# A Study on Detecting Packet Using Sniffing Method

Palak Girdhar
M.Tech, Bhagat Phool singh Mahila Vishvidhalaya, Khanpur, Kalan(Sonipat), India.

Vikas Malik
Chairperson, CSE IT, Bhagat Phool singh Mahila Vishvidhalaya, Khanpur, Kalan(Sonipat), India.

**Abstract – Packet Sniffing is a technique of monitoring every packet that crosses the network. A packet sniffer is a piece of software or hardware that monitors all network traffic. This is unlike standard network hosts that only receive traffic sent specifically to them. The security threat presented by sniffers is their ability to capture all incoming and outgoing traffic, including clear-text passwords and usernames or other sensitive material. In theory, it's impossible to detect these sniffing tools because they are passive in nature, meaning that they only collect data. While they can be fully passive, some are not therefore they can be detected Packet sniffer is a program running in a network attached Device that passively receives all data link layer frames passing through the device's network adapter. It is also known as Network or Protocol Analyzer or Ethernet Sniffer. The packet sniffer captures the data that is addressed to other machines, saving it for later analysis. It can be used legitimately by a network or system administrator to monitor and troubleshoot network traffic [1].**

**Index Terms – Packet Sniffing, Network, Protocol.**

## 1. INTRODUCTION

The very first step in auditing networks is to define where to analyze the traffic. Taking a common scenario for analysis, the following assumptions were made. There is a switched network made up of a number of switches, several terminals and a file server. Network performance has dropped, however the cause is unknown. There is no IDS (Intrusion Detection System) that can alarm or inform about attacks or network malfunction. Also, it is known that there are no problems with the transfer rate of the file server to LAN (Local Area Network) terminals [3].

Furthermore, network equipment does not have Netflow protocols to analyze traffic remotely. Wireshark was chosen to analyze the above scenario. The first doubt which arises is where to install Wireshark. It would seem logical to install Wireshark on the file server itself to analyze the traffic that flows through this network segment. However, there could be situations in which there is no access to the server physically or quite simply for security reasons.

When a computer sends a data to the network, it sends in the form of packets. These packets are the blocks of data that are actually directed to the certain deputed system. Every sent data has its receiving point. So, all the data are directly handled by specific computer. A system reads and receives only that data which is intended for it. The packet sniffing process involves a collaborate effort between the software and the hardware. This process is broken down into three steps.

1. Packet sniffer collects raw binary data from the wire. Normally this is done by switching the selected network Interface into unrestrained mode.

2. The collected binary data is converted into readable form. 3. The packet sniffer collected all data, verifies its protocol and begins its analysis [1]. The help of ip and Mac address, we can gather the information of network traffic by using any packet scanner.

## 2. NETWORK MONITORING TOOLS

The packet sniffing tools analyse and filter the packets transmitted in the network. There are many packet sniffing tools. Some of them are as described as follows:-

A. Wireshark: Wireshark is an open source packet filter. It is used for analyse the network traffic. Wireshark sees all traffic visible on that interface, not just traffic addressed to one of the interface's configured addresses and broadcast/multicast traffic. Wireshark is a tool that "understands" the structure of different networking protocols [3].Wireshark has the ability to capture all of those packets that are sent and received on the network and it can decode them for analysis. When you do anything on the Internet, such as browse websites, use VoIP, IRC etc, and the data is always converted into packets when it passes through your network interface or your LAN card. Wireshark will hunt for those packets in your TCP/ IP layer during the transmission and it will keep, and present this data, on GUI [4].

B. TCPDUMP: Tcpdump is a packet filter that runs on the command line interface. It displays TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Tcpdump run on the Unixlike operating systems: Linux, Solaris, BSD and Mac OS. Tcpdump analyses network behaviour, performance and applications that generate or receive network traffic [1]. TCPDUMP can do so many works like; TCPDUMP views the entire data portion of an Ethernet frame or other link layer protocol. TCPDUMP analyses and filter the IP packet and ARP packets or any protocol at a higher layer than Ethernet.

C. Nmap: Nmap stands for network mapper. Nmap is an open source tool used to explore and audit the network. It can determine what hosts are available on the network, what services are enabled , operating system and the version of the host ,what type of firewalls are in place and many other aspects of the network using raw ip packets. Nmap is a command line tool. It can also be used by attackers to scan a network in order to harm it [5] NMAP can perform different types of scans such as:

Connect

- SYN Stealth
- FIN, Xmas, Null
- Ping
- UDP Scan
- IP Protocol Scan
- ACK Scan
- Window Scan
- RPC Scan
- List Scan
- FTP Bounce

D. Zenmap: Zenmap is a tool which is similar to nmap. It is an open source tool and easy to use as compared to nmap because it is based on graphical user interface. The main difference between the nmap and zenmap is that nmap is command line and zenmap is GUI. Features of zenmap are as follows:

a) Based on graphical user interface (GUI).

b) Identifies the hosts on the network.

c) Identifies the operating system.

d) Easy to use as compared to nmap[6]

## 3. SNIFFING METHODS

IP Based Sniffing [3] IP based sniffing is the most commonly used method of packet sniffing. In this method a requirement of setting network card into promiscuous mode exist. When network card is set into promiscuous mode then host will be able to sniff all packets. A key point in the IP based sniffing is that it uses an IP based filter, and the packets matching the IP address filter is captured only. Normally the IP address filter is not set so it can capture all the packets. This method only works in non switched network [3].

MAC based Sniffing [3]This is another method of packet sniffing. This is as like IP based sniffing. Same concept of IP based sniffing is also used here besides using an IP based filter. Here also a requirement of setting network card into promiscuous mode exists. Here in place of IP address filter a MAC address filter is used and sniffing all packets matching the MAC addresses [3].

ARP based Sniffing [3] This method works a little different. It does not put the network card into promiscuous mode. This is not necessary because ARP packets will be sent to us. This is an effective method for sniffing in switched environment. Here sniffing is possible due to of being stateless nature of Address Resolution Protocol [3].

## 4. COMPUTATIONAL EXPERIMENTS

The purpose of our is to provide a framework for capturing, injecting and analyzing network packets for .NET applications.

This tool is a fully managed cross platform library. The same assembly runs under Microsoft .NET as well as Mono on both 32 and 64bit platforms.

## 5. CONCLUSION

This paper proposes an approach to detect packets through packet sniffing. It includes some negative aspects but besides these negative aspects it is much useful in sniffing of packets. Packet sniffer is not only used for hacking purpose but also it is used for network traffic analysis, packet/traffic monitoring, troubleshooting and other useful purposes. Packet sniffer is designed for capturing packets and a packet can contain clear text passwords, user names or other sensitive material. Sniffing is possible on both non switched and switched networks. We can use some tools to capture network traffic that are further used by researchers. We can conclude that packet sniffers can be used in intrusion detection. There exist some tools also that can be used for intrusion detection. In Future, Thus we can say that packet sniffing is a technique through which we can create an intrusion and through which we can detect an intrusion.

## REFERENCES

[1] EtherealPacketSniffing,Available:netsecurity.about.com/od/readbookreviews/gr/aapro52304.htm.
[2] Pallavi Asrodia, Hemlata Patel, "Network traffic analysis using packet sniffer", International Journal of Engineering Research and Application (IJERA), Vol.2, pp. 854-857, Issue 3, May-June 2012.
[3] Ryan Splanger, "Packet sniffing detection with Anti sniff", University of Wisconsin-Whitewater, May 2003.
[4] Tom King, "Packet sniffing in a switched environment", SANS Institute, GESC practical V1.4, option 1, Aug 4th 2002, updated june/july 2006.
[5] RyanSpangler, "Packetsniffingonlayer2switchedlocalareanetworks", PacketwatchResearch:http://www.packetwatch.net, Dec 2003.
[6] Sconvery, "HackingLayer2:FunwithEthernetSwitches", Blackhat, 2002, Available: http://www.blackhat.com/ presentations/bh-usa-02/bh-us-02-convery-switches.pdf.
[7] http://www.monkey.org/dufsong/dsniff/.
[8] http://www.fish2.com/cops/overview.html.
[9] http://nongnu.org/tiger/.
[10]http://www.securityteam.com/unixfocus/Detecting sniffers on your network .html.