

Cyber Security Essential

Submitted by- Ritik Dewan

Email id-

hritik22dewan@gmail.com

Assignment Day-4

Question 1: Find out the mail servers of the following domain

: Ibm.com

: Wipro.com

Answers

1.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

```

2. 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

```

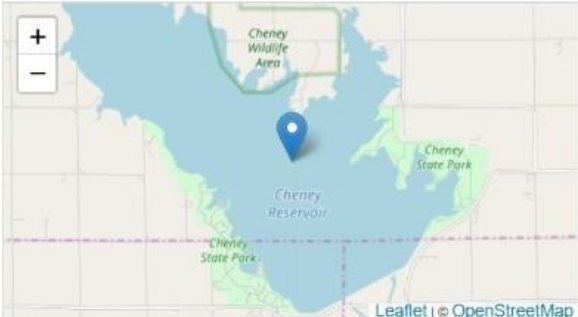
Question 2: Find the locations, where these email servers are hosted.

Answers

1. Ibm.com

129.42.38.10 FIND

IP Address	129.42.38.10 CHANGE
Latitude	37.751
Longitude	-97.822
Country	United States
Region	
City	
Organization	Events Infrastructure



Map showing the location of the IP address 129.42.38.10, which is located near Cheney Reservoir, Cheney Wildlife Area, and Cheney State Park.

2. Wipro.com

keycdn Tools Features Solutions ▾ Network Pricing Q Support

Web **IP Location Finder** LOOKUP IP ADDRESS OR HOSTNAME

Network

- IP Location Finder**
- DNS Checker
- Ping Test
- Ping IPv6 Test
- Traceroute Test
- BGP Looking Glass

Security

Other

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 13:04:43 (Asia/Singapore)
NETWORK	
IP address	104.47.125.36
Hostname	mail-sg2apc010036.inbound.protection.outlook.com
Provider	MICROSOFT-CORP-MSN-AS-BLOCK
ASN	8075

Question 3: Scan and find out
port numbers open
203.163.246.23

Answers

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:~#
```

As it is coming filtered due to firewall protection we try some other ways of breaking the firewall

Enter: **-sS -v -v -Pn**
203.163.246.23

For me it is still coming filtered so I'll further use the following command

Enter: `nmap -6 203.163.246.23`

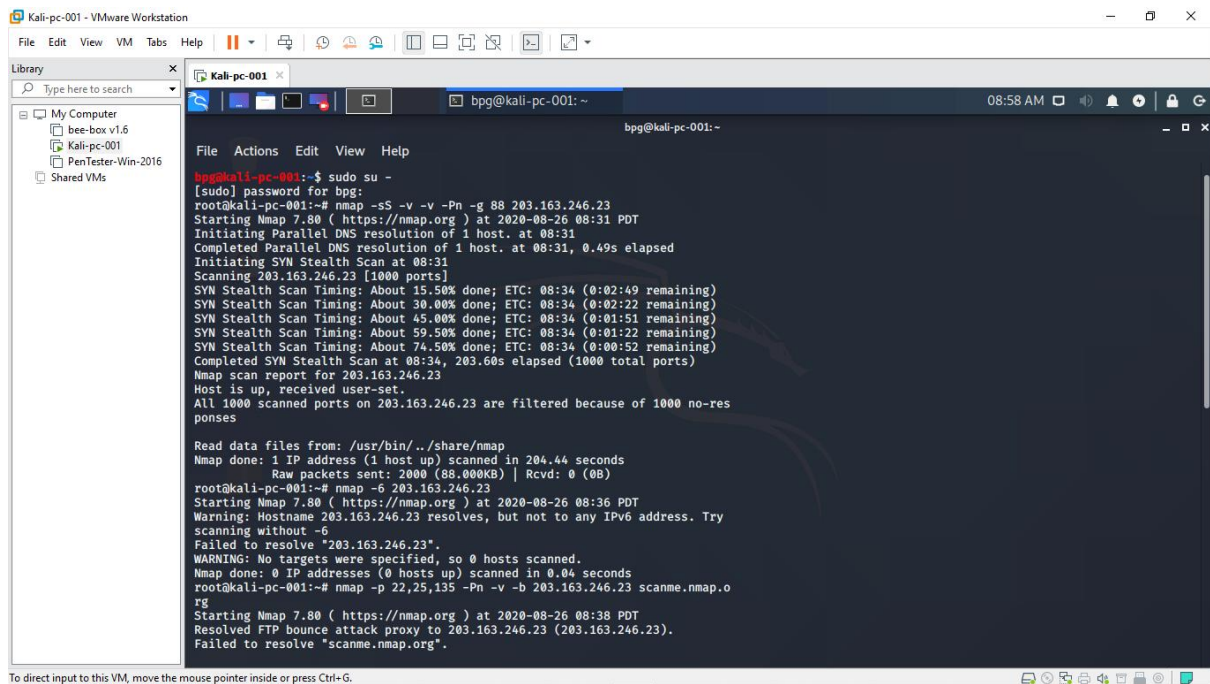
Again it is coming filtered for me so I'll further use the following command

Enter: `nmap -p 22,25,135 -Pn -v -b 203.163.246.23 scanme.nmap.org`

Again it is coming filtered for me so I'll further use the following command

Enter: `nmap -vv -n -sS -Pn --ip-options "L 203.163.246.23 " --reason 203.163.246.23`

Now I get only on



```
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".
```

e port open a

The screenshot shows a Kali Linux terminal window within a VMware Workstation. The terminal displays the output of two Nmap scans. The first scan is a basic scan with the command `root@kali-pc-001:~# nmap -p 22,25,135 -Pn -v -b 203.163.246.23 scanme.nmap.org`. The second scan is a SYN Stealth Scan with the command `root@kali-pc-001:~# nmap -vv -n -sS -Pn --ip-options "L 203.163.246.23" --reason 203.163.246.23`. The output of the second scan indicates that only one port, 514/tcp, is open, while all other 999 ports are closed due to resets.

```
File Actions Edit View Help
bpg@kali-pc-001: ~
bpg@kali-pc-001:~
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".
Read data files from: /usr/bin/./share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.05 seconds
root@kali-pc-001:~# nmap -vv -n -sS -Pn --ip-options "L 203.163.246.23" --reason 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 08:41 PDT
Initiating SYN Stealth Scan at 08:41
Scanning 203.163.246.23 [1000 ports]
Completed SYN Stealth Scan at 08:41, 1.35s elapsed (1000 total ports)
Nmap scan report for 203.163.246.23
Host is up, received user-set (0.0029s latency).
Scanned at 2020-08-26 08:41:11 PDT for 2s
Not shown: 999 closed ports
Reason: 999 resets
PORT      STATE SERVICE REASON
514/tcp   filtered shell no-response

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
Raw packets sent: 1001 (56.056KB) | Rcvd: 999 (39.960KB)
root@kali-pc-001:~#
```

s shown below

So out of the 1000 ports in the given ip address I get only 1 port open which is 514/tcp

Hence I conclude that only one port is open from the scanned port

Question4: Install Nessus in a VM and scan your laptop/desktop for CVE

Answer

Steps to Download

Steps1-open our browser

Steps2-now search for Nessus

Step3-click on download & wait for the download complete

Step4-after completion of download now open Nessus

& start scanning your desktop/laptop

