

Question 1:

Find out the mail servers of the following domain :

lbm.com

Wipro.com

```
default TTL = 1800 (30 mins)
> www.ibm.com
Server: UnKnown
Address: 192.168.192.2

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

dscx.akamaiedge.net
primary name server = n0dscx.akamaiedge.net
responsible mail addr = hostmaster.akamai.com
serial = 1598463682
refresh = 1000 (16 mins 40 secs)
retry = 1000 (16 mins 40 secs)
expire = 1000 (16 mins 40 secs)
default TTL = 1800 (30 mins)
```

```
> www.wipro.com
Server: UnKnown
Address: 192.168.192.2

Non-authoritative answer:
www.wipro.com canonical name = d361nqn33s63ex.cloudfront.net
> www.wipro.com
Server: UnKnown
Address: 192.168.192.2

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

d361nqn33s63ex.cloudfront.net
primary name server = ns-1658.awsdns-15.co.uk
responsible mail addr = awsdns-hostmaster.amazon.com
serial = 1
refresh = 7200 (2 hours)
retry = 900 (15 mins)
expire = 1209600 (14 days)
default TTL = 86400 (1 day)
> _
```

```
Administrator: Command Prompt - nslookup
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup
Default Server: UnKnown
Address: 192.168.192.2

> set type=mx
type=mx
> lbm.com
Server: UnKnown
Address: 192.168.192.2

Non-authoritative answer:
lbm.com MX preference = 5, mail exchanger = mx0b-001b2d01.pphosted.com
lbm.com MX preference = 5, mail exchanger = mx0a-001b2d01.pphosted.com

mx0b-001b2d01.pphosted.com internet address = 148.163.158.5
mx0a-001b2d01.pphosted.com internet address = 148.163.156.1
> wipro.com
Server: UnKnown
Address: 192.168.192.2

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

wipro-com.mail.protection.outlook.com internet address = 104.47.125.36
wipro-com.mail.protection.outlook.com internet address = 104.47.124.36
> _
```

Question 2:

Find the locations, where these email servers are hosted.

FileHelp

My Inbox

My Trace Reports

Trace Headers

Trace Address

Email Accounts

Settings

Export Rules

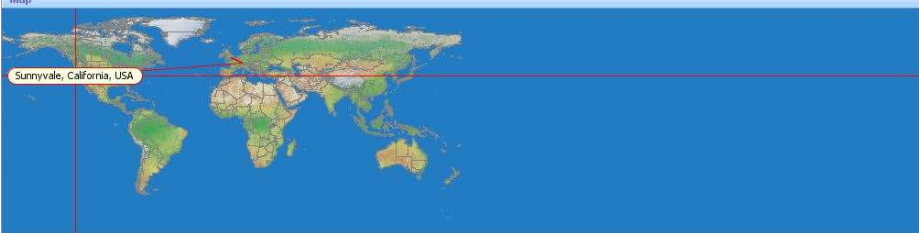
Trial Edition

Home | sowramac@in.ibm.com X

The trace is complete, the information found is displayed on the right

New TraceView Report

Map



#	Hop IP	Hop Name	Location
1	192.168.1.1		
3	192.168.16.65		
4	192.168.16.1		
5	192.168.0.193		
8	172.16.92.145		
9	172.25.115.29		
10	172.16.2.113		
15	149.14.196.81	hu0-4-0-1.agr21.lhr01.atlas.cogentco.com	Washington, DC, USA
16	130.117.48.137	be3671.ccr51.lhr01.atlas.cogentco.com	EU

For 24 hours only you can get up to 20% off eMailTrackerPro! [Click Here](#)

FileHelp

My Inbox

My Trace Reports

Trace Headers

Trace Address

Email Accounts

Settings

Export Rules


Trial Edition

Home | info@wipro.com X

The trace is complete, the information found is displayed on the right

New TraceView Report

Map



#	Hop IP	Hop Name	Location
1	192.168.1.1		
3	192.168.16.65		
4	192.168.16.1		
5	192.168.0.193		
7	136.232.13.177	136.232.13.177.static.jio.com	(India)
8	172.16.18.33		
9	172.25.115.31		
10	104.44.13.78	ae60-0.de101-96cbe-1b.ntwk.msn.net	Redmond, Washington, USA
11	104.44.42.140	ae24-0.ea02.maa02.ntwk.msn.net	Redmond, Washington, USA

For 24 hours only you can get up to 20% off eMailTrackerPro! [Click Here](#)

Email Summary

Email Address: sowramac@in.ibm.com
IP: 148.163.156.1
Location: Sunnyvale, California, USA
Abuse Address: abuse@proofpoint.com
System Information:

- The system is running a mail server (Blocked - see <https://ipcheck.proofpoint.com/?ip=112.196.181.23> port 25. This means that this system can be used to send email.
- There is no HTTP server running on this system (the port is closed).
- There is no HTTPS server running on this system (the port is closed).
- There is no FTP server running on this system (the port is closed).

[Network Whois](#)

[Domain Whois](#)

Email Summary

Email Address: info@wipro.com
IP: 104.47.126.36
Location: Busan, Pusan-jikhalsi, Korea
Abuse Reporting: To automatically generate an email abuse report [click here](#)
System Information:

- The system is running a mail server (Microsoft ESMTP MAIL Service) on port 25. This means that this system can be used to send email.
- There is no HTTP server running on this system (the port is closed).
- There is no HTTPS server running on this system (the port is closed).
- There is no FTP server running on this system (the port is closed).

[Network Whois](#)

[Domain Whois](#)

Question 3:

Scan and find out port numbers open 203.163.246.23

```
bpg@kali-pc-001:~$ sudo su -  
[sudo] password for bpg:  
root@kali-pc-001:~# nmap -Pn -sS 203.163.246.23  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 12:01 PDT  
Nmap scan report for 203.163.246.23  
Host is up.  
All 1000 scanned ports on 203.163.246.23 are filtered  
  
Nmap done: 1 IP address (1 host up) scanned in 201.50 seconds
```

Question 4:

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

Not secure | <https://localhost:8834/#/scans/reports/6/hosts>

nessus Essentials Scans Settings

Domain Controller

Configure Audit Trail Launch Report

Back to My Scans

Hosts 1 Vulnerabilities 14 History 2

Filter Search Hosts 1 Host

Host	Vulnerabilities
192.168.1.13	25

Scan Details

Policy: Advanced Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 1:33 AM
End: Today at 1:41 AM
Elapsed: 8 minutes

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Not secure | <https://localhost:8834/#/scans/reports/6/vulnerabilities>

nessus Essentials Scans Settings

Domain Controller

Configure Audit Trail Launch Report

Back to My Scans

Hosts 1 Vulnerabilities 14 History 2

Filter Search Vulnerabilities 14 Vulnerabilities

Sev	Name	Family	Count
MEDIUM	SMB Signing not required	Misc.	1
INFO	DCE Services Enumeration	Windows	8
INFO	SMB (Multiple Issues)	Windows	5
INFO	Microsoft Windows (Multiple Issu...	Windows	2
INFO	Authenticated Check : OS Name and I...	Settings	1
INFO	Authentication Failure - Local Checks ...	Settings	1
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Host Fully Qualified Domain Name (F...	General	1

Scan Details

Policy: Advanced Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 1:33 AM
End: Today at 1:41 AM
Elapsed: 8 minutes

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).