

CYBER SECURITY – ESSENTIALS

ASSIGNMENT DAY-4

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

a)Ibm.com b)Wipro.com

Ans:

```
Command Prompt - nslookup
> ibm.com
Server: UnKnown
Address: 192.168.43.1

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
> wipro.com
Server: UnKnown
Address: 192.168.43.1

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

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?

Ans:

```
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-A
```

```

OrgName:      Microsoft Corporation
OrgId:        MSFT
Address:      One Microsoft Way
City:         Redmond
StateProv:    WA
PostalCode:   98052
Country:      US
RegDate:      1998-07-10
Updated:      2017-01-20
Comment:      To report suspected security issues specific to traffic
                bution of malicious content or other illicit or illegal material through
Comment:      * https://cert.microsoft.com.
Comment:
Comment:      For SPAM and other abuse issues, such as Microsoft Account
Comment:      * abuse@microsoft.com.
Comment:
Comment:      To report security vulnerabilities in Microsoft products
Comment:      * secure@microsoft.com.

```

Identified Mail Server Locations: - IBM : Sunnyvale, CA – USA

Identified Mail Server Locations: - WIPRO : Redmond, WA – USA

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

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

```

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=0%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=0%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)

```