CIT 485 ADVANCED CYBERSECURITY-

Lab2: Enumeration tools

The purpose of this lab is:

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

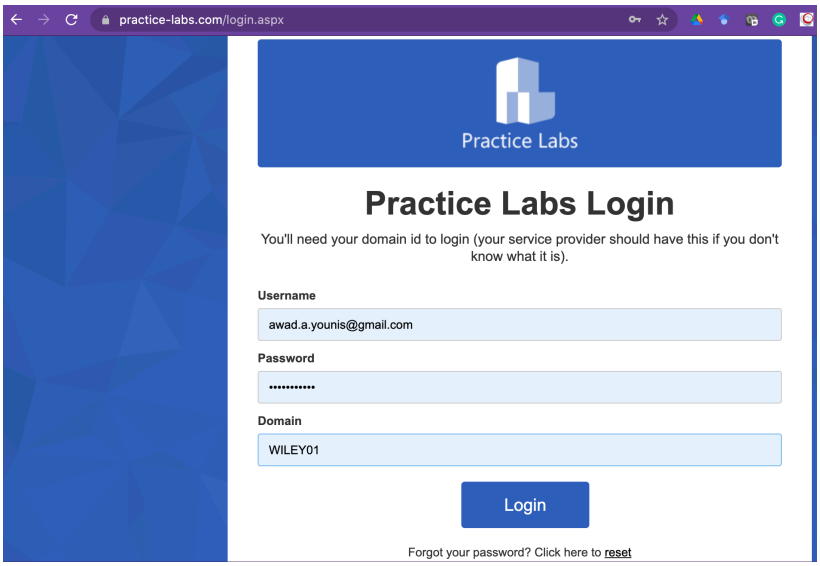
- Use Nmap
- Use the Hping Command
- Understand Active vs. Passive Enumeration
- Use the Responder

LAB INSTRUCTIONS:

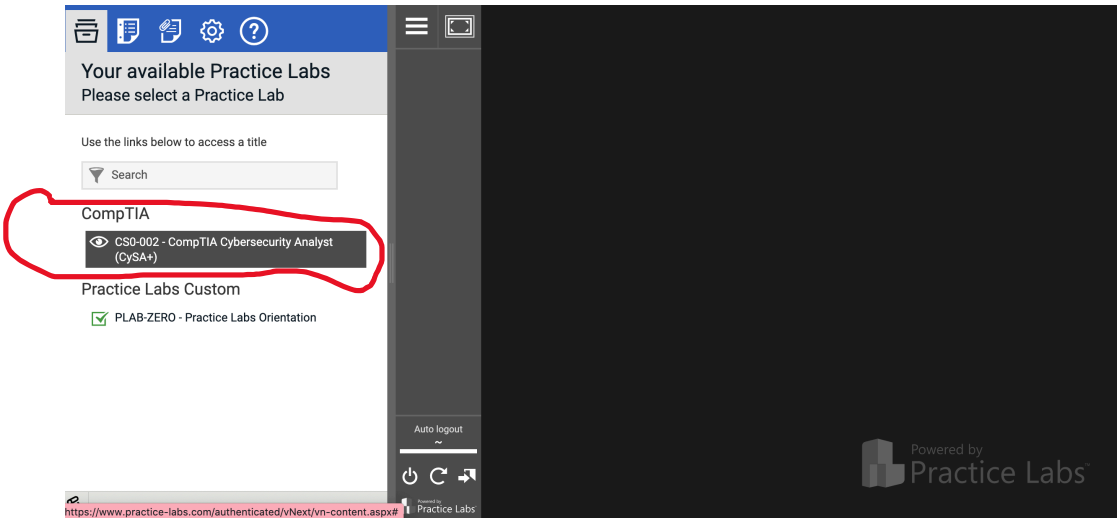
We assume you have completed lab0 and have created and activated your practice labs account. If you have not done that yet, please refer to lab0 instructions in Canvas, Week1, Lab0 section.

Lab2: Enumeration tools

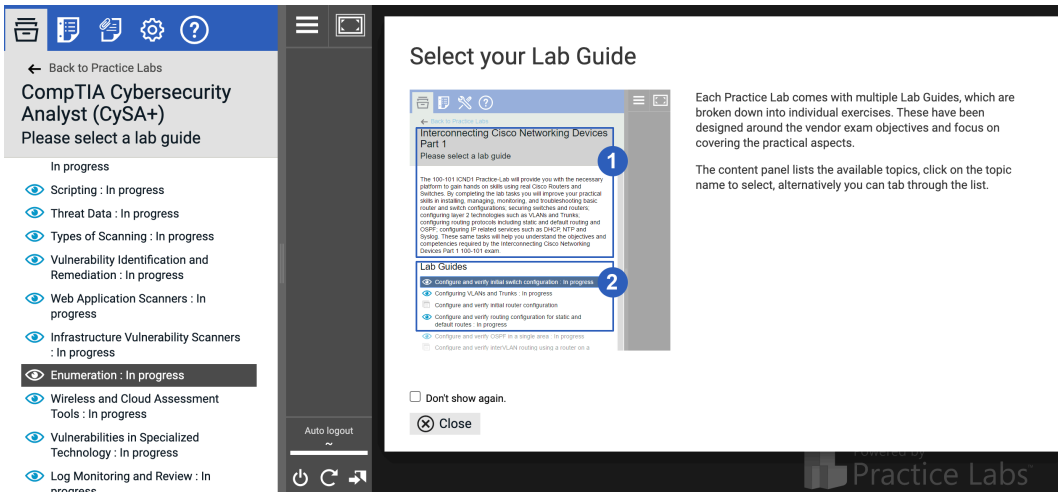
- Enter your credentials and the domain name at: www.practice-labs.com/login.aspx



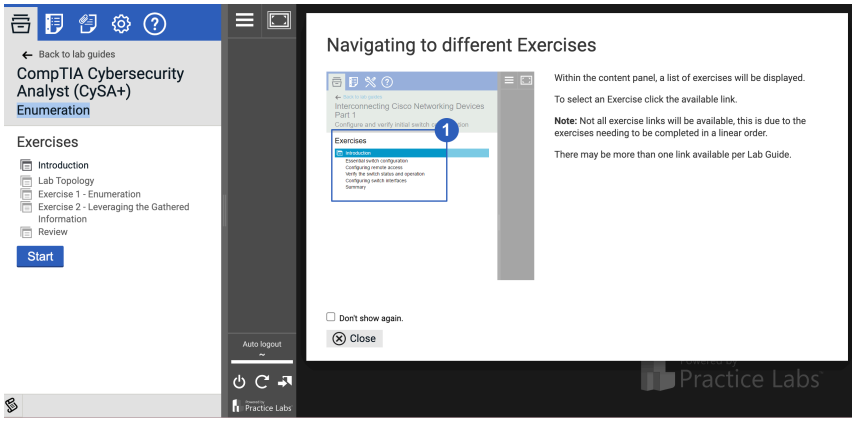
- On the “your available practice labs”, select CS0-002- CompTIA Cybersecurity Analyst



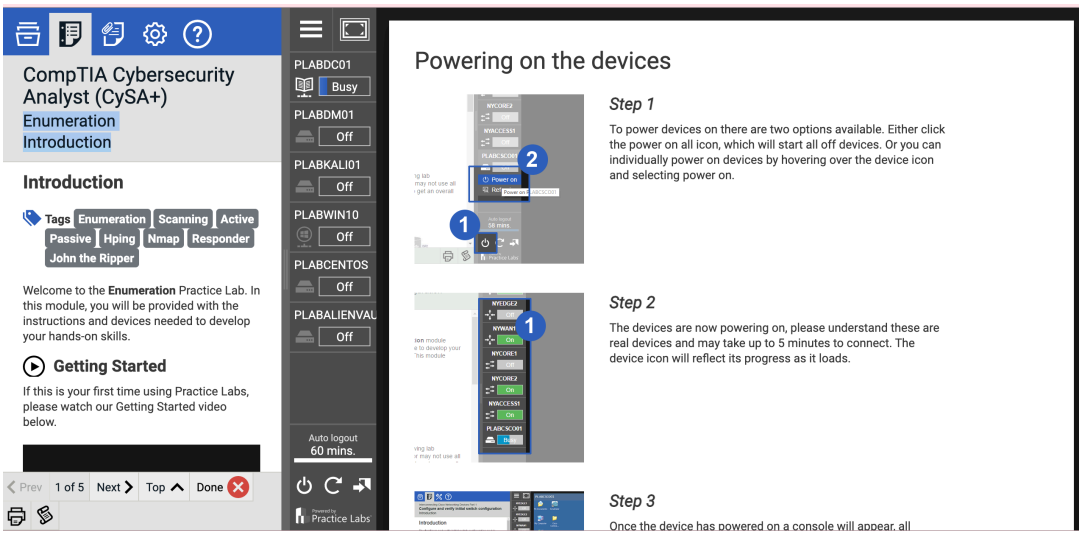
- From the lab guide, select Enumeration



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



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

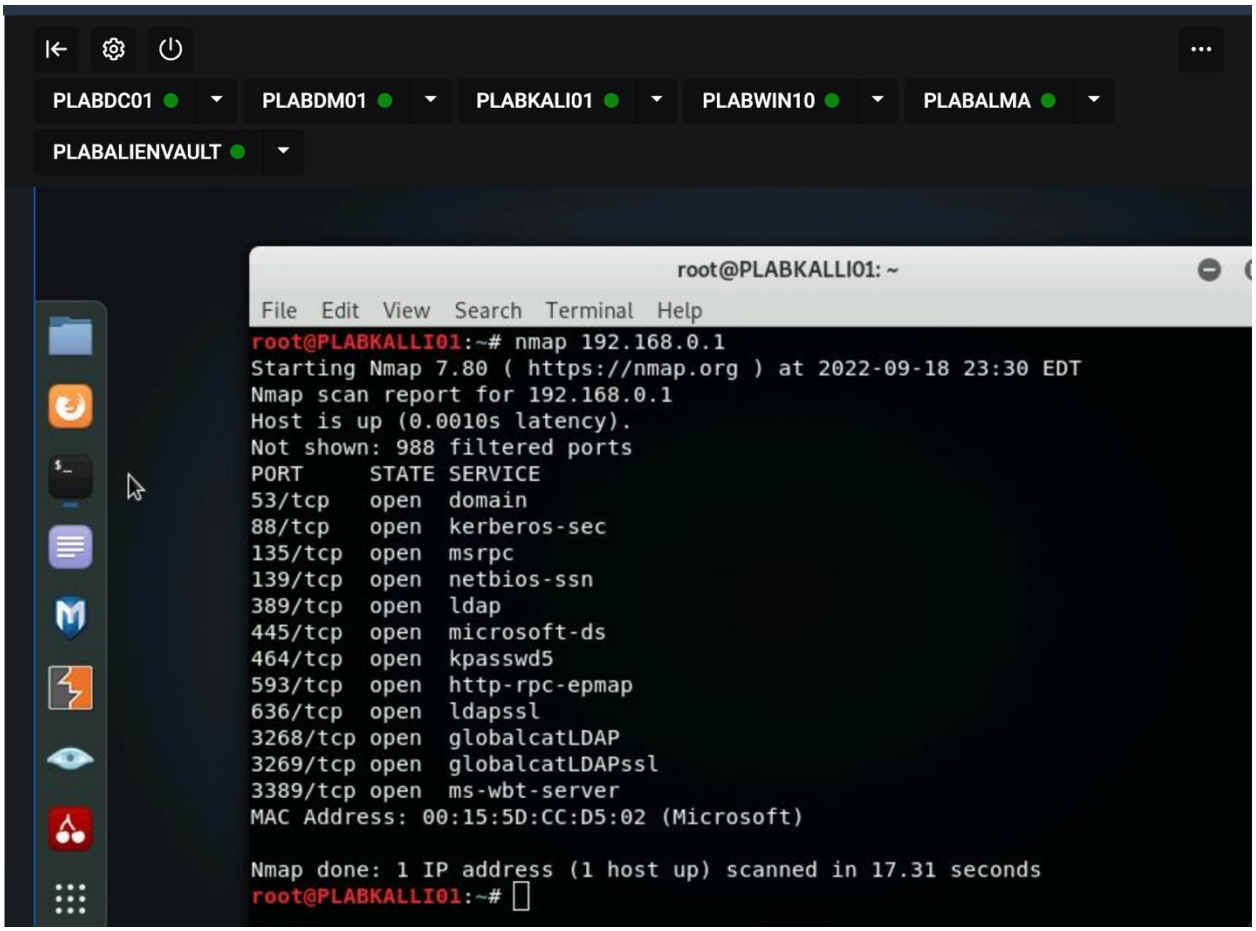


LAB SUBMISSION

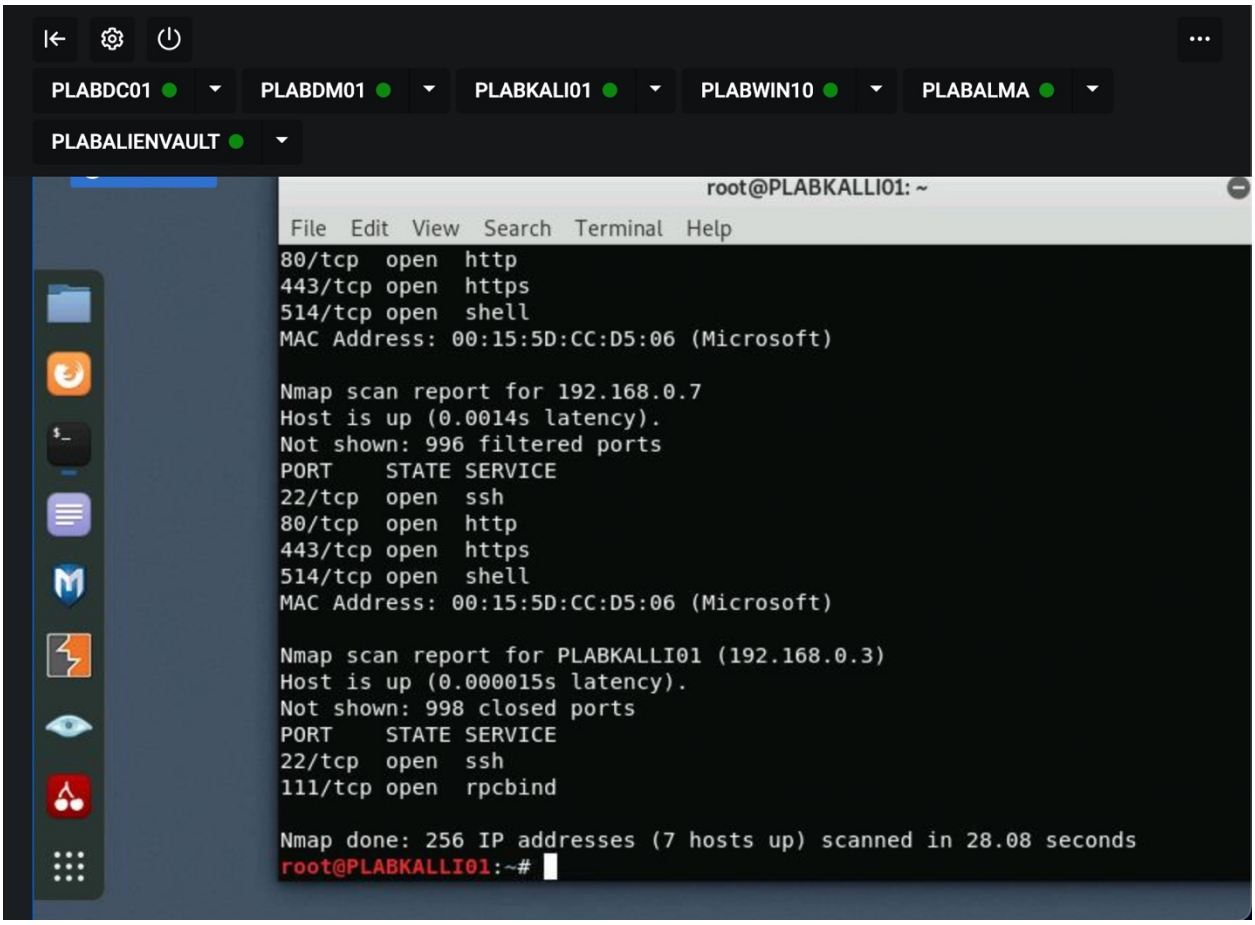
Please make sure to do all the exercises.

1) Active Reconnaissance

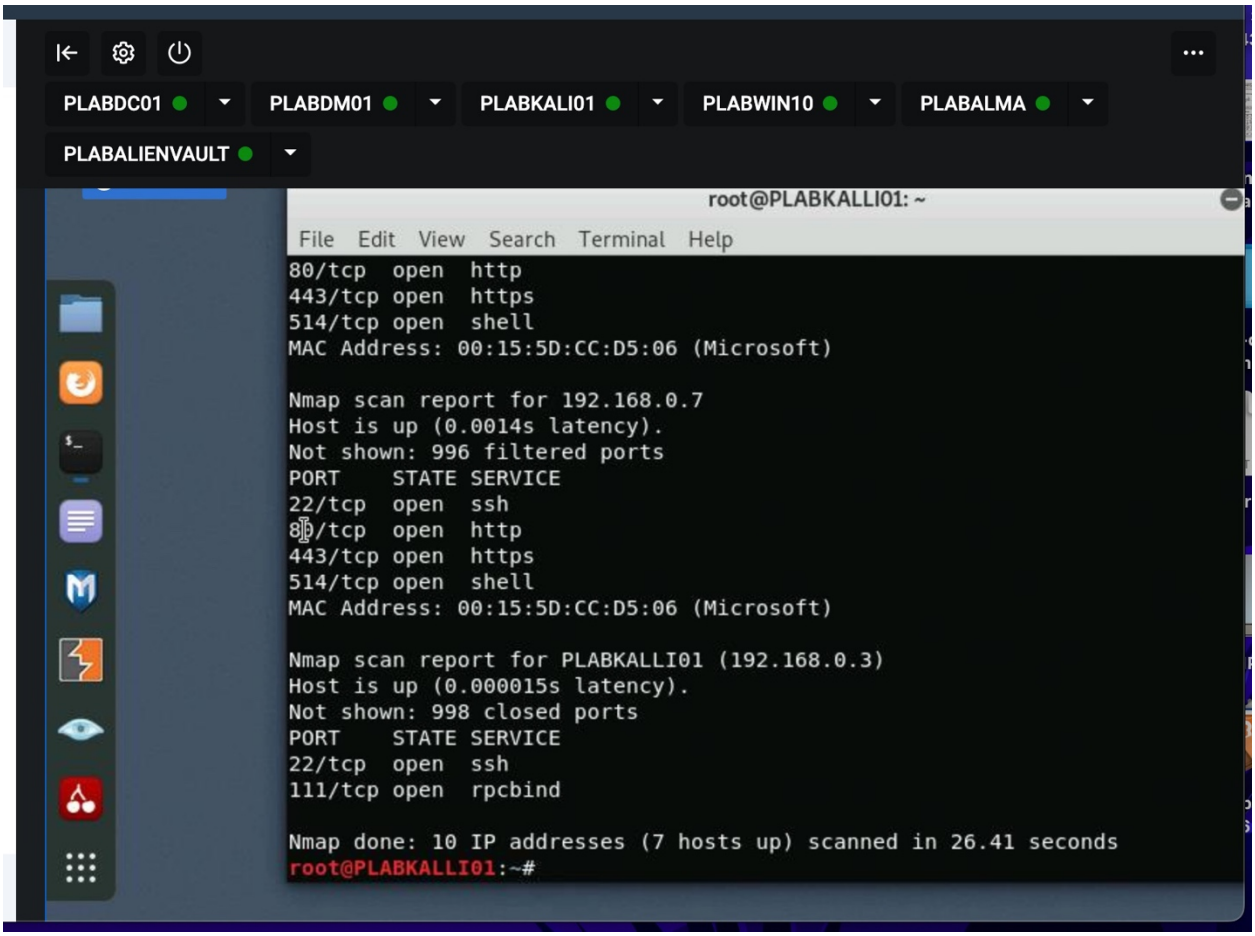
- Place the output screenshot of the following command here: **(if you get the message the host is down then start that host/vm up)**
  nmap 192.168.0.1



nmap 192.168.0.0/24,

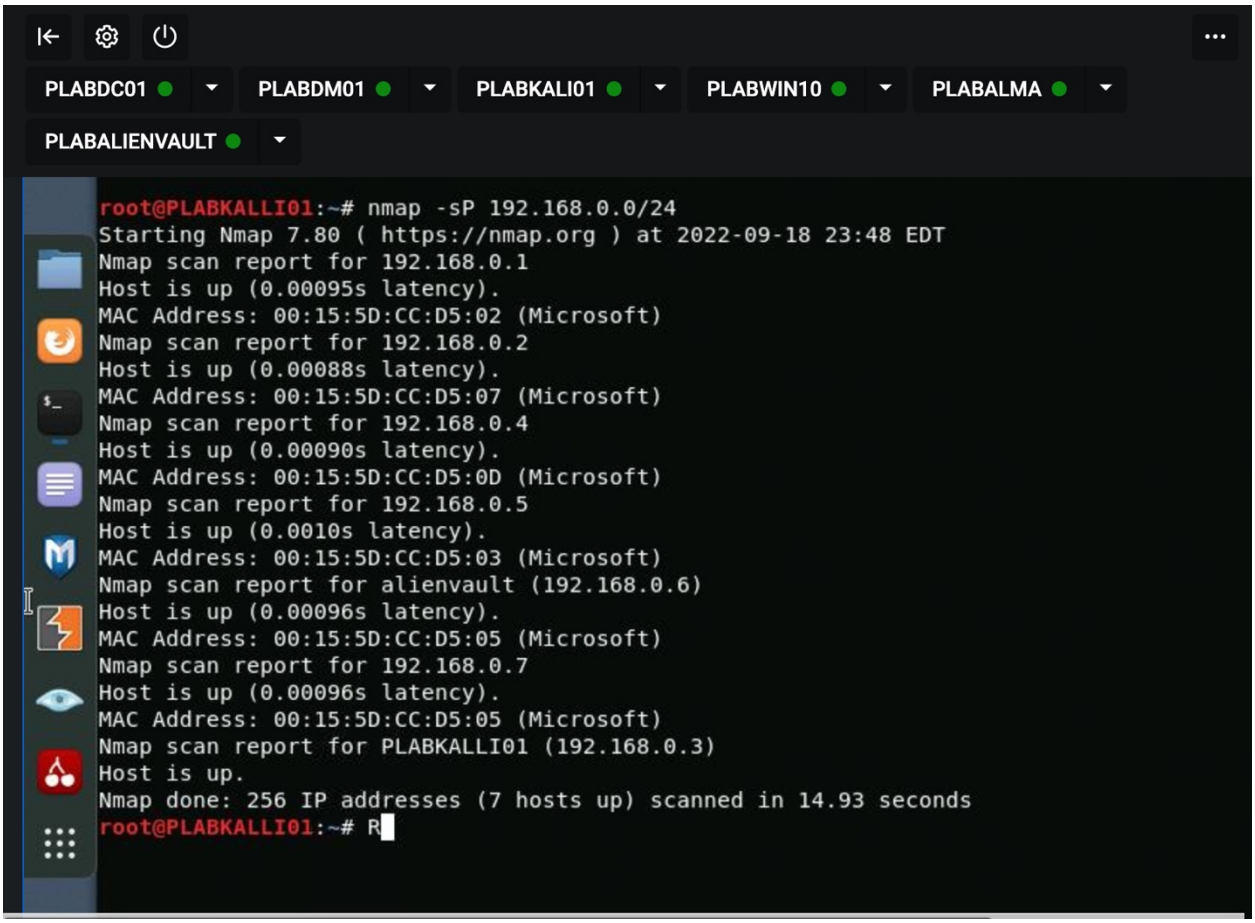


nmap 192.168.0.1-10

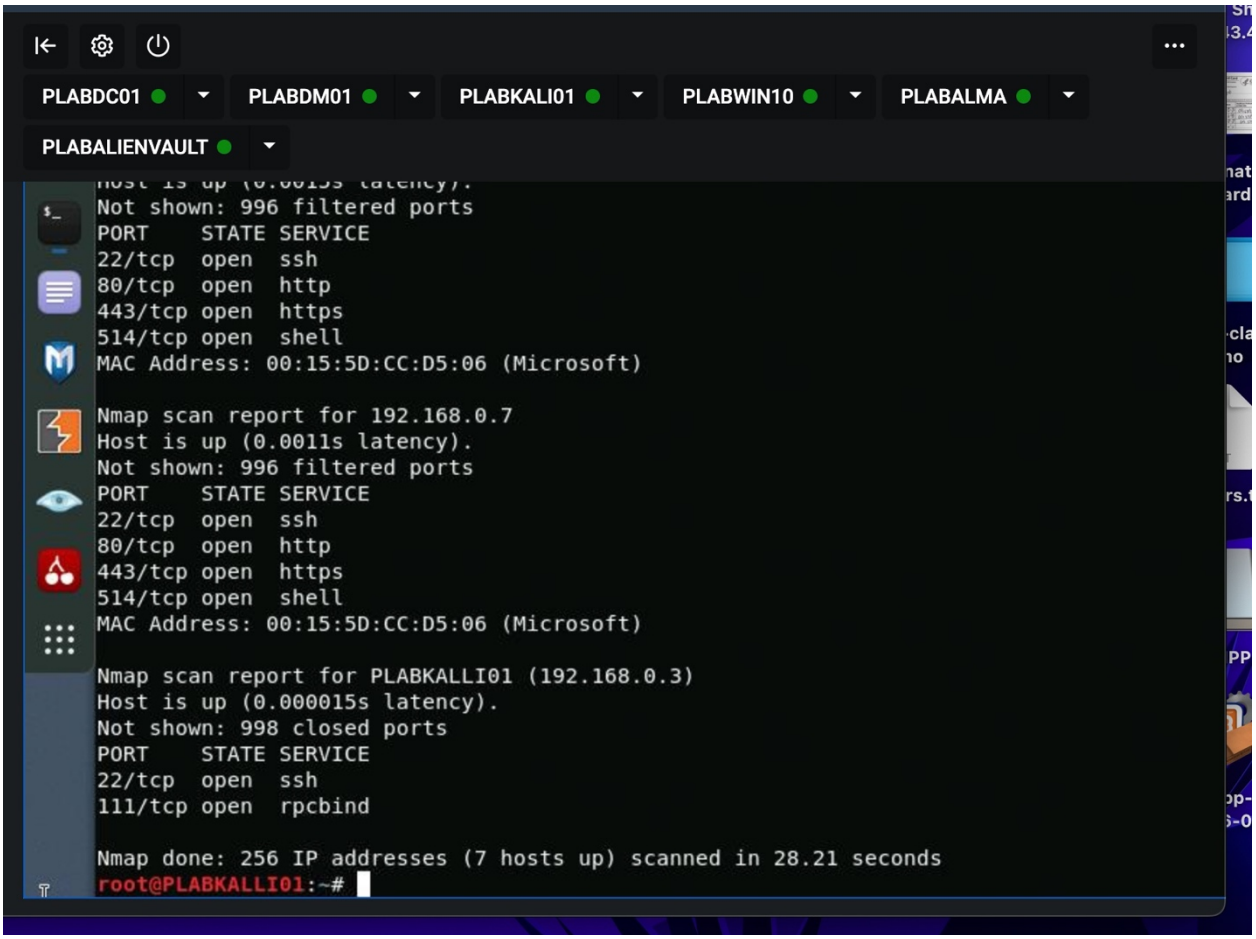


- Place the output screenshot for nmap for the following here: **(if you get the message the host is down then start that host/vm up)**

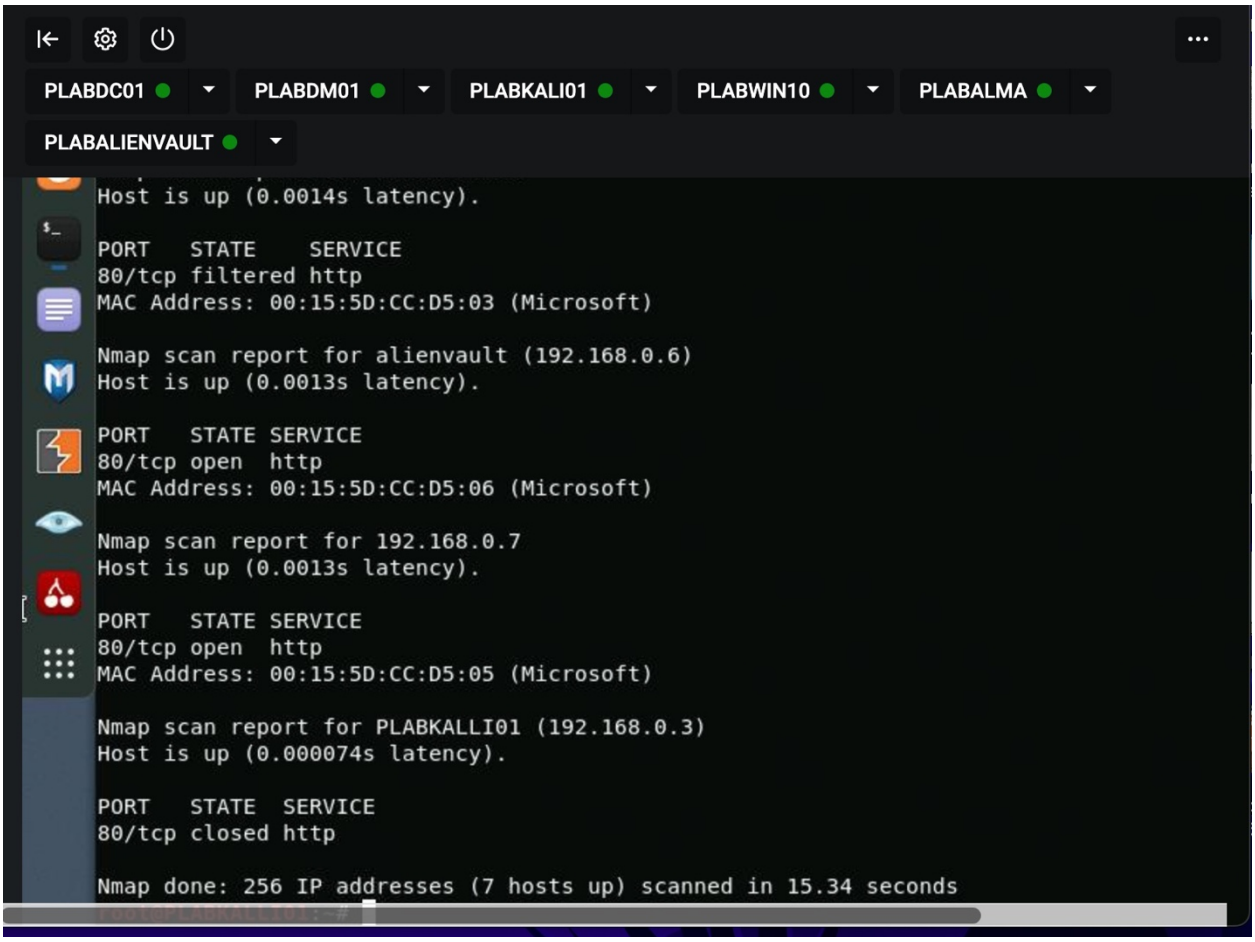
ping scan


PLABDC01
PLABDM01
PLABKALI01
PLABWIN10
PLABALMA
PLABALIENVAULT
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

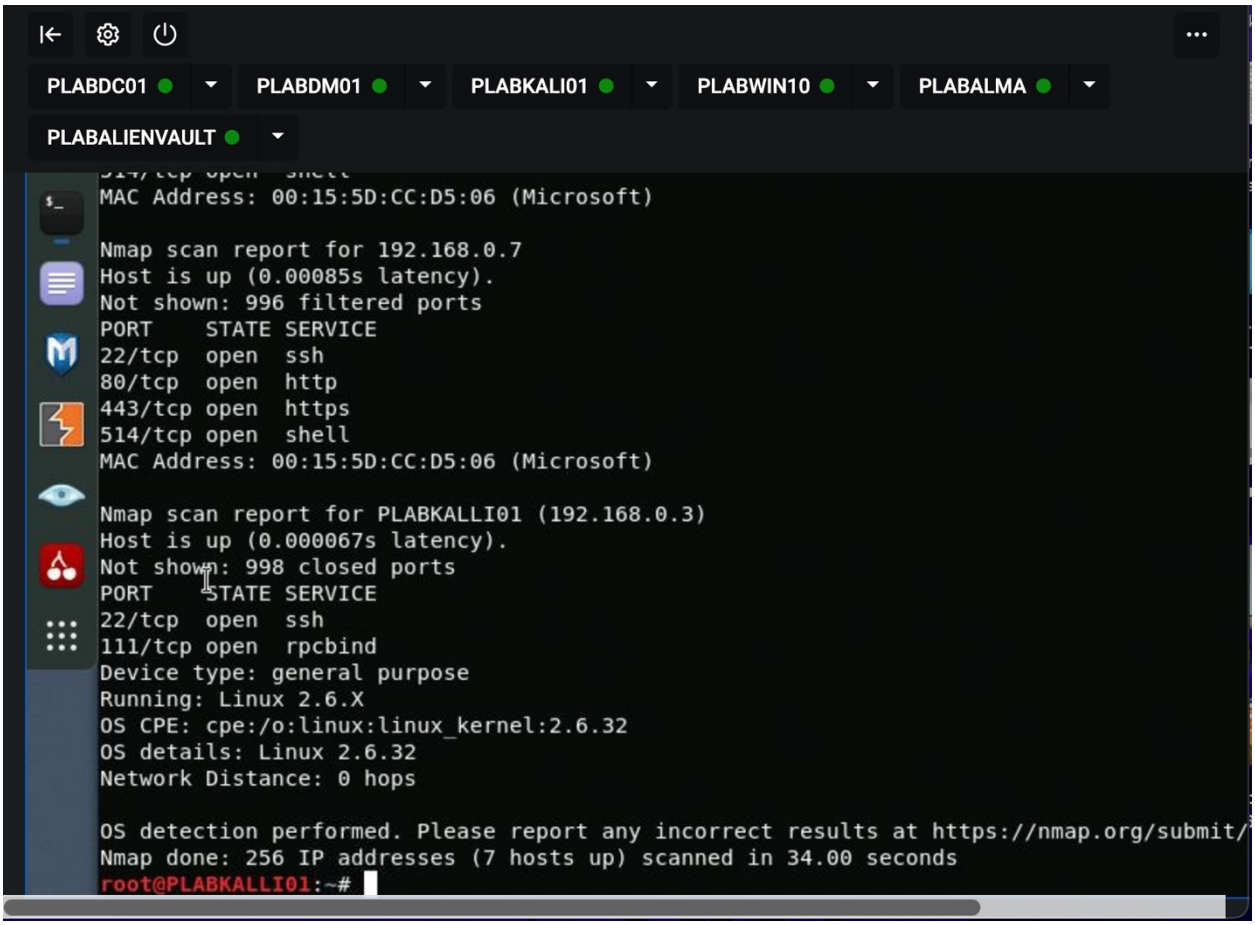
ARP scan


PLABDC01
PLABDM01
PLABKALI01
PLABWIN10
PLABALMA
PLABALIENVAULT
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 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 28.21 seconds
root@PLABKALLI01:~#

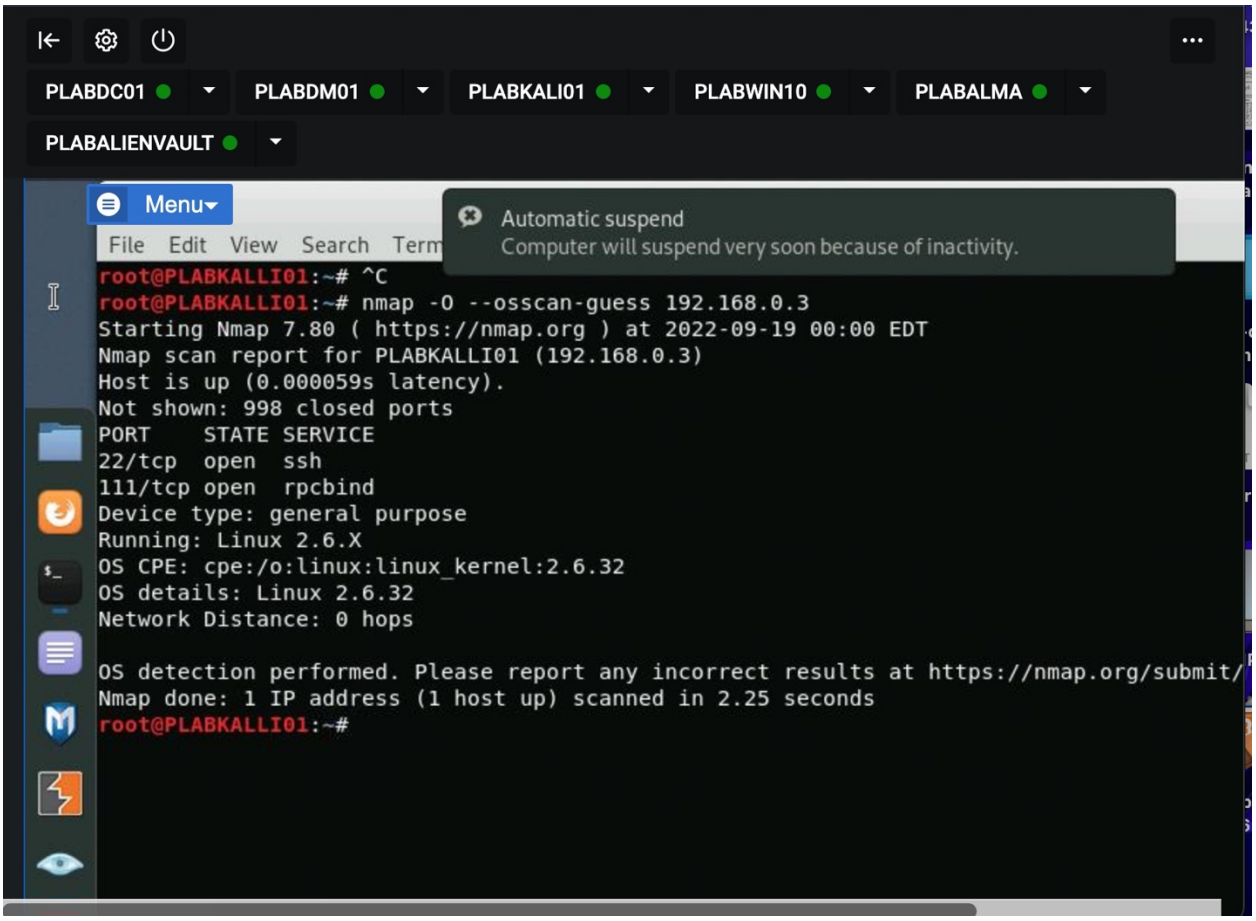
a port scan



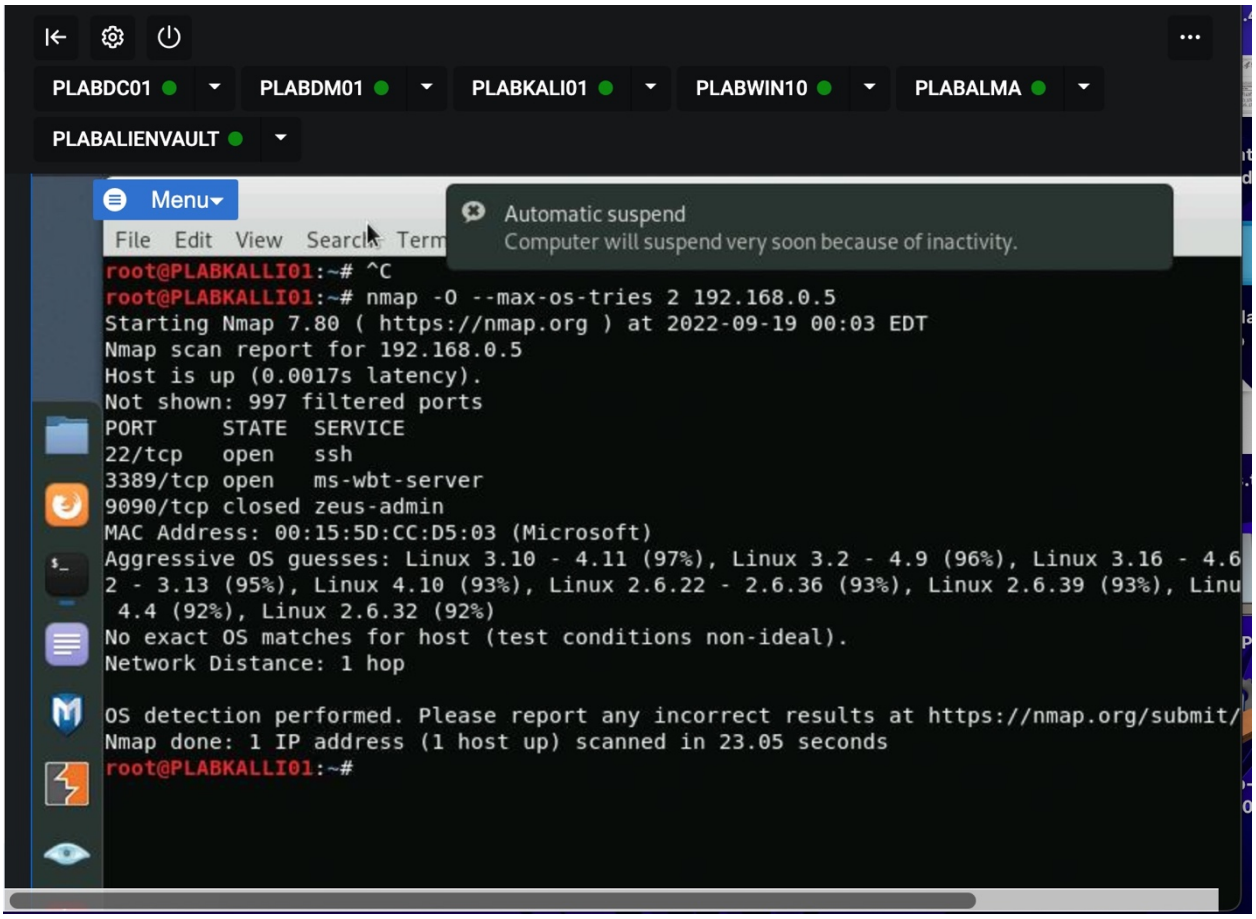
- Place the output screenshot of the following command here: **(if you get the message "host is down" then start that host/vm up)**
  nmap -O --osscan-limit 192.168.0.0/24



nmap -O --osscan-guess 192.168.0.3

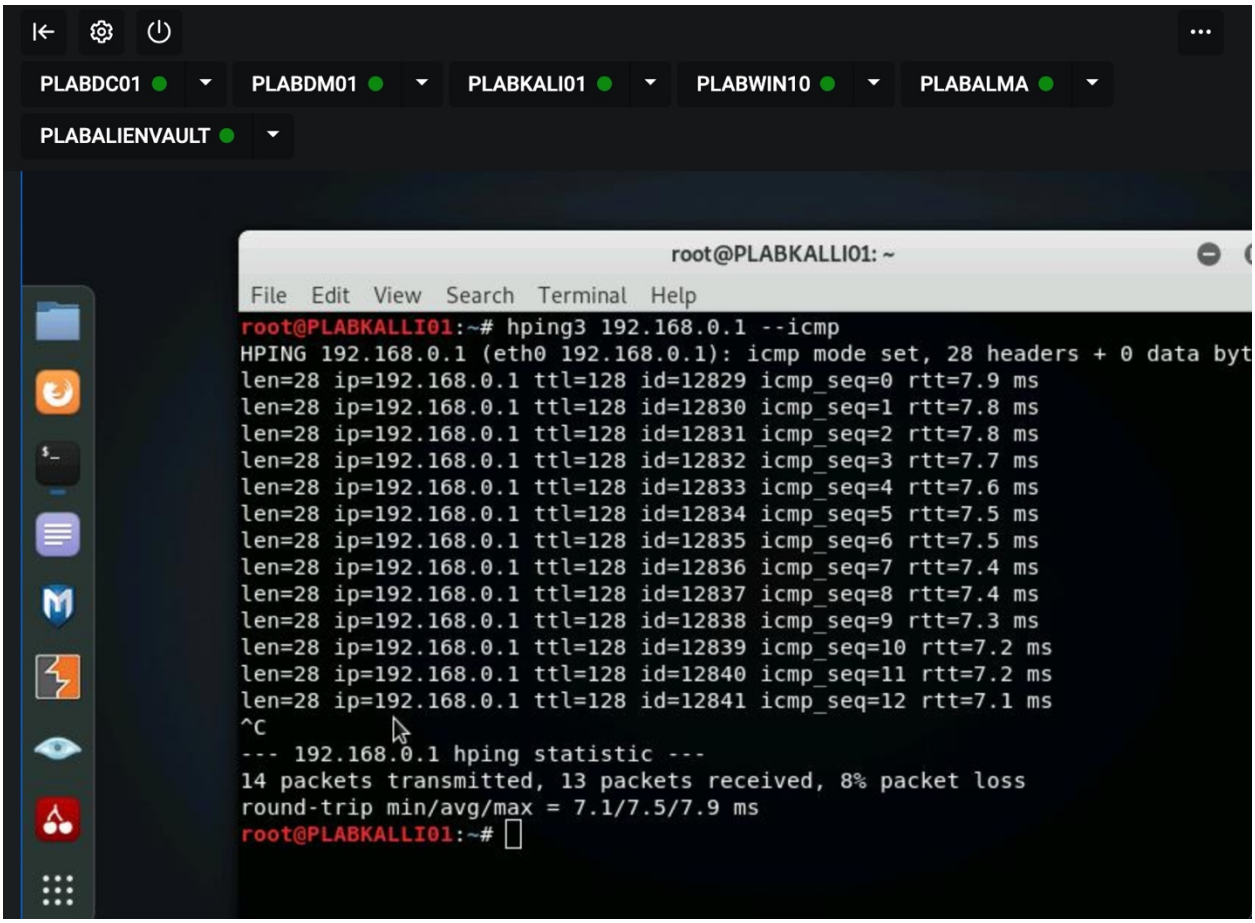


nmap -O --max-os-tries 2 192.168.0.5

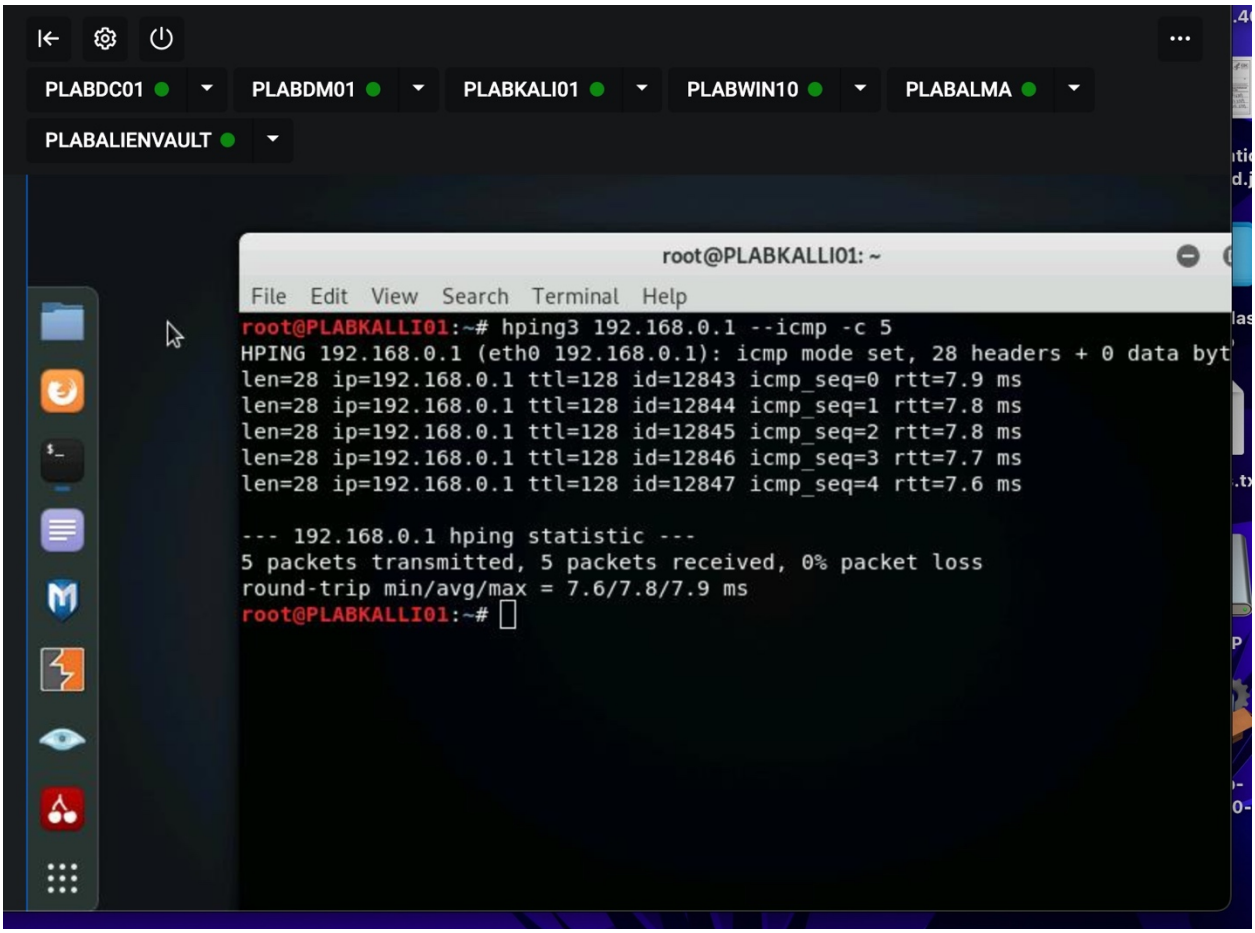


- Place the output screenshot for the command hping3 here:

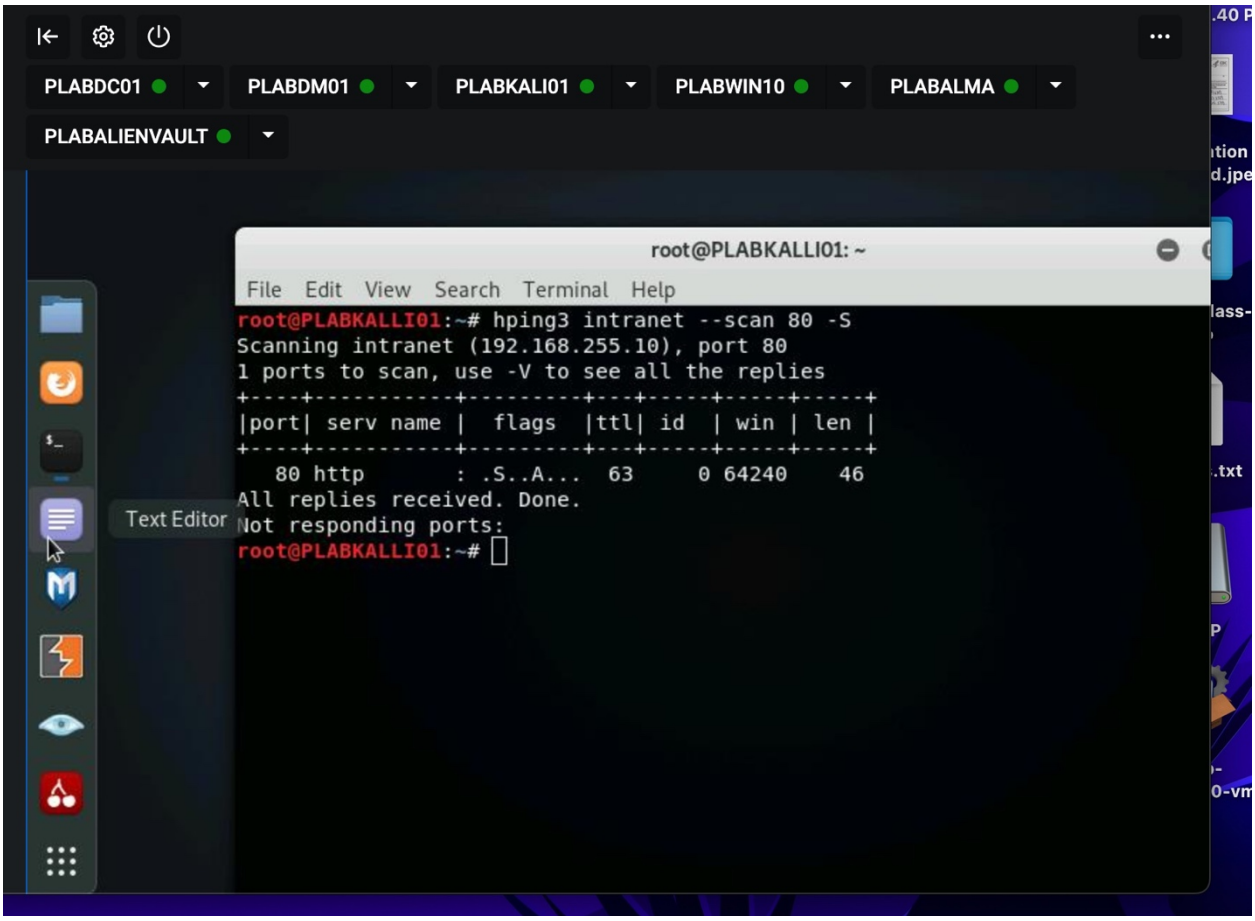
hping3 192.168.0.1 --icmp



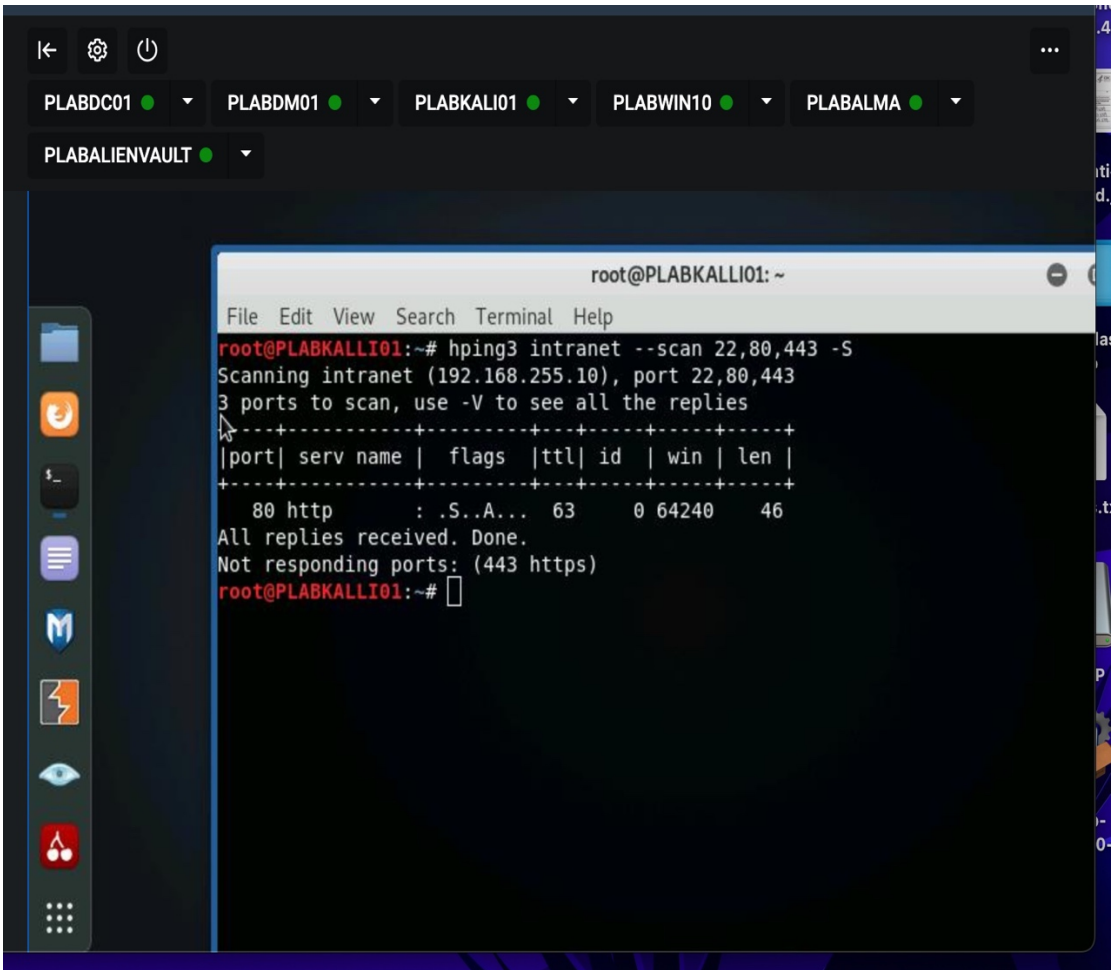
hping3 192.168.0.1 --icmp -c 5



hping3 intranet --scan 80 -S

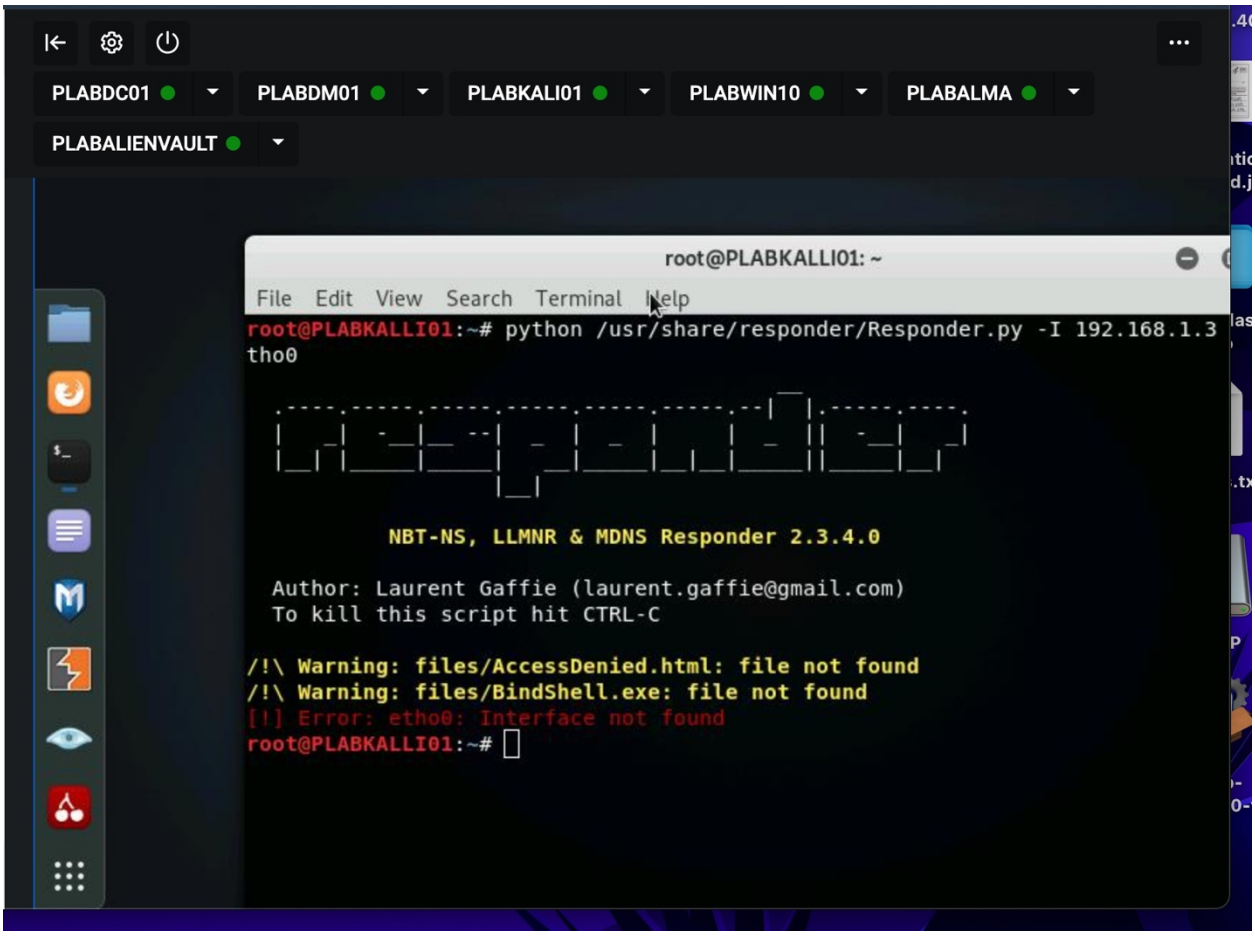


hping3 intranet --scan 22,80,443 -S



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

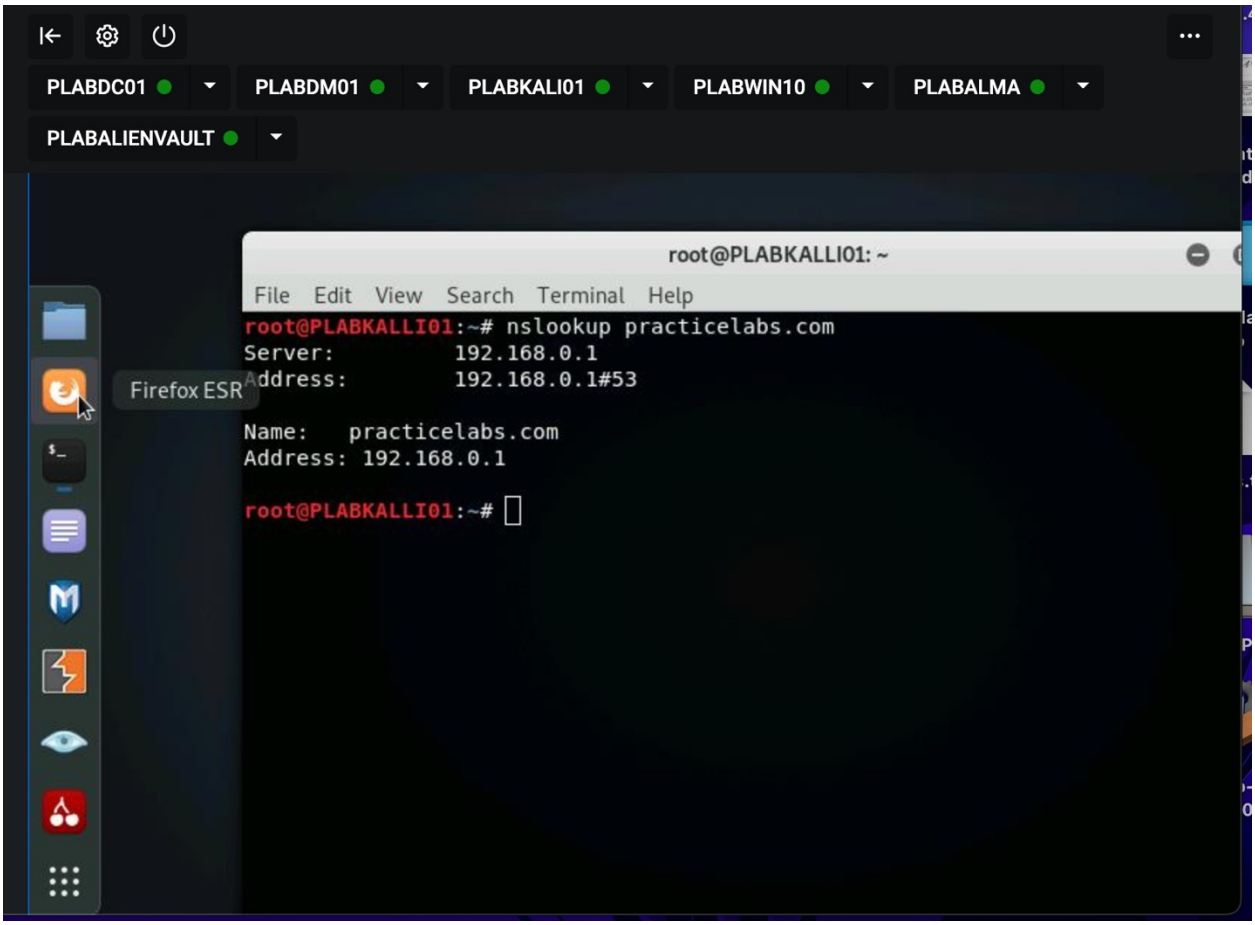
- IP history

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

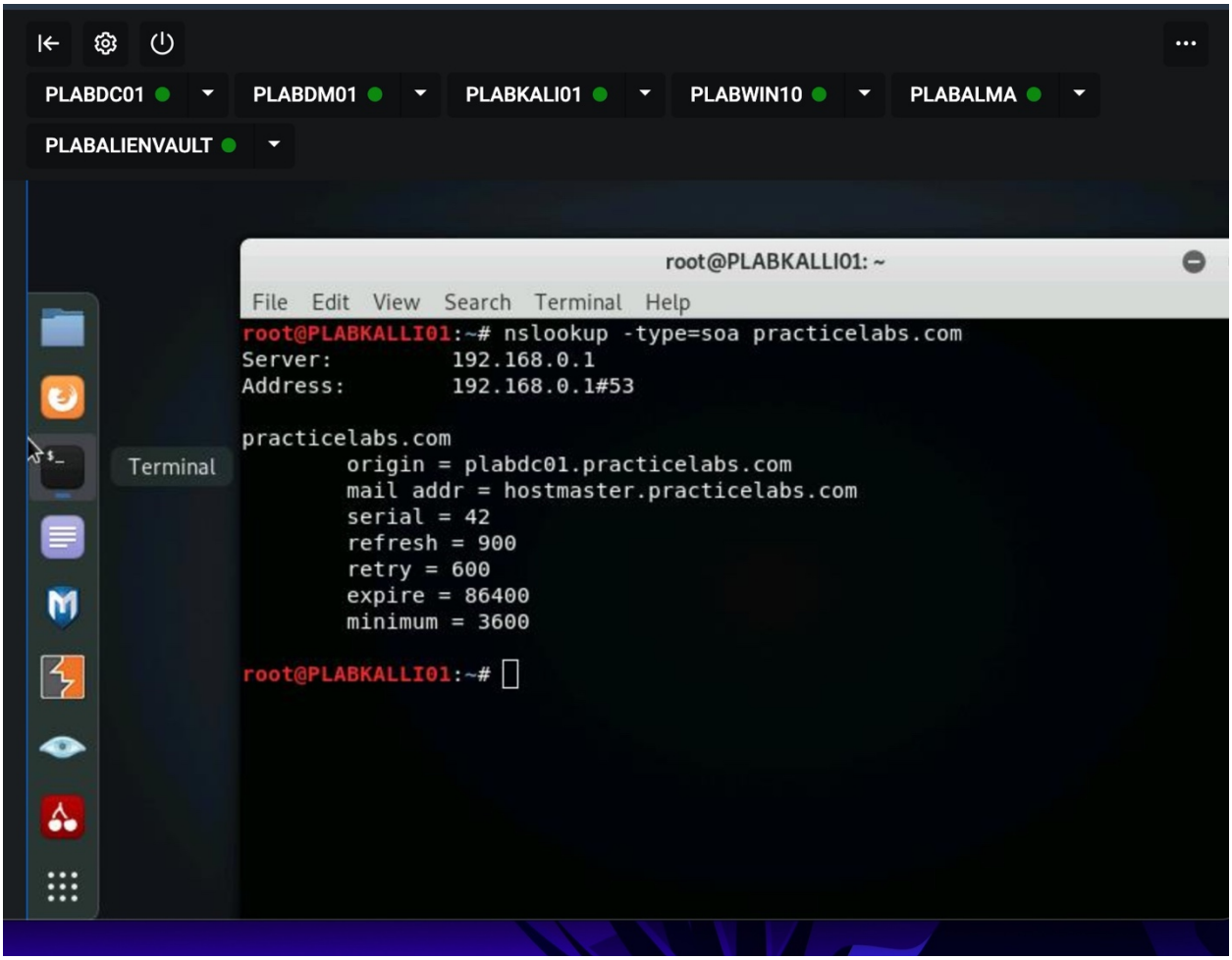
- Registrar history

Registrar History	5 registrars

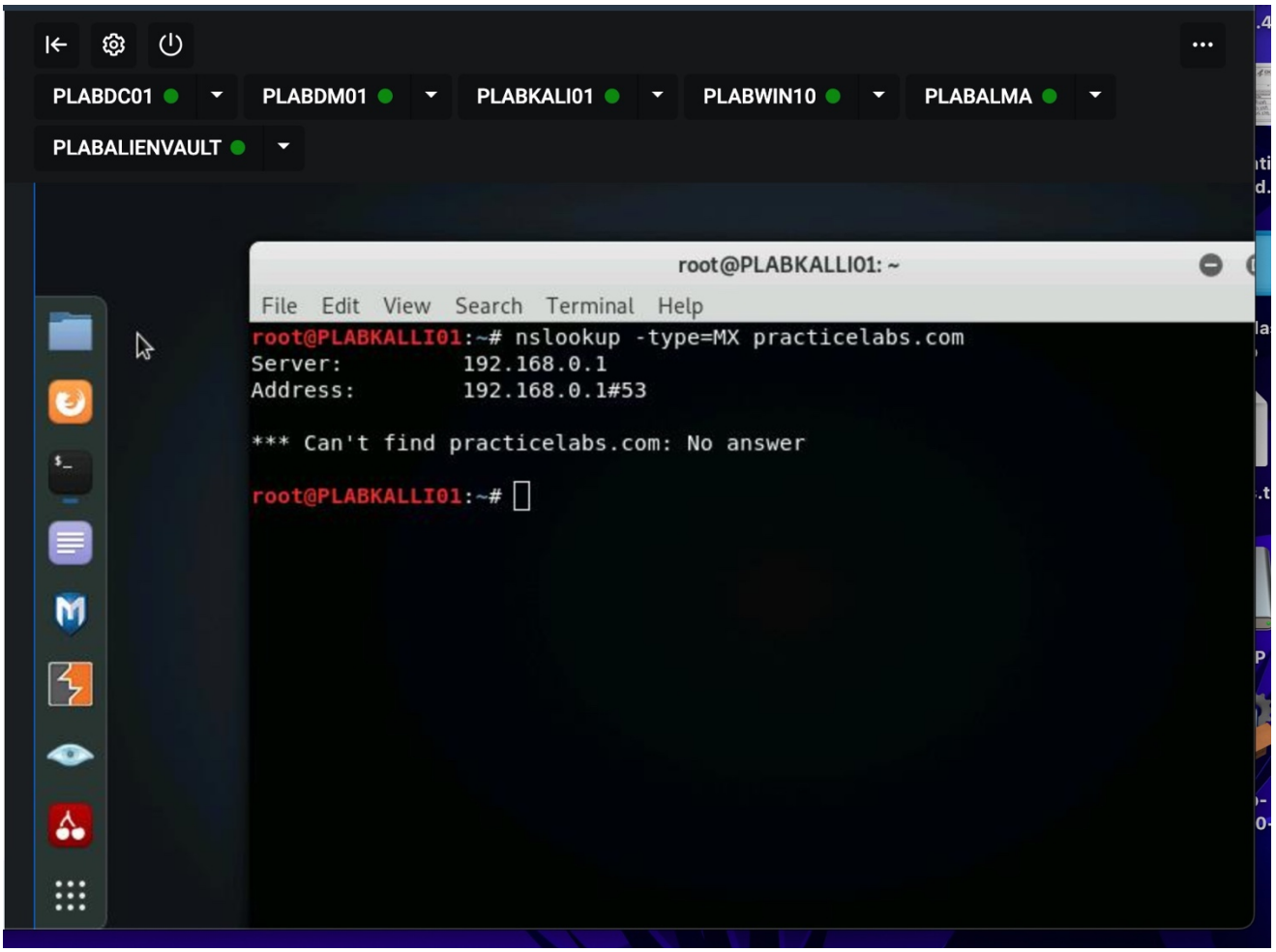
- Please the output screenshot of the following command here:
  nslookup practicelabs.com



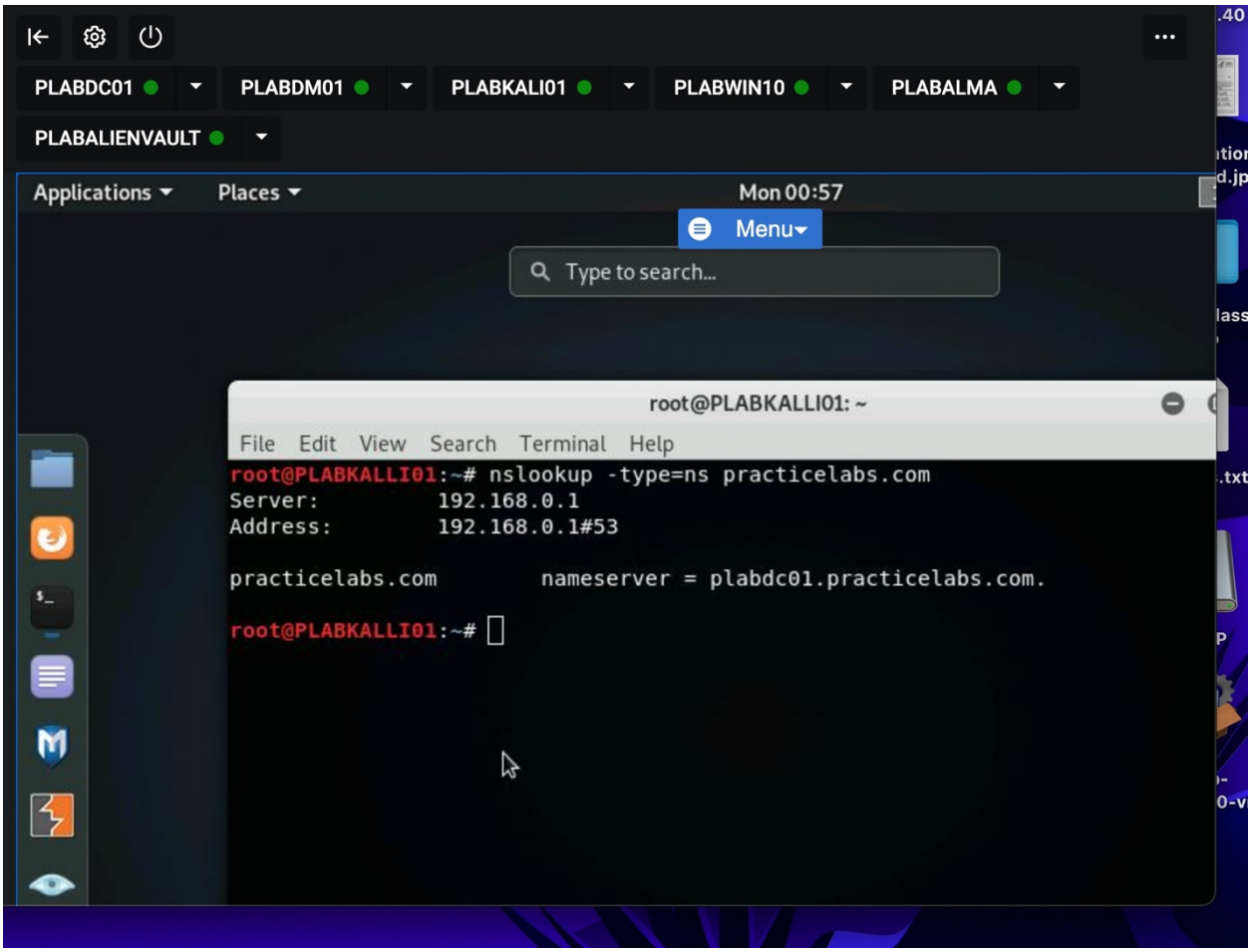
nslookup -type=soa practicelabs.com



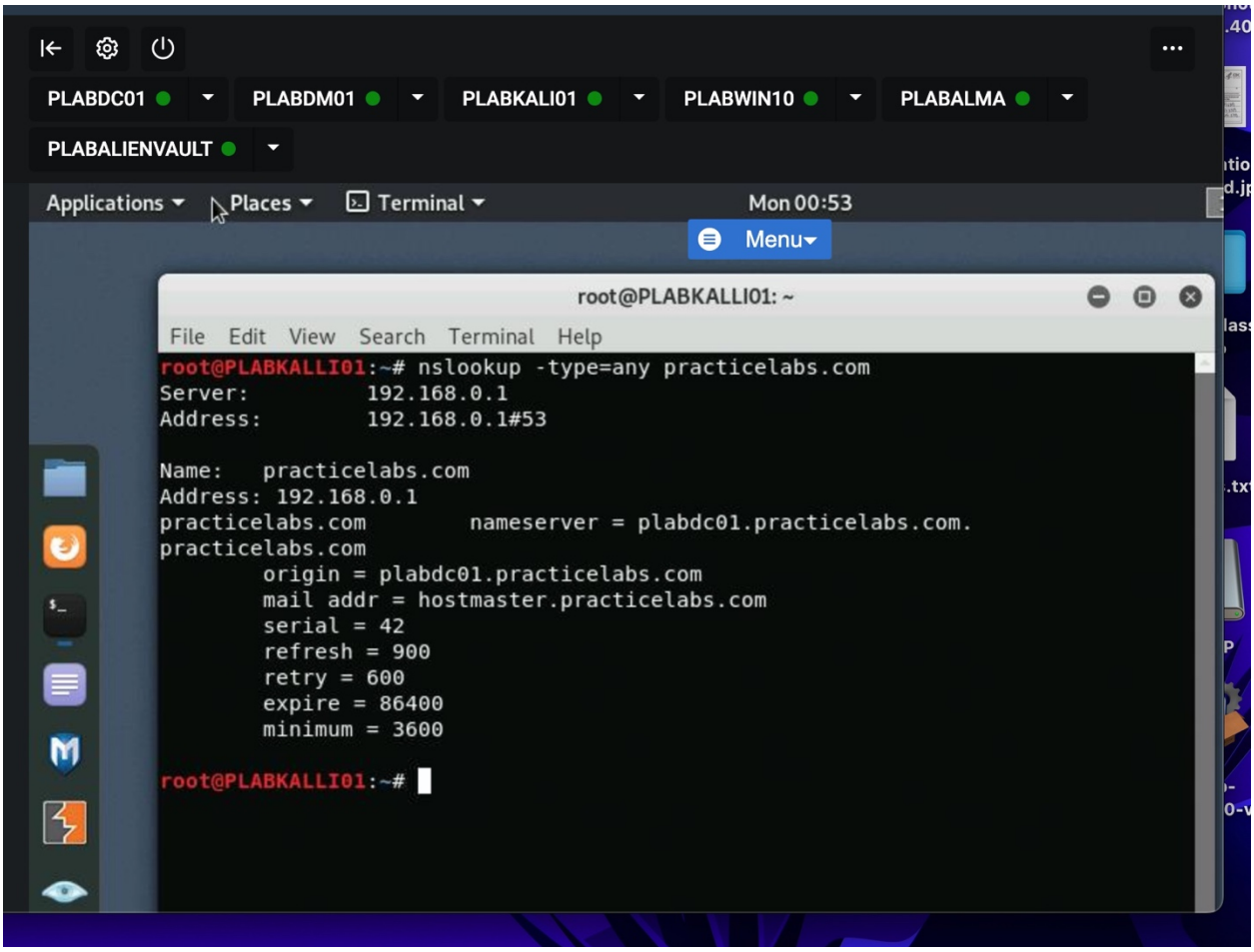
nslookup -type=MX practicelabs.com



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.