

Assignment | Day 4 | Cybersecurity | LetsUpgrade

Name: Prashnik Das

Registered Email: prashnik20@gmail.com

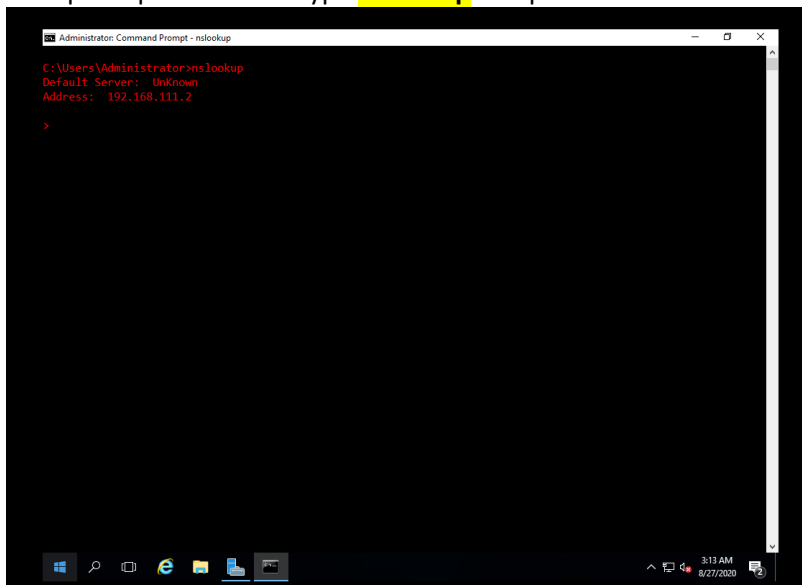
Q 1. Find out the mail servers of the following domain:

- a) **ibm.com**
- b) **Wipro.com**

Answer: *I am using the Windows Command Prompt in Pentester-Win-2016 virtual machine for solving this question*

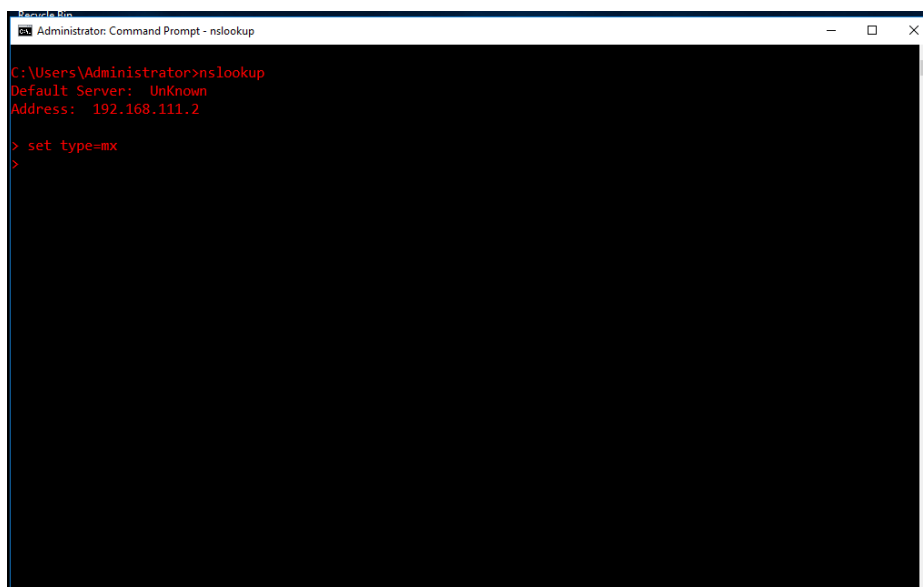
a) ibm.com

Step 1: Open cmd and type **nslookup** and press enter



```
Administrator: Command Prompt - nslookup
C:\Users\Administrator>nslookup
Default Server:  Unknown
Address:  192.168.111.2
>
```

Step 2: Now type **set type=mx** and press enter



```
Administrator: Command Prompt - nslookup
C:\Users\Administrator>nslookup
Default Server:  Unknown
Address:  192.168.111.2
> set type=mx
>
```

Step 3: Now type the web address whose mail server we want (in this case it is **www.ibm.com**)

```
Administrator: Command Prompt - nslookup

C:\Users\Administrator>nslookup
Default Server:  UnKnown
Address:  192.168.111.2

> set type=mx
> www.ibm.com
Server:  UnKnown
Address:  192.168.111.2

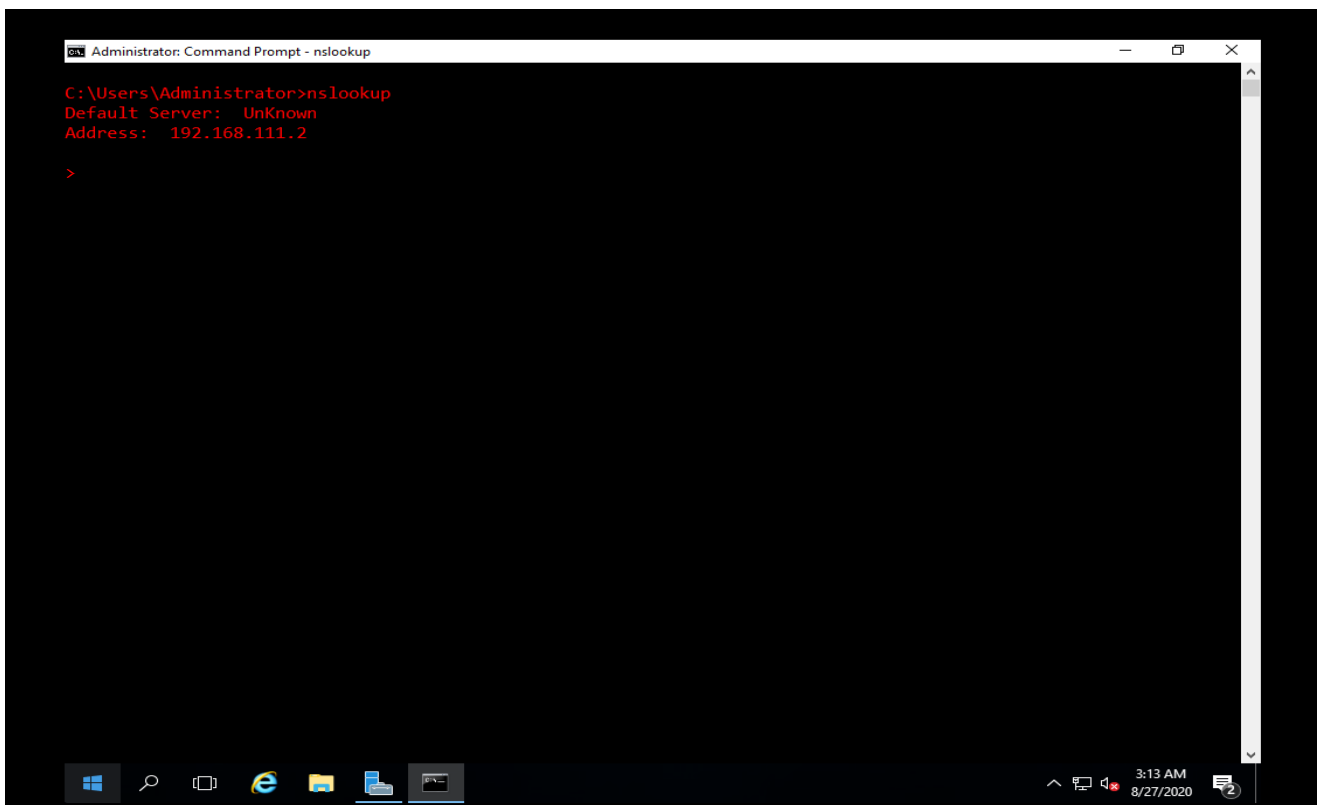
Non-authoritative answer:
www.ibm.com      canonical name = www.ibm.com.cs186.net
www.ibm.com.cs186.net canonical name = outer-ccdn-dual.ibmcom.edgekey.net
outer-ccdn-dual.ibmcom.edgekey.net canonical name = outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net
outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net canonical name = e2874.dscx.akamaiedge.net
dscx.akamaiedge.net
    primary name server = n0dscx.akamaiedge.net
    responsible mail addr = hostmaster.akamai.com
    serial = 1598523620
    refresh = 1000 (16 mins 40 secs)
    retry = 1000 (16 mins 40 secs)
    expire = 1000 (16 mins 40 secs)
    default TTL = 1800 (30 mins)
>
```

By this process we get the required mail server.

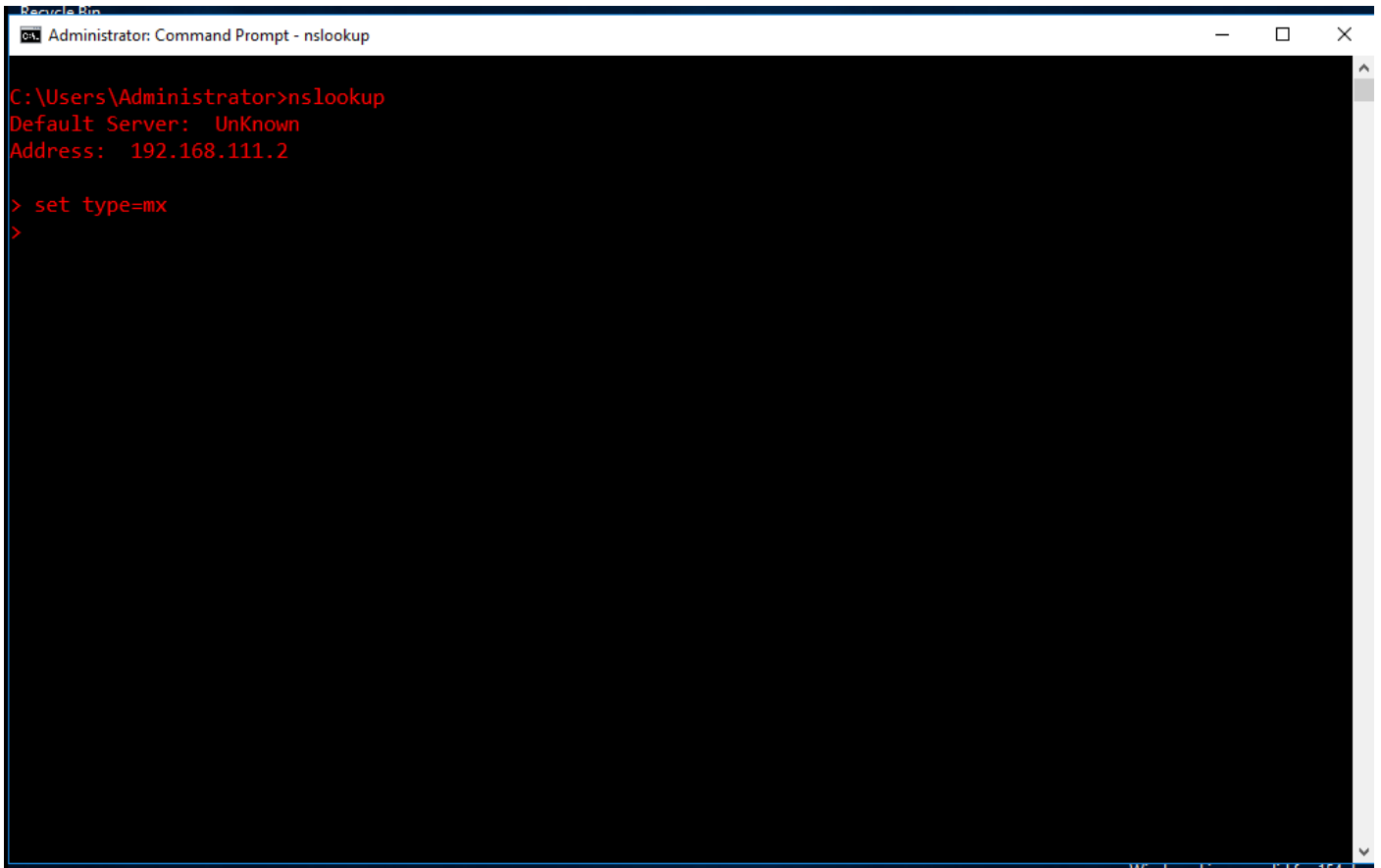
In this case the mail server is **hostmaster.akamai.com**

b) wipro.com

Step 1: Open cmd and type **nslookup** and press enter



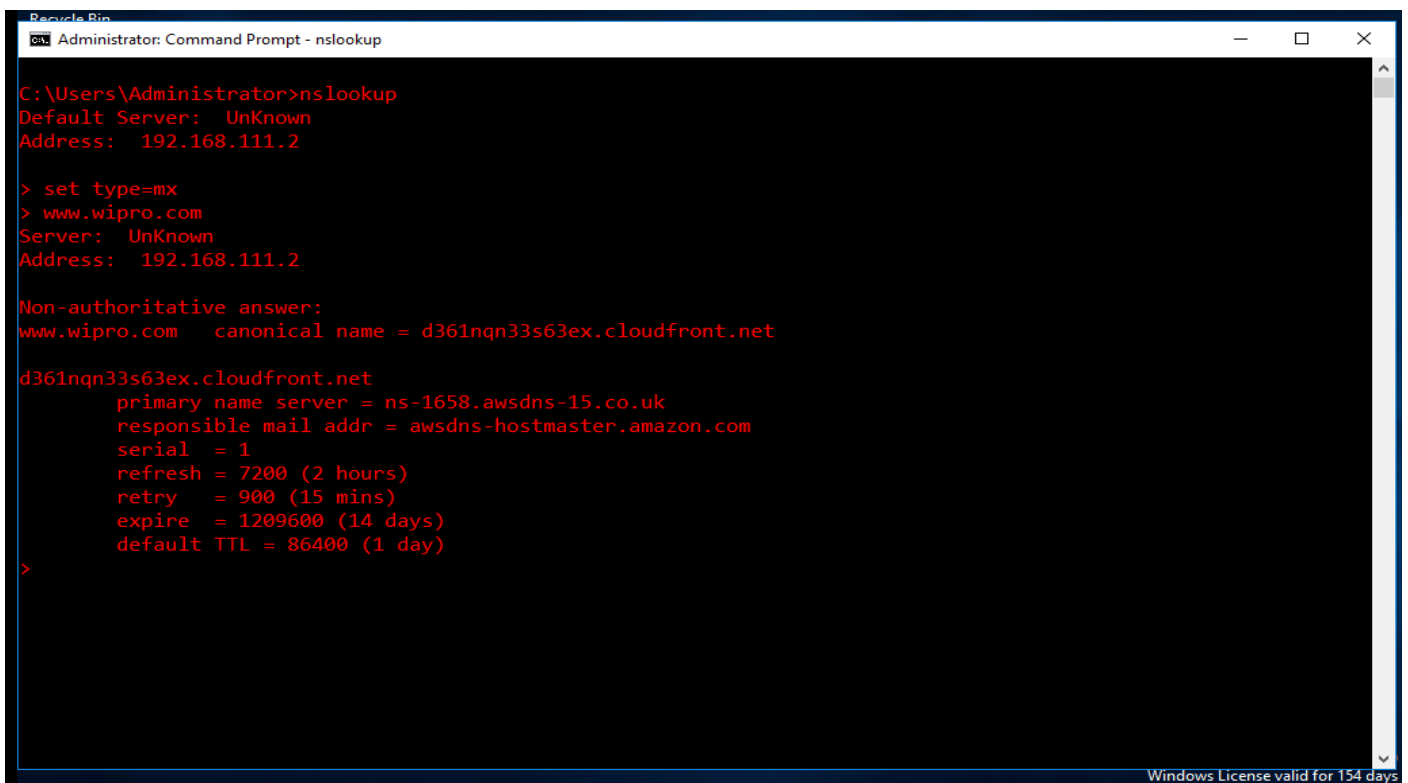
Step 2: Now type **set type=mx** and press enter



```
Administrator: Command Prompt - nslookup
C:\Users\Administrator>nslookup
Default Server: UnKnown
Address: 192.168.111.2

> set type=mx
>
```

Step 3: Now type the web address whose mail server we want. (In this case it is www.wipro.com)



```
Administrator: Command Prompt - nslookup
C:\Users\Administrator>nslookup
Default Server: UnKnown
Address: 192.168.111.2

> set type=mx
> www.wipro.com
Server: UnKnown
Address: 192.168.111.2

Non-authoritative answer:
www.wipro.com canonical name = d361nqn33s63ex.cloudfront.net

d361nqn33s63ex.cloudfront.net
    primary name server = ns-1658.awsdns-15.co.uk
    responsible mail addr = awsdns-hostmaster.amazon.com
    serial = 1
    refresh = 7200 (2 hours)
    retry = 900 (15 mins)
    expire = 1209600 (14 days)
    default TTL = 86400 (1 day)
>
```

By this process we get the required mail server.

In this case the mail server is **awsdns-hostmaster.amazon.com**

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

Answer: continuation of Q1.

a) *ibm.com*

Step 1: Open CMD >type and enter **nslookup> set type=mx> ibm.com**

```
Administrator: Command Prompt

outer-ccdn-dual.ibmcom.edgekey.net
outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net

> set type=mx
> ibm.com
Server: UnKnown
Address: 192.168.111.2

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

ibm.com nameserver = asia3.akam.net
ibm.com nameserver = ns1-99.akam.net
ibm.com nameserver = usw2.akam.net
ibm.com nameserver = eur2.akam.net
ibm.com nameserver = ns1-206.akam.net
ibm.com nameserver = eur5.akam.net
ibm.com nameserver = usc3.akam.net
ibm.com nameserver = usc2.akam.net
mx0b-001b2d01.pphosted.com internet address = 148.163.158.5
mx0a-001b2d01.pphosted.com internet address = 148.163.156.1
asia3.akam.net internet address = 23.211.61.64
```

Step 2: Open a browser and go to <https://tools.keycdn.com/geo?host=mx0a-001b2d01.pphosted.com> or any other IP location finder. Enter the IP address/hostname to get the results.

Address 1: mx0b-001b2d01.pphosted.com

IP address or hostname

Find

LOCATION

| | |
|-------------|---------------------------------------|
| Country | United States (US) |
| Continent | North America (NA) |
| Coordinates | 37.751 (lat) / -97.822 (long) |
| Time | 2020-08-27 06:50:37 (America/Chicago) |

NETWORK

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

Address 2: mx0a-001b2d01.pphosted.com

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 | 2020-08-27 06:54:04 (America/Chicago) |

NETWORK

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

b) wipro.com

Step 1: Open CMD >type and enter **nslookup> set type=mx> wipro.com**

```
Administrator: Command Prompt - nslookup
Server: UnKnown
Address: 192.168.111.2

Non-authoritative answer:
Name: wipro.com
Address: 209.11.159.61

>
> set type=mx
> wipro.com
Server: UnKnown
Address: 192.168.111.2

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

wipro.com      nameserver = ns1.webindia.com
wipro.com      nameserver = ns2.webindia.com
wipro.com      nameserver = ns3.webindia.com
ns1.webindia.com internet address = 50.16.170.116
>
```

Step 2: Open a browser and go to <https://tools.keycdn.com/geo?host=mx0a-001b2d01.pphosted.com> or any other IP location finder. Enter the IP address/hostname to get the results.

Address: wipro-com.mail.protection.outlook.com

IP address or hostname

wipro-com.mail.protection.outlook.com

Find

LOCATION

| | |
|-------------|--------------------------------------|
| City | Singapore |
| Postal code | 18 |
| Country | Singapore (SG) |
| Continent | Asia (AS) |
| Coordinates | 1.2929 (lat) / 103.8547 (long) |
| Time | 2020-08-27 20:12:49 (Asia/Singapore) |

NETWORK

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

Q 3. Scan and find out port numbers open 203.163.246.23

Answer: I will be using Kali Linux 2020.3 in VMware.

Step 1: Open the terminal and go to administrator mode

Command: `sudo su -`

(enter password and hit enter to enter administrator mode)

Step 2: In order to detect the open ports type `nmap 203.163.246.23` and hit enter.

```
root@kali:~# nmap 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 12:12 EDT
Nmap scan report for 203.163.246.23
Host is up (0.061s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
110/tcp   open  pop3

Nmap done: 1 IP address (1 host up) scanned in 55.26 seconds
```

Therefore, one port is open as shown in the screenshot.

(Performing more scans) **nmap -v -A 203.163.246.23**

```
kali@kali: ~  
File Actions Edit View Help  
Completed Ping Scan at 12:14, 0.00s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 12:14  
Completed Parallel DNS resolution of 1 host. at 12:14, 0.07s elapsed  
Initiating SYN Stealth Scan at 12:14  
Scanning 203.163.246.23 [1000 ports]  
Discovered open port 110/tcp on 203.163.246.23  
Increasing send delay for 203.163.246.23 from 0 to 5 due to 11 out of 13 dropped probes since last inc  
rease.  
Increasing send delay for 203.163.246.23 from 5 to 10 due to 11 out of 11 dropped probes since last in  
crease.  
Completed SYN Stealth Scan at 12:15, 52.22s elapsed (1000 total ports)  
Initiating Service scan at 12:15  
Scanning 1 service on 203.163.246.23  
Stats: 0:02:54 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan  
Service scan Timing: About 0.00% done  
Completed Service scan at 12:18, 156.36s elapsed (1 service on 1 host)  
Initiating OS detection (try #1) against 203.163.246.23  
Initiating Traceroute at 12:18  
Completed Traceroute at 12:18, 0.03s elapsed  
Initiating Parallel DNS resolution of 2 hosts. at 12:18  
Completed Parallel DNS resolution of 2 hosts. at 12:18, 2.02s elapsed  
NSE: Script scanning 203.163.246.23.  
Initiating NSE at 12:18  
Completed NSE at 12:18, 21.22s elapsed  
Initiating NSE at 12:18  
Completed NSE at 12:19, 21.05s elapsed  
Initiating NSE at 12:19  
Completed NSE at 12:19, 0.00s elapsed  
Nmap scan report for 203.163.246.23  
Host is up (0.0024s latency).  
Not shown: 999 filtered ports  
PORT      STATE SERVICE VERSION
```

```
kali@kali: ~  
File Actions Edit View Help  
Not shown: 999 filtered ports  
PORT      STATE SERVICE VERSION  
110/tcp   open  pop3?  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: WAP|general purpose  
Running: Actiontec embedded, Linux 2.4.X|3.X, Microsoft Windows XP|7|2012  
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:2.4.37 cpe:  
/o:linux:linux_kernel:3.2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft  
:windows_server_2012  
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Microsoft Windows X  
P SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012  
Network Distance: 2 hops  
TCP Sequence Prediction: Difficulty=256 (Good luck!)  
IP ID Sequence Generation: Incremental  
  
TRACEROUTE (using port 80/tcp)  
HOP RTT      ADDRESS  
1   0.14 ms  192.168.111.2  
2   0.05 ms  203.163.246.23  
  
NSE: Script Post-scanning.  
Initiating NSE at 12:19  
Completed NSE at 12:19, 0.00s elapsed  
Initiating NSE at 12:19  
Completed NSE at 12:19, 0.00s elapsed  
Initiating NSE at 12:19  
Completed NSE at 12:19, 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 255.26 seconds  
Raw packets sent: 2086 (93.988KB) | Rcvd: 499 (20.024KB)  
root@kali:~#
```

```
kali@kali: ~  
File Actions Edit View Help  
110/tcp   open  pop3  
  
Nmap done: 1 IP address (1 host up) scanned in 55.26 seconds  
root@kali:~# nmap -v -A 203.163.246.23  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 12:14 EDT  
NSE: Loaded 151 scripts for scanning.  
NSE: Script Pre-scanning.  
Initiating NSE at 12:14  
Completed NSE at 12:14, 0.00s elapsed  
Initiating NSE at 12:14  
Completed NSE at 12:14, 0.00s elapsed  
Initiating NSE at 12:14  
Completed NSE at 12:14, 0.00s elapsed  
Initiating Ping Scan at 12:14  
Scanning 203.163.246.23 [4 ports]  
Completed Ping Scan at 12:14, 0.00s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 12:14  
Completed Parallel DNS resolution of 1 host. at 12:14, 0.07s elapsed  
Initiating SYN Stealth Scan at 12:14  
Scanning 203.163.246.23 [1000 ports]  
Discovered open port 110/tcp on 203.163.246.23  
Increasing send delay for 203.163.246.23 from 0 to 5 due to 11 out of 13 dropped probes since last inc  
rease.
```

Command: **Nmap -Pn -sS 203.163.246.23**

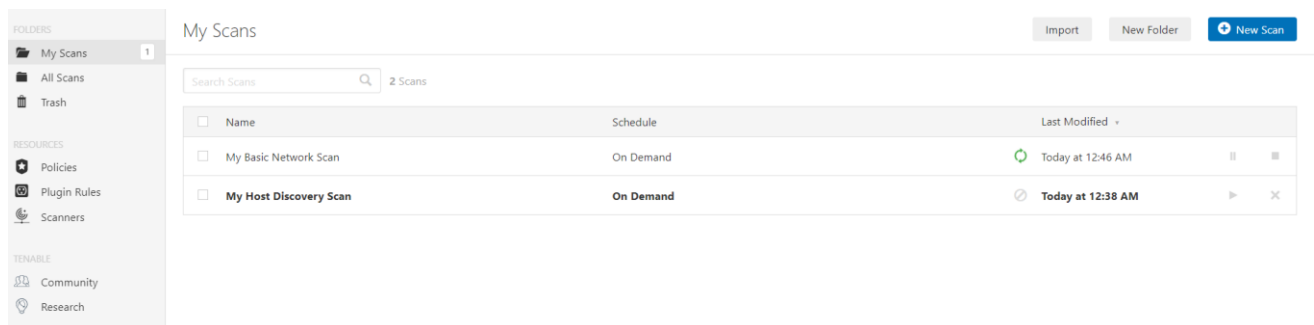
```
kali@kali:~$ sudo su -
[sudo] password for kali:
root@kali:~# nmap -Pn -sS 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 11:44 EDT
Stats: 0:01:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 69.70% done; ETC: 11:46 (0:00:41 remaining)
Stats: 0:02:57 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 81.30% done; ETC: 11:48 (0:00:41 remaining)
Stats: 0:03:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 81.65% done; ETC: 11:48 (0:00:41 remaining)
Stats: 0:03:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.00% done; ETC: 11:49 (0:00:41 remaining)
Stats: 0:04:47 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 87.55% done; ETC: 11:50 (0:00:41 remaining)
Stats: 0:07:57 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.10% done; ETC: 11:52 (0:00:19 remaining)
Nmap scan report for 203.163.246.23
Host is up (0.0046s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
25/tcp    closed smtp
110/tcp   open  pop3

Nmap done: 1 IP address (1 host up) scanned in 564.59 seconds
root@kali:~#
root@kali:~#
```

Q 4. Install Nessus in a VM and scan your laptop/desktop for CVE

Answer:

- Step 1: Open Pentester-Win 2016 VM and install Nessus in it and open it in a suitable browser.
- Step 2: Enter the Ipv4 address of your machine in the popup box and start Scanning.
- Step 3: The scan is now running. Wait for few seconds until the scan is over.



Step 4: Once the Scan is over, we can see the reports. (Click the Vulnerabilities tab to view the reports)

