Lets Upgrade

Cyber Security | August 2020

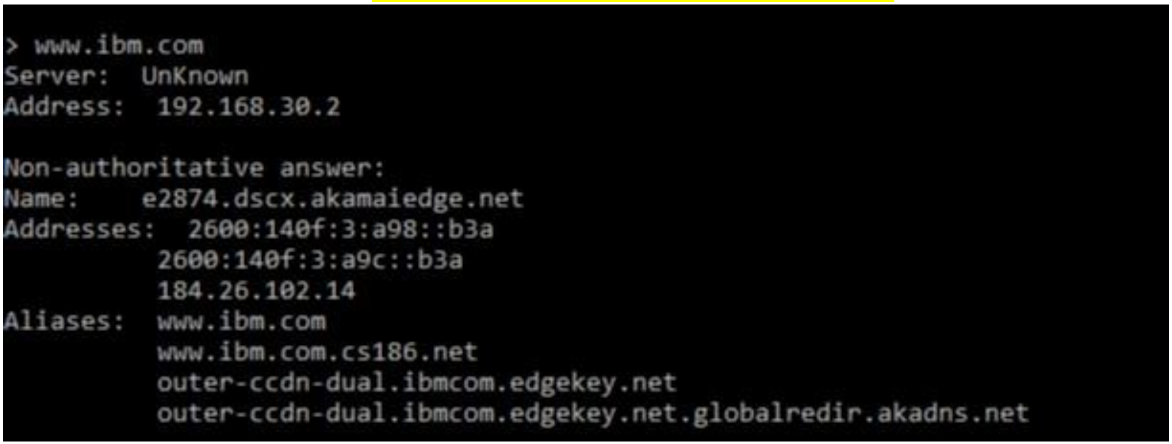
Assignment Day 4 | 23rd August 2020

Name: Athira Rajeev
Email: athirarajeev777@gmail.com

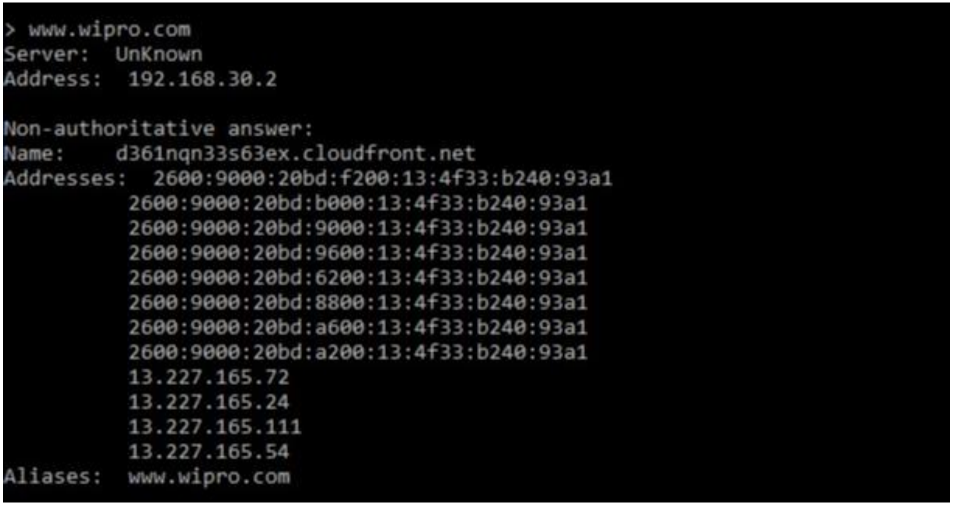
Question 1:

Find out the mail servers of the following domain :
Ibm.com
Wipro.com

Solution:
Step 1 - open cmd on windows
Step 2 - write command “nslookup”
Step 3 - type command “set type=mx” and then type site name
Mail servers of ibm.com = mx0b-001b2d01.pphosted.com and mx0a-001b2d01.pphosted.com
Mail servers of wipro.com = wipro-com.mail.protection.outlook.com



```
> www.ibm.com
Server:  UnKnown
Address:  192.168.30.2

Non-authoritative answer:
Name:    e2874.dscx.akamaiedge.net
Addresses:  2600:140f:3:a98::b3a
          2600:140f:3:a9c::b3a
          184.26.102.14
Aliases:  www.ibm.com
          www.ibm.com.cs186.net
          outer-ccdn-dual.ibmcom.edgekey.net
          outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net
```



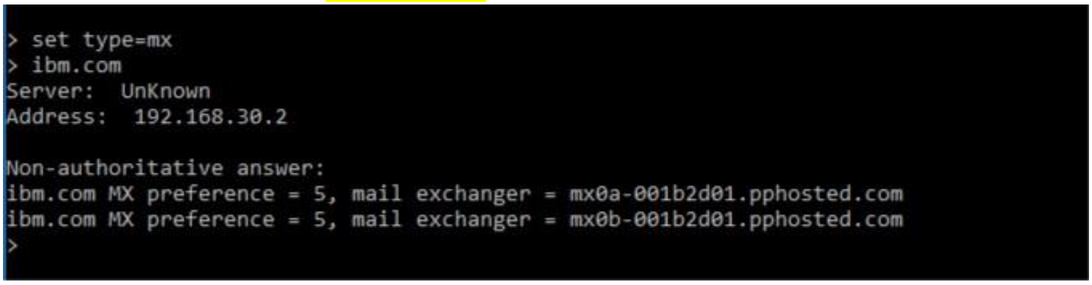
```
> www.wipro.com
Server:  UnKnown
Address:  192.168.30.2

Non-authoritative answer:
Name:    d361nqn33s63ex.cloudfront.net
Addresses:  2600:9000:20bd:f200:13:4f33:b240:93a1
          2600:9000:20bd:b000:13:4f33:b240:93a1
          2600:9000:20bd:9000:13:4f33:b240:93a1
          2600:9000:20bd:9600:13:4f33:b240:93a1
          2600:9000:20bd:6200:13:4f33:b240:93a1
          2600:9000:20bd:8800:13:4f33:b240:93a1
          2600:9000:20bd:a600:13:4f33:b240:93a1
          2600:9000:20bd:a200:13:4f33:b240:93a1
          13.227.165.72
          13.227.165.24
          13.227.165.111
          13.227.165.54
Aliases:  www.wipro.com
```

Question 2:

Find the locations, where these email servers are hosted.

Solution:

Step 1 - type command “set type=mx” and then type site name



```
> set type=mx
> ibm.com
Server:  UnKnown
Address:  192.168.30.2

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

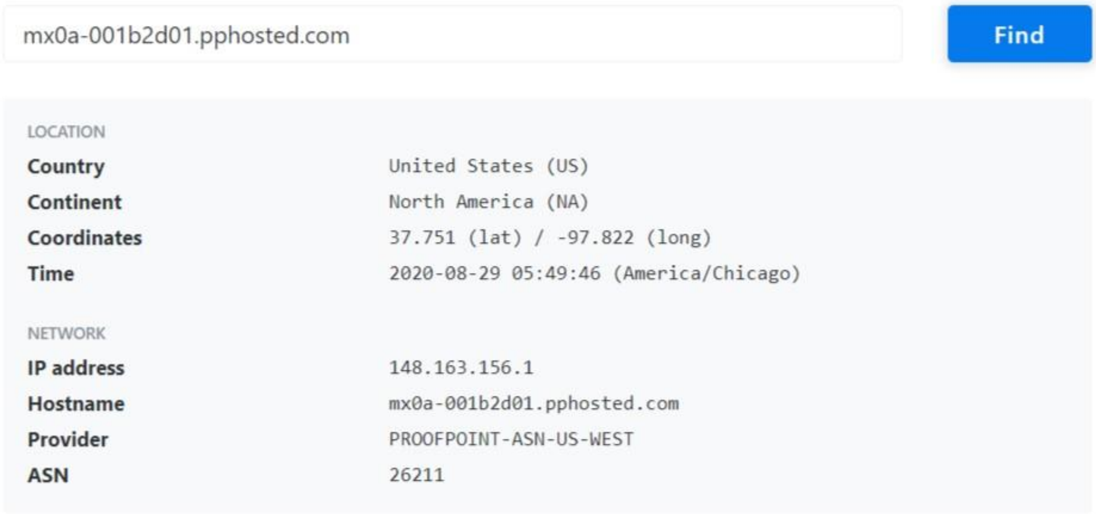
Step 2 - Open google chrome. Open IP Location Finder

Step 3 - Copy paste the url and find the location

Location of mail server of ibm.com =

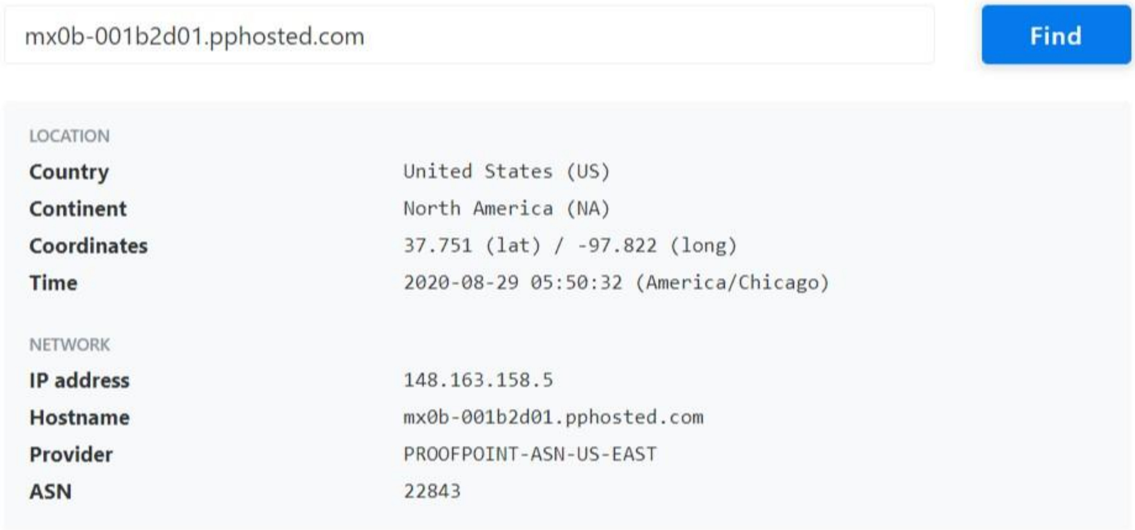
mx0a-001b2d01.pphosted.com

mx0b-001b2d01.pphosted.com



mx0a-001b2d01.pphosted.com

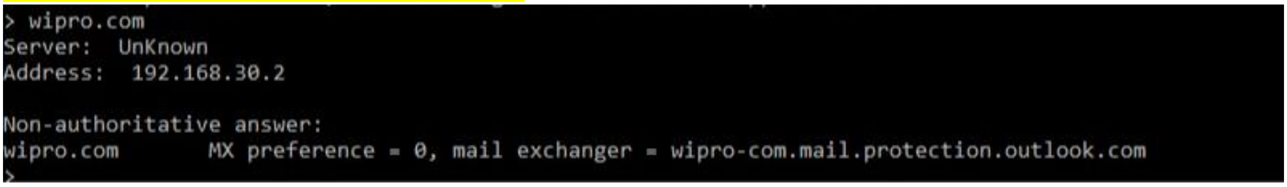
LOCATION	
Country	United States (US)
Continent	North America (NA)
Coordinates	37.751 (lat) / -97.822 (long)
Time	2020-08-29 05:49:46 (America/Chicago)
NETWORK	
IP address	148.163.156.1
Hostname	mx0a-001b2d01.pphosted.com
Provider	PROOFPOINT-ASN-US-WEST
ASN	26211



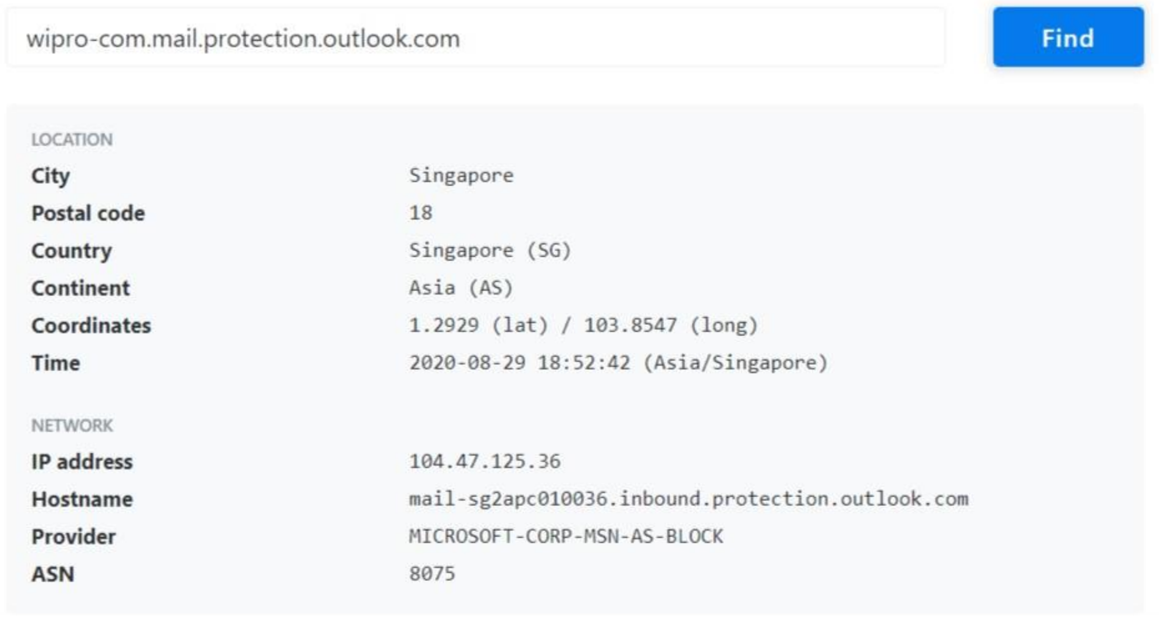
mx0b-001b2d01.pphosted.com

LOCATION	
Country	United States (US)
Continent	North America (NA)
Coordinates	37.751 (lat) / -97.822 (long)
Time	2020-08-29 05:50:32 (America/Chicago)
NETWORK	
IP address	148.163.158.5
Hostname	mx0b-001b2d01.pphosted.com
Provider	PROOFPOINT-ASN-US-EAST
ASN	22843

Location of mail server of wipro.com = wipro-com.mail.protection.outlook.com



```
> wipro.com
Server:  UnKnown
Address:  192.168.30.2

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



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	2020-08-29 18:52:42 (Asia/Singapore)
NETWORK	
IP address	104.47.125.36
Hostname	mail-sg2apc010036.inbound.protection.outlook.com
Provider	MICROSOFT-CORP-MSN-AS-BLOCK
ASN	8075

Question 3:

Scan and find out port numbers open 203.163.246.23

Step 1 - Open Kali pc

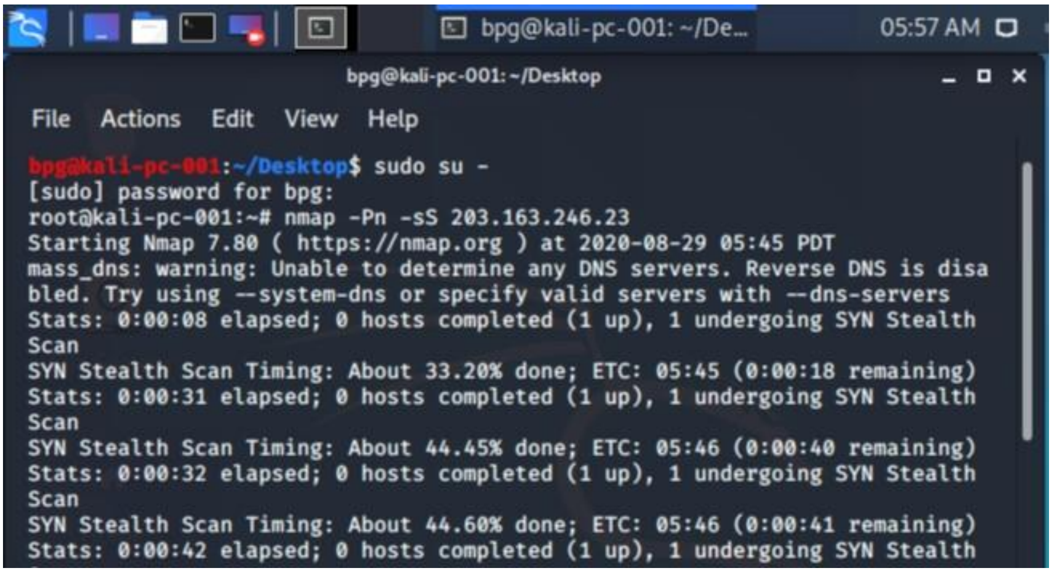
Step 2 - Open terminal in kali Linux

Step 3 - Type command:

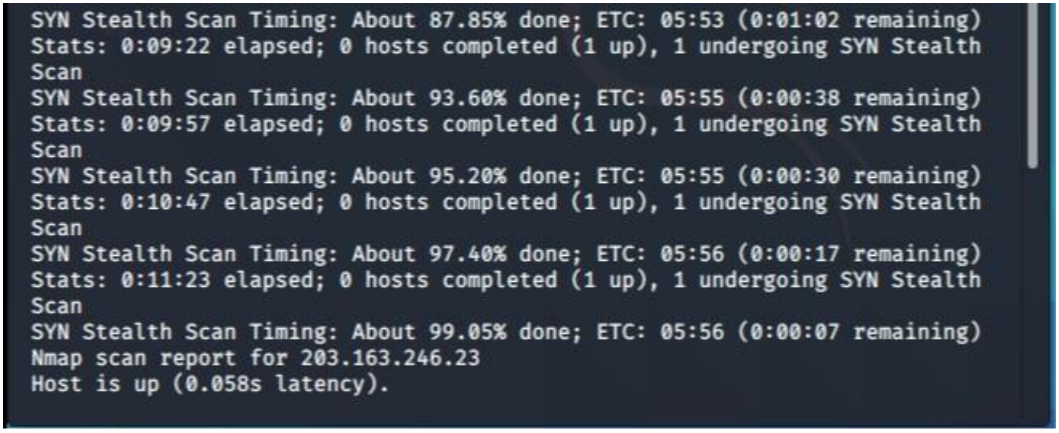
sudo su –

Enter password

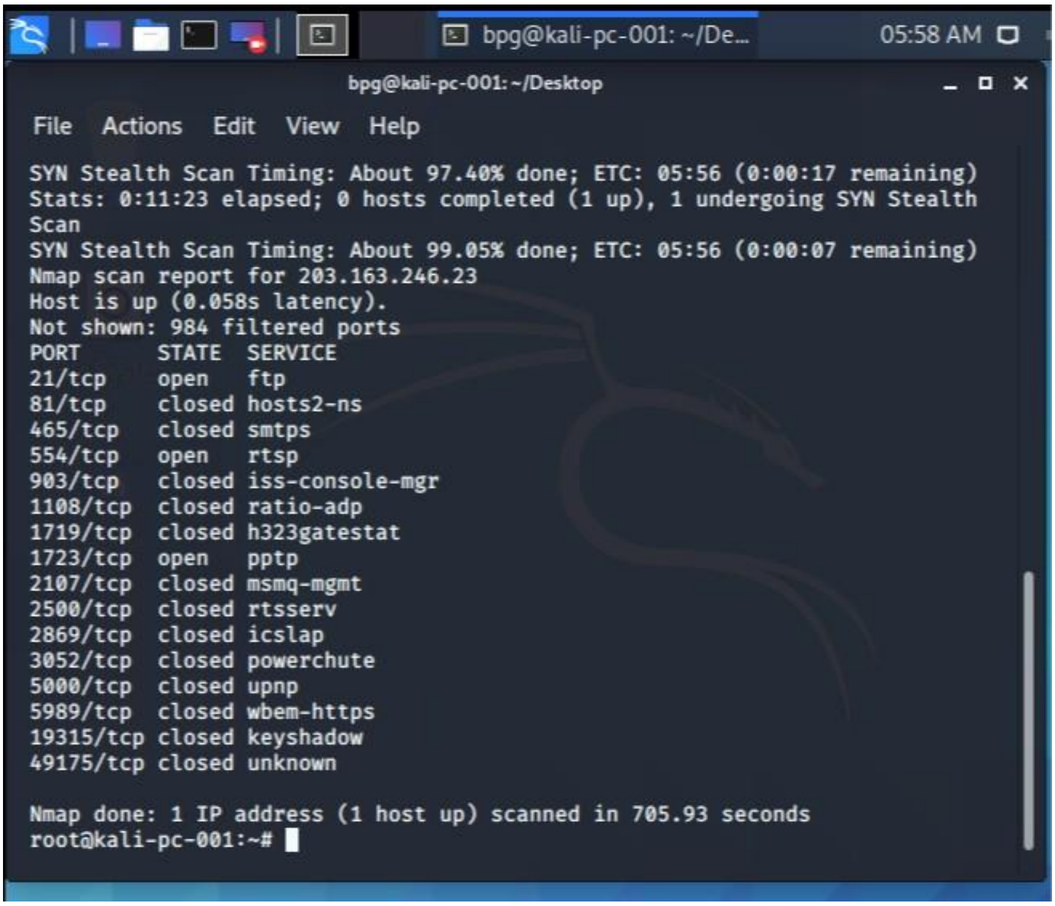
nmap –Pn –sS 203.163.246.23



```
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 2020-08-29 05:45 PDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disa
bled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 33.20% done; ETC: 05:45 (0:00:18 remaining)
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 44.45% done; ETC: 05:46 (0:00:40 remaining)
Stats: 0:00:32 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 44.60% done; ETC: 05:46 (0:00:41 remaining)
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
```



```
SYN Stealth Scan Timing: About 87.85% done; ETC: 05:53 (0:01:02 remaining)
Stats: 0:09:22 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 93.60% done; ETC: 05:55 (0:00:38 remaining)
Stats: 0:09:57 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 95.20% done; ETC: 05:55 (0:00:30 remaining)
Stats: 0:10:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 97.40% done; ETC: 05:56 (0:00:17 remaining)
Stats: 0:11:23 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 99.05% done; ETC: 05:56 (0:00:07 remaining)
Nmap scan report for 203.163.246.23
Host is up (0.058s latency).
```



```
SYN Stealth Scan Timing: About 97.40% done; ETC: 05:56 (0:00:17 remaining)
Stats: 0:11:23 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 99.05% done; ETC: 05:56 (0:00:07 remaining)
Nmap scan report for 203.163.246.23
Host is up (0.058s latency).
Not shown: 984 filtered ports
PORT      STATE  SERVICE
21/tcp    open   ftp
81/tcp    closed hosts2-ns
465/tcp   closed smtps
554/tcp   open   rtsp
903/tcp   closed iss-console-mgr
1108/tcp  closed ratio-adp
1719/tcp  closed h323gatestat
1723/tcp  open   pptp
2107/tcp  closed msmq-mgmt
2500/tcp  closed rtsserv
2869/tcp  closed icslap
3052/tcp  closed powerchute
5000/tcp  closed upnp
5989/tcp  closed wbem-https
19315/tcp closed keyshadow
49175/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 705.93 seconds
root@kali-pc-001:~#
```

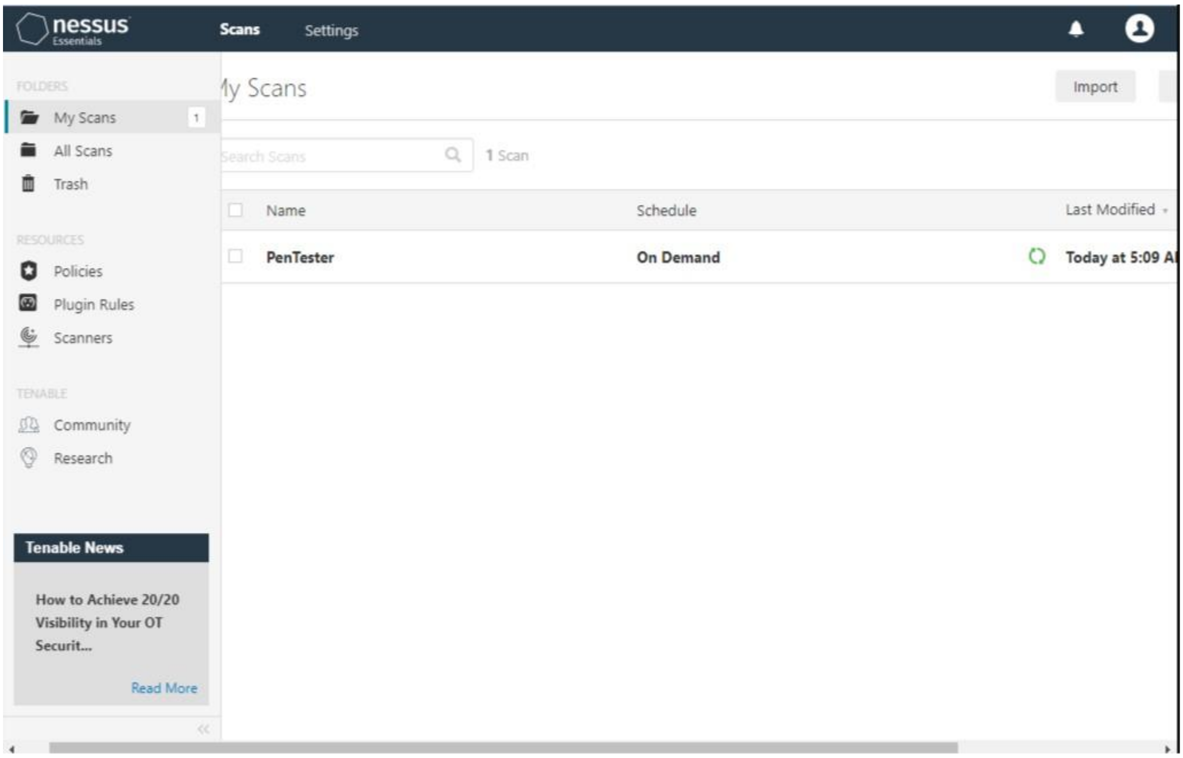
Question 4:

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

Solution:

Step 1 - Open PenTester in VMware workstation
Step 2 - Install Google Chrome. Install Nessus
Step 3 -

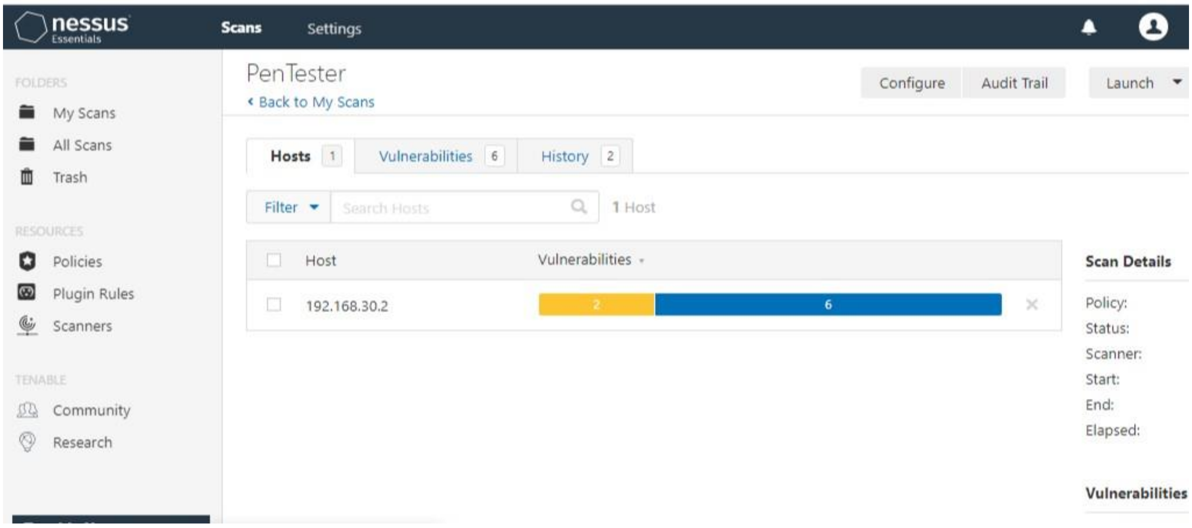
- Click on All scans
- Create a new scan
- Advance settings
- Windows
- Fill the required blanks in credentials as well
- Launch



My Scans

1 Scan

Name	Schedule	Last Modified
PenTester	On Demand	Today at 5:09 A



PenTester

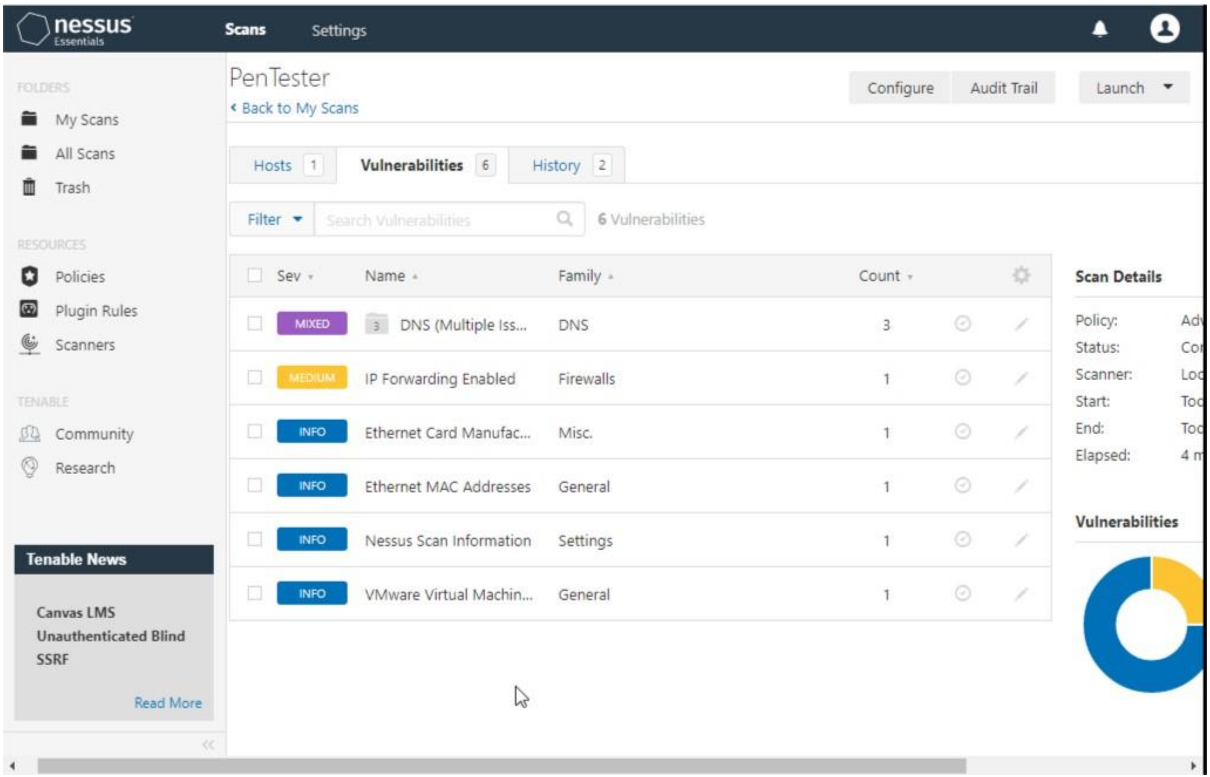
1 Host

Host	Vulnerabilities
192.168.30.2	2 6

Scan Details

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

Vulnerabilities



PenTester

6 Vulnerabilities

Sev	Name	Family	Count
MIXED	3 DNS (Multiple Iss...	DNS	3
MEDIUM	IP Forwarding Enabled	Firewalls	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

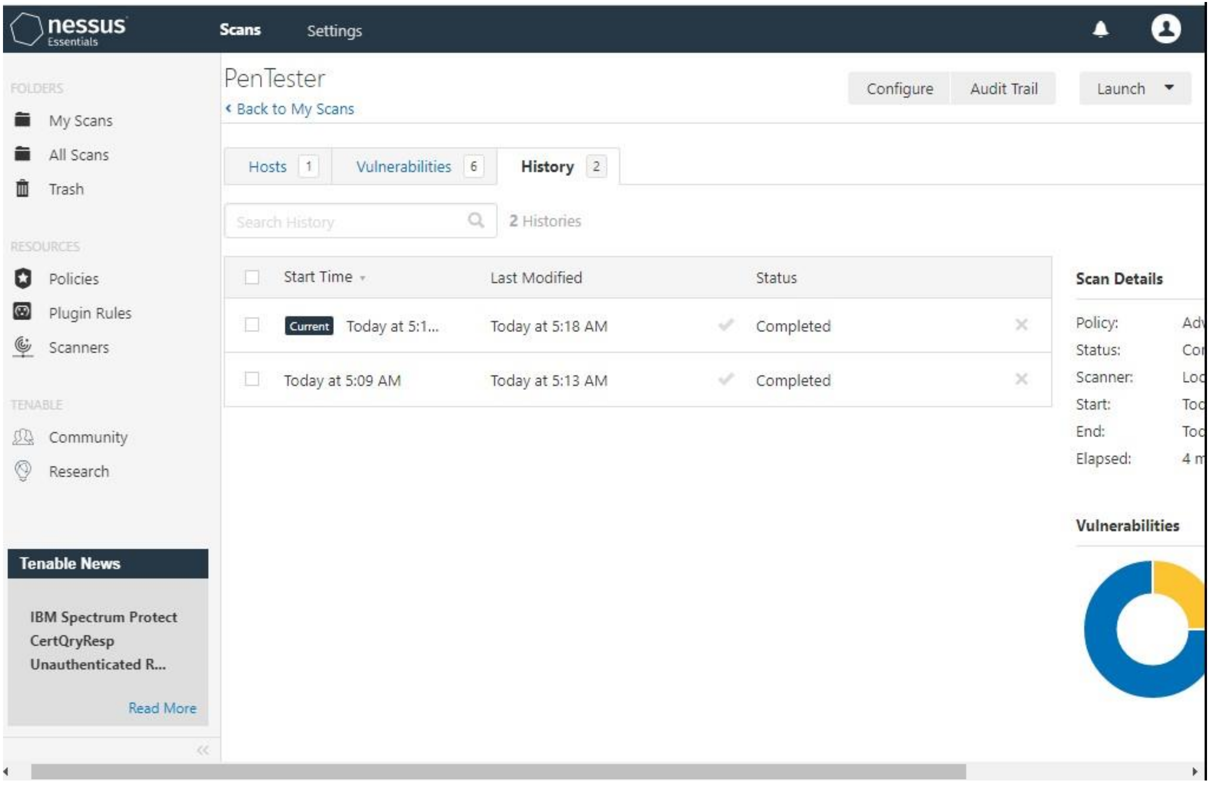
Scan Details

Policy: Ad
Status: Co
Scanner: Lo
Start: To
End: To
Elapsed: 4 m

Vulnerabilities

Tenable News

Canvas LMS Unauthenticated Blind SSRF



PenTester

2 Histories

Start Time	Last Modified	Status
Current Today at 5:1...	Today at 5:18 AM	Completed
Today at 5:09 AM	Today at 5:13 AM	Completed

Scan Details

Policy: Ad
Status: Co
Scanner: Lo
Start: To
End: To
Elapsed: 4 m

Vulnerabilities

Tenable News

IBM Spectrum Protect CertQryResp Unauthenticated R...