DAY 4 ASSIGNMENT 1

Question 1: Find out the mail servers of the following domains: ibm.com, wipro.com

Solution:

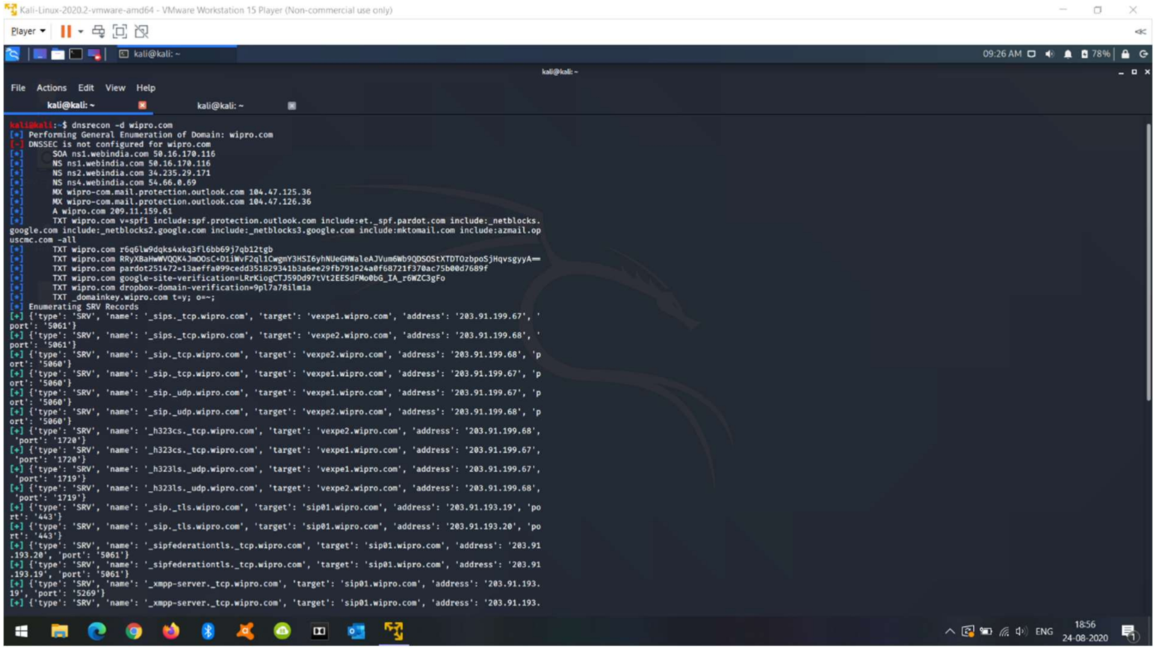
The domains were discovered using a kali tool by the name of "dnsrecon"

Command used:

```
sudo dnsrecon -d wipro.com
```

OUTPUT:

```
[*] Performing General Enumeration of Domain: wipro.com

[-] DNSSEC is not configured for wipro.com

[*]          SOA ns1.webindia.com 50.16.170.116

[*]          NS ns2.webindia.com 34.235.29.171

[*]          NS ns1.webindia.com 50.16.170.116

[*]          NS ns4.webindia.com 54.66.0.69

[*]          MX wipro-com.mail.protection.outlook.com 104.47.124.36     //MAIL SERVER

[*]          MX wipro-com.mail.protection.outlook.com 104.47.125.36     //MAIL SERVER

[*]          A wipro.com 209.11.159.61

[*]          TXT wipro.com pardot251472=13aeffa099cedd351829341b3a6ee29fb791e24a0f68721f370ac75b00d7689f
```



```
kali@kali:~$ dnsrecon -d wipro.com
[*] Performing General Enumeration of Domain: wipro.com
[-] DNSSEC is not configured for wipro.com
[*]      SOA ns1.webindia.com 50.16.170.116
[*]      NS ns1.webindia.com 50.16.170.116
[*]      NS ns2.webindia.com 34.235.29.171
[*]      NS ns4.webindia.com 54.66.0.69
[*]      MX wipro-com.mail.protection.outlook.com 104.47.125.36
[*]      MX wipro-com.mail.protection.outlook.com 104.47.126.36
[*]      A wipro.com 209.11.159.61
[*]      TXT wipro.com v=spf1 include:spf.protection.outlook.com include:et._spf.pardot.com include:_netblocks.
google.com include:_netblocks2.google.com include:_netblocks3.google.com include:mktomail.com include:azmail.op
uscmc.com -all
[*]      TXT wipro.com r6q6lw9dqks4xkq3fl6bb69j7qb12tgb
[*]      TXT wipro.com RRyXBaHwWVQQK4JmOOsC+D1iWvF2ql1CwgmY3HSI6yhNUeGHWaleAJVum6Wb9QDSOStXTDTOzbpoSjHqvsgyyA==
[*]      TXT wipro.com pardot251472=13aeffa099cedd351829341b3a6ee29fb791e24a0f68721f370ac75b00d7689f
[*]      TXT wipro.com google-site-verification=LRrKiogCTJ59Dd97tVt2EESdFMo0bG_IA_r6WZC3gFo
[*]      TXT wipro.com dropbox-domain-verification=9pl7a78ilm1a
[*]      TXT _domainkey.wipro.com t=y; o=~;
[*] Enumerating SRV Records
[+] {'type': 'SRV', 'name': '_sips._tcp.wipro.com', 'target': 'vexpe1.wipro.com', 'address': '203.91.199.67', '
port': '5061'}
[+] {'type': 'SRV', 'name': '_sips._tcp.wipro.com', 'target': 'vexpe2.wipro.com', 'address': '203.91.199.68', '
port': '5061'}
[+] {'type': 'SRV', 'name': '_sip._tcp.wipro.com', 'target': 'vexpe2.wipro.com', 'address': '203.91.199.68', 'p
ort': '5060'}
[+] {'type': 'SRV', 'name': '_sip._tcp.wipro.com', 'target': 'vexpe1.wipro.com', 'address': '203.91.199.67', 'p
ort': '5060'}
[+] {'type': 'SRV', 'name': '_sip._udp.wipro.com', 'target': 'vexpe1.wipro.com', 'address': '203.91.199.67', 'p
ort': '5060'}
[+] {'type': 'SRV', 'name': '_sip._udp.wipro.com', 'target': 'vexpe2.wipro.com', 'address': '203.91.199.68', 'p
ort': '5060'}
[+] {'type': 'SRV', 'name': '_h323cs._tcp.wipro.com', 'target': 'vexpe2.wipro.com', 'address': '203.91.199.68',
 'port': '1720'}
[+] {'type': 'SRV', 'name': '_h323cs._tcp.wipro.com', 'target': 'vexpe1.wipro.com', 'address': '203.91.199.67',
 'port': '1720'}
[+] {'type': 'SRV', 'name': '_h323ls._udp.wipro.com', 'target': 'vexpe1.wipro.com', 'address': '203.91.199.67',
 'port': '1719'}
[+] {'type': 'SRV', 'name': '_h323ls._udp.wipro.com', 'target': 'vexpe2.wipro.com', 'address': '203.91.199.68',
 'port': '1719'}
[+] {'type': 'SRV', 'name': '_sip._tls.wipro.com', 'target': 'sip01.wipro.com', 'address': '203.91.193.19', 'po
rt': '443'}
[+] {'type': 'SRV', 'name': '_sip._tls.wipro.com', 'target': 'sip01.wipro.com', 'address': '203.91.193.20', 'po
rt': '443'}
[+] {'type': 'SRV', 'name': '_sipfederationtls._tcp.wipro.com', 'target': 'sip01.wipro.com', 'address': '203.91
.193.20', 'port': '5061'}
[+] {'type': 'SRV', 'name': '_sipfederationtls._tcp.wipro.com', 'target': 'sip01.wipro.com', 'address': '203.91
.193.19', 'port': '5061'}
[+] {'type': 'SRV', 'name': '_xmpp-server._tcp.wipro.com', 'target': 'sip01.wipro.com', 'address': '203.91.193.
19', 'port': '5269'}
[+] {'type': 'SRV', 'name': '_xmpp-server._tcp.wipro.com', 'target': 'sip01.wipro.com', 'address': '203.91.193.
```

DAY 4 ASSIGNMENT 1

Command used:

sudo dnsrecon -d ibm.com

OUTPUT:

[*] Performing General Enumeration of Domain: ibm.com

[-] DNSSEC is not configured for ibm.com

[*]   SOA asia3.akam.net 23.211.61.64

[*]   NS ns1-206.akam.net 193.108.91.206

[*]   NS ns1-206.akam.net 2600:1401:2::ce

[*]   NS ns1-99.akam.net 193.108.91.99

[*]   NS ns1-99.akam.net 2600:1401:2::63

[*]   NS usc2.akam.net 184.26.160.64

[*]   NS usc3.akam.net 96.7.50.64

[*]   NS eur2.akam.net 95.100.173.64

[*]   NS asia3.akam.net 23.211.61.64

[*]   NS eur5.akam.net 23.74.25.64

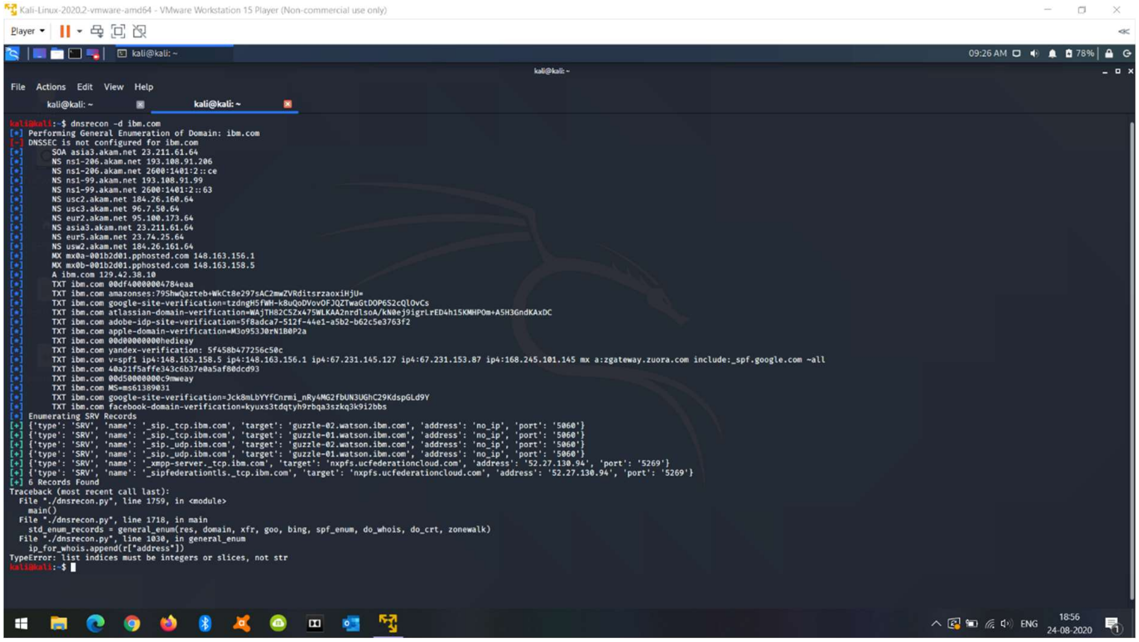
[*]   NS usw2.akam.net 184.26.161.64

[*]   MX mx0a-001b2d01.pphosted.com 148.163.156.1   //MAIL SERVER

[*]   MX mx0b-001b2d01.pphosted.com 148.163.158.5   //MAIL SERVER

[*]   A ibm.com 129.42.38.10

[*]   TXT ibm.com facebook-domain-verification=kyuxs3tdqtyh9rbqa3szkq3k9i2bbs



```
kali@kali:~$ dnsrecon -d ibm.com
[*] Performing General Enumeration of Domain: ibm.com
[-] DNSSEC is not configured for ibm.com
[*]      SOA asia3.akam.net 23.211.61.64
[*]      NS ns1-206.akam.net 193.108.91.206
[*]      NS ns1-206.akam.net 2600:1401:2::ce
[*]      NS ns1-99.akam.net 193.108.91.99
[*]      NS ns1-99.akam.net 2600:1401:2::63
[*]      NS usc2.akam.net 184.26.160.64
[*]      NS usc3.akam.net 96.7.50.64
[*]      NS eur2.akam.net 95.100.173.64
[*]      NS asia3.akam.net 23.211.61.64
[*]      NS eur5.akam.net 23.74.25.64
[*]      NS usw2.akam.net 184.26.161.64
[*]      MX mx0a-001b2d01.pphosted.com 148.163.156.1
[*]      MX mx0b-001b2d01.pphosted.com 148.163.158.5
[*]      A ibm.com 129.42.38.10
[*]      TXT ibm.com 00df40000004784eaa
[*]      TXT ibm.com amazonses:79ShwQazteb+WkCt8e297sAC2mwZVRditsrzaoxiHjU=
[*]      TXT ibm.com google-site-verification=tzdngH5fWH-k8uQoDVovOFJQZTwaGtDOP6S2cQlOvCs
[*]      TXT ibm.com atlassian-domain-verification=WAjTH82C5Zx475WLKAA2nrdlsoA/kN0ej9igrLrED4h15KMHPOm+A5H3GndKAxDC
[*]      TXT ibm.com adobe-idp-site-verification=5f8adca7-512f-44e1-a5b2-b62c5e3763f2
[*]      TXT ibm.com apple-domain-verification=M3o953J0rN1B0P2a
[*]      TXT ibm.com 00d00000000hedieay
[*]      TXT ibm.com yandex-verification: 5f458b477256c50c
[*]      TXT ibm.com v=spf1 ip4:148.163.158.5 ip4:148.163.156.1 ip4:67.231.145.127 ip4:67.231.153.87 ip4:168.245.101.145 mx a:zgateway.zuora.com include:_spf.google.com ~all
[*]      TXT ibm.com 40a21f5affe343c6b37e0a5af80dcd93
[*]      TXT ibm.com 00d50000000c9mweay
[*]      TXT ibm.com MS=ms61389031
[*]      TXT ibm.com google-site-verification=Jck8mLbYYfCnrmi_nRy4MG2fbUN3UGhC29KdspGLd9Y
[*]      TXT ibm.com facebook-domain-verification=kyuxs3tdqtyh9rbqa3szkq3k9i2bbs
[*] Enumerating SRV Records
[+] {'type': 'SRV', 'name': '_sip._tcp.ibm.com', 'target': 'guzzle-02.watson.ibm.com', 'address': 'no_ip', 'port': '5060'}
[+] {'type': 'SRV', 'name': '_sip._tcp.ibm.com', 'target': 'guzzle-01.watson.ibm.com', 'address': 'no_ip', 'port': '5060'}
[+] {'type': 'SRV', 'name': '_sip._udp.ibm.com', 'target': 'guzzle-02.watson.ibm.com', 'address': 'no_ip', 'port': '5060'}
[+] {'type': 'SRV', 'name': '_sip._udp.ibm.com', 'target': 'guzzle-01.watson.ibm.com', 'address': 'no_ip', 'port': '5060'}
[+] {'type': 'SRV', 'name': '_xmpp-server._tcp.ibm.com', 'target': 'nxpfs.ucfederationcloud.com', 'address': '52.27.130.94', 'port': '5269'}
[+] {'type': 'SRV', 'name': '_sipfederationtls._tcp.ibm.com', 'target': 'nxpfs.ucfederationcloud.com', 'address': '52.27.130.94', 'port': '5269'}
[+] 6 Records Found
Traceback (most recent call last):
  File "./dnsrecon.py", line 1759, in <module>
    main()
  File "./dnsrecon.py", line 1718, in main
    std_enum_records = general_enum(res, domain, xfr, goo, bing, spf_enum, do_whois, do_crt, zonewalk)
  File "./dnsrecon.py", line 1030, in general_enum
    ip_for_whois.append(r["address"])
TypeError: list indices must be integers or slices, not str
kali@kali:~$
```

SUBMITTED BY: ANSHUMAN MISHRA, juran9@gmail.com

Question 2: Find the locations, where these email servers are hosted.

Solution: The IP addresses were scanned through the online utility https://dnslytics.com

Commands:

```
firefox dnslytics.com/ip/104.47.124.36

firefox dnslytics.com/ip/104.47.125.36

firefox dnslytics.com/ip/148.163.156.1

firefox dnslytics.com/ip/148.163.158.5
```

OUTPUT:

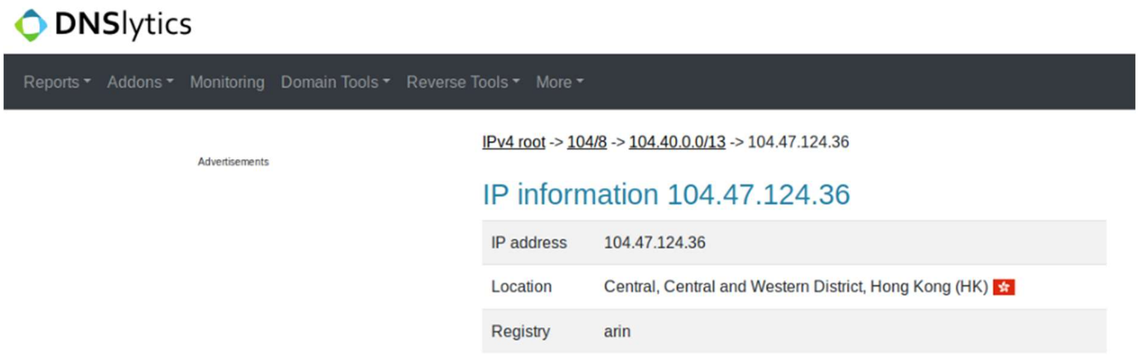
Locations:

104.47.124.36: Central and Western District, Hongkong (HK)

104.47.125.36: Singapore (SG)

148.163.156.1: United States (US)

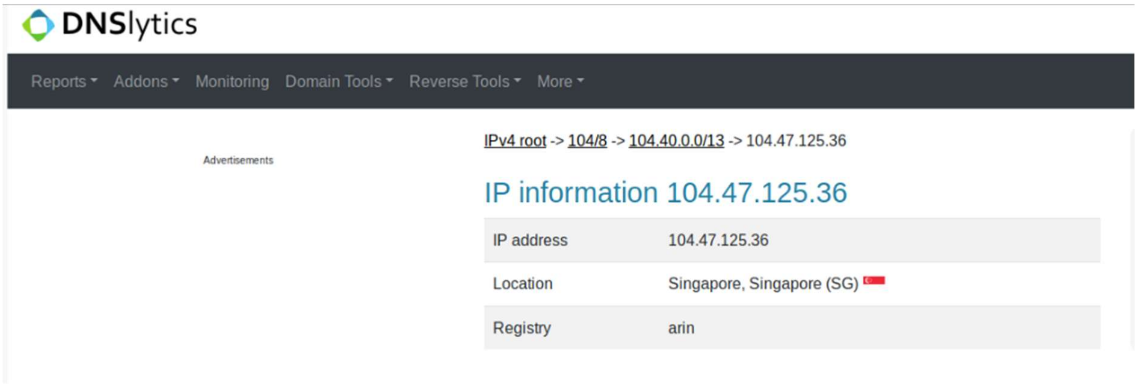
148.163.158.5: United States (US)



IPv4 root -> 104/8 -> 104.40.0.0/13 -> 104.47.124.36

IP information 104.47.124.36

IP address	104.47.124.36
Location	Central, Central and Western District, Hong Kong (HK)
Registry	arin

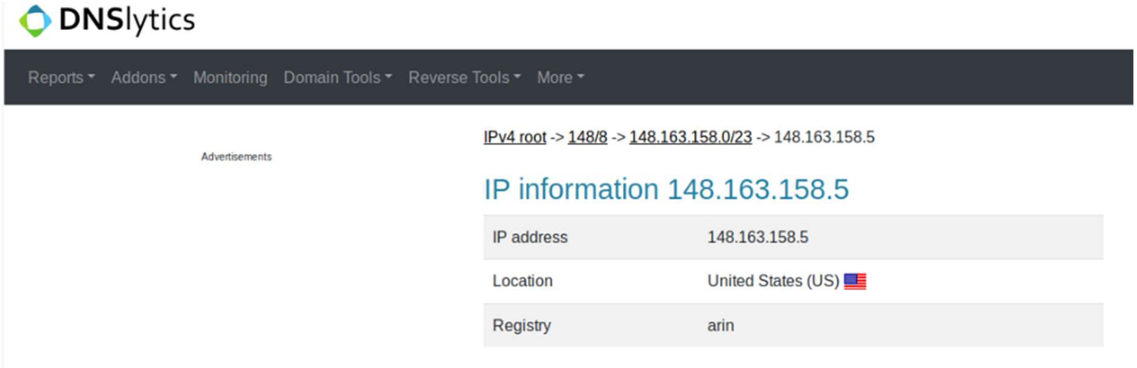


IPv4 root -> 104/8 -> 104.40.0.0/13 -> 104.47.125.36

IP information 104.47.125.36

IP address	104.47.125.36
Location	Singapore, Singapore (SG)
Registry	arin

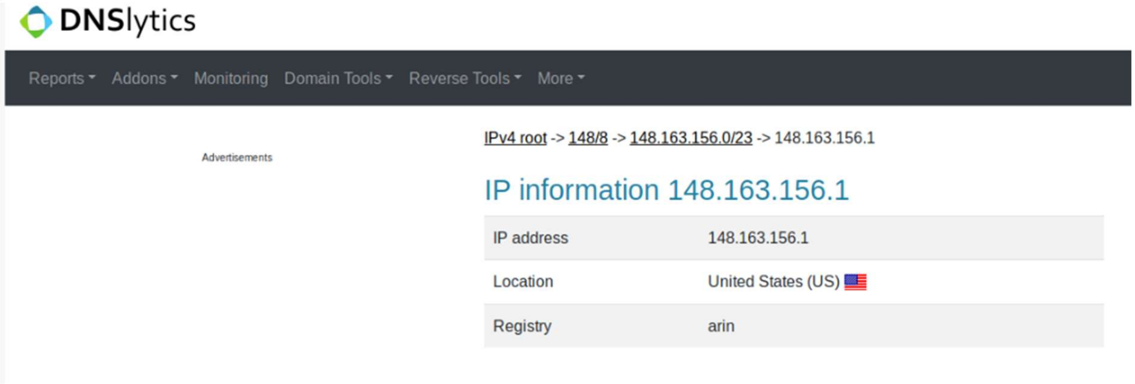
DAY 4 ASSIGNMENT 1



IPv4 root -> 148/8 -> 148.163.158.0/23 -> 148.163.158.5

IP information 148.163.158.5

IP address	148.163.158.5
Location	United States (US)
Registry	arin



IPv4 root -> 148/8 -> 148.163.156.0/23 -> 148.163.156.1

IP information 148.163.156.1

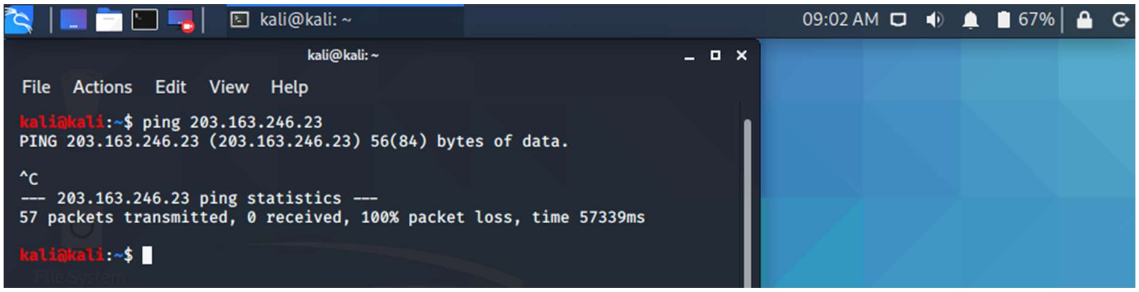
IP address	148.163.156.1
Location	United States (US)
Registry	arin

Question 3: Scan and find out port numbers open 203.163.246.23

Solution: The given IP was scanned using NMAP

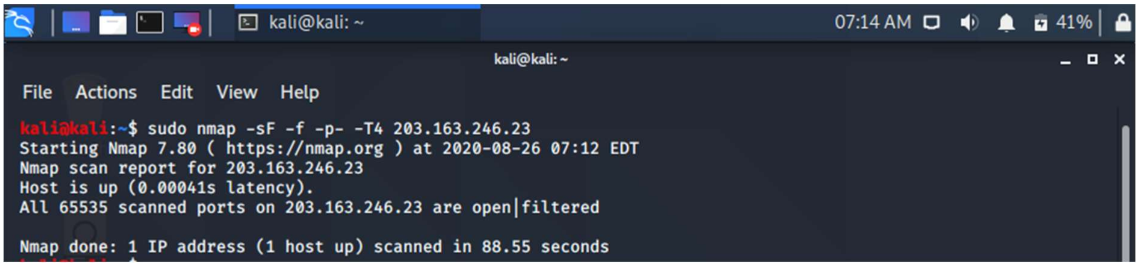
Command: nmap -Pn -T4 -v -A 203.163.246.23

ERROR: Host is unreachable or protected by a filter or firewall



```
kali@kali:~$ ping 203.163.246.23
PING 203.163.246.23 (203.163.246.23) 56(84) bytes of data.

^C
--- 203.163.246.23 ping statistics ---
57 packets transmitted, 0 received, 100% packet loss, time 57339ms

kali@kali:~$
```

Retrying with firewall evasion scan: nmap -sF -f -p- -T4 203.163.246.23



```
kali@kali:~$ sudo nmap -sF -f -p- -T4 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 07:12 EDT
Nmap scan report for 203.163.246.23
Host is up (0.00041s latency).
All 65535 scanned ports on 203.163.246.23 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 88.55 seconds
```

All ports are protected by firewall but appear to be open.

SUBMITTED BY: ANSHUMAN MISHRA, juran9@gmail.com

DAY 4 ASSIGNMENT 1

Question 4: Install Nessus in a VM and scan your laptop/desktop for CVE.

Solution:

1. Navigate to https://www.tenable.com/downloads/nessus

2. Download the appropriate version. Mine was Debian 64 bit

3. Register with the website with name and email to get the authentication code via email.

4. Go to Kali terminal, cd to Downloads folder.

5. Dpkg -i [installation file name]

6. After completion start the service by systemctl as prompted in the terminal

7. Navigate to the local host on port 8834 to start with Nessus.

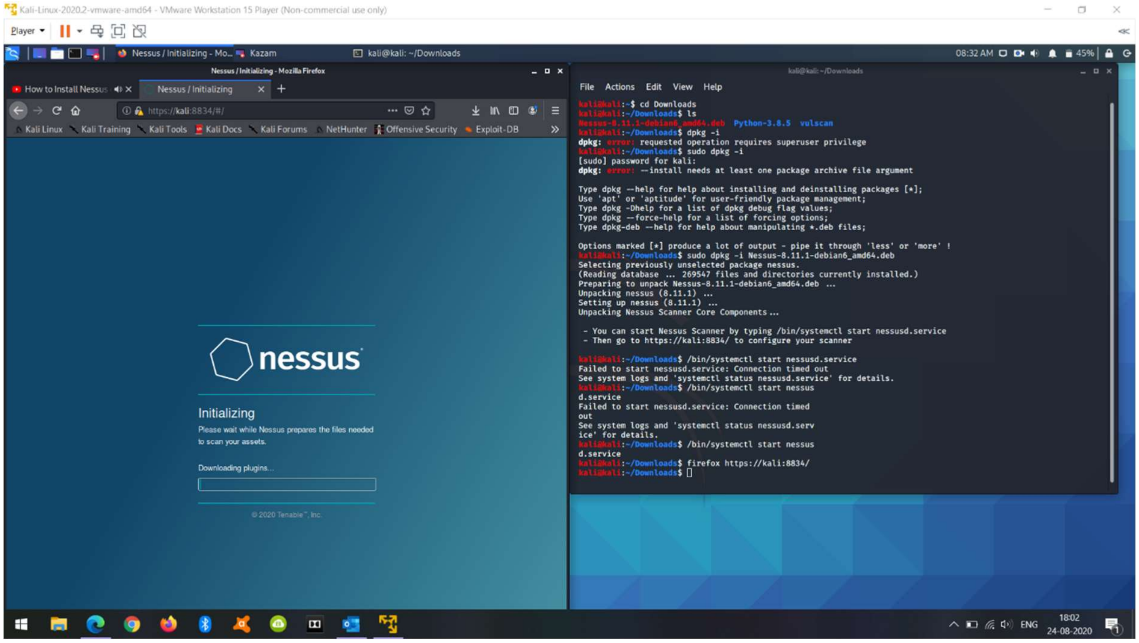
8. Enter AUTH code sent via email.

9. Wait for initialization to complete.

10. Log on to Nessus.

11.Goto Advanced tab and create a scan against the local system.

12. Click on the Scan to get the list of vulnerabilities



Initializing

Please wait while Nessus prepares the files needed to scan your assets.

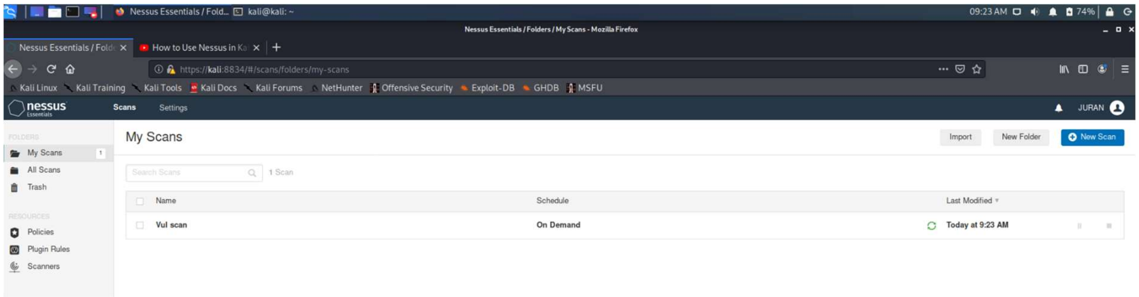
Downloading plugins...

© 2020 Tenable™, Inc.

kali@kali: ~/Downloads

File Actions Edit View Help

```
kali@kali:~$ cd Downloads
kali@kali:~/Downloads$ ls
Nessus-8.11.1-debian6_amd64.deb  Python-3.8.5  vulscan
kali@kali:~/Downloads$ dpkg -i
dpkg: error: requested operation requires superuser privilege
kali@kali:~/Downloads$ sudo dpkg -i
[sudo] password for kali:
dpkg: error: --install needs at least one package archive file argument

Type dpkg --help for help about installing and deinstalling packages [*];
Use 'apt' or 'aptitude' for user-friendly package management;
Type dpkg -Dhelp for a list of dpkg debug flag values;
Type dpkg --force-help for a list of forcing options;
Type dpkg-deb --help for help about manipulating *.deb files;

Options marked [*] produce a lot of output - pipe it through 'less' or 'more' !
kali@kali:~/Downloads$ sudo dpkg -i Nessus-8.11.1-debian6_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 269547 files and directories currently installed.)
Preparing to unpack Nessus-8.11.1-debian6_amd64.deb ...
Unpacking nessus (8.11.1) ...
Setting up nessus (8.11.1) ...
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://kali:8834/ to configure your scanner

kali@kali:~/Downloads$ /bin/systemctl start nessusd.service
Failed to start nessusd.service: Connection timed out
See system logs and 'systemctl status nessusd.service' for details.
kali@kali:~/Downloads$ /bin/systemctl start nessus
d.service
Failed to start nessusd.service: Connection timed
out
See system logs and 'systemctl status nessusd.serv
ice' for details.
kali@kali:~/Downloads$ /bin/systemctl start nessus
d.service
kali@kali:~/Downloads$ firefox https://kali:8834/
kali@kali:~/Downloads$ 
```



My Scans

1 Scan

□	Name	Schedule	Last Modified
□	Vul scan	On Demand	Today at 9:23 AM

**For security purposes the list of vulnerabilities cannot be displayed on the screenshots.

SUBMITTED BY: ANSHUMAN MISHRA, juran9@gmail.com