04/12/2020 **Mohd. Aftab Alam**
02013302717

EXPERIMENT 9

Aim: To Study Simulation Tool **- Wireshark**

Wireshark:

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, OS X, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License.

Functionality:

Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.

Wireshark lets the user put network interface controllers that support promiscuous mode into that mode, so they can see all traffic visible on that interface, not just traffic addressed to one of the interface's configured addresses and broadcast/multicast traffic. However, when capturing with a packet analyzer in promiscuous mode on a port on a network switch, not all traffic through the switch is necessarily sent to the port where the capture is done, so capturing in promiscuous mode is not necessarily sufficient to see all network traffic. Port mirroring or various network taps extend capture to any point on the network. Simple passive taps are extremely resistant to tampering.

On GNU/Linux, BSD, and OS X, with libpcap 1.0.0 or later, Wireshark 1.4 and later can also put wireless network interface controllers into monitor mode.

History:

In the late 1990s, Gerald Combs, a computer science graduate of the University of Missouri–Kansas City, was working for a small Internet service provider. The commercial protocol analysis products at the time were priced around $1500 and did not run on the company's primary platforms (Solaris and Linux), so Gerald began writing Ethereal and released the first version around 1998. The Ethereal trademark is owned by Network Integration Services.

In May 2006, Combs accepted a job with CACE Technologies. Combs still held copyright on most of Ethereal's source code (and the rest was re-distributable under the GNU GPL), so he used the contents of the Ethereal Subversion repository as the basis for the Wireshark repository. However, he did not own the Ethereal trademark, so he changed the name to Wireshark. In 2010 Riverbed Technology purchased CACE and took over as the primary sponsor of Wireshark. Ethereal development has ceased, and an Ethereal security advisory recommended switching to Wireshark.

Wireshark has won several industry awards over the years, including e-Week, InfoWorld, and PC Magazine.

Features:

- Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.
- Live data can be read from a number of types of networks, including Ethernet, IEEE 802.11, PPP, and loopback.
- Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, TShark.
- Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.
- Data display can be refined using a display filter.
- Plug-ins can be created for dissecting new protocols.
- VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.
- Raw USB traffic can be captured.
- Wireless connections can also be filtered as long as they transverse the monitored Ethernet.
- Various settings, timers, and filters can be set that ensure only triggered traffic appear.
- Wireshark's native network trace file format is the libpcap format supported by libpcap and WinPcap, so it can exchange captured network traces with other applications that use the same format, including tcpdump and CA NetMaster. It can also read captures from other network analyzers, such as snoop, Network General's Sniffer, and Microsoft Network Monitor.

Security:

Capturing raw network traffic from an interface requires elevated privileges on some platforms. For this reason, older versions of Ethereal/Wireshark and tethereal/TShark often ran with superuser privileges. Taking into account the huge number of protocol dissectors that are called when traffic is captured, this can pose a serious security risk given the possibility of a bug in a dissector. Due to the rather large number of vulnerabilities in the past (of which many have allowed remote code execution) and developers' doubts for better future development, OpenBSD removed Ethereal from its ports tree prior to OpenBSD 3.6.

Elevated privileges are not needed for all operations. For example, an alternative is to run tcpdump or the dumpcap utility that comes with Wireshark with superuser privileges to capture packets into a file, and later analyze the packets by running Wireshark with restricted privileges.

To emulate near real-time analysis, each captured file may be merged bymergecap into growing file processed by Wireshark. On wireless networks, it is possible to use the Air crack wireless security tools to capture IEEE 802.11 frames and read the resulting dump files with Wireshark.

As of Wireshark 0.99.7, Wireshark and TShark run dumpcap to perform traffic capture. Platforms that require special privileges to capture traffic need only dumpcap run with those privileges. Neither Wireshark nor TShark need to or should be run with special privileges.