CS358 2023 Assignment 2 - Export PCAP Using Scapy

Mayank Agarwal

Python 3.10.6 Install Instruction https://pastebin.com/7yWiMH6m

Deadline: 21 March, 2023. 23:59. All of your git repos shall be pulled after that. That will be the version which will be checked.

Warning: Sharing is Caring is good for cat videos. Sharing of program may lead to plagiarism and would effect in 0 to both.

Doubts: All Doubts relating to CS358 2023 Assignment shall be posted on Google Form https://docs.google.com/forms/d/e/1FAIpQLSdVylWbeelAnQKYDCfqoyxcqSwm_FiVJDbzszV2Mpg-zZCfU viewform?usp=sf_link

I will respond to the queries here: https://docs.google.com/spreadsheets/d/1jHhkLLGrRSToYZH857D6hM3SY8Bi0LoTtqDZ-rNrvGw/edit?usp=sharing

Please avoid email / wa / dm

So common doubts can be solved and we shall be able to keep track in an organized manner.

Pull This Git Repo - https://github.com/cs358/308_CS359 and copy the tut01 to your repo folder.

Git Requirements: At least 3 git commits should be there with meaningful comments (at least 4 words)

Library Requirements: You can use csv, pandas, or any inbuilt module, but for evaluation you need to explain each line of code.

Task: Hi All

https://scapy.net/

Your assignment is to write a python code using scapy library. Scapy is packet capture and manipulation.

You need to check the link for the website that you need to work with https://docs.google.com/spreadsheets/d/1EO1pIEfwAMmKHXOdHMyTXEjlBm4kAUC8c9wqJ8i2NUk/edit?usp=sharing

ARP
TCP 3_way_handshake_start (Check links for your roll)
TCP handshake_close (FIN Sequence) (Check links for your roll)
DNS request response (Check links for your roll)
PING request response (Check links for your roll, else try for a valid internet IP)
FTP_Connection_Start (any ftp site)
FTP_Connection_End (any ftp site)
ARP request response (ping to any local host)

The scapy code should save the above captures (in a filtered manner, for ex, exactly 3 packets for TCP handshake, 2 for DNS request and response)
The file name pattern is as follows
ARP_Roll_Num.pcap
TCP_3_way_handshake_start_Roll_Num.pcap

TCP_handshake_close_Roll_Num.pcap
DNS_request_response_Roll_Num.pcap
PING_request_response_Roll_Num.pcap
ARP_request_response_Roll_Num.pcap
FTP_Connection_Start_Roll_Num.pcap
FTP_Connection_End_Roll_Num.pcap

Make mulitple functions in scapy to capture the packets. The scapy code should save the filename in pcap format.