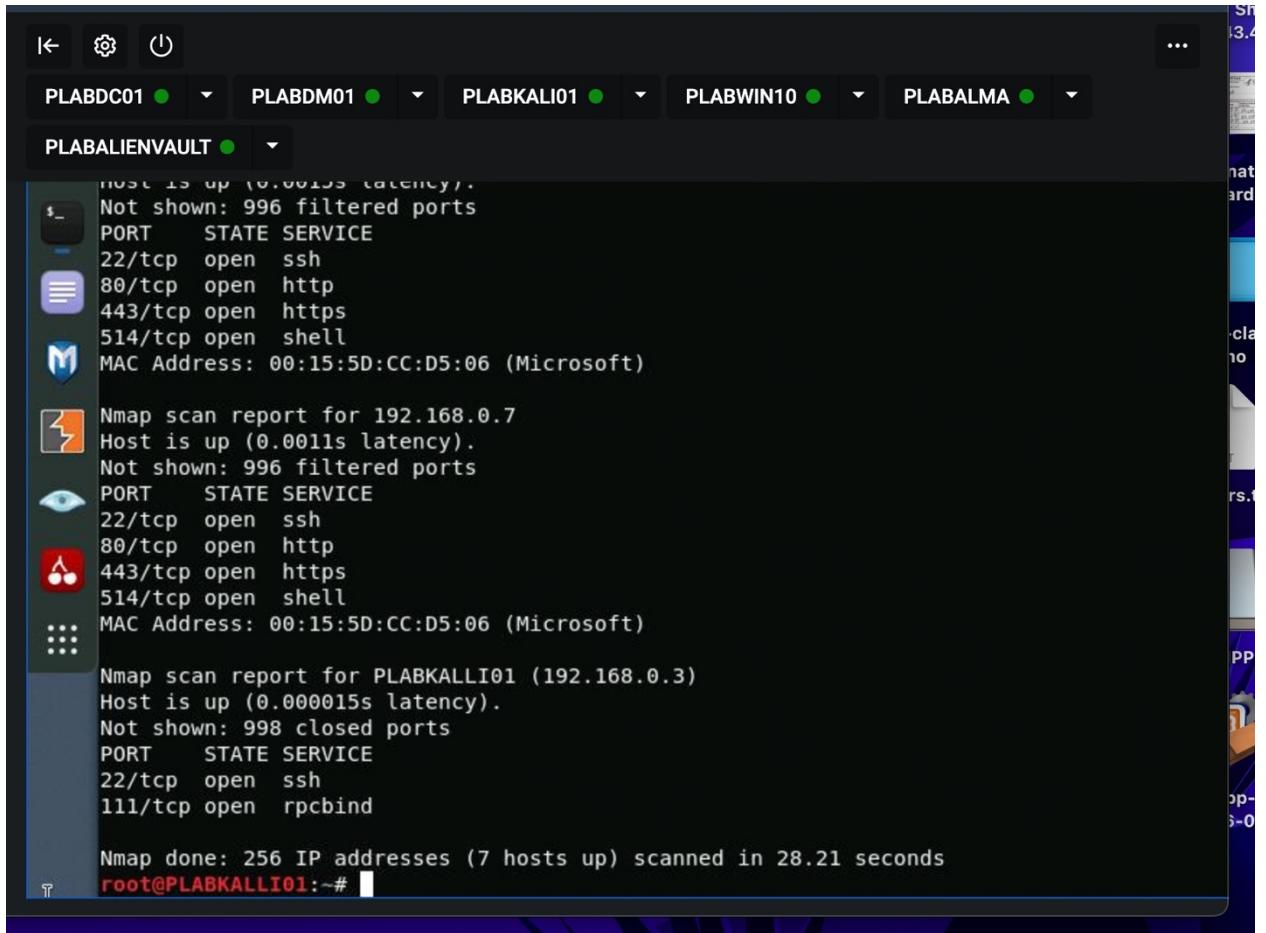
Nmap done: 10 IP addresses (7 hosts up) scanned in 26.41 seconds
root@PLABKALLI01:~#
```

- Place the output screenshot for nmap for the following here: **(if you get the message the host is down then start that host/vm up)**

ping scan

```
root@PLABKALLI01:~# nmap -sP 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-18 23:48 EDT
Nmap scan report for 192.168.0.1
Host is up (0.00095s latency).
MAC Address: 00:15:5D:CC:D5:02 (Microsoft)
Nmap scan report for 192.168.0.2
Host is up (0.00088s latency).
MAC Address: 00:15:5D:CC:D5:07 (Microsoft)
Nmap scan report for 192.168.0.4
Host is up (0.00090s latency).
MAC Address: 00:15:5D:CC:D5:0D (Microsoft)
Nmap scan report for 192.168.0.5
Host is up (0.0010s latency).
MAC Address: 00:15:5D:CC:D5:03 (Microsoft)
Nmap scan report for alienvault (192.168.0.6)
Host is up (0.00096s latency).
MAC Address: 00:15:5D:CC:D5:05 (Microsoft)
Nmap scan report for 192.168.0.7
Host is up (0.00096s latency).
MAC Address: 00:15:5D:CC:D5:05 (Microsoft)
Nmap scan report for PLABKALLI01 (192.168.0.3)
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 14.93 seconds
root@PLABKALLI01:~# R
```

ARP scan



The screenshot shows a terminal window with a dark theme. At the top, there are five host names listed in a header bar: PLABDC01, PLABDM01, PLABKALI01, PLABWIN10, and PLBALMA. Below this, the host PLBALIENVault is selected. The terminal displays three separate Nmap scan reports:

- PLBALIENVault**:
Host is up (0.0011s latency).
Not shown: 996 filtered ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp open https
514/tcp open shell
MAC Address: 00:15:5D:CC:D5:06 (Microsoft)
- Nmap scan report for 192.168.0.7**:
Host is up (0.0011s latency).
Not shown: 996 filtered ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp open https
514/tcp open shell
MAC Address: 00:15:5D:CC:D5:06 (Microsoft)
- Nmap scan report for PLABKALI01 (192.168.0.3)**:
Host is up (0.000015s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
111/tcp open rpcbind

At the bottom of the terminal, it says "Nmap done: 256 IP addresses (7 hosts up) scanned in 28.21 seconds". The prompt "root@PLABKALI01:~#" is visible.

a port scan

```
Host is up (0.0014s latency).
PORT      STATE      SERVICE
80/tcp    filtered  http
MAC Address: 00:15:5D:CC:D5:03 (Microsoft)

Nmap scan report for alienvault (192.168.0.6)
Host is up (0.0013s latency).

PORT      STATE      SERVICE
80/tcp    open       http
MAC Address: 00:15:5D:CC:D5:06 (Microsoft)

Nmap scan report for 192.168.0.7
Host is up (0.0013s latency).

PORT      STATE      SERVICE
80/tcp    open       http
MAC Address: 00:15:5D:CC:D5:05 (Microsoft)

Nmap scan report for PLABKALLI01 (192.168.0.3)
Host is up (0.000074s latency).

PORT      STATE      SERVICE
80/tcp    closed    http

Nmap done: 256 IP addresses (7 hosts up) scanned in 15.34 seconds
```

- Place the output screenshot of the following command here: **(if you get the message "host is down" then start that host/vm up)**
`nmap -O --osscan-limit 192.168.0.0/24`

The screenshot shows a terminal window with a dark background and light-colored text. At the top, there are several host status indicators: PLABDC01 (green), PLABDM01 (green), PLABKALI01 (green), PLABWIN10 (green), PLABALMA (green), and PLABALIENVULT (green). Below these, the host name PLABKALLI01 is selected. The main content of the terminal is the output of an Nmap scan:

```
MAC Address: 00:15:5D:CC:D5:06 (Microsoft)
Nmap scan report for 192.168.0.7
Host is up (0.00085s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
514/tcp   open  shell
MAC Address: 00:15:5D:CC:D5:06 (Microsoft)

Nmap scan report for PLABKALLI01 (192.168.0.3)
Host is up (0.000067s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 256 IP addresses (7 hosts up) scanned in 34.00 seconds
root@PLABKALLI01:~#
```

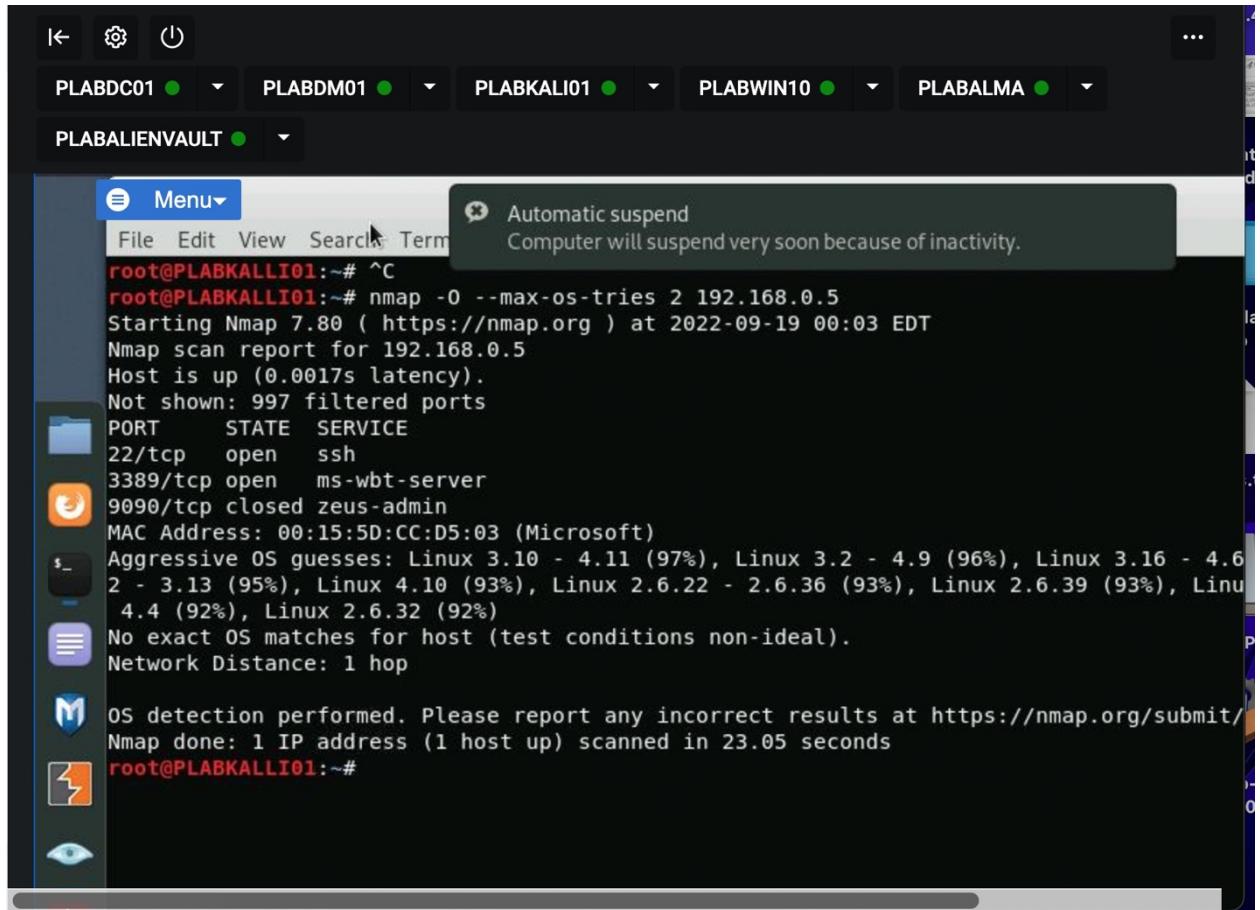
nmap -O --osscan-guess 192.168.0.3

The screenshot shows a terminal window with a dark theme. At the top, there are several tabs labeled with hostnames: PLABDC01, PLABDM01, PLABKALI01, PLABWIN10, and PLABALMA. Below these tabs, the current active tab is labeled "PLABALIENVULT". A tooltip message "Automatic suspend Computer will suspend very soon because of inactivity." is displayed near the top right. The main terminal area displays the output of an Nmap scan:

```
root@PLABKALLI01:~# ^C
root@PLABKALLI01:~# nmap -O --osscan-guess 192.168.0.3
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-19 00:00 EDT
Nmap scan report for PLABKALLI01 (192.168.0.3)
Host is up (0.000059s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 2.25 seconds
root@PLABKALLI01:~#
```

nmap -O --max-os-tries 2 192.168.0.5



The screenshot shows a terminal window in a Kali Linux desktop environment. The terminal title bar says "PLABALIENVAULT". A system tray icon indicates "Automatic suspend" is enabled. The terminal content is an nmap scan report for host 192.168.0.5:

```
root@PLABKALLI01:~# ^C
root@PLABKALLI01:~# nmap -O --max-os-tries 2 192.168.0.5
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-19 00:03 EDT
Nmap scan report for 192.168.0.5
Host is up (0.0017s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
3389/tcp  open  ms-wbt-server
9090/tcp  closed zeus-admin
MAC Address: 00:15:5D:CC:D5:03 (Microsoft)
Aggressive OS guesses: Linux 3.10 - 4.11 (97%), Linux 3.2 - 4.9 (96%), Linux 3.16 - 4.6
2 - 3.13 (95%), Linux 4.10 (93%), Linux 2.6.22 - 2.6.36 (93%), Linux 2.6.39 (93%), Linu
4.4 (92%), Linux 2.6.32 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 23.05 seconds
root@PLABKALLI01:~#
```

- Place the output screenshot for the command hping3 here:

hping3 192.168.0.1 --icmp

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@PLABKALLI01:~". The terminal content displays the output of the hping3 command, which is sending ICMP packets to the IP address 192.168.0.1. The output includes details like packet length, source IP, TTL, ID, sequence number, and round-trip time (RTT). It also shows a summary of the transmitted and received packets, including a 8% packet loss.

```
root@PLABKALLI01:~# hping3 192.168.0.1 --icmp
HPING 192.168.0.1 (eth0 192.168.0.1): icmp mode set, 28 headers + 0 data bytes
len=28 ip=192.168.0.1 ttl=128 id=12829 icmp_seq=0 rtt=7.9 ms
len=28 ip=192.168.0.1 ttl=128 id=12830 icmp_seq=1 rtt=7.8 ms
len=28 ip=192.168.0.1 ttl=128 id=12831 icmp_seq=2 rtt=7.8 ms
len=28 ip=192.168.0.1 ttl=128 id=12832 icmp_seq=3 rtt=7.7 ms
len=28 ip=192.168.0.1 ttl=128 id=12833 icmp_seq=4 rtt=7.6 ms
len=28 ip=192.168.0.1 ttl=128 id=12834 icmp_seq=5 rtt=7.5 ms
len=28 ip=192.168.0.1 ttl=128 id=12835 icmp_seq=6 rtt=7.5 ms
len=28 ip=192.168.0.1 ttl=128 id=12836 icmp_seq=7 rtt=7.4 ms
len=28 ip=192.168.0.1 ttl=128 id=12837 icmp_seq=8 rtt=7.4 ms
len=28 ip=192.168.0.1 ttl=128 id=12838 icmp_seq=9 rtt=7.3 ms
len=28 ip=192.168.0.1 ttl=128 id=12839 icmp_seq=10 rtt=7.2 ms
len=28 ip=192.168.0.1 ttl=128 id=12840 icmp_seq=11 rtt=7.2 ms
len=28 ip=192.168.0.1 ttl=128 id=12841 icmp_seq=12 rtt=7.1 ms
^C
--- 192.168.0.1 hping statistic ---
14 packets transmitted, 13 packets received, 8% packet loss
round-trip min/avg/max = 7.1/7.5/7.9 ms
root@PLABKALLI01:~#
```

hping3 192.168.0.1 --icmp -c 5

```
root@PLABKALLI01:~# hping3 192.168.0.1 --icmp -c 5
HPING 192.168.0.1 (eth0 192.168.0.1): icmp mode set, 28 headers + 0 data bytes
len=28 ip=192.168.0.1 ttl=128 id=12843 icmp_seq=0 rtt=7.9 ms
len=28 ip=192.168.0.1 ttl=128 id=12844 icmp_seq=1 rtt=7.8 ms
len=28 ip=192.168.0.1 ttl=128 id=12845 icmp_seq=2 rtt=7.8 ms
len=28 ip=192.168.0.1 ttl=128 id=12846 icmp_seq=3 rtt=7.7 ms
len=28 ip=192.168.0.1 ttl=128 id=12847 icmp_seq=4 rtt=7.6 ms

--- 192.168.0.1 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.6/7.8/7.9 ms
root@PLABKALLI01:~#
```

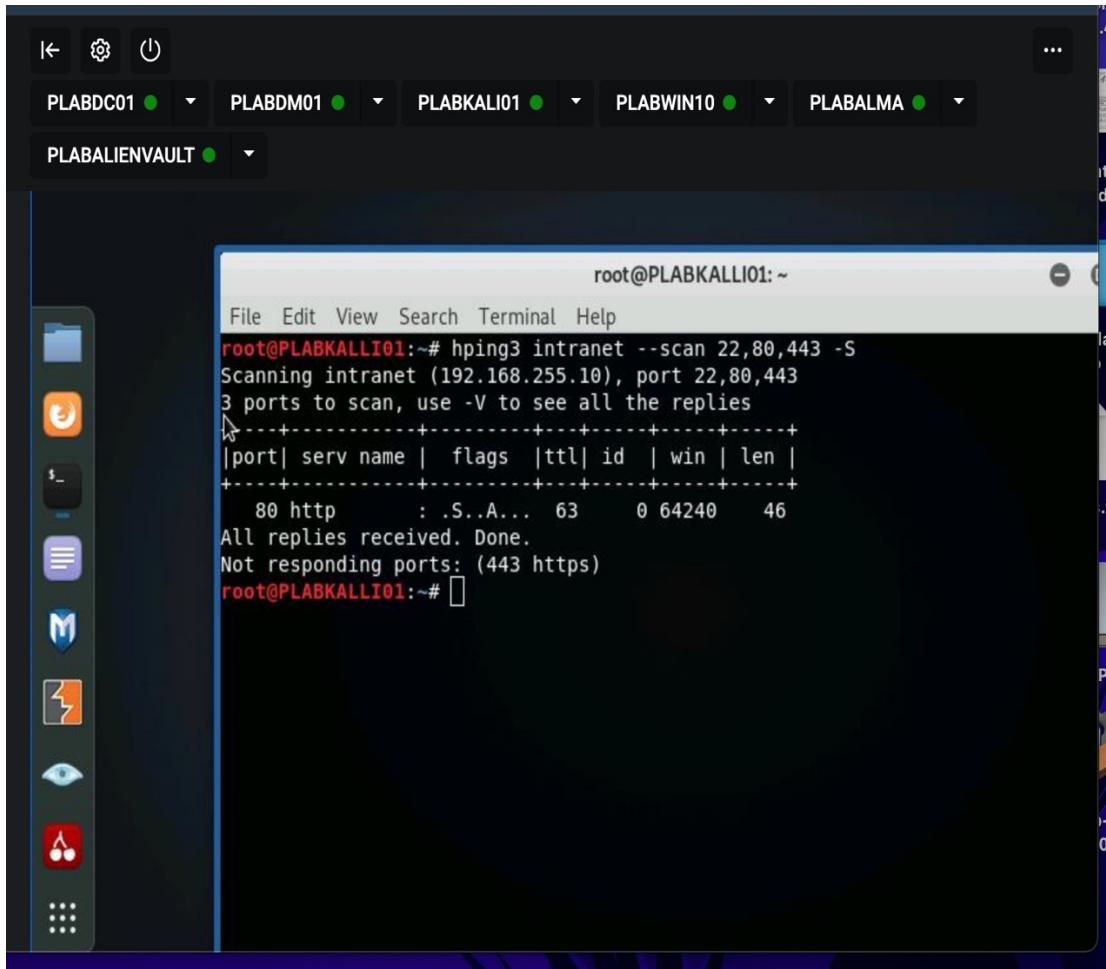
hping3 intranet --scan 80 -S

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "root@PLABKALLI01:~". The window contains the following text:

```
File Edit View Search Terminal Help
root@PLABKALLI01:~# hping3 intranet --scan 80 -S
Scanning intranet (192.168.255.10), port 80
1 ports to scan, use -V to see all the replies
+-----+
|port| serv name | flags | ttl| id | win | len |
+-----+
      80 http   : .S..A... 63    0 64240   46
All replies received. Done.
Text Editor Not responding ports:
root@PLABKALLI01:~#
```

The terminal window has a dark background with light-colored text. The window title bar includes the word "root". The desktop interface features a dock on the left with various icons, including a text editor icon which is currently selected.

hping3 intranet --scan 22,80,443 -S



The screenshot shows a Kali Linux desktop environment with several terminal windows open in a terminal emulator. The title bar of the active window reads "root@PLABKALLI01:~". The terminal window displays the following command and its output:

```
File Edit View Search Terminal Help
root@PLABKALLI01:~# hping3 intranet --scan 22,80,443 -S
Scanning intranet (192.168.255.10), port 22,80,443
3 ports to scan, use -V to see all the replies
|port| serv name | flags |ttl| id | win | len |
+---+-----+-----+-----+-----+
  80 http      : .S..A... 63    0 64240   46
All replies received. Done.
Not responding ports: (443 https)
root@PLABKALLI01:~#
```

Note:

The **hping3** command will continue for an indefinite time unless you stop it. To do this, press the **Ctrl + C** keys.

- Place the output screenshot for the command Responder.py step-1 to 16 here:

2) Passive Reconnaissance

- Place the output screenshots of the Whois Lookup command here:

Enter the www.practice-labs.com in the Whois Lookup search section and provide the following:

- Server type

Name Servers	NS-1153.AWSDNS-16.ORG (has 49,764 domains) NS-1938.AWSDNS-50.CO.UK (has 302 domains) NS-444.AWSDNS-55.COM (has 1,348 domains) NS-894.AWSDNS-47.NET (has 23 domains)
--------------	--

- IP address

IP Address	193.108.247.199 is hosted on a dedicated server
------------	---

- IP location

IP Location	 - Greater London - London - Venus Business Communications Limited
-------------	---

- IP history

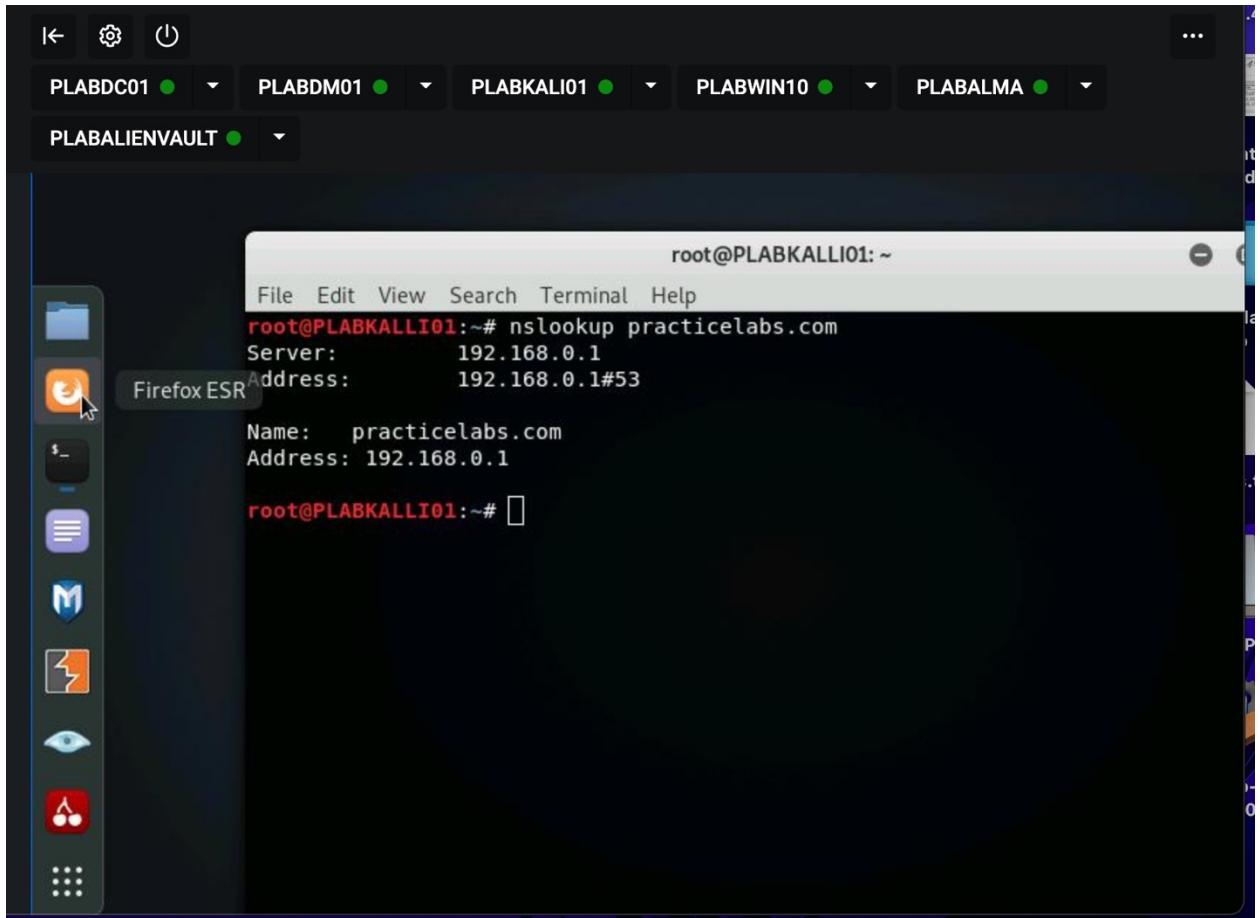
IP History	4 changes on 4 unique IP addresses over 11 years
------------	--

- Registrar history

Registrar History	5 registrars
-------------------	--------------

- Please the output screenshot of the following command here:

nslookup practicelabs.com



nslookup -type=soa practicelabs.com

The screenshot shows a terminal window titled "root@PLABKALLI01:~". The window contains the following command and its output:

```
root@PLABKALLI01:~# nslookup -type=soa practicelabs.com
Server:          192.168.0.1
Address:         192.168.0.1#53

practicelabs.com
    origin = plabdc01.practicelabs.com
    mail addr = hostmaster.practicelabs.com
    serial = 42
    refresh = 900
    retry = 600
    expire = 86400
    minimum = 3600

root@PLABKALLI01:~#
```

nslookup -type=MX practicelabs.com

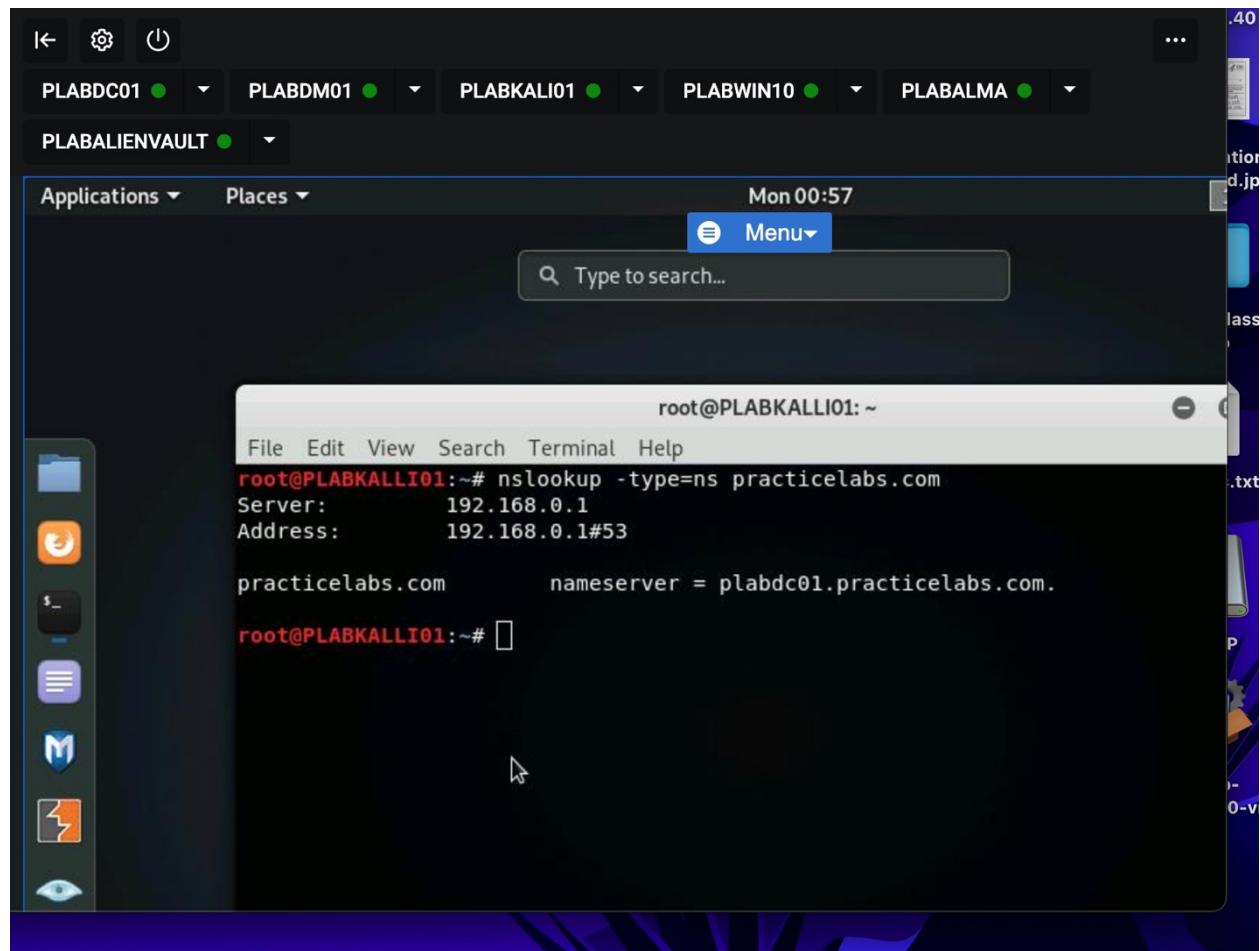
The screenshot shows a Kali Linux desktop environment. At the top, there is a dock with several icons: PLABDC01, PLABDM01, PLABKALI01, PLABWIN10, and PLABALMA. Below the dock, another row of icons includes PLABALIENVault. A vertical dock on the left contains icons for File Manager, Terminal, Dash, Mail, Network, Eye, and a terminal icon. The main window is a terminal window titled "root@PLABKALI01: ~". The terminal output is as follows:

```
root@PLABKALI01:~# nslookup -type=MX practicelabs.com
Server:          192.168.0.1
Address:         192.168.0.1#53

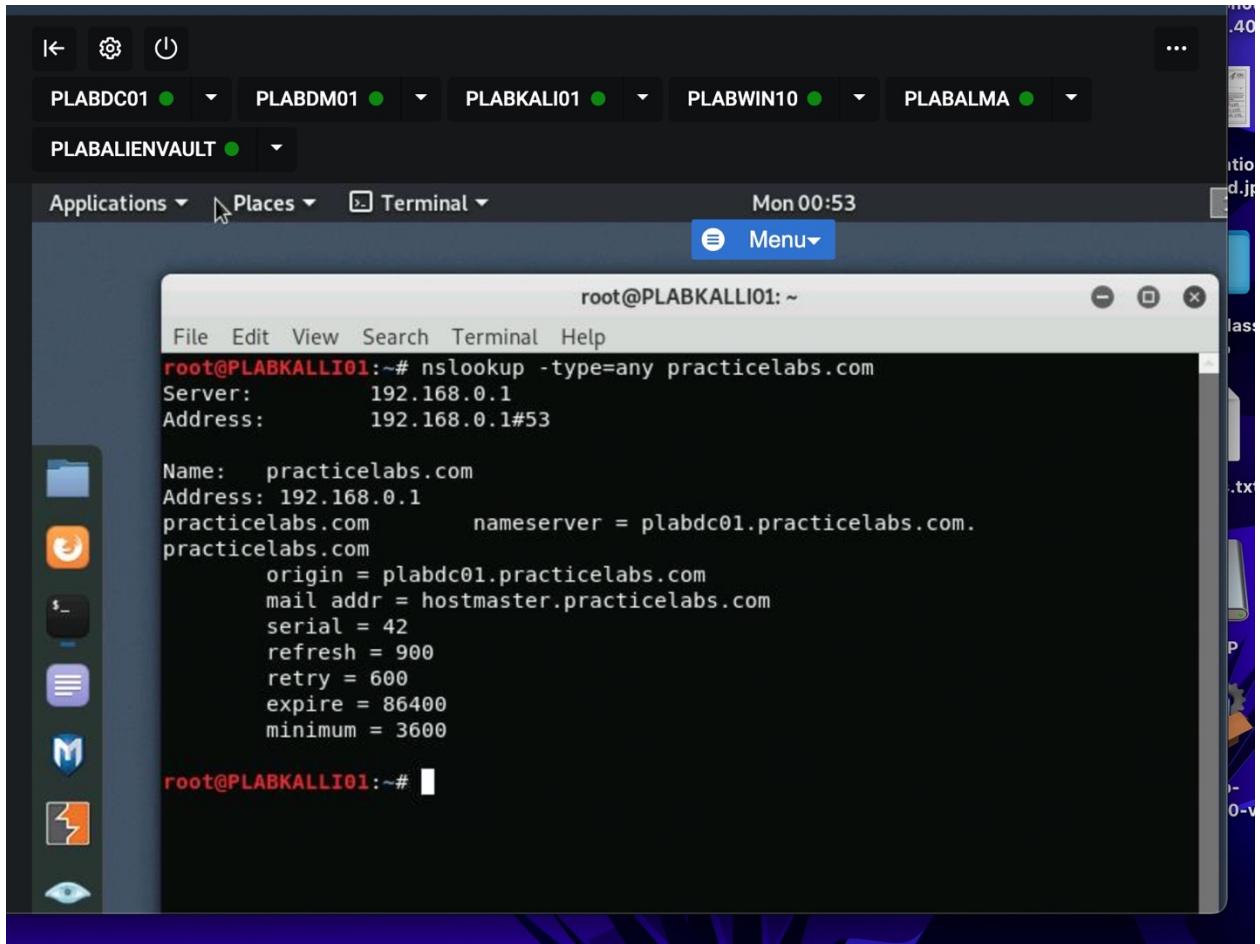
*** Can't find practicelabs.com: No answer

root@PLABKALI01:~#
```

`nslookup -type=ns practicelabs.com`



nslookup -type=any practicelabs.com



- Save the report as a docx file (first name and last name: ex. Awad_Mussa1.docx)
- Keep this file as you will upload it when you take the lab2's quiz.