Lets Upgrade

Cyber Security | August 2020

Assignment Day 4 | 23rd August 2020

Name :- Amit Meena

Email :-meenaji.024@gmail.com

Question 1:

Find out the mail servers of the following domain:

1. Ibm.com

2.Wipro.com

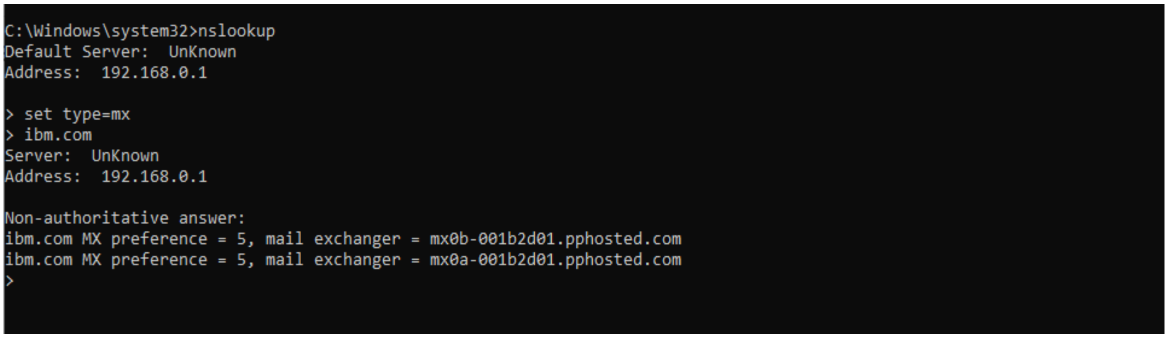
Solution:-

Step 1:- Open command prompt.

Step 2:- Type “nslookup”

Step 3:- “set type=mx”

Step 4:- ibm.com



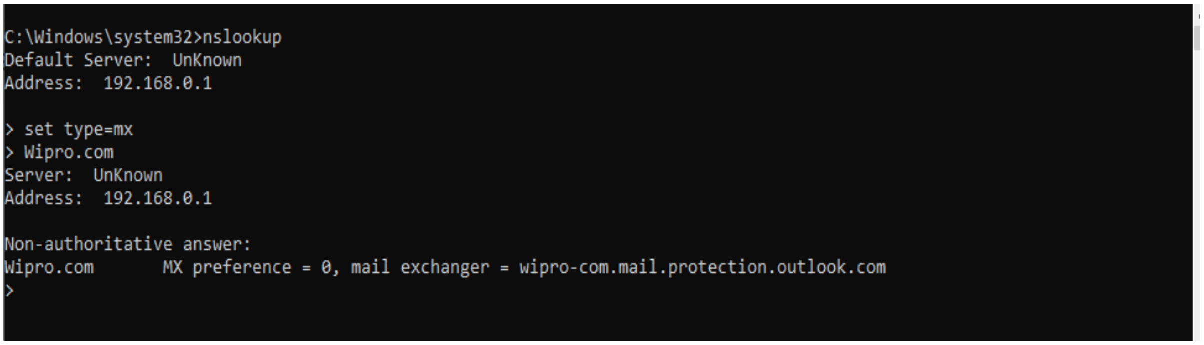
```
C:\Windows\system32>nslookup
Default Server:  UnKnown
Address:  192.168.0.1

> set type=mx
> ibm.com
Server:  UnKnown
Address:  192.168.0.1

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
>
```

Step 1:- Open command prompt.

Step 2:- Type “nslookup”

Step 3:- “set type=mx”

Step 4:- wipro.com



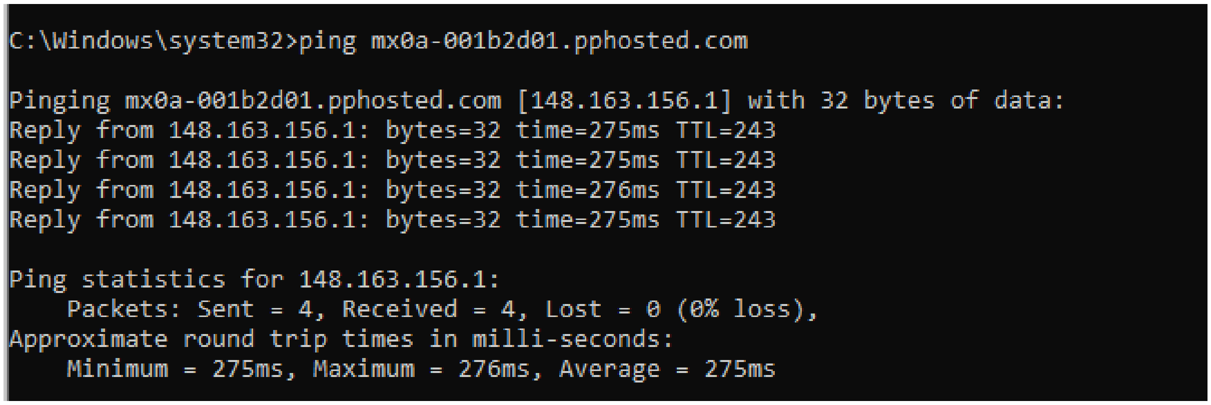
```
C:\Windows\system32>nslookup
Default Server:  UnKnown
Address:  192.168.0.1

> set type=mx
> Wipro.com
Server:  UnKnown
Address:  192.168.0.1

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

Question 2:

Find the locations, where these email servers are hosted.

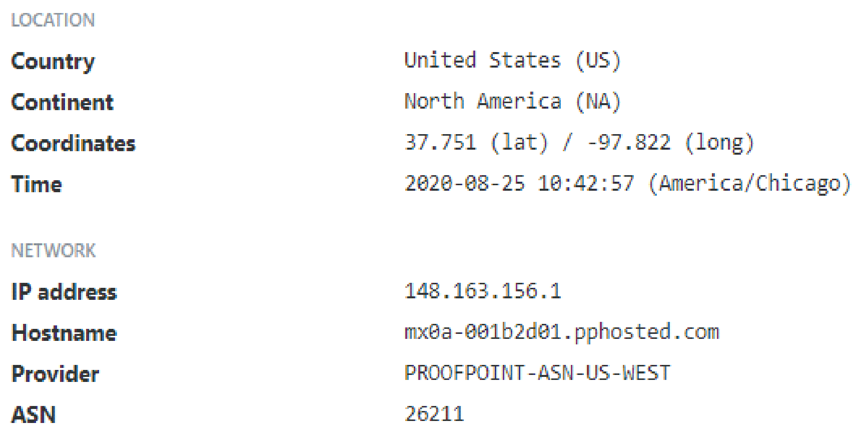
Solution:-

1)(a) ibm email server mx0a-001b2d01.pphosted.com



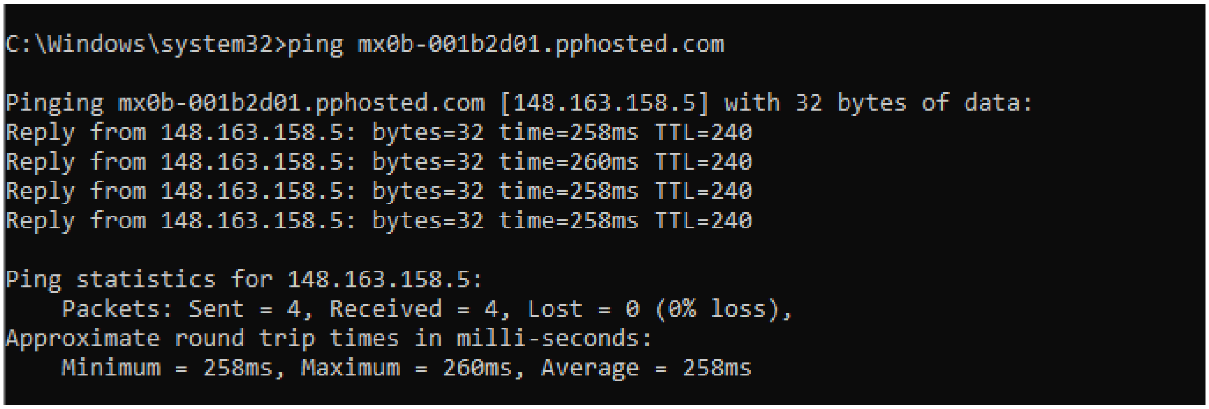
```
C:\Windows\system32>ping mx0a-001b2d01.pphosted.com

Pinging mx0a-001b2d01.pphosted.com [148.163.156.1] with 32 bytes of data:
Reply from 148.163.156.1: bytes=32 time=275ms TTL=243
Reply from 148.163.156.1: bytes=32 time=275ms TTL=243
Reply from 148.163.156.1: bytes=32 time=276ms TTL=243
Reply from 148.163.156.1: bytes=32 time=275ms TTL=243

Ping statistics for 148.163.156.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 275ms, Maximum = 276ms, Average = 275ms
```

LOCATION OF IBM (mx0a-001b2d01.pphosted.com) MAIL SERVER



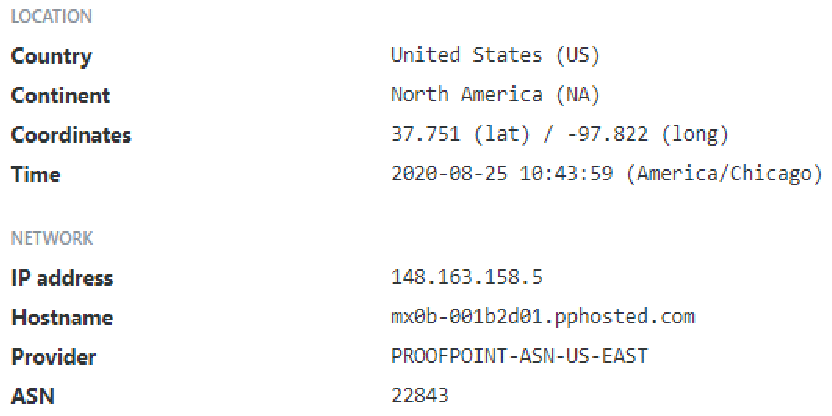
LOCATION	
Country	United States (US)
Continent	North America (NA)
Coordinates	37.751 (lat) / -97.822 (long)
Time	2020-08-25 10:42:57 (America/Chicago)
NETWORK	
IP address	148.163.156.1
Hostname	mx0a-001b2d01.pphosted.com
Provider	PROOFPOINT-ASN-US-WEST
ASN	26211

1)(b) ibm email server mx0b-001b2d01.pphosted.com



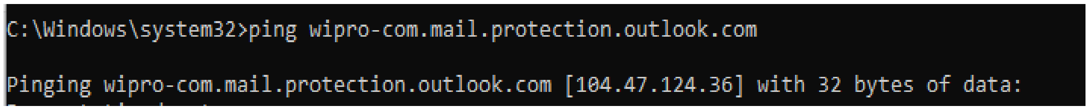
```
C:\Windows\system32>ping mx0b-001b2d01.pphosted.com

Pinging mx0b-001b2d01.pphosted.com [148.163.158.5] with 32 bytes of data:
Reply from 148.163.158.5: bytes=32 time=258ms TTL=240
Reply from 148.163.158.5: bytes=32 time=260ms TTL=240
Reply from 148.163.158.5: bytes=32 time=258ms TTL=240
Reply from 148.163.158.5: bytes=32 time=258ms TTL=240

Ping statistics for 148.163.158.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 258ms, Maximum = 260ms, Average = 258ms
```

LOCATION OF IBM (mx0b-001b2d01.pphosted.com) MAIL SERVER



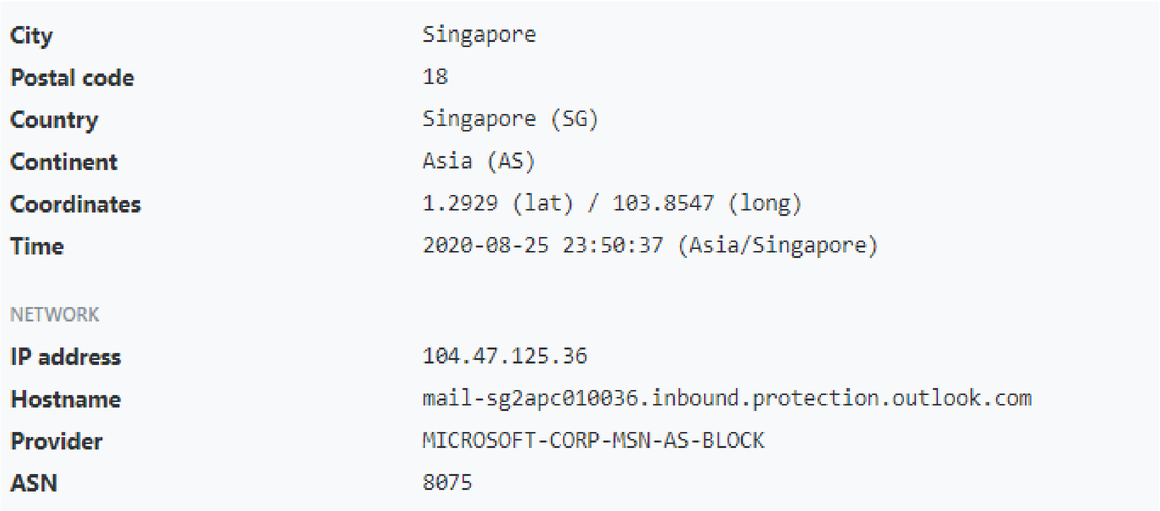
LOCATION	
Country	United States (US)
Continent	North America (NA)
Coordinates	37.751 (lat) / -97.822 (long)
Time	2020-08-25 10:43:59 (America/Chicago)
NETWORK	
IP address	148.163.158.5
Hostname	mx0b-001b2d01.pphosted.com
Provider	PROOFPOINT-ASN-US-EAST
ASN	22843

2) Wipro Email Server wipro-com.mail.protection.outlook.com



```
C:\Windows\system32>ping wipro-com.mail.protection.outlook.com

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

LOCATION OF WIPRO MAIL SERVER



City	Singapore
Postal code	18
Country	Singapore (SG)
Continent	Asia (AS)
Coordinates	1.2929 (lat) / 103.8547 (long)
Time	2020-08-25 23:50:37 (Asia/Singapore)
NETWORK	
IP address	104.47.125.36
Hostname	mail-sg2apc010036.inbound.protection.outlook.com
Provider	MICROSOFT-CORP-MSN-AS-BLOCK
ASN	8075

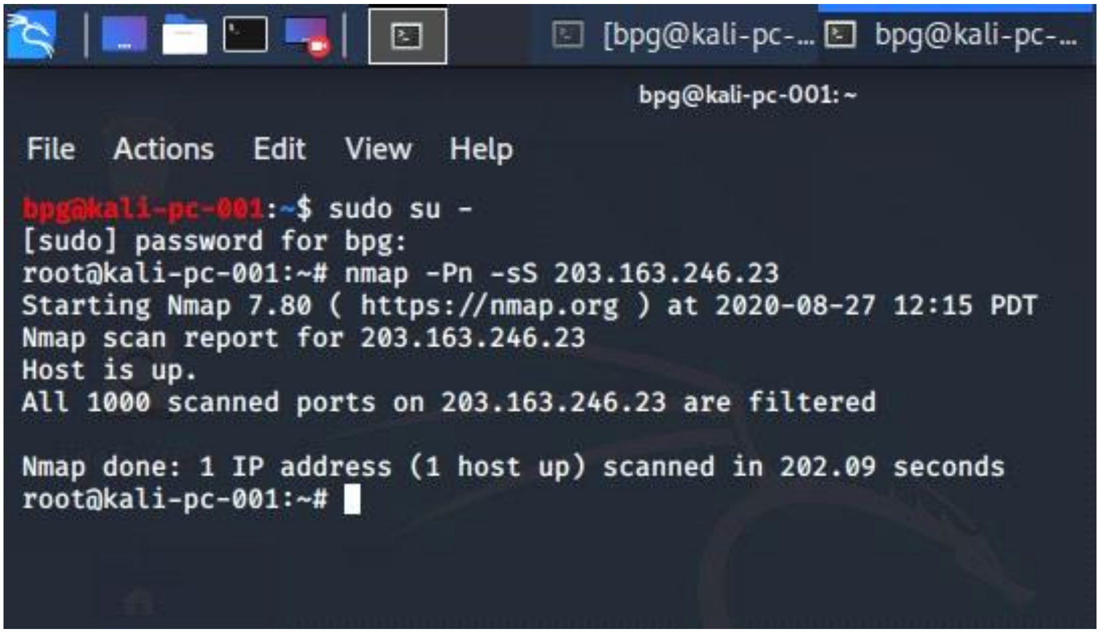
Question 3:

Scan and find out port numbers open **203.163.246.23**

Solution:-

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

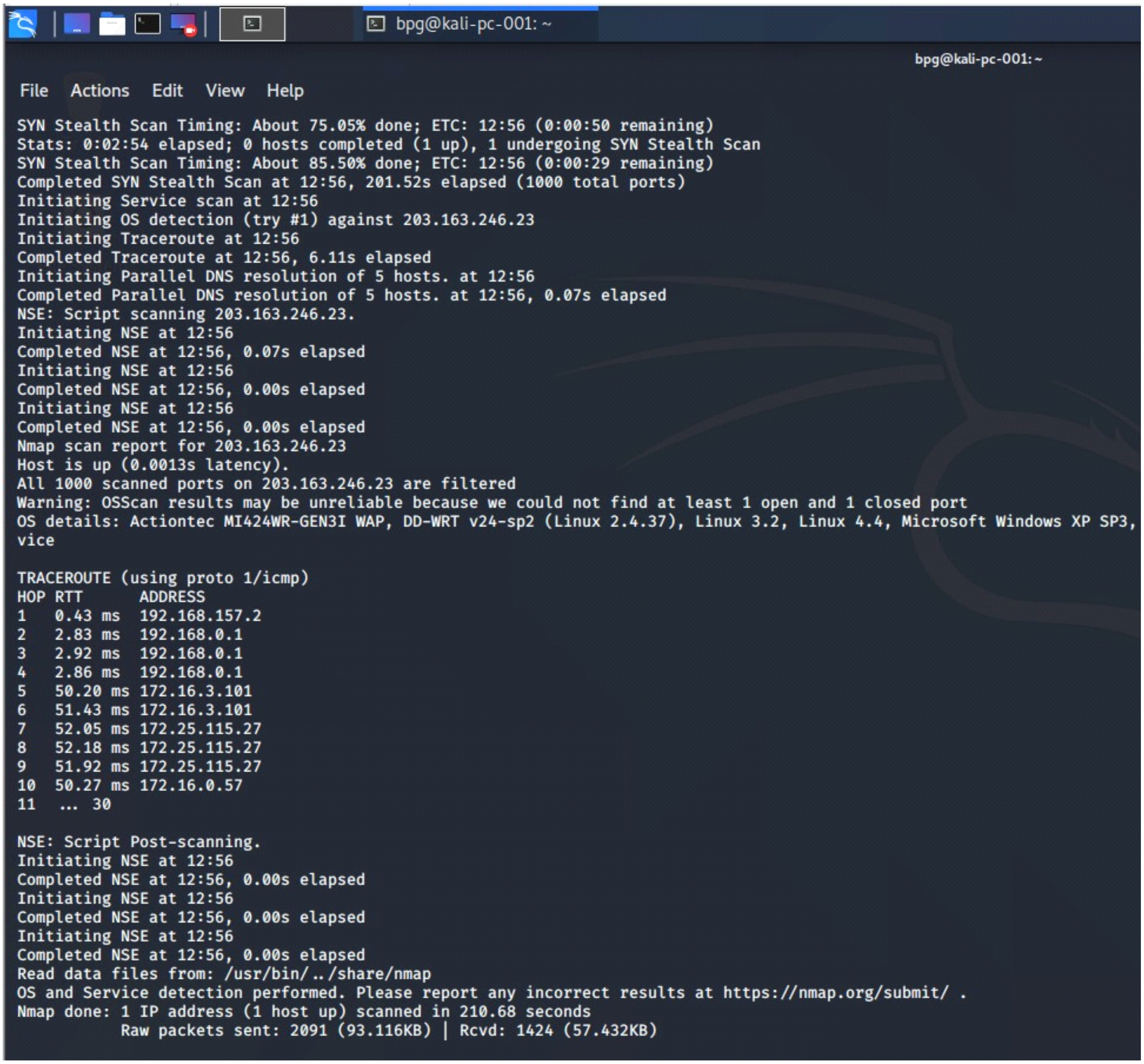
- Type:
- **sudo su –**
- Enter password
- Enter – **nmap –Pn –sS 203.163.246.23**



```
bpg@kali-pc-001:~$ 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 2020-08-27 12:15 PDT
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 202.09 seconds
root@kali-pc-001:~#
```

Same response even with stealth scan:

o Nmap -Pn -sS -A -v 203.163.246.23

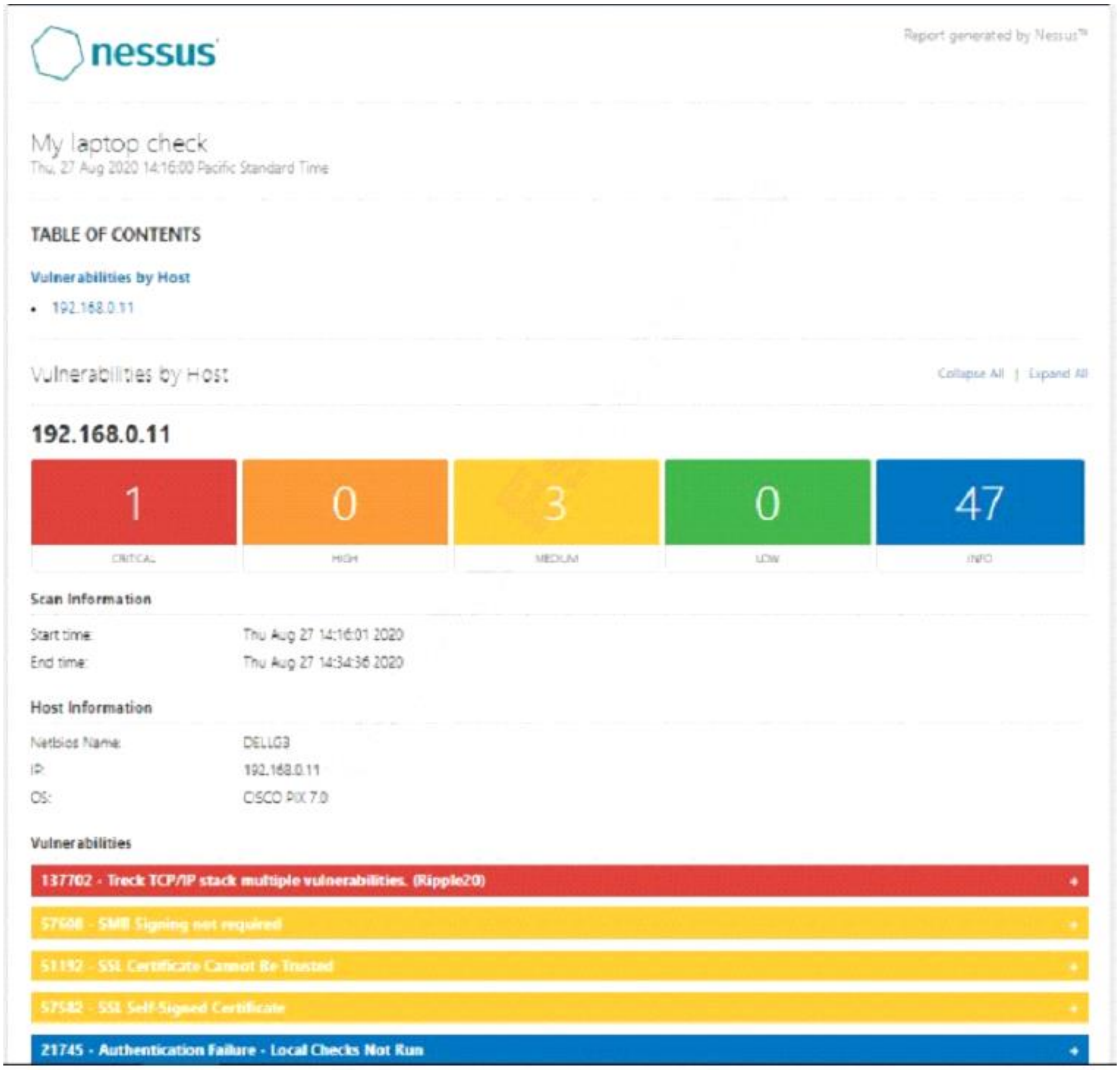


```
SYN Stealth Scan Timing: About 75.05% done; ETC: 12:56 (0:00:50 remaining)
Stats: 0:02:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.50% done; ETC: 12:56 (0:00:29 remaining)
Completed SYN Stealth Scan at 12:56, 201.52s elapsed (1000 total ports)
Initiating Service scan at 12:56
Initiating OS detection (try #1) against 203.163.246.23
Initiating Traceroute at 12:56
Completed Traceroute at 12:56, 6.11s elapsed
Initiating Parallel DNS resolution of 5 hosts. at 12:56
Completed Parallel DNS resolution of 5 hosts. at 12:56, 0.07s elapsed
NSE: Script scanning 203.163.246.23.
Initiating NSE at 12:56
Completed NSE at 12:56, 0.07s elapsed
Initiating NSE at 12:56
Completed NSE at 12:56, 0.00s elapsed
Initiating NSE at 12:56
Completed NSE at 12:56, 0.00s elapsed
Nmap scan report for 203.163.246.23
Host is up (0.0013s latency).
All 1000 scanned ports on 203.163.246.23 are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4, Microsoft Windows XP SP3,
vice

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   0.43 ms  192.168.157.2
2   2.83 ms  192.168.0.1
3   2.92 ms  192.168.0.1
4   2.86 ms  192.168.0.1
5   50.20 ms 172.16.3.101
6   51.43 ms 172.16.3.101
7   52.05 ms 172.25.115.27
8   52.18 ms 172.25.115.27
9   51.92 ms 172.25.115.27
10  50.27 ms 172.16.0.57
11  ... 30

NSE: Script Post-scanning.
Initiating NSE at 12:56
Completed NSE at 12:56, 0.00s elapsed
Initiating NSE at 12:56
Completed NSE at 12:56, 0.00s elapsed
Initiating NSE at 12:56
Completed NSE at 12:56, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 210.68 seconds
           Raw packets sent: 2091 (93.116KB) | Rcvd: 1424 (57.432KB)
```

Question 4:-

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

Solution:-



Report generated by Nessus™

My laptop check

Thu, 27 Aug 2020 14:16:00 Pacific Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

192.168.0.11

1	0	3	0	47
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Thu Aug 27 14:16:01 2020
End time:	Thu Aug 27 14:34:36 2020

Host Information

Netbios Name:	DELLG3
IP:	192.168.0.11
OS:	CISCO PIX 7.0

Vulnerabilities

- 137702 - Treck TCP/IP stack multiple vulnerabilities. (Ripple20) +
- 57608 - SMB Signing not required +
- 51192 - SSL Certificate Cannot Be Trusted +
- 57582 - SSL Self-Signed Certificate +
- 21745 - Authentication Failure - Local Checks Not Run +