

### Question 1:

Find out the mail servers of the following domain:

Ibm.com

Wipro.com

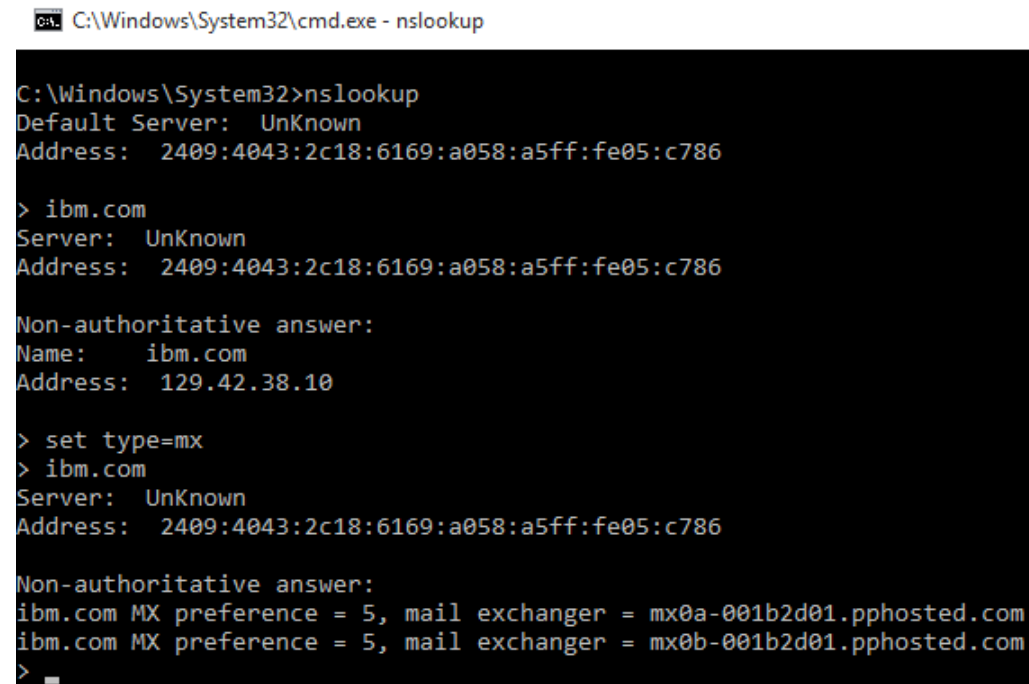
**Answer:** For Ibm.com

>nslookup

>ibm.com

>set type=mx

>ibm.com



```
C:\Windows\System32>nslookup
Default Server:  UnKnown
Address:  2409:4043:2c18:6169:a058:a5ff:fe05:c786

> ibm.com
Server:  UnKnown
Address:  2409:4043:2c18:6169:a058:a5ff:fe05:c786

Non-authoritative answer:
Name:    ibm.com
Address:  129.42.38.10

> set type=mx
> ibm.com
Server:  UnKnown
Address:  2409:4043:2c18:6169:a058:a5ff:fe05:c786

Non-authoritative answer:
ibm.com MX preference = 5, mail exchanger = mx0a-001b2d01.pphosted.com
ibm.com MX preference = 5, mail exchanger = mx0b-001b2d01.pphosted.com
> _
```

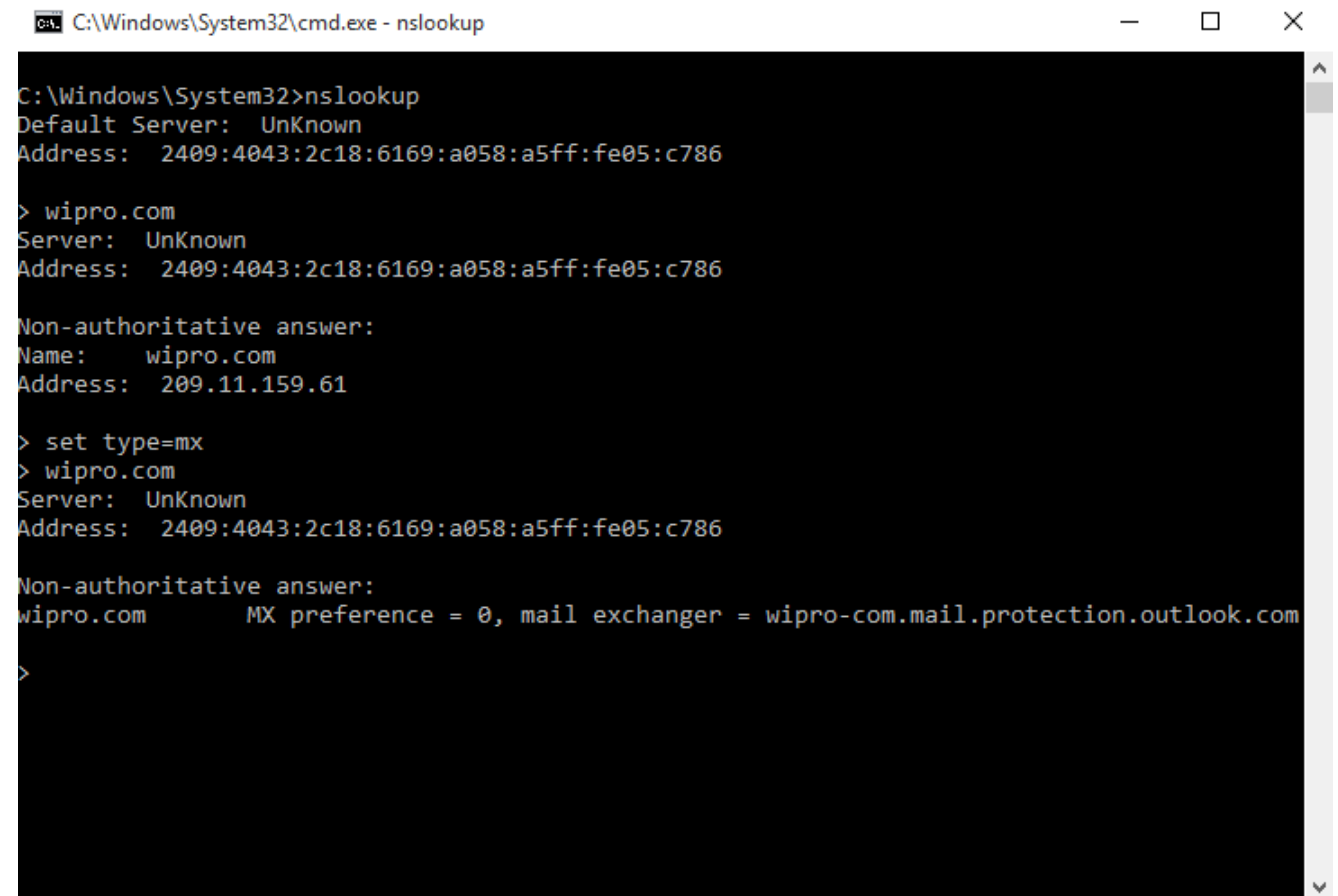
For Wipro.com

>nslookup

>wipro.com

>set type=mx

>wipro.com



```
C:\Windows\System32\cmd.exe - nslookup

C:\Windows\System32>nslookup
Default Server:  UnKnown
Address:  2409:4043:2c18:6169:a058:a5ff:fe05:c786

> wipro.com
Server:  UnKnown
Address:  2409:4043:2c18:6169:a058:a5ff:fe05:c786

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

> set type=mx
> wipro.com
Server:  UnKnown
Address:  2409:4043:2c18:6169:a058:a5ff:fe05:c786

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.

**Answer:**

For **mx0b-001b2d01.pphosted.com**

my-addr.com/email\_server\_location/e-mail\_box\_server\_location/locate\_email\_address\_for\_free.php?e

clients. Messages can also be retrieved using a web browser if the server hosts a suitable service.

Ads by Google   GPS Tracker   Free Email Checker   I Want to See My Emails

Don't forget that **email address location** tool showing info about email box geographic location, it can be not linked with real "sender" geographic location.

enter E-MAIL here   Go   new window: ☐

Ads by Google   I Want to See My Emails   Geo IP Location   Create a Email Account

**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

SPONSORED SEARCHES ⓘ

Email Address Lookup

Location Tracker

Copyright © 2020 **My-Addr.com**  
This website contains information about host's, ip's, geo's, dns, visitor's full information, ping and trace tools.  
All rights reserved

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

my-addr.com/email\_server\_location/e-mail\_box\_server\_location/locate\_email\_address\_for\_free.php?e

Verify E-MAIL for exist  
Trace E-MAIL sender location  
Find E-MAIL box location  
DNS and WHOIS tools  
Find e-mail/domain MX  
Domain lookup NS records  
Domain A record Lookup  
PTR lookup  
Domain DNS Lookup  
Domain WHOIS info Lookup  
Advanced WHOIS Lookup Tool  
Custom IP info, reverse lookup  
IP info Lookup  
Reverse Lookup  
IP/Domain/Url Trace-Ping tools  
Trace DOMAIN/IP  
Online Ping  
Check/Search Ports tools  
Check PORTS for DOMAIN/IP  
Search PORT description

SPONSORED SEARCHES  
Email Address Lookup  
Location Tracker

clients. Messages can also be retrieved using a web browser if the server hosts a suitable service.

Ads by GoogleGPS TrackerI Want to See My EmailsFree Email Checker

SONY  
Sony Center  
is now online  
www.shopatSC.com

SONY WIRELESS  
HEADPHONES AND BLUETOOTH SPEAKERS  
FOR WORK FROM HOME  
Shop Now

SAVE Up to **33%**  
off  
on Audio Products.  
\*Conditions apply

Don't forget that **email address location** tool showing info about email box geographic location, it can be not linked with real "sender" geographic location.

enter E-MAIL hereGo new window: ☐

Ads by GoogleI Want to See My EmailsGeo IP LocationSetup My Email

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

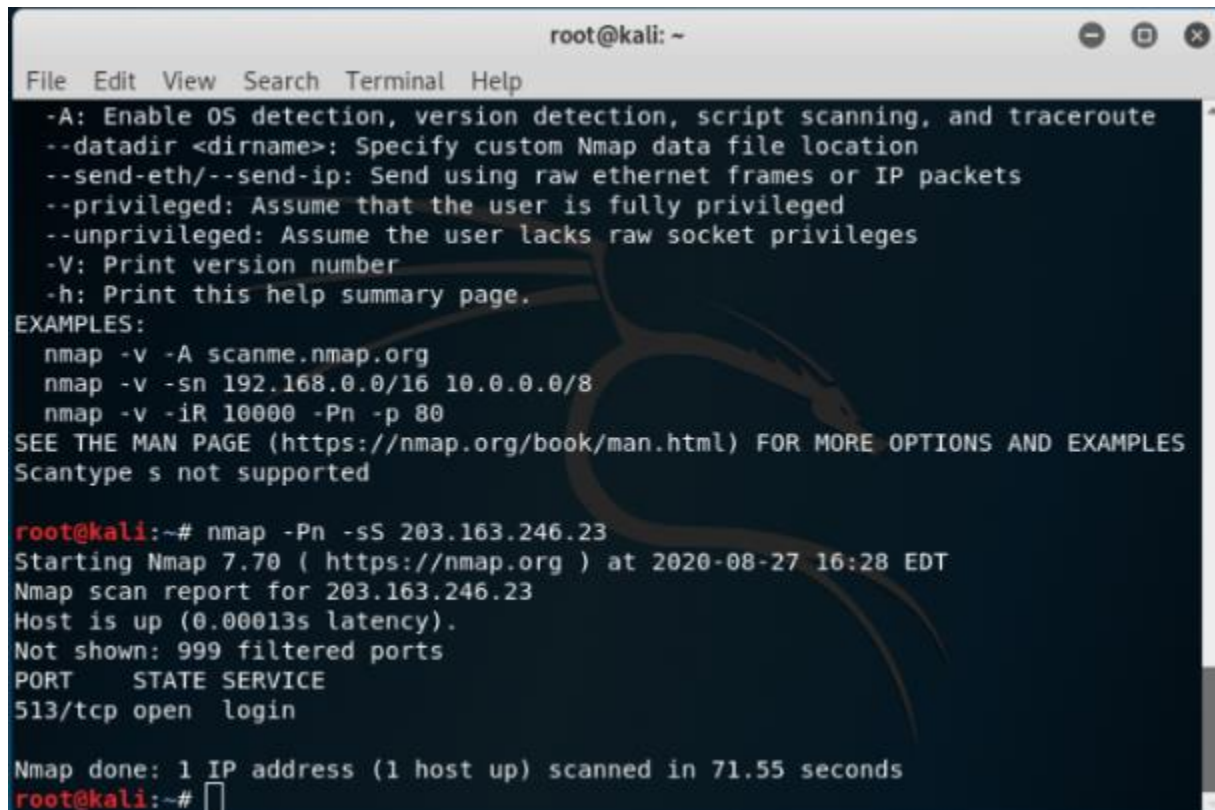
Copyright © 2020 My-Addr.com  
This website contains information about host's, ip's, geo's, dns, visitor's full information, ping and trace tools.  
All rights reserved

### Question 3:

Scan and find out port numbers open 203.163.246.23

**Answer:**

**>nmap -Pn -sS 203.163.246.23**



```
root@kali: ~  
File Edit View Search Terminal Help  
-A: Enable OS detection, version detection, script scanning, and traceroute  
--datadir <dirname>: Specify custom Nmap data file location  
--send-eth/--send-ip: Send using raw ethernet frames or IP packets  
--privileged: Assume that the user is fully privileged  
--unprivileged: Assume the user lacks raw socket privileges  
-V: Print version number  
-h: Print this help summary page.  
EXAMPLES:  
nmap -v -A scanme.nmap.org  
nmap -v -sn 192.168.0.0/16 10.0.0.0/8  
nmap -v -iR 10000 -Pn -p 80  
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES  
Scantype s not supported  
  
root@kali:~# nmap -Pn -sS 203.163.246.23  
Starting Nmap 7.70 ( https://nmap.org ) at 2020-08-27 16:28 EDT  
Nmap scan report for 203.163.246.23  
Host is up (0.00013s latency).  
Not shown: 999 filtered ports  
PORT      STATE SERVICE  
513/tcp   open  login  
  
Nmap done: 1 IP address (1 host up) scanned in 71.55 seconds  
root@kali:~#
```

#### Question 4:

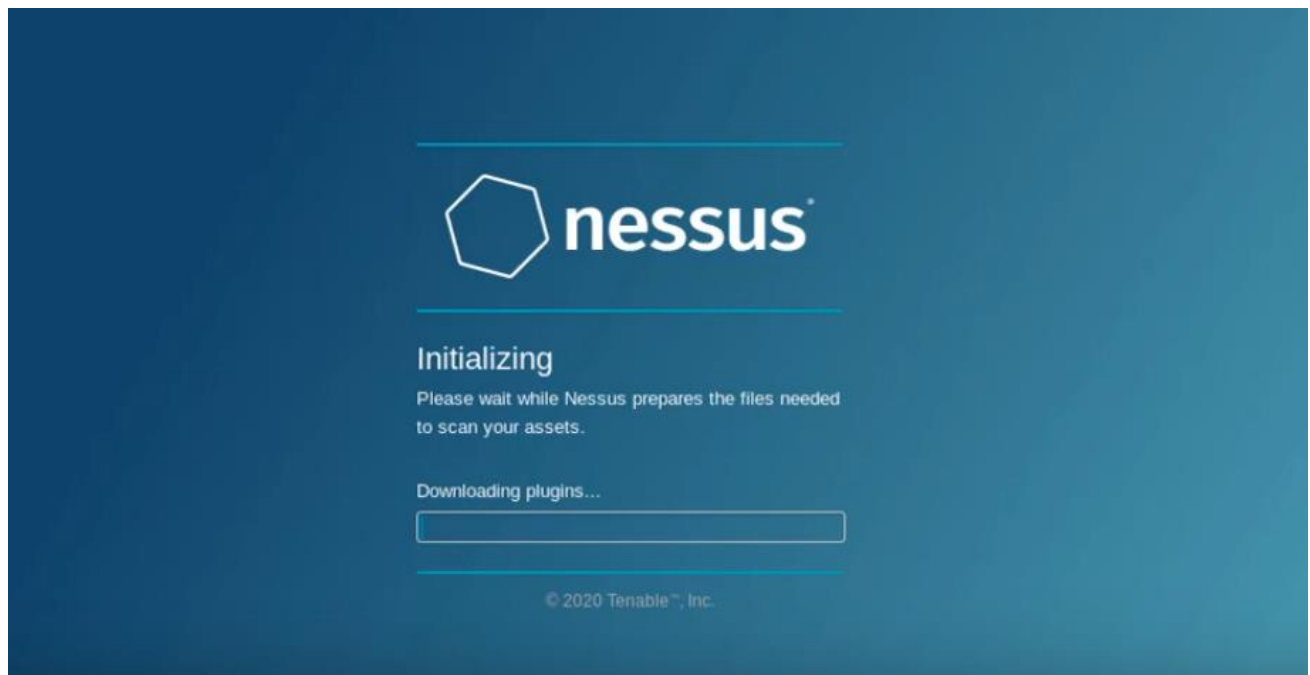
Install nessus in a VM and scan your laptop/desktop for CVE.

**Answer:**

```
root@kali: ~/Downloads
File Edit View Search Terminal Help
root@kali:~/Downloads# ls
Nessus-8.9.0-debian6_amd64.deb
root@kali:~/Downloads# dpkg -i "Nessus-8.9.0-debian6_amd64.deb"
Selecting previously unselected package nessus.
(Reading database ... 341450 files and directories currently installed.)
Preparing to unpack Nessus-8.9.0-debian6_amd64.deb ...
Unpacking nessus (8.9.0) ...
Setting up nessus (8.9.0) ...
Unpacking Nessus Scanner Core Components...

- You can start Nessus Scanner by typing /etc/init.d/nessusd start
- Then go to https://kali:8834/ to configure your scanner

Processing triggers for systemd (239-7) ...
root@kali:~/Downloads# /etc/init.d/nessusd start
Starting Nessus : .
root@kali:~/Downloads# https://kali:8834/
```



[← Back to My Scans](#)

Configure

Hosts 5 Vulnerabilities 12 History 1

Filter ▾ Search Hosts 🔍 5 Hosts

Host	Vulnerabilities	%
192.168.1.5	31 (100.00%)	0%
192.168.1.6	26	0%
192.168.1.2	13	0%
192.168.1.4	10	0%
192.168.1.1	6	4%

### Scan Details

Name: 192.168.1.0/24 Subnet  
Status: Running  
Policy: Advanced Scan  
Scanner: Local Scanner  
Start: Today at 11:31 PM

## Vulnerabilities

