Lets Upgrade| Cyber security

Assignment Day4| 28 August 2020

Name :Abdul nafih.k

Registered email:abdulnafih160@gmail.com

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

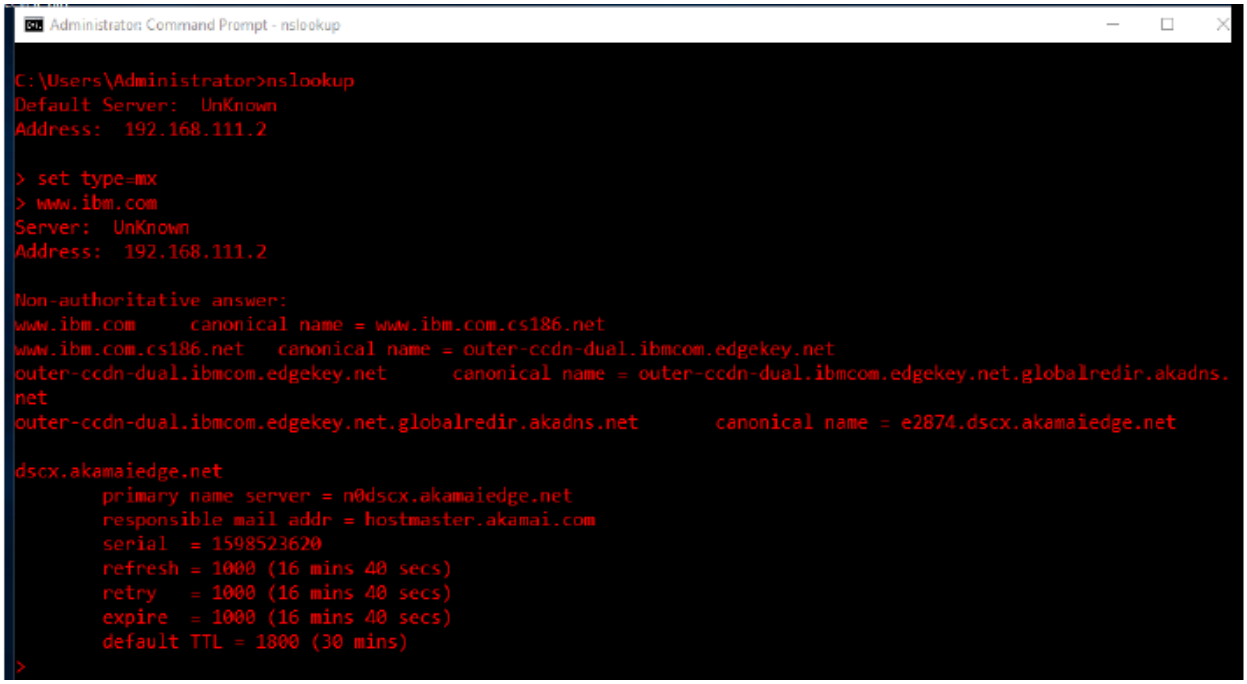
a)Ibm.com

Steps:

1:-open cmd using search cmd in windows search box

2:-Type nslookup open the nslookup tool

3:-Type command set type=mx ,then >(type targets id eg;www.Ibm.com)



b)Wipro.com

Steps:

1:-open cmd using search cmd in windows search box

2:-Type nslookup open the nslookup tool

3:-Type command set type=mx ,then >(type targets id eg;www.wipro.com)

```
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 = d36inqn33s63ex.cloudfront.net

d36inqn33s63ex.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)
>
```

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

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
```

Step2: Open a browser and go to https://tools.keycdn.com/geo?host=mx0a-001b2d01.pphosted.com

Address 1: mx0b-001b2d01.pphosted.com

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	2020-08-27 06:50:37 (America/Chicago)
NETWORK	
IP address	148.163.158.5
Hostname	mx0b-001b2d01.pphosted.com
Provider	PROOFPOINT-ASN-US-EAST
ASN	22843

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.

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

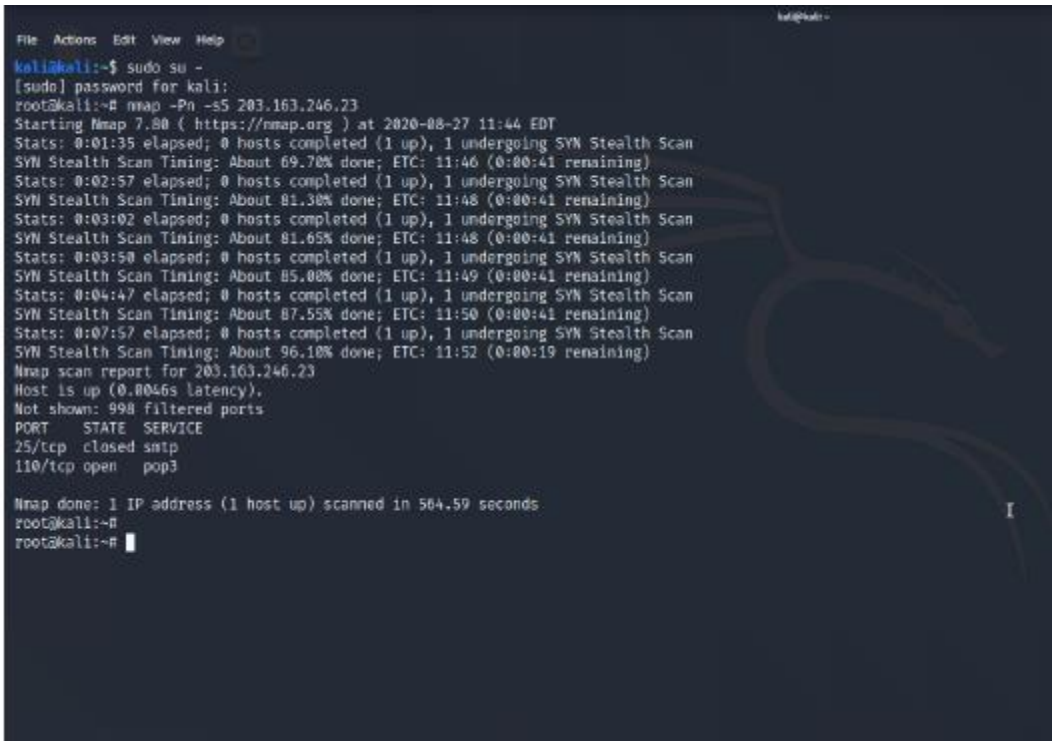
3.Scan and find out port numbers open 203.163.246.23

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
```

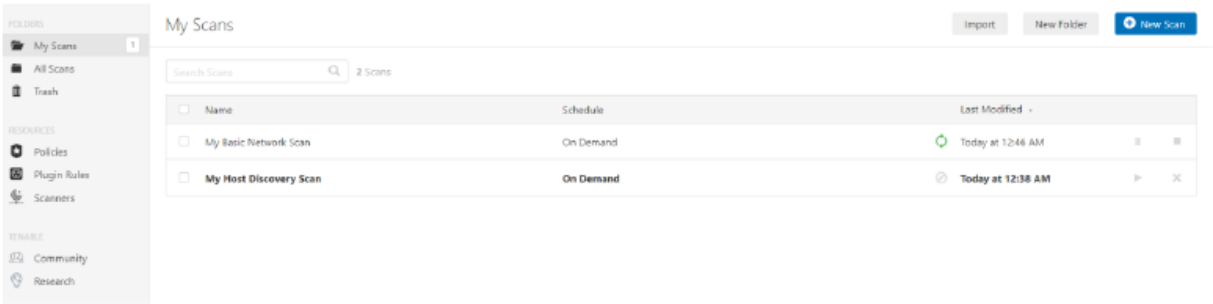


```
File  Actions  Edit  View  Help
kali@kali:~$ sudo su -
[sudo] password for kali:
root@kali:~# nmap -Pn -sS 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 11:44 EDT
Stats: 0:01:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 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:~#
```

4.Install Nessus in a vm and scan your laptop/Desktop for CVE

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)