

Submitted by: Akib Muhammad (100981004)

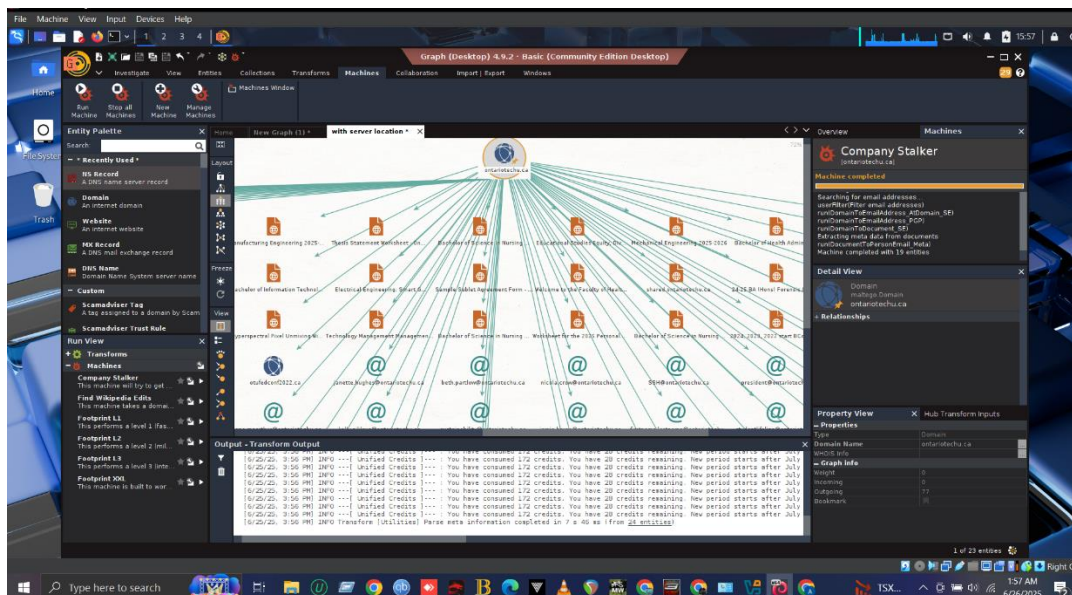
### Task 1:

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.

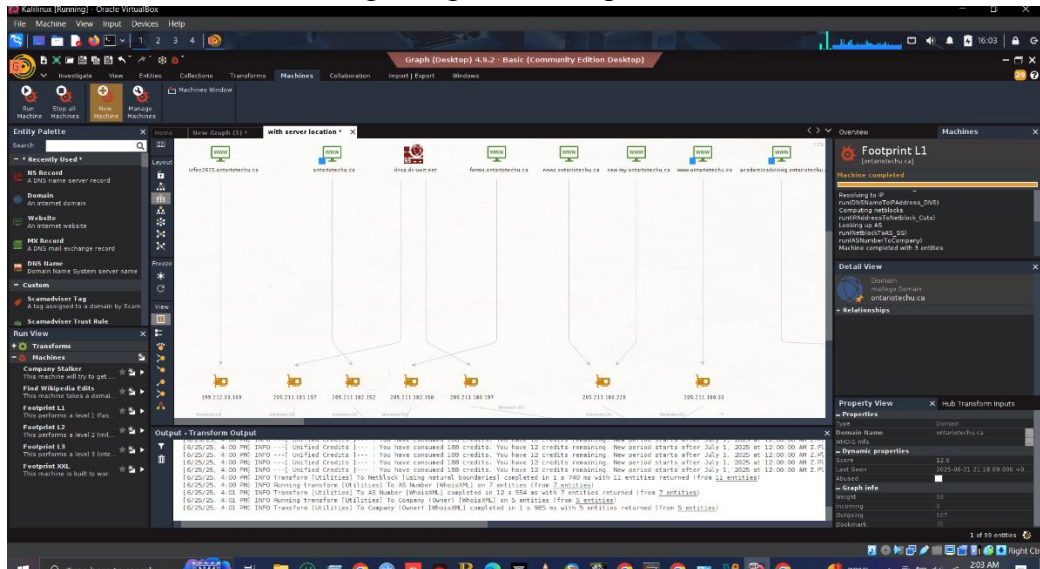
We will perform some passive reconnaissance tasks using Ontario Tech as our client.

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).

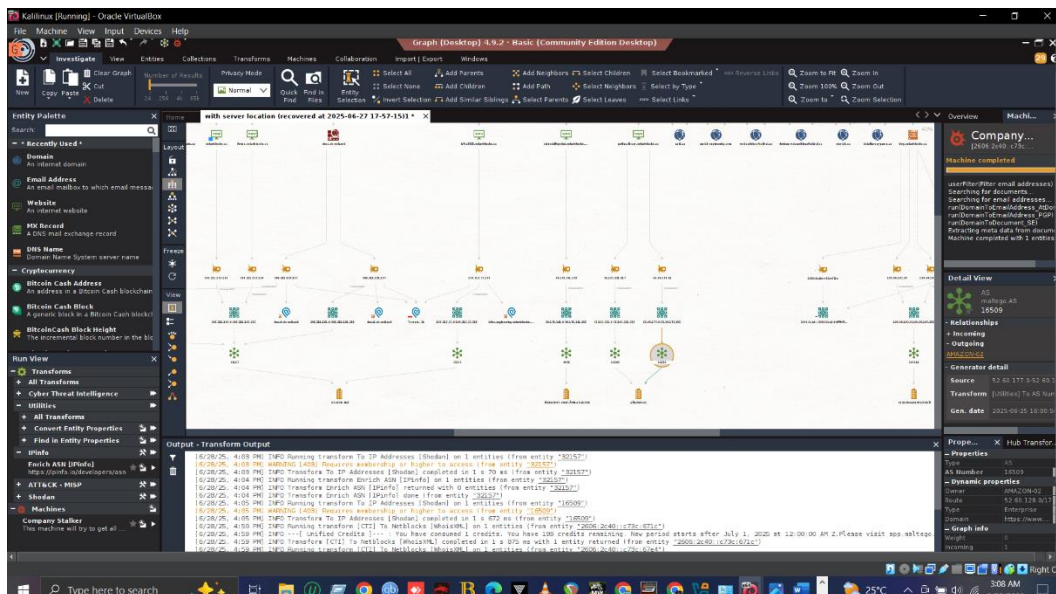
- Drag n Dropped the domain from entity palette and renamed it with client's
- Right clicked on the domain and under machines I ran the company stalker



- 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:

The screenshot shows a Kali Linux virtual machine running Oracle VM VirtualBox. The browser window displays the Shodan search engine results for the query 'asn:as32157'. The search results show 341 total results. The left sidebar lists top ports (80, 443, 22, 25, 5353) and top products (OpenSSH, Apache httpd, nginx, mDNS, Microsoft IIS httpd). The main content area shows a list of search results, including a 'Product Spotlight' for a new API for Fast Vulnerability Lookups. The bottom of the screen shows the Windows taskbar with various icons and the system clock.

TOP PORTS	Count
80	82
443	76
22	74
25	9
5353	9

TOP PRODUCTS	Count
OpenSSH	85
Apache httpd	69
nginx	25
mDNS	9
Microsoft IIS httpd	8

TOP OPERATING SYSTEMS	Count
Linux	87
Ubuntu	16
Windows	12
PAN-OS	4

## AS13335:

The screenshot shows a Kali Linux virtual machine running Oracle VM VirtualBox. The browser window displays the Shodan search engine results for the query 'asn:as13335'. The search results show 8,213,300 total results. The left sidebar lists top countries (United States, Germany, Australia, Hong Kong, Costa Rica) and top ports (2087, 443, 80, 8443, 2083). The main content area shows a list of search results, including a 'Product Spotlight' for a new API for Fast Vulnerability Lookups. The bottom of the screen shows the Windows taskbar with various icons and the system clock.

TOP COUNTRIES	Count
United States	6,087,382
Germany	33,945
Australia	18,131
Hong Kong	12,822
Costa Rica	10,574

TOP PORTS	Count
2087	724,577
443	714,774
80	701,982
8443	687,063
2083	685,587

## AS14618:

The screenshot shows a Kali Linux virtual machine running Oracle VM VirtualBox. The browser window displays the Shodan search engine results for the query 'asn:as14618'. The search results show 4,528,704 total results. The top countries are United States (4,528,690) and Hong Kong (14). The top ports are 443 (2,242,871), 80 (1,627,835), 22 (61,862), 5432 (7,691), and 8080 (6,969). The top organizations are Amazon Technologies Inc. (2,233,808), Amazon Data Services India (1,862,872), Amazon.com, Inc. (306,332), and HubSpot, Inc. (7,606).

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

**100.29.26.106**  
asn:100.29.26.106 company:1 amazon  
amazon Data Services India  
United States, Ashburn  
[Details]

**34.162.137.22**  
asn:34.162.137.22 company:1 amazon  
amazon Technologies Inc.  
United States, Ashburn  
[Details]

**16.222.142.154**  
asn:16.222.142.154 company:1 amazon  
amazon Technologies Inc.  
United States, Ashburn  
[Details]

**400 The plain HTTP request was sent to HTTPS port**  
asn:205.211.182.152  
asn:205.211.182.152 company:1 amazon  
amazon Data Services India  
[Details]

## AS16509:

The screenshot shows a Kali Linux virtual machine running Oracle VM VirtualBox. The browser window displays the Shodan search engine results for the query 'asn:as16509'. The search results show 168,359,172 total results. The top countries are China (133,646,240), United States (13,014,085), India (6,282,083), Japan (1,867,366), and Germany (1,574,213). The top ports are 443 (80,161,143), 80 (79,064,309), 22 (199,462), 444 (37,104), and 3389 (30,873). The top organizations are SAP NetWeaver Application Server Java (15,361,244.1), Amazon.com, Inc. (15,361,244.1), Amazon Data Services Japan (15,361,244.1), and Amazon Data Services India (15,361,244.1).

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using [InternetDB](#)

**13.37.228.190**  
asn:13.37.228.190 company:3 amazon  
amazon Data Services India  
France, Paris  
[Details]

**SAP NetWeaver Application Server Java**  
asn:15.361.244.1  
asn:15.361.244.1 company:1 amazon  
amazon Data Services India  
Italy, Milan  
[Details]

**54.238.175.54**  
asn:54.238.175.54 company:1 amazon  
amazon Data Services Japan  
Japan, Tokyo  
[Details]

**3.35.137.46**  
asn:3.35.137.46 company:1 amazon  
amazon Data Services India  
India, Republic of, New Delhi  
[Details]

# AS239: Permanently Moved!

KaliLinux (Running) - Oracle VirtualBox

File Machine View Input Devices Help

205.211.182.152 x Searching with: x asnsas239 - S x asnsas32157 - S x 205.211.182.152 x Site report for: x AS32157 DURH x Shodan Develo x 205.211.182.152 x IPinfo - Dashbo x

https://www.shodan.io/search?query=asn%3Aas239

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

SHODAN Explore Downloads Pricing 8371 as239 Account

TOTAL RESULTS: 340

View Report View on Map Advanced Search

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using [InternalDB](#)

**301 Moved Permanently**

142.130.235.245  
University of Toronto  
Canada, Toronto  
[Link]

HTTP/1.1 301 Moved Permanently  
Date: Sat, 28 Jun 2025 20:32:19 GMT  
Server: Apache/2.4.18 (Ubuntu)  
Location: https://repositorio.utoronto.ca/  
Content-Length: 128  
Content-Type: text/html; charset=utf-8

**401 Unauthorized**

142.130.235.245  
University of Toronto  
Canada, Toronto  
[Link]

SSL Certificate  
HTTP/1.1 401 Unauthorized  
Date: Sat, 28 Jun 2025 20:33:40 GMT  
Server: Apache/2.4.18 (Ubuntu)  
X-Frame-Options: SAMEORIGIN  
Referer-Policy: no-referrer  
WWW-Authenticate: Basic realm="VirtualWeb Server"  
Content-Length: 361  
Content-Type: text/html; charset=utf-8

**zki - Login**

128.130.18.85  
JPL Information Systems  
Canada, Toronto  
[Link]

SSL Certificate  
HTTP/1.1 200 OK  
Date: Sat, 28 Jun 2025 20:33:40 GMT  
Server: Apache/2.4.18 (Ubuntu)  
X-Frame-Options: SAMEORIGIN  
Referer-Policy: no-referrer  
WWW-Authenticate: Basic realm="VirtualWeb Server"  
Content-Length: 361  
Content-Type: text/html; charset=utf-8

TOP PORTS

Port	Count
443	92
80	73
8900	15
85	14
806	11

More...

TOP PRODUCTS

Product	Count
Apache httpd	67
nginx	23
Microsoft IIS httpd	10
Microsoft HTTPAPI httpd	8
Vitrina-EmWeb	3

More...

TOP OPERATING SYSTEMS

OS	Count
Windows	18
Ubuntu	12
Linux	1
Windows Server (version 2004) (build 10.0.19041)	1

# AS8075:

KaliLinux (Running) - Oracle VirtualBox

File Machine View Input Devices Help

205.211.182.152 x Searching with: x asnsas8075 - S x asnsas32157 - S x 205.211.182.152 x Site report for: x AS32157 DURH x Shodan Develo x 205.211.182.152 x IPinfo - Dashbo x

https://www.shodan.io/search?query=asn%3Aas8075

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

SHODAN Explore Downloads Pricing asnsas8075 Account

TOTAL RESULTS: 6,968,712

View Report Browse Images View on Map Advanced Search

Product Spotlight: We've launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

**Azure Container App - Unavailable**

138.130.154.132  
Microsoft Corporation  
Ireland, Dublin  
[Link]

HTTP/1.1 404 Not Found  
Content-Type: text/html; charset=utf-8  
Content-Length: 2946  
Date: Sat, 28 Jun 2025 21:13:17 GMT

**138.91.158.107**

Microsoft Corporation  
United States, San Jose  
[Link]

HTTP/1.1 404 Not Found  
Content-Type: text/html; charset=utf-8  
X-Content-Type-Options: nosniff  
Date: Sat, 28 Jun 2025 21:13:18 GMT  
Content-Length: 37

**Microsoft Azure Web App - Error 404**

138.130.154.132  
Microsoft Corporation  
Ireland, Dublin  
[Link]

HTTP/1.1 404 Site Not Found  
Content-Length: 3647  
Connection: close  
Content-Type: text/html  
Date: Sat, 28 Jun 2025 21:13:29 GMT

**Not Found**

138.130.154.132  
Microsoft Corporation  
Ireland, Dublin  
[Link]

HTTP/1.1 404 Not Found  
Content-Type: text/html; charset=utf-8  
Server: Microsoft-HTTPAPI/2.0  
Date: Sat, 28 Jun 2025 21:13:35 GMT  
Connection: close  
Content-Length: 315

**20.22.56.154**

Microsoft Corporation  
01:01 Server Response  
[Link]

TOP COUNTRIES

Country	Count
United States	2,880,257
Netherlands	979,816
Ireland	385,085
Japan	366,848
United Kingdom	332,368

More...

TOP PORTS

Port	Count
443	1,963,695
80	1,535,483
22	342,793
8081	329,936
8443	296,773

More...

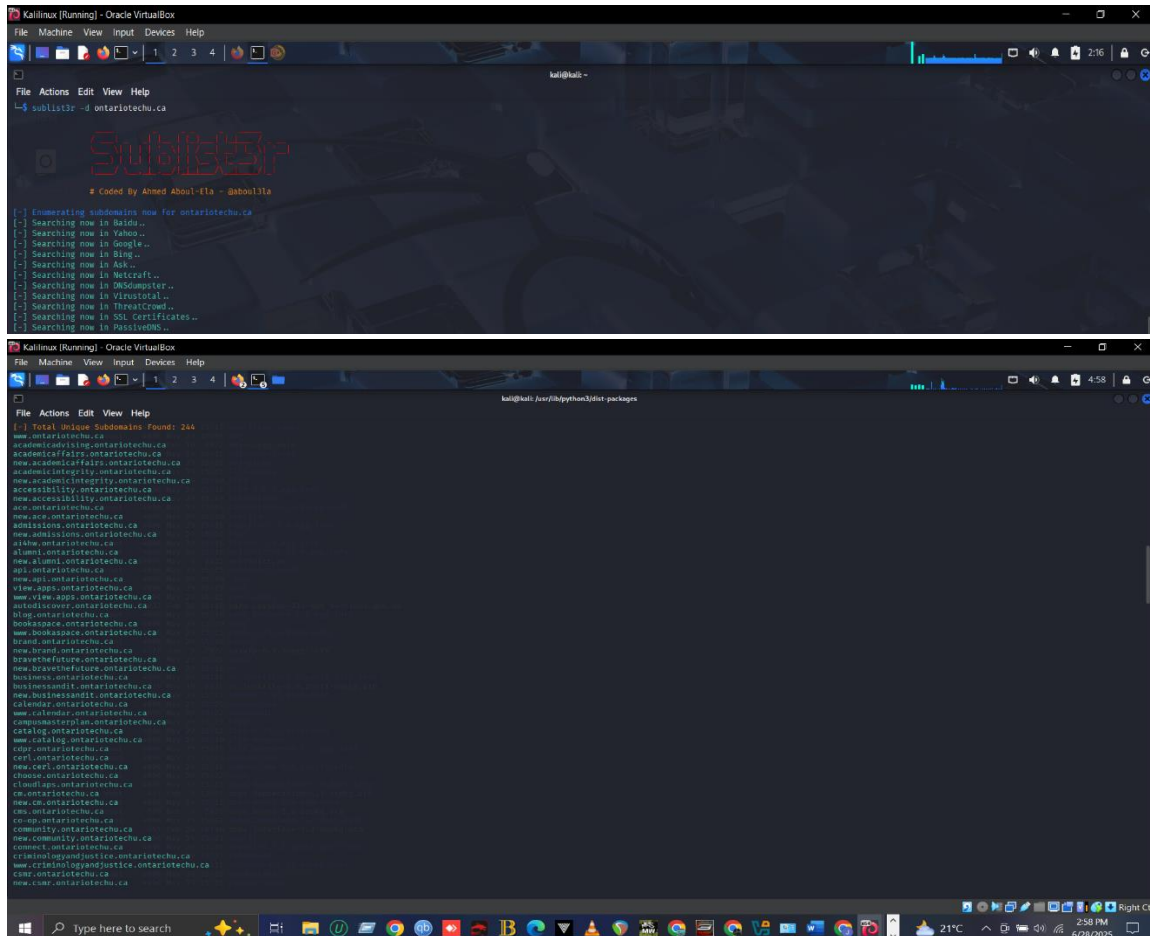
TOP ORGANIZATIONS

Organization	Count
Microsoft Corporation	31,011
Oracle Corporation	1,011

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 anything
- Ran the command **sudo apt install sublist3r** for installation
- Ran the command below for enumeration of the domain:

**Command: sublist3r -d ontariotechu.ca**



```
Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
sublist3r -d ontariotechu.ca

Sublist3r
# Codes By Ahmed Aboul-ela - ahbooll3la

[+] Enumerating subdomains now for ontariotechu.ca
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Metacrawler..
[-] Searching now in MSNometer..
[-] Searching now in VirusTotal..
[-] Searching now in Threatcrowd..
[-] Searching now in SSL certificates..
[-] Searching now in PassiveDNS..

[+] Total Unique Subdomains Found: 244
www.ontariotechu.ca
academicadvising.ontariotechu.ca
academicaffairs.ontariotechu.ca
new.academicaffairs.ontariotechu.ca
academicintegrity.ontariotechu.ca
new.academicintegrity.ontariotechu.ca
accessibility.ontariotechu.ca
new.accessibility.ontariotechu.ca
acc.ontariotechu.ca
new.sacs.ontariotechu.ca
admissions.ontariotechu.ca
new.admissions.ontariotechu.ca
alumni.ontariotechu.ca
new.alumni.ontariotechu.ca
api.ontariotechu.ca
new.api.ontariotechu.ca
view.apps.ontariotechu.ca
new.view.apps.ontariotechu.ca
autodiscover.ontariotechu.ca
blog.ontariotechu.ca
bookspace.ontariotechu.ca
www.bookspace.ontariotechu.ca
brand.ontariotechu.ca
new.brand.ontariotechu.ca
bravethefuture.ontariotechu.ca
new.bravethefuture.ontariotechu.ca
business.ontariotechu.ca
businessandit.ontariotechu.ca
new.businessandit.ontariotechu.ca
calendar.ontariotechu.ca
www.calendar.ontariotechu.ca
computerapp.ontariotechu.ca
catalog.ontariotechu.ca
www.catalog.ontariotechu.ca
cbr.ontariotechu.ca
cepl.ontariotechu.ca
med.cerl.ontariotechu.ca
choose.ontariotechu.ca
cloudapp.ontariotechu.ca
ca.ontariotechu.ca
new.ca.ontariotechu.ca
cna.ontariotechu.ca
co-op.ontariotechu.ca
community.ontariotechu.ca
new.community.ontariotechu.ca
connect.ontariotechu.ca
criminologyandjustice.ontariotechu.ca
www.criminologyandjustice.ontariotechu.ca
csmr.ontariotechu.ca
new.csmr.ontariotechu.ca
```



- theHarvester was pre-installed so ran the command below:

Kali Linux (Running) - Oracle VirtualBox

File Machine View Input Devices Help

1 2 3 4

kali@kali:~\$ theHarvester -d ontarioedu.ca -b all -l 200

Read proxies.yaml from /etc/theHarvester/proxies.yaml

.....

theHarvester

.....

\* theHarvester 4.8.0 \*

\* Coded by Christian Martorella \*

\* Edge-Security Research \*

\* cmartorella@edge-security.com \*

.....

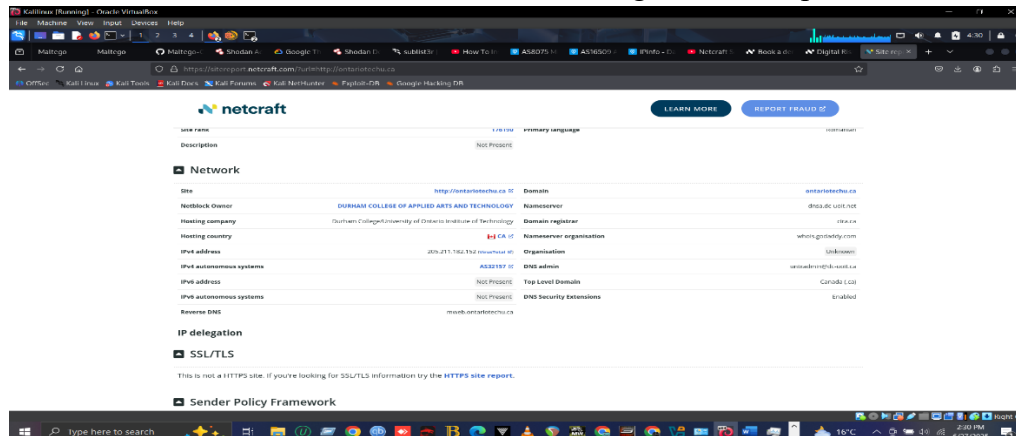
[\*] Target: ontarioedu.ca

Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

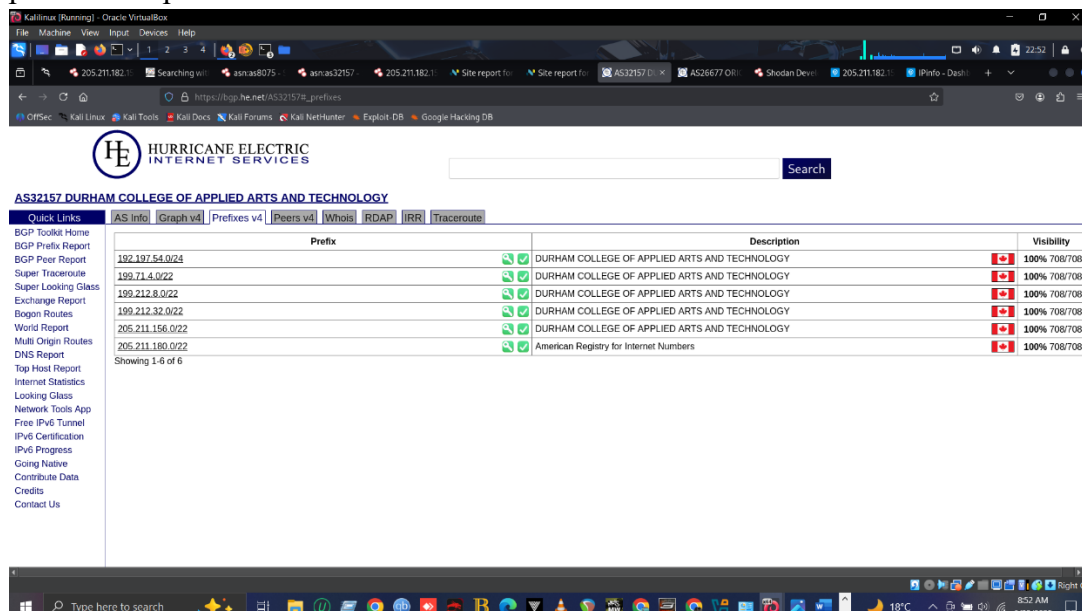
5. Use Netcraft to generate a site report of your client organization's website. Provide 1 screenshot of the generated report showing the organization's IP range.

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

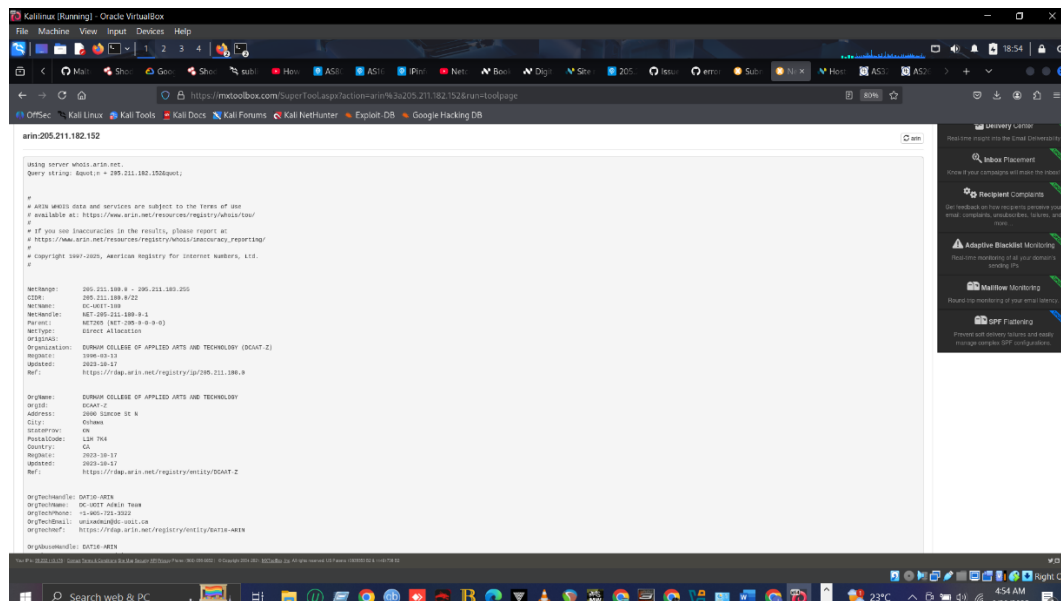


But if I click on the ASN it redirects to another link which is bgp.he.net where it shows the prefixes of ipv4:



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

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ PS1='[date +%D` `] Akib [date +%r` `] -[~]`'  
[06/27/25] Akib [12:51:30 AM] -[~]sudo nmap -sS -sV -O 192.168.100.4
```

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]

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ PS1='[date +%D` `] Akib [date +%r` `] -[~]`'  
[06/27/25] Akib [12:51:30 AM] -[~]sudo nmap -sS -sV -O 192.168.100.4  
[sudo] password for kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-27 00:51 EDT  
Nmap scan report for 192.168.100.4  
Host is up (8.00042s latency).  
Not shown: 996 filtered tcp ports (no-response)  
PORT      STATE SERVICE VERSION  
21/tcp    open  ftp      Microsoft FTP  
22/tcp    open  ssh      OpenSSH 7.1 (protocol 2.0)  
80/tcp    open  http     Microsoft IIS HTTP 7.5  
4848/tcp  open  ws/atsp  Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.1; Java 1.8)  
5985/tcp  open  http     Microsoft HTTPAPI httpd 2.0 (SSRP/ump)  
8000/tcp  open  http     Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.1; Java 1.8)  
8383/tcp  open  http     Apache httpd  
9200/tcp  open  http     Elasticsearch REST API 1.1.1 (name: beatty, lucene 4.7)  
49153/tcp open  mqrpc    Microsoft Windows RPC  
49154/tcp open  mqrpc    Microsoft Windows RPC  
49175/tcp open  java-rem Java RM  
49176/tcp open  tcpwrappers  
MAC Address: 08:00:27:07:CC:06 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose/linux/specialized  
Running (2025-06-27): Microsoft Windows 2008 R2 (x86_64)  
OS CPE: cpe:/o:microsoft/windows_server_2008_r2 cpe:/o:microsoft/windows_7 cpe:/o:microsoft/windows_8 cpe:/o:microsoft/windows_8.1 cpe:/o:microsoft/windows_vista cpe:/o:microsoft/windows_vista_sp1  
Aggressive OS guesses: Microsoft Windows Server 2008 R2 or Windows 7 SP1 (90%), Microsoft Windows 8.1 (90%), Microsoft Windows Phone 7.5 or 8.0 (90%), Microsoft Windows Embedded Standard 7 (90%), Microsoft Windows 7 or Windows Server 2008 R2 (92%), Microsoft Windows Server 2008 or 2008 R2 (92%), Microsoft Windows Server 2008 R2 or Windows 7 (92%), Microsoft Windows 7 Professional or Windows 8 (92%), Microsoft Windows Vista SP2 or SP1, Windows Server 2008 SP1 or Windows 7 (92%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (92%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 1 hop  
Service Info: OS: Windows; CPE: cpe:/o:microsoft/windows  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 75.65 seconds  
[06/27/25] Akib [12:54:31 AM] -[~]
```

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





## 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.

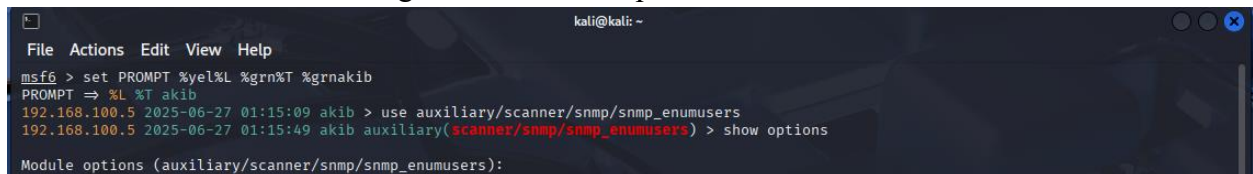
1- Start an msf console, and change the console prompt:

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



```
kali@kali: ~  
File Actions Edit View Help  
msf6 > set PROMPT %yel%L %grn%T %grnakib  
PROMPT => %L %T akib  
192.168.100.5 2025-06-27 01:15:09 akib > use auxiliary/scanner/snmp/snmp_enumusers  
192.168.100.5 2025-06-27 01:15:49 akib auxiliary(scanner/snmp/snmp_enumusers) > show options  
Module options (auxiliary/scanner/snmp/snmp_enumusers):
```

2- To use the snmp\_enumusers script, run the following commands using MS3WS2008 as your target machine:

msfconsole# use auxiliary/scanner/snmp/snmp\_enumusers

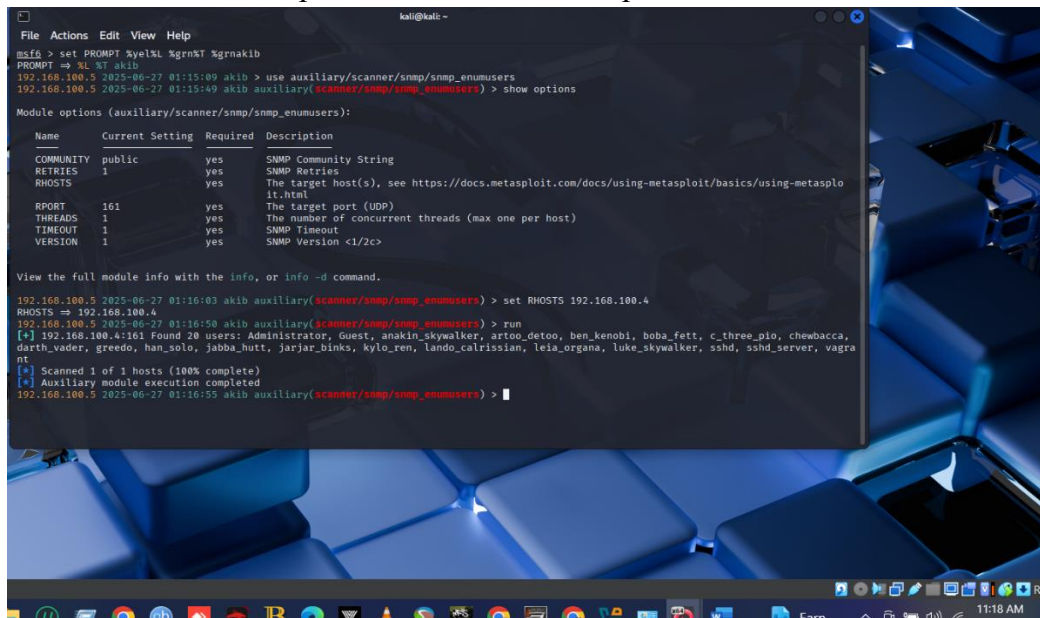
msfconsole# show options

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.



```
msf5 > set PROMPT %e%l%l %grn%T %grn%k%b
PROMPT => %T %T %k%b
192.168.100.5 2025-06-27 01:15:00 akib > use auxiliary/scanner/snmp/snmp_enumusers
192.168.100.5 2025-06-27 01:15:49 akib auxiliary(scanner/snmp/snmp_enumusers) > show options

Module options (auxiliary/scanner/snmp/snmp_enumusers):

  Name      Current Setting  Required  Description
  ---      -
  COMMUNITY  public           yes       SNMP Community String
  RETRIES    1                yes       SNMP Retries
  RHOSTS     192.168.100.5    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      161              yes       The target port (UDP)
  THREADS    1                yes       The number of concurrent threads (max one per host)
  TIMEOUT    1                yes       SNMP Timeout
  VERSION    1                yes       SNMP Version <1/2c>

View the full module info with the info, or info -d command.

192.168.100.5 2025-06-27 01:16:03 akib auxiliary(scanner/snmp/snmp_enumusers) > set RHOSTS 192.168.100.4
RHOSTS => 192.168.100.4
192.168.100.5 2025-06-27 01:16:50 akib auxiliary(scanner/snmp/snmp_enumusers) > run
[*] 192.168.100.4:161 Found 20 users: Administrator, Guest, anakin_skywalker, artoo_detoo, ben_kenobi, boba_fett, c_three_pio, chewbacca,
darth_vader, greedo, han_solo, jabba_hutt, jarjar_binks, kylo_ren, lando_calrissian, leia_organa, luke_skywalker, sshd, sshd_server, vagra
nt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
192.168.100.5 2025-06-27 01:16:55 akib auxiliary(scanner/snmp/snmp_enumusers) > |
```

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

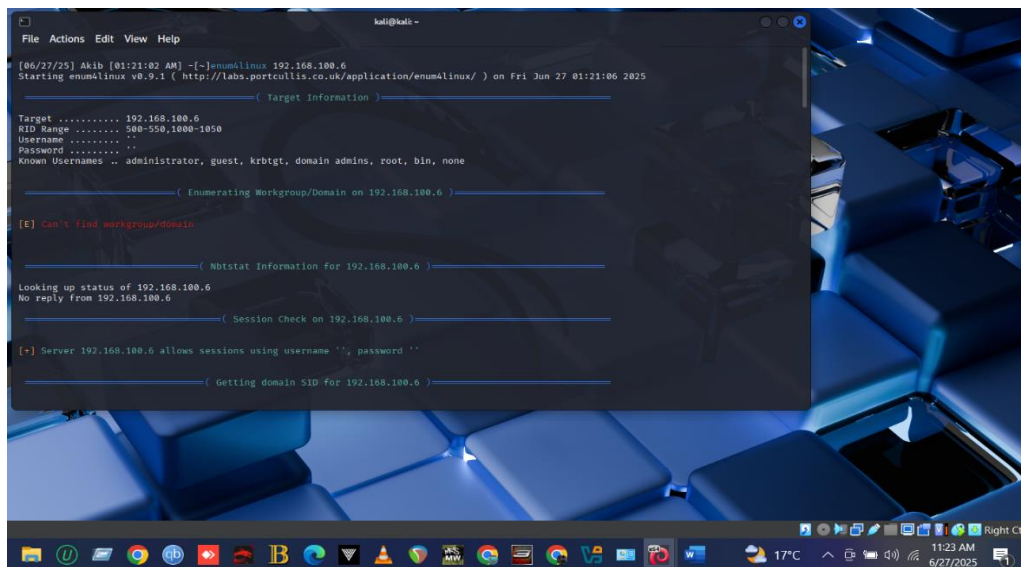
Step 2: Repeat Step 1 while targeting MS3UBUNTU machine, but use enum4linux command instead running the following command in the kali linux terminal:

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.





```
File Actions Edit View Help
[06/27/25] Akib [01:21:02 AM] ~[enum4linux 192.168.100.6]
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jun 27 01:21:06 2025

( Target Information )
Target ..... 192.168.100.6
RID Range ..... 500-550,1000-1050
Username ..... 
Password ..... 
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

( Enumerating Workgroup/Domain on 192.168.100.6 )

[E] Can't find workgroup/domain

( Nbtstat Information for 192.168.100.6 )
Looking up status of 192.168.100.6
No reply from 192.168.100.6

( Session Check on 192.168.100.6 )

[+] Server 192.168.100.6 allows sessions using username '', password ''

( Getting domain SID for 192.168.100.6 )
```

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.