

# Mail servers of the following domain:

**Ibm.com**

**Wipro.com**

- Use “**nslookup**” command and press enter
- After that type “**settype=mx**”
- Then type **www.ibm.com** and **www.wipro.com** to find their respective mail servers.

```
Select Administrator: C:\Windows\system32\cmd.exe - nslookup

C:\Users\Administrator>nslookup
Default Server:  Unknown
Address:  192.168.154.2

> www.facebook.com
Server:  Unknown
Address:  192.168.154.2

Non-authoritative answer:
Name:    star-mini.c10r.facebook.com
Addresses:  2a03:2880:f137:182:face:b00c:0:25de
           157.240.192.35
Aliases:  www.facebook.com

> set type=mx
> www.ibm.com
Server:  Unknown
Address:  192.168.154.2

ibm.com
primary name server = asia3.akam.net
responsible mail addr = dnsadm.us.ibm.com
serial = 1564134373
refresh = 43200 (12 hours)
retry = 7200 (2 hours)
expire = 604800 (7 days)
default TTL = 3600 (1 hour)
```

```
Select Administrator: C:\Windows\system32\cmd.exe - nslookup

C:\Users\Administrator>nslookup
Default Server:  Unknown
Address:  192.168.154.2

> www.facebook.com
Server:  Unknown
Address:  192.168.154.2

Non-authoritative answer:
Name:    star-mini.c10r.facebook.com
Addresses:  2a03:2880:f137:182:face:b00c:0:25de
           157.240.192.35
Aliases:  www.facebook.com

> set type=mx
> www.ibm.com
Server:  Unknown
Address:  192.168.154.2

ibm.com
primary name server = asia3.akam.net
responsible mail addr = dnsadm.us.ibm.com
serial = 1564134373
refresh = 43200 (12 hours)
retry = 7200 (2 hours)
expire = 604800 (7 days)
default TTL = 3600 (1 hour)

> www.wipro.com
Server:  Unknown
Address:  192.168.154.2

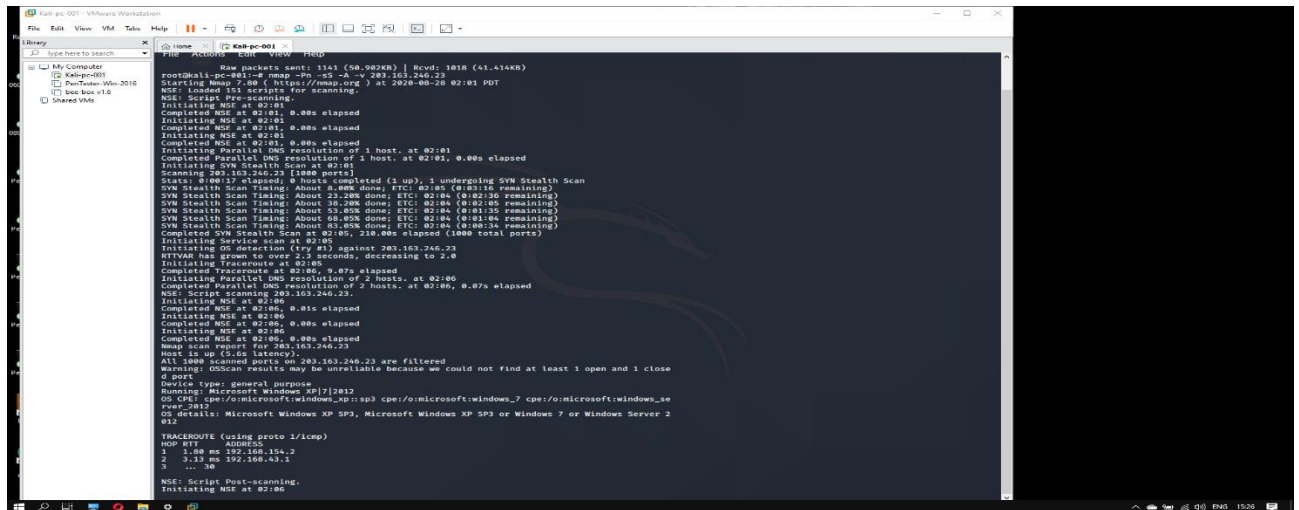
Non-authoritative answer:
www.wipro.com canonical name = d361nqn33s63ex.cloudfront.net
d361nqn33s63ex.cloudfront.net
primary name server = ns-1658.awsdns-15.co.uk
responsible mail addr = awsdns-hostmaster.amazon.com
serial = 1
refresh = 7200 (2 hours)
retry = 900 (15 mins)
expire = 1209600 (14 days)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

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

- Steps :
  1. Open terminal in kali linux
  2. Type `tracert www.ibm.com` for Ibm.com
  3. Type `tracert www.wipro.com` for Wipro.com

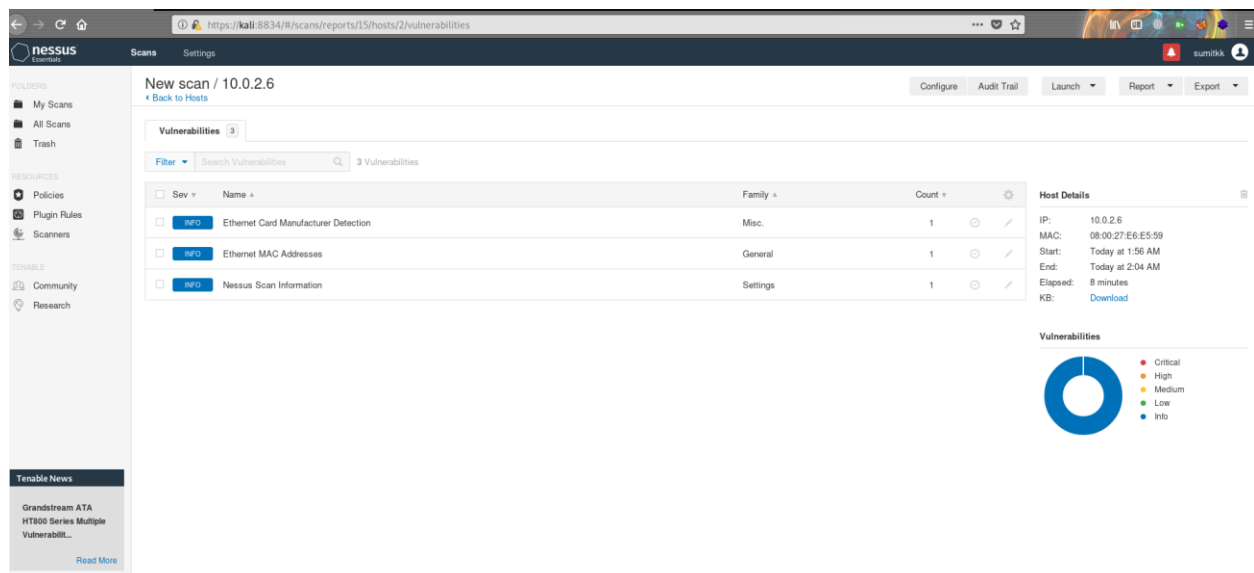
## 3. Question 3: Scan and find out port numbers open 203.163.246.23

The command is “`nmap -Pn -ss -A -v 203.163.246.23`”



```
Raw packets sent: 1141 (58.902KB) | Rcvd: 1818 (41.414KB)
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 02:01 PDT
NSE: Loaded NSE scripts for scanning:
NSE: Script Pre-scanning.
Initiating NSE at 02:01
Completed NSE at 02:01, 0.00s elapsed
Initiating NSE at 02:01
Completed NSE at 02:01, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host at 02:01
Completed Parallel DNS resolution of 1 host at 02:01, 0.00s elapsed
Initiating SYN Stealth Scan at 02:01
Scanning 203.163.246.23 [1000 ports]
State: 0/0/0/7 elapsed: 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.00% done; ETC: 02:06 (0:03:16 remaining)
SYN Stealth Scan Timing: About 22.20% done; ETC: 02:06 (0:02:36 remaining)
SYN Stealth Scan Timing: About 33.05% done; ETC: 02:06 (0:01:35 remaining)
SYN Stealth Scan Timing: About 43.90% done; ETC: 02:06 (0:01:04 remaining)
SYN Stealth Scan Timing: About 54.75% done; ETC: 02:06 (0:00:33 remaining)
Completed SYN Stealth Scan at 02:06, 216.00s elapsed (1000 total ports)
Initiating Service scan at 02:06
Initiating OS detection (try #1) against 203.163.246.23
RTTVAR has grown to over 2.5 seconds, decreasing to 2.0
Initiating Traceroute at 02:06
Completed Traceroute at 02:06, 9.87s elapsed
Initiating Parallel DNS resolution of 2 hosts at 02:06
Completed Parallel DNS resolution of 2 hosts at 02:06, 0.07s elapsed
NSE: Script scanning 203.163.246.23.
Initiating NSE at 02:06
Completed NSE at 02:06, 0.01s elapsed
Initiating NSE at 02:06
Completed NSE at 02:06, 0.00s elapsed
Initiating NSE at 02:06
Completed NSE at 02:06, 0.00s elapsed
Nmap scan report for 203.163.246.23
Host is up (5.6s latency).
All 1000 scanned ports on 203.163.246.23 are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 close
port
Device type: general purpose
Running: Microsoft Windows XP SP3
OS CPE: cpe:/o:microsoft:windows_xp:sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_se
ver_2012
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2
012
TRACEROUTE (using ip/icmp)
HOP RTT
0 0.00 ms 192.168.1.1
1 1.08 ms 192.168.154.2
2 0.13 ms 192.168.43.1
... 30
NSE: Script Post-scanning.
Initiating NSE at 02:06
```

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



The screenshot shows the Nessus web interface with the URL `https://kali:8834/#scans/reports/15/hosts/2/vulnerabilities`. The interface displays a table of vulnerabilities for the host 10.0.2.6. The table has columns for Severity, Name, Family, Count, and Host Details. The vulnerabilities listed are:

Sev	Name	Family	Count
Info	Ethernet Card Manufacturer Detection	Misc	1
Info	Ethernet MAC Addresses	General	1
Info	Nessus Scan Information	Settings	1

Host Details for 10.0.2.6:

- IP: 10.0.2.6
- MAC: 08:00:27:E6:E5:59
- Start: Today at 1:56 AM
- End: Today at 2:04 AM
- Elapsed: 8 minutes
- KB: Download

A donut chart titled 'Vulnerabilities' shows the distribution of severity levels: Critical (0), High (0), Medium (0), Low (0), and Info (3).

