Teachnook Major Project (Network Traffic Analyser)

Introduction

Hello! I am Naman Soni (registered e-mail id: namansoni2803@gmail.com); from Cybersecurity September-October blended program of Teachnoook. This is my submission for the major project: Network Traffic Analyser.

Programming Language used: Python

I have used python language to build this project and scapy library for the packet capture.

Files

- Please find the file named 'main.py' for the source code.
- The file named 'network_traffic.log' stores the information of the captured packets.
- `code.txt` is the text file of my source code stored in 'main.py'
- `logfile.txt` contains the logs of packets captured during final testing

FUNCTIONALITY

- It captures the packets, parse them, analyse them and display basic information about them like:
- Source IP address
    - Destination IP address
    - Protocol
    - Source port
    - Destination port
    - Bytes Transferred
- It analyses the protocol to detect HTTP, UDP, DNS traffic.
- In case of unusually high data/bytes transfer, it displays a warning message as seen in the log file.
- Filtering options like tcp, udp, port number are also included. On applying the filters, it only captures the packets that match the criteria.
- The log file is generated for record-keeping and further investigations.
- cmd+c is the keyboard interrupt used

INSTRUCTIONS

- To run the code on your system, you need to give root permissions to the scapy library. For that, run the following command in the terminal: `sudo python3 nameofthefile.py`
- On running the code, it prompts the user to enter their choice of filter
- It then asks for the number of packets to capture
- In case the packet capturing needs to be stopped immediately, press ctrl+c

OUTPUT DISPLAY EXAMPLE

- Capturing packets, Press Ctrl+C to stop.
- Filters: 1.TCP 2.UDP 3.IP 4.Port
- Enter your choice: 3
- Enter the number of packets to capture: 30

THANK YOU