Let's Upgrade –
Cyber Security Essentials

Day 4 Assignment | Report | 23rd August 2020

Report 1:-

```
Non-authoritative answer:
Name:   ibm.com
Address: 129.42.38.10
> wipro.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   wipro.com
Address: 209.11.159.61
> set type=MX
> ibm.com
Server:         192.168.0.1
Address:        192.168.0.1#53

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

Authoritative answers can be found from:
> wipro.com
Server:         192.168.0.1
Address:        192.168.0.1#53

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

Authoritative answers can be found from:
>
```

✓ **Identified mail servers:-**

- IBM : *mx0a-001b2d01.pphosted.com*
  mx0b-001b2d01.pphosted.com
- Wipro : *wipro-com.mail.protection.outlook.com*

Report 2:-

- ✓ Trying to identify and locate the mail servers of targets.

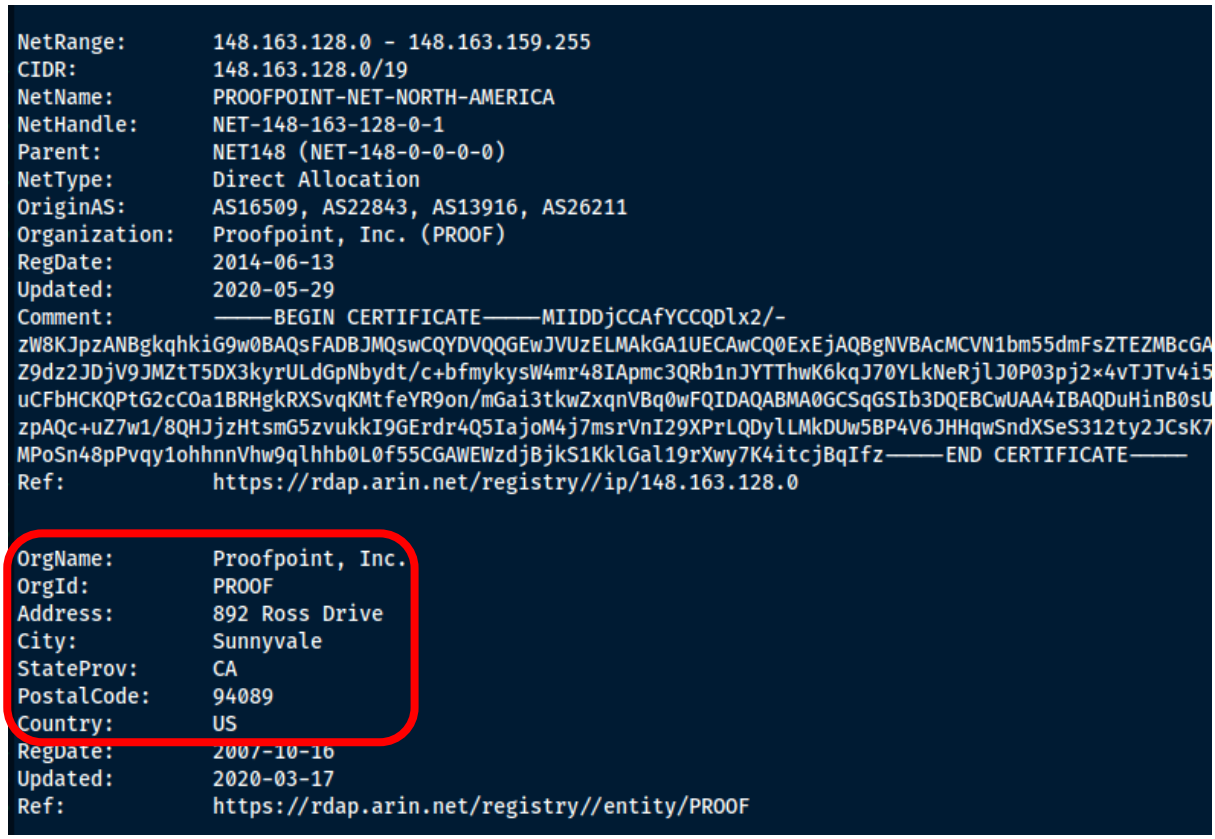
- ✓ ***Tools used:-***
  - **nslookup** => for retrieving the IP addresses of the target mail servers
  - **whois** => for obtaining details of the respective IPs obtained from previous step

- ✓ **Target - 1 [IBM]:-**

```
root@ghost:~# nslookup mx0b-001b2d01.pphosted.com
Server:         192.168.0.1
Address:        192.168.0.1#53

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

root@ghost:~# nslookup mx0a-001b2d01.pphosted.com
Server:         192.168.0.1
Address:        192.168.0.1#53

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

[continued…]

- ✓ Carrying out a **whois** lookup reveals the location of the server.
- ✓ The recon was done for both the discovered servers, the complete log of which can be found in the **"IBM_MailServ_1.txt"** and **"IBM_MailServ_1.txt"** files.



- ✓ Identified Mail Server locations :-
    - Sunnyvale, CA - USA
        - Both the servers have the same location.

- ✓ **<u>Target – 2 [Wipro]:-</u>**

- ✓ Using the same techniques as for IBM servers, the mail server details for Wipro are as given below:-
    - Provider = outlook.com
    - Location = Redmond, WA - USA
- ✓ The complete **whois** lookup for the Wipro mail servers can be found in **"Wipro_MailServ_1.txt"** & **"IBM_MailServ_2.txt"**

Report 3:-

- ✓ Target : 203.163.246.23
- ✓ **whois** lookup done - details can be found at **"IP_Lookup.txt"**
- ✓ Carrying out a **nmap** scan on the target host :

```
Nmap scan report for 203.163.246.23
Host is up, received user-set (0.0054s latency).
Scanned at 2020-08-24 00:30:40 MST for 19s
Not shown: 999 filtered ports
Reason: 999 no-responses
PORT   STATE SERVICE    REASON         VERSION
53/tcp open  tcpwrapped syn-ack ttl 63
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.16 - 4.6, Linux 3.2 - 4.9
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=8/24%OT=53%CT=%CU=%PV=N%DS=2%DC=T%G=N%TM=5F436CB3%P=x8
OS:6_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10B%TI=Z%TS=7)OPS(O1=M5B4ST11NW7%
OS:O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11
OS:)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%TG=40%
OS:W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%TG=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R
OS:=N)T3(R=N)T4(R=Y%DF=Y%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)U1(R=N)IE(R=N)

Uptime guess: 188.411 days (since Mon Feb 17 14:39:08 2020)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   3.58 ms 192.168.0.1
2   4.92 ms 203.163.246.23
```

- ✓ The Open port(s) discovered was:
  - Port 53

- ✓ Other (potential) details found:
  - Device running Linux 3.x | 4.x
  - Uptime guess 188 days

Report 4:-

Nessus advanced scan result for the target machine was done and no severe vulnerabilities were found.

- ✓ **Scan Results:-**

Scan Information

Start time:	Mon Aug 24 15:57:08 2020
End time:	Mon Aug 24 16:03:40 2020

Host Information

DNS Name:	Alpha-001
Netbios Name:	ALPHA-001
IP:	192.168.0.106
MAC Address:	C0:E4:34:E7:4E:7D
OS:	Windows

- ✓ **Medium Vulnerabilities detected :** Signing is not required on the remote SMB server.

- ✓ The full scan can be found at **"Target_Scan.html"**