Cyber Security Essentials | Batch 1 | Day 4 | LetsUpgrade – Assignment

By Sirajudeen Mahaboob Basha

Date: 28-08-2020

Email ID – siraj110981@gmail.com

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

Ibm.com Wipro.com

Answers:

Mail Server information of Ibm.com

```
C:\Users\siraj>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  192.168.1.1

> set type=mx
> ibm.com
Server:  UnKnown
Address:  192.168.1.1

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 Server Information of wipro.com

```
C:\Users\siraj>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  192.168.1.1

> set type=mx
> wipro.com
Server:  UnKnown
Address:  192.168.1.1

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

wipro.com       nameserver = ns2.webindia.com
wipro.com       nameserver = ns4.webindia.com
wipro.com       nameserver = ns1.webindia.com
>
```

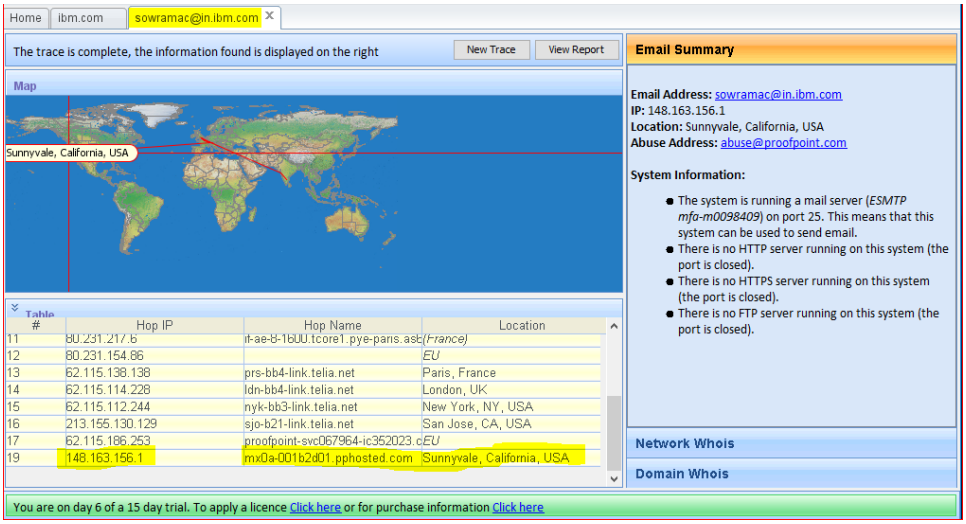
Question 2:

Find the locations, where these email servers are hosted.

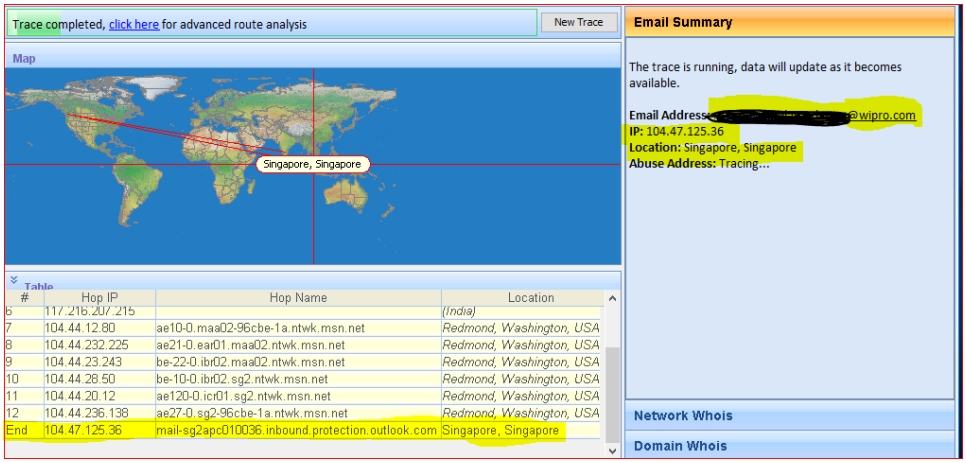
Ibm.com

ibm.com MX preference = 5, mail exchanger = mx0b-001b2d01.pphosted.com - 148.163.158.5

ibm.com MX preference = 5, mail exchanger = mx0a-001b2d01.pphosted.com - 148.163.156.1



Wipro.com



Question 3:

Scan and find out port numbers open 203.163.246.23.

No Open ports found while scanning this given IP address.

```
root@kali:~# nmap -v -A 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 08:33 EDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:33
Completed NSE at 08:33, 0.00s elapsed
Initiating NSE at 08:33
Completed NSE at 08:33, 0.00s elapsed
Initiating NSE at 08:33
Completed NSE at 08:33, 0.00s elapsed
Initiating Ping Scan at 08:33
Scanning 203.163.246.23 [4 ports]
Completed Ping Scan at 08:33, 1.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:33
Completed Parallel DNS resolution of 1 host. at 08:34, 13.00s elapsed
Initiating SYN Stealth Scan at 08:34
Scanning 203.163.246.23 [1000 ports]
SYN Stealth Scan Timing: About 26.00% done; ETC: 08:36 (0:01:34 remaining)
SYN Stealth Scan Timing: About 61.80% done; ETC: 08:35 (0:00:39 remaining)
adjust_timeouts2: packet supposedly had rtt of 40794949 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 40794949 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 40795153 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 40795153 microseconds.  Ignoring time.
```

```
Host is up (0.014s latency).
Not shown: 978 filtered ports
PORT      STATE  SERVICE         VERSION
417/tcp   closed onmux
903/tcp   closed iss-console-mgr
1043/tcp  closed boinc
1097/tcp  closed sunclustermgr
1098/tcp  closed rmiactivation
1102/tcp  closed adobeserver-1
1972/tcp  closed intersys-cache
2046/tcp  closed sdfunc
2099/tcp  closed h2250-annex-g
2910/tcp  closed tdaccess
3878/tcp  closed fotogcad
4004/tcp  closed pxc-roid
4567/tcp  closed tram
5500/tcp  closed hotline
5998/tcp  closed ncd-diag
6389/tcp  closed clariion-evr01
6788/tcp  closed smc-http
8081/tcp  closed blackice-icecap
9200/tcp  closed wap-wsp
9666/tcp  closed zoomcp
32771/tcp closed sometimes-rpc5
50000/tcp closed ibm-db2
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clos
ed port
```

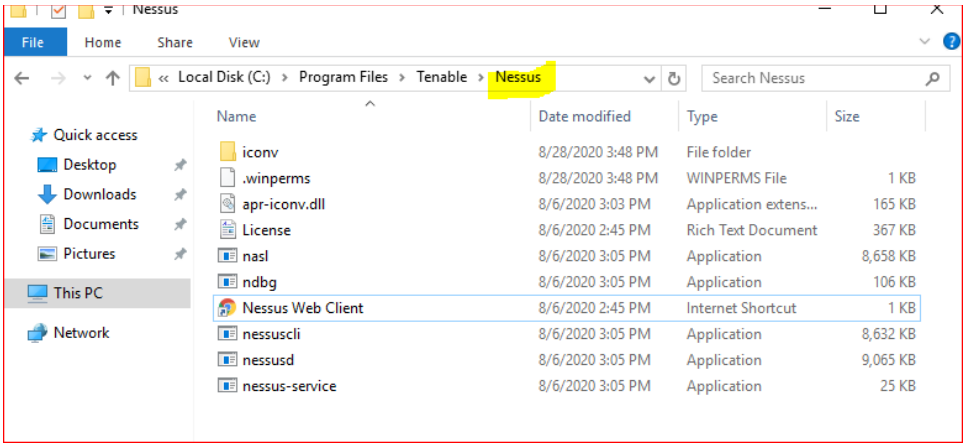
Another command used –open (to just scan open ports)

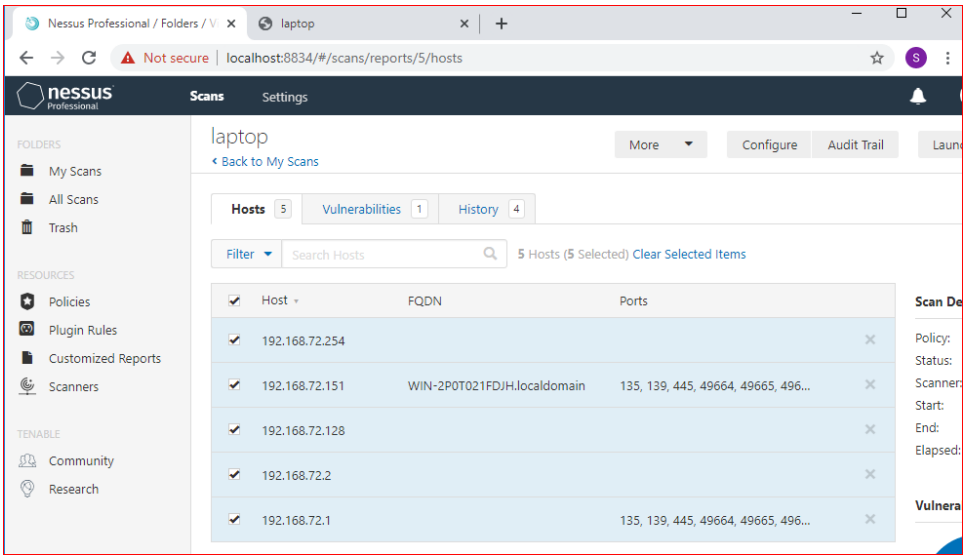
```
root@kali:~# nmap -v -A --open 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 08:46 EDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:46
Completed NSE at 08:46, 0.00s elapsed
Initiating NSE at 08:46
Completed NSE at 08:46, 0.00s elapsed
Initiating NSE at 08:46
Completed NSE at 08:46, 0.00s elapsed
Initiating Ping Scan at 08:46
Scanning 203.163.246.23 [4 ports]
Completed Ping Scan at 08:46, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:46
Completed Parallel DNS resolution of 1 host. at 08:46, 0.34s elapsed
Initiating SYN Stealth Scan at 08:46
Scanning 203.163.246.23 [1000 ports]
Completed SYN Stealth Scan at 08:46, 4.23s elapsed (1000 total ports)
Initiating Service scan at 08:46
Initiating OS detection (try #1) against 203.163.246.23
Retrying OS detection (try #2) against 203.163.246.23
Initiating Traceroute at 08:46
Completed Traceroute at 08:47, 9.08s elapsed
NSE: Script scanning 203.163.246.23.
Initiating NSE at 08:47
Completed NSE at 08:47, 0.01s elapsed
Initiating NSE at 08:47
Completed NSE at 08:47, 0.00s elapsed
Initiating NSE at 08:47
Completed NSE at 08:47, 0.00s elapsed
NSE: Script Post-scanning.
Initiating NSE at 08:47
Completed NSE at 08:47, 0.00s elapsed
Initiating NSE at 08:47
Completed NSE at 08:47, 0.00s elapsed
Initiating NSE at 08:47
Completed NSE at 08:47, 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/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.28 seconds
           Raw packets sent: 2145 (98.544KB) | Rcvd: 4 (160B)
```

Question 4:

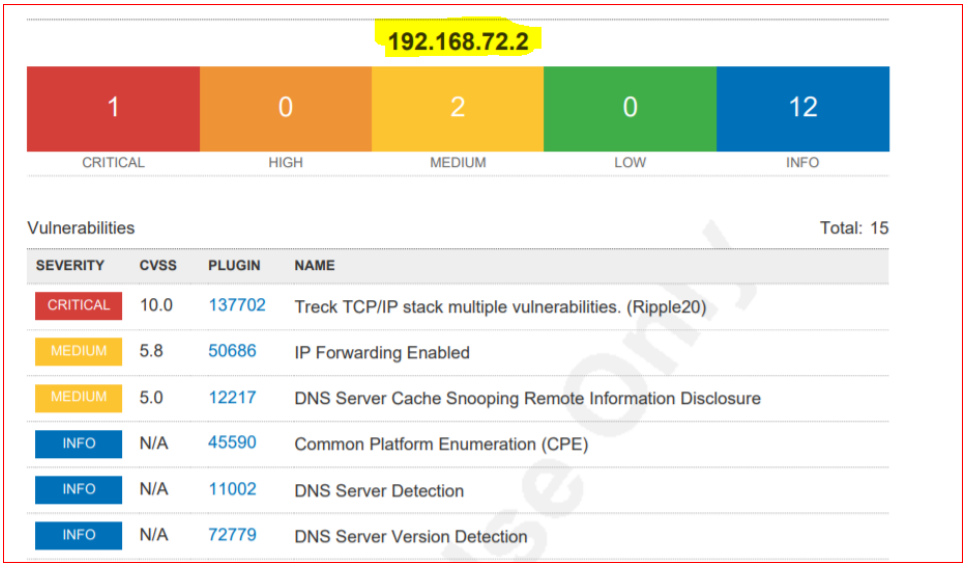
Install nessus in a VM and scan your laptop/desktop for CVE.

Nessus installation in a VM-





Scanned my VMware IP – 192.168.72.2 found below CVEs.



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