

## Cyber Security

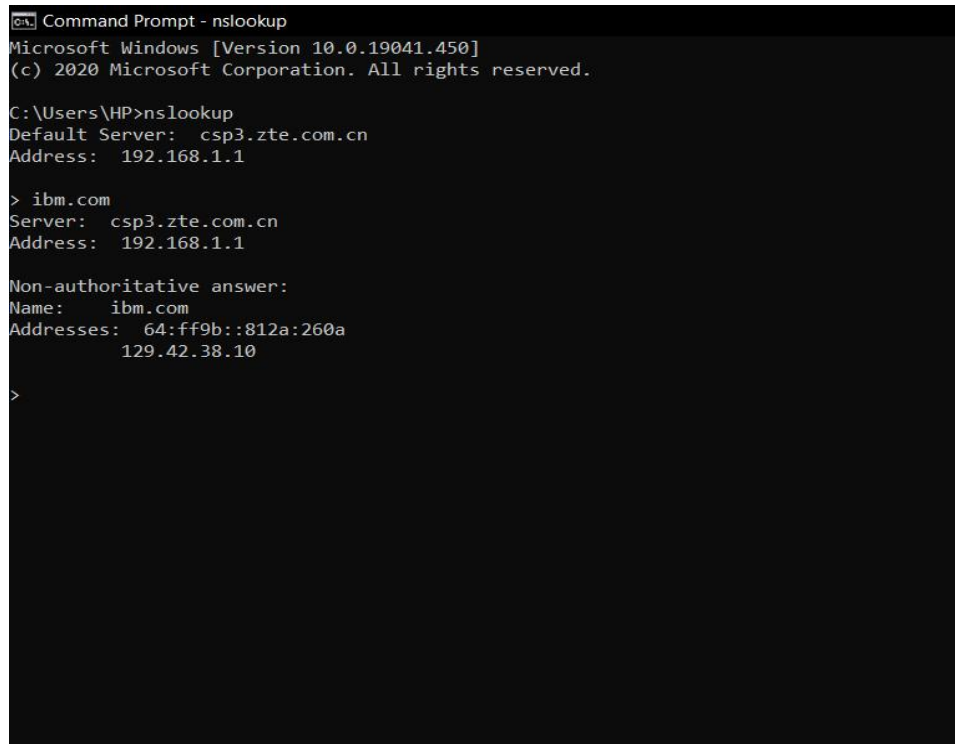
### Assignment

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

IBM.com

Wipro.com

Sol.



```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.19041.450]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\HP>nslookup
Default Server: csp3.zte.com.cn
Address: 192.168.1.1

> ibm.com
Server: csp3.zte.com.cn
Address: 192.168.1.1

Non-authoritative answer:
Name: ibm.com
Addresses: 64:ff9b::812a:260a
           129.42.38.10

>
```

Type **nslookup** in your command line.

Then, type **ibm.com** to find its mail server.

```
Command Prompt - nslookup
Microsoft Windows [Version 10.0.19041.450]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\HP>nslookup
Default Server:  csp1.zte.com.cn
Address:  192.168.1.1

> wipro.com
Server:  csp1.zte.com.cn
Address:  192.168.1.1

Non-authoritative answer:
Name:    wipro.com
Addresses:  64:ff9b::d10b:9f3d
           209.11.159.61

>
```

Type **nslookup** in your command line.

Then, type **wipro.com** to find its mail server.

2. Find the locations where these email servers are hosted?

Sol.

```

Command Prompt - nslookup
Microsoft Windows [Version 10.0.19041.450]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\HP>nslookup
Default Server: csp3.zte.com.cn
Address: 192.168.1.1

> set type=mx
> ibm.com
Server: csp3.zte.com.cn
Address: 192.168.1.1

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

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

```

Type **nslookup** in your command line.

Then, insert **set type=mx** and press Enter.

Then, type **ibm.com** to find its mail server hosted location.

```

Command Prompt - nslookup
Microsoft Windows [Version 10.0.19041.450]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\HP>nslookup
Default Server: csp1.zte.com.cn
Address: 192.168.1.1

> set type=mx
> wipro.com
Server: csp1.zte.com.cn
Address: 192.168.1.1

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

wipro.com nameserver = ns4.webindia.com
wipro.com nameserver = ns1.webindia.com
wipro.com nameserver = ns2.webindia.com
ns1.webindia.com internet address = 50.16.170.116
ns2.webindia.com internet address = 34.235.29.171
ns4.webindia.com internet address = 54.66.0.69
>

```

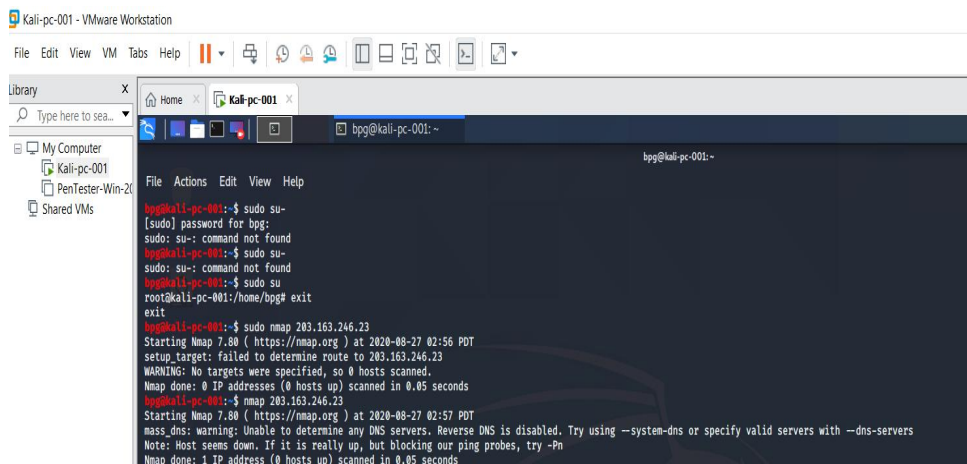
Type **nslookup** in your command line.

Then, insert **set type=mx** and press Enter.

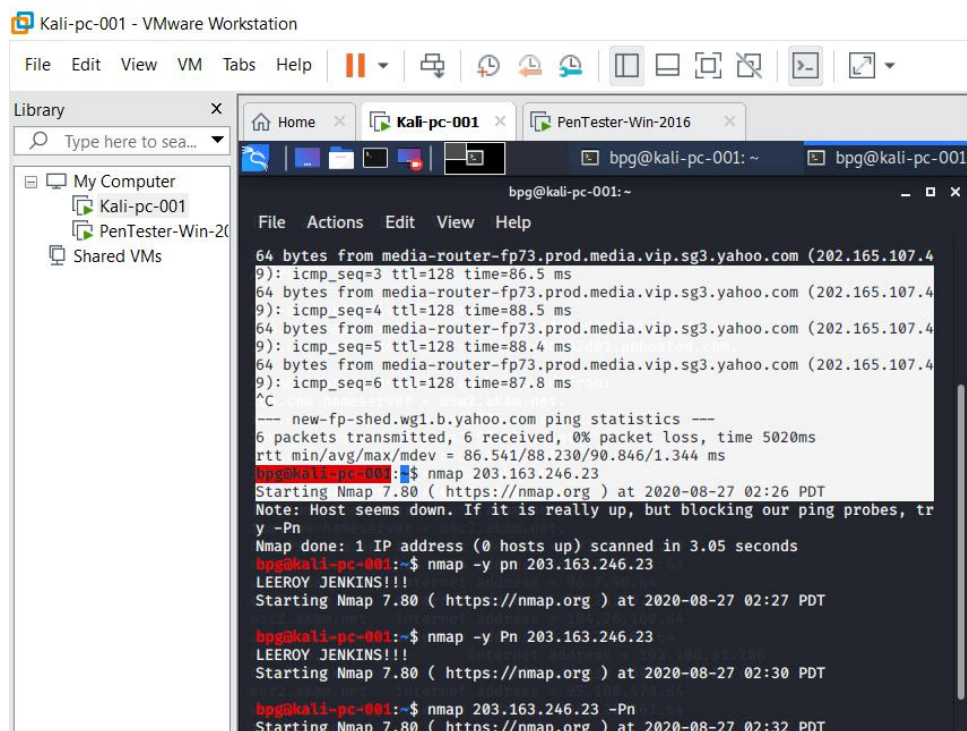
Then, type **wipro.com** to find its mail server hosted location.

3. Scan and find out port numbers open 203.163.246.23.

Sol.



```
Kali-pc-001 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Kali-pc-001
PenTester-Win-20
Shared VMs
bpg@kali-pc-001: ~
File Actions Edit View Help
bpg@kali-pc-001:~$ sudo su-
[sudo] password for bpg:
sudo: su-: command not found
bpg@kali-pc-001:~$ sudo su-
sudo: su-: command not found
bpg@kali-pc-001:~$ sudo su
root@kali-pc-001:~# exit
exit
bpg@kali-pc-001:~$ nslookup wipro.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 02:56 PDT
setup_target: failed to determine route to 203.163.246.23
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds
bpg@kali-pc-001:~$ nslookup wipro.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 02:57 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.05 seconds
```



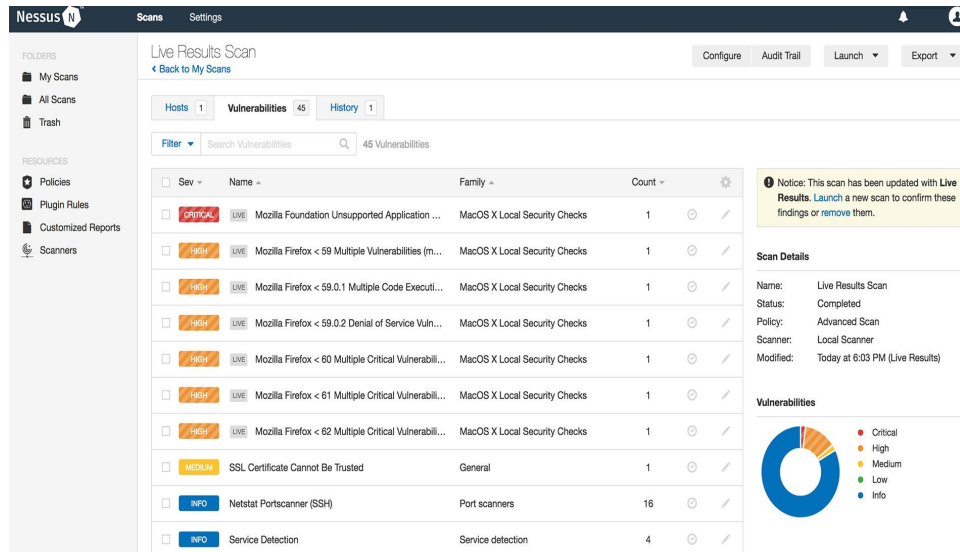
```
Kali-pc-001 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Kali-pc-001
PenTester-Win-20
Shared VMs
bpg@kali-pc-001: ~
File Actions Edit View Help
64 bytes from media-router-fp73.prod.media.vip.sg3.yahoo.com (202.165.107.49): icmp_seq=3 ttl=128 time=86.5 ms
64 bytes from media-router-fp73.prod.media.vip.sg3.yahoo.com (202.165.107.49): icmp_seq=4 ttl=128 time=88.5 ms
64 bytes from media-router-fp73.prod.media.vip.sg3.yahoo.com (202.165.107.49): icmp_seq=5 ttl=128 time=88.4 ms
64 bytes from media-router-fp73.prod.media.vip.sg3.yahoo.com (202.165.107.49): icmp_seq=6 ttl=128 time=87.8 ms
^C
-- new-fp-shed.wg1.b.yahoo.com ping statistics --
6 packets transmitted, 6 received, 0% packet loss, time 5020ms
rtt min/avg/max/mdev = 86.541/88.230/90.846/1.344 ms
bpg@kali-pc-001:~$ nmap 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 02:26 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.05 seconds
bpg@kali-pc-001:~$ nmap -y pn 203.163.246.23
LEEROY JENKINS!!!
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 02:27 PDT
bpg@kali-pc-001:~$ nmap -y Pn 203.163.246.23
LEEROY JENKINS!!!
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 02:30 PDT
bpg@kali-pc-001:~$ nmap 203.163.246.23 -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 02:32 PDT
```

Type **nmap** command in your kali Linux terminal

→ Nmap 208.163.246.23

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

Sol.



**Nessus** Scans Settings

Live Results Scan  
← Back to My Scans

Configure Audit Trail Launch Export

Hosts: 1 Vulnerabilities: 45 History: 1

Filter Search Vulnerabilities 45 Vulnerabilities

Sev	Name	Family	Count
Critical	Mozilla Foundation Unsupported Application ...	MacOS X Local Security Checks	1
High	Mozilla Firefox < 59 Multiple Vulnerabilities (m...	MacOS X Local Security Checks	1
High	Mozilla Firefox < 59.0.1 Multiple Code Executi...	MacOS X Local Security Checks	1
High	Mozilla Firefox < 59.0.2 Denial of Service Vuln...	MacOS X Local Security Checks	1
High	Mozilla Firefox < 60 Multiple Critical Vulnerabili...	MacOS X Local Security Checks	1
High	Mozilla Firefox < 61 Multiple Critical Vulnerabili...	MacOS X Local Security Checks	1
High	Mozilla Firefox < 62 Multiple Critical Vulnerabili...	MacOS X Local Security Checks	1
Medium	SSL Certificate Cannot Be Trusted	General	1
Info	Netstat Portscanner (SSH)	Port scanners	16
Info	Service Detection	Service detection	4

**Scan Details**

Name: Live Results Scan  
Status: Completed  
Policy: Advanced Scan  
Scanner: Local Scanner  
Modified: Today at 6:03 PM (Live Results)

**Vulnerabilities**

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

CVE scan of my laptop