

## Assignment Day 4 -

### Question 1 : Mail Server -

ibm.com/ wipro.com

```
Activities Terminal Aug 27 20:01 alex@Alex: ~
alex@Alex:~$ nslookup
> set type=mx
> www.ibm.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.ibm.com canonical name = www.ibm.com.cs186.net.
www.ibm.com.cs186.net canonical name = outer-ccdn-dual.ibmcom.edgekey.net.
outer-ccdn-dual.ibmcom.edgekey.net canonical name = outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net.
outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net canonical name = e2874.dscx.akamaiedge.net.

Authoritative answers can be found from:
>
```

```
Activities Terminal Aug 27 20:02 alex@Alex: ~
alex@Alex:~$ nslookup
> set type=mx
> www.ibm.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.ibm.com canonical name = www.ibm.com.cs186.net.
www.ibm.com.cs186.net canonical name = outer-ccdn-dual.ibmcom.edgekey.net.
outer-ccdn-dual.ibmcom.edgekey.net canonical name = outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net.
outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net canonical name = e2874.dscx.akamaiedge.net.

Authoritative answers can be found from:
> www.wipro.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.wipro.com canonical name = d361nqn33s63ex.cloudfront.net.

Authoritative answers can be found from:
>
```

## Question 2 : Locations of Email server Hosted -

mail@ibm.com

Mailbox Domain	mx0b-001b2d01.pphosted.com
IP	148.163.158.5
Country	United States
City	Sunnyvale
Latitude	37.424900054932
Longitude	-122.0074005127
ISP	N/A

mail@wipro.com

Mailbox Domain	wipro-com.mail.protection.outlook.com
IP	104.47.126.36
Country	Korea, Republic of
City	Busan
Latitude	35.102798461914
Longitude	129.04029846191
ISP	N/A

## Question 3 - port numbers open 203.163.246.23

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ sudo su -  
[sudo] password for kali:  
root@kali:~# nmap -T4 -p- -vv 203.163.246.23  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 12:01 EDT  
Failed to resolve "-T4".  
Failed to resolve "-p-".  
Initiating Ping Scan at 12:01  
Scanning 203.163.246.23 [4 ports]  
Completed Ping Scan at 12:01, 0.04s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 12:01  
Completed Parallel DNS resolution of 1 host. at 12:01, 0.76s elapsed  
Initiating SYN Stealth Scan at 12:01  
Scanning 203.163.246.23 [1000 ports]  
Completed SYN Stealth Scan at 12:01, 4.05s elapsed (1000 total ports)  
Nmap scan report for 203.163.246.23  
Host is up, received reset ttl 128 (0.00051s latency).  
All 1000 scanned ports on 203.163.246.23 are filtered because of 1000 no-responses  
  
Read data files from: /usr/bin/./share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 5.17 seconds  
Raw packets sent: 2007 (88.272KB) | Rcvd: 4 (160B)  
root@kali:~#
```

## Question 4 -

### Nessus Installed – Scan running

The screenshot shows the Nessus Essentials interface. The main heading is 'My Scans'. Below it is a search bar and a table with the following data:

Name	Schedule	Last Modified
Rushi	On Demand	Today at 1:55 AM

The left sidebar contains the following sections:

- FOLDERS: My Scans (1), All Scans, Trash
- RESOURCES: Policies, Plugin Rules, Scanners
- TENABLE: Community, Research
- Tenable News: Why Cybersecurity Leaders Struggle to Answer the Q... (Read More)

The screenshot shows the Nessus Essentials interface for a specific scan named 'Rushi'. The main heading is 'Rushi'. Below it is a 'Back to All Scans' link and a 'Configure' button. The main content area shows a table of hosts with the following data:

Host	Vulnerabilities	%
172.16.126.1	2 (66%)	100%
172.16.126.254	1 (5%)	5%

The right sidebar contains the following sections:

- Scan Details: Policy: Basic Network Scan, Status: Running, Scanner: Local Scanner, Start: Today at 1:55 AM
- Vulnerabilities: A donut chart showing the distribution of vulnerabilities by severity. The legend indicates: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Thank you.

