Security And Forensics Lab

23th September 2024

Assignment - 6

Note: Screenshots verifying your observation is mandatory in the report.

1. List 3 different protocols that appear in the protocol column in the unfiltered packet listing window. What is the MAC address and IP address of your Host?

2. Make a detailed analysis of the packets transmitted and received from your system when you open a web browser and type **https://www.google.com/**.

   a. What is the TCP destination port number used for communication and the IP address of the destination?

   b. Is any ARP request ? What is the MAC address of the next hop where packets are communicated?

   c. Is any DNS query made? If yes write the details of each layer information of the packet send and received starting application layer, transport layer , network layer and data links layer? d. You can check for a TCP connection being established. Give details of how the three-way handshake is established. Write details about the seq no and window size in the packets getting exchanged. e. HTTPS is a secure protocol, which protocol is used for the secure communication. What are the handshake messages being exchanged between the source and destination. Also mention the encryption technique used and the name of the Cipher Suite.

3. Repeat the above process by opening a http site instead of https and write the detail about the analysis made.

   a. Do you find any difference between the http and https protocol. If yes, give the details of the messages exchanged on using http ?

   b. What is the TCP destination port number used for communication and the IP address of the destination?

   c. Which HTTP version is used and the acceptable user agent?

   d. In the HTTP request and response highlight the HTTP header and body. What is the difference between them?

   e. How many HTTP GET request messages were sent by your browser?

   f. How many data-containing TCP segments were needed to carry the single HTTP response? g. What is the status code and phrase associated with the response to the HTTP GET request? h. Check whether the connection type is persistent or non-persistent HTTPS.

For carrying out these experiments, please download and install wireshark.