Experiment no.6

Aim: Study of packet sniffer tools: Wireshark

Download and install wireshark and capture icmp, tcp, and http packets in promiscuous mode and explore how the packets can be traced based on different filters.

Objectives: • Understand the need for traffic analysis. • Understand the how packet sniffing is done using wireshark. • Trace and understand various packets from dynamic traffic.

Outcomes: The learner will be able to • Sniff network packets and study insights of packets to get detail network information.

Hardware / Software Required: Unix/Linux/Windows, wireshark

Theory:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color-coding and other features that let you dig deep into network traffic and inspect individual packets.

Features of Wireshark:

- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.
- Export some or all packets in a number of capture file formats.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet display based on filters.

Create various statistics.

Capturing Packets:

After downloading and installing wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface. You can configure advanced features by clicking Capture Options.

Installation of Wireshark: sudo apt-get install wireshark

After downloading and installing wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface. You can configure advanced features by clicking Capture Options.

As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system. If you're capturing on a wireless interface and have promiscuous mode enabled in your capture options, you'll also see other the other packets on the network.

Click the stop capture button near the top left corner of the window when you want to stop capturing traffic.

Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-of-order.

Filtering Packets:

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type —dnsl and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.