LetsUpgrade ||CyberSecurity || August 2020

Assignment Day 4 || 23rd August 2020

{Name- RishiKesh Kumar}

Answer Sheet

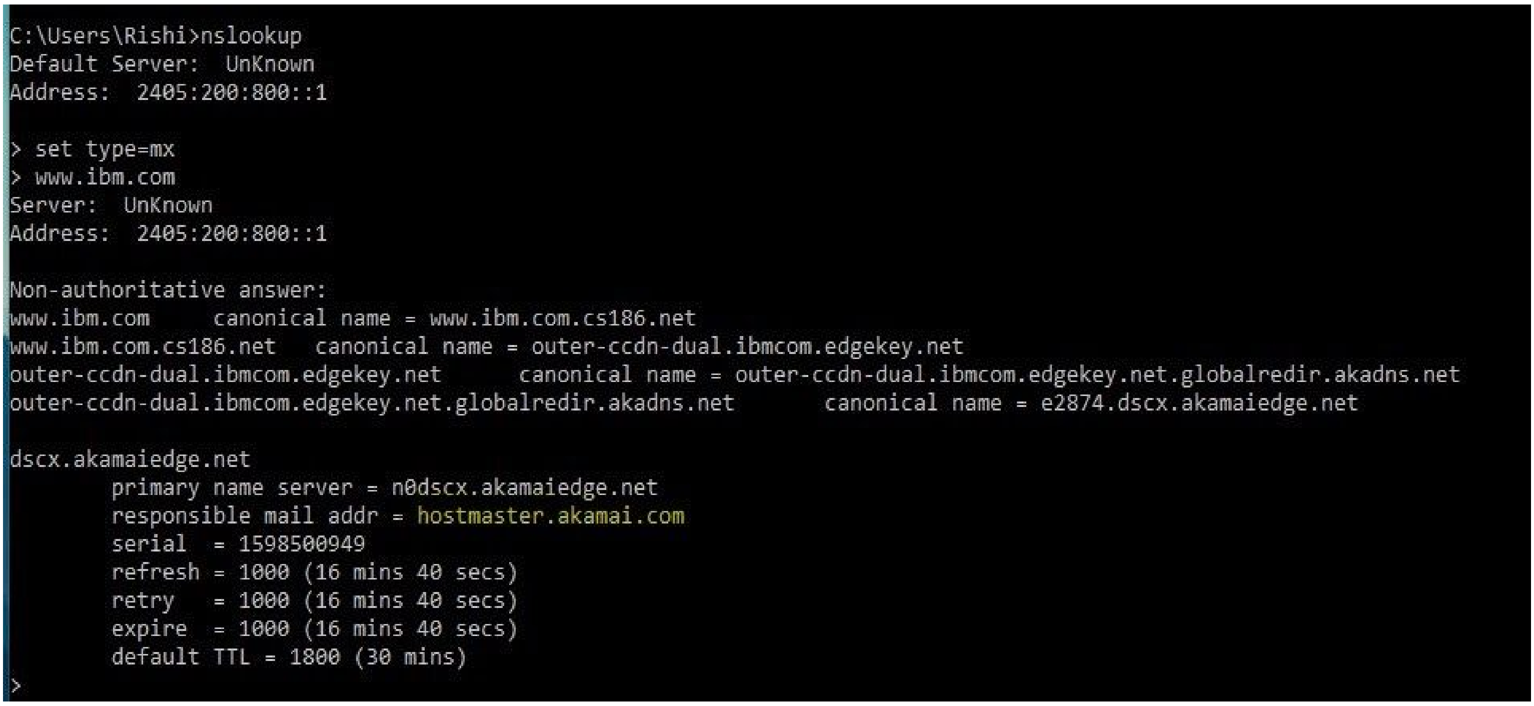
★ Question 1:

Find out the mail servers of the following domain :

➔ Ibm.com

➔ Wipro.com

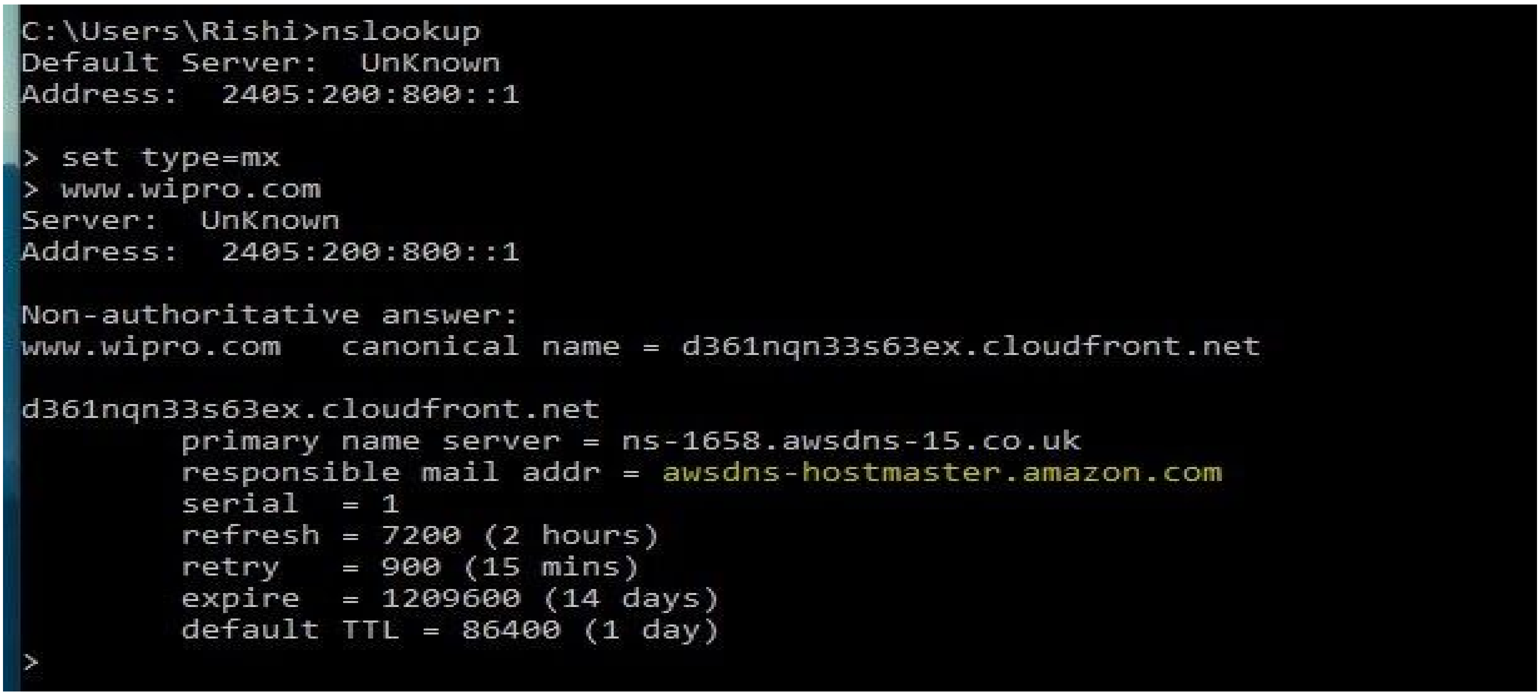
★www.ibm.com



```
C:\Users\Rishi>nslookup
Default Server:  UnKnown
Address:  2405:200:800::1

> set type=mx
> www.ibm.com
Server:  UnKnown
Address:  2405:200:800::1

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

dscx.akamaiedge.net
        primary name server = n0dscx.akamaiedge.net
        responsible mail addr = hostmaster.akamai.com
        serial  = 1598500949
        refresh = 1000 (16 mins 40 secs)
        retry   = 1000 (16 mins 40 secs)
        expire  = 1000 (16 mins 40 secs)
        default TTL = 1800 (30 mins)
>
```

★

★www.wipro.com



```
C:\Users\Rishi>nslookup
Default Server:  UnKnown
Address:  2405:200:800::1

> set type=mx
> www.wipro.com
Server:  UnKnown
Address:  2405:200:800::1

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

d361nqn33s63ex.cloudfront.net
        primary name server = ns-1658.awsdns-15.co.uk
        responsible mail addr = awsdns-hostmaster.amazon.com
        serial  = 1
        refresh = 7200 (2 hours)
        retry   = 900 (15 mins)
        expire  = 1209600 (14 days)
        default TTL = 86400 (1 day)
>
```

★

★

★Question 2:

Find the locations, where these email servers are hosted ?

➔Ibm.com = It is using Akamai Technologies to host there "mail servers"

- Mail Addr = hostmaster.akamai.com .....

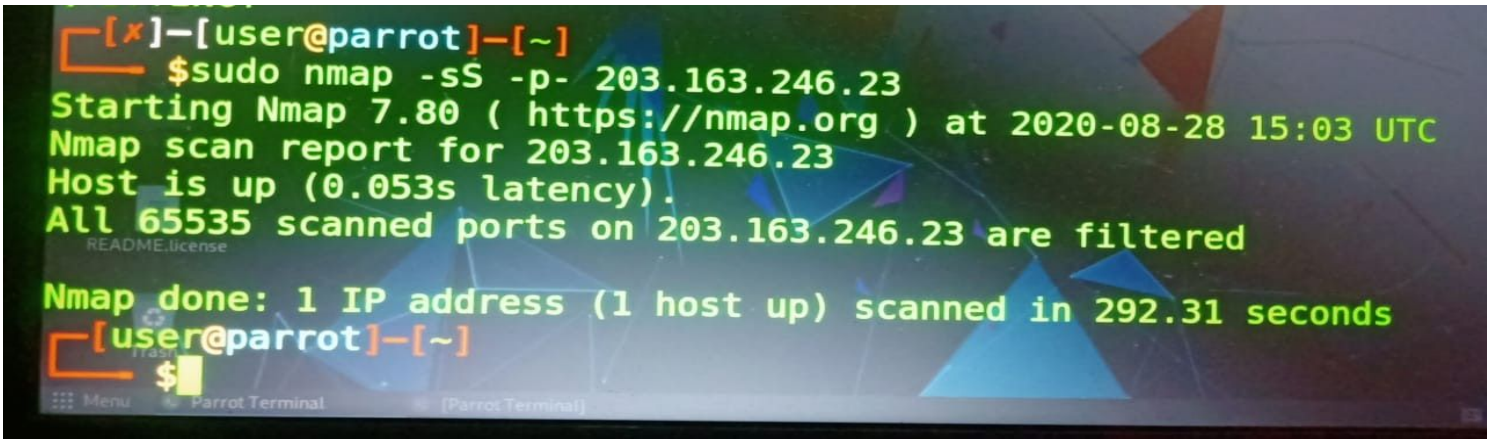
➔Wipro.com = It is using Amazon AWS to host there "mail servers"

- Mail Addr = awsdns-hostmaster.amazon.com .....

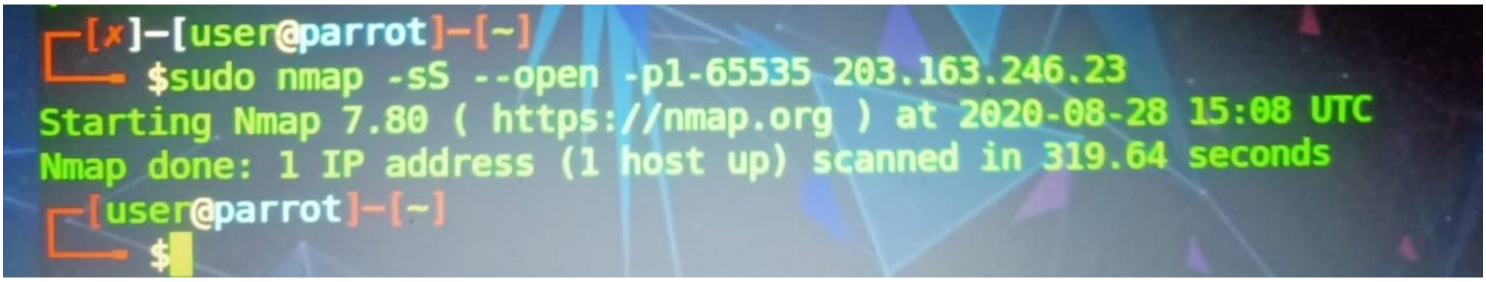
★Question 3:

Scan and find out port numbers open 203.163.246.23

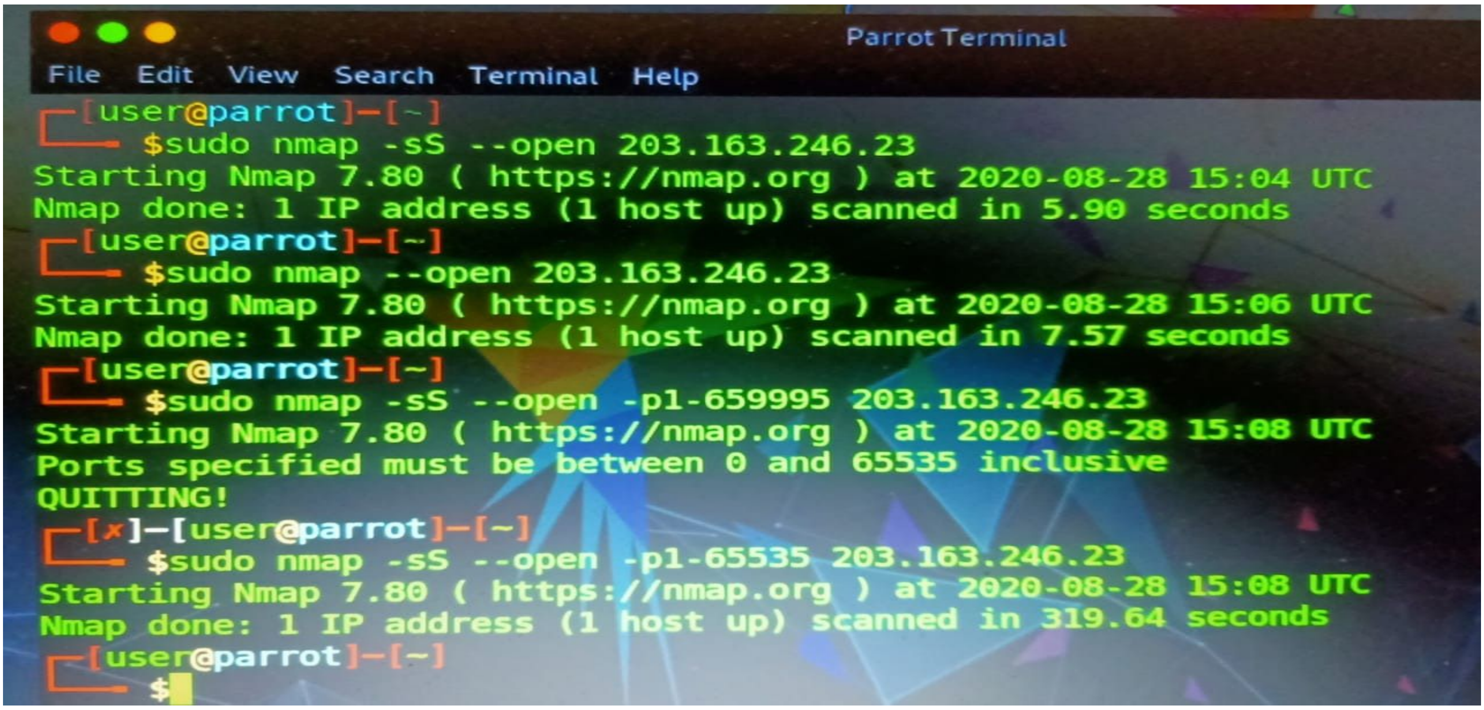
➔There is no open port showing..



```
┌─[✗]─[user@parrot]─[~]
└──╼ $sudo nmap -sS -p- 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 15:03 UTC
Nmap scan report for 203.163.246.23
Host is up (0.053s latency).
All 65535 scanned ports on 203.163.246.23 are filtered

Nmap done: 1 IP address (1 host up) scanned in 292.31 seconds
┌─[user@parrot]─[~]
└──╼ $
```



```
┌─[✗]─[user@parrot]─[~]
└──╼ $sudo nmap -sS --open -p1-65535 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 15:08 UTC
Nmap done: 1 IP address (1 host up) scanned in 319.64 seconds
┌─[user@parrot]─[~]
└──╼ $
```

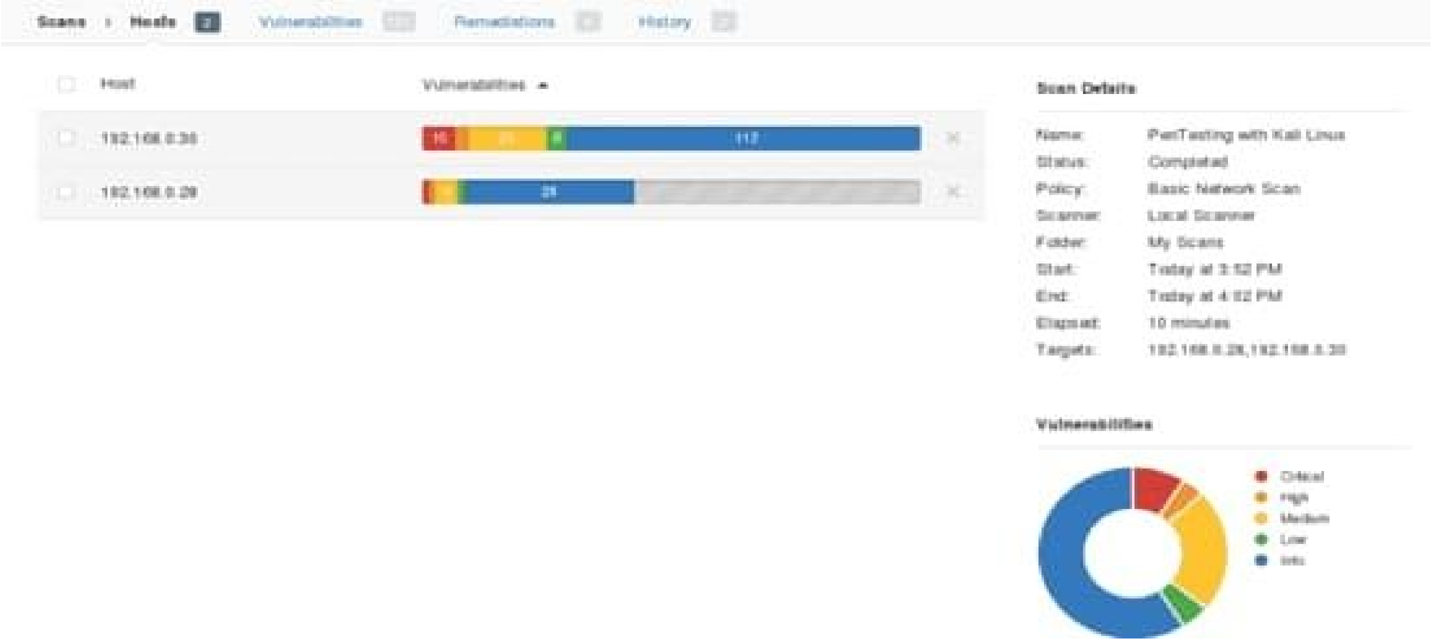


```
┌─[user@parrot]─[~]
└──╼ $sudo nmap -sS --open 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 15:04 UTC
Nmap done: 1 IP address (1 host up) scanned in 5.90 seconds
┌─[user@parrot]─[~]
└──╼ $sudo nmap --open 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 15:06 UTC
Nmap done: 1 IP address (1 host up) scanned in 7.57 seconds
┌─[user@parrot]─[~]
└──╼ $sudo nmap -sS --open -p1-659995 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 15:08 UTC
Ports specified must be between 0 and 65535 inclusive
QUITTING!
┌─[✗]─[user@parrot]─[~]
└──╼ $sudo nmap -sS --open -p1-65535 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 15:08 UTC
Nmap done: 1 IP address (1 host up) scanned in 319.64 seconds
┌─[user@parrot]─[~]
└──╼ $
```

★Question 4:

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

➔I have done this on My Window 7 and Kali Linux



□ Host	Vulnerabilities ▲
□ 192.168.0.30	16 21 6 112
□ 192.168.0.28	28

Scan Details

Name: PenTesting with Kali Linux
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Folder: My Scans
Start: Today at 3:52 PM
End: Today at 4:02 PM
Elapsed: 10 minutes
Targets: 192.168.0.28,192.168.0.30

Vulnerabilities

****

Thank You