Day 4 Assignment

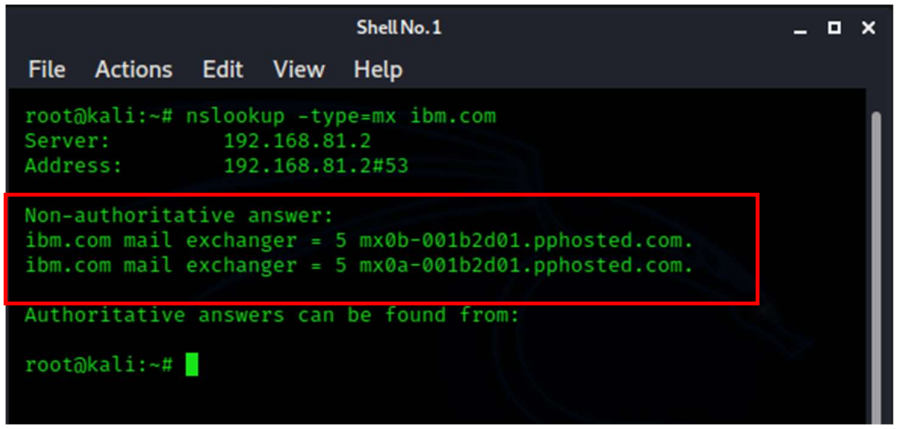
Registered Name: Arindam Pal

Registered email: arindampal705@gmail.com

1) Mail Servers

- Open terminal in kali Linux
- Type '**`nslookup -type=mx (domain name)`**'

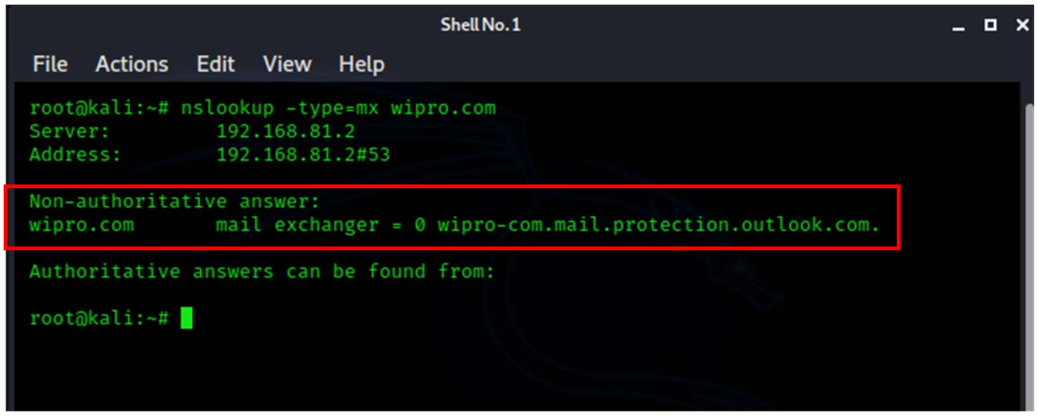
➢ For ibm.com



Therefore, there are two mail servers of ibm.com:

- ✓ **mx0b-001b2d01.pphosted.com.**
- ✓ **mx0a-001b2d01.pphosted.com.**

➢ For wipro.com



Therefore, there is only one mail server of wipro.com:

- ✓ **wipro-com.mail.protection.outlook.com**

2) Mail Servers Locations

- Firstly, install '**jq**'
- **`( Sudo apt-get install curl jq )`**

```
Shell No.1
File  Actions  Edit  View  Help
root@kali:~# sudo apt-get install curl jq
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
curl is already the newest version (7.68.0-1+b1).
jq is already the newest version (1.6-1).
The following packages were automatically installed and are no longer required:
  fonts-glyphicons-halflings gir1.2-appindicator3-0.1 libappindicator3-1
  libboost-iostreams1.67.0 libboost-system1.67.0 libboost-thread1.67.0 libcdio18
  libgdal26 libicu63 libmpdec2 libprotobuf22 libpython3.7-minimal
  libpython3.7-stdlib libqhull7 libre2-6 libx264-155 libx265-179 php7.3-mysql
  python3-flask-session python3-pcapfile python3.7 python3.7-minimal
  ruby-did-you-mean
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 17 not upgraded.
root@kali:~#
```

- Then find mx details by using **nslookup**
- Now find the mail server addresses from **nslookup**
- And then put it on `curl` **`https://ipinfo.io/(address)`**

➢ For ibm.com

1) These are the mail servers:

```
Shell No.1
File  Actions  Edit  View  Help
root@kali:~# nslookup -type=mx ibm.com
Server:         192.168.81.2
Address:        192.168.81.2#53

Non-authoritative answer:
ibm.com mail exchanger = 5 mx0b-001b2d01.pphosted.com.
ibm.com mail exchanger = 5 mx0a-001b2d01.pphosted.com.

Authoritative answers can be found from:

root@kali:~#
```

2) **Now find addresses of each mail server:**

```
Shell No. 1
File  Actions  Edit  View  Help
root@kali:~# nslookup mx0a-001b2d01.pphosted.com
Server:         192.168.81.2
Address:        192.168.81.2#53

Non-authoritative answer:
Name:   mx0a-001b2d01.pphosted.com
Address: 148.163.156.1

root@kali:~# nslookup mx0b-001b2d01.pphosted.com.
Server:         192.168.81.2
Address:        192.168.81.2#53

Non-authoritative answer:
Name:   mx0b-001b2d01.pphosted.com
Address: 148.163.158.5

root@kali:~#
```

3) **Then find each mail servers locations:**

```
Shell No. 1
File  Actions  Edit  View  Help
root@kali:~/Desktop#  curl https://ipinfo.io/148.163.156.1
{
  "ip": "148.163.156.1",
  "hostname": "mx0a-001b2d01.pphosted.com",
  "city": "Sunnyvale",
  "region": "California",
  "country": "US",
  "loc": "37.3688,-122.0363",
  "org": "AS26211 Proofpoint, Inc.",
  "postal": "94088",
  "timezone": "America/Los_Angeles",
  "readme": "https://ipinfo.io/missingauth"
```

```
root@kali:~/Desktop#  curl https://ipinfo.io/148.163.158.5
{
  "ip": "148.163.158.5",
  "hostname": "mx0b-001b2d01.pphosted.com",
  "city": "San Jose",
  "region": "California",
  "country": "US",
  "loc": "37.3394,-121.8950",
  "org": "AS22843 Proofpoint, Inc.",
  "postal": "95103",
  "timezone": "America/Los_Angeles",
  "readme": "https://ipinfo.io/missingauth"
}root@kali:~/Desktop#
```

➢ For wipro.com

1) **Find Wipro mail server address.**

```
Shell No.1
File  Actions  Edit  View  Help
root@kali:~# nslookup wipro-com.mail.protection.outlook.com
Server:         192.168.81.2
Address:        192.168.81.2#53

Non-authoritative answer:
Name:   wipro-com.mail.protection.outlook.com
Address: 104.47.126.36
Name:   wipro-com.mail.protection.outlook.com
Address: 104.47.125.36

root@kali:~#
```

2) **Here we got 2 addresses. Now find the location of each address:**

```
Shell No.1
File  Actions  Edit  View  Help
root@kali:~#  curl https://ipinfo.io/104.47.126.36
{
  "ip": "104.47.126.36",
  "hostname": "mail-pu1apc010036.inbound.protection.outlook.com",
  "city": "Dongnae",
  "region": "Busan",
  "country": "KR",
  "loc": "35.2016,129.0848",
  "org": "AS8075 Microsoft Corporation",
  "postal": "47738",
  "timezone": "Asia/Seoul",
  "readme": "https://ipinfo.io/missingauth"
}root@kali:~#
```

```
root@kali:~#  curl https://ipinfo.io/104.47.125.36
{
  "ip": "104.47.125.36",
  "hostname": "mail-sg2apc010036.inbound.protection.outlook.com",
  "city": "Singapore",
  "region": "Singapore",
  "country": "SG",
  "loc": "1.2897,103.8501",
  "org": "AS8075 Microsoft Corporation",
  "postal": "048508",
  "timezone": "Asia/Singapore",
  "readme": "https://ipinfo.io/missingauth"
root@kali:~#
```

3) Port scanning of 203.163.246.23

- For port scanning I'm using **Nmap.**

1) **First, try to scan normally**

```
Shell No.1
File  Actions  Edit  View  Help
root@kali:~# nmap 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-25 02:25 EDT
Nmap scan report for 203.163.246.23
Host is up (0.0034s latency).
All 1000 scanned ports on 203.163.246.23 are filtered

Nmap done: 1 IP address (1 host up) scanned in 60.38 seconds
root@kali:~#
```

Here it shows us that 'host is up' and all 1000 ports are filtered but they're not listed which means firewall is activated and it blocks our requests.

So now, we've to apply different method.

2) **At this time we'll use SYN mode (stealth mode) and verbose mode:**
   `nmap -sS -vv 20 203.163.246.23`

```
Shell No.1
File  Actions  Edit  View  Help
root@kali:~# nmap -sS -vv 20 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-25 02:35 EDT
Initiating Ping Scan at 02:35
Scanning 2 hosts [4 ports/host]
Completed Ping Scan at 02:35, 1.25s elapsed (2 total hosts)
Initiating Parallel DNS resolution of 2 hosts. at 02:35
Completed Parallel DNS resolution of 2 hosts. at 02:35, 0.09s elapsed
Nmap scan report for 20 (0.0.0.20) [host down, received no-response]
Initiating SYN Stealth Scan at 02:35
Scanning 203.163.246.23 [1000 ports]
Completed SYN Stealth Scan at 02:35, 4.98s elapsed (1000 total ports)
Nmap scan report for 203.163.246.23
Host is up, received reset ttl 128 (0.00037s latency).
All 1000 scanned ports on 203.163.246.23 are filtered because of 1000 no-

Read data files from: /usr/bin/../share/nmap
Nmap done: 2 IP addresses (1 host up) scanned in 6.44 seconds
           Raw packets sent: 2015 (88.576KB) | Rcvd: 46 (1.872KB)
root@kali:~#
```

But in this case also the result is same, we didn't get the port list.

3) **So Now we're trying to scan top 20 ports**

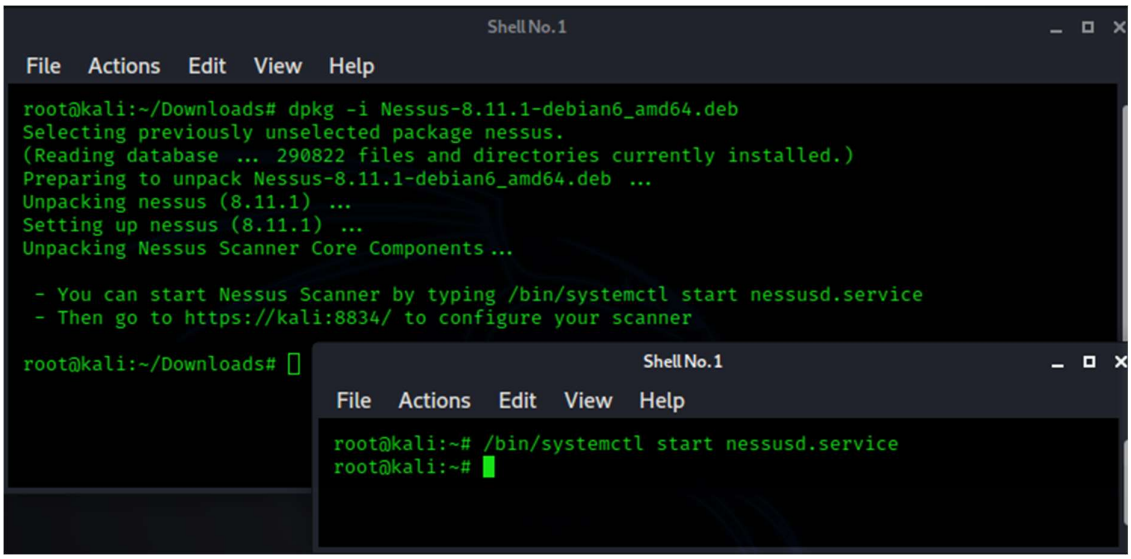
```
nmap -sS -vv --top-ports 20 20 203.163.246.23
```

```
Shell No.1
File  Actions  Edit  View  Help
root@kali:~# nmap -sS -vv --top-ports 20 20 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-25 02:43 EDT
Initiating Ping Scan at 02:43
Scanning 2 hosts [4 ports/host]
Completed Ping Scan at 02:43, 1.30s elapsed (2 total hosts)
Initiating Parallel DNS resolution of 2 hosts. at 02:43
Completed Parallel DNS resolution of 2 hosts. at 02:43, 0.08s elapsed
Nmap scan report for 20 (0.0.0.20) [host down, received no-response]
Initiating SYN Stealth Scan at 02:43
Scanning 203.163.246.23 [20 ports]
Completed SYN Stealth Scan at 02:43, 1.58s elapsed (20 total ports)
Nmap scan report for 203.163.246.23
Host is up, received reset ttl 128 (0.00045s latency).
Scanned at 2020-08-25 02:43:14 EDT for 3s

PORT     STATE    SERVICE       REASON
21/tcp   filtered ftp           no-response
22/tcp   filtered ssh           no-response
23/tcp   filtered telnet        no-response
25/tcp   filtered smtp          no-response
53/tcp   filtered domain        no-response
80/tcp   filtered http          no-response
110/tcp  filtered pop3          no-response
111/tcp  filtered rpcbind       no-response
135/tcp  filtered msrpc         no-response
139/tcp  filtered netbios-ssn   no-response
143/tcp  filtered imap          no-response
443/tcp  filtered https         no-response
445/tcp  filtered microsoft-ds  no-response
993/tcp  filtered imaps         no-response
995/tcp  filtered pop3s         no-response
1723/tcp filtered pptp          no-response
3306/tcp filtered mysql         no-response
3389/tcp filtered ms-wbt-server no-response
5900/tcp filtered vnc           no-response
8080/tcp filtered http-proxy    no-response

Read data files from: /usr/bin/../share/nmap
Nmap done: 2 IP addresses (1 host up) scanned in 3.19 seconds
           Raw packets sent: 53 (2.256KB) | Rcvd: 4 (192B)
root@kali:~#
```

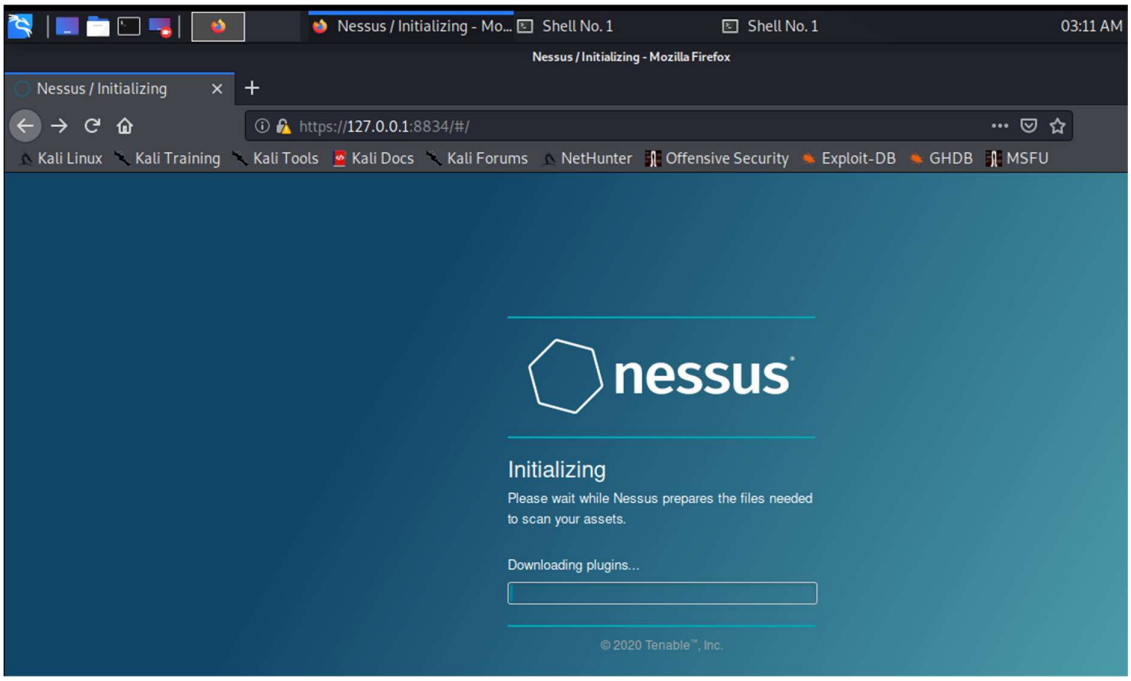
And, finally we got the port list. But due to firewall, all ports are filtered.

4) Installing Nessus in a VM and scan your laptop/desktop for CVE.

- **Installing Nessus on my kali machine:**



- **And then configuring it:**



- **Now I'm going to find my pc's IP for the scanning purpose**

```
C:\WINDOWS\system32\cmd.exe
   Link-local IPv6 Address . . . . . : fe80::e534:3417:c780:4a7c%14
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::144b:9d11:ad02:251%8
   IPv4 Address. . . . . . . . . . . : 192.168.1.13
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

- **Now scanning the IP which we got on Nessus: 192.168.1.13**

my pc

‹ Back to My Scans

Hosts 1 | Vulnerabilities 25 | History 1

Filter | Search Hosts | 1 Host

Host	Vulnerabilities	%
192.168.1.13	5 / 58	99%

Scan Details

Policy:	Basic Network Scan
Status:	Running
Scanner:	Local Scanner
Start:	Today at 4:32 AM

- **And finally, we got the CVE**

Output

```
Detected Treck TCP\IP network stack.
```

Port	Hosts
N/A	192.168.1.13

CVSS Base Score: 10.0

CVSS Temporal Score: 7.4

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Vulnerability Information

Exploit Ease: No known exploits are available

Patch Pub Date: June 17, 2020

Vulnerability Pub Date: June 17, 2020

Reference Information

CVE: CVE-2020-11896, CVE-2020-11897, CVE-2020-11898, CVE-2020-11899, CVE-2020-11900, CVE-2020-11901, CVE-2020-11902, CVE-2020-11903, CVE-2020-11904, CVE-2020-11905, CVE-2020-11906, CVE-2020-11907, CVE-2020-11908, CVE-2020-11909, CVE-2020-11910, CVE-2020-11911, CVE-2020-11912, CVE-2020-11913, CVE-2020-11914