GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Sniffers, What are they and How to Protect From Them
Jason Drury

Introduction

Sniffers are almost as old as the Internet itself. They are one of the first tools that allowed system administrators to analyze their network and pinpoint where a problem is occurring. Unfortunately, crackers also run sniffers to spy on your network and steal various kinds of data. This paper discusses what a sniffer is, some of the more popular sniffers, and ways to protect your network against them. It also talks about a popular tool called Antisniff, which allows you to automatically detect sniffers running on your network.

What is a Sniffer?

In a non-switched network, Ethernet frames broadcast to all machines on the network, but only the computer that the packets are destined for will respond. All of the other machines on that network still see the packet, but if they are not the intended receiver, they will disregard it. When a computer is running sniffer software and it's network interface is in promiscuous mode (where it listens for ALL traffic), then the computer has the ability to view all of the packets crossing the network.

If you are an Internet history buff and have been wondering where the term sniffer came from. Sniffer was a product that was originally sold by Network General. It became the market leader and people starting referring to all network analyzers as "sniffers." I guess these are the same people who gave the name Q-Tip to cotton swabs.

Who uses Sniffers?

LAN/WAN administrators use sniffers to analyze network traffic and help determine where a problem is on the network. A security administrator could use multiple sniffers, strategically placed throughout their network, as an intrusion detection system. Sniffers are great for system administrators, but they are also one of the most common tools a hacker uses. Crackers install sniffers to obtain usernames, passwords, credit card numbers, personal information, and other information that could be damaging to you and your company if it turned up in the wrong hands. When they obtain this information, crackers will use the passwords to attack other Internet sites and they can even turn a profit from selling credit card numbers.

Popular Sniffers

At SecurityFocus.com, there are 8 pages worth of sniffer tools. There is everything from Websniff, which specifically sniffs webserver login/auth information to Altivore that claims to be an alternative implementation of the FBI's infamous Carnivore. With so many kinds of sniffers, it is a wonder how system administrators sleep at night. Network Associates' Sniffer Pro is probably the most popular commercial sniffer for Windows.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Interestingly, Network Computing rated Sniffer Pro at number seven on its "10 Most Important Products of the Decade" list. I am not going to tell you who number one is, you will have to look for yourself:
http://www.networkcomputing.com/1119/1119f1products_intro.html.
Unlike some of the freeware sniffers, Sniffer Pro can break out each of the seven layers of the OSI Reference Model and provide you a detail analysis of what is happening with each. It also provides some nice graphs to impress your boss. Sniffer is one of the best product's to help you visualize what is going on with your network, but the cost might have you running and you might want to try out some of the good freeware/shareware tools that are available.

As far as Unix sniffers go, I would have to say that snoop would be my favorite choice. Snoop comes standard with Solaris and even though snoop is not as pretty as Sniffer Pro, it is a very powerful and highly customizable sniffer, plus it is free (with Solaris). Who can beat that? You can capture packets in real time for a quick snapshot or you can save your capture to a file for more in-depth analysis. If you would like to learn how to use snoop, then check out the guy who blows up stuff (Lance Spitzer) "The Secret of Snoop" http://www.enteract.com/~lspitz/snoop.html. He does a fine job of introducing the reader to snoop and gives you everything to have you snooping in no time. If you want to become a snoop guru, then you can read those exciting man pages.

Defeating Sniffers

One of the most obvious ways of protecting your network against sniffers is not to let them get broken into in the first place. If a cracker cannot gain access to your system, then there is no way for them to install a sniffer onto it. In a perfect world, we would be able to stop here. But since there are an unprecedented number of security holes found each month and most companies don't have enough staff to fix these holes, then crackers are going to exploit vulnerabilities and install sniffers. Since crackers favor a central location where the majority of network traffic passes (i.e. Firewalls, proxies), then these are going to be their prime targets and should be watched closely. Some other possible "victims" where crackers like to install sniffers are next to servers where personal information can be seen (i.e. Webservers, SMTP servers).

A good way to protect your network against sniffers is to segment it as much as possible using Ethernet switches instead of regular hubs. Switches have the ability to segment your network traffic and prevent every system on the network from being able to "see" all packets. The drawback to this solution is cost. Switches are two to three times more expensive then hubs, but the trade-off is definitely worth it.

Another option, which you can combine with a switched environment, is to use encryption. The sniffer still sees the traffic, but it is displayed as garbled data. Some drawbacks of using encryption are the speed and the chance of you using a weak encryption standard that can be easily broken. Almost all encryption will introduce delay into your network. Typically, the stronger the encryption, the slower the machines using it will communicate. System administrators and users have to compromise somewhere in

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the middle. Even though most system administrators would like to use the best encryption on the market, it is just not practical in a world where security is seen as a profit taker, not a profit maker. Hopefully the new encryption standard that should be out shortly, AES (Advanced Encryption Standard), will provide strong enough encryption and transparency to the user to make everybody happy. Some form of encryption is better then no encryption at all. If a cracker is running a sniffer on your network and notices that all of the data that he (or she) is collecting is garbled, then most likely they will move on to another site that does not use encryption. But a paid or determined hacker is going to be able to break a weak encryption standard, so it is better to play it smart and provide the strongest encryption as long as it will not have everybody giving you dirty looks when you walk down the halls at work.

Antisniff

In 1999, our buddies at L0pht Heavy Industries released a product called Antisniff. This product attempts to scan your network and determine if a computer is running in promiscuous mode. This is a helpful tool because if a sniffer is detected on your network, then 9 times out of 10, the system has been compromised. This happened to the Computer Science Department at California State University – Stanislaus. Here is what they posted on their local website: "A sniffer program has been found running on the Computer Science network. Sniffer programs are used to capture passwords. In order to protect yourself please change your password. Do not use a word out of a dictionary, put a number on the end of a word or use proper names. Be inventive, use special characters and have 8 characters in your password." I am sure there are hundreds of similar postings on internal websites throughout the world that don't make it public as they have.

Antisniff also helps you find those system administrators who run a sniffer to find out what is wrong with their local network, but forget to ask for authorization beforehand. If you need to run a sniffer, then you should get permission in writing. If your Security Administrator is running Antisniff, then there is a good chance they will find it and you will have to explain why you are running a sniffer without authorization. Hopefully your security policy has a section on sniffers and will provide some guidance if you need to run a sniffer.

At the time of this writing, Antisniff version 1.021 is the current release. There is a nice GUI available for Windows 95/98/and NT machines. A command line version is also available for Solaris, OpenBSD, and Linux. This version of Antisniff only works in a "flat non-switched" environment. If your network is designed with routers and switches, then Antisniff does not have the same functionality as in a non-switched environment. You can only use it on local networks that do not cross a router or switch. According to Lopht's website, the next major release of Antisniff will have the ability to figure out if a computer is running in promiscuous mode over routers and switches. The next release of Antisniff should definitely be more beneficial to system administrators because the price of switches are coming down and most companies are upgrading to switches to obtain 100/Full Mbps speeds. Even though you have a totally switched environment, you are

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

still not out of the water. There are still firewalls, proxies, webservers, ftp servers, etc. where crackers still have the ability to install a sniffer and capture data locally. The only difference is, you have taken away their ability to capture data over the network.

Antisniff can also be used by blackhats to find intrusion detection systems. If they know where your intrusion detection systems are, then they can become stealth attackers, causing you much pain because you just spend $150,000 on a new intrusion detection system and they found a way to bypass it.

Summary

In this paper, I described exactly what a sniffer is, some of the more popular sniffers out there, how to protect your network from sniffers, and using Antisniff to help you find out if a sniffer is running on your network. Sniffers might not be the threat they were five to ten years ago when networks where non-switched, but they still represent a serious enough problem that system administrators should be concerned. Who is to say that there will not be a new tool that comes out that will be able to sniff traffic even in switched environments. Sniffers can be a great tool for administrators, but they can also be very damaging when used by the wrong people. Hopefully, the second generation of Internet scanners/Antisniff tools will make it as easy to detect sniffers as some of the other common vulnerability.

Internet References

Sniffer Technologies. http://www.sniffer.com/ (2 November 2000)

SecurityFocus http://www.securityfocus.com/ (31 October 2000)

L0pht Heavy Industries, Inc. "AntisSniff Technical Details." http://www.l0pht.com/antisniff/tech-paper.html (31 October 2000)

Morrissey, Pete. "The 10 Most Important Products of the Decade." October 2, 2000 http://www.networkcomputing.com/1119/1119f1products_7.html (8 November 2000)

Machrone, Bill. "How Do I Hack Thee" http://www.zdnet.com/zdnn/stories/comment/0,5859,2385238,00.html (1 November 2000)

Edwards, Mark Joseph. "Antisniff Beta 2" http://www.win2000mag.com/Articles/Index.cfm?ArticleID=7258&SearchString=antisniff (1 November 2000)

Sprenger, Polly. "L0pht Releases AntiSniff" 23 July 1999 http://www.wired.com/news/technology/0,1282,20913,00.html (1 November 2000)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

California State University – Stanislaus February 5, 1995
http://yahi.csustan.edu/studnote.html (3 November 2000)

Spitzner, Lance. "The Secrets of Snoop." http://www.enteract.com/~lspitz/snoop.html (9 November 2000)

Book References

Anonymous, “Maximum Security”, SAMS, 1998

Skoudis, Edward “Current Hacker Tools and New Hacker Capabilities”, SANS December 19, 1999

© SANS Institute 2000 - 2002, Author retains full rights.