ACADEMIC YEAR: 2022-23

DEPARTMENT of COMPUTER ENGINEERING DEPARTMENT

CLASS: T.E. **SEMESTER: I**

SUBJECT: CNSL

ASSINGMENT NO.	C4
TITLE	To study the SSL protocol by capturing the packets using Wireshark tool.
PROBLEM STATEMENT /DEFINITION	To study the SSL protocol by capturing the packets using Wireshark tool while visiting any SSL secured website (banking, e-commerce etc.).
OBJECTIVE	Study Wireshark tool and SSL.
OUTCOME	Students must be able to comprehend basics of network security
S/W PACKAGES AND HARDWARE APPARATUS USED	Open-Source Operating System, Packet Tracer, Wireshark, Core I3/I5/I7 with 4GB RAM system
REFERENCES	1. Wireshark Foundation / Wireshark · GitLab 2. Wireshark · Go Deep. 3. What is SSL? - SSL.com
STEPS	1.Search for SSL secured website. 2.Download Wireshark and install it in your system. 3.Start Services of Wireshark in order to check for website traffic. 4.In Wireshark we can check for various option depending on GUI provided by software, and check for network traffic of packets.
INSTRUCTIONS FOR WRITING JOURNAL	1. Date 2. Assignment no. 3. Problem definition 4. Learning objective 5. Learning Outcome 6. Concepts related Theory 7. Algorithm 8. Test cases 10. Conclusion/Analysis

Prerequisites: Open-Source Operating System, Packet Tracer, Wireshark tool, Core I3/I5/I7 with 4GB RAM system

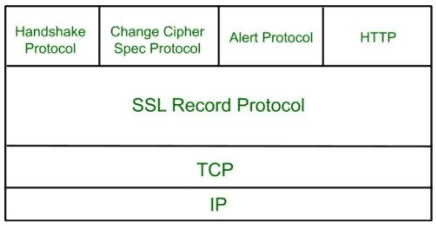
Concepts related Theory:

Secure Socket layer protocol is used for confirming security of data packets by considering encryption.

There are different types of SSL protocols there are as follows

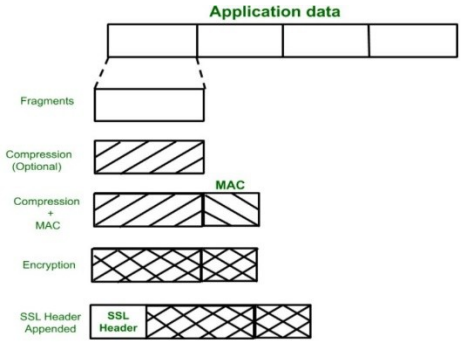
1. SSL record protocol-

   Confidentiality and message integrity are the major aim of this protocol.



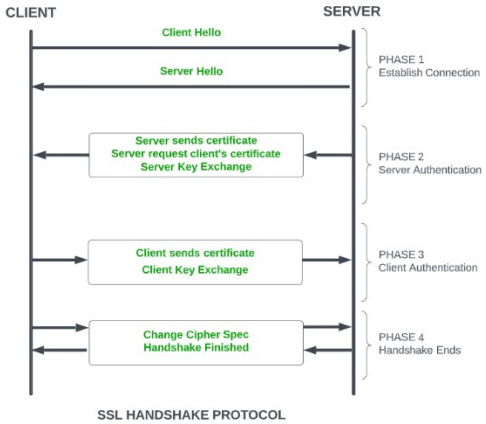
   (img ref: Secure Socket Layer (SSL) - GeeksforGeeks)

   SSL record protol wokrs in fragments.



   (img ref: Secure Socket Layer (SSL) - GeeksforGeeks)

2. Handshake Protocol – Connection is established in hand shake protocol between client and server by sening each other messages.



   (img ref: Secure Socket Layer (SSL) - GeeksforGeeks)

3. Change Cipher protocol-

   SSL record protocol is used in this change cipher protocol. It requires hand shake protocol to complete its operation to change the process state. Change cipher consist of

single message of one byte in length.The main purpose of this protocol is used to change pending state to current state.

(img ref: Secure Socket Layer (SSL) - GeeksforGeeks)

Wireshark is a free and open-source packet analyzer and it is world's foremost network protocol analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. With this tool we a track each and every small detail of network about processes running and data packets exchanged. This can be useful for administrative, education and government and nor profit enterprises as standard.

Features

- Wireshark works on "from the wire" concept.Live network connection is checked to capture also it can read from a file of already captured packets.
- Data can be read from various netwroks like Ethernet,IEEE,loopback etc.
- T shark terminal can be used tp browse network data if GUI is not available.
- It has feature of editcap in order to edit the programm of the read files.
- Display filter is used to refine data.
- We can add new plugin in this in order to extend functionality.
- It can also capture raw USB traffic.

Steps to install Wireshark on Fedora

- Open Terminal and type following command to install both QT and CLI version

```
$ sudo dnf install wireshark-qt
```

- Set Permission to Wireshark by typing following command

```
$ sudo usermod -a -G wireshark username
```

- Log out and Restart and start using Wireshark packet analyser tool.

Algorithm:

1.Analyse SSL website in which we have to perform SSL verification.

2.Download Wireshark tool for windows or required OS.

3.Start Capturing packets from website by selecting *capture* option in menu. Or you can simply click on *Enable Promiscuous mode on all interface option* and click on Strat button.

4.Understand the layers pf security provided by SSL.

Conclusion: Thus, after successfully understanding concepts related with SSL and Wireshark tool students are able to track packets in SSL verified websites.

Review Questions:

1.What is SSL?

2.What is mean by SSL Certificate?

3.Explain what are types of SSL certificates.

4.Explain in detail about Wireshark tool? Explain its significance in terms of security.

5.What is packet? How packets are transferred in network?