EXPERIMENT NO: 07

AIM: Study of packet sniffer tools like wireshark, :- 1) Observe the performance in promiscuous as well as non-promiscuous mode 2) show the packets can be traced based on different filters.

THEORY:

Packet sniffing is the process of capturing each packet that is transmitted over the network and analyzing its content. Most of the time, packet sniffing is used to troubleshoot network problems or to gather network statistics. The software or device used for capturing packet data is called packet sniffer.The Packet Sniffing Tool PRTG offers a quick graphical overview as well as detailed statistics about different parameters such as CPU usage or network bandwidth.

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.

Applications:

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals beside these examples can be helpful in many other situations too.

Features:

- 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.

1) Observer Performance in Promiscuous and Non-Promiscuous Mode

Wireshark can operate in two distinct modes: promiscuous mode and non-promiscuous mode. The mode in which the network interface operates directly affects the packets that can be captured.

Promiscuous Mode:

Definition: In promiscuous mode, the network interface captures all packets that travel across the network, regardless of whether they are addressed to the machine running Wireshark.

Performance:

- In this mode, Wireshark captures packets from all devices on the network segment (local network). This is useful in monitoring all traffic and analyzing how the network behaves.
- Performance may vary based on the number of devices and the amount of traffic in the network. The machine capturing packets can become overloaded with large volumes of traffic in high-traffic networks, which can impact its performance.
- It is essential for network diagnostics because it allows the user to analyze communication between devices even if they are not directly involved in the communication.

Non Promiscuous Mode:

Definition: In non-promiscuous mode, the network interface only captures packets that are specifically addressed to the machine running Wireshark.

Performance:

- The network interface only captures packets that are relevant to the system itself, leading to fewer packets being captured and analyzed.
- This mode is less resource-intensive compared to promiscuous mode because the machine only processes traffic relevant to itself, thus reducing the amount of data it has to handle.
- It is useful for capturing communication between the local system and other devices but will not reveal the network traffic between other devices that the system is not a part of.

2) Showing the Packets Can Be Traced Based on Different Filters

Wireshark provides a powerful set of filters that allow users to selectively capture and display specific types of packets. Filters are categorized into capture filters (used during the packet capture process) and display filters (used to refine the view of captured data).

Capture Filters:

Capture filters are applied before packets are captured. They limit the data that is stored and analyzed, which is useful for narrowing down the packet capture to only relevant traffic.

- **Host Filtering**: To capture packets from or to a specific IP address
- **Port Filtering**: To capture packets on a specific port (e.g., HTTP on port 80)
- **Protocol Filtering**: To capture packets of a specific protocol, like TCP, UDP, or ICMP

Display Filters:

Display filters are applied after the packets have been captured. They allow you to focus on specific packets that meet your filtering criteria from the entire capture dataset.

- **IP Filtering**: To display packets sent to or from a specific IP address
- **Protocol Filtering**: To display packets of a particular protocol (e.g., HTTP)
- **TCP Filter**: To filter packets with a specific TCP flag set (e.g., SYN packets)
- **Packet Content Filtering**: To filter based on data content, such as a string within HTTP packets

Wireshark Installation :

Step 1: Visit the oficial Wireshark wefbsite using any web browser.

Step 2: Click on Download, a new webpage will open with different installers of Wireshark.

Step 3: Downloading of the executable file will start shortly. It is a small 73.69 MB file that will take some time.

Step 4: Now check for the executable file in downloads in your system and run it.

Step 5: It will prompt confirmation to make changes to your system. Click on Yes.

Step 6: Setup screen will appear, click on Next.

Step 7: The next screen will be of License Agreement, click on Noted.

Step 8: This screen is for choosing components, all components are already marked so don't change anything just click on the Next button.
Step 9: This screen is of choosing shortcuts like start menu or desktop icon along with file extensions which can be intercepted by Wireshark, tick all boxes and click on Next button.

Step 10: Next screen has an option to install Npcap which is used with Wireshark to capture packets*p*capmeans packet capture so the install option is already checked don't change anything and click the next button.

Step 11: Next screen is about USB network capturing so it is one's choice to use it or not, click on Install.

Step 12: After this installation process will start

Step 13: This installation will prompt for Npcap installation as already checked so the license agreement of Npcap will appear to click on the *I Agree* button.
Step 14: Next screen is about different installing options of *npcap*, don't do anything click on Install.

Step 15: After this installation process will start which will take only a minute.

Step 16: After this installation process will complete click on the Next button.

Step 17: Click on Finish after the installation process is complete.

Step 18: After this installation process of Wireshark will complete click on the Next button.

Step 19: Click on Finish after the installation process of Wireshark is complete.

CONCLUSION:

In this experiment we analyze various packet sniffing tools that monitor network traffic transmitted between legitimate users or in the network. The packet sniffer is network monitoring tool.