Packet Sniffer Detection with AntiSniff

Ryan Spangler
University of Wisconsin - Whitewater
Department of Computer and Network Administration

May 2003

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. 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. While packet sniffers can be fully passive, some aren't, therefore they can be detected. This paper discusses the different methods that AntiSniff uses to detect these sniffing programs.

Table of Contents

1.0 Introduction

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.

2.0 What is a packet sniffer?

A packet sniffer is a tool that plugs into a computer network and monitors all network traffic. It monitors traffic destined to itself as well as to all other hosts on the network. Packet sniffers can be run on both non-switched and switched networks.

2.1 Uses of a packet sniffer

Sniffing programs are found in two forms. Commercial packet sniffers are used to help maintain networks, while underground packet sniffers are used by attackers to gain unauthorized access to remote hosts. Listed below are some common uses of sniffing programs:

- Searching for clear-text usernames and passwords from the network.
- Conversion of network traffic into human readable form.
- Network analysis to find bottlenecks.
- Network intrusion detection to monitor for attackers.

3.0 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. This information was taken from an article on LinuxJournal.com by Sumit Dhar.

- 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.

3.1 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.

3.1.1 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.

3.1.2 MAC-based sniffing

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

3.1.3 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 cache[1] 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. See Diagram 1 for a general idea of the way it works.

[1] Here is a paper that explains ARP poisoning (http://www.node99.org/projects/arpspoof/arpspoof.pdf).

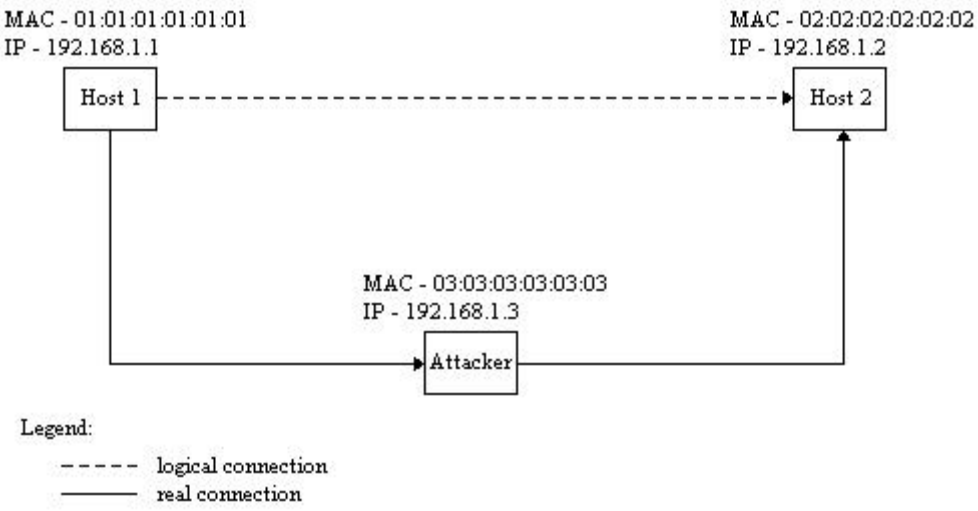

Diagram 1: ARP sniffing method

4.0 AntiSniff detection methods

AntiSniff is a tool made by L0pht Heavy Industries designed to detect hosts on an Ethernet/IP network segment that are promiscuously gathering data. The most current version (1.02.1) is designed to work on a non-switched network. AntiSniff performs different types of tests to determine whether a host is in promiscuous mode. The tests are broken down into the following three classes: DNS tests, operating system specific tests, and network and machine latency tests. These tests are described below.

4.1 DNS test

This test is here because many packet sniffing tools perform IP address to name lookups to provide DNS names in place of IP addresses. This information is useful to attackers because most of the time hosts are named for what they provide. An example would be a mail server being named mail.abc.com. Hosts not watching traffic destined to them will not attempt to resolve the IP addresses in the packets. To test this, AntiSniff places the network card into promiscuous mode and sends packets out onto the network aimed to bogus hosts. If any name lookups from the bogus hosts are seen, a sniffer might be in action on the host performing the lookups.

4.2 Operating system specific tests

This class of tests is aimed at certain operating systems. There is the ARP test that is designed for Microsoft Windows 95, 98, and NT. The second test is known as the Ether Ping test which is designed for Linux and NetBSD kernels. Each test will be described below.

4.2.1 ARP test

This test is to exploit the flaw found in they way Microsoft operating systems analyze broadcast ARP packets. This is found in Microsoft Windows 95, 98, and NT. When in promiscuous mode the driver for the network card checks for the MAC address being that of the network card for unicast packets, but only checks the first octet of the MAC address against the value 0xff to determine if the packet is broadcast or not. Note that the address for a broadcast packet is ff:ff:ff:ff:ff:ff. To test for this flaw, AntiSniff sends a packet with a MAC address of ff:00:00:00:00:00 and the correct destination IP address of the host. After receiving a packet, the Microsoft OS using the flawed driver will respond while in promiscuous mode. It should be noted that this flaw is based on the default Microsoft driver shipped with the OS.

4.2.2 Ether Ping test

In older Linux kernels there is a specific condition that allows users to determine whether a host is in promiscuous mode or not. When a network card is placed in promiscuous mode every packet is passed on to the OS. Some Linux kernels looked only at the IP address in the packets to determine whether they should be processed or not. To test for this flaw, AntiSniff sends a packet with a bogus MAC address and a valid IP address. Vulnerable Linux kernels with their network cards in promiscuous mode only look at the valid IP address. To get a response, an ICMP echo request message is sent within the bogus packet leading to vulnerable hosts in promiscuous mode to respond.

4.3 Network and machine latency tests

These last sets of tests are here because hosts in promiscuous mode don't have low level hardware filtering. This dramatically increases network traffic not meant for the host leading to the OS kernel to do the filtering. The increased filtering done by the kernel causes more latency. The following tests will be explained: ICMP Time Delta test, Echo test, and the Ping Drop test.

4.3.1 ICMP Time Delta test

This test uses baseline results to determine network and machine latency. AntiSniff probes the host by sending ICMP echo request messages with microsecond timers to determine the average response time. After the baseline has been created, it floods the local network with non-legitimate traffic. During the flood of traffic, it sends another round of ICMP echo request probes to determine the average response time. Hosts in promiscuous mode have a much higher latency time.

4.3.2 Echo test

This test is actually an option for the ICMP Time Delta test. The user has the option to use the ECHO service for time deltas, if it's available on the remote host.

4.3.3 Ping Drop test

This test is also run during the flood of traffic. It involves sending a large amount of ICMP echo request messages to the host. It keeps track of the number of dropped ping responses. When a host

is in promiscuous mode it will have a much higher level of network traffic to process leading to network latency which causes the host to drop packets because it can't keep up.

5.0 Conclusion

When computers communicate over networks, they normally just listen to the traffic specifically for them. However, network cards have the ability to enter promiscuous mode, which allows them to listen to all network traffic regardless of if it's directed to them. Packet sniffers can capture things like clear-text passwords and usernames or other sensitive material. Because of this packet sniffers are a serious matter for network security. Fortunately, not all sniffers are fully passive. Since they aren't tools like AntiSniff can detect them. Since sniffing is possible on non-switched and switched networks, it's a good practice to encrypt your data communications.

6.0 References

Dhar, Sumit. "SwitchSniff." March 5, 2002. URL: http://www.linuxjournal.com/article.php?sid=5869 (May 11, 2003).

Ettercap. "ettercap." URL: http://ettercap.sourceforge.net/ (May 11, 2003).

Graham, Robert. "Sniffing (network wiretap, sniffer) FAQ." September 14, 2000. URL: http://www.robertgraham.com/pubs/sniffing-faq.html (May 11, 2003).

L0pht Heavy Industries. "AntiSniff – Technical Details." July 19, 1999. URL: https://www.nsacom.net:1952/txt/Website_Mirrors/Hack/www.l0pht.com/antisniff/tech-paper.html (May 11, 2003).

L0pht Heavy Industries. "AntiSniff – User Guide." July 19, 1999. URL: https://www.nsacom.net:1952/txt/Website_Mirrors/Hack/www.l0pht.com/antisniff/user-guide.html (May 11, 2003).

Zouridaki, Charikleia. "Packet Sniffing: The invisible threat and how to be protected." October 11, 2001. URL: http://mason.gmu.edu/~czourida/publications/sniffers.pdf. (May 11, 2003).