Exp 7: passive Network rccoonnaince tool

Execute the following commands
-whois <website url>
-dig <website url>
-nslookup <website url>
-traceout <website url>

-> go to archive.org -> enter a web url -> check all the tabs
-> go to whois.com -> in the top right enter the url of the website -> search
-> go to netcraft.com -> **execute at home**

Exp8: ZENMAP

Select Target -> scanme.nmap.org => Profile -> Ping Scan -> Scan -> (Take SS of Ports Topology etc)
-Quick Scan
-Intense Scan

Tells us about the organization, Which ports are active, Topology,

EXPERIMENTB 9 : DDos attack ifconfig

Open terminal -> run the following commands
Hostname -I

(Repeat 2 times)
Sudo hping3 192.168.3.147
Ctrl c

Open new terminal
Execute sudo wireshark
After opening go down to any and click on it

Put the filter ICMP
Stop capturing
Start capturing

In the old terminal execute this commandas
Sudo hping3 192.168.3.147 -1
Open wireshark and observe the packets

In the old terminal execute this commandas
Sudo hping3 192.168.3.147 –fast

Experiment – 10: Study of Intrusion detection system using SNORT

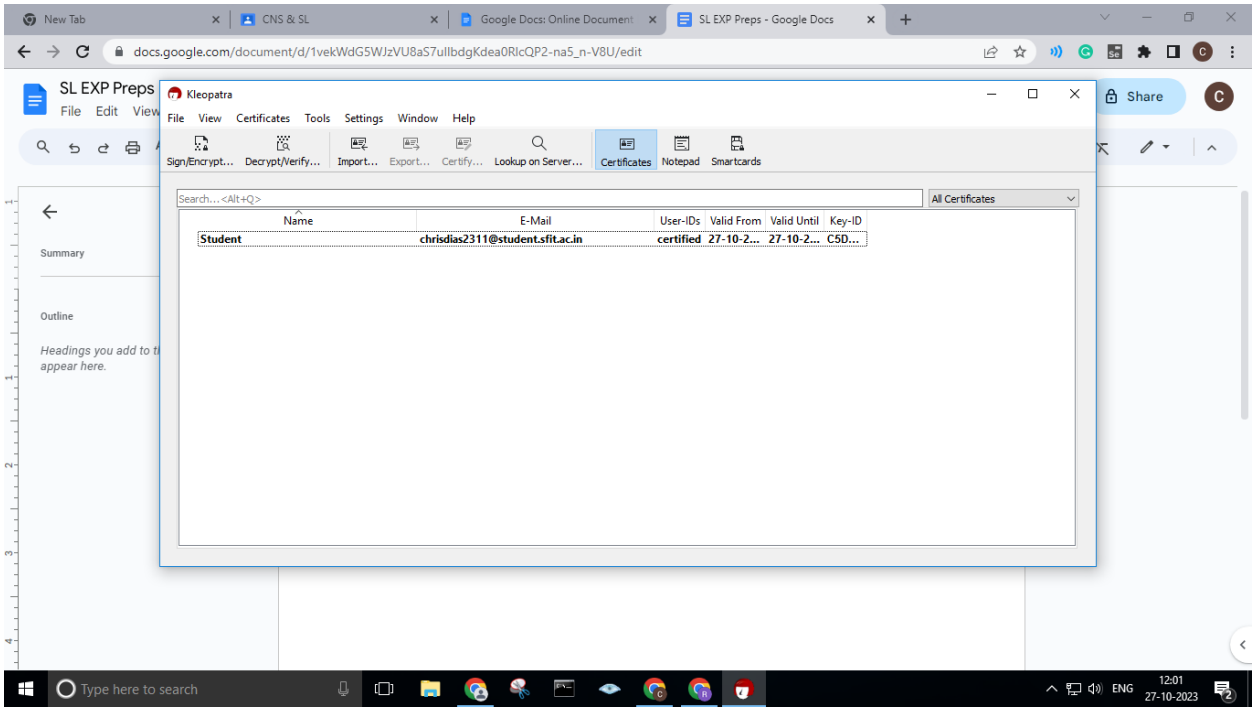
Open file explorer -> Go to SNORT bin in C drive -> copy path -> Open cmd -> cd C:\Snort\bin

To check IP address cd .. got to root C -> cd Windows/system32

4. Learn commands to use snort as IDS. Observe the snort rule file (i.e., snort.conf file). Analyze the rule file to configure it for your network environment.
Snort -dev -l C:\Snort\log -h 192.168.1.0/24 -c snort.conf

Experiment – 11: Implementation of Email security

Open Kleopatra in PC -> Go to certificates -> New Key pair -> Enter email -> Click on create -> Make a backup of your key -> navigate to Desktop -> Save finish



Right click on email -> Export

->The key that is exported is public key and the one that is Saved in desktop is private key

->Mail the public key to another email

Receivers End
Click on import -> Import the public key mailed to you -> Right click on the imported key -> Certify

Open notepad -> Write a message -> Click on Sign/Encrypt option (This will convert .txt file to .nsg file) -> Set a password (eg: 0000)
Now via Gmail send the .nsg file

Senders end
Download the file -> Click on Decrypt -> Import the file -> Enter the password (0000) The .txt file will automatically get downloaded