Project-1

#letsupgrade

2020

Cyber-Security-Essentials

ABOUT

Different Types Of Domain Tracking Through LINUX ,WINDOWS ,WEBSITES etc. Scan vulnerability in system.

ABHISHEK SACHAN

Abhisheksachan461@gmail.com

8687511247

8/28/2020

Question 1:

Find out the mail servers of the following domain :
Ibm.com.
Wipro.com

Solution→

CMD.

NSLOOKUP
Set type=MX
(DOMAIN NAME)

```
Microsoft Windows [Version 10.0.18363.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Abhishek_Sachan>nslookup
Default Server:  UnKnown
Address:  192.168.43.1

> set type=mx
> ibm.com
Server:  UnKnown
Address:  192.168.43.1

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
> 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
>
```

Ibm.com.

mx0a-001b2d01.pphosted.com →148.163.156.1

mx0b-001b2d01.pphosted.com →148.163.158.5

Wipro.com

wipro-com.mail.protection.outlook.com →104.47.126.36

```
C:\Users\Abhishek_Sachan>nslookup mx0a-001b2d01.pphosted.com
Server:  UnKnown
Address:  192.168.43.1

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


C:\Users\Abhishek_Sachan>nslookup mx0b-001b2d01.pphosted.com
Server:  UnKnown
Address:  192.168.43.1

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


C:\Users\Abhishek_Sachan>nslookup wipro-com.mail.protection.outlook.com
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    wipro-com.mail.protection.outlook.com
Addresses:  104.47.124.36
          104.47.126.36
```

Below records found trhough Websites

Network information

DNS server (NS records)	asia3.akam.net (23.211.61.64) eur2.akam.net (95.100.173.64) usc2.akam.net (184.26.160.64) eur5.akam.net (23.74.25.64) usc3.akam.net (96.7.50.64) usw2.akam.net (184.26.161.64) ns1-206.akam.net (193.108.91.206) ns1-99.akam.net (193.108.91.99)
Mail server (MX records)	mx0a-001b2d01.pphosted.com (148.163.156.1) mx0b-001b2d01.pphosted.com (148.163.158.5)

Question 2:

Find the locations, where these email servers are hosted.

Ibm.com.

mx0a-001b2d01.pphosted.com →148.163.156.1 → UNITED STATES

IP information 148.163.156.1

IP address	148.163.156.1
Location	United States (US)
Registry	arin

mx0b-001b2d01.pphosted.com →148.163.158.5 →UNITED STATES

IP information 148.163.158.5

IP address	148.163.158.5
Location	United States (US)
Registry	arin

Wipro.com

wipro-com.mail.protection.outlook.com →104.47.126.36→ Busan, South Korea (KR)

IP information 104.47.126.36

IP address	104.47.126.36
Location	Busan, Busan, South Korea (KR)
Registry	arin

Question 3:

Scan and find out port numbers open 203.163.246.23

Solution →

Scan through kali nmap

```
bpg@kali-pc-001:~$ nmap 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 09:13 PDT
Note: Host seems down. If it is really up, but blocking our ping probes, tr
y -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.20 seconds
```

Windows Cmd also not ping with this IP

```
C:\Users\Abhishek_Sachan>ping 203.163.246.23

Pinging 203.163.246.23 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 203.163.246.23:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
```

Scan ports through Websites found below result.

HTTP	tcp80	Closed ✔
HTTPS	tcp443	Closed ✔
DNS	udp53	Closed ✔
Network Time Protocol (NTP)	udp123	Closed ✔
NetBIOS Name Service	udp137	Closed ✔
Session Initiation Protocol (SIP)	udp5060	Closed ✔

Question 4:

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

Solution→

Not Complete due to lack of time and system Configuration.

Sorry for inconvenience.

Nessus Activation code →160E-7E4E-0CE6-****-****

THANK YOU