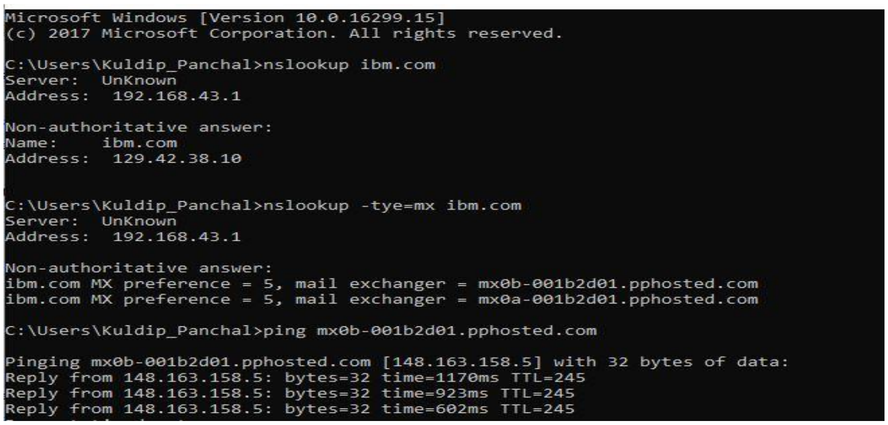
Name: Panchal Parth Mukeshbhai (LetsUpgrader)

Email : parthiv7911@gmail.com

Q1. Find out the mail servers of the following domain :

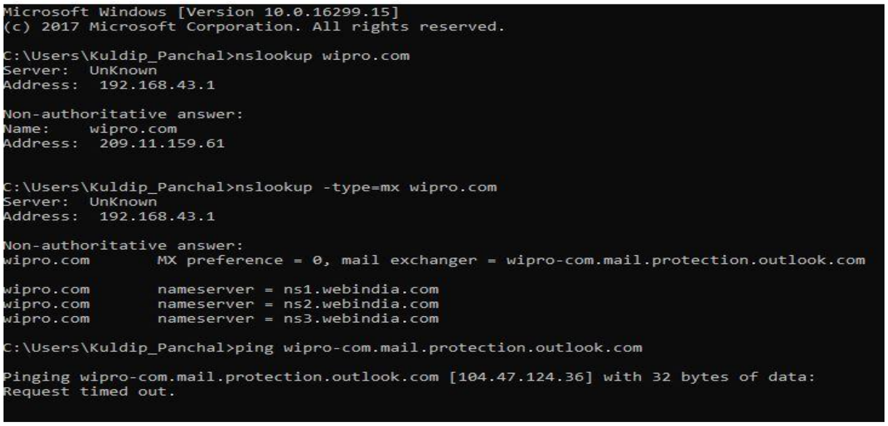
Ibm.com
Wipro.com

1) Command :
nslookup ibm.com
nslookup –type=mx ibm.com



```
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Kuldip_Panchal>nslookup ibm.com
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    ibm.com
Address:  129.42.38.10


C:\Users\Kuldip_Panchal>nslookup -tye=mx ibm.com
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
ibm.com MX preference = 5, mail exchanger = mx0b-001b2d01.pphosted.com
ibm.com MX preference = 5, mail exchanger = mx0a-001b2d01.pphosted.com

C:\Users\Kuldip_Panchal>ping mx0b-001b2d01.pphosted.com

Pinging mx0b-001b2d01.pphosted.com [148.163.158.5] with 32 bytes of data:
Reply from 148.163.158.5: bytes=32 time=1170ms TTL=245
Reply from 148.163.158.5: bytes=32 time=923ms TTL=245
Reply from 148.163.158.5: bytes=32 time=602ms TTL=245
```

2) Command :
nslookup wipro.com
nslookup –type=mx wipro.com



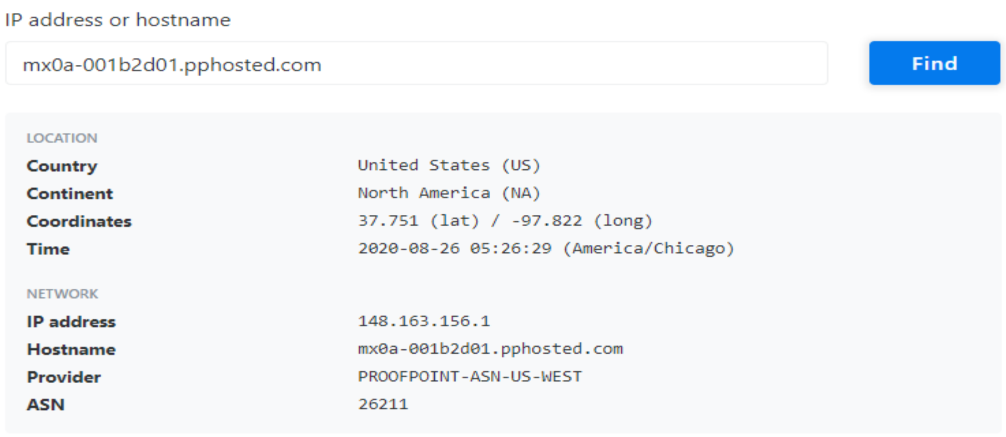
```
Microsoft Windows [Version 10.0.16299.15]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Kuldip_Panchal>nslookup wipro.com
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    wipro.com
Address:  209.11.159.61


C:\Users\Kuldip_Panchal>nslookup -type=mx wipro.com
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
wipro.com       MX preference = 0, mail exchanger = wipro-com.mail.protection.outlook.com

wipro.com       nameserver = ns1.webindia.com
wipro.com       nameserver = ns2.webindia.com
wipro.com       nameserver = ns3.webindia.com

C:\Users\Kuldip_Panchal>ping wipro-com.mail.protection.outlook.com

Pinging wipro-com.mail.protection.outlook.com [104.47.124.36] with 32 bytes of data:
Request timed out.
```

Q2.Find the locations, where these email servers are hosted.

Open google chrome

Open IP Location Finder

Address 1: For ibm Mailserver location



IP address or hostname

mx0a-001b2d01.pphosted.com

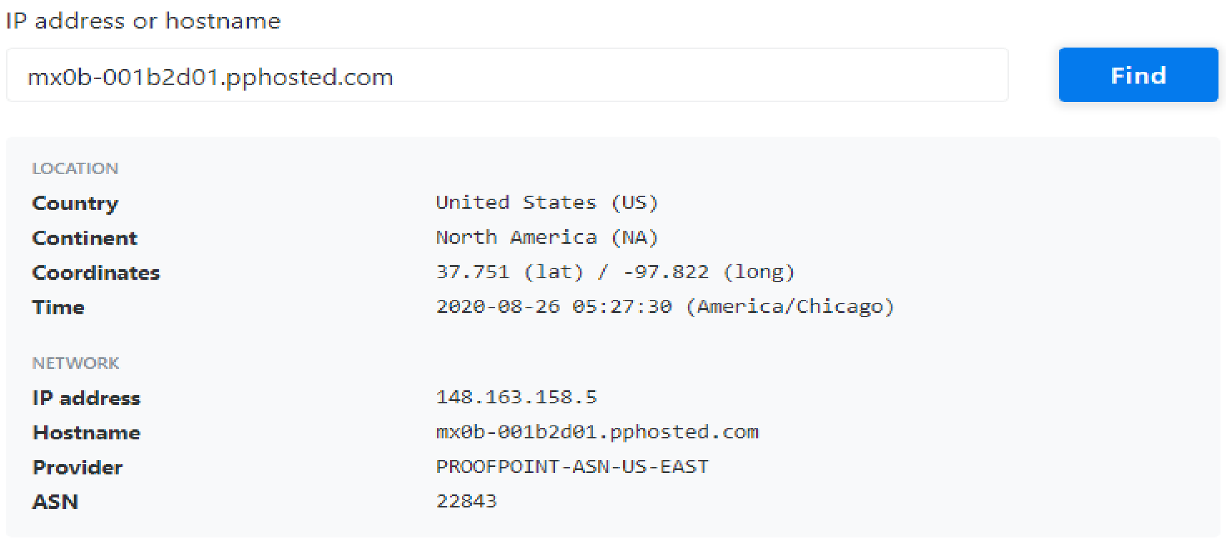
LOCATION

Country	United States (US)
Continent	North America (NA)
Coordinates	37.751 (lat) / -97.822 (long)
Time	2020-08-26 05:26:29 (America/Chicago)

NETWORK

IP address	148.163.156.1
Hostname	mx0a-001b2d01.pphosted.com
Provider	PROOFPOINT-ASN-US-WEST
ASN	26211

Address 2: For ibm Mailserver location



IP address or hostname

mx0b-001b2d01.pphosted.com

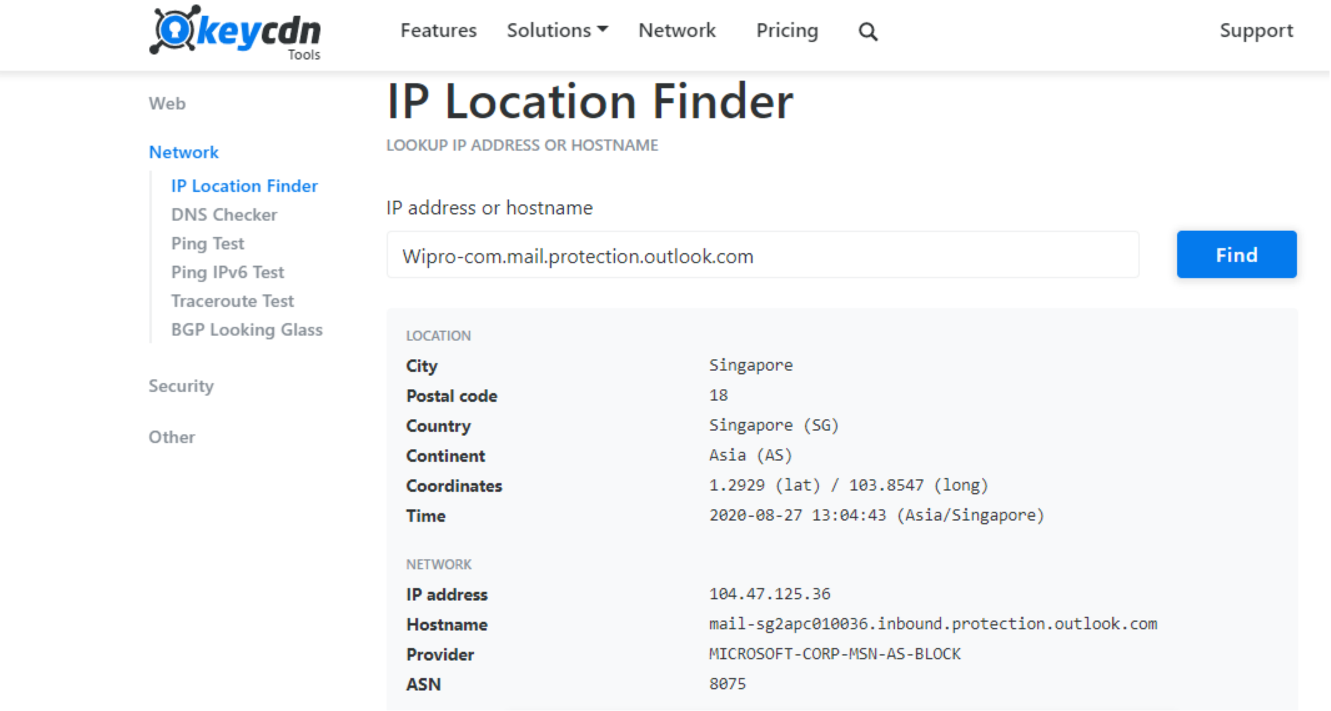
LOCATION

Country	United States (US)
Continent	North America (NA)
Coordinates	37.751 (lat) / -97.822 (long)
Time	2020-08-26 05:27:30 (America/Chicago)

NETWORK

IP address	148.163.158.5
Hostname	mx0b-001b2d01.pphosted.com
Provider	PROOFPOINT-ASN-US-EAST
ASN	22843

Address 1 : For wipro mail server location



IP Location Finder

LOOKUP IP ADDRESS OR HOSTNAME

IP address or hostname

Wipro-com.mail.protection.outlook.com

LOCATION	
City	Singapore
Postal code	18
Country	Singapore (SG)
Continent	Asia (AS)
Coordinates	1.2929 (lat) / 103.8547 (long)
Time	2020-08-27 13:04:43 (Asia/Singapore)

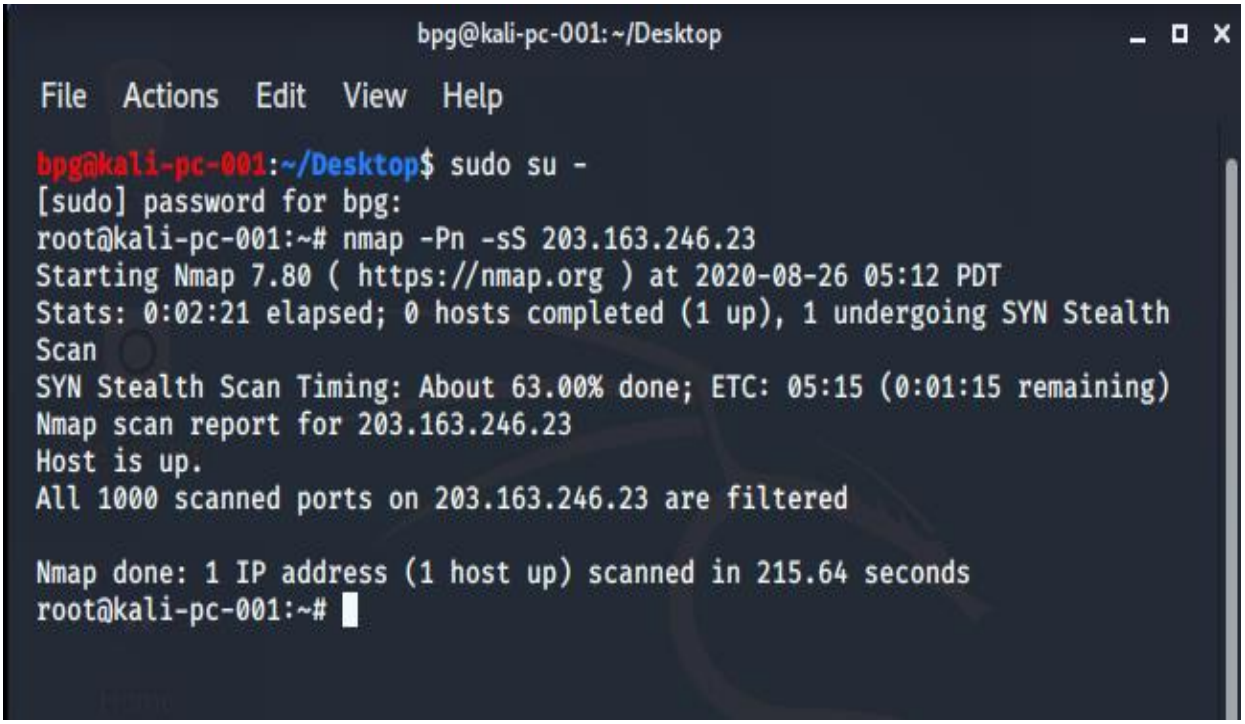
NETWORK	
IP address	104.47.125.36
Hostname	mail-sg2apc010036.inbound.protection.outlook.com
Provider	MICROSOFT-CORP-MSN-AS-BLOCK
ASN	8075

Q3.Scan and find out port numbers open 203.163.246.23

Open Kali-pc
Right click on the screen and Open Terminal

Type:
sudosu –

Enter password
Enter – nmap –Pn –sS 203.163.246.23



```
bpg@kali-pc-001:~/Desktop$ sudo su -
[sudo] password for bpg:
root@kali-pc-001:~# nmap -Pn -sS 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 05:12 PDT
Stats: 0:02:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 63.00% done; ETC: 05:15 (0:01:15 remaining)
Nmap scan report for 203.163.246.23
Host is up.
All 1000 scanned ports on 203.163.246.23 are filtered

Nmap done: 1 IP address (1 host up) scanned in 215.64 seconds
root@kali-pc-001:~#
```

As it is coming filtered due to firewall protection we try some other ways of breaking the firewall

Enter: -sS -v -v -Pn 203.163.246.23

For me it is still coming filtered so I'll further use the following command

Enter: nmap -6203.163.246.23

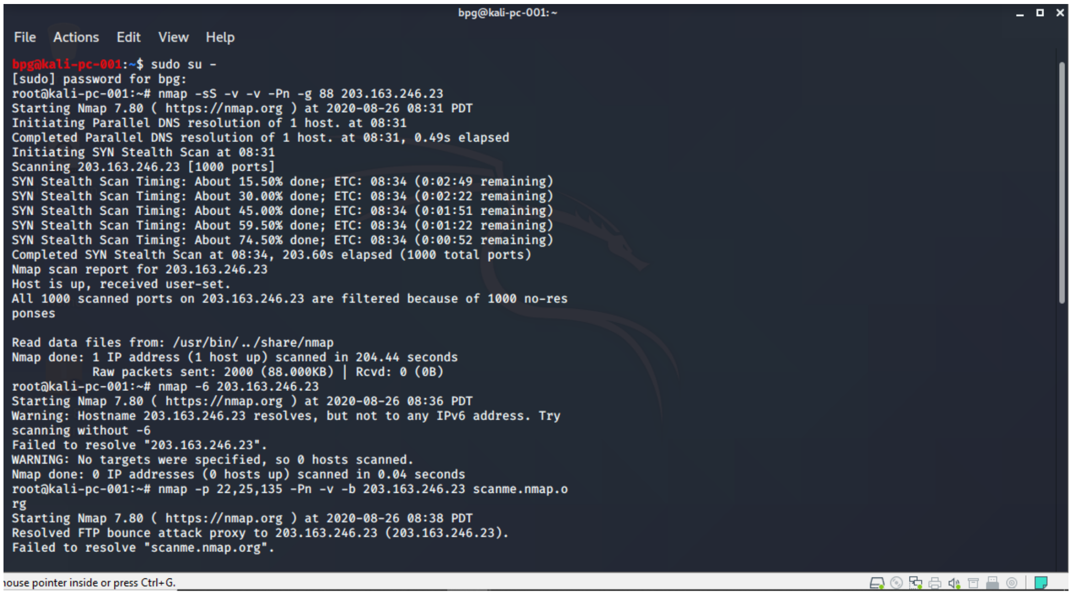
Again it is coming filtered for me so I'll further use the following command

Enter :**nmap -p 22,25,135 -Pn -v –b**203.163.246.23**scanme.nmap.org**

Again it is coming filtered for me so I'll further use the following command

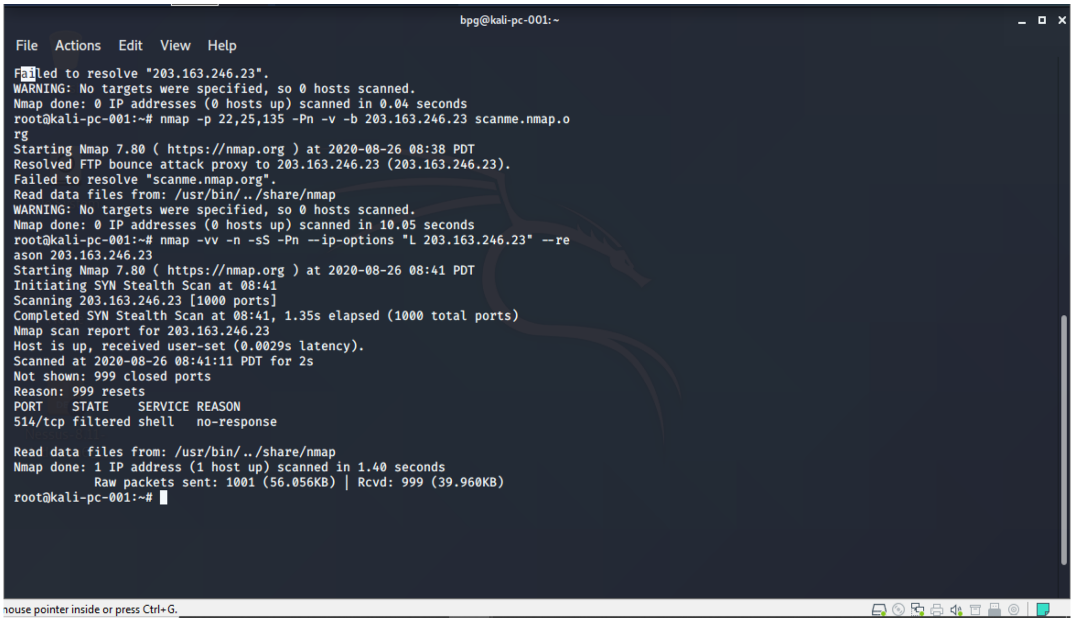
Enter: nmap -vv -n -sS -Pn --ip-options "L203.163.246.23" --reason203.163.246.23

Now I get only one port open as shown below



bpg@kali-pc-001:~
File Actions Edit View Help
ouse pointer inside or press Ctrl+G.

```
bpg@kali-pc-001:~$ sudo su -
[sudo] password for bpg:
root@kali-pc-001:~# nmap -sS -v -v -Pn -g 88 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 08:31 PDT
Initiating Parallel DNS resolution of 1 host. at 08:31
Completed Parallel DNS resolution of 1 host. at 08:31, 0.49s elapsed
Initiating SYN Stealth Scan at 08:31
Scanning 203.163.246.23 [1000 ports]
SYN Stealth Scan Timing: About 15.50% done; ETC: 08:34 (0:02:49 remaining)
SYN Stealth Scan Timing: About 30.00% done; ETC: 08:34 (0:02:22 remaining)
SYN Stealth Scan Timing: About 45.00% done; ETC: 08:34 (0:01:51 remaining)
SYN Stealth Scan Timing: About 59.50% done; ETC: 08:34 (0:01:22 remaining)
SYN Stealth Scan Timing: About 74.50% done; ETC: 08:34 (0:00:52 remaining)
Completed SYN Stealth Scan at 08:34, 203.60s elapsed (1000 total ports)
Nmap scan report for 203.163.246.23
Host is up, received user-set.
All 1000 scanned ports on 203.163.246.23 are filtered because of 1000 no-res
ponses

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 204.44 seconds
           Raw packets sent: 2000 (88.000KB) | Rcvd: 0 (0B)
root@kali-pc-001:~# nmap -6 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 08:36 PDT
Warning: Hostname 203.163.246.23 resolves, but not to any IPv6 address. Try
scanning without -6
Failed to resolve "203.163.246.23".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds
root@kali-pc-001:~# nmap -p 22,25,135 -Pn -v -b 203.163.246.23 scanme.nmap.o
rg
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 08:38 PDT
Resolved FTP bounce attack proxy to 203.163.246.23 (203.163.246.23).
Failed to resolve "scanme.nmap.org".
```



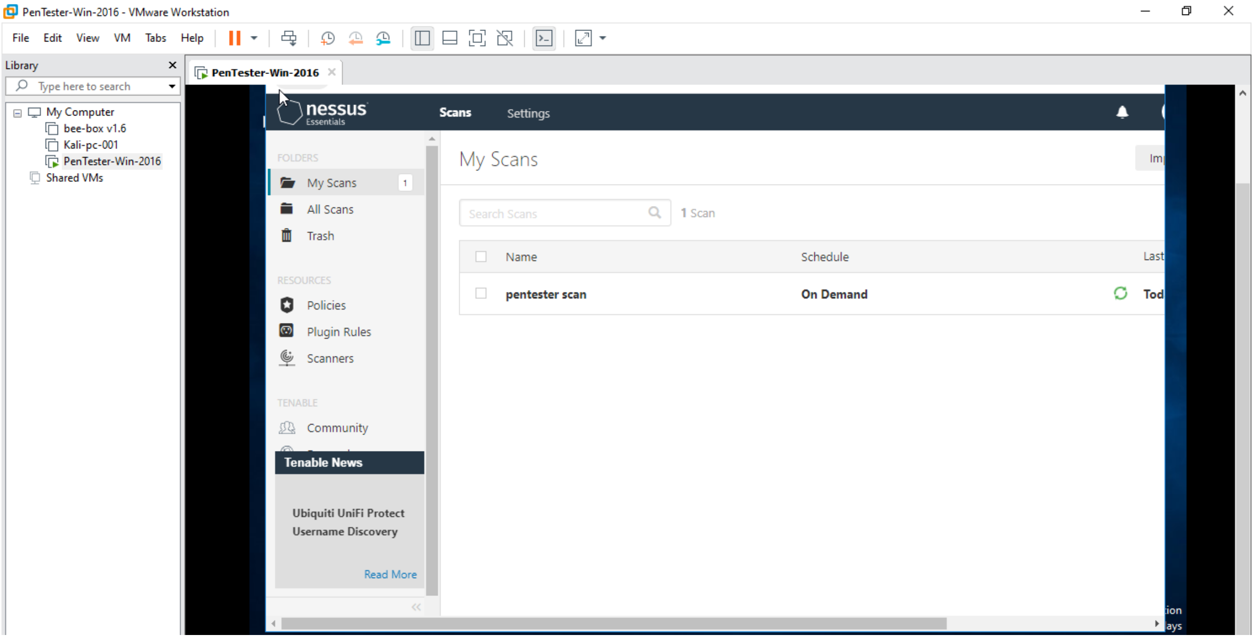
bpg@kali-pc-001:~
File Actions Edit View Help
ouse pointer inside or press Ctrl+G.

```
Failed to resolve "203.163.246.23".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds
root@kali-pc-001:~# nmap -p 22,25,135 -Pn -v -b 203.163.246.23 scanme.nmap.o
rg
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 08:38 PDT
Resolved FTP bounce attack proxy to 203.163.246.23 (203.163.246.23).
Failed to resolve "scanme.nmap.org".
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.05 seconds
root@kali-pc-001:~# nmap -vv -n -sS -Pn --ip-options "L 203.163.246.23" --re
ason 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 08:41 PDT
Initiating SYN Stealth Scan at 08:41
Scanning 203.163.246.23 [1000 ports]
Completed SYN Stealth Scan at 08:41, 1.35s elapsed (1000 total ports)
Nmap scan report for 203.163.246.23
Host is up, received user-set (0.0029s latency).
Scanned at 2020-08-26 08:41:11 PDT for 2s
Not shown: 999 closed ports
Reason: 999 resets
PORT    STATE    SERVICE REASON
514/tcp filtered shell   no-response

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
           Raw packets sent: 1001 (56.056KB) | Rcvd: 999 (39.960KB)
root@kali-pc-001:~# 
```

***I get only 1 port open which is 514/tcp**

Q4.Install nessus in a VM and scan your laptop/desktop for CVE

1)

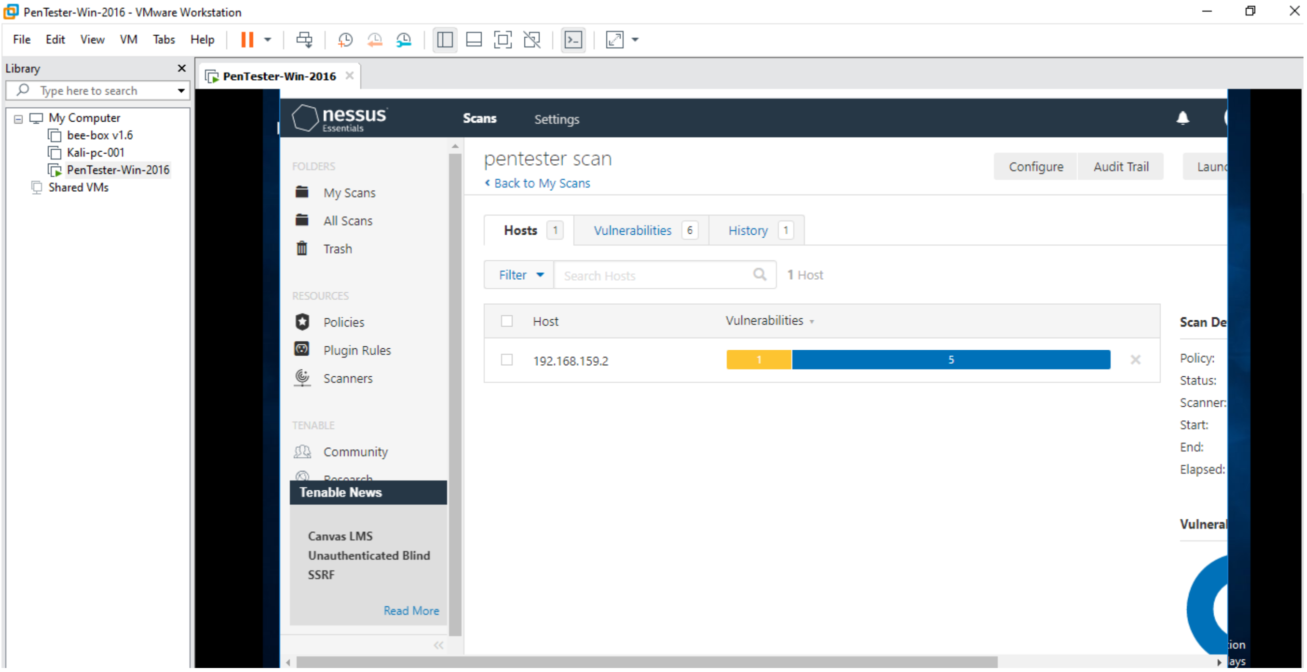


My Scans

Search Scans 1 Scan

Name	Schedule	Last
pentester scan	On Demand	Tod

2)



pentester scan

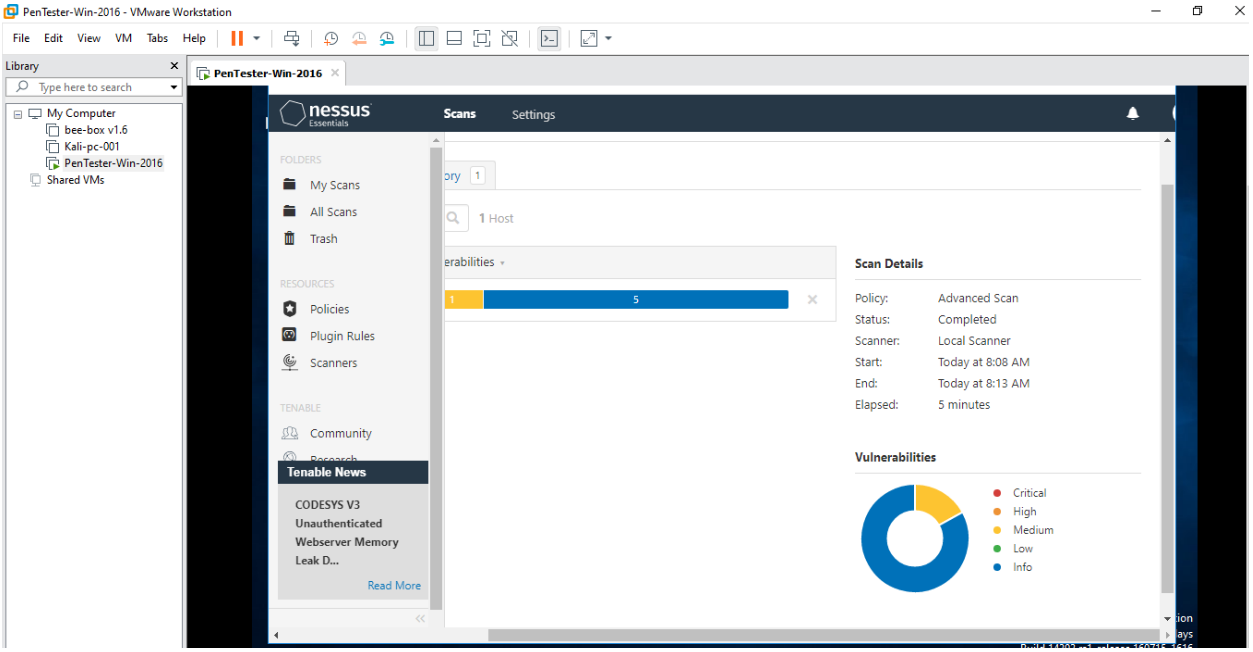
1 Host

Host	Vulnerabilities
192.168.159.2	1 5

Scan De

Policy:
Status:
Scanner:
Start:
End:
Elapsed:

3)



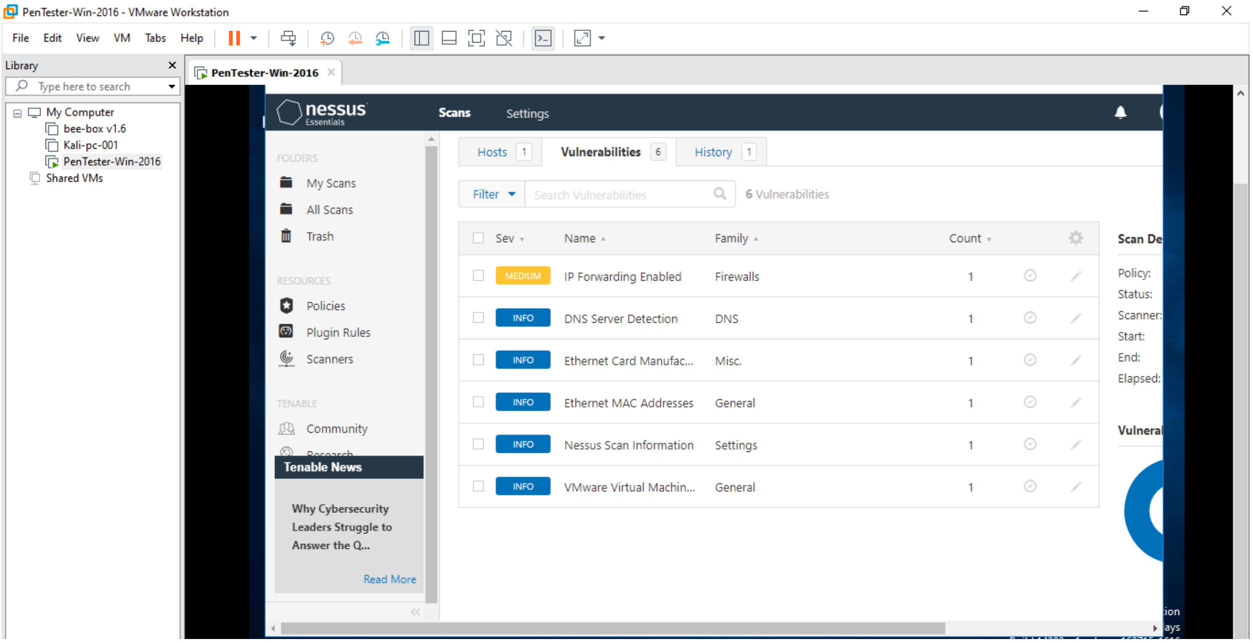
Scan Details

Policy: Advanced Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 8:08 AM
End: Today at 8:13 AM
Elapsed: 5 minutes

Vulnerabilities

- ● Critical
- ● High
- ● Medium
- ● Low
- ● Info

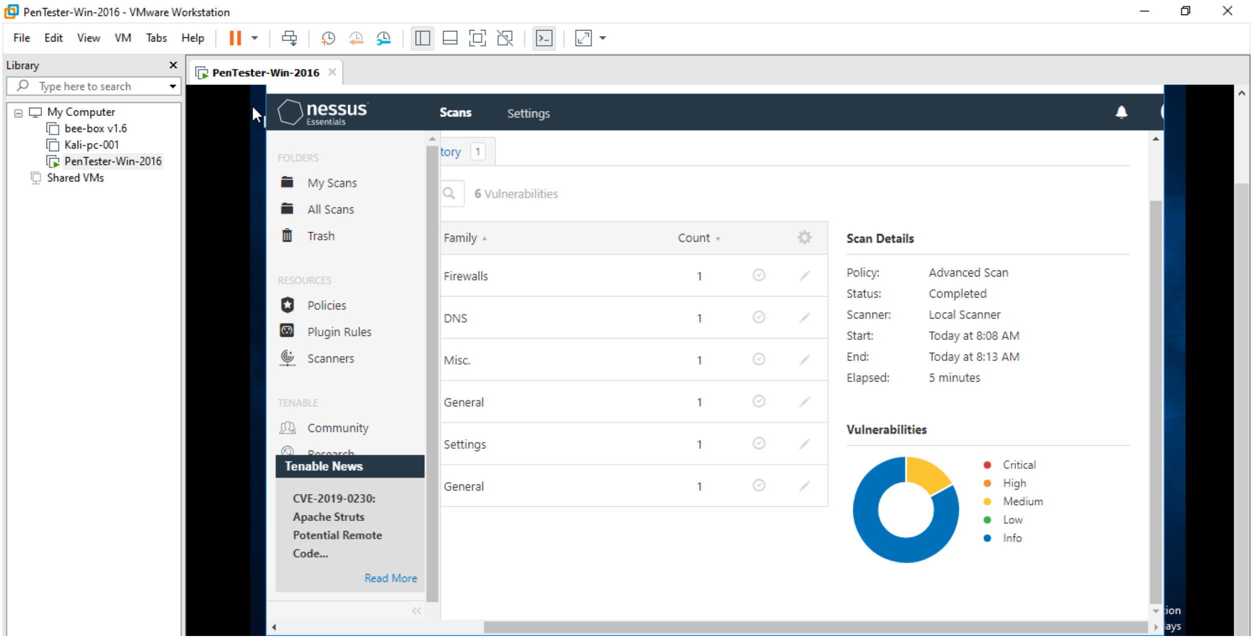
4)



6 Vulnerabilities

Sev	Name	Family	Count
MEDIUM	IP Forwarding Enabled	Firewalls	1
INFO	DNS Server Detection	DNS	1
INFO	Ethernet Card Manufac...	Misc.	1
INFO	Ethernet MAC Addresses	General	1
INFO	Nessus Scan Information	Settings	1
INFO	VMware Virtual Machin...	General	1

5)



6 Vulnerabilities

Family	Count
Firewalls	1
DNS	1
Misc.	1
General	1
Settings	1
General	1

Scan Details

Policy: Advanced Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 8:08 AM
End: Today at 8:13 AM
Elapsed: 5 minutes

Vulnerabilities

Tenable News

CVE-2019-0230: Apache Struts Potential Remote Code...

Read More