31341

Assignment 7

Problem Statement: Write a program to analyze following packet formats captured through Wireshark for wired network.

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

Objectives

1. To understand packet formats captured through Wireshark for wired network
2. To understand various protocols used in networking

Learning Outcomes: Students will be able to

1. Demonstrate captured packet format through Wireshark
2. Exhibit an understanding of the various protocols used

Requirements:

1. Open source linux based OS
2. GCC/G++ compiler

Theory:

Packet Sniffer

A packet sniffer (also known as a network analyzer, protocol analyzer or for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyzes its content. A packet sniffer is a wire-tap device that plugs into computer networks and eavesdrops on the network

31341

Computer-network administrators have used packet sniffers for years to monitor their networks and perform diagnostic tests or troubleshoot problems. Essentially, a packet sniffer is a program that can see all of the information passing over the network it is connected to. As data streams back and forth on the network, the program looks at, or "sniffs," each packet. A packet is a part of a message that has been broken up. Normally, a computer only looks at packets addressed to it and ignores the rest of the traffic on the network. But when a packet sniffer is set up on a computer, the sniffer's network interface is set to promiscuous mode. This means that it is looking at everything that comes through. The amount of traffic largely depends on the location of the computer in the network. A client system out on an isolated branch of the network sees only a small segment of the network traffic, while the main domain server sees almost all of it.

Ways to setup packet sniffer:

1. Unfiltered - captures all of the packets
2. Filtered - captures only those packets that contain specific data elements

Working of packet sniffers:

1. Ethernet hardware is built with a filter that ignores all traffic that doesn't belong to it. It does this by ignoring all frames whose MAC addresses don't match
2. A sniffer program turns off this filter, putting the Ethernet hardware into "promiscuous mode". Thus, it can see all the traffic among all machines that are on the same Ethernet wire.

Uses:

1. Analyze network problems
2. Detect network intrusion attempts
3. Detect network misuse by internal and external users
4. Isolate exploited systems
5. Monitor bandwidth

6. Monitor network usage
7. Debug network protocol implementations
8. Verify internal control system effectiveness (firewall, proxies, web/spam filters, ...)

FTP

The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network.

FTP is built on a client-server model architecture using separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP).

Syntax: ftp://user:password@host:port/url-path

Data types

1. ASCII (Type A) - Used for text
2. Image (Type I) - Binary mode
3. EBCDIC (Type E) - Used in communication in EBCDIC character set
4. Local (Type L n) - Used in non 8-bit systems

File structures

1. F or FILE structure (stream-oriented)
2. R or RECORD structure (record-oriented)
3. P or PAGE structure (page-oriented)

Data transfer

1. Stream mode (S) - Data is sent as a continuous stream
2. Block mode (B) - Data is sent in several blocks (for record-oriented files)
3. Compressed mode (C) - Extends mode B with data compression

IP (Internet Protocol)

The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables inter-networking, and essentially establishes the Internet.

IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.

The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet. Its successor is Internet Protocol Version 6 (IPv6), which has been in increasing deployment on the public Internet since 2006.

Wireshark:

1. It is an open-source multi-platform network protocol analyzer
2. It allows you to examine data from a live network or from a capture file on a disk. You can interactively browse the capture data, down to the level of packets.
3. It includes a display filter language and ability to view the reconstructed stream of a TCP session.
4. It also supports hundreds of protocols and media types.

Conclusion

Hence, we have successfully implemented a program to analyze the packets captured by Wireshark for various protocols.