Packet Sniffing: Monitoring and Analysis Using Sniffing Method

Mrs. R. Kirubakumari.MPhil [#1], S. Saranya *[2]
[#1] Head of the department,
PG &Research department of computer science &computer applying,
Padmavani arts and science college for women,
Salem 11.

*[2] Padmavani arts and science college for women,
Salem 11.

Abstract

A sniffer is an application that can capture network packets. Sniffers are also known as network protocol analizers. While protocol analyzers are really network troubleshooting tools, they are also used by hackers for hacking network. If the network packets are not encrypted, the data within the network packet can be read using a sniffer. Sniffing refers to the process used by attackers to capture network traffic using a sniffer. Once the packet is captured using a sniffer, the contents of packets can be analyzed. Sniffers are used by hackers to capture sensitive network information, such as passwords, account information etc. Today we are seeing that computer networks are increasing in their sizes very rapidly. Number of its user increased in past few years and traffic flows in networks also increased, so it's very important to monitor networks traffic as well as its user's activities to keep the network smooth and efficient. For complex network it's very tough task to maintain and monitor the network, because large amount of data available. For this purpose packet sniffing is used. Packet sniffing is important in network monitoring to watch network activities which help network administrators to find out problems.

Keyword

Network monitor, Packet capture, Network Monitoring, Network analysis, Packet sniffing.

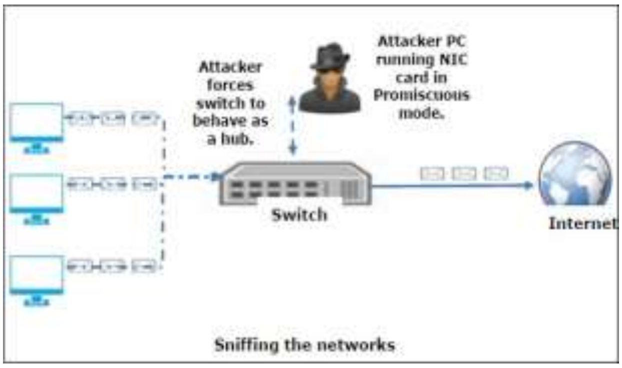
1. Introduction

Packages are the basis of all data sent on the Internet, although they are often used in an insecure manner. The manipulation of the live packages and the process that takes to alter the packets that travel through the network are becoming easier. Packet detection is commonly described as monitoring packets as they pass through a network. The packet sniffer is usually software based, but it can be pieces of hardware installed directly across the network. The crawlers can go beyond the network hosts seen in local area networks (LANs) that only handle data that is sent to them specifically. Packet Sniffing mainly used in network management, monitoring and ethical hacking. To perform sniffing we use tool named packet sniffer.

A packet tracker, sometimes called a network analyzer, that can be used by a network administrator to monitor and troubleshoot network traffic.

2. Concept of Packet Sniffing

Machines connected to a network send data to other machines in a format called packages. The packages are essentially the pieces of data that must be transferred from the origin to the destination and then pass through many intermediate devices. Create information packages. Visiting all websites, sending emails and sending instant messages use the package as their most basic transportation. A node whose NIC is set in the promiscuous mode receives all information travels in network. The NIC is a Short for Network Interface Card, the NIC is also referred to as an Ethernet card and network adapter. It is an expansion card that enables a computer to connect to a network. When NIC accept packets, packets are copied to driver memory then it passes to kernel and kernel passes it to user application.


Attacker forces switch to behave as a hub.
Attacker PC running NIC card in Promiscuous mode.
Switch
Internet
Sniffing the networks

Conceptualization of NIC

A network interface card (NIC) is a circuit board or card that is installed in a computer so that it can be connected to a network. NIC is also referred to as an Ethernet card and network adapter.

Unswitched Network

Since all the machines in a non-switched LAN are connected to the same hub, packets of any connected networks are sent to all machines on the local network. When packets get packets, they are sent to the entire LAN.

However, if they are not sent specifically, the machines will not pay attention to the package. There is a way to change this. By changing the state of the machine in "Miscellaneous mode", the network interface controller (NIC) on the machine is determined for any machine, but it can check the packets passed through it. This is the easiest way to smell a cable. Switched networks, separate from non-switched hubs, become fast and cheap over time. So most non-switched networks have been converted to a switched network.

Switched Network

In antiquity, when everyone used hub-based networks, packet detection was as easy as connecting a laptop to a port in one of those hubs. Although the most modern switching networks provide more efficiency and speed to move network data, they can be a headache for those who analyze packets in a network.

Switch networks are a switch connected to the entire hub instead of each hub. Each machine in the switch keeps track of the machines using information as unique mac addresses. When the packet reaches a specific MAC address, the switch sends it through the cable to the specified machine. If a package switch comes for a machine that does not save, it will send an ARP request to get machine names in the network. Then, when a match is found, it caches the information and sends the packet to that machine. These traffic can be sent directly to the destination. The crawler, therefore, can not get access to the traffic by tracking the wire.

How does a packet sniffer work?

A packet sniffer works by looking at every packet sent in the network, including packets not intended for itself. This is accomplished in a variety of ways. These sniffing methods will be described below. Sniffers also work differently depending on the type of network they are in. Here is a good set of definitions I found on the two types of Ethernet environments.

Shared Ethernet: In a shared ethernet environment, all hosts are connected to the same bus and compete with each other for bandwidth.In such an environment, packets destined for a machine are received by all other machines. Therefore, in any such environment, any machine installed in various modes will be able to capture the packet of the other machines and therefore, all the traffic on the network can be heard.

Switched Ethernet: An Ethernet environment that is connected to a host instead of a host is called a switched Ethernet. The switch maintains a table that tracks the MAC address of each computer and provides specific pockets for a machine in the port where it is connected.

The switch is an intelligent device that sends packets to the intended equipment only and does not transmit to all the machines in the network, as in the previous case. This switched Ethernet environment was intended for better network performance, but as an added benefit, a machine in promiscuous mode will not work here. As a result of this, most network administrators assume that sniffers don't work in a Switched Environment.

3. Sniffer Method

There are three types of sniffing methods. Some methods work in non-switched networks while others work in switched networks. The sniffing methods are:

IP-based sniffing, MAC-based sniffing, and ARP-based sniffing

IP-based sniffing

This is the original way of packet sniffing. It works by putting the network card into promiscuous mode and sniffing all packets matching the IP address filter. Normally, the IP address filter isn't set so it can capture all the packets. This method only works in non-switched networks.

MAC-based sniffing

This method works by putting the network card into promiscuous mode and sniffing all packets matching the MAC address filter.

ARP-based sniffing

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

4. How packet sniffer works

packet sniffer's working can be understood in both switched and non switched environment. For setup of a local network there exist machines.

When a non switched environment is considered then all nodes are connected to a hub which broadcast network traffic to everyone. So as soon as a packet comes in the network, it gets transmitted to all the available hosts on that local network. Since all computers on that local network share the same wire, so in normal situation all machines will be able to see the traffic

passing through. When a packet goes to a host then firstly network card checks it MAC address, if MAC address matches with the host's MAC address then the host will be able to receive the content of that packet otherwise it will forward the packet to other host connected in the network.

A switch is considered in the environment, all hosts are connected to a hub instead of a switch, it is called Ethernet switch. Since in switched environment packet sniffing is more complex in comparison to non switched network, because a switch does not broadcast network traffic. Switch works on unicast method, it does not broadcast network traffic, it sends the traffic directly to the destination host. This happens because switches have CAM Tables. These tables store information like MAC addresses, switch port and VLAN information. This is a table that stores both MAC addresses and IP addresses of the corresponding hosts. This table exists in local area network. Before sending traffic a source host should have its destination host, this destination host is checked in the ARP cache table. If destination host is available in the ARP cache then traffic will be sent to it through a switch, but if it is not available in the ARP cache then source host sends a ARP request and this request is broadcasted to all the hosts. When the host replies the traffic can be send to it. This traffic is sent in two parts to the destination host. First of all it goes from the source host to the switch and then switch transfers it directly on the destination host. So sniffing is not possible.

There are several methods through which we can sniff traffic in switched environment. These methods are:-

CAM Table Flooding

Content addressable memory table works by flooding the CAM tables. CAM table is a table that stores information like your MacH address and switch port with your virtual LAN information .A certain number of eateries are stored by CAM table due to of being its fix size. As its name implies "CAM table flooding" here flooding means floods the switch with MAC addresses and this is repeated till a point atwhere switch starts to broadcast network traffic.

Switch Port Stealing

As its name implies "switch port stealing" here in this method we have to steal the switches port of that host for which traffic is designed to send. When this switch port is stolen by the user then user will be able to sniff the traffic because traffic goes through the switch port first, then to the target host.

5. Sniffer Detection

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 aren’t therefore they can be detected. This paper discusses the different packet sniffing methods and explains how AntiSniff tries to detect these sniffing programs.

6. Packet Injection and Spoofing

Although not directly related to tracking, the other issue of significant value is the package's spoofing. When a packet is sent, their host has an IP address, but this address is not verified by the IP protocol. It can change the package of opponents and send users. An attacker might pretend to be someone else, hide their true location or hijack network traffic. Crawlers can use this vulnerability to change the contents of packages such as links and images. Therefore, only sniffer can not access your data, they can change what they see and do. It is important to protect against such attacks.

7. Protection

A clear hardware solution is switched to a switched network that has a personal line from a computer switch, so that an appliance can access another person's packets on the wire. Although it is not a perfect solution, it is best to use an obsolete non-switch network. Users can protect themselves from sniffers in different ways. The best defense against package detection and modification make contact with reliable sites, above all, Many sites do not use modern encryption methods to protect their users' confidential information. Most crawlers will have a hard time getting meaningful information when they are encrypted. An excellent way to protect encryption information.

Safe Guards

Good alert to take on link level and end-to-end encryption encryption trackers. Link layer encryption from node to node across the network, where the tracker usually listen. End-to-end encryption occurs in the last host, where the sender encrypts the host packets and decrypts the recipient host.

The best application-level encryption practices are SSL and TLS that protect the user interface level of applications. These are widely used and sites that do not use these precautions should be avoided. Sites that use any type of encryption will have "HTTPS" instead of "HTTP" and their modern information will display a green padlock beside the most recent browser site URL.

A virtual private network (VPN) is a powerful layer of security when using public internet. It allows a user to send all traffic to a secure server which will encrypt all data and manage user requests. Provides strong protection to a properly configured VPN user and provides a protection that is not guaranteed by a public Internet.

8. Conclusion

Packet sniffer is not just a hacker’s tool. It can be used for network traffic monitoring, traffic analysis, troubleshooting and other useful purposes. Packet sniffers can capture things like passwords and usernames or other sensitive information and Data is sent across the internet in the form of packets. Detection of packets can be used for any network or malicious purposes. You can help and monitor with traffic and network research. Opponents can also use it to steal data in plain text or observe the actions of a user. There are software to help detect a crawler in a network. Business systems often set up to maintain their information security. Without using modern security and best practices, attackers can easily view data transmitted over the network. It is important to access that the sites you access are using available security guards, which means that encryption and sites can not be avoided.

9. Reference

1. Dabir, A. Matrawy, "Bottleneck Analysis of Traffic Monitoring Using Wire shark", *4th* International Conference on Innovations in

Information Technology 2007 IEEE Innovations , Nov. 2007.

2. S. Ansari, S.G. Rajeev, H.S Chandrasekhar, "Packet Sniffing: A brief Introduction", IEEE Potentials Dec 2002–Jan 2003.
3. Pallavi Asrodia, Hemlata Patel, “Network traffic analysis using packet sniffer”, International Journal of Engineering Research and Application (IJERA),June 2012.
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. AbdelallahElhadj H., Khelalfa H., and Kortebi H., “An Experimental Sniffer Detector: SnifferWall,” Technical Document, Securie des Communications sur Internet, 2002.
6. Khan A., Qureshi K., and Khan S., “Enhanced Switched Network Sniffer Detection Technique Based on IP Packet Routing,” Computer Journal of System Security 2009.
7. A. Dabir, A. Matrawy, “Bottleneck Analysis of Traffic Monitoring Using Wireshark”, 4th International Conference on Innovations in Information Technology, 2007.
8. Asrodia, Pallavi, and Hemlata Patel. "Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis." International Journal of Electrical, Electronics and Computer Engineering (2012)

.

9. Trabelsi Z., “Switched Network Sniffers Detection Technique Based on IP Packet Routing,” Computer Journal of System Security Journal, 2005.
10. Qadeer M.A., Zahid M., Iqbal A., Siddiqui M.R “Network Analysis and Intrusion Detection Using Packet Sniffer ICCSN ' Second International Conference, 2010.
11. Liqiang Zhang, Huanguo Zhang “An Introduction to Data Capturing” International Symposium on Electronic Commerce and Security.
12. "4 Ways to Avoid Packet Sniffing and Data Theft." Hacker Not Cracker. N.p., n.d. Web. Dec. 2015.