**Day 4 Assignment**

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

**>Ibm.com**

**>Wipro.com**

>The given task is to find the mail servers of given domains

#Step 1 :Open command prompt (press ‘home(windows)+r’ then type ‘cmd’ and press enter)



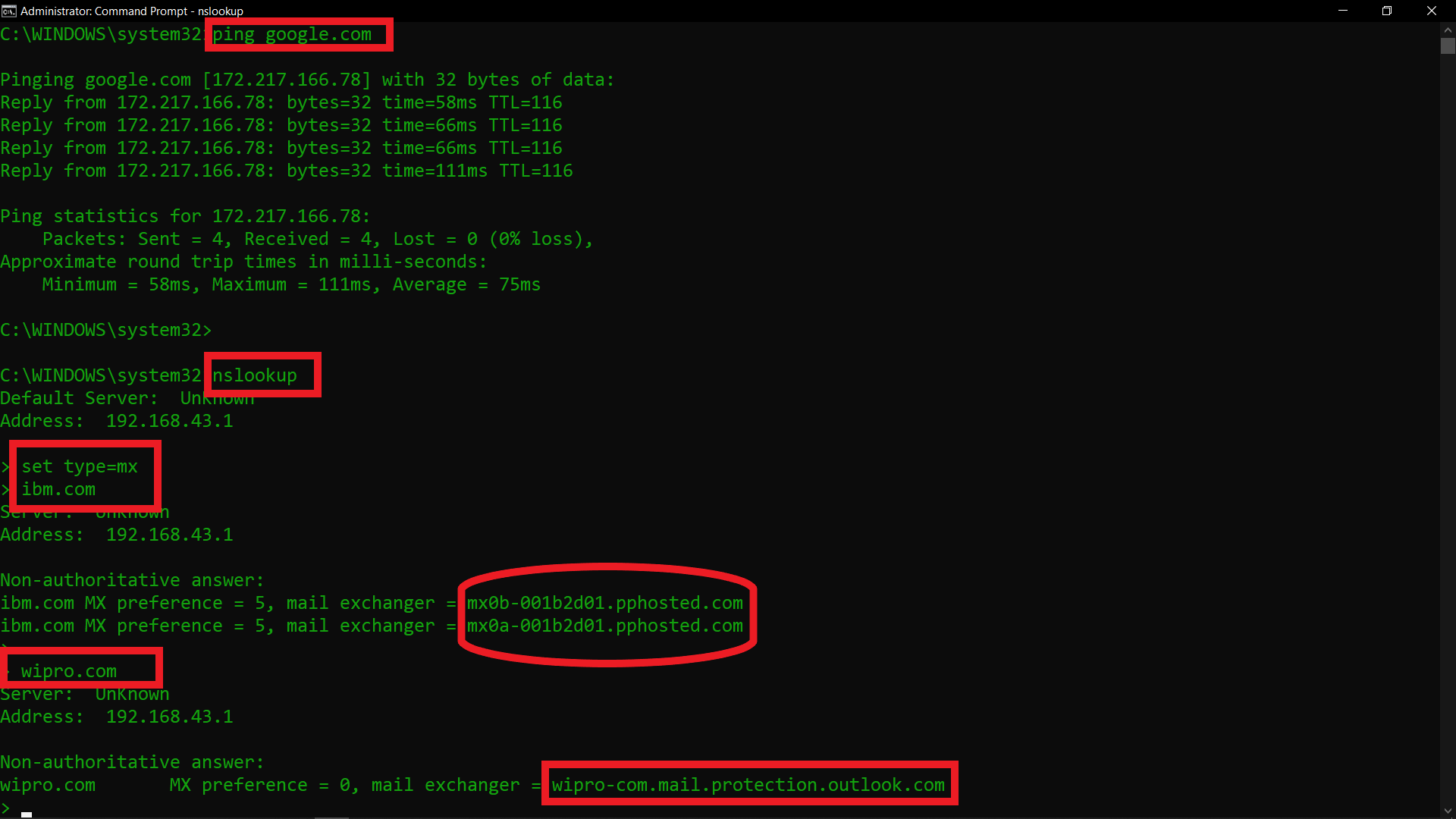
#Step 2 :Make sure that you are connected to a network for results

>To check (ping google.com) . If it pings then continue.

>type “nslookup” ( For querying the Domain Name System to obtain domain name or IP address mapping, or other DNS records)

>To get mail servers (type: set type=mx)

>enter domain name to see the mail servers (eg:ibm.com,wipro.com)



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

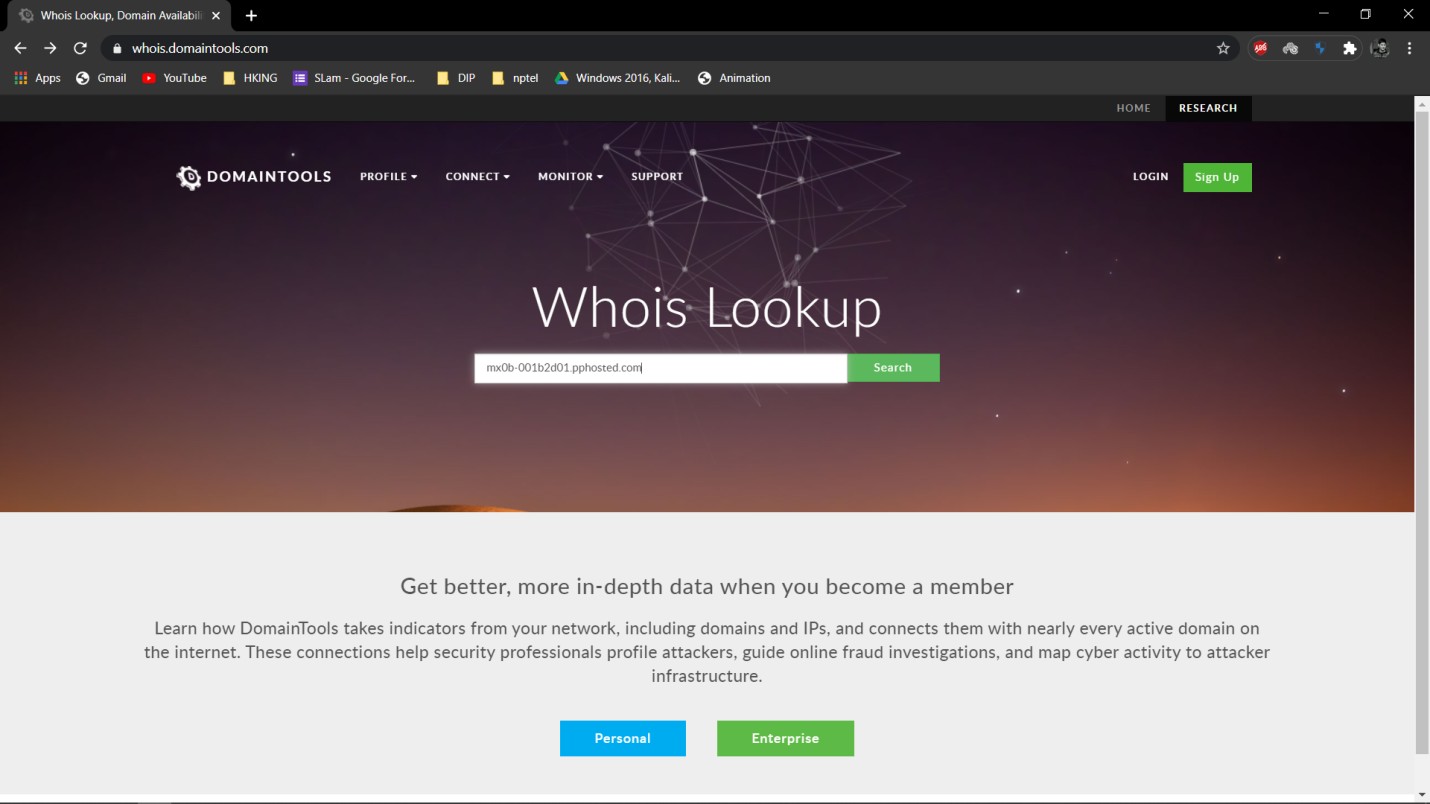
>The given task is to find the location of the mail servers from where they were hosted

>For this task we have many ways in google like iplookup,whoislookup,...etc

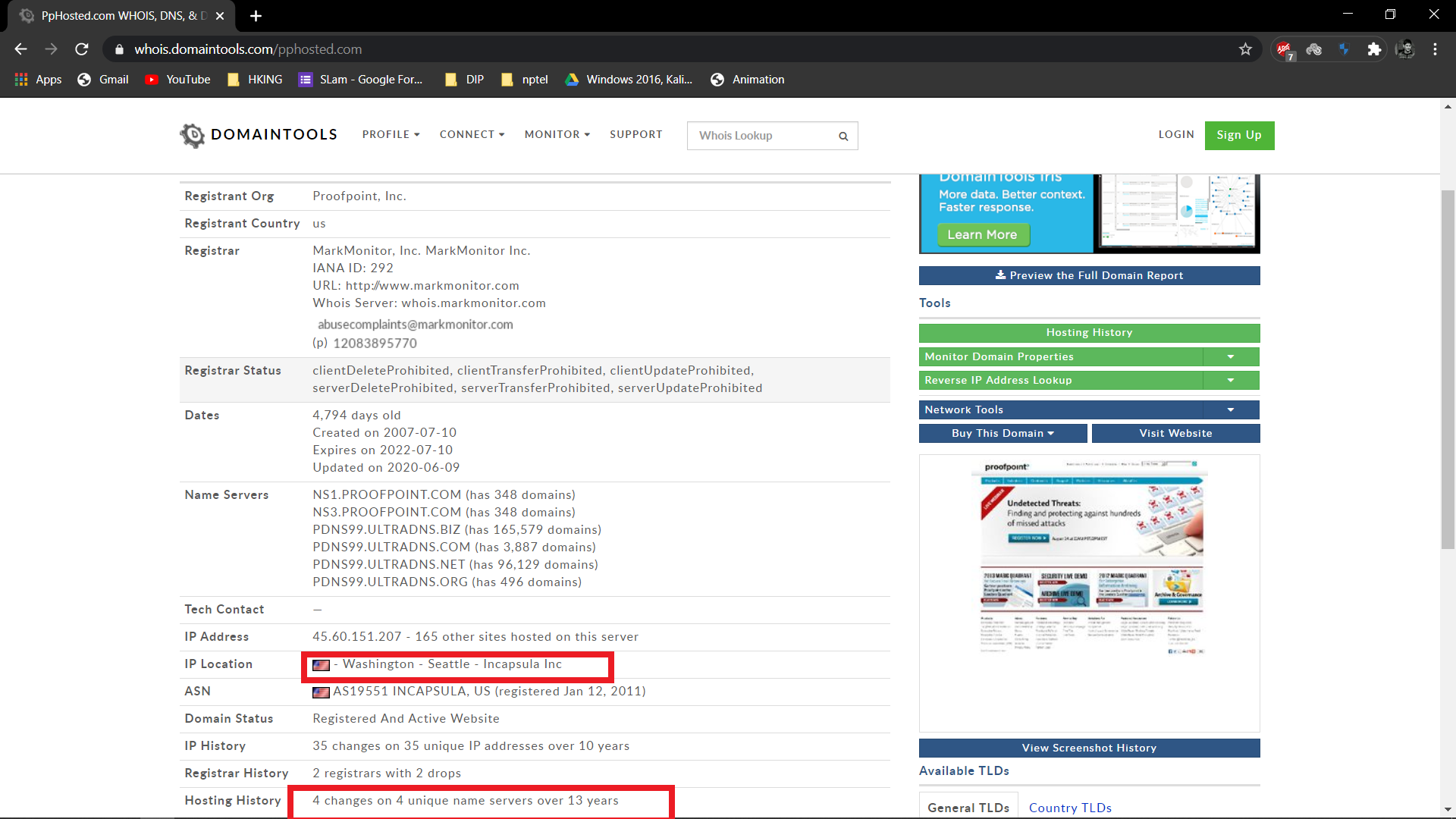
>I’ll go with <https://whois.domaintools.com/>

>Enter the MailServers that you found in the last question

>The web page interface will be as below :



>Complete the ‘reCAPTCHA’ and click on ‘GO’



>Similarly we can also check the Remaining.

**3:scan and find out port numbers open in 203.163.246.23 .**

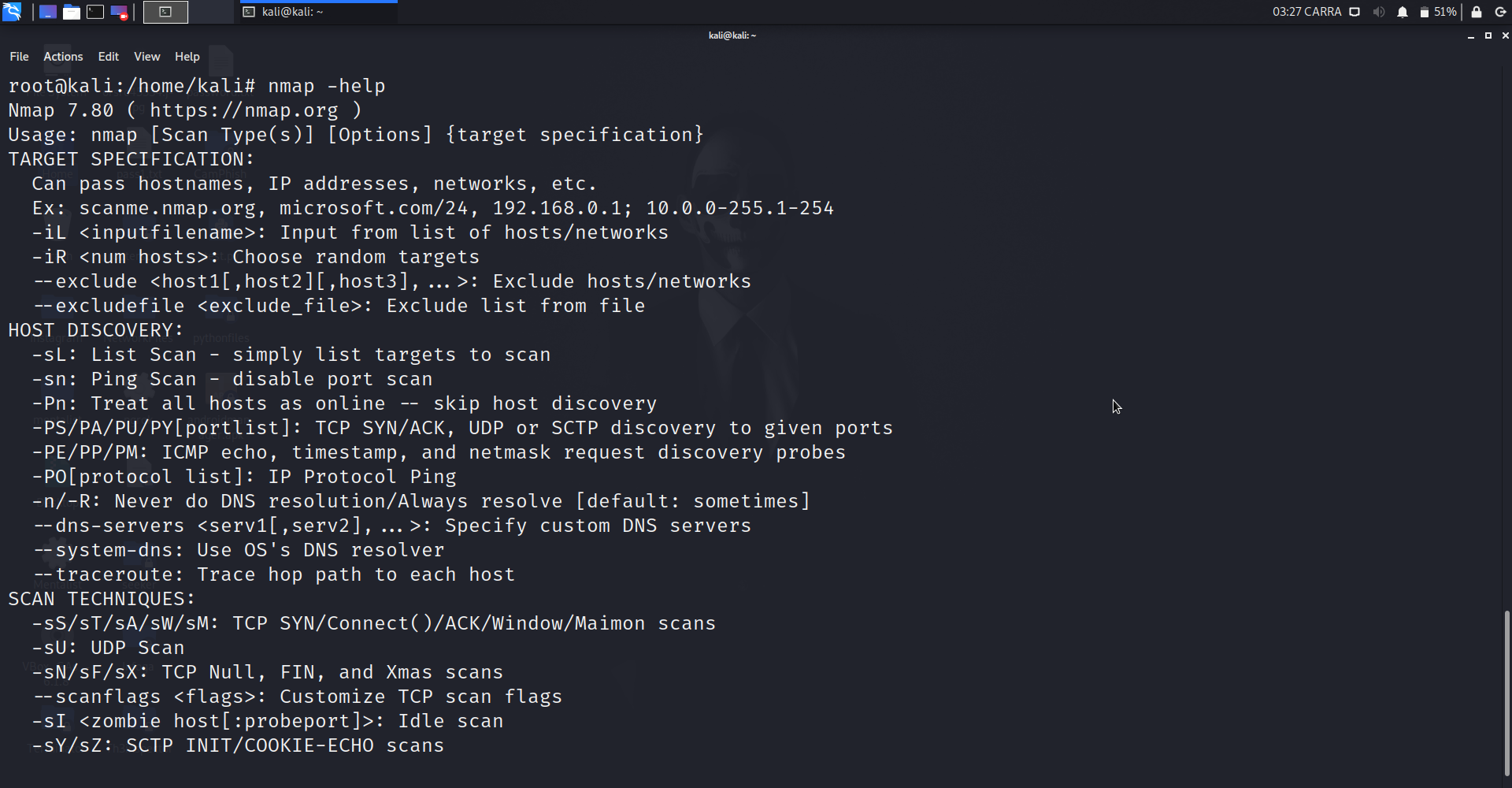
>To complete this task we use “nmap” tool which is a built-in tool in KALI LINUX

>nmap: It is a free and open-source network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and OS detection

>Open terminal (In Kali Linux)

>type ‘sudo su’ (to enter as root user) hit enter and then type your ‘kali\_password’ and hit enter to get the root privileges

> type ‘nmap –help’ to check the options in it.

> Usage : nmap [Scan Type(s)] [Options] {target specification} 

**CMD : nmap 203.163.246.23**

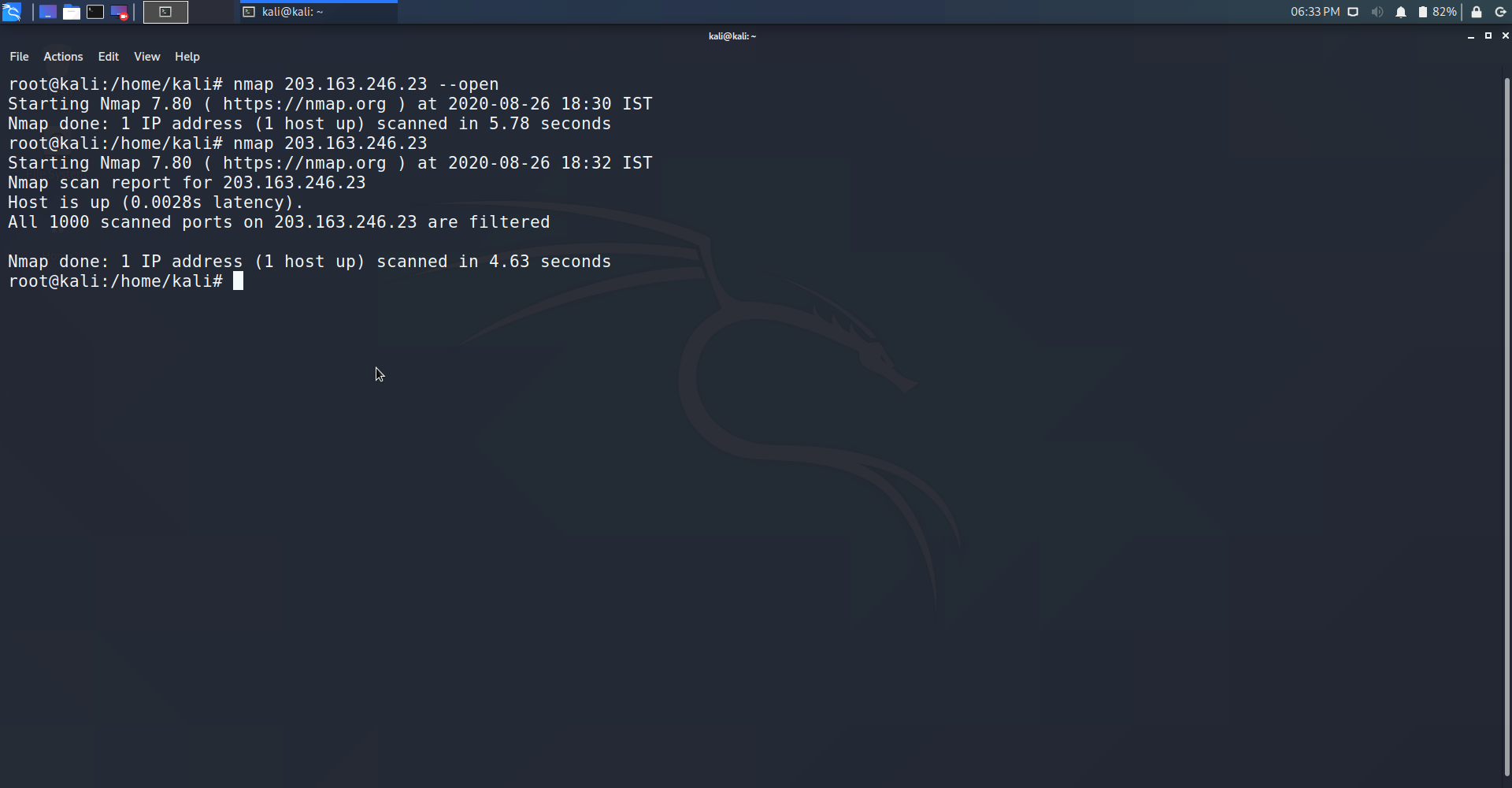
**Actually The About Command is just an normal scan of an ip/domain shows the open ports ....**

**Actually The result is (When i scanned first the open ports are) :**

**# port 80 open http**

**# port 443 open https**

**But later it’s showing all the ports are filtered i think bcoz of the Host seems to be down**



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

>” **Nessus**” is a proprietary vulnerability scanner developed by Tenable,

>” **Nessus**” is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could **use to** gain access to any computer you have connected to a network.

Steps to create a CVE :

>Download NESSUS from <https://www.tenable.com/products/nessus>

> Log in to your Nessus machine : <https://localhost:8834/>

> Click on Scans > Select New Scan

>Choose **Advanced Scan**template.

>Under the scan '**REPORT**' settings, please ensure you have the option **"Hide results from plugins initiated as a dependency"**enabled**.**

>Please also make sure the advanced setting **Auto Enable Plugin Dependencies**and **Silent Plugin Dependencies**are enabled.

> You can find the settings under Settings>Advanced

 >To aim the scan at only specific CVEs you will need to click the 'Plugins' tab, then click "Filter" to create a filter for viewing all of the plugins. Set the filter to "CVE" and then search the specific CVEs you are interested in. You can then enable all of the plugins associated with the CVEs.

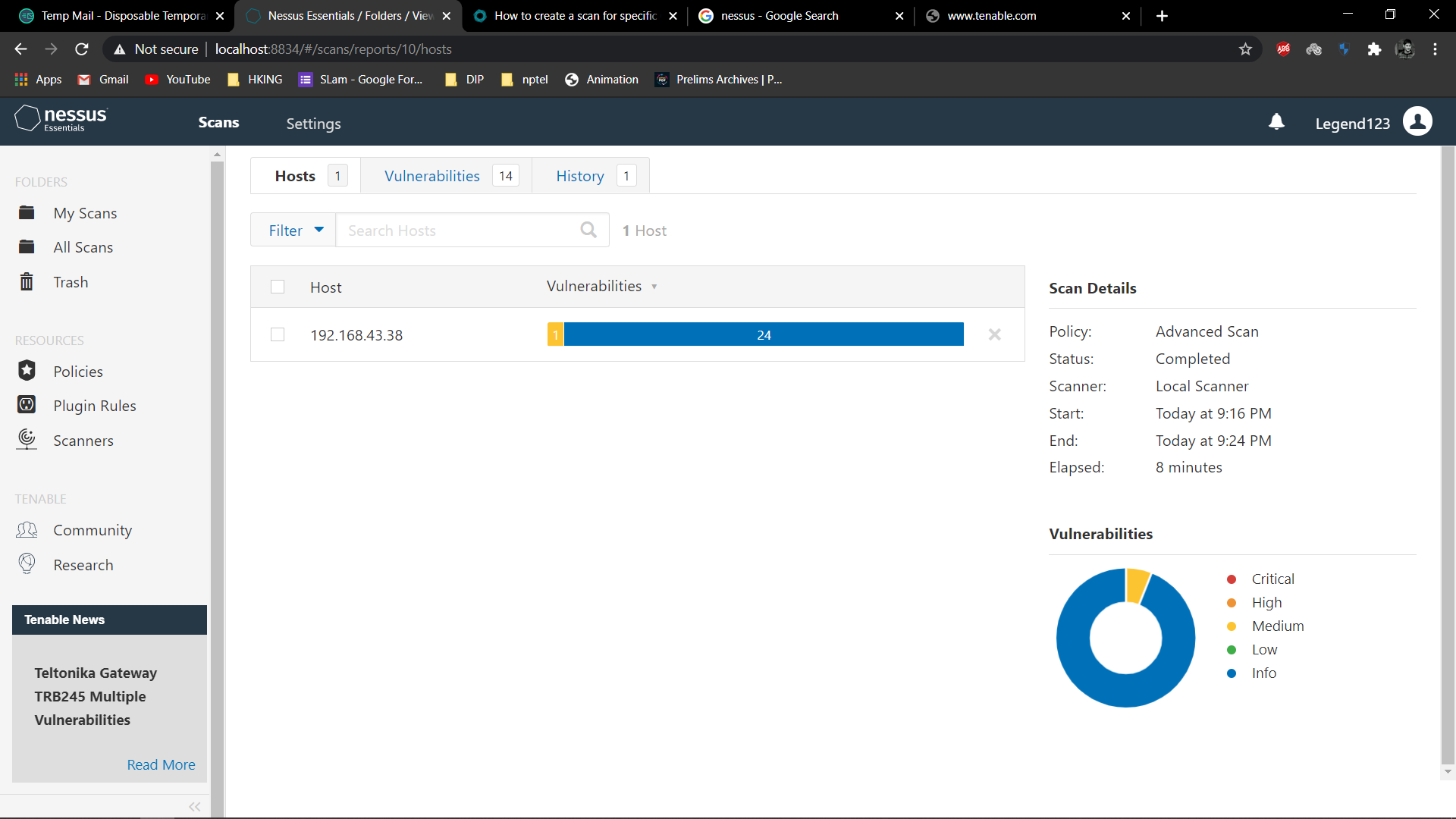
>Goto **Basic** Tab Under this Click On **General**

>Give your report a **name** and **target ip**

>Goto **Credentials** Tab Click on **Windows** Enter your User & Password.

>**Save/Launch** your scan and it will be ready to run

**Below image is my CVE AdvancedScan Report :**



**❖ END ❖**