Passive Network Auditing with dsniff

Dug Song
University of Michigan CITI

Merit Joint Technical Staff meeting
September 14, 2000

Introduction

dsniff - sniffing tools for penetration testing

- I wrote these tools with honest intentions - to audit my own network, and to demonstrate the insecurity of cleartext network protocols

- Please do not abuse this software

Motivation

Current network security assessment techniques are incomplete:

- Active - vulnerability scanning
  - search for holes
  - network scanners - ISS, CyberCop, HackerShield, nessus
- Passive - intrusion detection
  - watch for attacks
  - network IDS - NFR, Dragon, RealSecure

But how to detect (and enforce) policy violations?

Concept

A tool to be used in detection and deterrance

- virtual tar and feathers, e.g. http://www.citi.umich.edu/dsniff.html

Provide admins with a tool to procure a security budget

- nothing says "fix me" like showing the boss her own password

Requirements

Detect policy violations via passive monitoring

- cleartext passwords
- password sharing
- contraband content or traffic
- forensics - tracking misuse

Defend against active evasion

- TCP/IP reassembly
- basic application layer protocol parsing
- traffic shaping or redirection

Design

Portability

- support all major platforms (*BSD, Linux, Solaris, win32)

Ease of use

- intuitive interfaces, log compression, etc.

Flexibility

- Unix tool paradigm

Resistance to abuse

- large library dependencies, etc.

Implementation

9 tools:

- arpspoof
- macof
- tcpkil
- tcpnice
- dsniff
- filesnarf
- mailsnarf
- urlsnarf
- webspy

arpspoof

- Facilitates man-in-the-middle sniffing via ARP spoofing
- Enables sniffing on switched networks
- Can be used to poison the ARP caches of all, or arbitrary hosts on the LAN
- Plays well with others - will restore the original ARP mapping on exit

macof

- Floods the LAN with random MAC addresses
- Some network switches fail open in repeating mode
- Zen koan: Switch becomes hub, sniffing is good

tcpkill

- Selectively kills TCP connections
- Useful in initializing connection state on a LAN for stateful, TCP/IP reassembling sniffers
- OK, so maybe this is a little evil

tcpnice

- "You’re talking too fast, slow down!"
- Slows down selected TCP connections via "active" traffic shaping (shrinking TCP window advertisements and ICMP source quenches)
- In theory, could be abused to enforce local (unilateral) QoS policy, e.g. to hog bandwidth for my Napster downloads

dsniff

The mother of all password sniffers

- Handles FTP, Telnet, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, NFS, YP, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL*Net, Sybase and Microsoft SQL

- HTTP module also does QUERY_STRING and x-www-form-urlencoded parsing, to catch most CGI-based auth schemes

dsniff (cont.)

- Supports magic(5)-style automatic protocol detection. e.g. telnet on arbitrary ports, etc.
- Supports full TCP/IP reassembly, and best-effort half-duplex TCP reassembly (in case of lossy sniffing, or asymmetric routing)
- Uses Berkeley DB for storage, only saving unique auth info

filesnarf

- Sucks down files sniffed from cleartext NFS v2, v3, UDP or TCP traffic
- Practical exploit for theoretical attacks against X11, SSH, PGP. e.g. ~/.Xauthority, ~/.ssh/identity, ~/.pgp/secring.pgp
- CIFS, AFS are next
- Motivation for our NFSv4 work at http://www.citi.umich.edu/projects/nfsv4/

mailsnarf

- Output e-mail sniffed from POP, SMTP traffic in Berkeley mbox format
- Supports regular expression matching against mail header and body
- Your own private Carnivore!

urlsnarf

- Output URLs sniffed from HTTP traffic in Common Log Format (e.g. Apache access_log)
- Crunch through your favorite log analyzer, determine web surfing trends

webspy

- Watch someone's web surfing in real-time, in your own browser
- Fun party trick!

Conclusions

- dsniff can be a good deterrent to bad user behaviour
- It can also be a bad incentive for good network security
- Either way, you win!

Future work

Addition of active man-in-the-middle attack tools:

- dnsspoof
- tcpspoof

Other tools for forensics:

- msgsnarf
- implement Vern Paxson's backdoor, stepping stone detection algorithms

Availability

dsniff is freely available under a BSD-style license

- http://www.monkey.org/~dugsong/dsniff/