Research Article Impact Factor: 0.621 ISSN: 2319-507X
Sonali Karale, IJPRET, 2014; Volume 2 (9): 654-661 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

PACKET SNIFFING

MS. SONALI A. KARALE[1], MS. PUNAM P. HARKUT[2]
HVPM COET Amravati.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: With the development and popularization of network Technology, the management, maintenance and monitoring of network is Important to keep the network smooth and improve Economic efficiency. For this purpose packet sniffer is used. Packet sniffing is important in network monitoring to troubleshoot and to log network activities which will benefit both the network Software engineers and network administrators. There are various packet sniffers are available in market by which we can perform packet sniffing. This paper focuses on the basics of packet sniffer; it's working Principle and various packets sniffing tools their working and their capabilities for network monitoring and analysis. Packet sniffing is important in network monitoring to troubleshoot and to log network. Packet sniffers are useful for analyzing network traffic over wired or wireless networks. This paper focuses on the basics of packet sniffer; it's working Principle which used for analysis Network traffic. A technique in which attackers surreptitiously insert a software program at remote network switches or host computers. The program monitors information packets as they are sent through networks and sends a copy of the information retrieved to the hacker. By picking up the first 125 keystrokes of a connection, attackers can learn passwords and user identifications, which, in turn, they can use.

Keywords: Packet capture, Network Monitoring, Packet sniffer.

PAPER-QR CODE

Corresponding Author: MS. SONALI A. KARALE

Access Online On:

www.ijpret.com

How to Cite This Article:

Sonali Karale, IJPRET, 2014; Volume 2 (9): 654-661

INTRODUCTION

A packet sniffer is a wire-tap devices software that plugs into computer networks and eavesdrops on the network traffic. Like a telephone wiretap. Allows us to listen in on other people's conversations. A "sniffing" program lets someone listen in on computer conversations. A packet sniffer is a device that is used by network administrators to monitor the data that is being transmitted over a network. Packet sniffers are used for network management and network security and they can also be used by unauthorized users to scheduling. A device is added between your server and the Web. It listens and analyzes requests sent and received by the server. This method does not require adding any tags to the page content, but does involve installing additional hardware and/or software in (all) datacenter(s) serving content to be tracked. This may present scalability challenges for large sites.

2.TYPES OF PACKET SNIFFING

ARP Sniffing: ARP sniffing involves information packets that are sent to the administrator through the ARP cache of both network hosts. Instead of sending the network host. Instead of sending the network traffic to both host. It forwards the traffic directly to the administrator.

IP Sniffing: IP sniffing works through the network card by sniffing all of the information packets that correspond with the IP address filter. This allows the sniffer to capture all of the information packets for analysis and examination.

MAC Sniffing: MAC sniffing also works through a network card which allows the device to sniff all of the information packets that correspond with the MAC address Filter.

3.THE TERM USED IN SNIFFING

Ethernet MAC address

Since many machines may share a single Ethernet wire, each must have an individual identifier. This doesn't happen with dial-up modems, because it is assumed that any data you send to the modem is destined for the other side of the phone line. But when you send data out onto an Ethernet wire, you have to be clear which machine you intend to send the data to. Sure, in many cases today there are only two machines talking to each other, but you have to remember that Ethernet was designed for thousands of machines to share the same wire. This is accomplished by putting a unique 12-digit hex number in every piece of Ethernet hardware. Raw transmission and reception on Ethernet is governed by the Ethernet equipment. You just can't send data raw over the wire, you must first do something to it that Ethernet understands. Following a is a brief explanation how this works:

Packet Sniffing from FTP connection

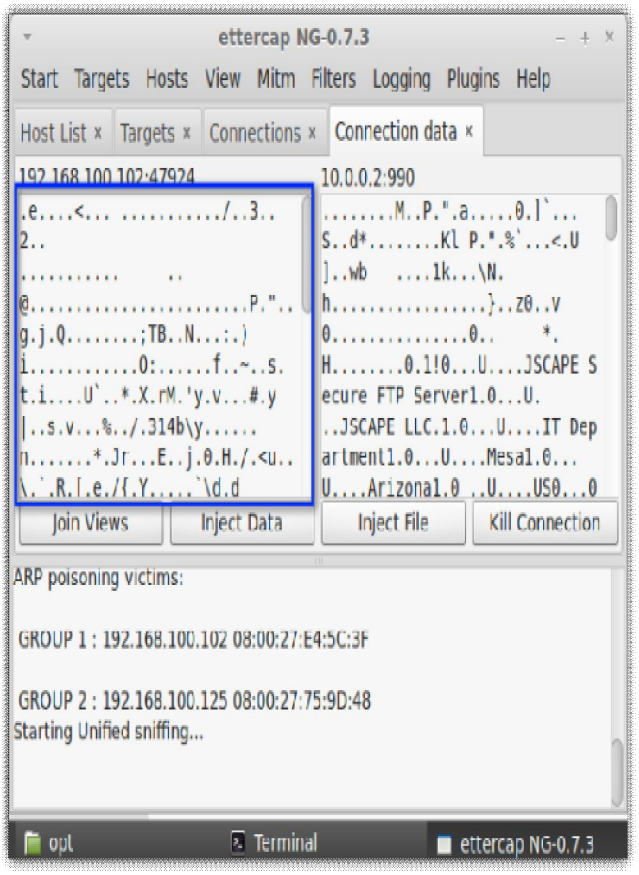

Fig.3.1Packet sniffer FTP Connection

4. How a Packet Sniffer Works

A Packet sniffer can view a wide variety of information that is being transmitted over the network as well as the network it is linked to packet sniffers exist in the form of software of hardware and can capture network traffic that is both inbound and outbound and monitor password use and user names along with other sensitive information. A Packet sniffer allows you to set the interface of the network to view all of the information that is transmitted over the network. When the data passes through the system, it is captured and stored in memory so the information can be analyzed.

The packet sniffer gets its name from normal computer usages where the individual computer inspects packets of data that match the address of the computer. However, with a packet

sniffer, it can examine all of the data from all of the computers that are connected to the network by viewing every packet that is sent over the network. A Packet sniffer that is sent over the network by viewing. But Packet Sniffers set up on a computer work slightly differently. Instead of just picking up the packets that are addressed to them, they set their network cards to what's known as ***promiscuous mode*** and grab a copy of every packet that goes past. This lets the packet sniffers see all data traffic on the network segment to which they're attached - if they're fast enough to be able to process all that mass of data, that is. This means that it is looking at everything that comes through. The amount of traffic largely depends on the location of the computer in the network. A ***client system*** out on an isolated branch of the network sees only a small segment of the network traffic, while the main domain server sees almost all of it.

A packet sniffer can usually be set up in one of the two modes:

Unfiltered - captures all of the packets

Filtered - captures only those packets containing specific data elements

Packets that contain targeted data are copied onto the hard disk as they pass through. These copies can then be analyzed carefully for specific information or patterns.

When you connect to the Internet, you are joining a network maintained by your Internet service provider (ISP). The ISP's network communicates with networks maintained by other ISPs to form the foundation of the Internet. A packet sniffer

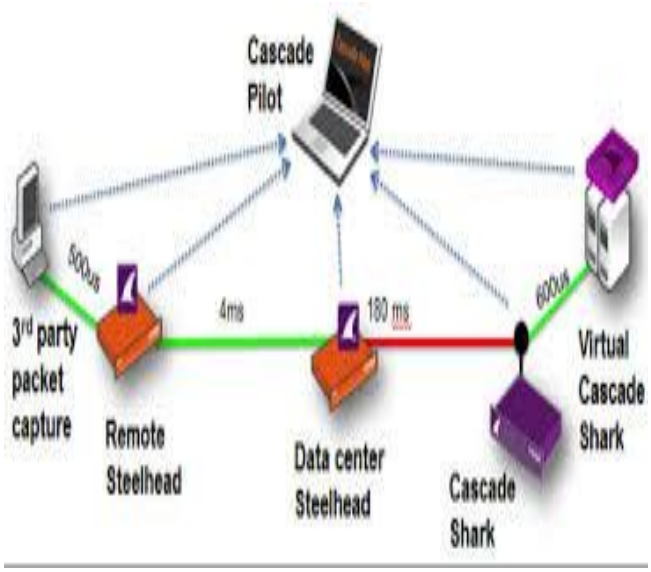

Fig.4.1 Packet sniffer work in data center

5.The components of a packet sniffer

A. 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, jitters, negotiation errors, and so forth.

B. Capture driver

Once the frames are captured from the network, they are stored in a buffer. There are a couple captures modes: capture until the buffer fills up, or use the buffer as a "round robin" where the newest data replaces the oldest data. Some products (like the Black ICE Sentry IDS from Network ICE) can maintain a full round-robin capture buffer on disk at full 100-mbps speeds. This allows have hundreds of gigabytes of buffer rather than the meager 1-gigabyte you're likely to have in a memory-based buffer.

C. Real-time analysis

Pioneered by the Network General Sniffer, this feature does some minor bit of analysis of the frames as they come off the wire. This is able to find network performance issues and faults while capturing. Real-Time display of captured packets, incoming Network packets will be immediately decoded and added to the Packet list, this eats up a whole lot of resources.

D. Decode

This displays the contents of network traffic with descriptive text so that an analysts can figure out what is going on. In the Packet Decoding view packets are decoded and displayed in a format that is comprehensible.

E. Packet editing/transmission

Some products contain features that allow you to edit your own network packets and transmit them onto the network.

6. WHY PACKET SNIFFING WORKS?

The reason that packet sniffing works is due to the way Ethernet networks send their packets. Ethernet was built around a "shared" principle: all machines on a local network share the same wire. Any time that a PC sends out a packet, it is sent out as a broadcast. This implies that all machines are able to "see" all the traffic on the 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". In order to sniff on the wire, a driver must be written that both puts the adapter into promiscuous mode, as well as buffers the incoming frames.

As mentioned, packet sniffing works by making a copy of each packet as it flows across the network. In the past, it has been difficult to tell if anyone on your network is engaging in packet sniffing. After all, no one is hacking into a server or anything, so the audit logs wouldn't indicate any sort of unusual activity. A person who's packet sniffing is merely reading information as it comes to them.

7. CAPTURING OF PACKETS BY SNIFFERS

A sniffer captures the data coming in and going out of the Network Interface card or modem and displays that information in a table.

the analysis of a captured frame

The following is a captured frame that is actually an HTTP GET request issued from my PC to another host. This frame was captured using the Windows NT Server (4.0) Network Monitor.

3C	2E	AC	00	01	01	00	01	D0	E1	66	80	08	00	45	00
01	F7	E8	80	40	00	80	06	39	40	C2	7E	57	A5	D1	01
EC	1A														

Fig.2A Captured Frame

Each box represents a byte of the frame. The number in each box is actually a hexadecimal number. This frame can be broken down into different parts:

The Ethernet header - Bytes 1 to 14

The IP header - Bytes 15 to 35

The TCP header - Bytes 36 to 56

The actual data i.e. the HTTP GET request.

The Ethernet Header

3C	2E	AC	00	01	01	00	01	D0	E1	66	80	08	00	

Fig. 7.1 The Ethernet Header

The Ethernet header is 14 bytes long. Ethernet operates at the Network Access layer and is a type of data link protocol.

CONCLUSIONS

Thus Sniffers capture packet traffic across a network, usually an Ethernet. These can be placed surreptitiously on your drives. A sniffer can catch all packet traffic on a particular network block (or segment). Prevention of compromise is a two-fold process: encryption and compartmentalization. Encrypted communications can be used to prevent the capture of passwords if a sniffer attack is underway. It can be assert that one can benefit greatly by running a sniffer on a network, even if only for a day. This will familiarize him with what problems are faced to implement various attacks. Also, if one is proficient with a sniffer, one can see for himself what type of information can actually be gleaned from your particular network configuration Packet sniffer is a network monitoring tool. It can be used for network traffic monitoring, traffic analysis, troubleshooting and other useful purposes. There are many available tools used to capture network traffic that researcher used in their work, but there is a

REFERENCES

1. S. Ansari, Rajeev S.G. and Chandrasekhar H.S., "Packet Sniffing: A Brief Introduction", *IEEE Potentials*, Dec 2002-Jan. 2003, Volume: 21 Issue: 5, pp: 17-19 (2002-2003).

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

3. A. Dabir, A. Matrawy, "Bottleneck Analysis of Traffic Monitoring Using Wireshark", 4th International Conference on Innovations in Information Technology, 2007, IEEE Innovations '07, 18-20 Nov. (2007), Page(s): 158-162(2007).

4. UltimateSniffin' the Ether v2_0. http://networking.earthweb.com

5. Tapping across a network. http://www.wiretapped.net/

6. Qadeer M.A., Zahid M., Iqbal A., Siddiqui M.R "Network Traffic Analysis and Intrusion Detection UsingPacketSniffer"ICCSN'10 *Second International Conference*, (2010), Page(s): 313-317(2010).

7. A. Dabir, A. Matrawy, "Bottleneck Analysis of Traffic Monitoring Using Wireshark", 4th International Conference on Innovations in Information Technology, 2007, IEEE Innovations '07, 18-20 Nov. (2007), Page(s): 158-

8. SnifferPackages. http://packetstormecurity.org and http://www.wiretapped.net

9. Sniffers –the Network Analyzers http://www.networkingunlimited.com

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

11. All about Wireshark [Online] Available http://www.wireshark.org/.

12. All about Tcpdump [Online] Available http://www.tcpdump.org/.

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

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

15. Bo Yu" Based on the network sniffer implement network monitoring Computer Application and System Modeling (ICCASM), 2010 *International Conference on Volume:* 7, 2010, Page(s): V7-1-V7-3(2010). *Conference*, January, Pages 259-270(1993).

16. 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).

17. S. Mc Canne and V. Jacobson. "The BSD Packet Filter: New