Page No.:

31332

Assignment - 07

Title :- Write a program in C/C++ to analyze following packets captured through wireshark for wired network.

1. FTP
2. IP
3. TCP
4. UDP

Objective :-

To analyze the packets received through wired network using Wireshark Analyzer Tool.

Outcome :-

Student will be able to -

1) To use wireshark packet analyzer tool
2) To distinguish between various packets according to there protocol.

Theory :-

Wireshark Packet Analyzer Tool -

→ Wireshark is a network analysis tool
→ It captures all the packets sent to or from your computer

It provides features such as -

1) Rich VOIP analysis
2) Live capture and offline analysis
3) Decryption support
4) Standard three pane browser

File Transfer Protocol-

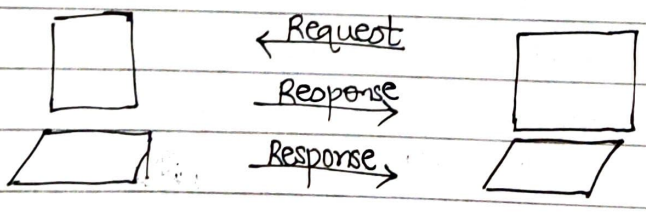
→ FTP is a standard internet protocol provided by TCP/IP for transmitting the files from one host to another.
→ It is mainly used for transfering web pages files from their creator to the computer that acts as a server for other computes on the internet
→ It is also used for downloading the files from server.

Internet protocol

→ Internet protocol is connectionless and unreliable protocol
→ It ensures no guarantee of successful data transmission
→ There are two versions of internet protocol
  1) IPv4
  2) IPv6

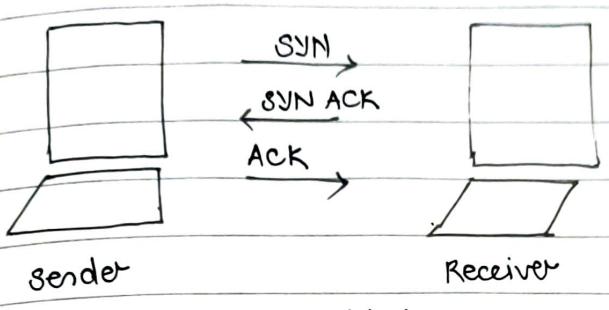
User Datagram Protocol

→ UDP is a connectionless communication protocol
→ It is a transport layer protocol
→ It doesn't provide ordering and error checking functionality.
→ UDP is used for multi casting.



Transmission Control Protocol

→ TCP is connection oriented protocol
→ It provides error checking and correction mechanism
→ TCP operates in client server point to point mode
→ TCP provides flow control and quality of service



TCP Handshake.

Algorithm -

1. Open wireshark packet capture CSV file.
2. Declare a map for storing distinct packet formats and their respective count.
3. Read the file line by line
4. Find protocol string from each line, increment the respective count in map.
5. Sum up all the protocol count to get the total count.
6. Find non-IP count

   non IP count = count of ARP packets + count of RARP packets.
7. Print total count, non-IP count and IP count

   IP count = total count - non-IP count.

CONCLUSION

Through this assignment, packets are captured and analysed using wireshark tool. Packets are categorised into IP and non IP packets based on protocols.