Assignment 3
Submitted by: Akib Muhammad (100981004)

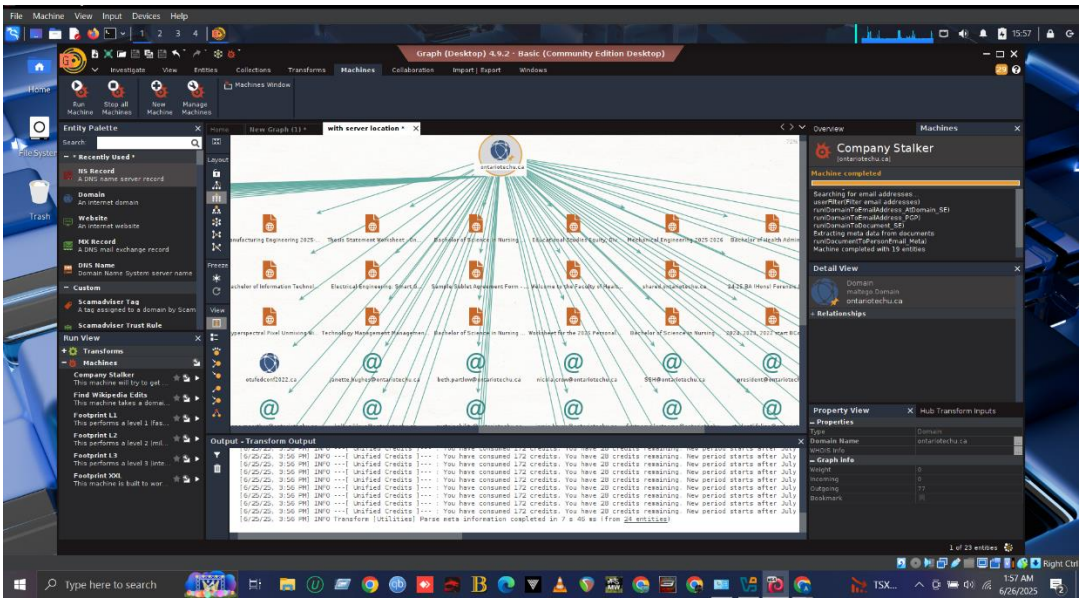
Task 1:

This lab is limited to collecting publicly available information. You are expected to do passive information collection only with publicly available information. You do not have permission to perform any active network scanning, enumeration, or vulnerability assessment in this lab.

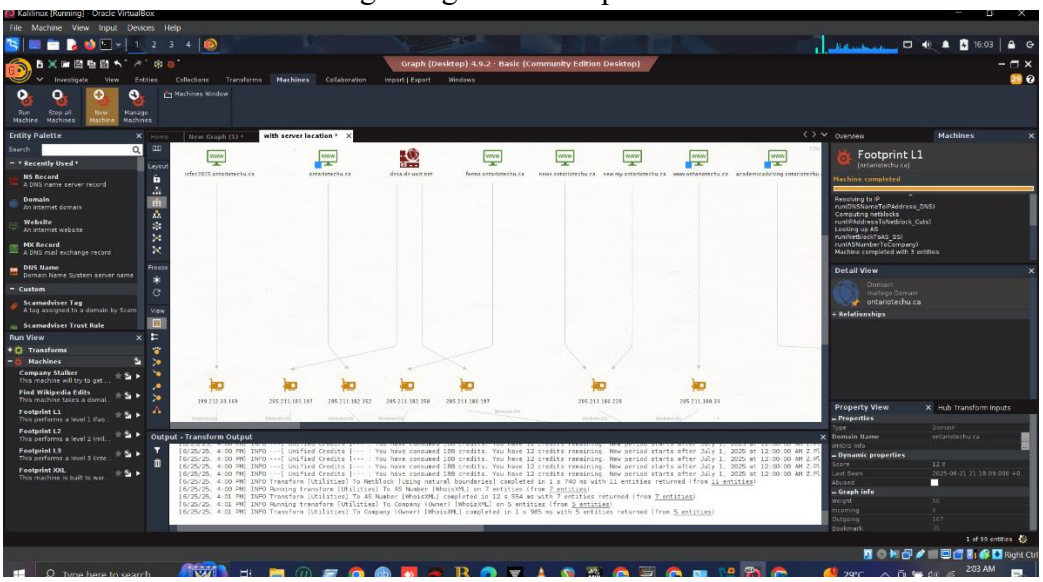
We will perform some passive reconnaissance tasks using Ontario Tech as our client.

1. On your KaliVM, use Maltego free edition to find information about your client organization. Provide 2 screenshots of your most important findings (e.g., Company Stalker, and URL To Network and Domain Information).

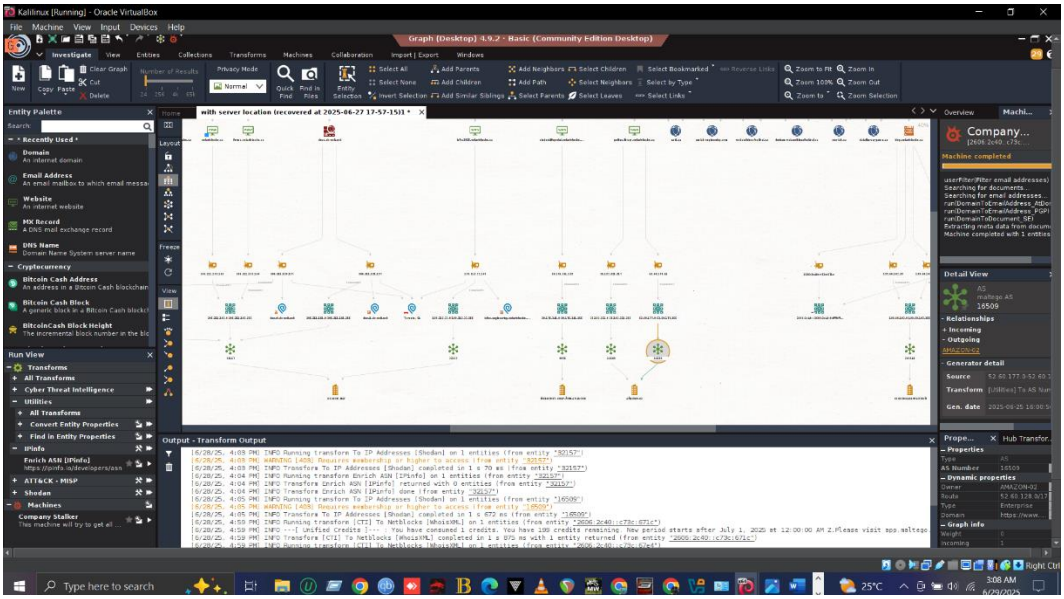
- Drag n Dropped the domain from entity palette and renamed it with client's
- Right clicked on the domain and under machines I ran the company stalker



- For url and domain info regarding IP ran footprint level 1

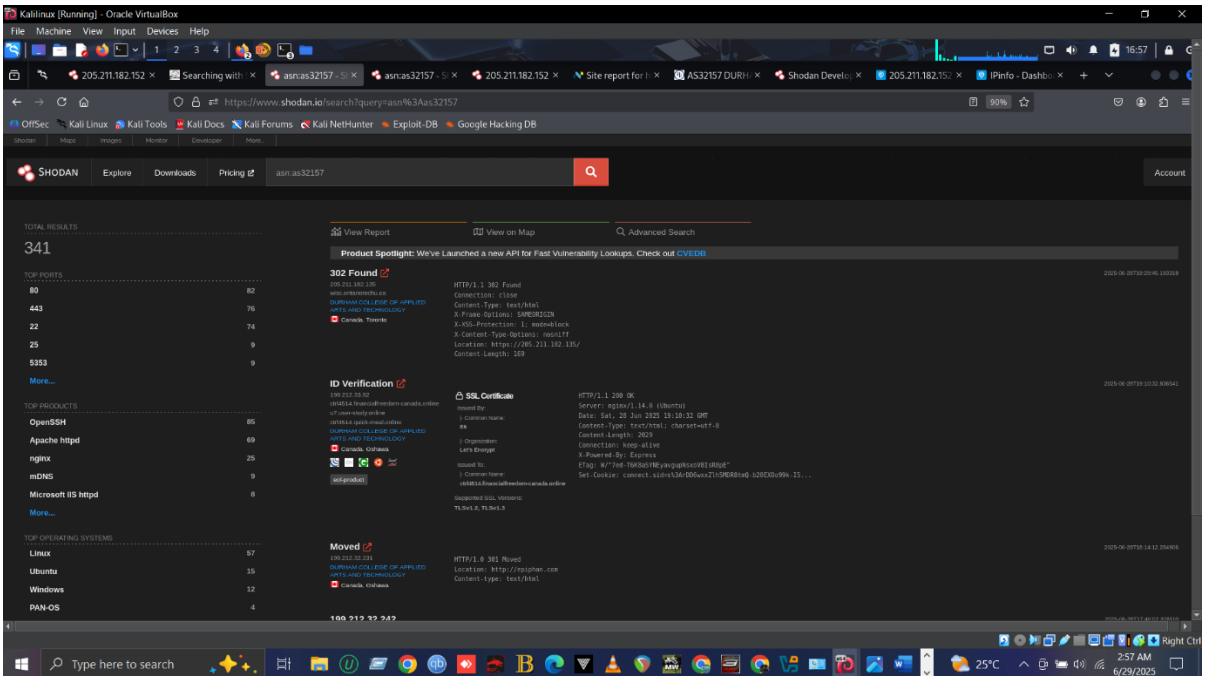


2. Find the asn (Autonomous System Number) of the client organization, and run it through Shodan. Provide 1 screenshot of your most important findings

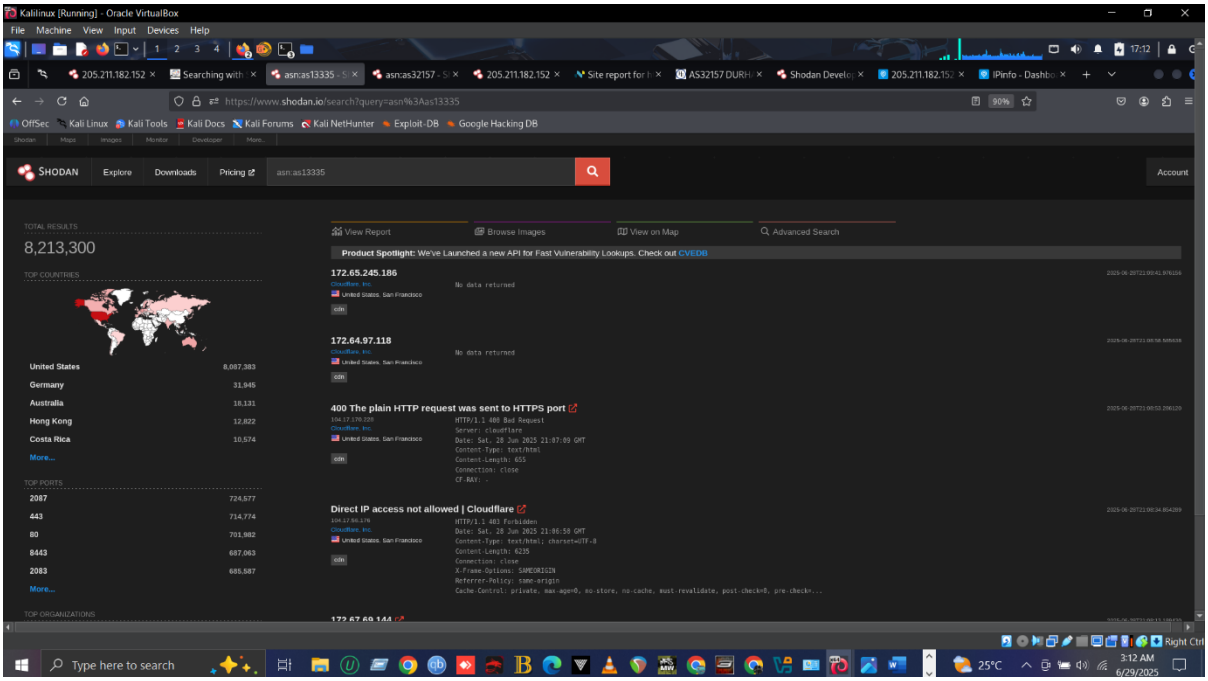


As directly running from maltego requires membership. I have used shodan.io to run the found ASN.

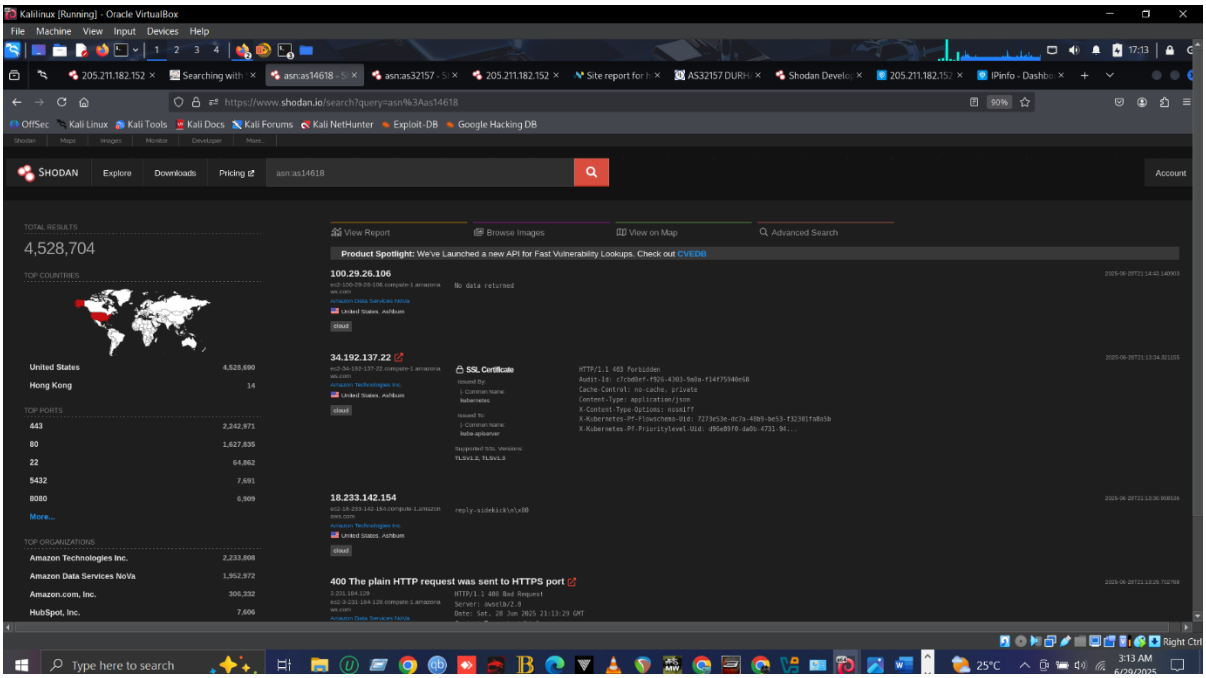
AS32157:



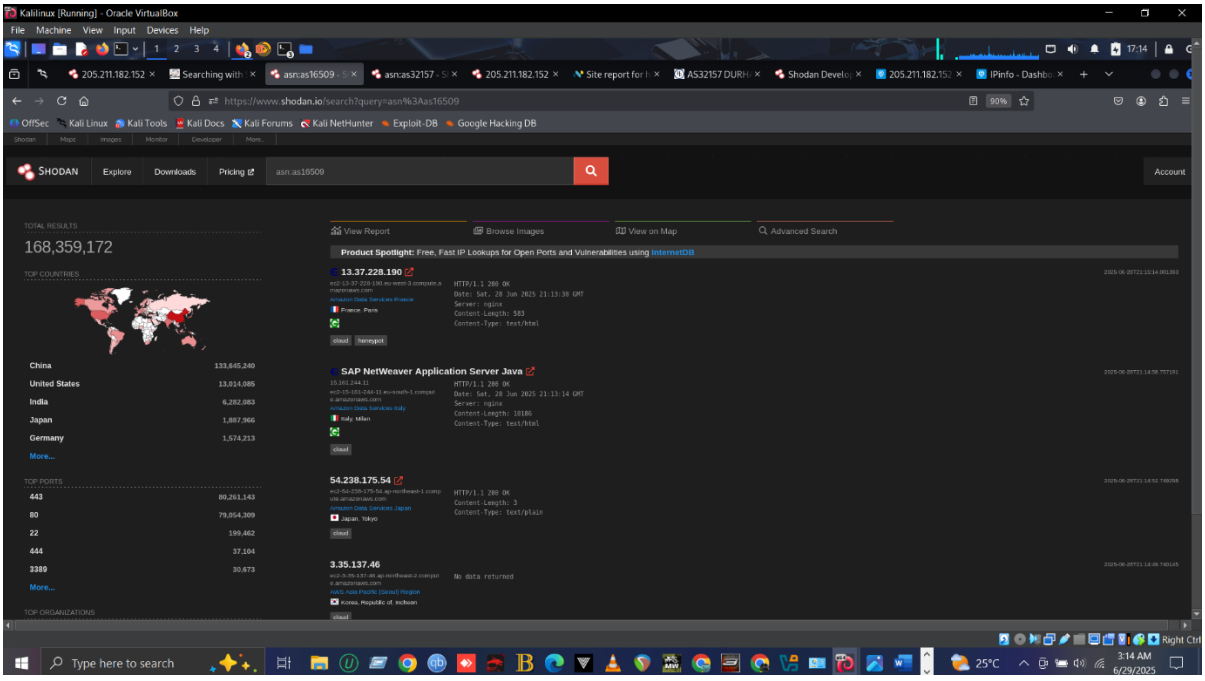
AS13335:



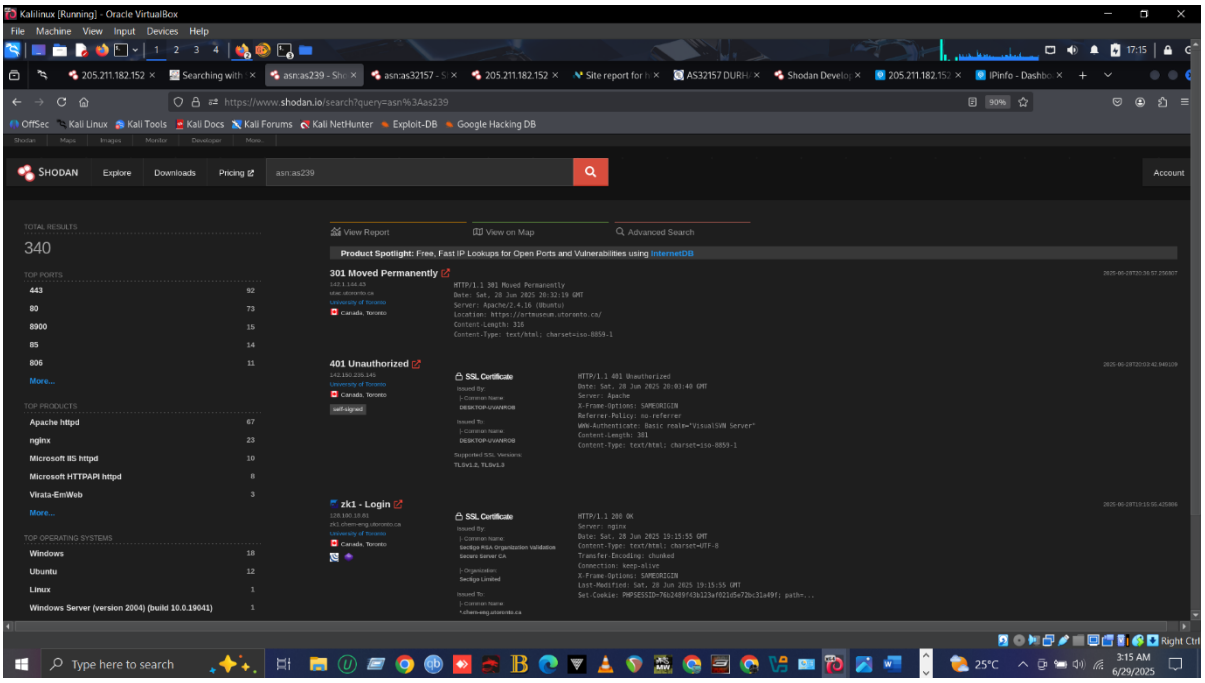
AS14618:



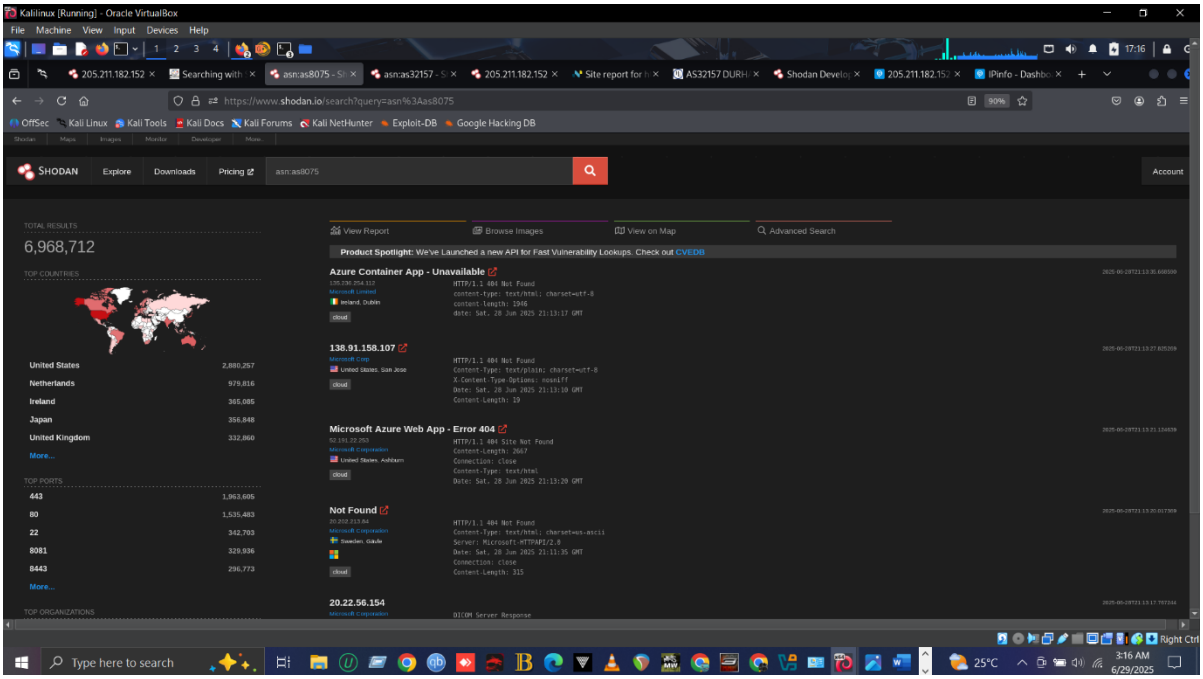
AS16509:



AS239: Permanently Moved!



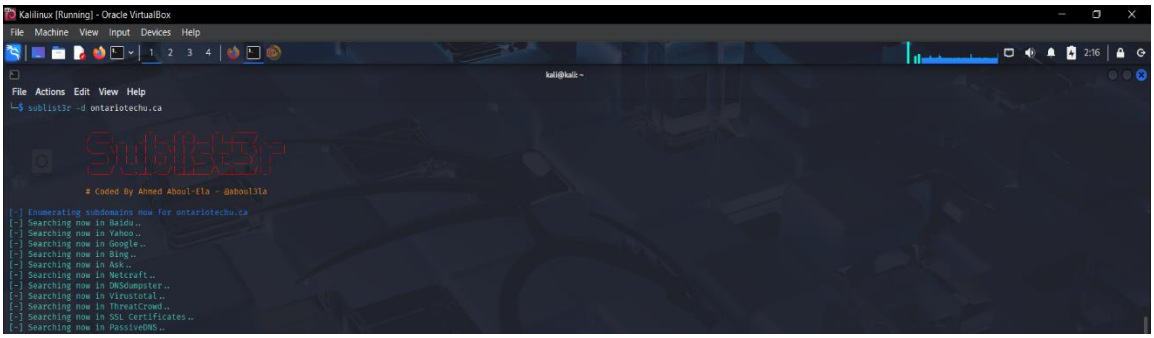
AS8075:

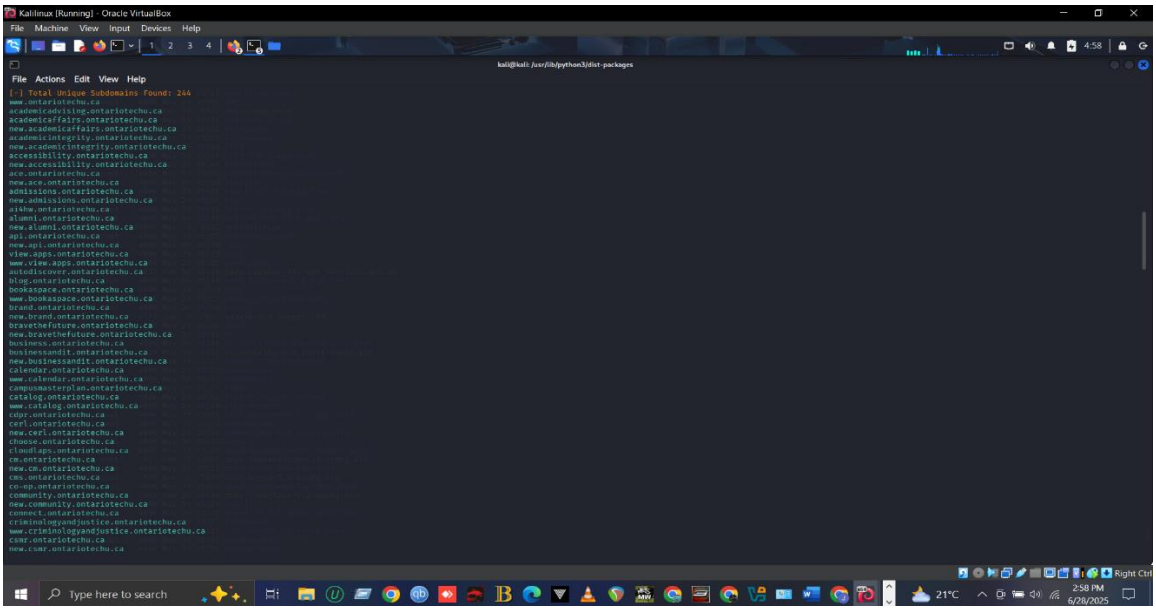


3. Use sublist3r to collect information on your client organization, and provide 1 screenshot of your findings. Include the command you ran in sublist3r.

- Opened up the Terminal on Desktop
- Try to check the version of sublist3r but didn't show nothing
- Ran the command **sudo apt install sublist3r** for installation
- Ran the command below for enumeration of the domain:

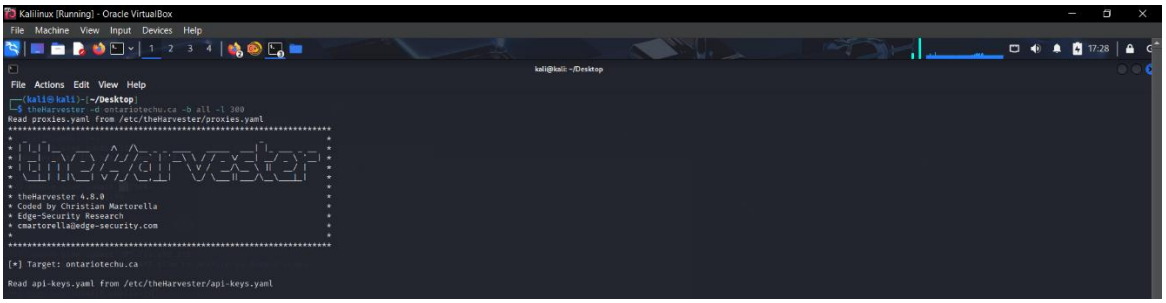
Command: sublist3r -d ontariotechu.ca



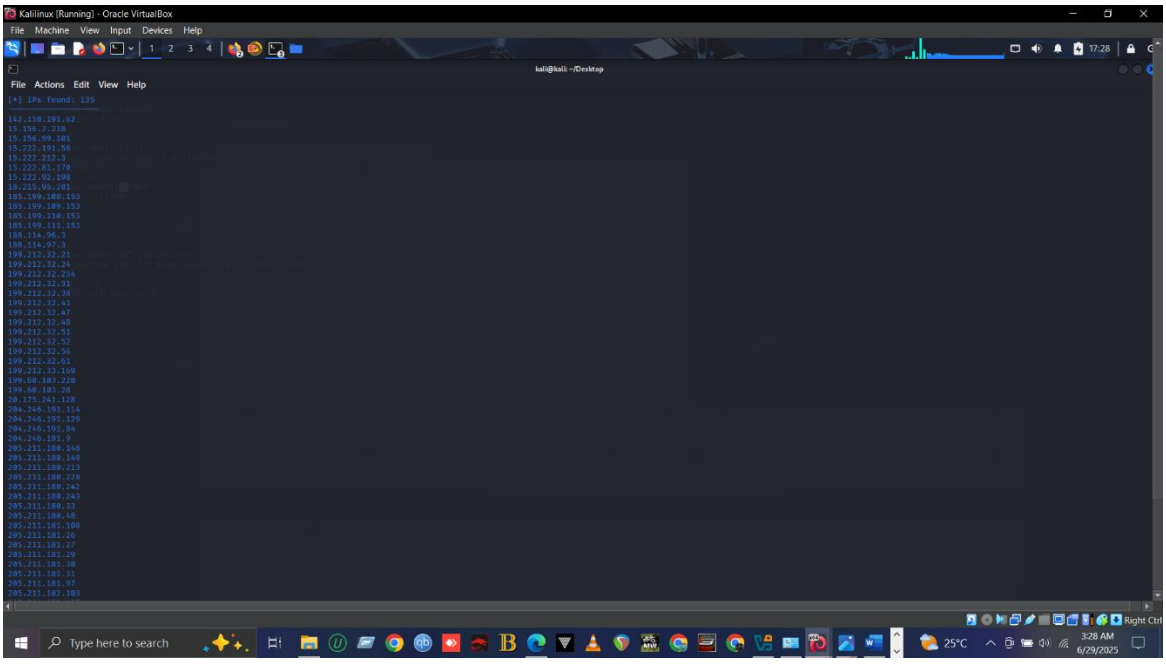


4. Use the Harvester to find collect information about your client organization. Provide 1 screenshot of the most important findings. Include the command you ran in the Harvester.
- theHarvester was pre-installed so ran the command below:

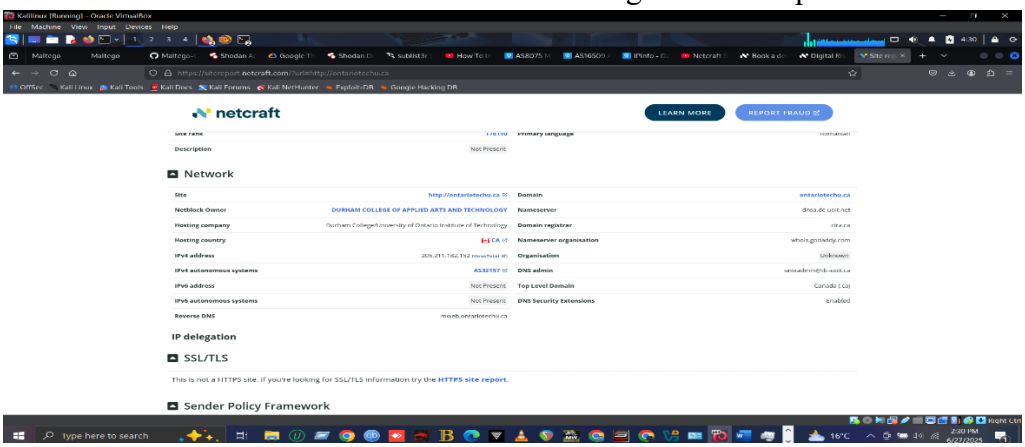
Command: theHarvester -d ontariotechu.ca -b all -l 300



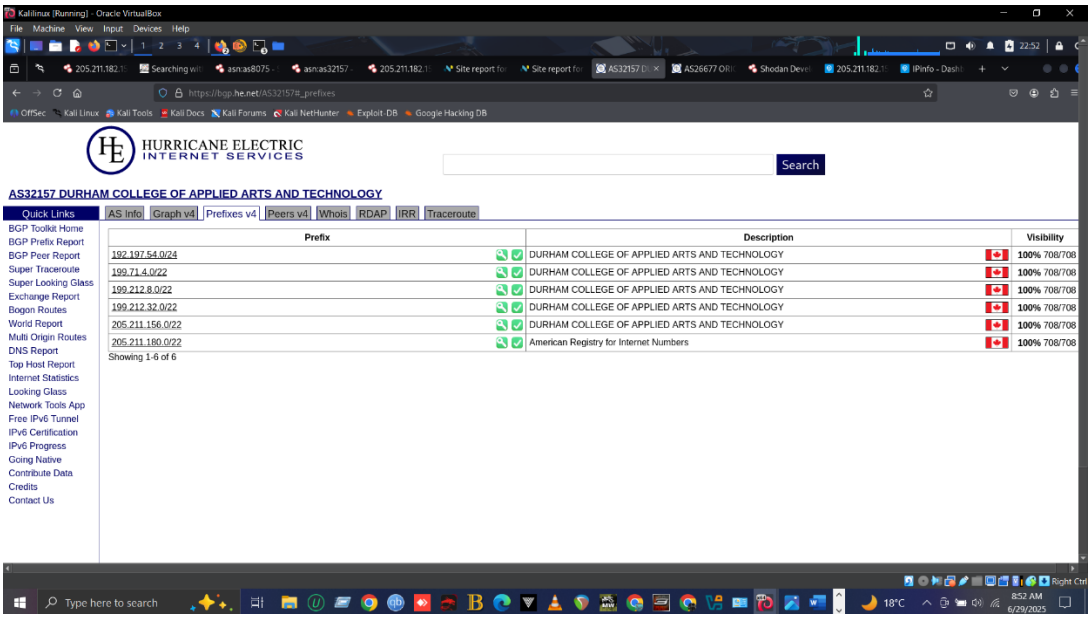
In my opinion the most important finding was the list of Ips. Where theHarvester found 135 of those.



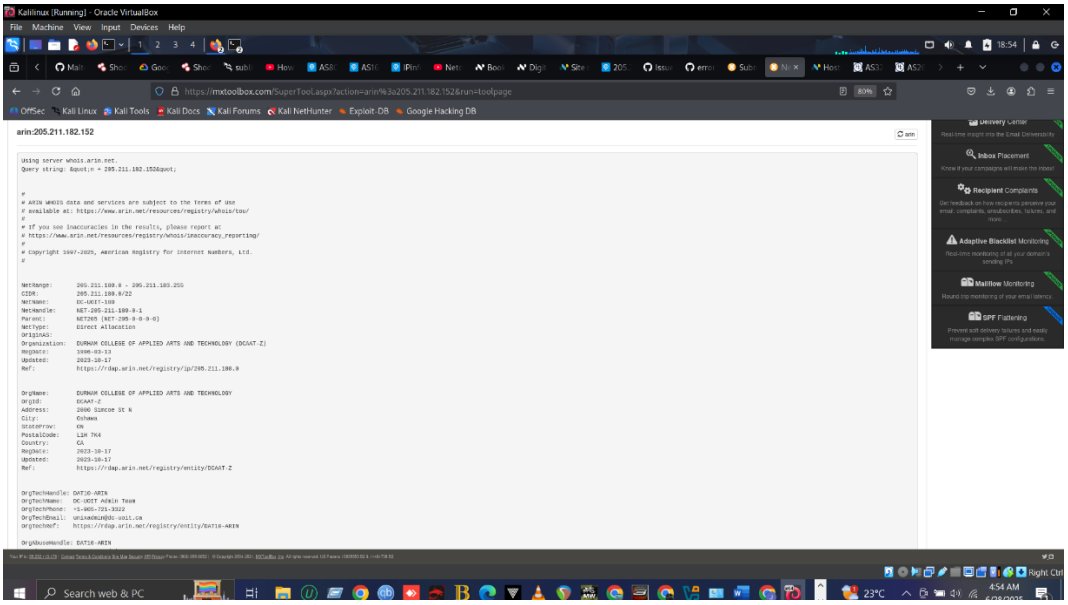
5. Use Netcraft to generate a site report of your client organization's website. Provide 1 screenshot of the generated report showing the organization's IP range.
Used the Netcraft but under the IP delegation there's no IP range of the organization mentioned.
- Launched firefox went to the netcraft search engine to lookup client



But if I click on the ASN it redirects to another link which is bgp.he.net where it shows the prefixes of ipv4:



Additionally, to get more clear range mxtoolbox was used:



Task 2:

Part 1 – Network Scanning

Step 1: Start the lab virtual machines

1. Start your Kali virtual machine (KaliVM), your Mestapolitable3 Windows Server 2008 machine (MS3WS2008), and Metaspolitable3 Ubuntu (MS3UBUNTU) machine.

2. Login to each machine, and take a note of each machine's IP address. Write the

IP addresses in your answer file.

Question 1 – What is the IP address of your KaliVM, MS3WS2008, and MS3UBUNTU? Write your answers in the answer file.

-> For KaliVM after running command ifconfig in terminal got the inet which is 192.168.100.5, For MS3WS2008 after running ipconfig in powershell it's 192.168.100.4, For Metasploitable3 Ubuntu it's after running command ifconfig in terminal got the inet 192.168.100.6.

3. On your KaliVM, change the terminal prompt to be your first name. You can do that using the following command:

(kali@kali)-[~] PS1='[`date "+%D"`] yourfirstname [`date "+%r"`] -[~]'
Your terminal should look similar to the screen below
- Launched terminal and ran the following command

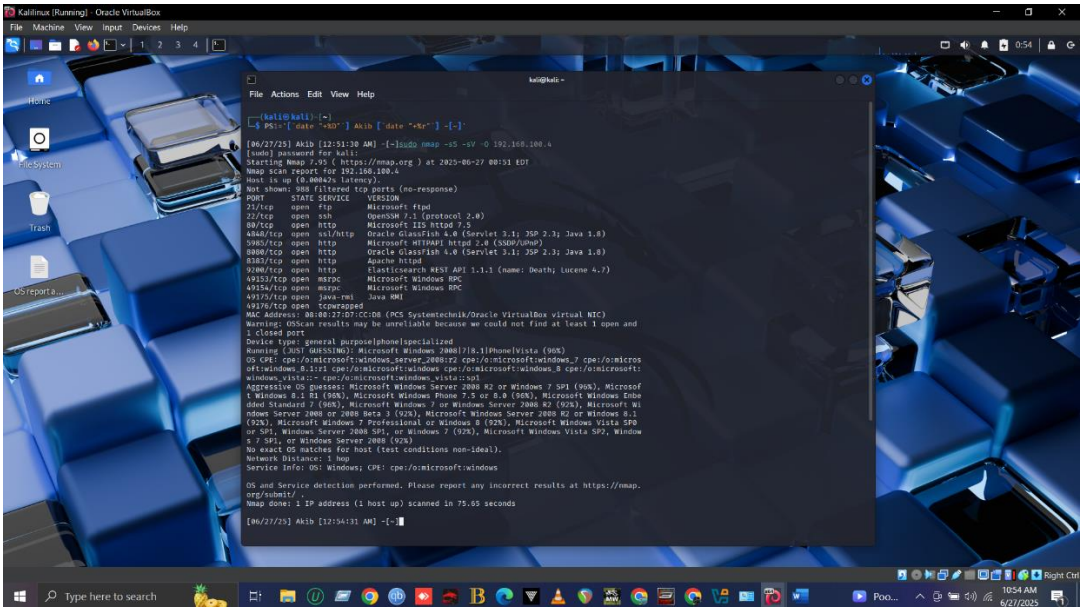
All commands in the following tasks are to be run on your KaliVM, targeting your MS3WS2008 and MS3UBUNTU VMs.
Step 2: Scanning MS3WS2008 using nmap
We will use nmap to scan our target machines and find the services running on them:

1. On your KaliVM, scan the MS3WS2008 machine, using the IP address you obtained in the previous step:

Take a screenshot to replace the one below, and place it under Screenshot#1 in the

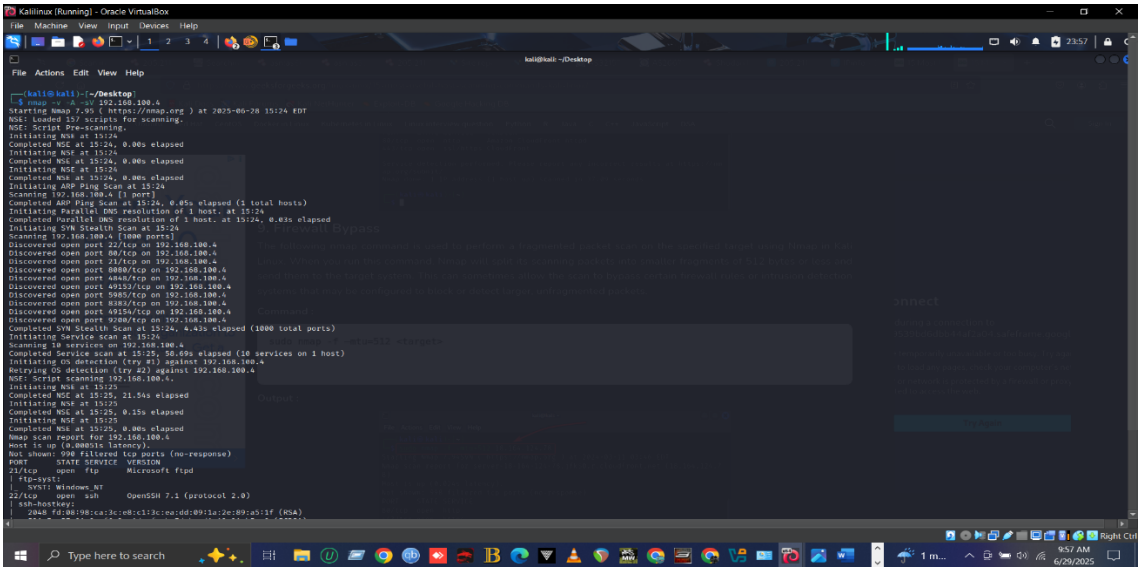
answer file.

- nmap was preinstalled so just launched terminal and ran the command below:
KaliVM# sudo nmap –sS –sV -O [target IP address]

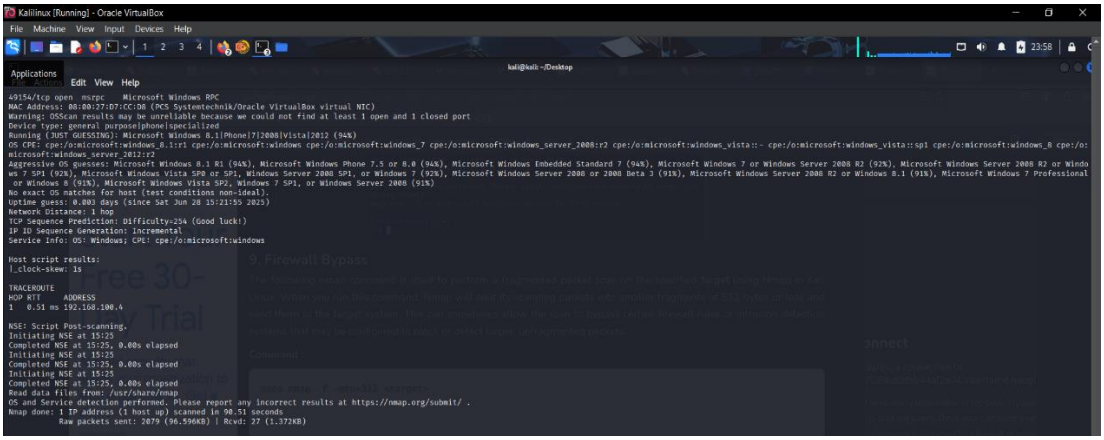


The command returned that the OSScan is not reliable as there's firewall active maybe that had something to do with this other than that there's a list of open ports which are 21, 22 80, 4848, 5985, 8000, 8383, 9200, 49153, 49154, 49175, 49176.

Additionally, when I was surfing through the tool documentation on kali.org I came up with a command which gives more detailed report about the open ports and the OS:
Command: sudo -v -A -sV 192.168.100.4



Os Report:



Based on the results of your scan, answer the following questions:

Question 2 - What is the OS reported by nmap of the target machine?
At first the Osscan guessed the os to be MS windows 2008 or 7 or 8.1 or phone or vista with a probability of 96%. Then there's os cpe(common platform enumeration) which included either ms windows server 2008:r2, 7, 8 , 8.1 or vista sp1. During the aggressive OS guesses it reported ms windows server 2008:r2 or windows 7 sp1 with a probability of 96% and there's other suggestions like ms windows phone 7.5, ms windows embedded standard 7, windows 2008 server beta 3.

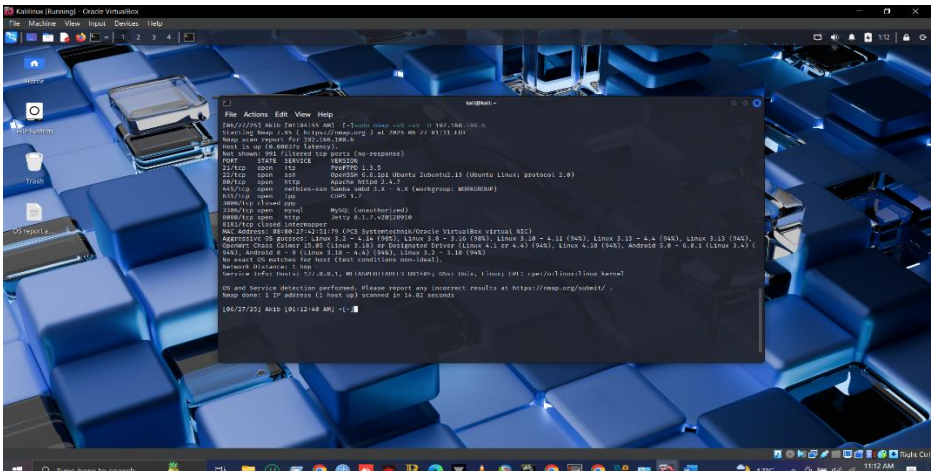
Question 3 - List 5 of the running services with their version and the ports they are running on.
- 1. Service name: Ssh, Version: OpenSSH 7.1(protocol 2.0), Port: 22
  2. Service name: http, Version: Microsoft IIS httpd 7.5, Port: 80
  3. Service name: ssl/http, Version: Oracle Glassfish 4.0(Servlet 3.1: JSP 2.3; Java 1.8), Port: 4848

4. Service name: msrpc, Version: Microsoft Windows RPC, Port: 49153
5. Service name: java-rmi, Version: Java RMI, Port: 49175

Step 3: Scanning MS3UBUNTU using nmap

Repeat Step 2 while targeting MS3UBUNTU machine.

Take a screenshot to replace the one below, and place it under Screenshot#2 in the answer file.
- Ran the same command with a different target ip



Based on the results of your scan, answer the following questions:

Question 4 - What is the OS reported by nmap of the target machine?
-> First of it didn't provide any initial guesses. It dived into the aggressive guess where it stated provided of 98% possibility of the os might be a Linux 3.2 - 4.14 machine. Furthermore, it also provided another 98% possibility on Linux 3.10 – 4.11. Other than that, there's 94% possibility on Linux 3.13 – 4.4, OpenWrt Chaos Calmer 15.05, Linux 4.1 or 4.4, 4.10, Android5.0 – 6.0.1 (Linux 3.4), Android 8 – 9 (Linux 3.18 – 4.4), Linux 3.2 – 3.10.

Question 5 - List 5 of the running services with their version and the ports they are running on.
-> 1. Service name: ssh, Version: OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0), Port: 22
-> 2. Service name: http, Version: Apache httpd 2.4.7, Port: 80
-> 3. Service name: netbios-ssn, Version: Samba smbd 3.x – 4.x (workgroup: WORKGROUP), Port: 445
-> 4. Service name: ipp, Version: CUPS 1.7, Port: 631
-> 5. Service name: mysql, Version: MySQL(unauthorized), Port: 3306

End of Part 1 – Scanning Network

Part 2 - Enumeration

Step 1: Enumerating users with snmp_enumusers

In this task, we will use the msfconsole on your KaliVM to run snmp_enumusers

script.

1- Start an msf console, and change the console prompt:
KaliVM# msfconsole

Msf6> set PROMPT %yel%L %grn%T %grnyourfirstname
- Launched the terminal ran msfconsole and ran the following set prompt command to change the interface name
- Ran the commands below to get enumusers script

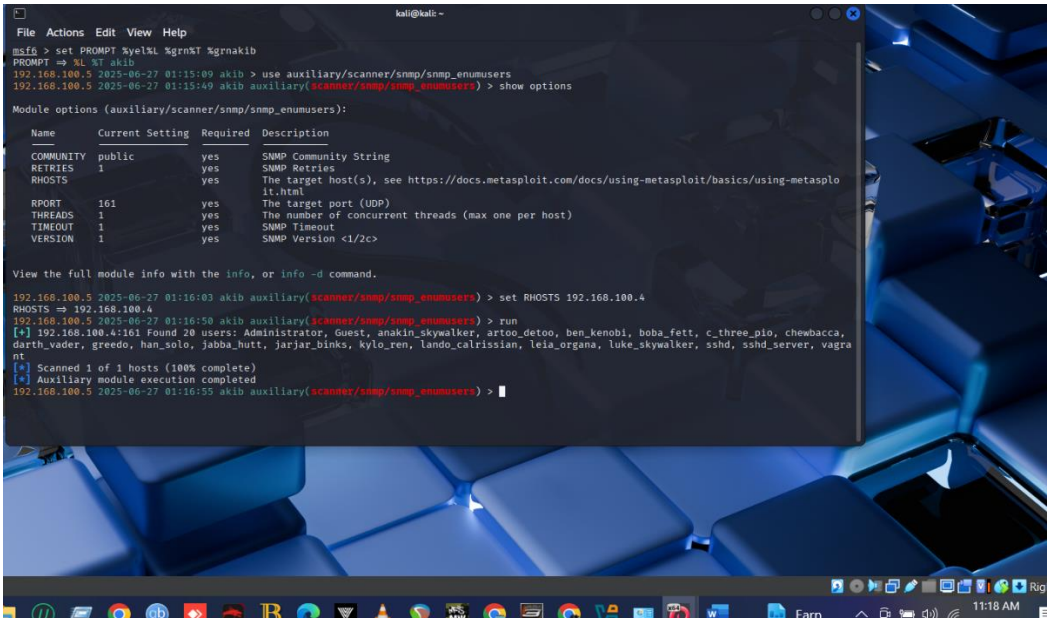
2- To use the snmp_enumusers script, run the following commands using MS3WS2008 as your target machine:
msfconsole# use auxiliary/scanner/snmp/snmp_enumusers

msfconsole# show options

msfconsole# set RHOSTS [target IP address]

msfconsole# run

Take a screenshot to replace the one below, and place it under Screenshot#3 in the answer file.



Question 6 - List 3 user accounts that were found by the

snmp_enumusers script Exit msfconsole.

-> User account 1 -> Administrator
-> User account 2 -> Anakin_skywalker
-> User account 3 -> c_three_pio

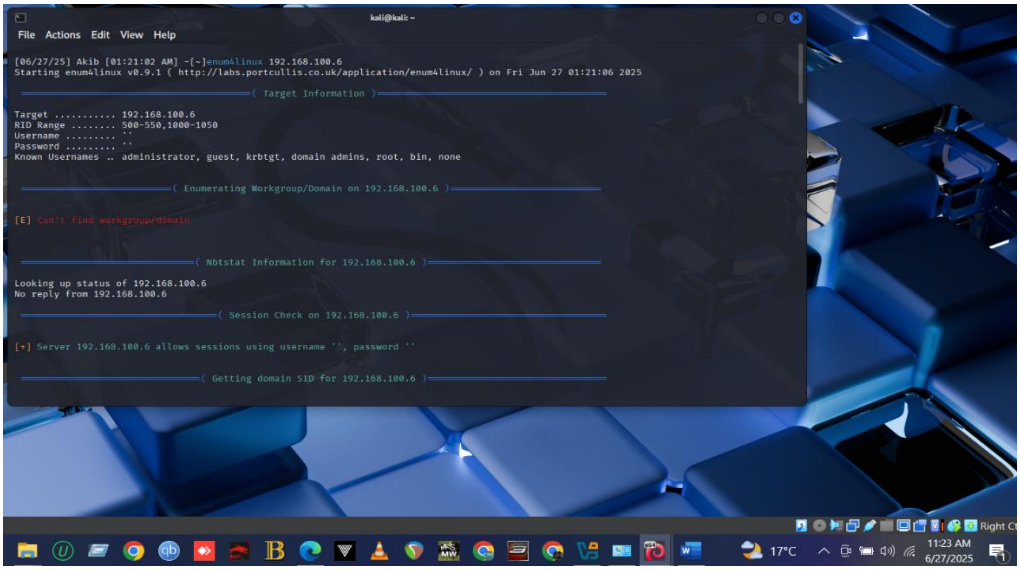
Step 2: Repeat Step 1 while targeting MS3UBUNTU machine, but use

enum4linux command instead running the following command in the

kali linux terminal:

KaliVM# enum4linux
- Exit msfconsole and ran enum4linux with different target IP
- After waiting couple of minutes it returned back RID Range, Usernames, Enumerated logon info and group lists that are builtin

Take a screenshot to replace the one below, and place it under Screenshot#4 in the answer file.



Question 7 - List 3 user accounts that were found by the enum4linux script

-> Known users from domain: administrator, krbtgt, root
-> Enumerated logon accounts username: nobody, none, Chewbacca
-> Enumerated groups: administrators, power users, server operators

Submission Guidelines: Submit a report explaining, in your own words, the steps you used to get your results. Students must attach screenshots.