

## Assignment Day 4 | 23th Aug 2020

### Question 1:

Find out the mail servers of the following domain :

[ibm.com](http://ibm.com)

```
C:\Users\rashmin_patel>nslookup wipro.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:     wipro.com
Address:  209.11.159.61

C:\Users\rashmin_patel>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> set type=mx
> ibm.com
Server:  dns.google
Address:  8.8.8.8

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](http://Wipro.com)

```
>
C:\Users\rashmin_patel>nslookup
Default Server:  dns.google
Address:  8.8.8.8

> set type=mx
> wipro.com
Server:  dns.google
Address:  8.8.8.8

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


## Question 2:

Find the locations, where these email servers are hosted.


www.wipro.com

Is the data shown below not accurate enough? Please read [geolocation accuracy](#) info to learn why.

Geolocation data from [IP2Location](#) (Product: DB6, updated on 2020-9-1)

IP Address	Country	Region	City
104.47.126.36	Korea (Republic of) 	Busan-gwangyeoksi	Busan
ISP	Organization	Latitude	Longitude
Microsoft Corporation	Not Available	35.1028	129.0403


Geolocation data from [ipinfo.io](#) (Product: API, real-time)

IP Address	Country	Region	City
104.47.126.36	South Korea 	Busan	Dongnae
ISP	Organization	Latitude	Longitude
Microsoft Corporation	Microsoft Corporation (microsoft.com)	35.2016	129.0848


www.ibm.com

Is the data shown below not accurate enough? Please read [geolocation accuracy](#) info to learn why.

Geolocation data from [IP2Location](#) (Product: DB6, updated on 2020-9-1)

IP Address	Country	Region	City
148.163.158.5	United States of America 	California	Sunnyvale
ISP	Organization	Latitude	Longitude
Proofpoint Inc.	Not Available	37.4012	-122.0075

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

IP Address	Country	Region	City
148.163.158.5	United States 	California	San Jose
ISP	Organization	Latitude	Longitude
Proofpoint, Inc.	Proofpoint, Inc. (proofpoint.com)	37.3394	-121.8950

### Question 3:

Scan and find out port numbers open 203.163.246.23

```
root@kali-pc-001:~# nmap 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 11:30 PDT
Nmap scan report for 203.163.246.23
Host is up (0.0017s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
25/tcp    closed smtp
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   closed smtps

Nmap done: 1 IP address (1 host up) scanned in 4.81 seconds
root@kali-pc-001:~#
```

### Question 4:

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

Nessus Professional / Firefox | Certificate error | https://localhost:8834/#/scans/reports/5/hosts

nessus Professional

Scans Settings

admin

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

TENABLE

- Community
- Research

TestPC

Back to My Scans

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 28 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities
172.16.40.29	6 74

Scan Details

Policy: Advanced Scan  
Status: Completed  
Scanner: Local Scanner  
Start: Today at 6:27 PM  
End: Today at 6:33 PM  
Elapsed: 6 minutes

Vulnerabilities

Windows Taskbar: Type here to search | 18:41 26/08/2020

Nessus Professional / Firefox | Certificate error | https://localhost:8834/#/scans/reports/5/vulnerabilities

nessus Professional

Scans Settings

admin

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

TENABLE

- Community
- Research

Hosts 1 Vulnerabilities 28 History 1

Filter Search Vulnerabilities 28 Vulnerabilities

Sev	Name	Family	Count
MIXED	SSL (Multiple Issues)	General	8
MIXED	Microsoft Windows (Multiple Issu...	Misc.	3
MIXED	TLS (Multiple Issues)	Service detection	3
INFO	DCE Services Enumeration	Windows	15
INFO	Nessus SYN scanner	Port scanners	14
INFO	HTTP (Multiple Issues)	Web Servers	6
INFO	SMB (Multiple Issues)	Windows	5
INFO	Service Detection	Service detection	4
INFO	VNC (Multiple Issues)	Service detection	3
INFO	Additional DNS Hostnames	General	1

Scan Details

Policy: Advanced Scan  
Status: Completed  
Scanner: Local Scanner  
Start: Today at 6:27 PM  
End: Today at 6:33 PM  
Elapsed: 6 minutes

Vulnerabilities

Windows Taskbar: Type here to search | 18:42 26/08/2020

[illegible]