

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

```
C:\WINDOWS\system32>nslookup
Default Server: UnKnown
Address: 192.168.43.1

> set type=mx
> ibm.com
Server: UnKnown
Address: 192.168.43.1

Non-authoritative answer:
ibm.com MX preference = 5, mail exchanger = mx0b-001b2d01.pphosted.com
ibm.com MX preference = 5, mail exchanger = mx0a-001b2d01.pphosted.com
>
```

```
C:\WINDOWS\system32>nslookup
Default Server: UnKnown
Address: 192.168.43.1

> set type=mx
> wipro.com
Server: UnKnown
Address: 192.168.43.1

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.

mail@ibm.com	
Mailbox Domain	mx0b-001b2d01.pphosted.com
IP	148.163.158.5
Country	United States
City	Sunnyvale
Latitude	37.424900054932
Longitude	-122.0074005127
ISP	N/A

mail@wipro.com	
Mailbox Domain	wipro-com.mail.protection.outlook.com
IP	104.47.126.36
Country	Korea, Republic of
City	Busan
Latitude	35.102798461914
Longitude	129.04029846191
ISP	N/A

Question 3: Scan and find out port numbers open 203.163.246.23

```
root@kali:~# nmap -Pn -sS -A -v 203.163.246.23
Starting Nmap 7.70 ( https://nmap.org ) at 2020-08-29 12:18 IST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:18
Completed NSE at 12:18, 0.00s elapsed
Initiating NSE at 12:18
Completed NSE at 12:18, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 12:18
Completed Parallel DNS resolution of 1 host. at 12:18, 0.22s elapsed
Initiating SYN Stealth Scan at 12:18
Scanning 203.163.246.23 [1000 ports]
SYN Stealth Scan Timing: About 15.25% done; ETC: 12:22 (0:02:52 remaining)
SYN Stealth Scan Timing: About 30.00% done; ETC: 12:22 (0:02:22 remaining)
SYN Stealth Scan Timing: About 45.00% done; ETC: 12:22 (0:01:51 remaining)
SYN Stealth Scan Timing: About 60.00% done; ETC: 12:22 (0:01:21 remaining)
SYN Stealth Scan Timing: About 74.50% done; ETC: 12:22 (0:00:52 remaining)
Completed SYN Stealth Scan at 12:22, 202.76s elapsed (1000 total ports)
Initiating Service scan at 12:22
Initiating OS detection (try #1) against 203.163.246.23
Retrying OS detection (try #2) against 203.163.246.23
Initiating Traceroute at 12:22
Completed Traceroute at 12:22, 9.07s elapsed
Initiating Parallel DNS resolution of 7 hosts. at 12:22
Completed Parallel DNS resolution of 7 hosts. at 12:22, 0.14s elapsed
NSE: Script scanning 203.163.246.23.
Initiating NSE at 12:22
Completed NSE at 12:22, 0.01s elapsed
Initiating NSE at 12:22
Completed NSE at 12:22, 0.00s elapsed
Nmap scan report for 203.163.246.23
Host is up.
All 1000 scanned ports on 203.163.246.23 are filtered
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 95.43 ms 192.168.0.1
2 95.44 ms 10.80.0.1
3 96.71 ms 125.99.88.1
4 95.59 ms 203.212.193.30
5 95.88 ms 125.99.55.254
6 96.85 ms 125.99.55.253
7 96.93 ms 136.232.27.245.static.jio.com (136.232.27.245)
8 ... 30

NSE: Script Post-scanning.
Initiating NSE at 12:22
Completed NSE at 12:22, 0.00s elapsed
Initiating NSE at 12:22
Completed NSE at 12:22, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 223.60 seconds
Raw packets sent: 2124 (96.800KB) | Rcvd: 7 (512B) All 1000 scanned ports on 203.163.246.23 are filtered
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 95.43 ms 192.168.0.1
2 95.44 ms 10.80.0.1
```

```

3 96.71 ms 125.99.88.1
4 95.59 ms 203.212.193.30
5 95.88 ms 125.99.55.254
6 96.85 ms 125.99.55.253
7 96.93 ms 136.232.27.245.static.jio.com (136.232.27.245)
8 ... 30

```

NSE: Script Post-scanning.

Initiating NSE at 12:22

Completed NSE at 12:22, 0.00s elapsed

Initiating NSE at 12:22

Completed NSE at 12:22, 0.00s elapsed

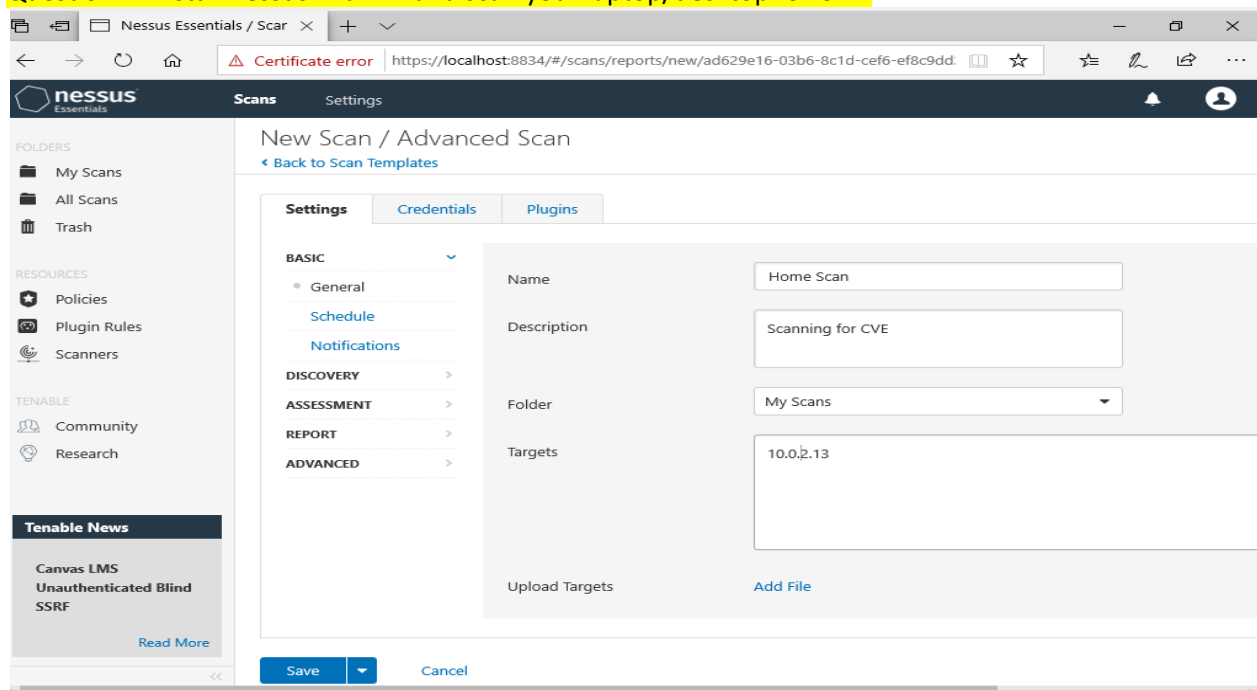
Read data files from: /usr/bin/./share/nmap

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 223.60 seconds

Raw packets sent: 2124 (96.800KB) | Rcvd: 7 (512B)

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



Nessus Essentials / Scan

Certificate error https://localhost:8834/#/scans/reports/new/ad629e16-03b6-8c1d-cef6-ef8c9dd

nessus Essentials Scans Settings

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Scanners

TENABLE

- Community
- Research

Tenable News

Canvas LMS
Unauthenticated Blind
SSRF

Read More

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Home Scan

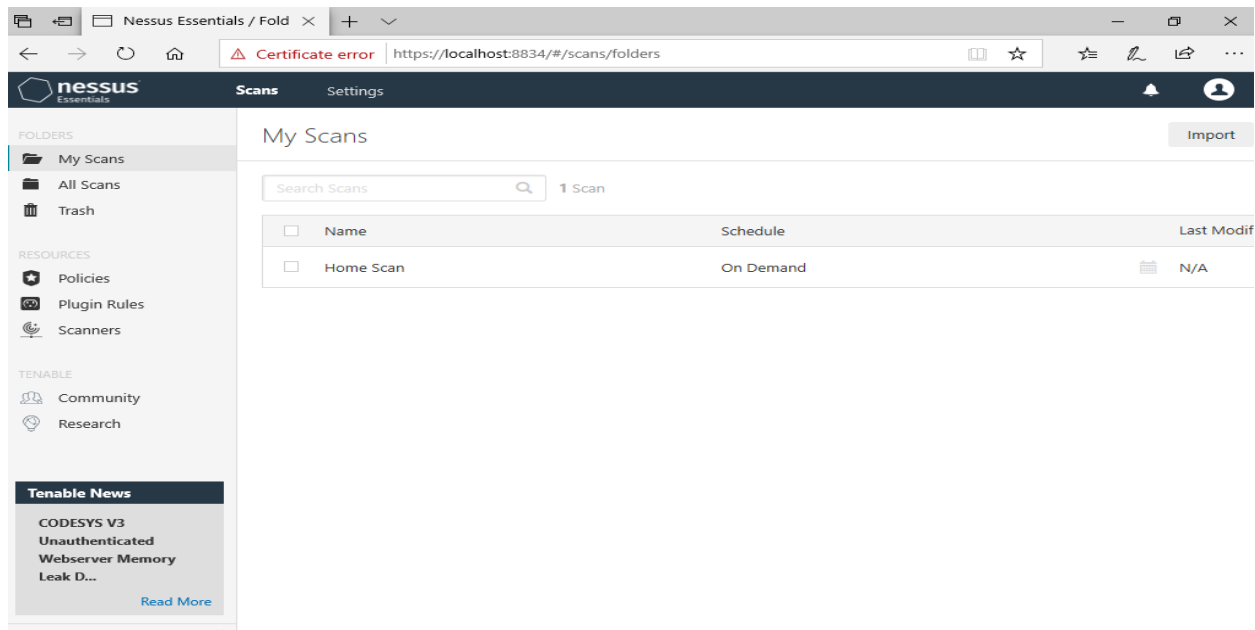
Description: Scanning for CVE

Folder: My Scans

Targets: 10.0.2.13

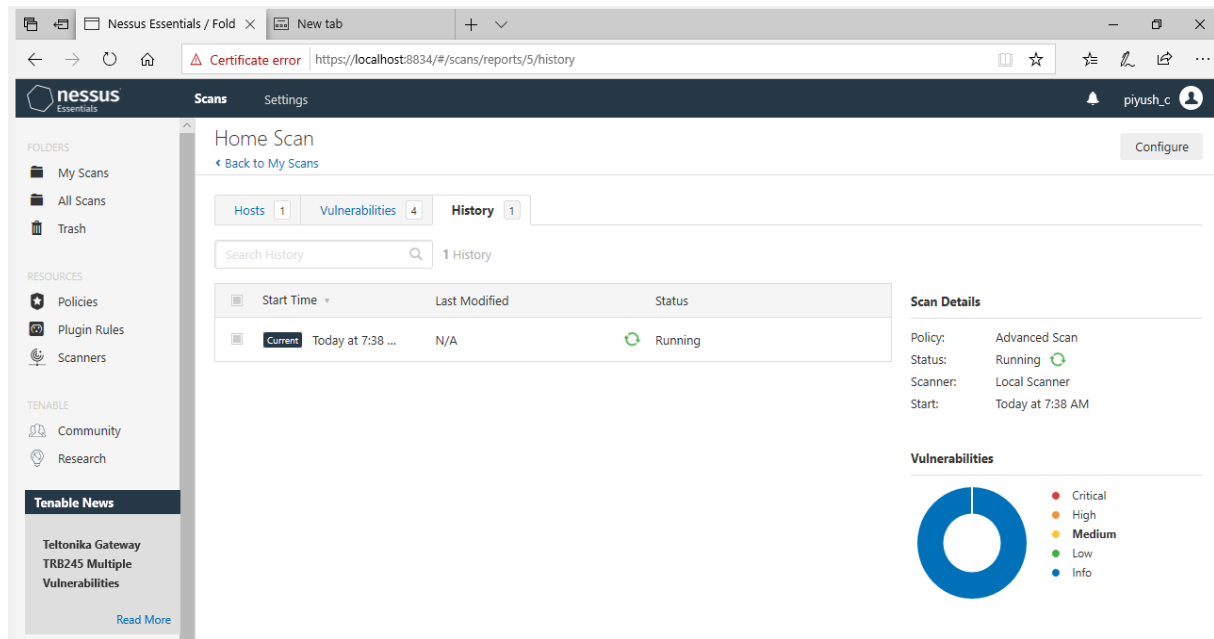
Upload Targets Add File

Save Cancel



The screenshot shows the Nessus Essentials web interface. The left sidebar contains navigation links for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Scanners), and TENABLE (Community, Research). A 'Tenable News' section at the bottom of the sidebar highlights a 'CODESYS V3 Unauthenticated Webserver Memory Leak D...' with a 'Read More' link. The main content area is titled 'My Scans' and includes a search bar and a table with one scan entry:

<input type="checkbox"/>	Name	Schedule	Last Modified
<input type="checkbox"/>	Home Scan	On Demand	N/A



The screenshot shows the 'Home Scan' details page in Nessus Essentials. The left sidebar is identical to the previous screenshot. The main content area is titled 'Home Scan' and includes a 'Back to My Scans' link and a 'Configure' button. Below the title are tabs for 'Hosts' (1), 'Vulnerabilities' (4), and 'History' (1). The 'History' tab is active, showing a search bar and a table with one history entry:

<input type="checkbox"/>	Start Time	Last Modified	Status
<input type="checkbox"/>	Current Today at 7:38 ...	N/A	Running

To the right of the table is a 'Scan Details' section:

- Policy: Advanced Scan
- Status: Running
- Scanner: Local Scanner
- Start: Today at 7:38 AM

Below the scan details is a 'Vulnerabilities' section featuring a donut chart and a legend:

- Critical
- High
- Medium
- Low
- Info

Nessus Essentials / Fold X New tab

Certificate error https://localhost:8834/#/scans/reports/5/history

nessus Essentials Scans Settings piyush_c

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Scanners

TENABLE

- Community
- Research

Tenable News

How to Achieve 20/20 Visibility in Your OT Securit...
[Read More](#)

Home Scan

[Back to My Scans](#)

Hosts 1 Vulnerabilities 13 History 1


Search History

Start Time	Last Modified	Status
Current	Today at 7:38 AM	Completed

Scan Details

Policy: Advanced Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 7:38 AM
End: Today at 7:44 AM
Elapsed: 6 minutes

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

Nessus Essentials / Fold X New tab

Certificate error https://localhost:8834/#/scans/reports/5/vulnerabilities

nessus Essentials Scans Settings piyush_c

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Scanners

TENABLE

- Community
- Research

Tenable News

How to Achieve 20/20 Visibility in Your OT Securit...
[Read More](#)

Vulnerabilities


Filter Search Vulnerabilities 13 Vulnerabilities

Sev	Name	Family	Count
MEDIUM	SMB Signing not requir...	Misc.	1
INFO	DCE Services Enumerati...	Windows	9
INFO	SMB (Multiple Issu...	Windows	5
INFO	Microsoft Window...	Windows	2
INFO	Authenticated Check : ...	Settings	1
INFO	Common Platform Enu...	General	1
INFO	Device Type	General	1
INFO	Host Fully Qualified Do...	General	1
INFO	Local Checks Not Enabl...	Settings	1
INFO	Missing Scan Information	Settings	1

Scan Details

Policy: Advanced Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 7:38 AM
End: Today at 7:44 AM
Elapsed: 6 minutes

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

