

### Assignment 4

#### Question 1:

Find out the mail servers of the following domain :

**ibm.com**

**Wipro.com**

Solution:

Using **nslookup** and **setting type=mx** . On searching I found these results :-

Mail servers of ibm.com = **mx0b-001b2d01.pphosted.com** and **mx0a-001b2d01.pphosted.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
>
```

Mail servers of wipro.com = **wipro-com.mail.protection.outlook.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.

Solution:

Location of mail server of ibm.com:-

[mx0a-001b2d01.pphosted.com](https://mx0a-001b2d01.pphosted.com)

### LOCATION

<b>Country</b>	United States (US)
<b>Continent</b>	North America (NA)
<b>Coordinates</b>	37.751 (lat) / -97.822 (long)
<b>Time</b>	2020-08-28 02:17:58 (America/Chicago)

### NETWORK

<b>IP address</b>	148.163.156.1
<b>Hostname</b>	mx0a-001b2d01.pphosted.com
<b>Provider</b>	PROOFPOINT-ASN-US-WEST
<b>ASN</b>	26211



mx0b-001b2d01.pphosted.com

#### LOCATION

<b>Country</b>	United States (US)
<b>Continent</b>	North America (NA)
<b>Coordinates</b>	37.751 (lat) / -97.822 (long)
<b>Time</b>	2020-08-28 02:16:09 (America/Chicago)

#### NETWORK

<b>IP address</b>	148.163.158.5
<b>Hostname</b>	mx0b-001b2d01.pphosted.com
<b>Provider</b>	PROOFPOINT-ASN-US-EAST
<b>ASN</b>	22843



Location of mail server of wipro.com:-

wipro-com.mail.protection.outlook.com

LOCATION

<b>City</b>	Singapore
<b>Postal code</b>	18
<b>Country</b>	Singapore (SG)
<b>Continent</b>	Asia (AS)
<b>Coordinates</b>	1.2929 (lat) / 103.8547 (long)
<b>Time</b>	2020-08-28 15:21:26 (Asia/Singapore)

NETWORK

<b>IP address</b>	104.47.125.36
<b>Hostname</b>	mail-sg2apc010036.inbound.protection.outlook.com
<b>Provider</b>	MICROSOFT-CORP-MSN-AS-BLOCK
<b>ASN</b>	8075



### Question 3:

### Scan and find out port numbers open 203.163.246.23

Solution :-

Using simple command `nmap -T4 -p- -vv -A 203.163.246.23` we get following results:

```
C:\WINDOWS\system32\nmap -T4 -p- -vv -A 203.163.246.23
Starting Nmap 2.00 ( https://nmap.org ) at 2020-08-28 12:22 India Standard Time
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 12:22
Completed NSE at 12:22, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 12:22
Completed NSE at 12:22, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 12:22
Completed NSE at 12:22, 0.00s elapsed
Initiating Ping Scan at 12:22
Scanning 203.163.246.23 [4 ports]
Completed Ping Scan at 12:22, 0.76s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:22
Completed Parallel DNS resolution of 1 host. at 12:22, 0.01s elapsed
Initiating SYN Stealth Scan at 12:22
Scanning 203.163.246.23 [65535 ports]
SYN Stealth Scan Timing: About 20.57% done; ETC: 12:25 (0:02:00 remaining)
SYN Stealth Scan Timing: About 48.10% done; ETC: 12:24 (0:01:00 remaining)
SYN Stealth Scan Timing: About 69.92% done; ETC: 12:24 (0:00:39 remaining)
Completed SYN Stealth Scan at 12:24, 122.90s elapsed (65535 total ports)
Initiating Service scan at 12:24
Initiating OS detection (try #1) against 203.163.246.23
Retrying OS detection (try #2) against 203.163.246.23
Initiating Traceroute at 12:24
Completed Traceroute at 12:24, 3.02s elapsed
Initiating Parallel DNS resolution of 5 hosts. at 12:24
Completed Parallel DNS resolution of 5 hosts. at 12:24, 0.07s elapsed
NSE: Script scanning 203.163.246.23.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 12:24
Completed NSE at 12:24, 0.01s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 12:24
Completed NSE at 12:24, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 12:24
Completed NSE at 12:24, 0.00s elapsed
Nmap scan report for 203.163.246.23
Host is up, received reset ttl 124 (0.061s latency).
All 65535 scanned ports on 203.163.246.23 are filtered because of 65535 no-responses
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing an open TCP port so results incomplete
Aggressive OS guesses: Cisco Adaptive Security Appliance (ASA 9.2) (96%), Synology RT1900ac router (96%), Asus RT-53N WAP (95%), Cisco Adaptive Security Appliance 5510 or 5540 Firewall (ASA 8.0) (95%), Cisco ACE load balancer (95%), Cisco 3925 router (IOS 12.4) (95%), Cisco 3550 switch (IOS 12.2) (95%), Cisco ASA 5510 Firewall (PIX OS 8.2) (95%), Foundry Networks BigIron 8000 switch (IronWare 07.0.02eT53) (95%), Linux 2.6.32 (95%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(47.08%  
40.00/28000-NCI-NCU-SPW-WRO-SBDC-TG6-WTH-SF48AA30D-1686-pc-windows-windows)
Tg(4-W20-W51G-980u-2000RS-a3a-S3f-AR20-SRD-89Q-)
U1(R-W)
U1(R-W)
LE(R-W)
Network Distance: 6 hops
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 2.00 ms 192.168.43.1
2 ...
3 44.00 ms 10.72.192.101
4 44.00 ms 192.168.24.194
5 45.00 ms 192.168.24.197
6 45.00 ms 203.163.246.23
```

```
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 2.00 ms 192.168.43.1
2 ...
3 44.00 ms 10.72.192.101
4 44.00 ms 192.168.24.194
5 45.00 ms 192.168.24.197
6 45.00 ms 203.163.246.23

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 12:24
Completed NSE at 12:24, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 12:24
Completed NSE at 12:24, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 12:24
Completed NSE at 12:24, 0.00s elapsed
Read data files from: C:\Program Files (x86)\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 132.27 seconds
Raw packets sent: 131223 (5.778MB) | Rcvd: 110 (4.582KB)
```

we can also use a tool called **red hawk** to know the open ports

commands to install and run red hawk

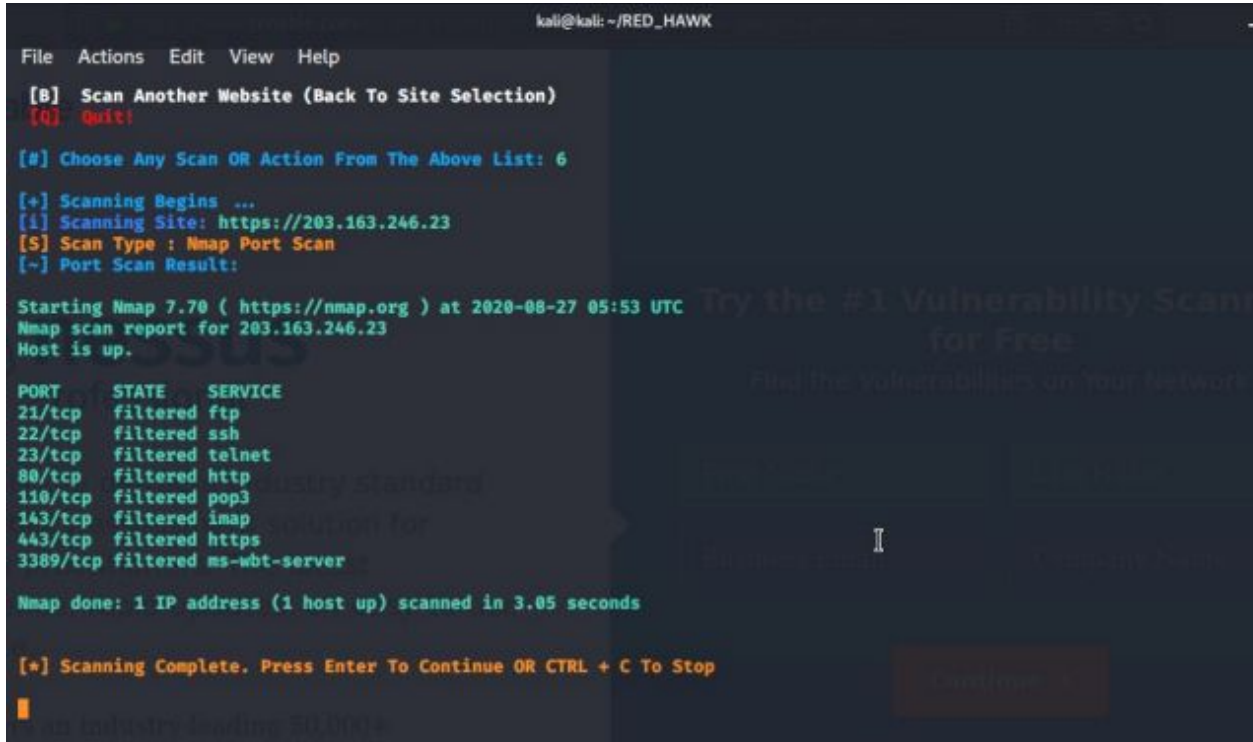
1.git clone [https://github.com/Tuhinshubhra/RED\\_HAWK](https://github.com/Tuhinshubhra/RED_HAWK)

2.cd RED\_HAWK

3.php rhawk.php

enter the ip or domain name then find the open ports.

I used Kali VM for better performance.



```
kali@kali: ~/RED_HAWK
File Actions Edit View Help
[B] Scan Another Website (Back To Site Selection)
[Q] Quit!

[0] Choose Any Scan OR Action From The Above List: 6

[+] Scanning Begins ...
[+] Scanning Site: https://203.163.246.23
[+] Scan Type : Nmap Port Scan
[+] Port Scan Result:

Starting Nmap 7.70 ( https://nmap.org ) at 2020-08-27 05:53 UTC
Nmap scan report for 203.163.246.23
Host is up.

PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
80/tcp    filtered http
110/tcp   filtered pop3
143/tcp   filtered imap
443/tcp   filtered https
3389/tcp  filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 3.05 seconds

[+] Scanning Complete. Press Enter To Continue OR CTRL + C To Stop
```

#### Question 4:

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

Solution :

I downloaded Nessus on my **PARROT Virtual machine** because **my system hangs up with KALI Linux**

Step 1) Downloaded **Nessus-8.11.1-debian6\_amd64.deb** from the official site.




```
[pentester@parrot]-(~/Downloads)
$ls
cacert.der
GPUCache
Nessus-8.11.1-debian6_amd64.deb
```



Step 2) Installing Nessus using `sudo dpkg -i Nessus-8.11.1-debian6_amd64.deb` command .

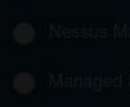
```
[x]~[pentester@parrot]~[~/Downloads]
$ sudo dpkg -i Nessus-8.11.1-debian6_amd64.deb
[sudo] password for pentester:
Selecting previously unselected package nessus.
(Reading database ... 402732 files and directories currently installed.)
Preparing to unpack Nessus-8.11.1-debian6_amd64.deb ...
Unpacking nessus (8.11.1) ...
Setting up nessus (8.11.1) ...
Unpacking Nessus Scanner Core Components...
Created symlink /etc/systemd/system/nessusd.service → /lib/systemd/system/nessusd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/nessusd.service → /lib/systemd/system/nessusd.service.

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://parrot:8834/ to configure your scanner
```

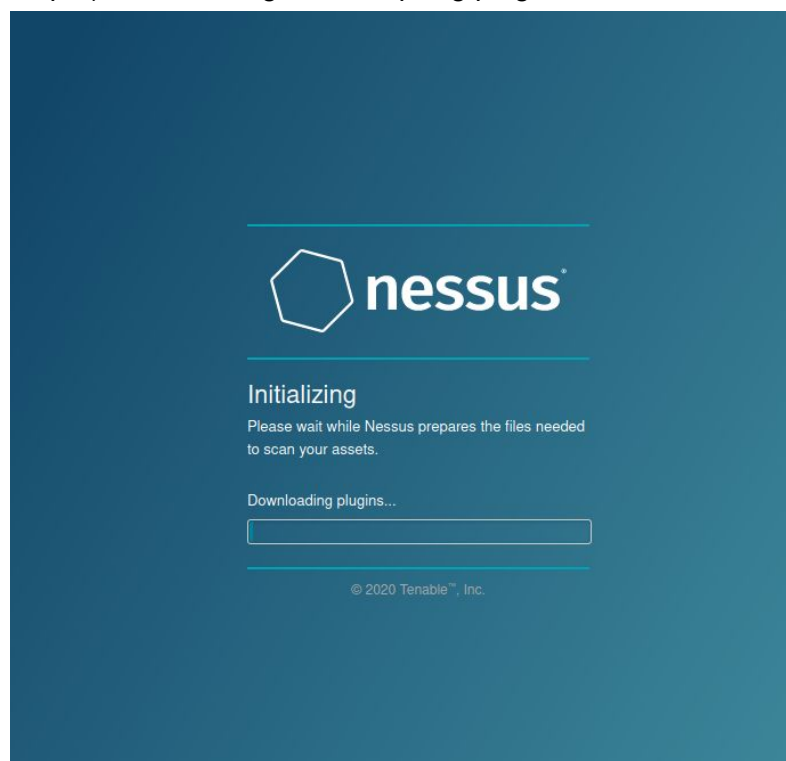
The image shows the Nessus logo and a "Welcome to Nessus" screen. It includes a heading "Welcome to Nessus" and a subheading "I want to deploy Nessus. Select a". Below this, there are two radio button options: "Nessus Essentials" and "Nessus Professional".

Step 3) Starting Nessus Daemon service using `sudo /bin/systemctl start Nessus.service` command

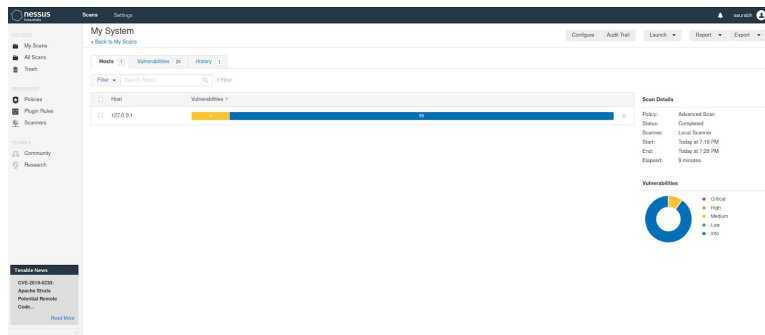
```
[x]~[pentester@parrot]~[~/Downloads]
$ /bin/systemctl start nessusd.service
[pentester@parrot]~[~/Downloads]
$ /bin/systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; enabled; vendor prese
   Active: active (running) since Tue 2020-08-25 12:38:36 MDT; 10s ago
     Main PID: 2401 (nessus-service)
        Tasks: 13 (limit: 4939)
       Memory: 79.7M
      CGroup: /system.slice/nessusd.service
              └─2401 /opt/nessus/sbin/nessus-service -q
                 └─2402 nessusd -q
lines 1-9/9 (END)...skipping...
```

The image shows the output of the systemctl status command for the nessusd.service. It includes details about the service's state, such as "Loaded: loaded (/lib/systemd/system/nessusd.service; enabled; vendor prese", "Active: active (running) since Tue 2020-08-25 12:38:36 MDT; 10s ago", "Main PID: 2401 (nessus-service)", "Tasks: 13 (limit: 4939)", "Memory: 79.7M", and "CGroup: /system.slice/nessusd.service". It also shows the process tree for the service.

Step 4) Downloading and compiling plugins in the browser using <https://parrot.8834/> url.



Step 5) Started scan for ip = 127.0.0.1



Step 6) Report for the scan of the local system.

