

Question 1 :

Find out the mail servers of the following domain

IBM.Com

Wipro.com

```
root@kali-pc-001:~# nslookup
> set type=mx
> ibm.com
Server:          192.168.139.2
Address:         192.168.139.2#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 = eur5.akam.net.
ibm.com nameserver = ns1-206.akam.net.
ibm.com nameserver = usc3.akam.net.
ibm.com nameserver = usc2.akam.net.
ibm.com nameserver = asia3.akam.net.
ibm.com nameserver = eur2.akam.net.
ibm.com nameserver = ns1-99.akam.net.
ibm.com nameserver = usw2.akam.net.
eur2.akam.net internet address = 95.100.173.64
eur5.akam.net internet address = 23.74.25.64
usc2.akam.net internet address = 184.26.160.64
usc3.akam.net internet address = 96.7.50.64
usw2.akam.net internet address = 184.26.161.64
asia3.akam.net internet address = 23.211.61.64
ns1-99.akam.net internet address = 193.108.91.99
ns1-206.akam.net internet address = 193.108.91.206
```

```
ns1-99.akam.net has AAAA address 2600:1401:2::63
> wipro.com
Server:          192.168.139.2
Address:         192.168.139.2#53

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

Authoritative answers can be found from:
wipro.com nameserver = ns4.webindia.com.
wipro.com nameserver = ns1.webindia.com.
wipro.com nameserver = ns2.webindia.com.
> █
```

```
Administrator: C:\Windows\System32\cmd.exe - nslookup
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>nslookup
Default Server: UnKnown
Address: 192.168.139.2

> set type=mx
> ibm.com
Server: UnKnown
Address: 192.168.139.2

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

ibm.com nameserver = ns1-99.akam.net
ibm.com nameserver = usw2.akam.net
ibm.com nameserver = usc3.akam.net
ibm.com nameserver = asia3.akam.net
ibm.com nameserver = eur2.akam.net
ibm.com nameserver = eur5.akam.net
ibm.com nameserver = ns1-206.akam.net
ibm.com nameserver = usc2.akam.net
eur2.akam.net internet address = 95.100.173.64
eur5.akam.net internet address = 23.74.25.64
usc2.akam.net internet address = 184.26.160.64
usc3.akam.net internet address = 96.7.50.64
usw2.akam.net internet address = 184.26.161.64
asia3.akam.net internet address = 23.211.61.64
ns1-99.akam.net internet address = 193.108.91.99
ns1-206.akam.net internet address = 193.108.91.206
ns1-99.akam.net AAAA IPv6 address = 2600:1401:2::63
> wipro.com
Server: UnKnown
Address: 192.168.139.2

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

wipro.com nameserver = ns4.webindia.com
wipro.com nameserver = ns1.webindia.com
wipro.com nameserver = ns2.webindia.com
```

Question 2 :

Find the locations where the email servers are hosted

Ibm.com

mail@ibm.com	
Mailbox Domain	mx0a-001b2d01.pphosted.com
IP	148.163.156.1
Country	United States
City	Sunnyvale
Latitude	37.424900054932
Longitude	-122.0074005127
ISP	N/A

Alternate:

```
bpg@kali-pc-001:~/Desktop$ ping ibm.com
PING ibm.com (129.42.38.10) 56(84) bytes of data.
 64 bytes from 129.42.38.10 (129.42.38.10): icmp_seq=1 ttl=128 time=298 ms
 64 bytes from 129.42.38.10 (129.42.38.10): icmp_seq=2 ttl=128 time=299 ms
 64 bytes from 129.42.38.10 (129.42.38.10): icmp_seq=3 ttl=128 time=301 ms
 64 bytes from 129.42.38.10 (129.42.38.10): icmp_seq=4 ttl=128 time=301 ms
 64 bytes from 129.42.38.10 (129.42.38.10): icmp_seq=5 ttl=128 time=299 ms
 64 bytes from 129.42.38.10 (129.42.38.10): icmp_seq=6 ttl=128 time=297 ms
 64 bytes from 129.42.38.10 (129.42.38.10): icmp_seq=7 ttl=128 time=301 ms
 64 bytes from 129.42.38.10 (129.42.38.10): icmp_seq=8 ttl=128 time=300 ms
 64 bytes from 129.42.38.10 (129.42.38.10): icmp_seq=9 ttl=128 time=306 ms
 64 bytes from 129.42.38.10 (129.42.38.10): icmp_seq=10 ttl=128 time=326 ms
 64 bytes from 129.42.38.10 (129.42.38.10): icmp_seq=11 ttl=128 time=299 ms
 64 bytes from 129.42.38.10 (129.42.38.10): icmp_seq=12 ttl=128 time=298 ms
 64 bytes from 129.42.38.10 (129.42.38.10): icmp_seq=13 ttl=128 time=301 ms
^C
--- ibm.com ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12023ms
rtt min/avg/max/mdev = 297.231/302.106/325.952/7.168 ms
```

```
bpg@kali-pc-001:~/Desktop$ whois 129.42.38.10

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy\_reporting/
#
# Copyright 1997-2020, American Registry for Internet Numbers, Ltd.
#

NetRange:      129.42.0.0 - 129.42.255.255
CIDR:          129.42.0.0/16
NetName:       IBM-RSCH-NET2
NetHandle:     NET-129-42-0-0-1
Parent:        NET129 (NET-129-0-0-0-0)
NetType:       Direct Assignment
OriginAS:
Organization:  IBM (IBM-1)
RegDate:       1987-07-29
Updated:       2015-10-20
Ref:           https://rdap.arin.net/registry/ip/129.42.0.0
```

OrgName: IBM
 OrgId: IBM-1
 Address: 3039 Cornwallis Road
 City: Research Triangle Park
 StateProv: NC
 PostalCode: 27709-2195
 Country: US
 RegDate: 1992-02-08
 Updated: 2017-11-30
 Ref: <https://rdap.arin.net/registry/entity/IBM-1>

OrgAbuseHandle: RAIN-ARIN
 OrgAbuseName: Registrar Authority, Internet numbers
 OrgAbusePhone: +1-800-426-7378
 OrgAbuseEmail: ipreg@us.ibm.com
 OrgAbuseRef: <https://rdap.arin.net/registry/entity/RAIN-ARIN>

OrgTechHandle: RAIN-ARIN
 OrgTechName: Registrar Authority, Internet numbers
 OrgTechPhone: +1-800-426-7378
 OrgTechEmail: ipreg@us.ibm.com
 OrgTechRef: <https://rdap.arin.net/registry/entity/RAIN-ARIN>

Wipro.com

mail@wipro.com	
Mailbox Domain	wipro-com.mail.protection.outlook.com
IP	104.47.125.36
Country	Singapore
City	Singapore
Latitude	1.2930999994278
Longitude	103.85579681396
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

mail@wipro.com	
Mailbox Domain	wipro-com.mail.protection.outlook.com
IP	104.47.124.36
Country	United States
City	Redmond
Latitude	47.680099487305
Longitude	-122.12059783936
ISP	N/A

Alternate:

```
hpg@kali-pc-001:~/Desktop$ ping wipro.com
PING wipro.com (209.11.159.61) 56(84) bytes of data.
```

```
hpg@kali-pc-001:~/Desktop$ whois 209.11.159.61
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy\_reporting/
#
# Copyright 1997-2020, American Registry for Internet Numbers, Ltd.
#

# start

NetRange:          209.11.128.0 - 209.11.191.255
CIDR:              209.11.128.0/18
NetName:           QTS-209-11-128-0-18
NetHandle:         NET-209-11-128-0-1
Parent:            NET209 (NET-209-0-0-0-0)
NetType:           Direct Allocation
OriginAS:          AS40913
Organization:      Quality Technology Services, LLC (QTS-9)
RegDate:           1999-03-16
Updated:           2012-02-24
Ref:               https://rdap.arin.net/registry/ip/209.11.128.0
```


OrgName: Quality Technology Services, LLC
OrgId: QTS-9
Address: 300 Satelllite BLVD
City: Suwanee
StateProv: GA
PostalCode: 30043
Country: US
RegDate: 2006-06-15
Updated: 2019-11-07
Ref: <https://rdap.arin.net/registry//entity/QTS-9>

OrgAbuseHandle: QTSAB-ARIN
OrgAbuseName: QTS-ABUSE
OrgAbusePhone: +1-866-239-5000
OrgAbuseEmail: abuse@qtsdatacenters.com
OrgAbuseRef: <https://rdap.arin.net/registry//entity/QTSAB-ARIN>

OrgTechHandle: NOC2886-ARIN
OrgTechName: NOC
OrgTechPhone: +1-866-239-5000
OrgTechEmail: support@qtsdatacenters.com
OrgTechRef: <https://rdap.arin.net/registry//entity/NOC2886-ARIN>

OrgNOCHandle: NOC2886-ARIN
OrgNOCName: NOC
OrgNOCPhone: +1-866-239-5000
OrgNOCEmail: support@qtsdatacenters.com
OrgNOCRef: <https://rdap.arin.net/registry//entity/NOC2886-ARIN>

end

start

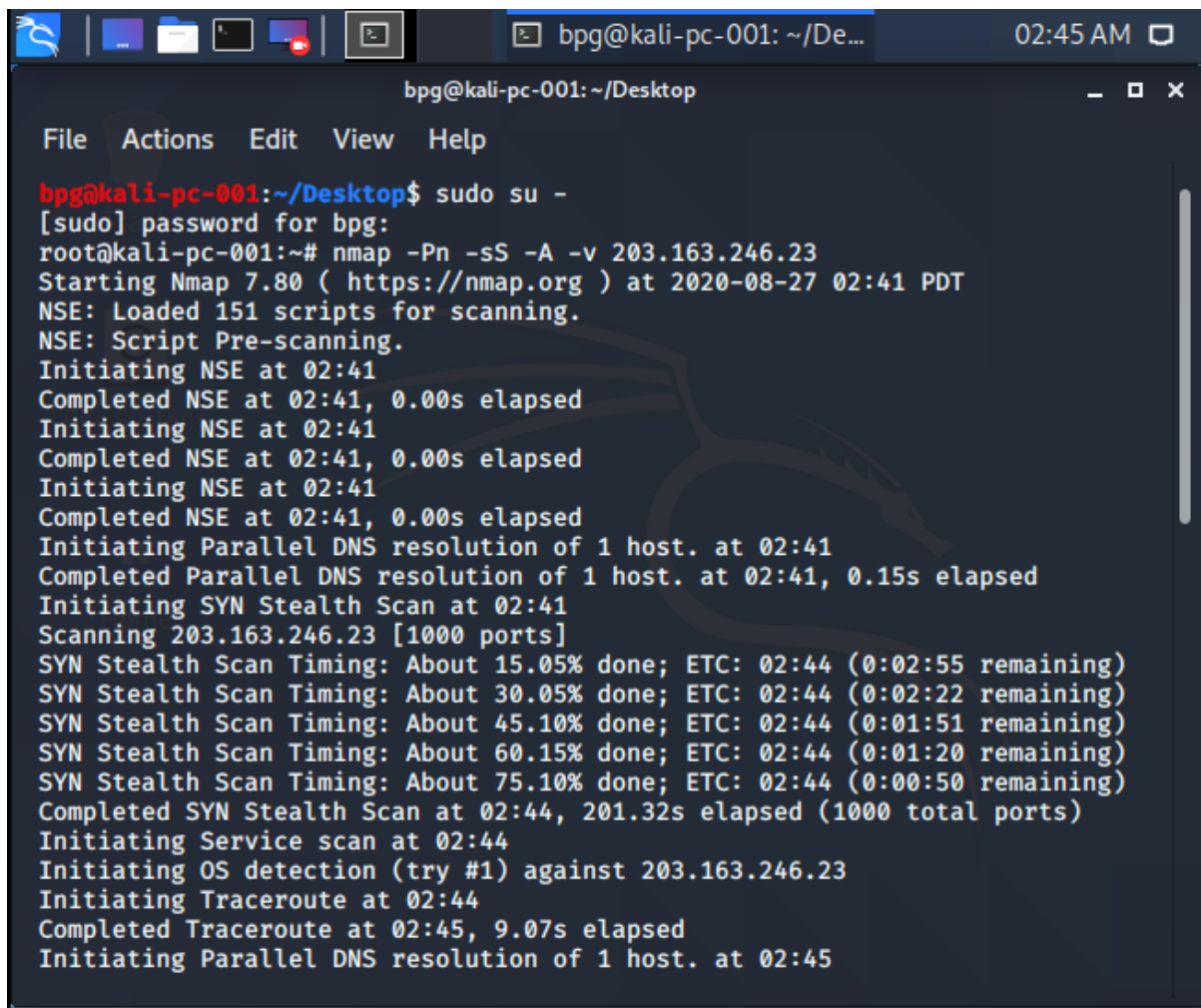
NetRange: 209.11.159.0 - 209.11.159.255
CIDR: 209.11.159.0/24
NetName: QTS-209-11-159-0-24
NetHandle: NET-209-11-159-0-1
Parent: QTS-209-11-128-0-18 (NET-209-11-128-0-1)
NetType: Reassigned
OriginAS: AS40913
Customer: IBIS Inc. (C04876229)
RegDate: 2014-02-24
Updated: 2014-02-24
Ref: <https://rdap.arin.net/registry//ip/209.11.159.0>

```
CustName:      IBIS Inc.  
Address:       2807 MIssion College Blvd  
City:          Santa Clara  
StateProv:     CA  
PostalCode:    95054  
Country:       US  
RegDate:       2014-02-24  
Updated:       2014-02-24  
Ref:           https://rdap.arin.net/registry//entity/C04876229  
  
OrgAbuseHandle: QTSAB-ARIN  
OrgAbuseName:   QTS-ABUSE  
OrgAbusePhone:  +1-866-239-5000  
OrgAbuseEmail:  abuse@qtsdatacenters.com  
OrgAbuseRef:    https://rdap.arin.net/registry//entity/QTSAB-ARIN  
  
OrgTechHandle:  NOC2886-ARIN  
OrgTechName:    NOC  
OrgTechPhone:   +1-866-239-5000  
OrgTechEmail:   support@qtsdatacenters.com  
OrgTechRef:     https://rdap.arin.net/registry//entity/NOC2886-ARIN
```

```
OrgNOCHandle:  NOC2886-ARIN  
OrgNOCName:    NOC  
OrgNOCPhone:   +1-866-239-5000  
OrgNOCEmail:   support@qtsdatacenters.com  
OrgNOCRef:     https://rdap.arin.net/registry//entity/NOC2886-ARIN  
  
# end
```

Question 3 :

Scan and find out port numbers open 203.163.246.23

A terminal window on a Kali Linux system. The user 'bpg' is at the prompt 'bpg@kali-pc-001: ~/Desktop'. They run 'sudo su -' to become root. Then they run 'nmap -Pn -sS -A -v 203.163.246.23'. The terminal shows the Nmap 7.80 interface, including NSE script pre-scanning, parallel DNS resolution, and a SYN Stealth Scan of 1000 ports. The scan progress is shown in real-time with percentage done and time remaining. The scan completes at 02:44 with 201.32s elapsed. Subsequent actions include service scan, OS detection, and traceroute, all completed by 02:45.

```
bpg@kali-pc-001: ~/Desktop
File Actions Edit View Help

bpg@kali-pc-001:~/Desktop$ sudo su -
[sudo] password for bpg:
root@kali-pc-001:~# nmap -Pn -sS -A -v 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 02:41 PDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:41
Completed NSE at 02:41, 0.00s elapsed
Initiating NSE at 02:41
Completed NSE at 02:41, 0.00s elapsed
Initiating NSE at 02:41
Completed NSE at 02:41, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 02:41
Completed Parallel DNS resolution of 1 host. at 02:41, 0.15s elapsed
Initiating SYN Stealth Scan at 02:41
Scanning 203.163.246.23 [1000 ports]
SYN Stealth Scan Timing: About 15.05% done; ETC: 02:44 (0:02:55 remaining)
SYN Stealth Scan Timing: About 30.05% done; ETC: 02:44 (0:02:22 remaining)
SYN Stealth Scan Timing: About 45.10% done; ETC: 02:44 (0:01:51 remaining)
SYN Stealth Scan Timing: About 60.15% done; ETC: 02:44 (0:01:20 remaining)
SYN Stealth Scan Timing: About 75.10% done; ETC: 02:44 (0:00:50 remaining)
Completed SYN Stealth Scan at 02:44, 201.32s elapsed (1000 total ports)
Initiating Service scan at 02:44
Initiating OS detection (try #1) against 203.163.246.23
Initiating Traceroute at 02:44
Completed Traceroute at 02:45, 9.07s elapsed
Initiating Parallel DNS resolution of 1 host. at 02:45
```



```
bpg@kali-pc-001: ~/De... 02:46 AM
bpg@kali-pc-001: ~/Desktop
File Actions Edit View Help
Completed Parallel DNS resolution of 1 host. at 02:45, 0.01s elapsed
NSE: Script scanning 203.163.246.23.
Initiating NSE at 02:45
Completed NSE at 02:45, 0.07s elapsed
Initiating NSE at 02:45
Completed NSE at 02:45, 0.00s elapsed
Initiating NSE at 02:45
Completed NSE at 02:45, 0.00s elapsed
Nmap scan report for 203.163.246.23
Host is up (0.00035s latency).
All 1000 scanned ports on 203.163.246.23 are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012, VMware Player virtual NAT device

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 0.76 ms 192.168.139.2
2 ... 30

NSE: Script Post-scanning.
Initiating NSE at 02:45
Completed NSE at 02:45, 0.00s elapsed
Initiating NSE at 02:45
Completed NSE at 02:45, 0.00s elapsed
```

```
Initiating NSE at 02:45
Completed NSE at 02:45, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 216.36 seconds
Raw packets sent: 2109 (93.620KB) | Rcvd: 1700 (68.016KB)
```

Question 4 :

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

The screenshot displays the Nessus Essentials web interface in a browser window. The address bar shows the URL `localhost:8834/#/scans/reports/6/hosts`. The interface has a dark blue header with the 'nessus Essentials' logo and navigation tabs for 'Scans' and 'Settings'. A left sidebar contains sections for 'FOLDERS' (My Scans, All Scans, Trash), 'RESOURCES' (Policies, Plugin Rules, Scanners), and 'TENABLE' (Community, Research). A 'Tenable News' section at the bottom left features a link to 'Grandstream ATA HT800 Series Multiple Vulnerabilit...'. The main content area is titled 'PenTester-Win-2016' and includes buttons for 'Configure', 'Audit Trail', and 'Launch'. Below the title are tabs for 'Hosts' (1), 'Vulnerabilities' (24), 'Remediations' (1), and 'History' (1). A search bar labeled 'Filter' and 'Search Hosts' shows '1 Host'. A table lists the host '192.168.139.128' with a 'Vulnerabilities' bar chart showing 5 critical (red), 26 high (orange), 19 medium (yellow), and 71 low (blue) vulnerabilities. On the right, a 'Scan Details' panel shows fields for Policy, Status, Scanner, Start, End, and Elapsed. Below this is a 'Vulnerabilities' section with a donut chart.

Host	Vulnerabilities
192.168.139.128	5 Critical, 26 High, 19 Medium, 71 Low