

## **Day 4**

### **1. Find out the mail servers of the following domain:**

- **IBM.com**
- **Wipro.com**

**Open PenTester VMware workstation**

**Open Command Prompt**

**Type**

**ipconfig**

**nslookup**

**[www.ibm.com](http://www.ibm.com)**

```
> www.Ibm.com
Server: www.routerlogin.com
Address: 192.168.1.1

Non-authoritative answer:
Name: e2874.dscx.akamaiedge.net
Addresses: 2600:140f:c000:185::b3a
           2600:140f:c000:181::b3a
           106.51.145.132
Aliases: www.Ibm.com
          www.ibm.com.cs186.net
          outer-ccdn-dual.ibmcom.edgekey.net
          outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net
```

**[www.Wipro.com](http://www.Wipro.com)**

```
> www.Wipro.com
Server: www.routerlogin.com
Address: 192.168.1.1

Non-authoritative answer:
Name: d361nqn33s63ex.cloudfront.net
Addresses: 2600:9000:215c:ec00:13:4f33:b240:93a1
           2600:9000:215c:b400:13:4f33:b240:93a1
           2600:9000:215c:c00:13:4f33:b240:93a1
           2600:9000:215c:6600:13:4f33:b240:93a1
           2600:9000:215c:ac00:13:4f33:b240:93a1
           2600:9000:215c:a600:13:4f33:b240:93a1
           2600:9000:215c:9600:13:4f33:b240:93a1
           2600:9000:215c:b000:13:4f33:b240:93a1
           13.249.221.103
           13.249.221.64
           13.249.221.39
           13.249.221.15
Aliases: www.Wipro.com
```

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

### **Cont. of Question 1**

#### **Type:**

**set type=mx**

**lbm.com**

```
> set type=mx
> lbm.com
Server: www.routerlogin.com
Address: 192.168.1.1

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
```

#### **Open google chrome**

#### **Open IP Location Finder**

#### **Copy paste the url and find the location**

#### **Address 1:**

##### **IP Location Finder**

LOOKUP IP ADDRESS OR HOSTNAME

IP address or hostname

mx0a-001b2d01.pphosted.com

Find

###### LOCATION

|             |                                       |
|-------------|---------------------------------------|
| Country     | United States (US)                    |
| Continent   | North America (NA)                    |
| Coordinates | 37.751 (lat) / -97.822 (long)         |
| Time        | 2020-08-26 05:26:29 (America/Chicago) |

###### NETWORK

|            |                            |
|------------|----------------------------|
| IP address | 148.163.156.1              |
| Hostname   | mx0a-001b2d01.pphosted.com |
| Provider   | PROOFPOINT-ASN-US-WEST     |
| ASN        | 26211                      |

#### **Address 2:**

IP address or hostname

mx0b-001b2d01.pphosted.com

Find

LOCATION

|             |                                       |
|-------------|---------------------------------------|
| Country     | United States (US)                    |
| Continent   | North America (NA)                    |
| Coordinates | 37.751 (lat) / -97.822 (long)         |
| Time        | 2020-08-26 05:27:30 (America/Chicago) |

NETWORK

|            |                            |
|------------|----------------------------|
| IP address | 148.163.158.5              |
| Hostname   | mx0b-001b2d01.pphosted.com |
| Provider   | PROOFPOINT-ASN-US-EAST     |
| ASN        | 22843                      |

## **Wipro.com**

```
> Wipro.com
Server: www.routerlogin.com
Address: 192.168.1.1

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

## **Open google chrome**

## **Open IP Location Finder**

## **Copy paste the URL and find the location**

## **Address:**

IP address or hostname

wipro-com.mail.protection.outlook.com

Find

LOCATION

|             |                                  |
|-------------|----------------------------------|
| City        | Busan                            |
| Region      | Busan (26)                       |
| Postal code | 48943                            |
| Country     | South Korea (KR)                 |
| Continent   | Asia (AS)                        |
| Coordinates | 35.1003 (lat) / 129.0442 (long)  |
| Time        | 2020-08-26 19:34:26 (Asia/Seoul) |

NETWORK

|            |  |
|------------|--|
| IP address | 104.47.126.36                                    |
| Hostname   | mail-pu1apc010036.inbound.protection.outlook.com |
| Provider   | MICROSOFT-CORP-MSN-AS-BLOCK                      |
| ASN        | 8075   |

### **3. Scan and find out port numbers open 203.163.246.23**

**Open Kali-pc**

**Right click on the screen and Open Terminal**

**Type:**

**sudo su -**

**Enter password**

**Enter - nmap -Pn -sS 203.163.246.23**

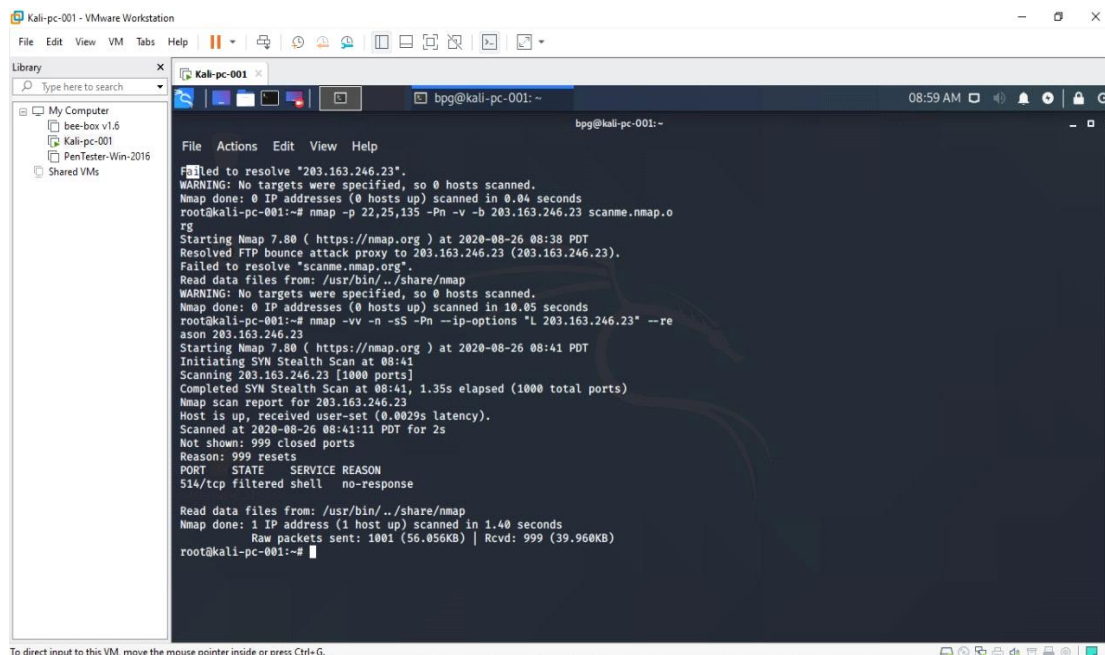
```
bpg@kali-pc-001: ~/Desktop
File Actions Edit View Help
bpg@kali-pc-001:~/Desktop$ sudo su -
[sudo] password for bpg:
root@kali-pc-001:~# nmap -Pn -sS 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 05:12 PDT
Stats: 0:02:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 63.00% done; ETC: 05:15 (0:01:15 remaining)
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 215.64 seconds
root@kali-pc-001:~#
```

```
Kali-pc-001 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
bee-box v1.6
Kali-pc-001
PenTester-Win-2016
Shared VMs
bpg@kali-pc-001: ~
08:58 AM
bpg@kali-pc-001: ~
File Actions Edit View Help
bpg@kali-pc-001:~$ sudo su -
[sudo] password for bpg:
root@kali-pc-001:~# nmap -sS -v -v -Pn -g 88 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 08:31 PDT
Initiating Parallel DNS resolution of 1 host. at 08:31
Completed Parallel DNS resolution of 1 host. at 08:31, 0.49s elapsed
Initiating SYN Stealth Scan at 08:31
Scanning 203.163.246.23 [1000 ports]
SYN Stealth Scan Timing: About 15.50% done; ETC: 08:34 (0:02:49 remaining)
SYN Stealth Scan Timing: About 30.00% done; ETC: 08:34 (0:02:22 remaining)
SYN Stealth Scan Timing: About 45.00% done; ETC: 08:34 (0:01:51 remaining)
SYN Stealth Scan Timing: About 59.50% done; ETC: 08:34 (0:01:22 remaining)
SYN Stealth Scan Timing: About 74.50% done; ETC: 08:34 (0:00:52 remaining)
Completed SYN Stealth Scan at 08:34, 203.60s elapsed (1000 total ports)
Nmap scan report for 203.163.246.23
Host is up, received user-set.
All 1000 scanned ports on 203.163.246.23 are filtered because of 1000 no-responses

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 204.44 seconds
Raw packets sent: 2000 (88.000KB) | Rcvd: 0 (0B)
root@kali-pc-001:~# nmap -6 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 08:36 PDT
Warning: Hostname 203.163.246.23 resolves, but not to any IPv6 address. Try scanning without -6
Failed to resolve "203.163.246.23".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds
root@kali-pc-001:~# nmap -p 22,25,135 -Pn -v -b 203.163.246.23 scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 08:38 PDT
Resolved FTP bounce attack proxy to 203.163.246.23 (203.163.246.23).
Failed to resolve "scanme.nmap.org".
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



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

#### **Open PenTester VMware workstation**

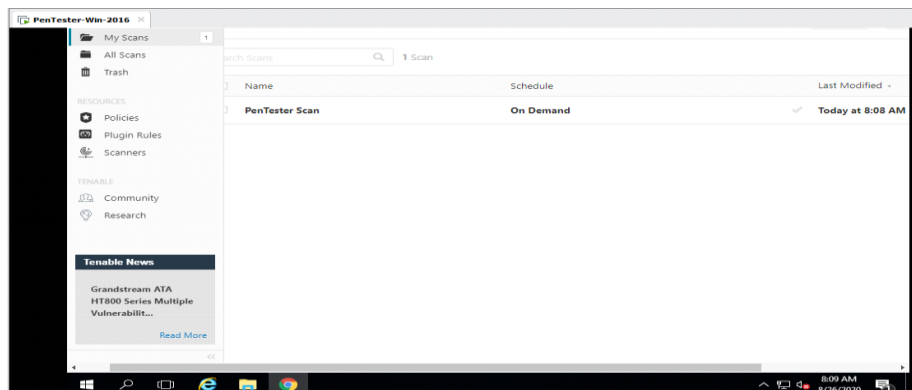
#### **Install Google Chrome**

#### **Install Nessus**

#### **Click on All scans**

#### **Create a new scan Advance settings Windows**

#### **Fill the required blanks in credentials as well Launch Report**



FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Scanners

TENABLE

Community

Research

Tenable News

PenTester Scan

Configure

Hosts0

Vulnerabilities0

History1

Search History1 History

| <input type="checkbox"/> | Start Time | Last Modified     | Status           |
|--------------------------|------------|-------------------|------------------|
| <input type="checkbox"/> | Current    | Today at 8:08 ... | Today at 8:08 AM |
|                          |            |                   | ✓ Completed      |

## Scan Details

|          |                  |
|----------|------------------|
| Policy:  | Advanced Scan    |
| Status:  | Completed        |
| Scanner: | Local Scanner    |
| Start:   | Today at 8:08 AM |
| End:     | Today at 8:08 AM |
| Elapsed: | a few seconds    |