Question 1:

Find out the mail servers of the following domain :

Ibm.com

Type the command ==nslookup==

==set type=mx==

==ibm.com==

```
Default Server:  dsldevice.lan
Address:  192.168.1.1

> set type=mx
> ibm.com
Server:  dsldevice.lan
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
>
```

Wipro.com

Type the command ==nslookup==

==set type=mx==

==wipro.com==

```
C:\Users\pawar>nslookup
Default Server:  dsldevice.lan
Address:  192.168.1.1

> set type=mx
> wipro.com
Server:  dsldevice.lan
Address:  192.168.1.1

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

wipro.com       nameserver = ns1.webindia.com
wipro.com       nameserver = ns3.webindia.com
wipro.com       nameserver = ns2.webindia.com
>
```

Question 2:

Find the locations, where these email servers are hosted.

Type the command <mark>nslookup</mark>

<mark>set type=mx</mark>

Question 3:

Scan and find out port numbers open 203.163.246.23

nmap 203.163.246.23

```
Starting Nmap 7.70 ( https://nmap.org ) at 2020-08-24 09:03 EDT
Nmap scan report for 203.163.246.23
Host is up (0.00027s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
513/tcp open  login

Nmap done: 1 IP address (1 host up) scanned in 10.67 seconds
```

Question 4:

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

First, you have to create a scan. To create your scan:

1. In the menu, click Scans.
2. In My Scans page, click the New Scan button.
3. Choose scan template
4. Configure scan settings by selecting following:
    a. Name of scan
    b. Description of scan
    c. Folder for saving scan results
    d. Targets to be scanned
5. Configure other settings and credentials
6. **To view vulnerabilities:**
7. Click Scans.
8. Click the scan for which you want to view results.
9. Do one of the following:
    a. Click a specific host to view vulnerabilities found on that host.
    b. Click the Vulnerabilities tab to view all vulnerabilities.
10. Clicking on the vulnerability row will open the vulnerability details page, displaying plugin information and output for each instance on a host.