

Question 1: Find out the mail servers of the following domain : lbm.com Wipro.com

```
C:\WINDOWS\system32\cmd.exe - nslookup
Microsoft Windows [Version 10.0.18363.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\admin>nslookup
Default Server: XiaoQiang
Address: 192.168.31.1

> set type=mx
> lbm.com
Server: XiaoQiang
Address: 192.168.31.1

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
lbm.com MX preference = 5, mail exchanger = mx0a-001b2d01.pphosted.com
lbm.com MX preference = 5, mail exchanger = mx0b-001b2d01.pphosted.com
> wipro.com
Server: XiaoQiang
Address: 192.168.31.1

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

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

lbm .com has hosted their mailserver with pphosted.com

Wipro.com has hosted their mail server with outlook.com

Question 3: Scan and find out port numbers open 203.163.246.23

```
kali@kali:~$ nmap -Pn 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 13:57 EDT
Stats: 0:00:33 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 75.00% done; ETC: 13:58 (0:00:11 remaining)
Nmap scan report for 203.163.246.23
Host is up (0.020s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
25/tcp    open  smtp
Nmap done: 1 IP address (1 host up) scanned in 110.37 seconds
kali@kali:~$
```

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

The screenshot displays the Nessus Essentials web interface in a browser window. The address bar shows the URL `https://localhost:8834/#/scans/reports/6/vulnerabilities`. The interface is for a scan named 'mysystem'. On the left, there is a sidebar with 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Scanners, Tenable Community, Research). The main content area shows a table of 14 vulnerabilities. The table has columns for Severity, Name, Family, and Count. The vulnerabilities listed include 'SMB Signing not required' (Medium), 'DCE Services Enumeration' (Info), 'SMB (Multiple Issues)' (Info), 'Microsoft Windows (Multiple Issues)' (Info), 'Authenticated Check : OS Name and I...' (Info), 'Authentication Failure - Local Checks ...' (Info), 'Common Platform Enumeration (CPE)' (Info), 'Device Type' (Info), and 'Host Fully Qualified Domain Name (F...' (Info). To the right of the table, there is a 'Scan Details' section showing 'Policy: Advanced Scan', 'Status: Completed', 'Scanner: Local Scanner', 'Start: Today at 3:48 PM', 'End: Today at 3:55 PM', and 'Elapsed: 8 minutes'. Below this is a 'Vulnerabilities' donut chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). The Windows taskbar at the bottom shows the time as 4:36 PM on 26-Aug-20.

Sev	Name	Family	Count
MEDIUM	SMB Signing not required	Misc.	1
INFO	DCE Services Enumeration	Windows	8
INFO	SMB (Multiple Issues)	Windows	5
INFO	Microsoft Windows (Multiple Issues)	Windows	2
INFO	Authenticated Check : OS Name and I...	Settings	1
INFO	Authentication Failure - Local Checks ...	Settings	1
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Host Fully Qualified Domain Name (F...	General	1