Lets Upgrade Assignment Day 4

Assignment by: Vishal Monteiro

Email.id : vishalmonteiro056@gmail.com

***Question 1***:

Find out the mail servers of the following domain:

Ibm.com

Wipro.com

***Solution***:

1. Open Pentester, put the password and run as administrator.
2. Right click on windows and open run, type cmd.
3. Type:

set type=mx

Ibm.com

(you will get the mail servers for Ibm.com)

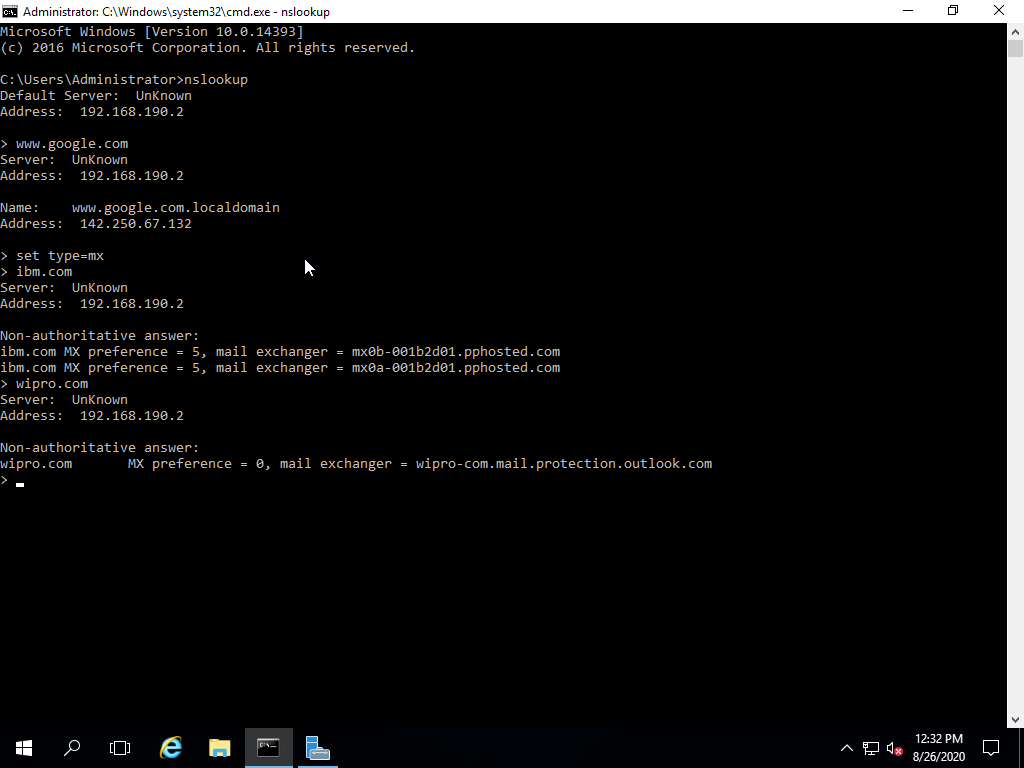
The Mail server for Ibm.com is: mx0b-001b2d01.pphosted.com

set type=mx

Wipro.com

(you will get the mail servers for Wipro.com)

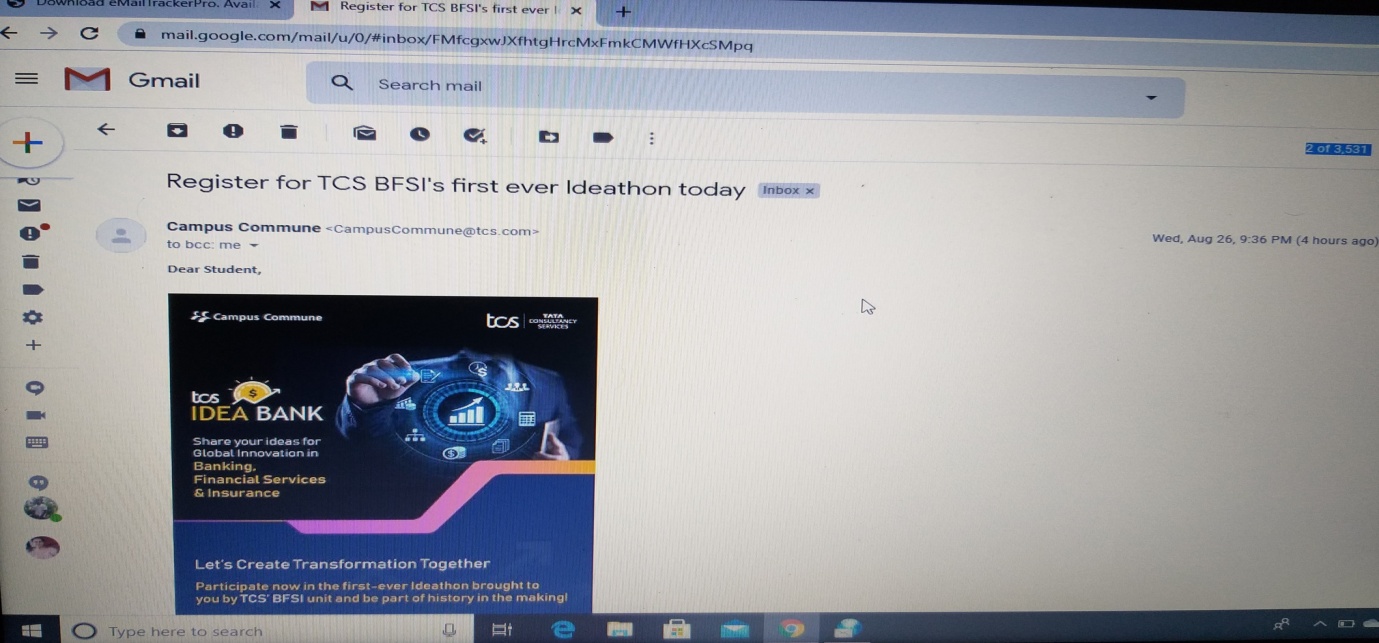
The Mail server for Wipro.com is: wipro-com.mail.protection.outlook.com



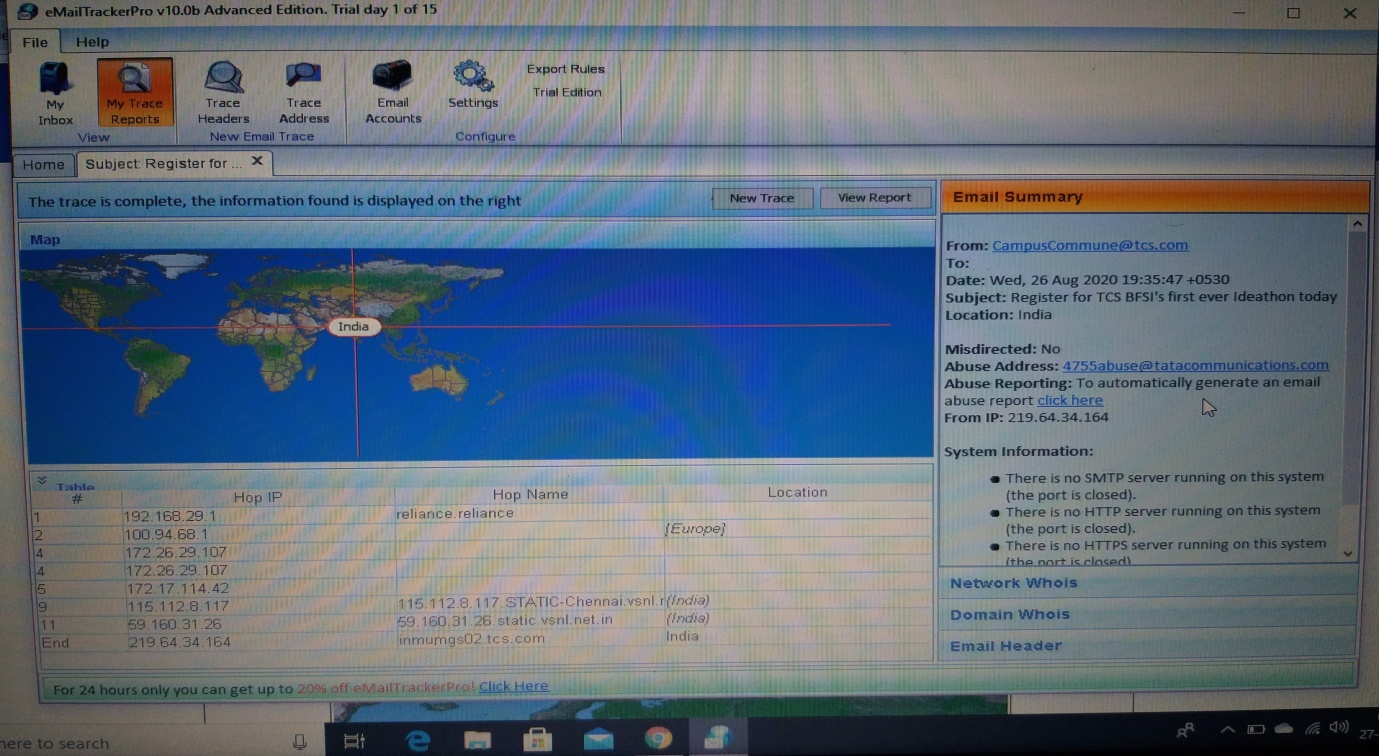
***Question 2:*** Find the locations, where these email servers are hosted.

***Solutions:***

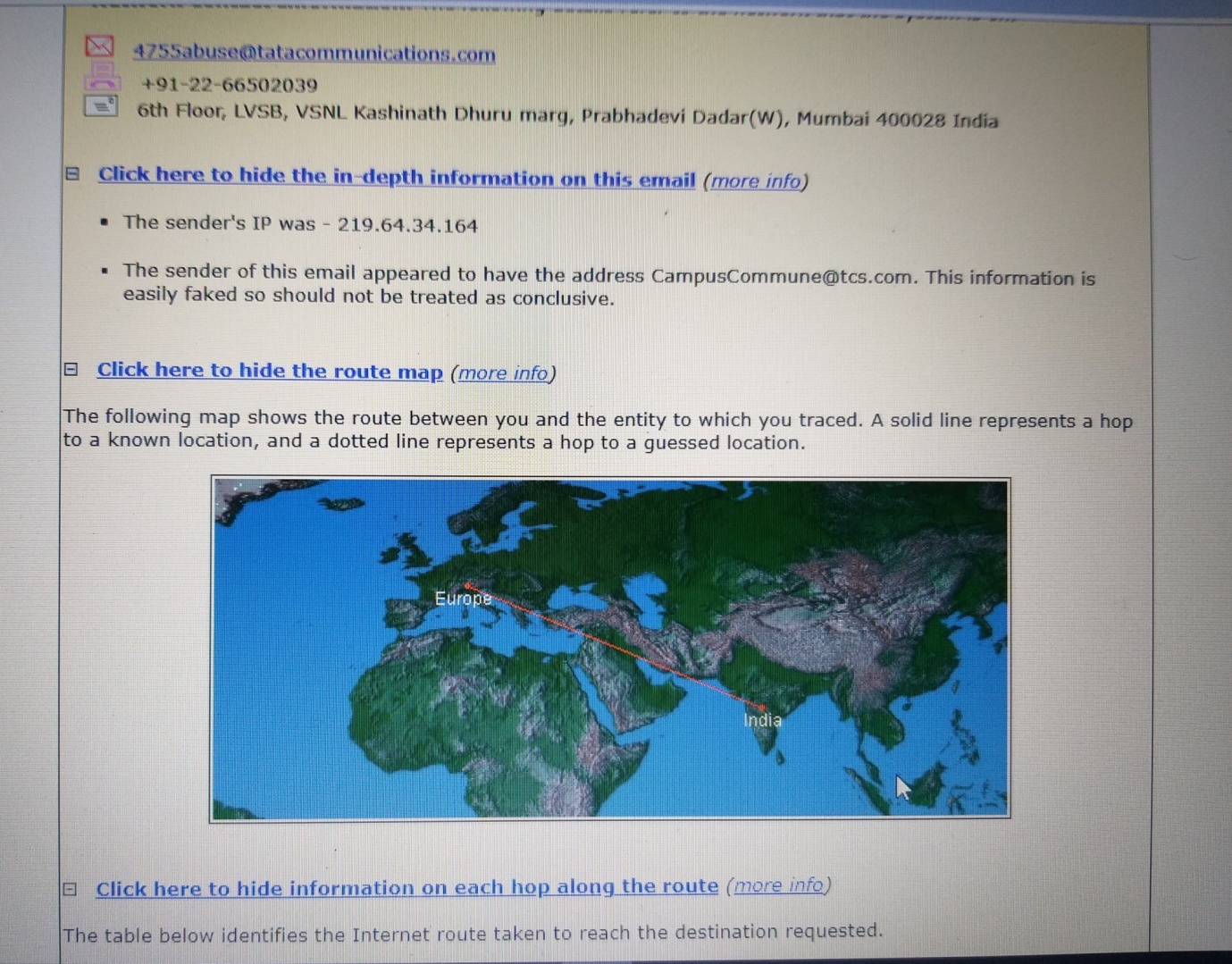
1. Download Chrome from internet explorer
2. Go to Chrome and type **download email tracker pro.**
3. once it is downloaded open any of your mail ( In this case I opened one of my spam mail)

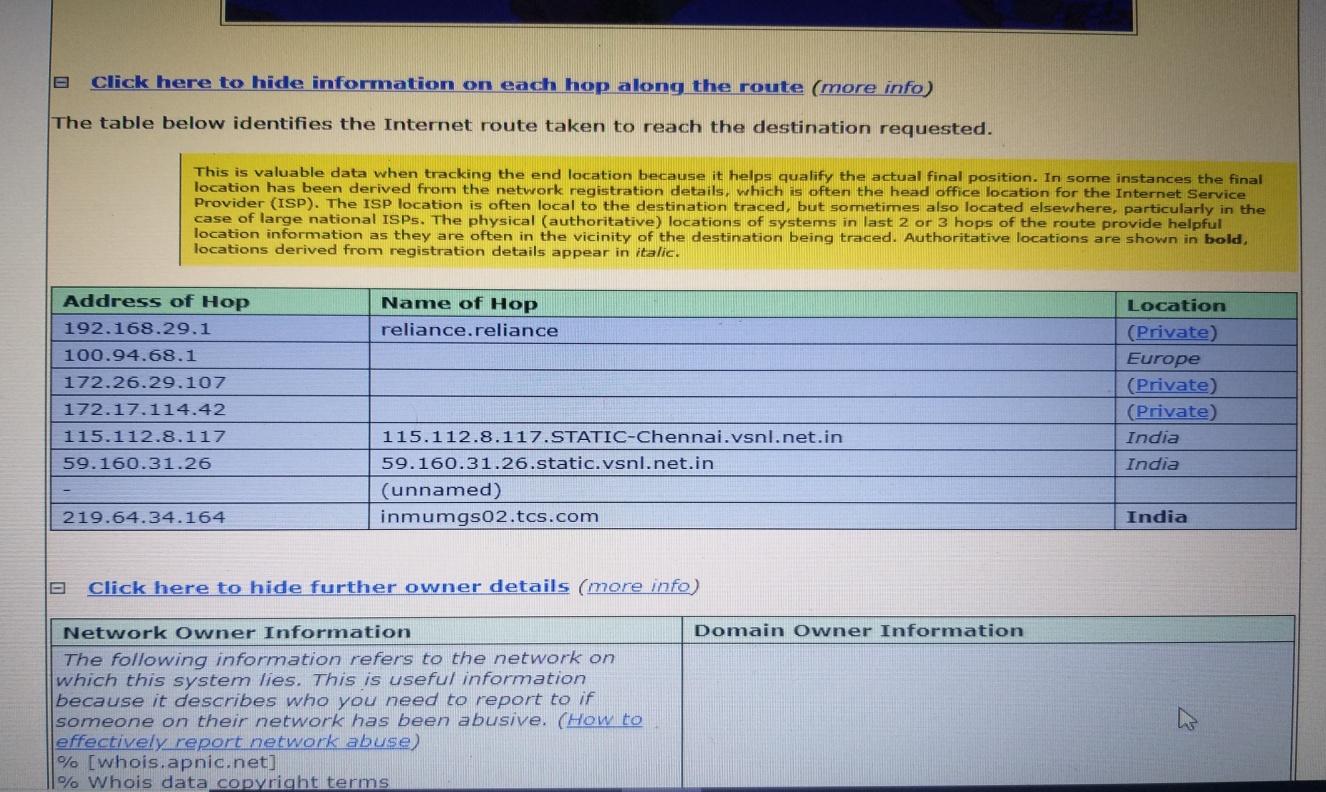


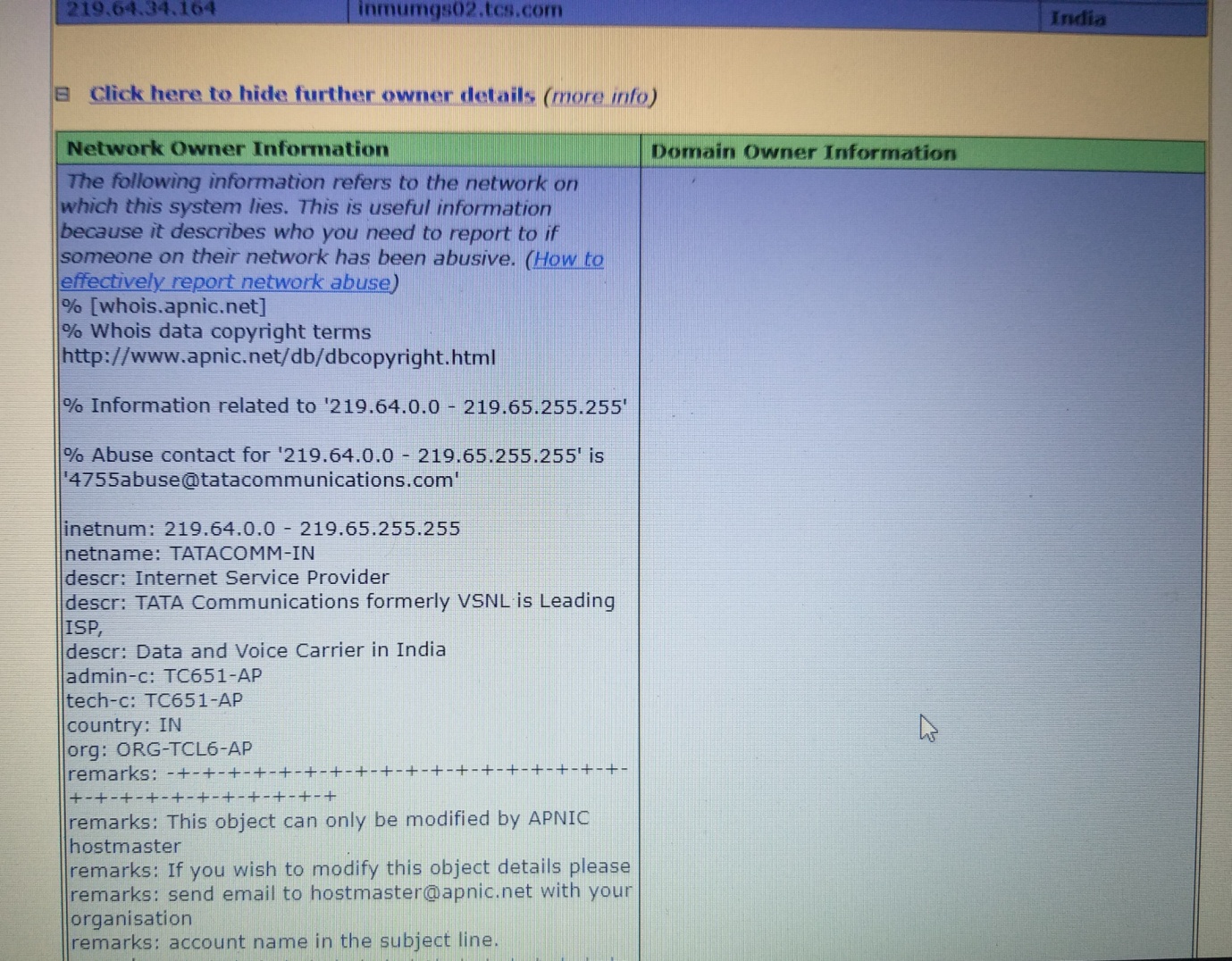
1. click on ‘show original’
2. the once the page is open click on “**copy to clipboard”**
3. simultaneously in email tracker pro, click on 🡪my trace reports the click on 🡪 trace headers
4. click on the email headers box and it gets copied there, click on **Trace.**



1. click on **view report**





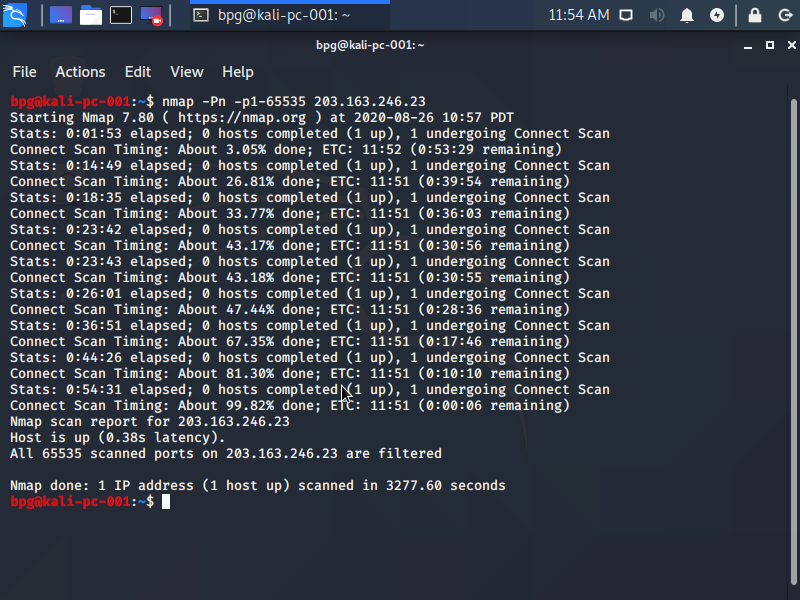


Hence by this method you can track the location from which an Email has been sent.

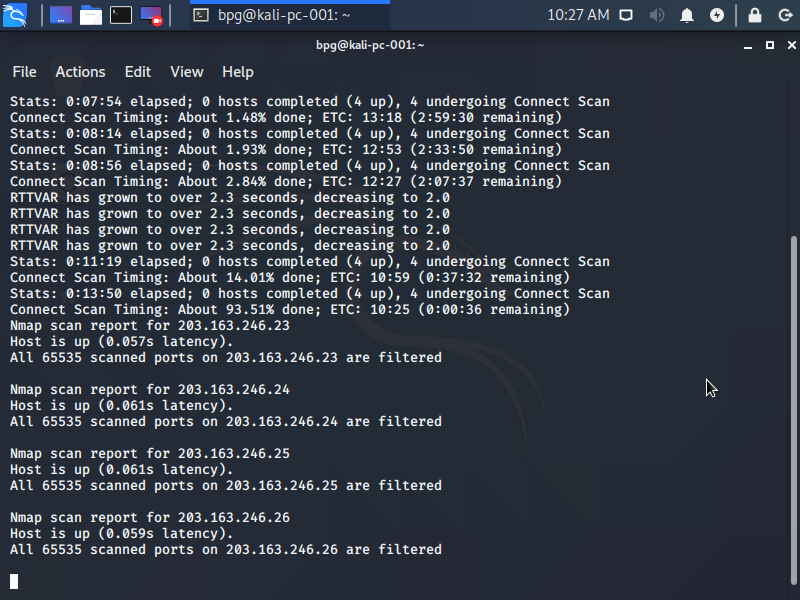
***Question 3:*** Scan and find out port numbers open 203.163.246.23

***Solution:***

1. Open Kali in Vm workstation.
2. Open the terminal and using **nmap** function we can trace out the open ports in an IP address or website.
3. For this we need to type the command **nmap –Pn –p1-65535 203.163.246.23**.



1. If it comes that it is filtered then it means that it is behind a firewall and cannot be accessed.
2. You can even try to find for all the IP addresses from 203.163.246.23-255, by using the command **nmap –Pn –p1-65535 203.163.246.23-255.**



***Question4:*** Install nessus in a VM and scan your laptop/desktop for CVE.

***Solution:***

1. Open Chrome and download nessus, click on localhost8834 and you get a link for where it will direct you to tenable community.
2. From where you can download nessus for free. (you need to have a professional Email ID)
3. Once nessus is opened put in your username and password.
4. Go to 🡪 New scan, and then advanced scan.
5. Name: Domain controller not updated

Targets: write down the IP address

1. The go to credentials and then windows, type in the username and then type in the password, put in the domain
2. Once it is done click on 🡪 Scan, then launch.
3. Once the scan is completed, click on it and you will be able to see the report (vulnarabilities)
4. Click on reports🡪 HTML🡪custom🡪 generate report. And you will get access to the CVE’s.

(AS I do not have a professional email so I could not complete the 4th question properly, I’m really sorry for it and I will try my best to fix it but now as I’m running out of time I’m submitting this assignment, I request you to forgive my mistake and I’m really sorry for the inconvenience caused.\* I will be uploading a picture of CVE that I found in browser)

