

Re: Good sniffer software

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2004-05/0745.html>

From: XC-88-1K-4 (XC16_at_127.0.0.1)

Date: 05/21/04

Date: Thu, 20 May 2004 18:33:34 -0400

Zorpetus wrote:

- > *Could somebody recommend me some good*
- > *network "sniffer" software that could be used*
- > *to intercept data on the LAN where I am sysadm.*
- >
- > *I would like to test security of our corporate*
- > *LAN (some 300 workstations, 25 servers)*
- > *which is entirely based on HP Procurve*
- > *switches (so, therefore there is no single*
- > *broadcast Ethernet domain). In short, I would*
- > *like to see if it is still possible that someone*
- > *installs some network equipment (PC+software)*
- > *and "sniff" data on the network.*
- >
- > *Any pointer to software that could be used*
- > *for testing or any other related URL is*
- > *more than welcome.*

You want Dsniff.

<http://monkey.org/~dugsong/dsniff/>

A bit of info..

====

In a nutshell, dsniff is the Swiss army knife of privacy invasion. The package ships with a handful of powerful tools, including urlsnarf, webspy, mailsnarf, and the dsniff tool. Urlsnarf grabs every URL that passes across the wire and stores it for later examination. Webspy can grab URLs off the wire and open the URL in your local browser window so you can follow along and view what a remote user is seeing on his or her Web browser. Mailsnarf is just as nasty as webspy?it can sniff SMTP-related packets off the wire and reassemble entire email messages into a common format that popular mail clients can read. The dsniff tool is one of the most powerful password grabbers I've seen. It can snag passwords off the wire from many different protocols, including FTP, Telnet, Web, POP3, IMAP, LDAP, Citrix ICA, pcAnywhere, SMB, Oracle SQL*Net, and numerous others.

Even though the tools found in the dsniff package are written for UNIX platforms, you still need to be aware that these tools exist because they could be used against your Windows-based networks. Song's package is incredibly powerful, whether used with good or bad intent. The tools point out a well-known problem with networks in general: malicious users can easily sniff clear text from packets to glean sensitive data. Although blocking ARP redirects and monitoring ARP traffic and tables can help protect against tools like arpredirect, those tactics are certainly not cure-alls. They help prevent packets from becoming misdirected, but most data still travels in clear text over your networks, which means localized intruders can glean sensitive data with packet-sniffing tools. To better protect your data, you must encrypt it at some level before sending it out on the wire, and you must use sniffer-detecting tools to help stop the snoops.

The decision about which tactics to use for data protection depends on your data and your organization, so I can't give you much more advice on the matter. Just be aware that ARP poisoning and data sniffing are real problems that you need to guard against. Until next time, have a great week.