Packet sniffing

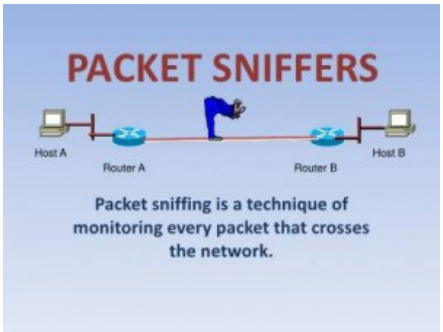
Packet Sniffing Abstract

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

Packet Sniffing Video

what is Packet Sniffing?]
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.

Packet sniffers can capture things like clear-text passwords and usernames or other sensitive material. Packet sniffers are a serious matter for network security. Since sniffing is possible on non-switched and switched networks, it's a good practice to encrypt your data communications



How packet sniffing works?

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.

Shared Ethernet:

In a shared Ethernet environment, all hosts are connected to the same bus and compete with one another for bandwidth. In such an environment packets meant for one machine are received by all the other machines. Thus, any machine in such an environment placed in promiscuous mode will be able to capture packets meant for other machines and can therefore listen to all the traffic on the network.

Switched Ethernet:

An Ethernet environment in which the hosts are connected to a switch instead of a hub is called a Switched Ethernet. The switch maintains a table keeping track of each computer's MAC address and delivers packets destined for a particular machine to the

port on which that machine is connected. The switch is an intelligent device that sends packets to the destined computer only and does not broadcast to all the machines on 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.

Sniffing methods

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.

1) 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.

2) MAC-based sniffing:-

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

3) ARP-based sniffing:-

This method works a little different. It doesn't put the network card into promiscuous mode. This isn't necessary because ARP packets will be sent to us. This happens because the ARP protocol is stateless. Because of this, sniffing can be done on a switched network. To perform this kind of sniffing, you first have to poison the ARP cache1 of the two hosts that you want to sniff, identifying yourself as the other host in the connection. Once the ARP caches are poisoned, the two hosts start their connection, but instead of sending the traffic directly to the other host it gets sent to us. We then log the traffic and forward it to the real intended host on the other side of the connection. This is called a man-in-the-middle attack.

Types of Sniffers

Today, sniffers exist in two broad varieties:

- The first is a stand-alone product incorporated into a portable computer that consultants can carry to customer sites and plug into the network to gather diagnostic data.
- The second is part of a larger package of network-monitoring hardware and software for helping organizations keep tabs on their LANs, WANs and Web services.

Thus Commercial packet sniffers are used to help maintain networks. Underground packet sniffers are used to break into computers.

Component of Packet-sniffing

- Hardware : standard network adapters .
- Capture Filter : This is the most important part . It captures the network traffic from the wire, filters it for the particular traffic you want, then stores the data in a buffer.
- Buffers : used to store the frames captured by the Capture Filter .
- Real-time analyzer: a module in the packet sniffer program used for traffic analysis and to shift the traffic for intrusion detection.
- Decoder :- "Protocol Analysis" . it's analysis to all protocol

TOP 10 Packet sniffers]
1.Wireshark
2.Kismet
3.Tcpdump
4.Cain and Abel
5.Ettercap
6.Dsniff
7.NetStumbler
8.Ntop
9.Ngrep
10.EtherApe

Packet Sniffers Advantages]

- Capturing clear-text usernames and passwords
- Capturing and replaying Voice over IP telephone conversations
- Mapping a network
- Breaking into a target computer and installing remotely controlled sniffing software.
- Redirecting communications to take a path that includes the intruders computer.
- Conversion of Network traffic into human readable form.
- Network analysis to find the bottlenecks.
- Network intrusion detection to monitor for attackers.