

## Question 1: Find out the mail servers of the following domains: ibm.com, wipro.com

**Solution:** Open Terminal.

**For ibm.com -**

Type the command **nslookup**

**set type=mx**

**ibm.com**

```
File Actions Edit View Help
root@kali-pc-001:~# nslookup
> ibm.com
Server:      192.168.150.2
Address:     192.168.150.2#53

Non-authoritative answer:
Name:   ibm.com
Address: 129.42.38.10
> set type=mx
> ibm.com
Server:      192.168.150.2
Address:     192.168.150.2#53

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

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

**For wipro.com -**

Type the command **nslookup**

**set type=mx**

**wipro.com**

```
File Actions Edit View Help
root@kali-pc-001:~# nslookup
> wipro.com
Server:      192.168.150.2
Address:     192.168.150.2#53

Non-authoritative answer:
Name:   wipro.com
Address: 209.11.159.61
> set type=mx
> wipro.com
Server:      192.168.150.2
Address:     192.168.150.2#53

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

Authoritative answers can be found from:
wipro.com nameserver = ns3.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
ns3.webindia.com internet address = 216.55.142.32
> █
```

## Question 2: Find the locations, where these email servers are hosted.

**Solution:**

Mail server locations for ibm.com are :-

1. **mx0a-001b2d01.pphosted.com**

enter DOMAIN here		<input type="button" value="Go"/> new window: <input type="checkbox"/>	
<b>mx0a-001b2d01.pphosted.com</b>			
IP	<a href="#">148.163.156.1</a>		
COUNTRY NAME	United States		
REGION NAME	CA		
CITY	Sunnyvale		
PROVIDER (ORG)	N/A		
<b>Common records</b>			
<b>A</b>			
host	class	ttd	ip
<a href="#">mx0a-001b2d01.pphosted.com</a>	IN	1800	148.163.156.1
<i>ip: An IPv4 addresses in dotted decimal notation.</i>			

2. **mx0a-001b2d01.pphosted.com**

enter DOMAIN here		<input type="button" value="Go"/> new window: <input type="checkbox"/>	
<b>mx0b-001b2d01.pphosted.com</b>			
IP	<a href="#">148.163.158.5</a>		
COUNTRY NAME	United States		
REGION NAME	CA		
CITY	Sunnyvale		
PROVIDER (ORG)	N/A		
<b>Common records</b>			
<b>A</b>			
host	class	ttd	ip
<a href="#">mx0b-001b2d01.pphosted.com</a>	IN	1800	148.163.158.5
<i>ip: An IPv4 addresses in dotted decimal notation.</i>			

Mail server location for wipro.com is :-

**wipro-com.mail.protection.outlook.com**

enter DOMAIN here  new window: ☐

**wipro-com.mail.protection.outlook.com**

IP	<a href="#">104.47.125.36</a>
IP 1	<a href="#">104.47.126.36</a>
COUNTRY NAME	Singapore
REGION NAME	00
CITY	Singapore
PROVIDER (ORG)	N/A

**Common records**

A			
host	class	ttl	ip
<a href="#">wipro-com.mail.protection.outlook.com</a>	IN	10	104.47.126.36
<a href="#">wipro-com.mail.protection.outlook.com</a>	IN	10	104.47.125.36

*ip: An IPv4 addresses in dotted decimal notation.*

### Question 3: Scan and find out port numbers open 203.163.246.23

**Solution:** The given IP was scanned using NMAP

Command: nmap 203.163.246.23

```

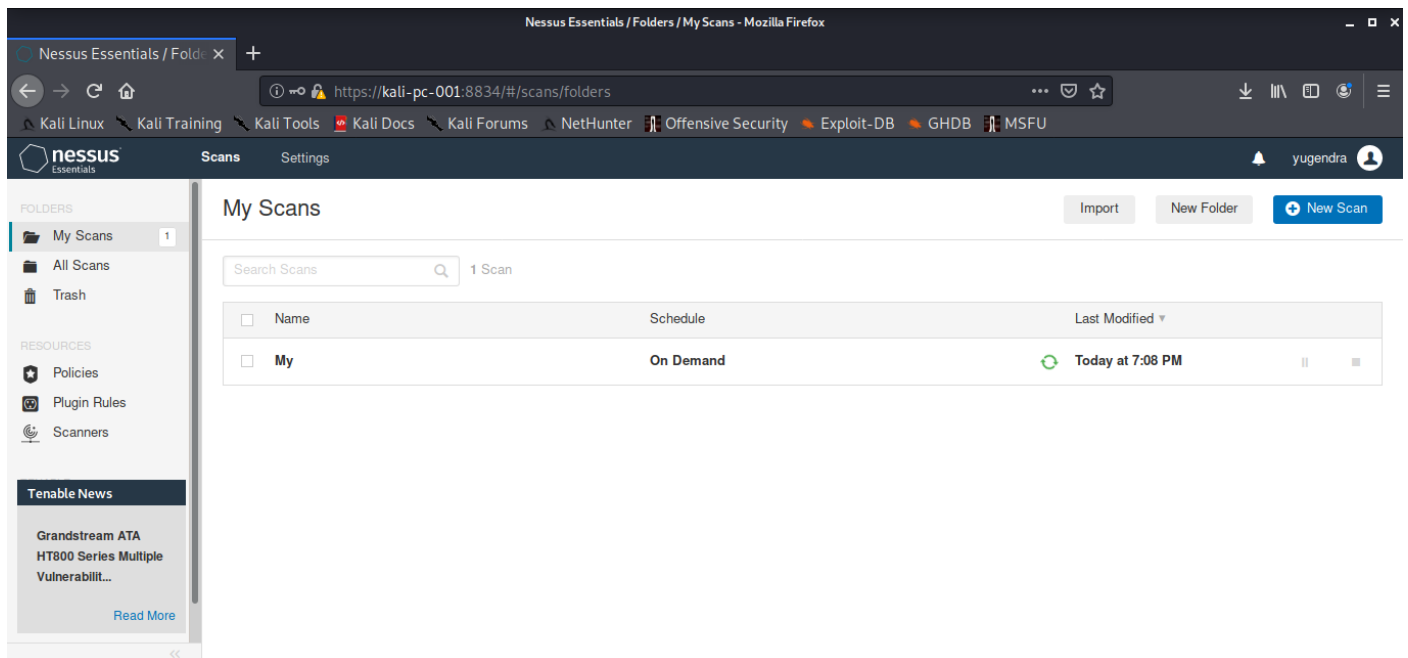
kali@kali: ~
File Actions Edit View Help
root@kali:/home/kali# nmap 203.163.246.23 --open
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 18:30 IST
Nmap done: 1 IP address (1 host up) scanned in 5.78 seconds
root@kali:/home/kali# nmap 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 18:32 IST
Nmap scan report for 203.163.246.23
Host is up (0.0028s latency).
All 1000 scanned ports on 203.163.246.23 are filtered
Nmap done: 1 IP address (1 host up) scanned in 4.63 seconds
root@kali:/home/kali#

```

### Question 4: Install Nessus in a VM and scan your laptop/desktop for CVE.

**Solution:**

1. Navigate to <https://www.tenable.com/downloads/nessus>
2. Download the appropriate version.



3. Register with the website with name and email to get the authentication code via email.

4. Go to Kali terminal, cd to Downloads folder.

5. Dpkg -i < file name>

6. type command /bin/systemctl start nessusd,server

8. Open link https://kali:8834/

7. Enter AUTH code sent via email.

9. Wait for initialization to complete.

10. Log on to Nessus.

11. Goto Advanced tab and create a scan against the local system.

12. Click on the Scan to get the list of vulnerabilities

