

Question 1: Find out the mail servers of the following domain :

IBM.com

Wipro.com

Ans:



```
Applications ▾ Places ▾ Terminal ▾
Thu 19:12
root@kali:~#
root@kali:~# nslookup
> settype:mx
Server:      192.168.42.129
Address:    192.168.42.129#53

** server can't find settype:mx: NXDOMAIN
> www.ibm.com
Server:      192.168.42.129
Address:    192.168.42.129#53

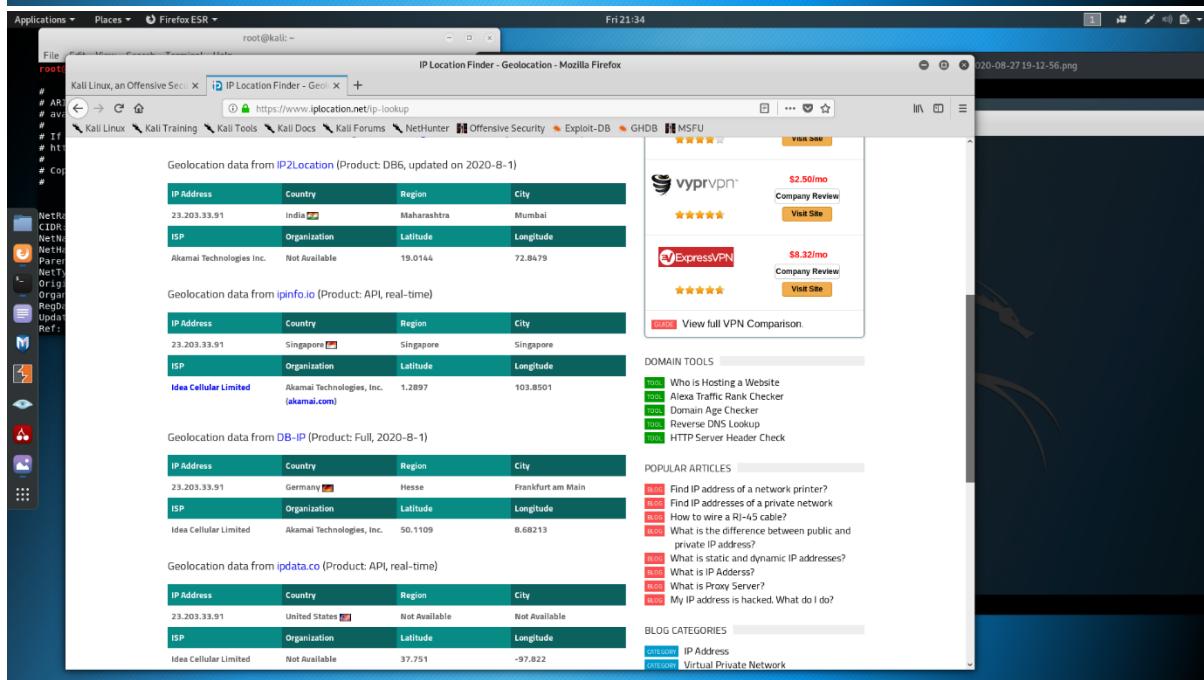
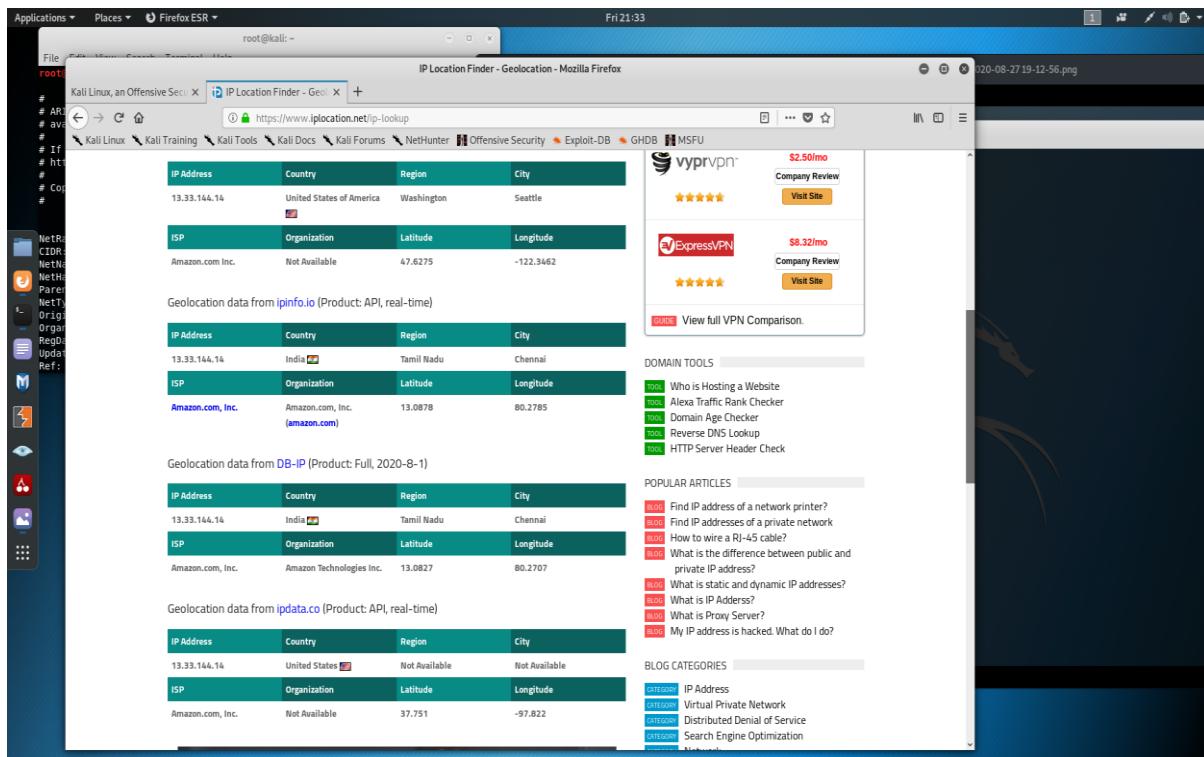
Non-authoritative answer:
www.ibm.com canonical name = www.ibm.com.cs186.net.
www.ibm.com.cs186.net canonical name = outer-ccdn-dual.ibmcom.edgekey.net.
outer-ccdn-dual.ibmcom.edgekey.net canonical name = outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net.
outer-ccdn-dual.ibmcom.edgekey.net.globalredir.akadns.net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

Name:   e2874.dspx.akamaiedge.net
Name:   2400:700:100:1:84:b3a
Name:   e2874.dspx.akamaiedge.net
Address: 2400:700:100:1:86:b3a
> www.wipro.com
Server:      192.168.42.129
Address:    192.168.42.129#53

Non-authoritative answer:
www.wipro.com canonical name = d361nq33s63ex.cloudfront.net.
Name:   d361nq33s63ex.cloudfront.net
Address: 13.33.144.14
Name:   d361nq33s63ex.cloudfront.net
Address: 13.33.144.107
Name:   d361nq33s63ex.cloudfront.net
Address: 13.33.144.114
Name:   d361nq33s63ex.cloudfront.net
Address: 2609:9000:20b:0:13:4f33:b240:93a1
> []
```

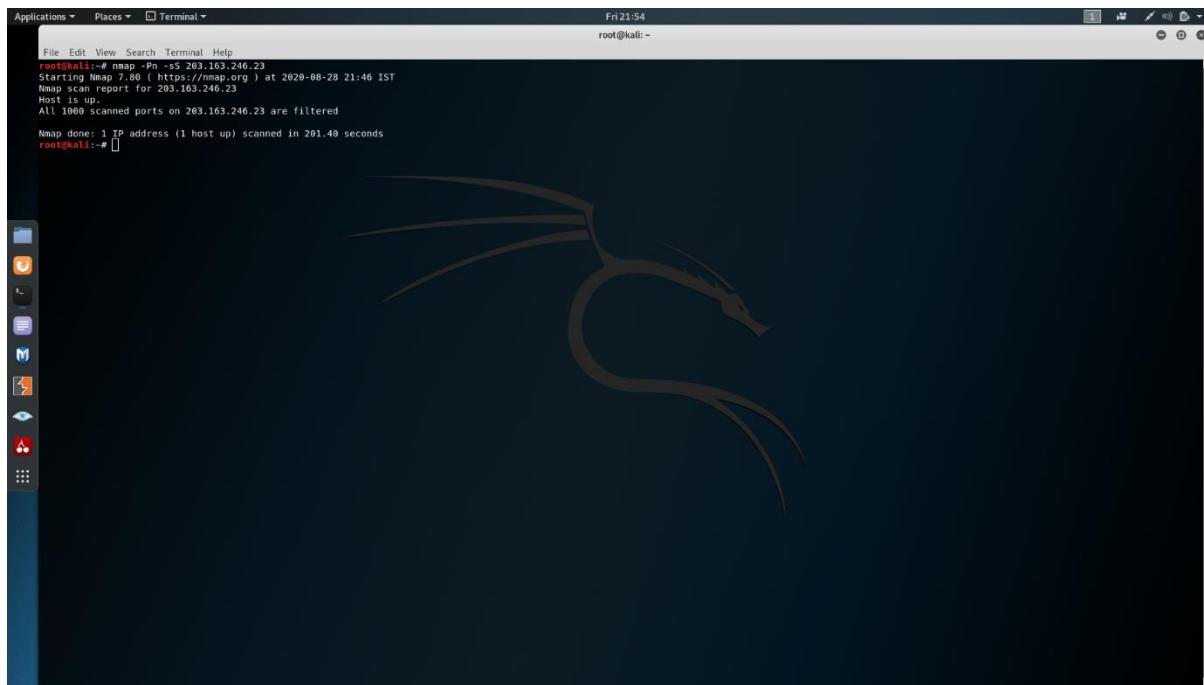
Question 2: Find the locations, where these email servers are hosted

Answer



Question 3: Scan and find out port numbers open
203.163.246.23

Ans



Here all the ports are filtered so we cannot get the open ports using nmap

Question 4: Install nessus in a VM and scan your laptop/desktop for CVE

Ans:

A screenshot of the Nessus Essentials web interface. The top navigation bar shows tabs for 'Nessus Essentials / Login', 'Nessus Essentials / Folders / View', and 'windows'. The main content area shows a scan named 'windows' with one host, 192.168.159.129, which has 31 vulnerabilities found. The 'Scan Details' panel on the right shows the scan was completed locally today at 2:58 PM. A 'Vulnerabilities' section includes a pie chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).