PACKET SNIFFER

Mr. Shobhit Kumar (Assistant Professor)[1], Raghvi Bhatnagar [2]

CCSIT, TMU, MORADABAD

[1]**raghvibhatnagar5@gmail.com**

[2]**Shobhit.computers@tmu.ac.in**

Abstract-—**A packet sniffer, the network scanner, is a wire-tap device that plugs into computer network and listen in on the network traffic. Today we are looking that computer networks are enlarge in their sizes very fast and the number of its users is also being increased. For complicated network its very tough task to maintain the network, because large amount of data access. For this purpose packet sniffer is used. Packet sniffer is a approach of tapping each packet as it run over the network. By using this developers can simply capture the information of the packet, such as sizes, structure, and data. To gaining the data going over the network is called sniffing. This paper gives a brief addition of what is a packet sniffer and what is its working.**

I. .INTRODUCTION-

Packet sniffer is a method of capturing the information forward over the network. A packet sniffer is a piece of hardware and software that guide all the network traffic. It can be achieved in both switched and non switched environment. In a switched environment dare to eavesdrop on network traffic. Because
Usually switches will only transfer the network traffic to the computer. In a non switched environment is a good accepted technology. An another reason is to use a packet sniffing software which gives the information of the network. Examples of packet sniffing are Wire shark, Capsa Network Analyzer, Sky Grabber, Microsoft Network Monitor etc. When a device sends data in the network it send in the form of packet. Usually every send data has a receiving point. A system in a
Network is composed to read and receive only those data which are intended for it, but when we install the packet sniffer on a network it looks out for all the data travelling across the network. There are two types of sniffing- passive and active. Passive sniffing includes listening and capturing traffic. Active sniffing includes launching an Address Resolution Protocol (ARP) spoofing.

II. HOW PACKET SNIFFER WORKS-PACKET

sniffer's working can be understood in both switched and non switched environment. One of the most functions of networking is the switched environment because businesses are always adding devices to the wired network, and they will do through the switch. Switches are the devices that connect the computers, printers, and serves within a building or campus. When a non switched environment is designed then all the nodes are connected to a hub, it is a common connection point of devices in a network. A hub contains multiple ports. So as soon as a packet comes in a network, it transmitted to all the hosts in the network. Since all the computers on the local network share the same wire, so all devices will be able to see the traffic. When a packet goes to a host then network cards checks its MAC address, in local area network or other network the MAC (Media Access Control) address is your computer unique hardware number. If MAC address matches the host MAC address then the host is able to receive the packet otherwise it forward the packet to other host. So we can say that when the host NIC is setup then the entire packet is captured easily by the host. A network interface card is a circuit card that is installed in a computer so that it can be connected to a network.

Fig 1.Packet sniffing in non-switched environment

When a switched network id designed all the hosts connected to a switched rather of a hub. In switched environment packet sniffing is more complex comparison to non switched environment, because the switched does not transmission network traffic. Switches works on unicast method it can not broadcast the network traffic it send the traffic to destination. If we understand the working of packet sniffer in switched environment we consider an ARP cache table. This table stores the IP address and MAC address of the host. It exist in local area network. Destination host is checked in ARP table, before sending the packet to the source host. This packet transmitted to the destination in two parts. First the packet arrive source host to switch and then switch transfer packet directly to the destination. So sniffing is not possible here.

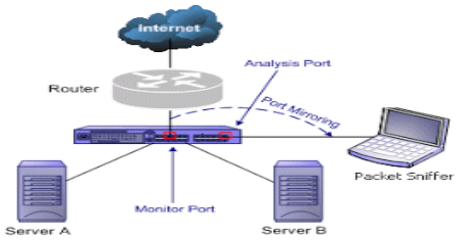

Fig 2.Packet sniffing in switched environment

III. KEY FEATURES OF POPULAR SNIFFERS-

Top 5 passive packet sniffer are used: Wire shark, TCPdump, Cola soft packet sniffer- Cola soft Capsa, ether detect and ettercap. Here we discuss Wire shark, TCPdump, and Cola soft Capsa.

A. Wireshark-

Wireshark a network analyzer tool capture packets in real time and show then in human readable format. Wireshark is licensed under the GNU (General Public License). Wireshark can capture data from many different network media type involving wireless LAN as well. It can open packets captured from a large number of other capture programs. Wireshark is not an intrusion detection system.

B. TCPdump

TCPdump is a device used for packet capturing and network guiding. It is works on the Linux based system. TCPdump is free and open source software. Open source mean that something people can modify and share because its design is publicly accessible. It can be used to real live capture. TCPdump run remotely by Telnet. It understand Boolean search operators and use the host name, IP addresses and protocol as argument.

C. Colasoft Capsa

Colasoft Capsa handles most of the features of Wireshark with TCP flow analysis. We chose the Colasoft Capsa because it has powerful customizable alarm and Email monitor, auto-saving Email content. Capsa is a portable network analyzer application for both LAN and WAN which performs real time packet capturing capability. One of the loss of point of Capsa is that it is quite expensive. But a free version is

available with limited features. Disadvantage of Colasoft Capsa is that it works on only window platform.

IV. CHARACTERISTIC EVALUATION-

To compare the above device we need to finalize some parameters.

A. TCPdump vs. Wireshark

Both TCPdump and Wire shark have wide range of packet filters to filter the incoming traffic through NIC. TCPdump and Wire shark both has no intrusion detection function. They cannot generate alarm for the attacks. Wire shark is a powerful sniffer which can decode lots of protocol. TCPdump decode limited protocol. If anybody looking to manipulate data on the network then he should above both approach fail in the area of manipulation.

B. TCPdump vs. Cola soft Capsa-

TCPdump is a common packet analyzer that runs under the command line. Cola soft Capsa allows you to apply filters to view select type of packets. Filters can be applied by addresses, port, and protocol. TCPdump allows the user to display TCP and other packets over a network to which the computer is connected.

V. RESULT-

From the above argument one can find out the greatest method on the behavior or the characteristics required. For example if a user wants to watch anything graphically, then he should prefer Wire shark or Cola soft Capsa. And if a person wants to work remotely with least bandwidth usage, then he should prefer TCPdump over Wire shark or Cola soft. But we can seen the there is a similar characteristics between Wire shark and Cola soft. We can generally compare the Wire shark and Cola soft but we cannot compare the TCPdump with these methods because TCPdump does not have any graphical interface to show the bounded output.

VI. SNIFFING COMPONENTS-

Sniffer is a combination of hardware and software. Basic components are-

The Hardware-Most sniffing products can work with standard adapters. Some sniffer supports only wireless adapters and other can support multi-adapters. If you install a sniffer on your computer then you should sure that what type of adapter your sniffer require.

Capture Driver-In packet sniffing the capture driver is the most important tool. It capture the network traffic from the wire.

Buffer-If the frames are captured by the capture driver on the network then it stored in the buffer.

VII. SNIFFING METHODS-

Here we will discuss three types of sniffing methods.

A. -In packet sniffing,

IP-based sniffing is a method that commonly used. In this method all the requirements of setting network card exist in promiscuous mode. Promiscuous mode allow a network device to read every network packet that appear in its entity. It uses an IP based filter, those packets match with the IP based filter is only captured. It works only in non switched environment.

B. MAC-based sniffing

It's concept similar to IP based sniffing. In MAC based sniffing requirements of setting network card exist in promiscuous mode. But here we use MAC address filter in place of IP based filter.

.3 ARP-based sniffing

-The working of this method is different, it does not put the network card into promiscuous mode. ARP(Address Resolution Protocol) is an effective method for packet sniffing.

VIII. CONCLUSION-

Packet sniffer is not a hacking tool, hacking tool is a program designed to help a hacker with hacking. By the help of packet sniffer we can monitoring the traffic and capture packets. This paper proposes an approach to detect packets by packet sniffer. Packet sniffer used in both switched and non switched environment. It can capture clear text passwords, user name and many other things.

ACKNOWLEDGEMENT-

It is indeed a matter of great pleasure and privilege to be able to present this report on packet sniffer under the valuable guidance of **Asst. Prof. Mr. Shobhit Kumar** and faculty of **CCSIT of Teerthanker Mahaveer University Moradabad.** I would like to express my deep sense of gratitude to our guide for his valuable guidance, advice and constant to my work. I am also thankful to our honorable principal **Prof. Dr. R.K Dwivedi** who made all facilities for us in college premises.

REFERENCES-

1. [1] A Research study on Packet Sniffing Tool TCPDUMP-International
2. [2] Network Traffic Analysis using Packet Sniffer-IJERA
3. [3] Packet Sniffer- A Comparative study-IJCNCS
4. [4] "Tutorial on Wire shark". Internet: http://webhost.bridgew.edu/sattar/CS430/HW/LABS/Wireshark.htm.
5. [5] S. An sari, Rajeev S.G, "Packet Sniffing: Brief Introduction", IEEE Potentials, Dec 2002-Jan 2003.

[6] "Tutorial on Wire shark". Internet: http://webhost.bridgew.edu/sattar/CS430/HW/LABS/Wire shark.htm
[7] Research paper proceeding of the 2nd National Conference.
[8] Implementation of IEEE 802.15.4 Packet Analyzer
[9] Liqiang Zhang, Huanguo Zhang "An Introduction to data Capturing" International Symposium on Electronic Commerce and security.
[10] Daniel Magers "Packet Sniffing: An Integral Part of NetworDefense".
[11] All about Tools Available: http://www.sectools.org/
[12] Packet Sniffing Basics Linux Journal by Adrian Hannah
[13] Linux Journal on Tcpdump
[14] http://nongnu.org/tiger/.
[15] http://www.fish2.com/cops/overview.html.
[16] http://www.monkey.org/dufsong/dsniff/.