ASSIGNMENT

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

- **Ibm.com**
- **Wipro.com**

WWW.IBM.COM

```
> www.Ibm.com
Server:  www.routerlogin.com
Address:  192.168.1.1

Non-authoritative answer:
Name:    e2874.dscx.akamaiedge.net
Addresses:  2600:140f:c000:185::b3a
          2600:140f:c000:181::b3a
          106.51.145.132
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

```
> www.Wipro.com
Server:  www.routerlogin.com
Address:  192.168.1.1

Non-authoritative answer:
Name:    d361nqn33s63ex.cloudfront.net
Addresses:  2600:9000:215c:ec00:13:4f33:b240:93a1
          2600:9000:215c:b400:13:4f33:b240:93a1
          2600:9000:215c:c00:13:4f33:b240:93a1
          2600:9000:215c:6600:13:4f33:b240:93a1
          2600:9000:215c:ac00:13:4f33:b240:93a1
          2600:9000:215c:a600:13:4f33:b240:93a1
          2600:9000:215c:9600:13:4f33:b240:93a1
          2600:9000:215c:b000:13:4f33:b240:93a1
          13.249.221.103
          13.249.221.64
          13.249.221.39
          13.249.221.15
```

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

- **using mx command**

```
> set type=mx
> Ibm.com
Server:  www.routerlogin.com
Address:  192.168.1.1

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
```

3: Scan and find out port numbers open 203.163.246.23

```
root@kali:~# nmap -Pn -sS -v  -p-  203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 13:50 EDT
Initiating Parallel DNS resolution of 1 host. at 13:50
Completed Parallel DNS resolution of 1 host. at 13:50, 0.36s elapsed
Initiating SYN Stealth Scan at 13:50
Scanning 203.163.246.23 [65535 ports]
```

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