EtherSnoop Light (A Packet Sniffing Tool)

Jaswinder kaur[1]
[1]Master of Technology, Department of Computer Engineering
Punjabi University, Patiala

Abstract: ***The management, maintenance and monitoring of network is Important to keep the network smooth and efficient. For this purpose the packet sniffers are used. Packet sniffers are basically applications. These are used to capture packets that travel across the network. Packet analysis can help us to understanding network characteristics, learn who is on a network, to determine who is utilizing available bandwidth, identify peak network usage times, identify possible attacks or malicious activity etc. By using packet sniffers developers can easily obtain the information of the packet such as structures, types, sizes and data etc. Consequently, network administrator find and correct errors rapidly and conveniently. This paper focuses on the basics of packet sniffer EtherSnoop Light Tool, it's working Principle and availability. This application does not transmit any data onto the network and this has friendly GUI and it is very easy to install.***

Keywords: sniffing, Working of packet sniffers, EtherSnoop Light, Features of EtherSnoop Light, WinPcap.

I. INTRODUCTION

Packet sniffing is a technique of monitoring every packet that crosses the network. Packet sniffer is a tool that plugs into computer network eavesdrops on the network traffic. These tools have ability to capture all incoming and outgoing traffic including clear- text password and username or other sensitive material etc. [1][4]. By using these tools user, administrators, developers can easily obtain information about packet size, type of protocol used, data, Source address, destination address etc. Some packet sniffer tool are passive software's. These can observes only message being send and receive by computer but can't sends packet themselves. Some packet sniffers have ability to generate a message and send to the network. Network administrator use these tool for detecting network intrusion or Analyses network Problems. Security engineers use these tools for investigating network traffic for security issues.Someone use these tools to learn how their network works But attackers utilize these sniffing tools for eavesdrop the network traffic and steal private information. [1][2].

II. WORKING OF PACKET SNIFFER

Packet sniffers require some hardware or software components through which packet sniffer able to capture the packet or network traffic as :

1. The hardware: Most products work from standard network adapters, though some require special hardware. If you use special hardware, you can analyze hardware faults like CRC errors, voltage problems, cable programs, "dribbles", "jitter", negotiation errors, and so forth.
2. Capture driver: Capture driver like WinPcap, Libcap etc is the most important component of packet sniffer. It captures the network traffic from the wire, filters it for the particular traffic that anyone wants, and then stores the data in a buffer.
3. Buffer: Once the frames are captured from the network, they are stored in a buffer. The size of the buffer is depends on the sniffing tools. For eg. Buffer Size for EtherSnoop Light is 100Mb.
4. Decoder: Decoder displays the contents of all fields within a protocol message with descriptive text so that an analysis can figure out what is going on
5. Packet editing/transmission : Some products contain features that allow anyone to edit his own network packets and transmit them onto the network[3]

A packet sniffer works by looking at every packet sent in a network, including packet not for intended for itself. Sniffers works on different type of network like:

1. Shared Ethernet: Shared Ethernet was built around a "Shared principle" i.e all machines on a local network shared the same wire. This implies that all machines are able to see all the traffic on same wire. Thus, 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 address doesn't match. A sniffer program turns off this filter, putting the Ethernet hardware into "promiscuous mode". Thus, Mark can see all the traffic among all machines, as long as they are on the same Ethernet wire.[1][6]
2. Switch Ethernet: In Switch Ethernet the hosts or computers are connected to the switch other than hub. Through which packet is deliver to a specific computer because switch maintain a table which keeps each computer's MAC address. So switch is called intelligent device. Because switch does not broadcast the packet. Most network administrators assume that sniffers don't work in a switched environment.[1][2][6]

III. ETHERSNOOP LIGHT

EtherSnoop Light is a very simple free network sniffer used for capturing packets passing through a network. It lists the capture data in real time passing through dial up connection

or network Ethernet card and analyzes data and displays it in a readable format. It runs only on a WIN32 environment and has convenient and easy to use graphical user interface. See fig.1 [3][7].

As shown in fig.1, EtherSnoop Light display window consists of three panes :

The left pane displays the packet logical tree structure. It displays Ethernet header, IP header, UDP header, TCP header, ICMP header and data.

The right pane displays the captured protocol summary including time stamp, packet length, source and destination MAC addresses, protocol type and source and destination IP addresses and port numbers.

The bottom pane displays the packet details in hexadecimal and ASCII formats. EtherSnoop Light Packet sniffer tool has all basic features that anyone would expect in a sniffer and but several features are not seen in EtherSnoop Light. In EtherSnoop Light with its powerful filter, anyone can customize his need to capture and avoid irrelevant packets.[3]

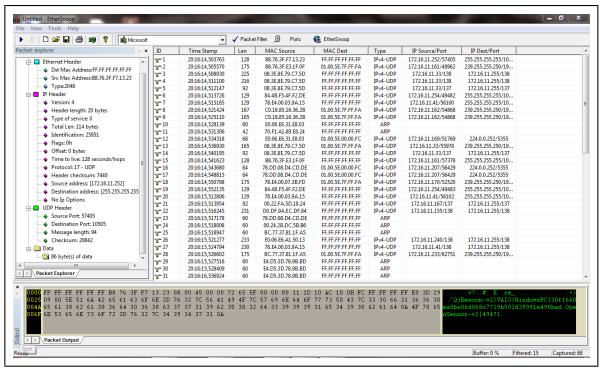

Figure 1: EtherSnoop Light Window

IV. FEATURES OF ETHERSNOOP LIGHT

a) EtherSnoop Capture IP packets on only Ethernet LAN with no packets losing

b) EtherSnoop Parse and decode any variety of network protocol

c) EtherSnoop has ability to Support saving captured packets for reopening afterward

d) EtherSnoop Light has a filtering mechanism to capture specific packets

e) In EtherSnoop Light Syntax is highlighted in data output selection.

V. COMMANDS IN TOOLBAR WINDOW OF ETHERSNOOP LIGHT

a) Start : Start packet capturing

b) Stop : Packets capturing

c) New Window : Create a new window

d) Open : Open a packets file, saved previously

e) Save : Save current captured packets into a file for future reopening

f) Print : Print the window

g) View network adapters : View all network adapters

h) About : Display program information, version number and copyright

VI. PROTOCOLS SUPPORTED BY ETHERSNOOP

EtherSnoop supports a limited number of network protocols. Protocols supported are IPv4, ARP, ICMP, TCP and UDP. EtherSnoop light does not support IPv6 protocol. In EtherSnoop there is a filter that filter protocols like ARP, TCP, UDP, ICMP. Selecting any of these protocol, filters will cause EtherSnoop to drop any packet that does not meet the conditions set by the filter. In EtherSnoop there is a port filters that filter the ports HTTP, SMTP, POP3, FTP and Telnet. When any of these filters are checked, only packets that met the filter are captured. EtherSnoop does not provide any statistical information about the captured data. [3]

VII. CAPTURE DRIVER WINPCAP

The WinPcap Driver is necessary for EtherSnoop Light Tool. With the help of WinPcap, EtherSnoop Light is able to capture the network traffic. WinPcap is an open source library for packet capturing and network analysis for Win32. WinPcap is tool for link-layer network access in Windows environments. It allows sniffing tools to capture and transmit network packets through the network. WinPcap is a powerful set of libraries which can be used for various tasks, very important in network programming: obtain all available network adapters, obtain information about an adapter, like the name and the description of the adapter, capture network packets using one of the network interface cards of the computer, send network packets across the network, or filter the captured packets, to obtain only the desired ones [8]The purpose of WinPcap is to give this kind of access to Win32 applications; it provides facilities to :

1. Capture packets, both the ones destined to the machine where it's running and the ones exchanged by other hosts
2. filter the raw packets according to user-specified rules before dispatching them to the application
3. Transmit raw packets to the network

VIII. LIMITATIONS OF ETHERSNOOP LIGHT

1. EtherSnoop support Ethernet only
2. EtherSnoop just displays the packet information without availability to change or control the packet and for large network

3. EtherSnoop does not support IPv6 Protocol
4. EtherSnoop does not provide the user with analysis tools and statistical reports

IX. CONCLUSION

When computers communicate over networks, they normally just listen to the traffic specifically for them. However, network cards have the ability to enter promiscuous mode, which allows them to listen to all network traffic regardless of if it's directed to them. Packet sniffers can capture things like clear-text passwords and usernames or other sensitive material. Because of this, packet sniffers are a serious matter for network security. Fortunately, not all sniffers are fully passive. Since they aren't tools like Anti-Sniff can detect them. Since sniffing is possible on non-switched and switched networks, it's a good practice to encrypt your data communications. EtherSnoop Light is a packet sniffing tools. which is open source tool that is freely available but has lot of limitations as compared to other tools like Wireshark, TCPdump ect

X. ACKNOWLEDEMENT

I would like to show my sincere gratitude to my advisor Er. LAL CHAND PANWAR, Assistant Professor at DCE(Punjabi University Patiala), for providing me the chance to work on this study, and for acting as a guiding light throughout the duration of the study.

I am also indebted to many of my colleagues for their valuable comments, and moral support in times of distress.

References

[1] All about ethersnoop light. `www.ethersnoop-light.com-about.com`.

[2] All about winpcap. `www.winpcap.org`.

[3] Pallavi Asrodia and Hemlata Patel. Analysis of various packet sniffing tools for network monitoring and analysis. *International Journal of Electrical, Electronics and Computer Engineering*, 1(1):55–58, 2012.

[4] Victor A Clincy and Nael Abu-Halaweh. a taxonomy of free network sniffers for teaching and research.

[5] Anshul Gupta. A research study on packet sniffing tool tcpdump. *International Journal of Communication and Computer Technologies*, 1(49):525–532, 2013.

[6] Muna M. Taher Jawhar and Monica Mehrotra. System design for packet sniffer using ndis hooking. *International Journal of Computer Science and Communication*, 1:171–173, 2010.

[7] D.K. Mishra Rupal Sinha. Anti packet sniffing: A zero hacking. In *Proceeding of the 2nd National Conference; INDIACom-2008 Computer For Nation Development*, 2008.

[8] Rajeev S.G. S. Ansari and Chandrasekhar H.S. Packet sniffing: A brief introduction. *IEEE Potentials*.

