

# CYBER SECURITY – ESSENTIALS

## ASSIGNMENT DAY-4

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

Ibm.com

Wipro.com

```
Applications ▾ Places ▾ Terminal ▾ Thu 00:49
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nslookup
> ibm.com
Server:      203.187.215.35
Address:     203.187.215.35#53

Non-authoritative answer:
Name:   ibm.com
Address: 129.42.38.10
> set type=MX
> ibm.com
Server:      203.187.215.35
Address:     203.187.215.35#53

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

Authoritative answers can be found from:
ibm.com nameserver = asia3.akam.net.
ibm.com nameserver = eur5.akam.net.
ibm.com nameserver = ns1-99.akam.net.
ibm.com nameserver = eur2.akam.net.
ibm.com nameserver = usc3.akam.net.
ibm.com nameserver = usw2.akam.net.
ibm.com nameserver = usc2.akam.net.
ibm.com nameserver = ns1-206.akam.net.
eur2.akam.net internet address = 95.100.173.64
eur5.akam.net internet address = 23.74.25.64
usc2.akam.net internet address = 184.26.160.64
usc3.akam.net internet address = 96.7.50.64
usw2.akam.net internet address = 184.26.161.64
asia3.akam.net internet address = 23.211.61.64
ns1-99.akam.net internet address = 193.108.91.99
ns1-99.akam.net has AAAA address 2600:1401:2::63
ns1-206.akam.net internet address = 193.108.91.206
```

```
Applications ▾ Places ▾ Terminal ▾ Thu 00:51
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nslookup
> wipro.com
Server:      203.187.215.35
Address:     203.187.215.35#53

Non-authoritative answer:
Name:   wipro.com
Address: 209.11.159.61
> set type=MX
> wipro.com
Server:      203.187.215.35
Address:     203.187.215.35#53

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

Authoritative answers can be found from:
wipro.com nameserver = ns4.webindia.com.
wipro.com nameserver = ns2.webindia.com.
wipro.com nameserver = ns1.webindia.com.
ns1.webindia.com internet address = 50.16.170.116
ns2.webindia.com internet address = 34.235.29.171
ns4.webindia.com internet address = 54.66.0.69
>
```

## Identified Mail Servers: -

✚ **IBM:** mx0a-001b2d01.pphosted.com  
mx0b-001b2d01.pphosted.com

✚ **Wipro:** wipro-com.mail.protection.outlook.com

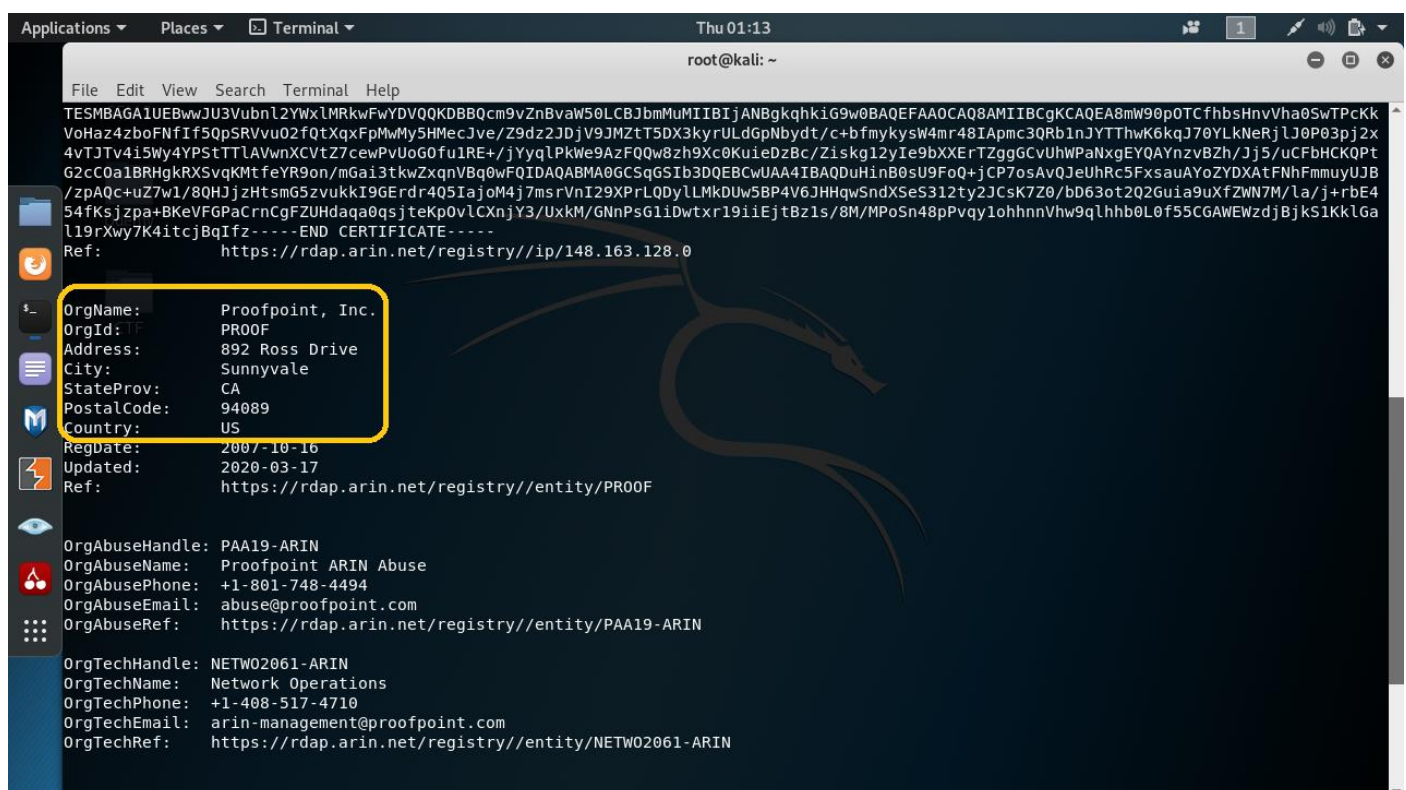
**Q.2.** Find the locations, where these email servers are hosted.

==> **Objective:** Trying to find the location and identify the mail servers of the targets.

## Tools Used: -

- **nslookup:** Retrieving the IP addresses of the target mail servers.
- **whois:** Obtaining details of the respective IPs obtained via nslookup.

## Target-1 (IBM): -

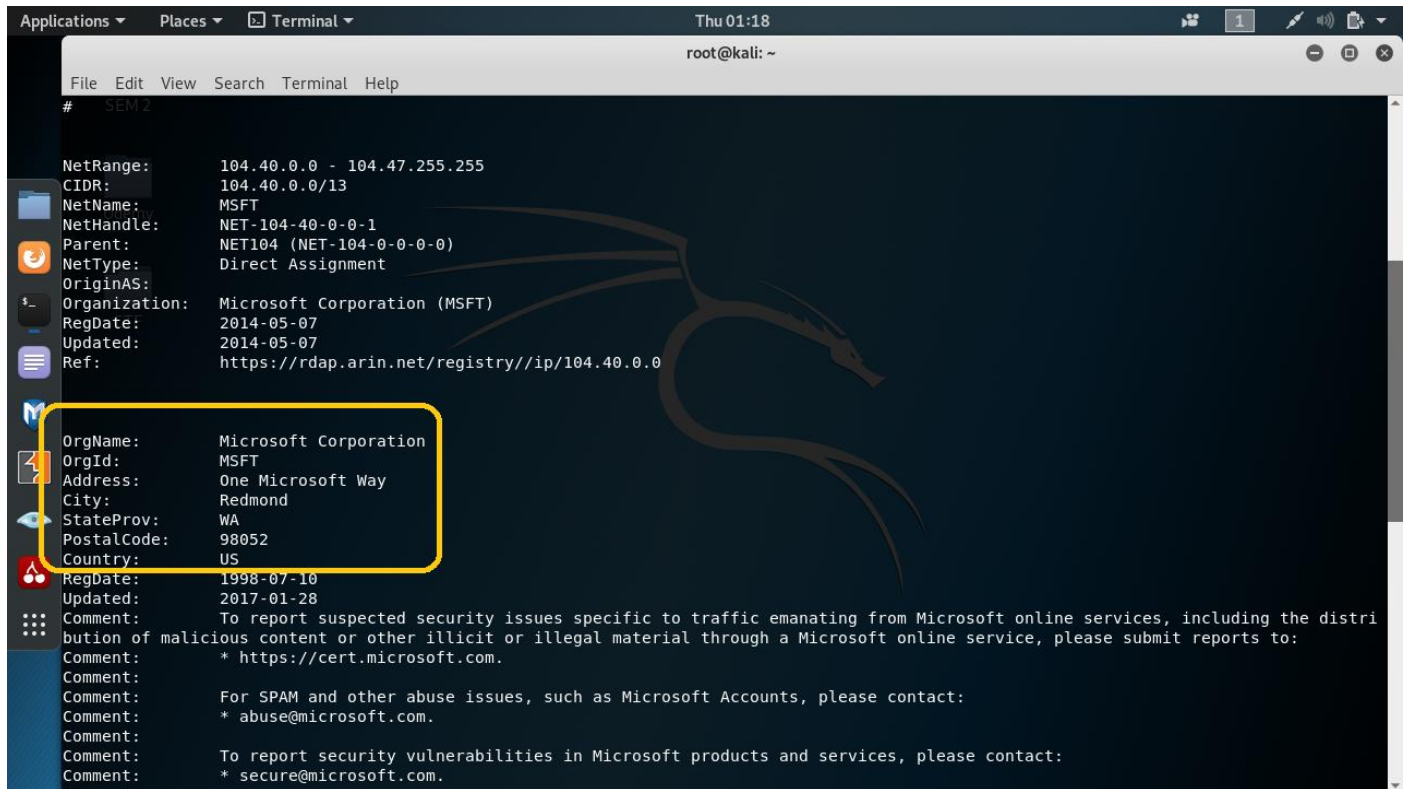


```
root@kali: ~  
File Edit View Search Terminal Help  
TESMBAGAIUEBwJU3Vubnl2YwXLMRkFwYDVQKDBBQcm9vZnBvaW50LCBjbmuMIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8AMIIBCgKCAQEA8mW90p0TCfhbsHnvVha0SwTPcKk  
VoH4z4boFNfIf5QpSRVvu02fQtXqFpMwMy5HMecJve/Z9dz2JDjV9JMztT5DX3kyrULdGpNbydt/c+bfmykysW4mr48IApmc3QRb1nJYTTThwK6kqJ70YLkNeRjLJ0P03pj2x  
4vTJTv4i5WY4YPStTTLAVwnXCVtZ7cewPvUoG0fu1RE+/jYyqLPkWe9AzFQ0w8zh9Xc0KuiEdZBc/Ziskg12yIe9bXXErTZggGCVUHPaXNgEYQAYnzvBZh/Jj5/uCFbHCK0Pt  
G2cC0a1BRHhgkRXSvqKmtfeYR9on/mGai3tkwZxqnVBq0wFQIDAQABMA0GCSqGSIb3DQEBEwUAA4IBAQDuHinB0sU9FoQ+jCP7osAvQJJeUhrC5FxsauAYoZYDXAtFNhFmmuyUJB  
/zPAQc+uZ7w1/8QHJjzHtsmG5zvukkI9GErdr4Q5Iajom4j7msrVnI29XPrLQDyLLMkDUw5BP4V6JHHqWsndXSeS312ty2JCsK7Z0/bD63ot2Q2Guia9uXfZW7M/la/j+rbE4  
54Fksjzpa+BKeVFGPaCrnCGFZUHdaqa0qsjteKpOvLCXnjY3/UxKM/GNnPSG1iDwtxr19i1EjtBz1s/8M/MPoSn48pPvqy1ohhnnVhw9qlhbb0L0f55CGAWewzdjBjks1KklGa  
l19rXwy7K4itcjBqIfz-----END CERTIFICATE-----  
Ref: https://rdap.arin.net/registry/ip/148.163.128.0  
  
OrgName: Proofpoint, Inc.  
OrgId: PROOF  
Address: 892 Ross Drive  
City: Sunnyvale  
StateProv: CA  
PostalCode: 94089  
Country: US  
RegDate: 2007-10-16  
Updated: 2020-03-17  
Ref: https://rdap.arin.net/registry/entity/PROOF  
  
OrgAbuseHandle: PAA19-ARIN  
OrgAbuseName: Proofpoint ARIN Abuse  
OrgAbusePhone: +1-801-748-4494  
OrgAbuseEmail: abuse@proofpoint.com  
OrgAbuseRef: https://rdap.arin.net/registry/entity/PAA19-ARIN  
  
OrgTechHandle: NETW02061-ARIN  
OrgTechName: Network Operations  
OrgTechPhone: +1-408-517-4710  
OrgTechEmail: arin-management@proofpoint.com  
OrgTechRef: https://rdap.arin.net/registry/entity/NETW02061-ARIN
```

Carrying out the **whois lookup** reveals the location of the server. The complete log for both the mail servers could be found in a separate .txt file attached herewith for the same.

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

## Target-2 (Wipro): -



```
Applications ▾ Places ▾ Terminal ▾ Thu 01:18
root@kali: ~
File Edit View Search Terminal Help
# SEM 2

NetRange: 104.40.0.0 - 104.47.255.255
CIDR: 104.40.0.0/13
NetName: MSFT
NetHandle: NET-104-40-0-0-1
Parent: NET104 (NET-104-0-0-0-0)
NetType: Direct Assignment
OriginAS:
Organization: Microsoft Corporation (MSFT)
RegDate: 2014-05-07
Updated: 2014-05-07
Ref: https://rdap.arin.net/registry/ip/104.40.0.0

OrgName: Microsoft Corporation
OrgId: MSFT
Address: One Microsoft Way
City: Redmond
StateProv: WA
PostalCode: 98052
Country: US
RegDate: 1998-07-10
Updated: 2017-01-28
Comment: To report suspected security issues specific to traffic emanating from Microsoft online services, including the distribution of malicious content or other illicit or illegal material through a Microsoft online service, please submit reports to:
Comment: * https://cert.microsoft.com.
Comment:
Comment: For SPAM and other abuse issues, such as Microsoft Accounts, please contact:
Comment: * abuse@microsoft.com.
Comment:
Comment: To report security vulnerabilities in Microsoft products and services, please contact:
Comment: * secure@microsoft.com.
```

Carrying out the **whois lookup** reveals the location of the server. The complete log for both the mail servers could be found in a separate .txt file attached herewith for the same.

Identified Mail Server Locations: - Redmond, WA - USA

✦ Both the servers have the same location.

**Q.3.** Scan and find out port numbers open 203.163.246.23

==>

Carrying out nmap scan on the target host it is found that the open port is **Port: 53**

Further details can be found in the respective .txt files attached herewith.

```

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

```

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

==>

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

Details of the scan are attached in a downloaded .html file which is attached alongwith.

=====