

## Assignment Day 4

Q1 Find out the mail servers of the following domain :

lbn.com

```
minimum = 86400
> www.ibm.com
Server:      192.168.203.2
Address:     192.168.203.2#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.ed
gekey.net.globalredir.akadns.net.
outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net canonical name = e
2874.dscx.akamaiedge.net.

Authoritative answers can be found from:
dscx.akamaiedge.net
  origin = n0dscx.akamaiedge.net
  mail addr = hostmaster.akamai.com
  serial = 1598612098
  refresh = 1000
  retry = 1000
  expire = 1000
  minimum = 1800
> █
```

Wipro.com

```
root@kali-pc-001:~# nslookup
> set type=mx
> www.wipro.com
Server:      192.168.203.2
Address:     192.168.203.2#53

Non-authoritative answer:
www.wipro.com canonical name = d361nqn33s63ex.cloudfront.net.

Authoritative answers can be found from:
d361nqn33s63ex.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
> █
```

Q2 Find the locations, where these email servers are hosted.

ibm.com

mail@ibm.com	
Mailbox Domain	mx0a-001b2d01.pphosted.com
IP	148.163.156.1
Country	United States
City	Sunnyvale
Latitude	37.424900054932
Longitude	-122.0074005127
ISP	N/A

wipro.com

mail@wipro.com	
Mailbox Domain	wipro-com.mail.protection.outlook.com
IP	104.47.124.36
Country	United States
City	Redmond
Latitude	47.680099487305
Longitude	-122.12059783936
ISP	N/A

Q3 Scan and find out port numbers open 203.163.246.23

```
root@kali-pc-001:~# nmap -pn 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 03:47 PDT
Found no matches for the service mask 'n' and your specified protocols
QUITTING!
root@kali-pc-001:~# nmap -Pn 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 03:48 PDT
Nmap scan report for 203.163.246.23
Host is up.
All 1000 scanned ports on 203.163.246.23 are filtered

Nmap done: 1 IP address (1 host up) scanned in 201.38 seconds
```

Q4 Install nessus in a VM and scan your laptop/desktop for CVE.

Soln: It is in installing phase as we can see in the snapshot below

