

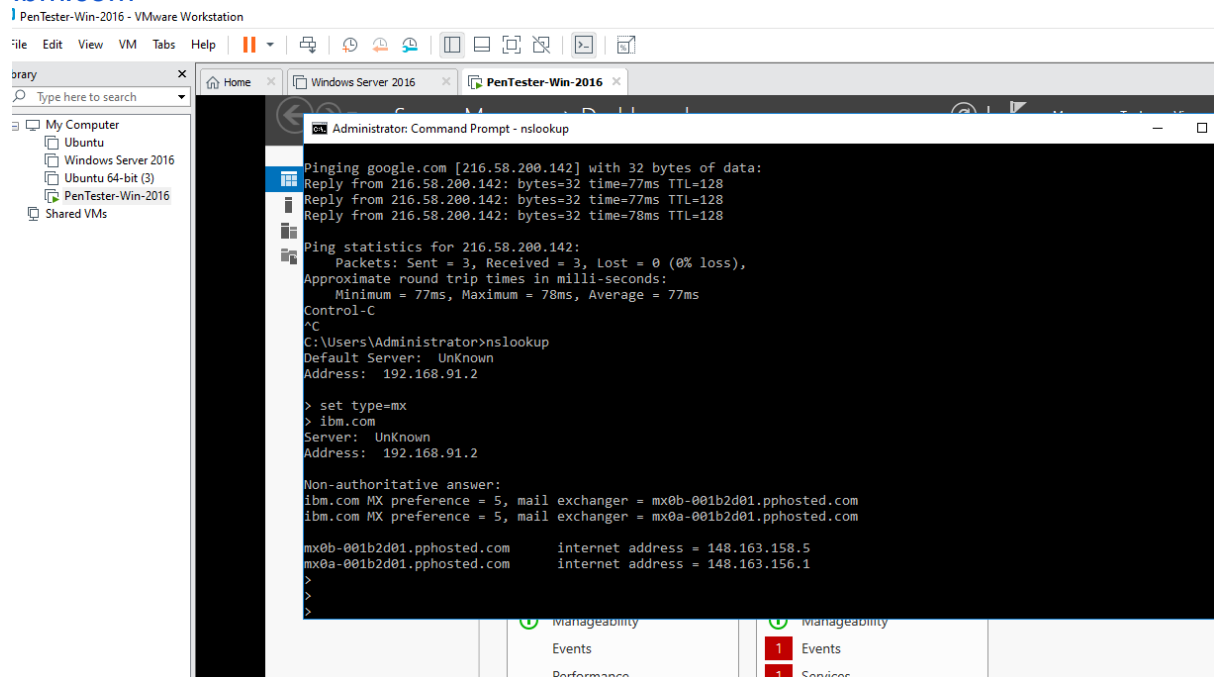
Cyber Security Essentials

Day 4

Question 1:

Find out the mail servers of the following domain :

ibm.com



```
Administrator: Command Prompt - nslookup

Pinging google.com [216.58.200.142] with 32 bytes of data:
Reply from 216.58.200.142: bytes=32 time=77ms TTL=128
Reply from 216.58.200.142: bytes=32 time=77ms TTL=128
Reply from 216.58.200.142: bytes=32 time=78ms TTL=128

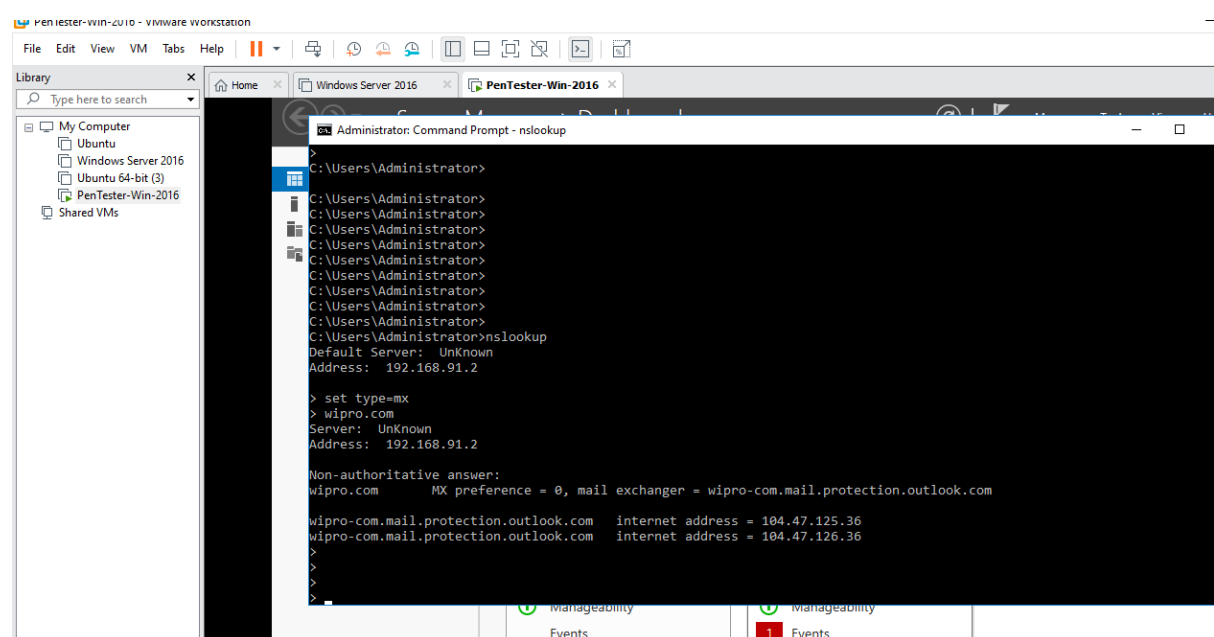
Ping statistics for 216.58.200.142:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 77ms, Maximum = 78ms, Average = 77ms
Control-C
^C
C:\Users\Administrator>nslookup
Default Server: UnKnown
Address: 192.168.91.2

> set type=mx
> ibm.com
Server: UnKnown
Address: 192.168.91.2

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

mx0b-001b2d01.pphosted.com    internet address = 148.163.158.5
mx0a-001b2d01.pphosted.com    internet address = 148.163.156.1
>
>
>
```

[Wipro.com](http://wipro.com)



```
Administrator: Command Prompt - nslookup

C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>nslookup
Default Server: UnKnown
Address: 192.168.91.2

> set type=mx
> wipro.com
Server: UnKnown
Address: 192.168.91.2

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

wipro-com.mail.protection.outlook.com    internet address = 104.47.125.36
wipro-com.mail.protection.outlook.com    internet address = 104.47.126.36
>
>
>
```

Question 2:

Find the locations, where these email servers are hosted.

```
ibm.com nameserver = usc3.akam.net
ibm.com nameserver = ns1-99.akam.net
ibm.com nameserver = asia3.akam.net
ibm.com nameserver = usw2.akam.net
ibm.com nameserver = usc2.akam.net

eur5.akam.net internet address = 23.74.25.64
eur2.akam.net internet address = 95.100.173.64
ns1-206.akam.net internet address = 193.108.91.206
ns1-206.akam.net AAAA IPv6 address = 2600:1401:2::ce
usc3.akam.net internet address = 96.7.50.64
ns1-99.akam.net internet address = 193.108.91.99
ns1-99.akam.net AAAA IPv6 address = 2600:1401:2::63
usw2.akam.net internet address = 184.26.161.64
usc2.akam.net internet address = 184.26.160.64
> nmap www.ibm.com
Server: e2874.dscx.akamaiedge.net
Addresses: 2600:1417:3f:693::b3a
           2600:1417:3f:685::b3a
           184.29.23.144
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.ibm.com can't find nmap: No response from server
> nmap www.wipro.com
Server: d361nqn33s63ex.cloudfront.net
Addresses: 2600:9000:21fe:3600:13:4f33:b240:93a1
           2600:9000:21fe:ae00:13:4f33:b240:93a1
           2600:9000:21fe:a000:13:4f33:b240:93a1
           2600:9000:21fe:b000:13:4f33:b240:93a1
           2600:9000:21fe:1e00:13:4f33:b240:93a1
           2600:9000:21fe:e400:13:4f33:b240:93a1
           2600:9000:21fe:5c00:13:4f33:b240:93a1
           2600:9000:21fe:e200:13:4f33:b240:93a1
           54.182.0.117
           54.182.0.123
           54.182.0.37
           54.182.0.105
Aliases:  www.wipro.com

*** www.wipro.com can't find nmap: No response from server
>
```

The screenshot shows a web browser window with the URL geopllookup.net/ip/148.163.158.5. The page content includes a brief introduction, followed by two main sections: "IP General Information" and "IP Geolocation Information".

IP General Information

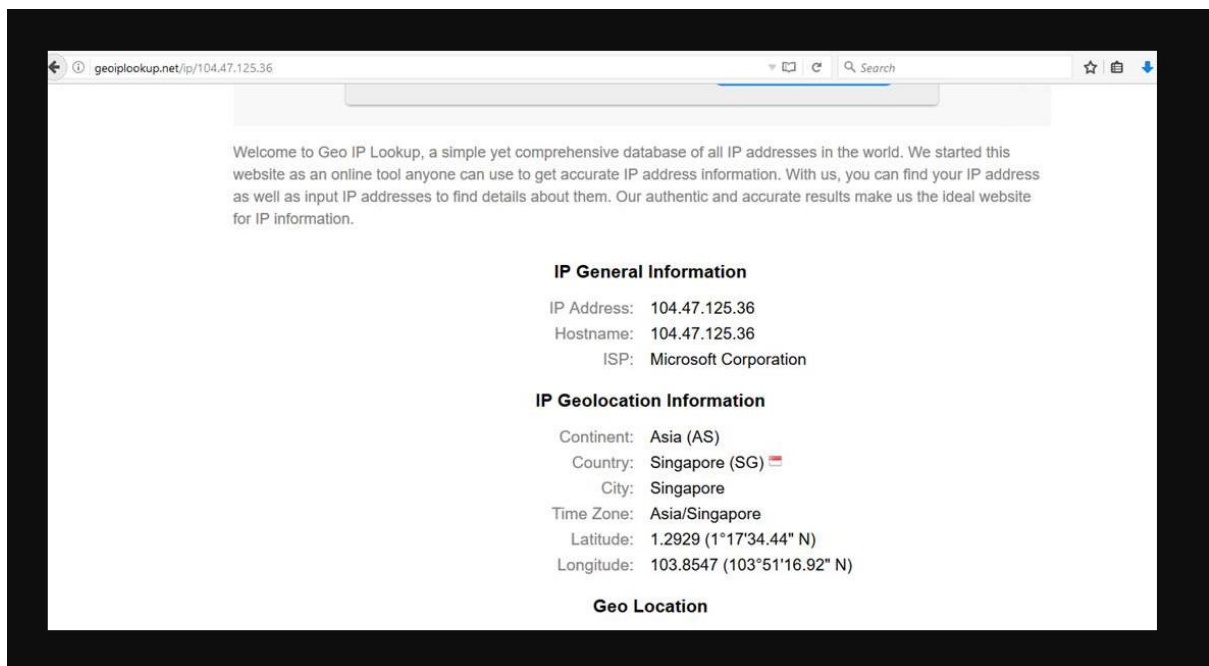
- IP Address: 148.163.158.5
- Hostname: 148.163.158.5
- ISP: Proofpoint, Inc.

IP Geolocation Information

- Continent: North America (NA)
- Country: United States (US) 🇺🇸
- City:
- Time Zone: America/Chicago
- Latitude: 37.751 (37°45'3.6" N)
- Longitude: -97.822 (97°49'19.2" S)

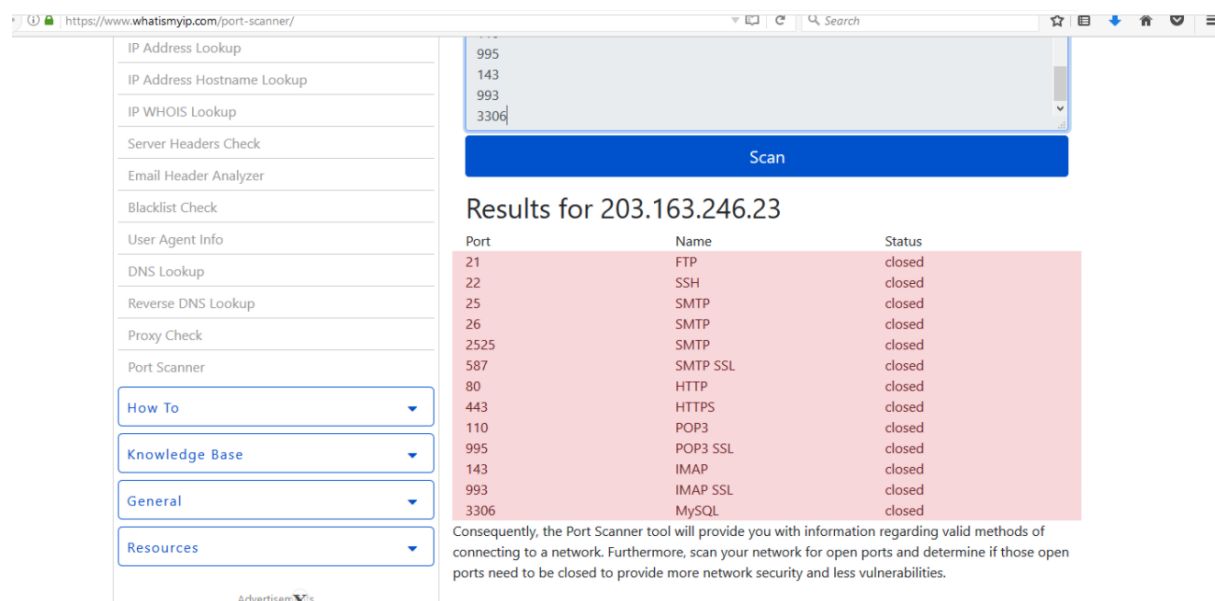
Geo Location

At the bottom of the page, there is a banner for "Free Live Chat for 3 Agents".



Question 3:

Scan and find out port numbers open 203.163.246.23



Question 4:

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

The screenshot shows the Nessus Professional web interface. The browser address bar displays a certificate error and the URL `https://localhost:8834/#/scans/reports/5/hosts`. The interface includes a sidebar with folders (My Scans, All Scans, Trash) and resources (Policies, Plugin Rules, Customized Reports, Scanners). The main content area is titled 'TestPC' and shows a summary of the scan results: 1 Host, 28 Vulnerabilities, and 1 History item. A table lists the host 172.16.40.29 with a vulnerability count of 6. A donut chart shows the distribution of vulnerability severity levels: Critical (0), High (0), Medium (0), Low (0), and Info (6). The Scan Details section indicates the policy is 'Advanced Scan', status is 'Completed', scanner is 'Local Scanner', start time is 'Today at 6:27 PM', end time is 'Today at 6:33 PM', and elapsed time is '6 minutes'.

Host	Vulnerabilities
172.16.40.29	6

Scan Details

- Policy: Advanced Scan
- Status: Completed
- Scanner: Local Scanner
- Start: Today at 6:27 PM
- End: Today at 6:33 PM
- Elapsed: 6 minutes

Vulnerabilities

- Critical: 0
- High: 0
- Medium: 0
- Low: 0
- Info: 6

The screenshot shows the Nessus Professional web interface, displaying the 'TestPC' scan results for vulnerabilities. The browser address bar displays a certificate error and the URL `https://localhost:8834/#/scans/reports/5/vulnerabilities`. The interface includes a sidebar with folders (My Scans, All Scans, Trash) and resources (Policies, Plugin Rules, Customized Reports, Scanners). The main content area is titled 'TestPC' and shows a summary of the scan results: 1 Host, 28 Vulnerabilities, and 1 History item. A table lists the vulnerabilities, including their severity, name, family, and count. A donut chart shows the distribution of vulnerability severity levels: Critical (0), High (0), Medium (0), Low (0), and Info (6). The Scan Details section indicates the policy is 'Advanced Scan', status is 'Completed', scanner is 'Local Scanner', start time is 'Today at 6:27 PM', end time is 'Today at 6:33 PM', and elapsed time is '6 minutes'.

Sev	Name	Family	Count
MIXED	SSL (Multiple Issues)	General	8
MIXED	Microsoft Windows (Multiple Issues)	Misc.	3
MIXED	TLS (Multiple Issues)	Service detection	3
INFO	DCE Services Enumeration	Windows	15
INFO	Nessus SYN scanner	Port scanners	14
INFO	HTTP (Multiple Issues)	Web Servers	6
INFO	SMB (Multiple Issues)	Windows	5
INFO	Service Detection	Service detection	4
INFO	VNC (Multiple Issues)	Service detection	3
INFO	Additional DNS Hostnames	General	1

Scan Details

- Policy: Advanced Scan
- Status: Completed
- Scanner: Local Scanner
- Start: Today at 6:27 PM
- End: Today at 6:33 PM
- Elapsed: 6 minutes

Vulnerabilities

- Critical: 0
- High: 0
- Medium: 0
- Low: 0
- Info: 6

