

Day 4 – Assignment

Question 1 : Find out the mail servers of the following domain :

1. Ibm.com
2. Wipro.com

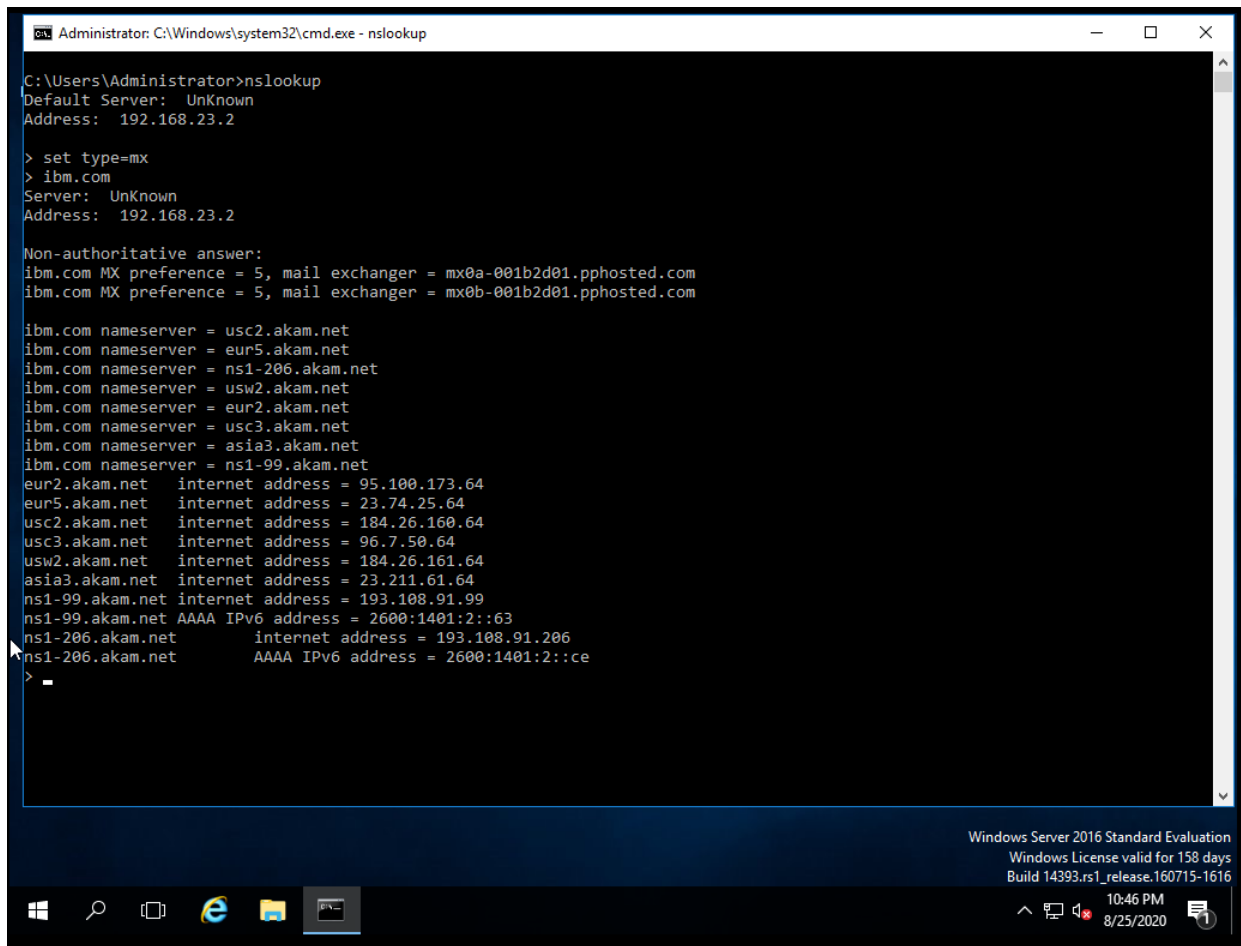
Solution:

Step 1: Open command prompt (press 'home(windows)+r' then type 'cmd' and press enter).

Step 2: Type "nslookup"

Step 3: > "set type=mx"

Step 4: > ibm.com



```
Administrator: C:\Windows\system32\cmd.exe - nslookup

C:\Users\Administrator>nslookup
Default Server:  UnKnown
Address:  192.168.23.2

> set type=mx
> ibm.com
Server:  UnKnown
Address:  192.168.23.2

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

ibm.com nameserver = usc2.akam.net
ibm.com nameserver = eur5.akam.net
ibm.com nameserver = ns1-206.akam.net
ibm.com nameserver = usw2.akam.net
ibm.com nameserver = eur2.akam.net
ibm.com nameserver = usc3.akam.net
ibm.com nameserver = asia3.akam.net
ibm.com nameserver = ns1-99.akam.net
eur2.akam.net internet address = 95.100.173.64
eur5.akam.net internet address = 23.74.25.64
usc2.akam.net internet address = 184.26.160.64
usc3.akam.net internet address = 96.7.50.64
usw2.akam.net internet address = 184.26.161.64
asia3.akam.net internet address = 23.211.61.64
ns1-99.akam.net internet address = 193.108.91.99
ns1-99.akam.net AAAA IPv6 address = 2600:1401:2::63
ns1-206.akam.net internet address = 193.108.91.206
ns1-206.akam.net AAAA IPv6 address = 2600:1401:2::ce
>
```

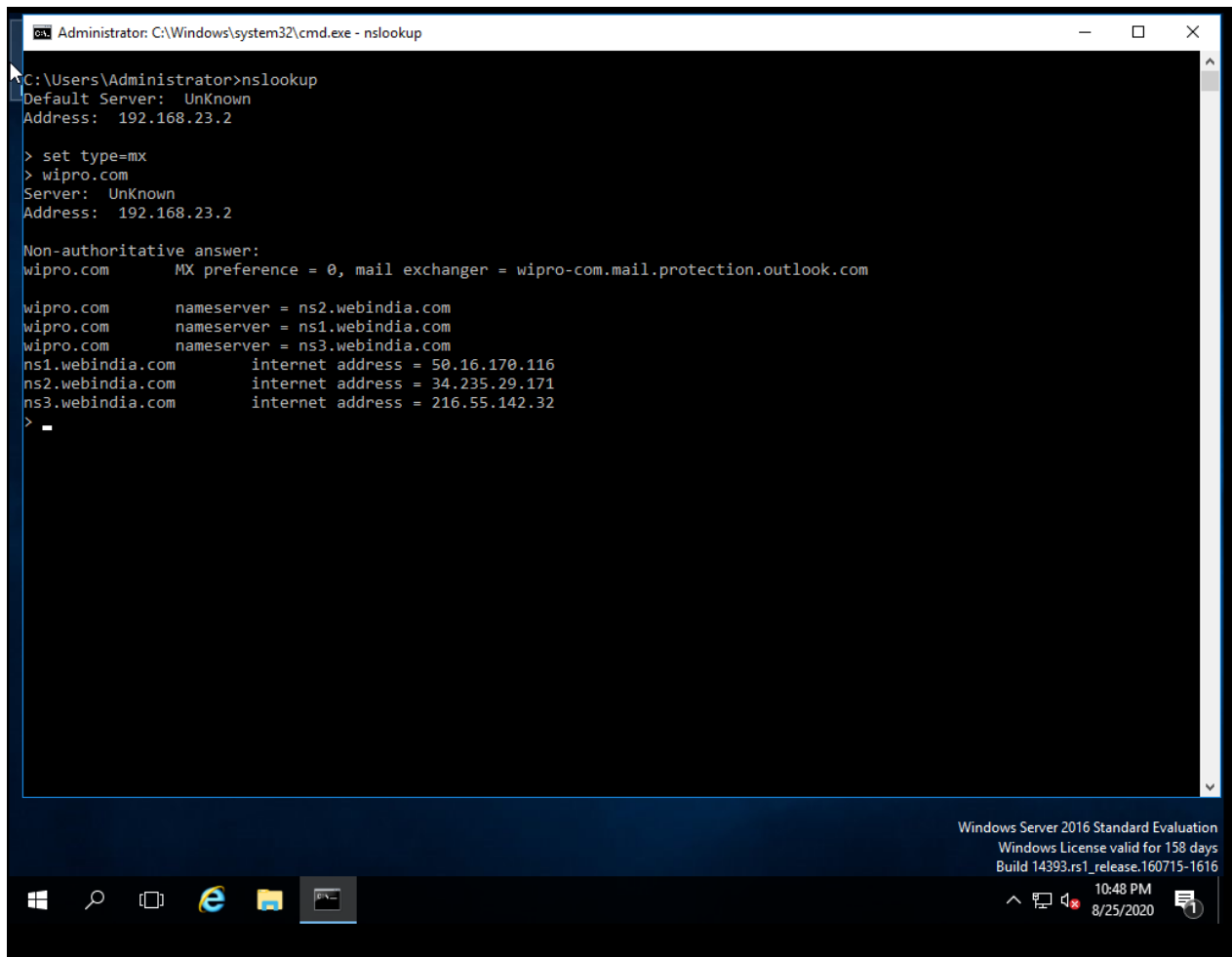
Windows Server 2016 Standard Evaluation
Windows License valid for 158 days
Build 14393.rs1_release.160715-1616
10:46 PM
8/25/2020

Step 1: Open command prompt (press 'home(windows)+r' then type 'cmd' and press enter).

Step 2: Type "nslookup"

Step 3: > "set type=mx"

Step 4: > wipro.com



```
Administrator: C:\Windows\system32\cmd.exe - nslookup
C:\Users\Administrator>nslookup
Default Server:  UnKnown
Address:  192.168.23.2

> set type=mx
> wipro.com
Server:  UnKnown
Address:  192.168.23.2

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

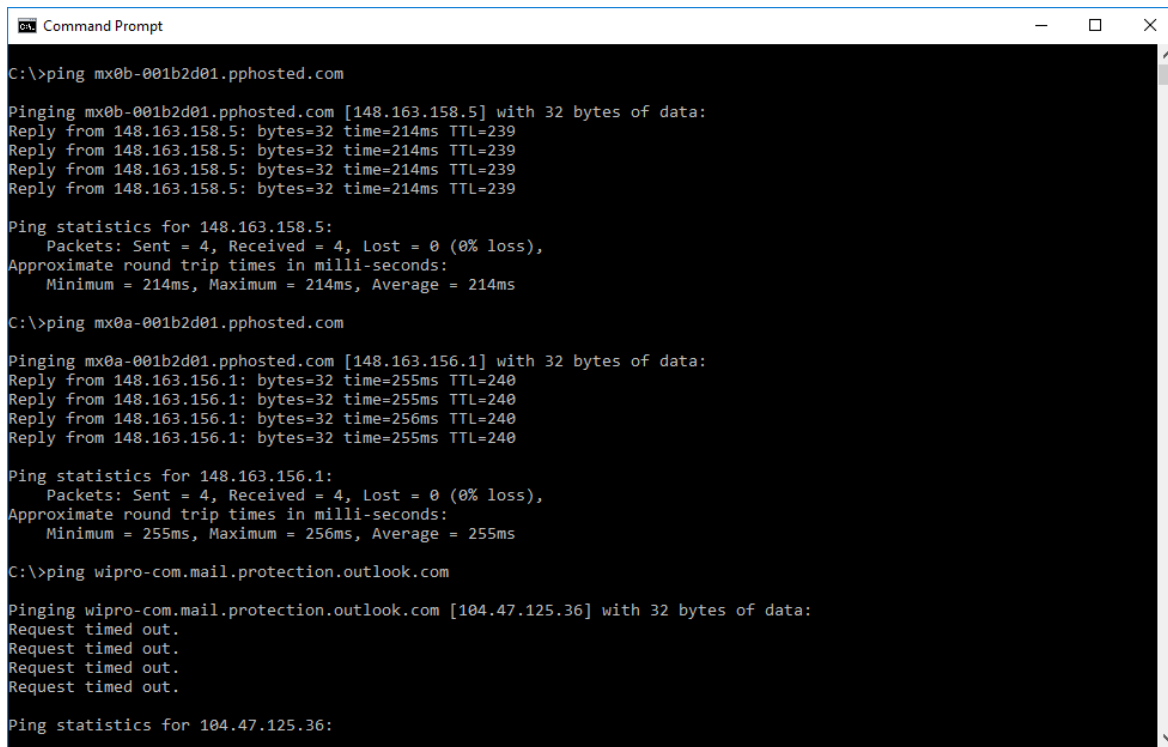
wipro.com      nameserver = ns2.webindia.com
wipro.com      nameserver = ns1.webindia.com
wipro.com      nameserver = ns3.webindia.com
ns1.webindia.com      internet address = 50.16.170.116
ns2.webindia.com      internet address = 34.235.29.171
ns3.webindia.com      internet address = 216.55.142.32
>
```

Windows Server 2016 Standard Evaluation
Windows License valid for 158 days
Build 14393.rs1_release.160715-1616
10:48 PM
8/25/2020

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

Solution:

Step 1: Ping the mail servers of **ibm.com** and **wipro.com** which I got from above and noted down the IP Address of each:



```
C:\>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=214ms TTL=239
Reply from 148.163.158.5: bytes=32 time=214ms TTL=239
Reply from 148.163.158.5: bytes=32 time=214ms TTL=239
Reply from 148.163.158.5: bytes=32 time=214ms TTL=239

Ping statistics for 148.163.158.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 214ms, Maximum = 214ms, Average = 214ms

C:\>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=255ms TTL=240
Reply from 148.163.156.1: bytes=32 time=255ms TTL=240
Reply from 148.163.156.1: bytes=32 time=256ms TTL=240
Reply from 148.163.156.1: bytes=32 time=255ms TTL=240

Ping statistics for 148.163.156.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 255ms, Maximum = 256ms, Average = 255ms

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

Pinging wipro-com.mail.protection.outlook.com [104.47.125.36] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 104.47.125.36:
```

Mail Servers	IP Address
mx0b-001b2d01.pphosted.com	148.163.158.5
mx0a-001b2d01.pphosted.com :-	148.163.156.1
wipro-com.mail.protection.outlook.com	104.47.125.36

Step 2 : Use the acquired IP Address to find the locations of the mails servers using <https://www.iplocation.net/>

← → ↻ iplocation.net/ip-lookup
Apps Netflix Prime Video (452) YouTube

Geolocation data from [IP2Location](#) (Product: DB6, updated on 2020-8-1)

IP Address	Country	Region	City
148.163.158.5	United States of America	California	Sunnyvale

ISP	Organization	Latitude	Longitude
Proofpoint Inc.	Not Available	37.4012	-122.0075

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

IP Address	Country	Region	City
148.163.158.5	United States	California	San Jose

ISP	Organization	Latitude	Longitude
Proofpoint, Inc.	Proofpoint, Inc. (proofpoint.com)	37.3394	-121.8950

Geolocation data from [DB-IP](#) (Product: Full, 2020-8-1)

IP Address	Country	Region	City
148.163.158.5	United States	Georgia	Atlanta

ISP	Organization	Latitude	Longitude
Proofpoint, Inc.	Proofpoint, Inc.	33.749	-84.388

Geolocation data from [ipdata.co](#) (Product: API, real-time)

IP Address	Country	Region	City
148.163.158.5	United States	Not Available	Not Available

ISP	Organization	Latitude	Longitude
Proofpoint, Inc.	Not Available	37.751	-97.822

← → ↻ iplocation.net/ip-lookup
Apps Netflix Prime Video (452) YouTube

Is the data shown below not accurate enough? Please read [geolocation accuracy](#) info to learn why.

Geolocation data from [IP2Location](#) (Product: DB6, updated on 2020-8-1)

IP Address	Country	Region	City
148.163.156.1	United States of America	California	Sunnyvale

ISP	Organization	Latitude	Longitude
Proofpoint Inc.	Not Available	37.4012	-122.0075

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

IP Address	Country	Region	City
148.163.156.1	United States	California	Sunnyvale

ISP	Organization	Latitude	Longitude
Proofpoint, Inc.	Proofpoint, Inc. (proofpoint.com)	37.3688	-122.0363

Geolocation data from [DB-IP](#) (Product: Full, 2020-8-1)

IP Address	Country	Region	City
148.163.156.1	United States	California	San Jose

ISP	Organization	Latitude	Longitude
Proofpoint, Inc.	Proofpoint, Inc.	37.3382	-121.886

Geolocation data from [ipdata.co](#) (Product: API, real-time)

IP Address	Country	Region	City
148.163.156.1	United States	Not Available	Not Available

ISP	Organization	Latitude	Longitude
Proofpoint, Inc.	Not Available	37.751	-97.822

Is the data shown below not accurate enough? Please read [geolocation accuracy](#) info to learn why.

Geolocation data from [IP2Location](#) (Product: DB6, updated on 2020-8-1)

IP Address	Country	Region	City
104.47.125.36	Singapore	Singapore	Singapore

ISP	Organization	Latitude	Longitude
Microsoft Corporation	Not Available	1.2897	103.8501

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

IP Address	Country	Region	City
104.47.125.36	Singapore	Singapore	Singapore

ISP	Organization	Latitude	Longitude
Microsoft Corporation	Microsoft Corporation (microsoft.com)	1.2897	103.8501

Geolocation data from [DB-IP](#) (Product: Full, 2020-8-1)

IP Address	Country	Region	City
104.47.125.36	Singapore	Not Available	Singapore (Downtown Core)

ISP	Organization	Latitude	Longitude
Microsoft Corporation	Microsoft Corporation	1.28239	103.852

Geolocation data from [ipdata.co](#) (Product: API, real-time)

IP Address	Country	Region	City
104.47.125.36	Singapore	Not Available	Singapore

ISP	Organization	Latitude	Longitude
Microsoft Corporation	Not Available	1.2829	103.8547

Question 3: Scan and find out port numbers open in 203.163.246.23:

Solution:

Step 1: Turn up the kali machine:-

Step 2: Open Terminal

Step 3: Use `nmap -sS -Pn -A 203.163.246.23`

Step 4: **Found all ports as filtered**

```

bpg@kali-pc-001: ~
File Actions Edit View Help
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 2020-08-25 23:59 PDT
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.50% done; ETC: 00:03 (0:03:41 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 201.29 seconds
root@kali-pc-001:~#
  
```

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

Solution :

Steps to create a CVE :

1. Download NESSUS from <https://www.tenable.com/products/nessus>
2. Log in to your Nessus machine : <https://localhost:8834/>
3. Click on Scans > Select New Scan > Choose Advanced Scan template.
4. Make sure the advanced setting Auto Enable Plugin Dependencies and Silent Plugin Dependencies are enabled.
5. Go to Basic Tab, then Click On General
6. Give your report a Name and Target IP (of your system)
7. Go to Credentials Tab Click on Windows and Enter your Username & Password.

The CVE Advanced Scan Report :

