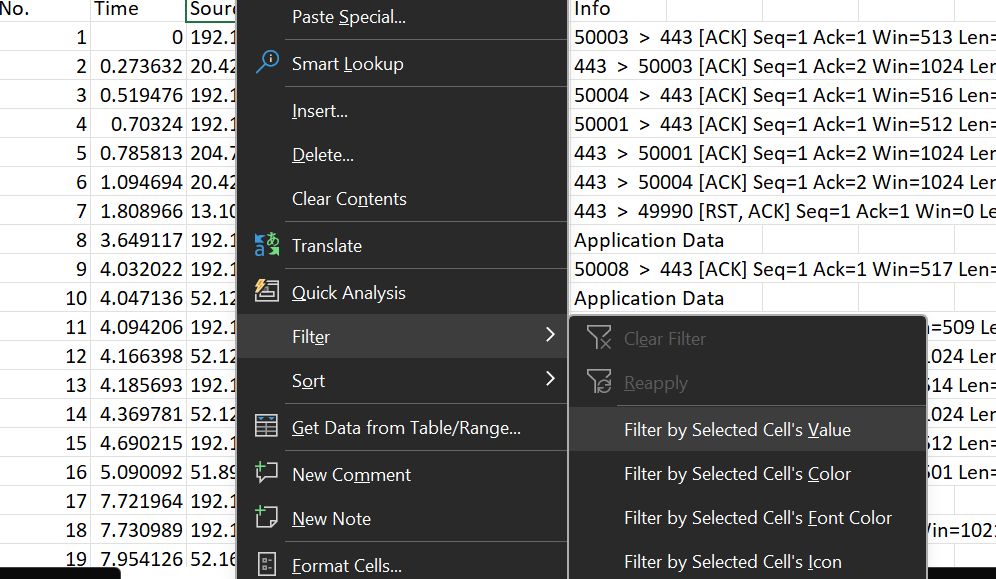
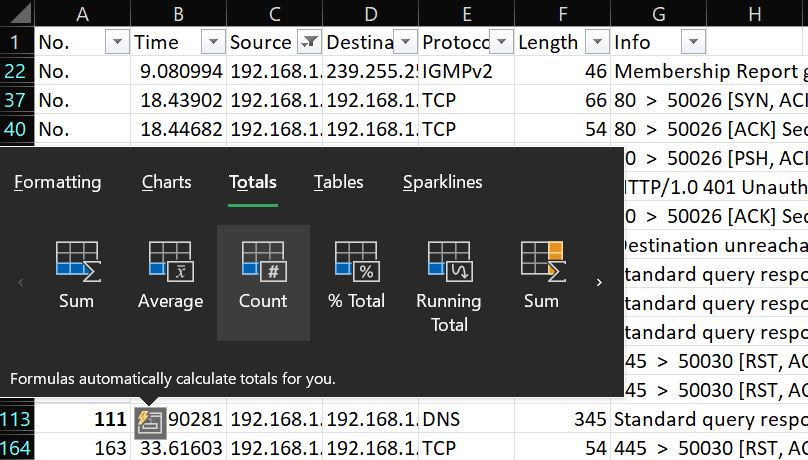
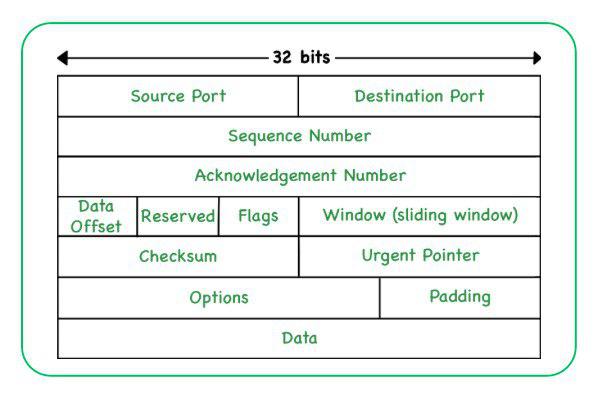
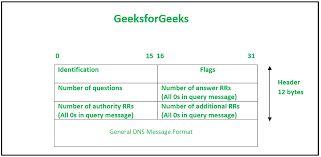
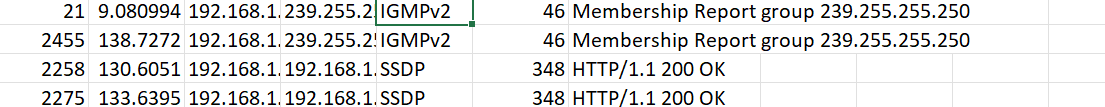
EXP NO :1 ATTACK INFORMATION ANALYSIS USING WIRESHARK  
DATE:  
  
AIM:  
 To obtain the information required to attack a given network using wireshark data.  
  
SOFTWARE REQUIRED:  
 PC with wireshark.  
  
THEORY:  
 Network:  
 A interconnected and interrelated group of systems that are able to communicate with each other forms a network. There are several types of network like Local Area Network(LAN) , Wide Area Network(WAN) etc.,   
  
 Wireshark:  
 It is a open source network analyser that can capture and display the real-time details of network traffic. It is mainly used for troubleshooting network issues, analyse network protocols and ensuring network security. The data such as packet number, time, source, destination, protocol and length are provided by the wireshark file capturing.  
  
PROCEDURE:  
 1. First connect the PC to a network.  
 2. Install Wireshark in the system. (https://2.na.dl.wireshark.org/win64/Wireshark-4.2.5-x64.exe)  
 3.Now open the wireshark application, the list of connections from the system will be shown, select the required connection to be monitored.  
 4. Go to the capture tab and start capturing, once enough packets are captured stop capturing.  
 5. The captured packets can be extracted as csv files.  
 6. From the captured packets we need obtain the information for attacking and so analysis must be done based on that.  
 7. For attacking the main information required will be about the sources that initiates packet transfer, hence the sources in the network is required.  
  
  
 (Filtering the sources)  
  
 8.The sources enlisted now. And the number of packets send from each sources must be calculated. This is done by filtering the source to be monitored and using count function we can know the number of packets sent.  
 9. Select the column upto which the packets to be counted and press CTRL + Q for quick analysis.  
  
  
 (Counting function for analysis of number of packets)  
  
 10. Based on this a graph is plotted to find the sources with maximum interaction in the network as number of packets sent from each sources is noted.  
  
  
 (sources and number of packets sent from them into the network)  
  
 11.From the above graph we see that 104.85.108.106, 142.250.195.138, 184.84.2333.226, 192.168.1.1 are the sources from which most number of packets are sent into the network. Hence these must the targets for attack in the network.  
 12. Next, individually each sources are analysed with their usage of different protocols and the observations are shown below.  
  
   
 (Protocol analysis for 104.85.108.106)  
  
 13. In source 104.85.108.106 the TCP protocol is used maximum number of times, this means that this source involves mainly working at transport layer and responsible for successful transfer of messages.  
So to disrupt the proper transmission of packets into the network this system must be attacked.  
  
TCP:  
 Transmission Control Protocol is a transport layer protocol that enables the higher network layers to send messages in the network.  
 

(Packet format of TCP)  
  
  
 (Sample information of tcp packet)  
  
 14. On matching the packet format with sample packet information from wireshark it is observed that the length of message is 66, the sequence is acknowledged, the window size are also observed. So to attack this “TCP reset attack” is used which involves forging packets with false information to terminate the communication.  
  
  
   
 (Protocol analysis for 142.250.195.138)  
  
 15. In 142.250.195.138 the most used protocol is QUIC as observed from the above graph.  
QUIC:  
 Quick UDP Internet Connection Protocol is a transport layer protocol that improves web connection reliability and speed. It encrypts all the transport information and it is more difficult to attack than TCP.   
  
  
 (sample packet info for QUIC)  
  
 16. The initial phase of QUIC involves handshaking and then protected packets containing messages are sent over the network.  
  
   
 (Protocol analysis for 184.84.2333.226)  
  
 17.At 184.84.2333.226 also the QUIC protocol is used. Hence we can say that this system involves message transfer over web applications. This follows the same principle to that of 142.250.195.138. Further the other protocols used are TLSv1.2 and v1.3 which are used to prevent eavesdropping into the network.  
  
  
  
   
 (Protocol analysis for 192.168.1.1)  
  
 18. The 192.168.1.1 system uses DNS protocol as its maximum combined with TCP protocol.  
The DNS (Domain Name System) uses a domain name to match with the IP Address of the required website. It is a application layer protocol to send messages from client to server.  
  
  
 (DNS message packets)  
  
   
 (packet format of DNS protocol)  
  
 19.Other protocols like SSDP are used here (Simple Service Discovery Protocol) and IGMPv2 are used. SSDP is a network layer protocol used to advertise and discover each other services in a network. The IGMPv2 (Internet Group Management Protocol) is used to identify hosts in a LAN.  
  
  
 (packets of IGMPv2 and SSDP protocols)  
  
 20.From this we can get the subnet information and the packet length of the packets used. As this system uses IGMPv2 protocol is used 192.168.1.1 must be one of the end to end user in the communication.  
  
  
OBSERVATION:  
 The attack information in a network can be obtained using the knowledge of the protocols used in the devices of a network. With that information duplicate packets of same format are created and sent over the network for DoS, eavesdropping etc.,  
  
RESULT:  
 Hence the informations required to attack a network are obtained using wireshark captured files.