ASSIGNMENT DAY 4:

Question 1:

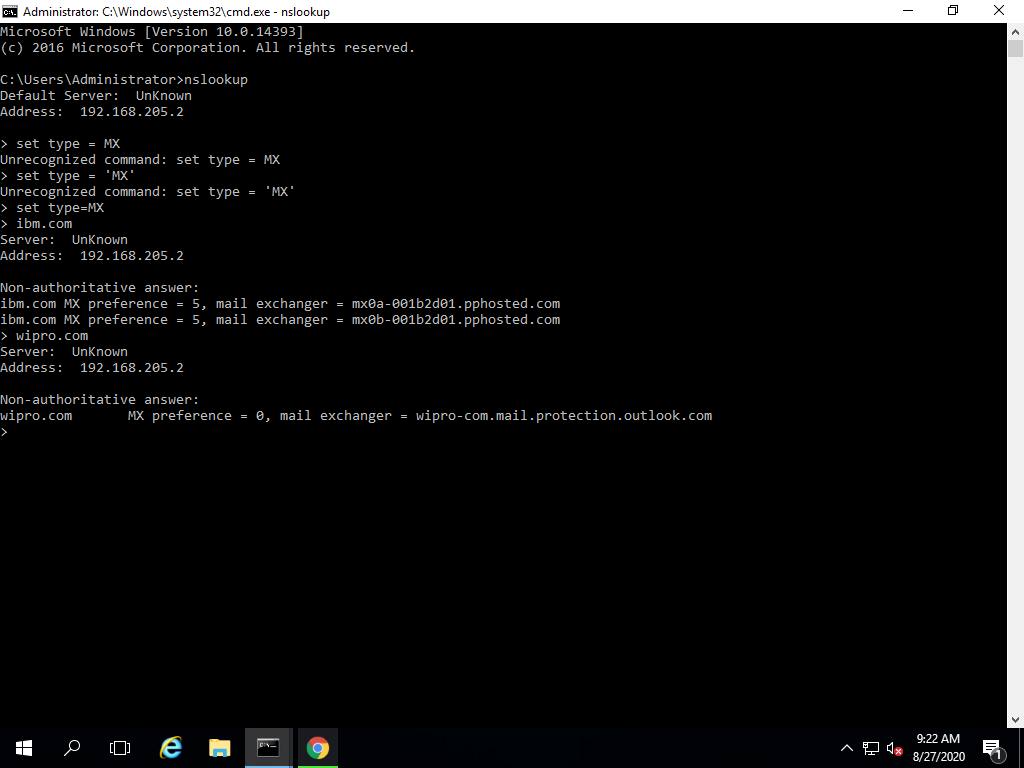
Find out the mail servers of the following domain :

Ibm.com

Wipro.com

Answer:

First we open command prompt. Then we write the command nslookup. After that we have to set the type to mail exchange by using the command set type=MX. After its done we can start to look the mail servers of the given domain. We searched for the mail servers of ibm.com and wipro.com and the result is given below. We got 2 mail servers for ibm and 1 for wipro.

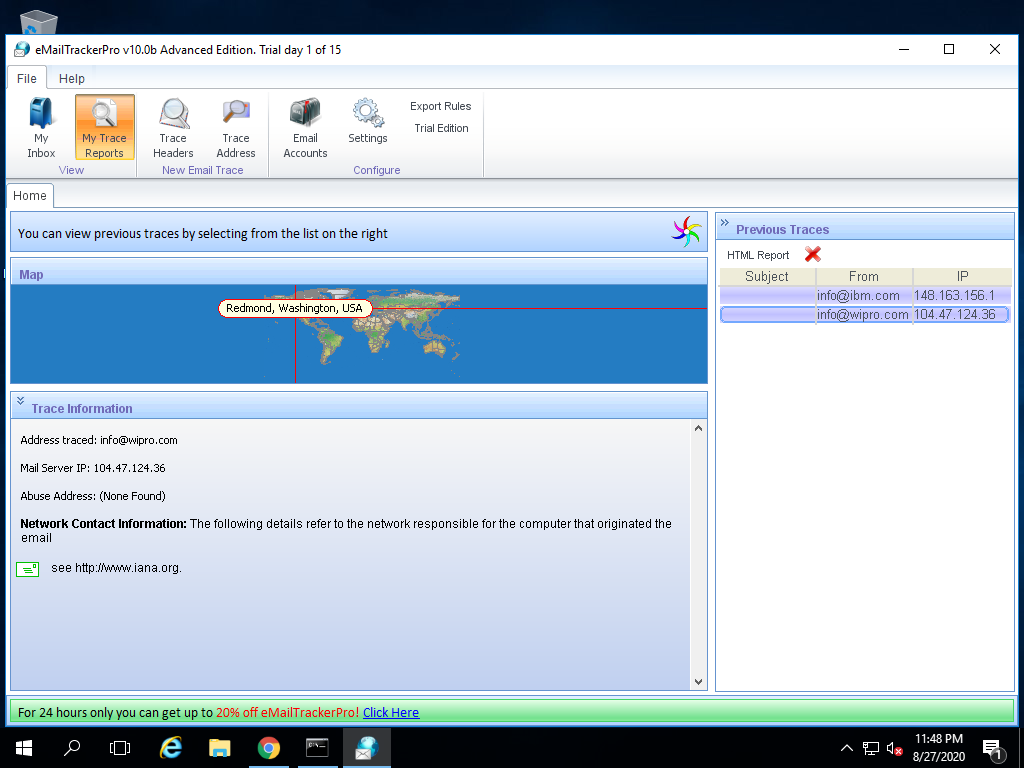


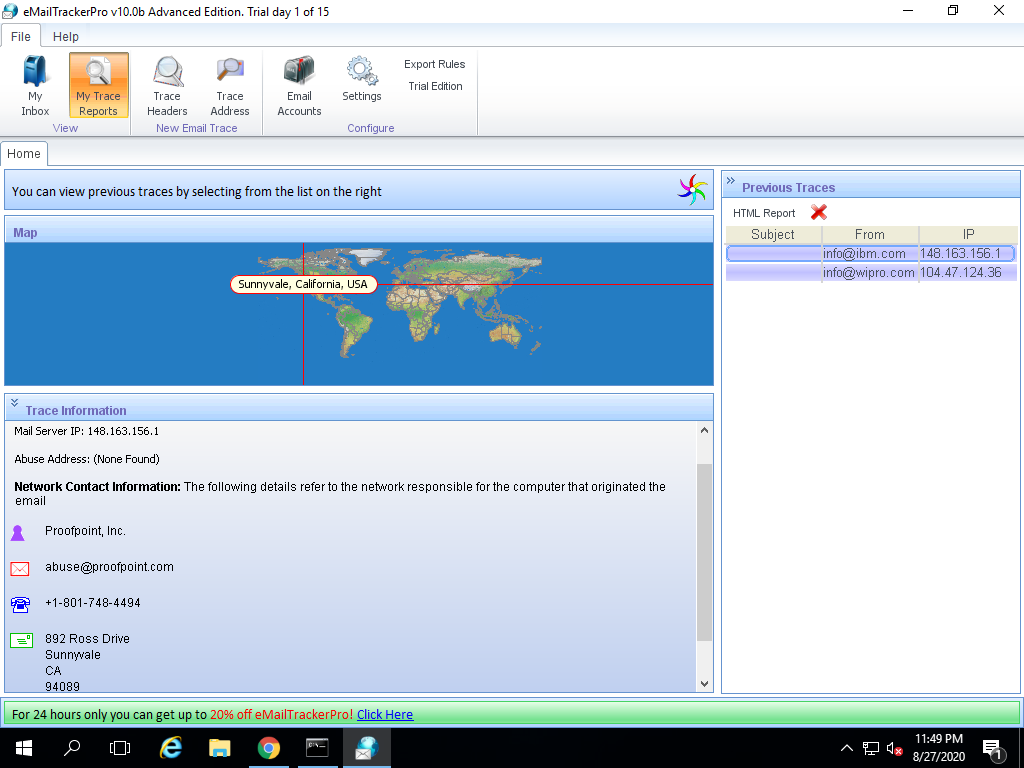
Question 2:

Find the locations, where these email servers are hosted.

Answer:

I have used the eMailTrackerPro to find the locations of the given companies to see where their email servers are hosted. I provided a dummy email with the domain of these companies and the tool immediately located the locations. Wipro’s server is located in Redmond, Washington, USA whereas the location of IBM servers were found to be hosted from Sunnyvale, California, USA. Bunch of other information such as IP addresses, number of hops and various other data was provided in the detailed report.



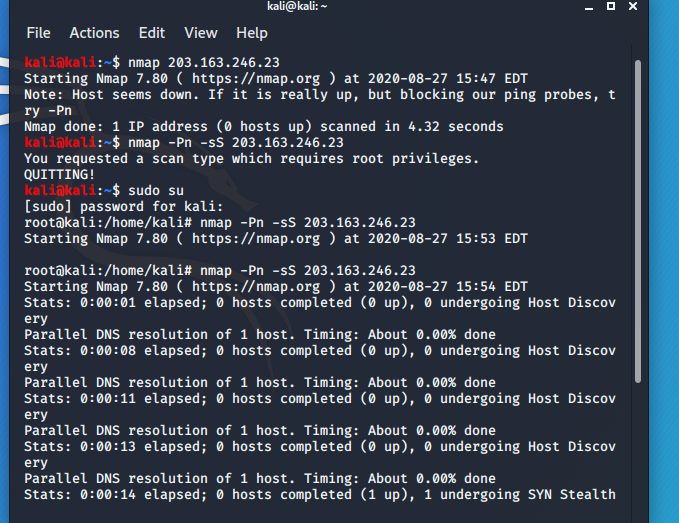


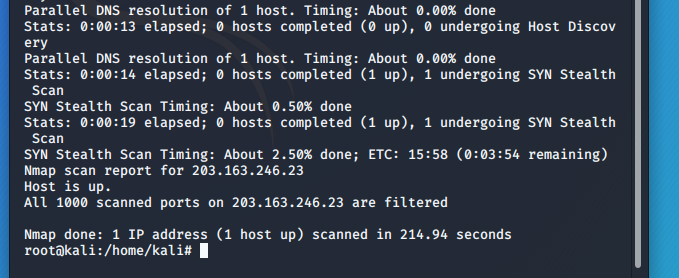
Question 3:

Scan and find out port numbers open 203.163.246.23

Answer:

I used the nmap command in kali linux to scan the given IP address for open ports. I couldn’t get through so I used the Pn command for pinging and sS command for stealth scan. These commands require root privileges. So I used sudo su command for accessing the root. Upon entering the password the nmap started scanning 203.163.246.23. After sometime the scanning was completed and it showed that all 1000 ports were filtered and we won’t be able to see which ports are open.





Question 4:

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

Answer:

I used nessus to scan my windows 2016 for CVE. First I registered on nessus. After registration I was given multiple options such as scanning for web applications or local host. We can also do a quick or advanced scan. I did the advanced scanning option. It took couple of minutes for the scan to be completed but it provided with all the vulnerabilities. I received 10 critical 32 high and 12 medium level vulnerabilities. Below is the detailed report of the scan.

