Assignment Day 4 | 23rd August 2020

Name: AnguRaj R

Email: anguraj@my.com

Question 1:

Find out the mail servers of the following domain :

   a) Wipro.com
   b) IBM.com

Answer:

```
root@ella:~# nslookup
> set type=mx
> wipro.com
Server:         169.254.169.254
Address:        169.254.169.254#53

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

Authoritative answers can be found from:
```

```
> ibm.com
Server:         169.254.169.254
Address:        169.254.169.254#53

Non-authoritative answer:
ibm.com mail exchanger = 5 mx0a-001b2d01.pphosted.com.
ibm.com mail exchanger = 5 mx0b-001b2d01.pphosted.com.

Authoritative answers can be found from:
```

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

Answer:

```
> www.wipro.com
Server:          169.254.169.254
Address:         169.254.169.254#53

Non-authoritative answer:
www.wipro.com    canonical name = d36lnqn33s63ex.cloudfront.net.

Authoritative answers can be found from:
d36lnqn33s63ex.cloudfront.net
        origin = ns-1658.awsdns-15.co.uk
        mail addr = awsdns-hostmaster.amazon.com
        serial = 1
        refresh = 7200
        retry = 900
        expire = 1209600
        minimum = 86400
```

```
> www.ibm.com
Server:          169.254.169.254
Address:         169.254.169.254#53

Non-authoritative answer:
www.ibm.com      canonical name = www.ibm.com.cs186.net.
www.ibm.com.cs186.net    canonical name = outer-ccdn-dual.ibmcom.edgekey.net.
outer-ccdn-dual.ibmcom.edgekey.net      canonical name = outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns
.net.
outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net      canonical name = e2874.dscx.akamaiedge.net.

Authoritative answers can be found from:
dscx.akamaiedge.net
        origin = n0dscx.akamaiedge.net
        mail addr = hostmaster.akamai.com
        serial = 1598584427
        refresh = 1000
        retry = 1000
        expire = 1000
        minimum = 1800
```

Question 3: Scan and find out port numbers open 203.163.246.23

Answer:

```
root@ella:~# nmap -Pn -p 1-65535 203.163.246.23 -T 4
Starting Nmap 7.70 ( https://nmap.org ) at 2020-08-28 06:42 UTC
Nmap scan report for 203.163.246.23
Host is up.
All 65535 scanned ports on 203.163.246.23 are filtered

Nmap done: 1 IP address (1 host up) scanned in 6564.10 seconds
```

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

Answer: