International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 01, January 2017
www.ijates.com
ijates
ISSN 2348 - 7550

COMPARATIVE ANALYSIS OF PACKET SNIFFERS : A STUDY

Jyoti
Senior Engineer, Bharat Electronics Limited (India)

ABSTRACT

Today everything is being centralized through a common dedicated network to ease its use, make it more user friendly and increase its efficiency. The size of these centric networks is also increasing rapidly. So the management, maintenance and monitoring of these networks is important to keep network smooth and improve economic efficiency. Packet sniffing or packet analysis is the process of capturing data passed over the local network and looking for any information that may be useful. There is a wide variety of packet sniffers available in the market that can be exploited for this purpose. This paper focuses on the basics of packet sniffer, its working principle and a comparative study of various packet sniffers.

Keywords: Packet Capture; Packet Sniffer; network monitoring; wireshark; NIC

I INTRODUCTION

A packet sniffer is a program that can see all of the information passing over the network it is connected to. As data steams back and forth on the network the program looks at it or 'sniffs' each packet. A packet is a part of a message that has been broken up. Packet analysis can help us understand network characteristics, learn who is on network, determine who or what is utilizing available bandwidth, identify peak network usage times, identify possible attacks or malicious activity, and find unsecured and bloated applications[1].

II WORKING

There are two modes in which a network interface of a machine work i.e Promiscuous and Non-promiscuous. Promiscuous mode in one in which the NIC of the machine can take over all packets and a frame it receives on network, namely this machine (involving its software) is sniffer. As shown in the following diagram*[2]*

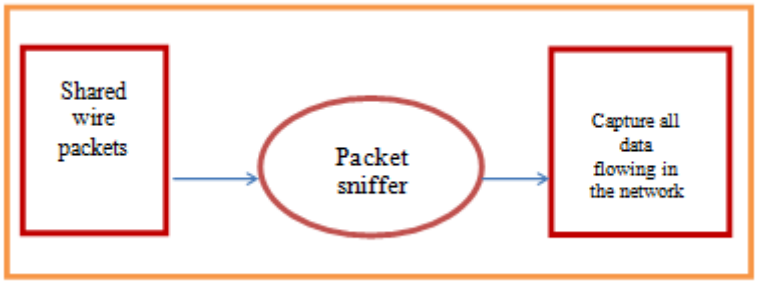

Fig. 1 Promiscuous Mode

When a data packet is transmitted in non-promiscuous mode, all the LAN devices "listen to" the data to determine is the network address included in the data packet is theirs. If it isn't, the data packet is passed onto

the next LAN device until the device with correct network address is reached. That device receives and reads the data. As shown in the diagram:-

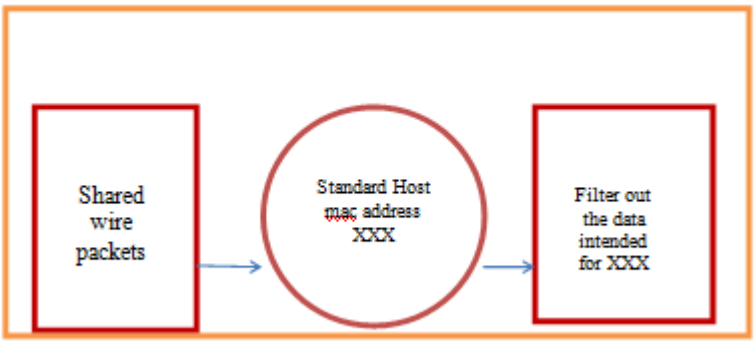

Fig. 2 Non- Promiscuous Mode

2.1 Components

Sniffer is a combination of hardware and software. Different sniffers may have various configurations on account of designation and final usage, but basically, a sniffer is composed of four parts:

- **Hardware: -** most sniffing products can work with standard adapters. Some sniffers only support Ethernet or wireless adapters whereas others support multi-adapters and allow customization.
- **Drive program: -** this is a core component of a sniffer. Each sniffing product has its own drive program, only after completing installation can a sniffer start to capture traffic and data from network.
- **Buffer: -**a buffer is a storage device for captured data from network. In general, there are two modes of buffers: keep capturing until the storage place full, or keep capturing and overflowing as the latest captured data keep replacing the oldest data.
- **Packet Analysis:-**packet analysis can be done on real time or we can analyze packets after storing it. We can analyze both header and actual data, when we store data in memory or we perform real time analysis, decoder is used to decode the data store in packets.

2.2 Working Principle

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 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.[3]

2.3 WIRESHARK

Wireshark, known as Ethereal until a trademark dispute in summer 2006, is an open source multi-platform network protocol analyzer. A TcpDump like non-GUI console version named Tshark in included. It runs on LINUX, OS X, BSD, Solaris, some other Unix like operating system and on Microsoft windows. Wireshark is very similar to TcpDump, but has a graphical front-end, plus some integrated sorting and filtering options. Wireshark lets the user put NIC that supports 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.Being in promiscuous mode, isn't necessarily sufficient as all the traffic through the switch is not necessarily sent to the port where capturing is done.

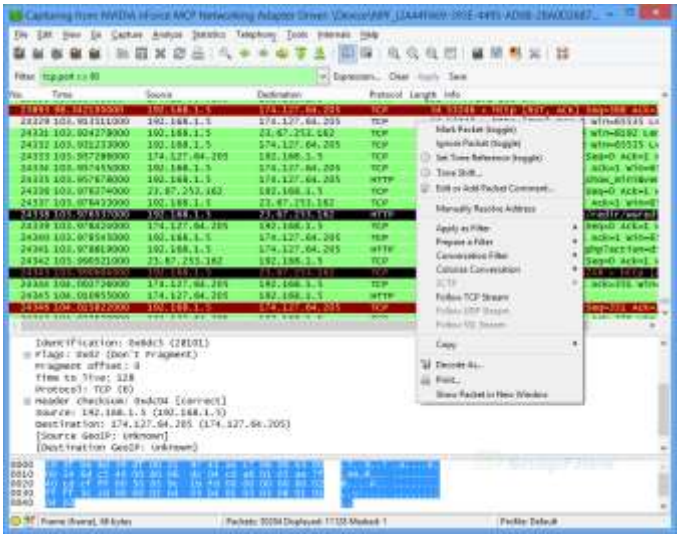

Fig. 3Wireshark Tool

2.4 TCPDUMP

TCPDUMP is a packet filter that runs on the command line interface and parsing tool ported to several platforms. It allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which computer is attached. TCPDUMP works by capturing and displaying packet headers and matching them against a set of criteria. TCPDUMP is accompanied by the lipcap library. Lipcap is a C library for capturing packets. The procedures included in lipcap provide a standardized interface to all common (Unix-based) operating systems, including Linux and FreeBSD. The interface of the lipcap is usable even under windows but there the library is called Wincap. TCPDUMP analyzes and filter IP packet and ARP packets or any protocol at a higher layer than Ethernet.[4]

TCPDUMP is very economical in terms of memory because its installation file is just 484KB. But TCPDUMP doesn't have a user friendly graphical user interface(GUI). So the user has to study those commands and get acquainted with the commands prompt like screen. TCPDUMP doesn't analyze the packet, it just able to report only what it finds in the packet. If any IP address is forged in the packet, TCPDUMP has no ability to report anything else. For large network centric systems where millions of messages flow in between the different modules, it's very difficult to debug using TCPDUMP. It lacks precision in displaying the particular message

required. It is not suitable for integration and testing of large network centric systems where millions of message flow and precision is required in displaying the message contents and that tool should be efficient also[5].

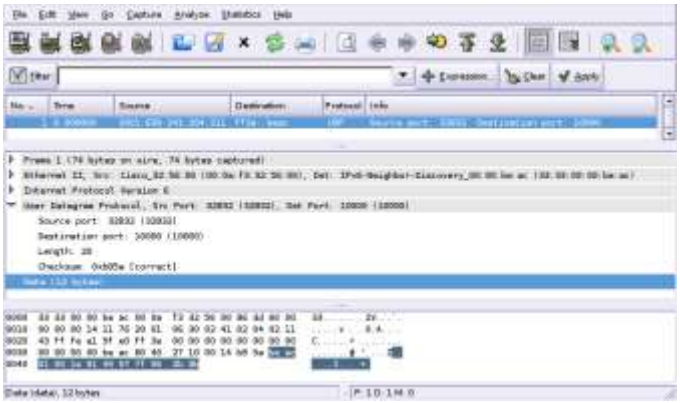

Fig. 4 TCPDUMP Tool

2.5 CASPA

CASPA is a powerful network analysis tool. It consists of a well-integrated set of functions that can resolve network problems. CASPA can list all of the network packets in real-time from multi-network card and can also support capturing packets based on applications. You can capture and observe all traffic of the application which is a potential issue. The CASPA GUI eliminates the learning curve and makes it easy to understand and simple to use. It has several plug-ins for different protocols such as Ethernet, IP, TCP, UDP, PPP, SMTP, POP3 and so on.[6]

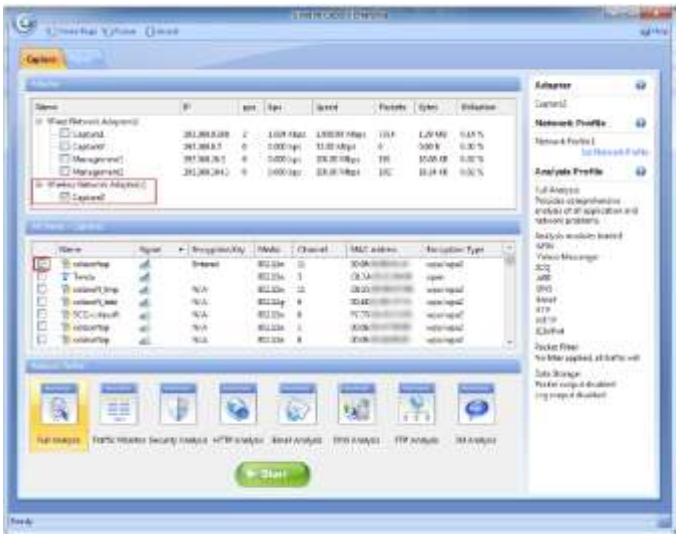

Fig. 5 CASPA Tool

I. ETHERAPE

EtherApe is a graphical network monitor for Unix modeled after etherman. Featuring link layer, IP andTCP modes, it displays network activity graphically. Hosts and links change in size with traffic. Colorcoded protocols display.It supports Ethernet, FDDI, Token Ring, ISDN, PPP, SLIP and WLAN devices, plus severalencapsulation formats. It can filter traffic to be shown, and can read packets from a file as well as livefrom the network.Node statistics can be exported.[7]

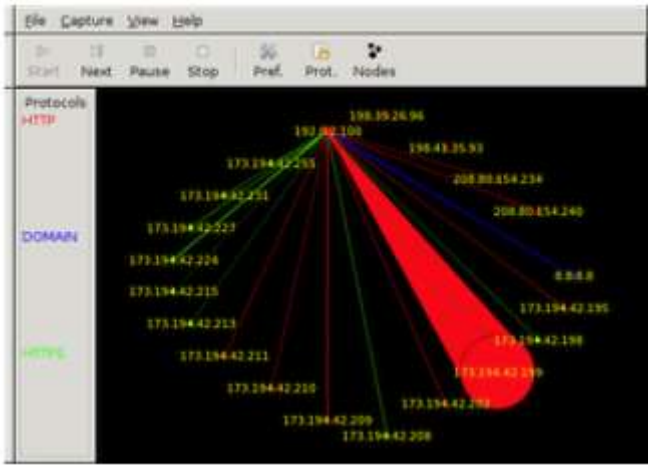

Fig. 6 Etherape Tool

III SOFTPERFECT NETWORK PROTOCOL ANALYZER

SoftPerfect Network Protocol Analyzer is a free professional tool for analyzing, debugging, maintaining and monitoring local networks and Internet connections. Itcaptures the data passing through the dial-up connection or Ethernet network card, analyses this data and then represents it in a readable form.This is a useful tool for network administrators, security specialists, network application developers and anyone who needs a comprehensive picture of the trafficpassing through their network connection or a segment of a local area network.

SoftPerfect Network Protocol Analyzer presents the results of its analysis in a convenient and easily understandable format. It can defragment and reassemblenetwork packets into streams. The program also features full decoding and analysis of network traffic based on the following low-level Internet protocols: AH, ARP,ESP, ICMP, ICMPv6, IGMP, IP, IPv6, IPX, LLC, MSG, REVARP, RIP, SAP, SER, SNAP, SPX, TCP and UDP. It also performs a full reconstruction of top-level protocols such as HTTP, SMTP, POP, IMAP, FTP, TELNET and others.The flexible system of fully-configurable filters can be used to discard all network traffic except for the specific traffic patterns you wish to analyze. There is also a packet builder, which allows you to build your own customnetwork packets and send them into the network. You could use the packet builder feature to check the network's protection againstattacks and intruders. [8]

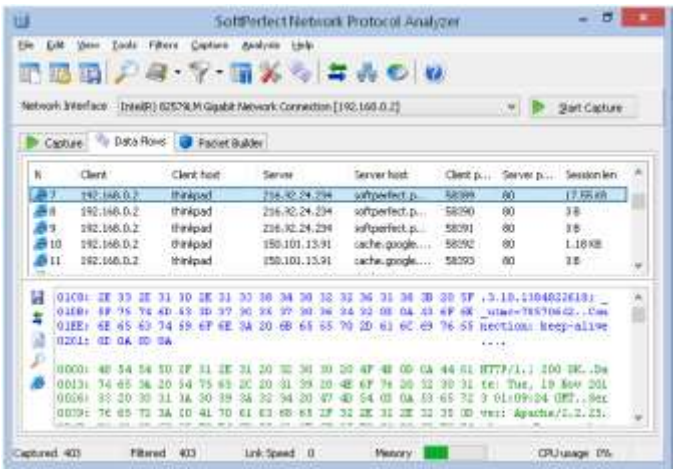

FIG. 7 SOFT PERFECT NETWORK PROTOCOL ANALYZER

IV CONCLUSION

In this paper we have analyzed various packet sniffing tools that monitor the data traffic over the network it is used. Packet sniffer isn't just a hacking tool; it can also be exploited for useful purposes. It can be used over a switched or non-switched dedicated network to monitor its traffic, analyze it and do troubleshooting if required. Of all the tools we have analyzed above, have some limitations. Some have memory issues, some doesn't analyze data, some have data filtering issue while some have GUI problem. If packet sniffing need to be used for penetration testing against a particular network for integration and other purposes then a packet sniffer need to be developed which overcome the above limitations and provide better filtering, better analysis of data for troubleshooting. At the end we conclude that packet sniffing concept can be exploited for integration and testing of network with heavy traffic flow.

REFERENCES

[1] (Chris Sanders and Chris Sanders, "Practical Packet Analysis" Pub. Date: May 17, 2007 ISBN-13:978-1-59327-149-7)

[2] Qadeer M.A., Zahid M., Iqbal A., Siddiqui M.R "Network Analysis and Intrusion Detection Using Packet Sniffer ICCSN ' Second International Conference, 2010, Page(s): 313 – 317

[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 vol.1 no.1 pp. 55-58(2012).

[4] S. McCanne and V.Jacobson. "The BSD Packet Filter: New Architecture for User Level Packet Capture", *USENIX Conference*, January, Pages 259-270(1993)..

[5] Dulal C. Kar Felix Fuentes. Ethereal vs. tcpdump: A comparative study on packet sniffing tools for educational purpose. Journal of Computing Sciences in Colleges archive, Volume **20**(4), pp 169-176, (2005)..

[6] All about capsa [Online] Available www.colasoft.com.

[7] All about Tools [Online] Available: http://www. sectools.org.

[8] All about soft perfect network protocol analyzer [Online] Available http://www.softperfect.com/products/networksniffer/