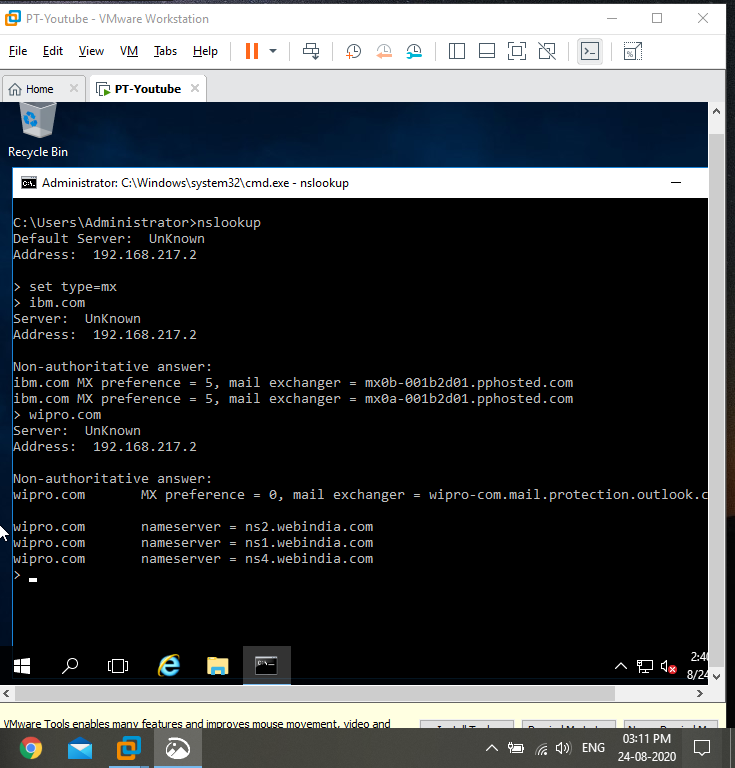
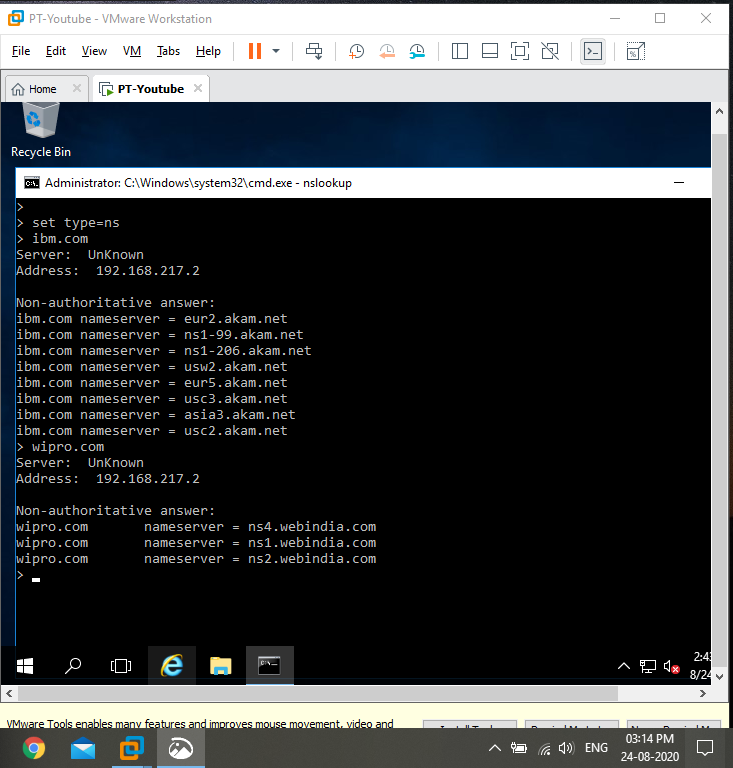
***ASSIGNMENT***

***QUESTION 1***

Find out the mail servers of following domain

Ibm.com

Wipro.com****

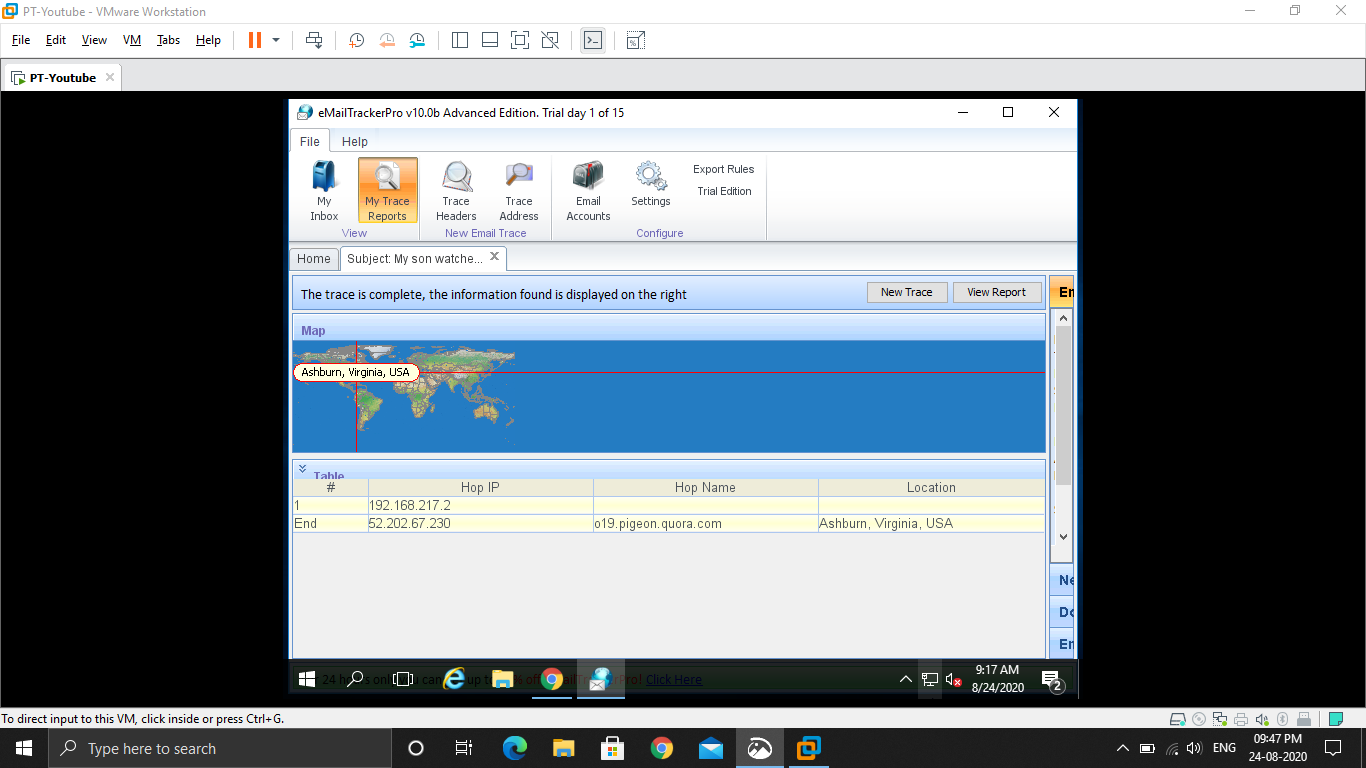
Step1: open vm and pentester windows 2016

Step2: open the cmd prompt

Step3: type the cmd nslookup ,it will give us the address of the website

Step4: type the cmd set type=mx,it will give you the mail server of the particular web address

***QUESTION 2***

Find the location where the mail servers are hosted

Step1: open vm and power on the pentester windows 2016

Step2: enable remote desktop and connect to the remote desktop

Step3: first download the google chrome and install it

Step4: open the chrome, and download email tracker pro then install it

Step5: open the email tracker pro, we can see there standard edition and current edition

Step6: click ok

Step7: and click on my trace reports, then click trace headers

Step8: goto chrome and search gmail and sign in to your gmail account

Step9: goto spam, pick a spam and open it and click on show original

Step10: copy to clip board

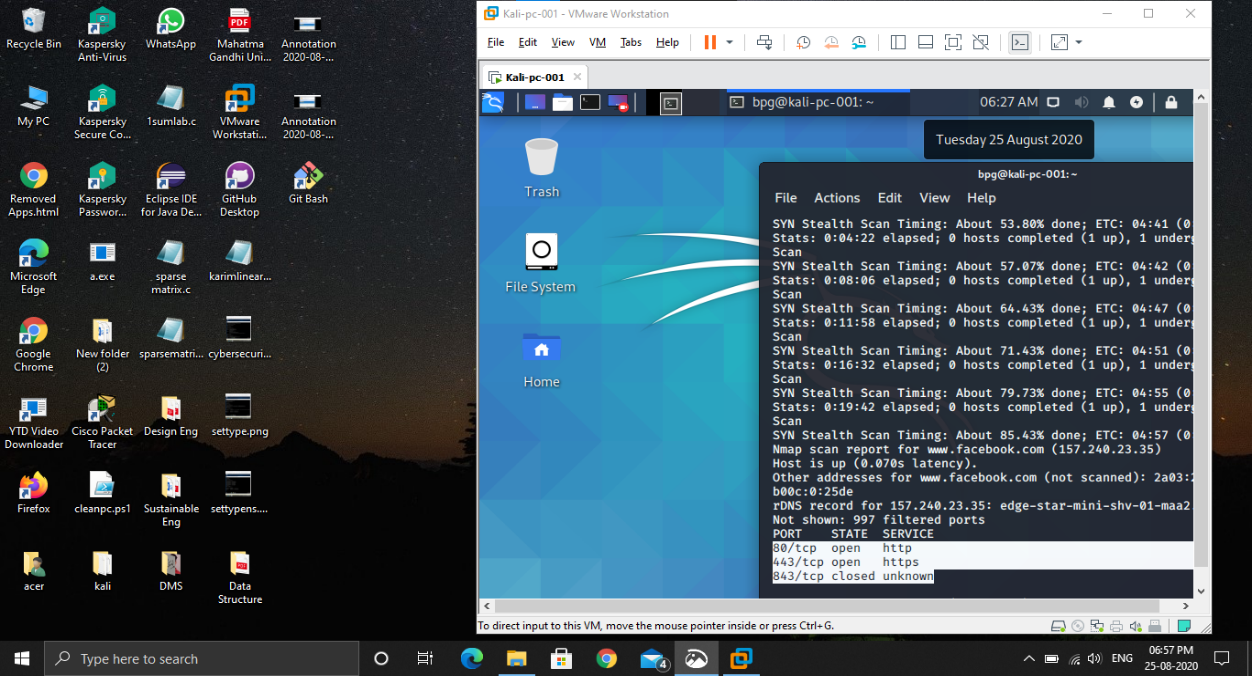
Step11: goto your email tracker pro, then click trace

Step12:it will show where the mail has comes from

Step13: click on view report, then we can collect more details about the mail.

***QUESTION3***

Scan and find out port numbers open 203.163.246.23



Step1: open vm ,and power on kali

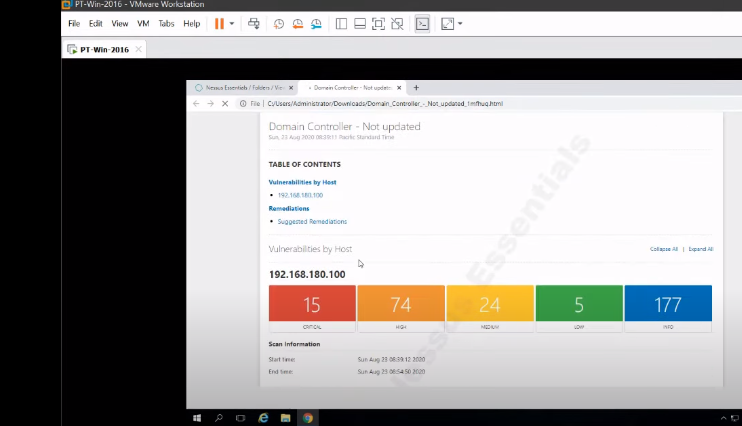
Step2: open cmd in kali

Step3: type nmap -Pn -p1-65535 203.163.246.23

Step 4: it will show us how many ports are open there and which they are.

***QUESTION 4***

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

**

*Step1: open the pentester machine*

*Step2: goto google chrome and search for NESSUS and download it.*

*Step3: you can download it from* [*www.tenable.com*](http://www.tenable.com) *. NESSUS is used for vulnerabity test*

*Step4: click the site address and sign in over there*

*Step5: then open your domain controller, and goto kali*

*Step6: In kali open the cmd .and type sudo su – and type the password.*

*Step7: Then type the command nmap -Pn -sS -A -v <ip address>.This will show you how many ports open in the ip address*

*Step8: goto NESSUS ,and login to it.*

*Step9: goto view scan*

*Step10: goto advanced scan*

*Step11: type the details about the system*

*Step12: goto credentials, goto windows and type the user name, password and domain and launch it.*

*Step13: after the launching, just click on the name and we will see the result over there.*

*Step14: now we can see the different type of vulnerabilities there.to download the reports, click on report and html and click on custom and generate report.*

*Step15: click on the downloaded report, we can see the whole report there .it will shows different CVE there .*