

Defending Your Network



Adam Getchell

College of Agricultural &
Environmental Sciences Deans'
Office

ACGetchell@ucdavis.edu

IT Security Symposium

June 22-24, 2005

Goals of this class (ambitious)

- Discuss network detection, honeypots, IDS, and tarpits
- Inspect network traffic patterns using Etherape
- Build and configure a working honeypot using HOACD
- Build and configure a working IDS using OpenIDS
- Build and configure a working SMTP gateway using MailDroid

All of these tools are based on



What is OpenBSD?

- The OpenBSD project was started by Theo de Raadt
 - <http://www.openbsd.org>
- The most secure general-purpose operating system
 - 1 remote hole found in 8 years
- Source code audited to proactively fix security bugs since 1996
 - Bugs fixed for correctness, e.g., replace strcpy(), strcat(), and sprintf() with strncpy(), strlcat(), and snprintf()
- Clean system design doesn't require a Unix guru to run a locked-down system
 - All configuration files stored in /etc
 - All devices in /dev
 - All logs stored in /var/log
 - Newsyslog automatically rotates logfiles
 - All unnecessary services turned off by default
- Clean ports/packages system for installing software
 - Important for this class!

What is OpenBSD? Part 2

Security integrated throughout the operating system:

- Buffer overflow protection with ProPolice compiler (non-exec stack via canaries, avoid pointer corruption via reordering)
- W^X memory page protection on some architectures (non-exec heap)
- Most services run in privilege separated (PrivSep) mode (including X Window server and xconsole, Apache, sendmail)
- Systrace - system call policy filter (executable sandbox)
- Daily insecurity report mailed to root
 - Usesmtree, directory hierarchy mapping program that checks permissions and checksums
- Privilege separation for a large number of services
 - httpd
 - ftpd
 - tcpdump
 - afsd
 - mopd
 - pppoe
 - rbootd
 - dhcrelay
 - dhclient
 - dhcpd
 - tftpd
 - pflogd
 - bgpd
 - syslogd
 - X-Windows

What is OpenBSD ? Part 3

- Integrated cryptography throughout
 - Kerberos (IV, V)
 - Integrates OpenSSH, a free replacement for insecure utilities ftp, telnet, r*
 - IPSEC
 - Blowfish
 - Hardware crypto-acceleration cards
 - One-time passwords
- New releases occur approximately every 6 months, in June and December
- Man pages are useful, up to date, and worth reading
- Easily upgraded from source via CVS, CVSup, or patching (e.g. tepatche, <http://www.gwolf.cx/soft/tepatche/>)
 - -current branch incorporates latest and greatest
 - -stable branch includes all known bug fixes and vulnerability patches
- Offers binary emulation of other operating systems (Linux, HP-UX, FreeBSD, Solaris, BSD/OS)
- Can run on flash memory and USB devices (e.g., OpenSoekris, OpenBrick)

OpenBSD Resources



OpenBSD website:

- <http://www.openbsd.org>

OpenBSD man pages:

- <http://www.openbsd.org/cgi-bin/man.cgi>

Insecure at UC Davis

- <http://insecure.ucdavis.edu>

Absolute OpenBSD, by Michael Lucas, ISBN 1-886411-99-9

Secure Architectures with OpenBSD, by Brandon Palmer and Jose Nazario, ISBN 03-21193-66-0



nmap

```
# pkg_add -v  
ftp://ftp5.usa.openbsd.org/pub/OpenBSD/  
3.7/packages/i386/nmap-3.81.tgz
```

```
# sudo nmap -v <target>
```

Many, many options - still one of the best
portscanners around

For more details, see Professor Bishop's
"Advanced UNIX Security" presentation

Fun with nmap



What do these do?

```
# nmap -sT aaa.bbb.ccc.0/24
```

```
# nmap -vv -O -sS -PO www.xxx.yyy.zzz
```

```
# nmap -vv -O -sF -PO -Daaa.bbb.ccc.ddd www.xxx.yyy.zzz
```

Network Detection with EtherApe

The screenshot displays the EtherApe application interface. The main window shows a network graph with nodes and connections. A protocol list on the left includes SOCKS, TCP, WWW, WHO, OSFP, NETBIOS-NS, SNMP, UDP_UNKOWN, X11-2, BOOTPC, BOOTFS, SMB, RPC, YPSERV, FAX, HYLAFAX, NETBIOS-SSN, FINGER, TCP_UNKOWN, and PORTMAP. A status window for 'JPAYAN' is open, showing statistics for its connection.

Name:	JPAYAN
Numeric Name:	JPAYAN <00> (Workstation/Redirector)
Instantaneous:	Accumulated
0 bps	249 bytes
Inst. Inbound:	Accu. Inbound
0 bps	0 bytes
Inst. Outbound:	Accu. Outbound
0 bps	249 bytes

EtherApe hints

- Run etherape -n as root (or use sudo)
- Use IP mode and select the correct interface
- Double-click on nodes for detailed information
- Edit preferences to change persistence, color, filtering, etc.
- Use /etc/ethers to define MAC address-name relationships (especially for routers)
- To resolve MAC addresses into IP addresses (and hence names via DNS), do:
 - # ping <somehost>
 - # arp -a
- <http://etherape.sourceforge.net/>

What is a honeypot?

- Lance Spitzner, "Open Source Honeypots: Learning with Honeyd"
 - <http://www.securityfocus.com/infocus/1659>
- "A honeypot is a security resource whose value lies in being probed, attacked, or compromised. The key point with this definition is honeypots are not limited to solving only one problem, they have a number of different applications. To better understand the value of honeypots, we can break them down into two different categories: production and research. Production honeypots are used to protect your network, they directly help secure your organization. Research honeypots are different; they are used to collect information. That information can then be used for a variety of purposes, such as early warning and prediction, intelligence gathering, or law enforcement."

HOACD=Honeyd + OpenBSD + Arpd on CD

- Bootable CD which uses CD as OS and hard drive as log and config file source
- Install mode sets up disk, normal mode initializes Honeyd
- Uses Arpd to conduct ARP spoofing in order to direct traffic for IP addresses to Honeyd
- Honeyd is quite powerful - we'll barely scratch the surface of its capabilities

Honeyd



Written by Niels Provos (a NetBSD/OpenBSD developer), Honeyd is incredibly powerful:

<http://www.honeyd.org/index.php>

1. Can simulate large network topologies with one host (tested to 65536)
2. Can simulate an entire LAN, including latency, loss, and bandwidth
3. Can simulate multiple entry routers with asymmetric routing
4. Can simulate GRE tunneling for distributed networks
5. Can assume personality of multiple operating systems using nmap or xprobe fingerprints or pOf rules
6. Subsystem Virtualization -- simulate multiple services (web, ftp, CISCO router login) using scripts
7. Tarpit keyword causes Honeyd to slow TCP connections and act like a Tarpit (c.f. LaBrea)
8. Dynamic Templates - can change networking behavior based on source address, operating system, or time

Honeyd Live Statistics



<http://www.honeyd.org/live.php>

HOACD Hints

- Select n when it asks if you want to erase the disk (or your install will take a long time!)
- /dev/wd0a, 10M should be /
- /dev/wd0b, 2xRAM should be swap
- /dev/wd0d, 10M should be /etc
- Make /dev/wd0e, 100M for /dev
- Make /dev/wd0f, 64M for /tmp
- Make /dev/wd0g, rest for /var
- Arpd will snag all IP addresses you give it using ARP spoofing, so:
 - don't overlap with (physical) lab machines!
 - don't overlap with other virtual machines!
- Use a strong root password
- Setup normal user for remote SSH (remote root disabled)
- Default setup spoofs Windows XP SP1 -- Checkout /var/honeyd/conf/honeyd.conf for details

Testing HOACD



- Reboot into normal mode
- Have someone ping or nmap you
- For nice output, try:

```
# cd /var/honeyd/honeydsum-v0.3  
# ./honeydsum.pl -c honeydsum.conf  
  ../log/honeyd.log.<use tab completion> | less
```

- honeydsum.pl generates web pages using -w

Troubleshooting



- Read <http://www.honeynet.org.br/tools/hoacd/README-1.1> carefully
- You can sometimes confuse people (like Network Operations) or yourself as to what machine is where
- If you're not careful about which addresses you capture, you could tarpit your own legitimate traffic! (port 9100, 135, 445 are common)

Extra Credit: Pretty website statistics



- We want to see the results
- Enable Apache on OpenBSD

```
# vi /etc/rc.conf.local
```

Add `httpd_flags=""` (or `"-DSSL"` after reading `man ssl(8)`)
- We want accurate time for our charts

```
Add ntpd_flags=""
```

You should now see `httpd` as a network daemon

Whip up cronjob to copy results into `/var/www`

Extra Credit: More neat things to do



- If you're ambitious, you can attempt to simulate a network using:
 - http://www.paladion.net/papers/simulating_networks_with_honeyd.pdf
 - <http://www.honeyd.org/config/honeyd.conf.bloat>
- Check out the Honeyd challenge:
 - <http://www.citi.umich.edu/u/provos/honeyd/ch01-results/>
 - Honeycomb (Generate Snort signatures from attackers)
 - RandomNet (Random honeyd hosts generator, written in Java, with GUI)

Honeyd Resources



Honeyd website:

- <http://www.honeyd.org/index.php>

Honeynet.BR website

- <http://www.honeynet.org.br/>

HOACD

- <http://www.honeynet.org.br/tools/>

Lance Spitzner, "Open Source Honeyd: Learning with Honeyd"

- <http://www.securityfocus.com/infocus/1659>

Simulating Networks with Honeyd

- http://www.paladion.net/papers/simulating_networks_with_honeyd.pdf
- <http://www.honeyd.org/config/honeyd.conf.networks>

Intrusion Detection Systems

IP Criteria *any*
 TCP Criteria *any*
 Payload Criteria *any*

Added 245 alert(s) to the Alert cache

Alert #17
 << Previous #15-(1-438) >> Next #17-(1-440)

Meta	ID #	Time	Triggered Signature														
		1 - 147	2003-08-22 04:05:29	[cve][icat][snort] WEB-IIS +.htr code fragment attempt													
Sensor	name	interface	filter														
	192.168.2.31	le1	none														
Alert Group	none																
IP	source addr	dest addr	Ver	Hdr Len	TOS	length	ID	flags	offset	TTL	chksum						
	192.168.2.30	192.168.2.1	4	5	0	91	33651	0	0	128	61881						
	FQDN	Source Name	Dest. Name														
		Unable to resolve address	Unable to resolve address														
Options	none																
TCP	source port	dest port	R	R	U	A	P	R	S	F	seq #	ack	offset	res	window	urp	chksum
	2009	80			X	X					348663030	856604606	.5	0	65535	0	8724
Options	none																
length	51																

OpenIDS



- OpenBSD 3.5
 - Operating system
 - Sets up password for SSL website
 - Sets up password to exchange SSH keys for sensors
- Snort
 - Intrusion Detection system
- BASE
 - Web interface for Snort alerts
- Snortlog
 - Reporting tool for Snort alerts
- Mysql
 - Database to log alerts
- Oinkmaster
 - Download latest Snort signatures
- Pigsentry
 - Realtime analysis of Snort alerts

Snort



Snort is another powerful open-source IDS originally by Marty Roesch, who has since turned it into Sourcefire, a commercial offering

1. Real-time traffic and protocol analysis
2. Rules-based language, with updates (can also write your own)
3. Notification mechanism
4. Modular architecture (e.g. BASE)

See

http://www.snort.org/docs/snort_htmanuals/htmanual_233/node16.html

OpenIDS Demonstration



<https://169.237.124.31/index.htm>

OpenIDS hints

- Two interfaces needed: a public one for reporting, a stealth interface for sniffing
- Start off with standalone installation
- htaccess sets password protected access to web interface
- Two letter country code et. al for self-signed SSL
- Challenge password for SSH tunnels
- Y to enable RSS support
- N for firewall modules
- Q to quit extra applications
- K for root ksh, then Q to continue
- N to enable routing
- Y to reboot

Testing OpenIDS



- Login as root
- Have someone ping or nmap you
- Goto `https://<your IP address>`
 - Enter your htaccess username/password
 - Look at BASE, Symon, etc
- Ensure that snort and mysqld are running

Extra Credit: Additional Sensors



- Try doing a sensor installation of another machine hooked up to central station, see Appendix:
 - <http://www.prowling.nu/OpenIDS%20Installation%20and%20configuration%20guide%201.0.pdf>
- Try firewall log installation with Hatcher, pfw

OpenIDS Resources



OpenIDS web site

- <http://www.prowling.nu/>
- <http://www.prowling.nu/OpenIDS%20Installation%20and%20configuration%20guide%201.0.pdf>

OpenIDS mirror

- <http://openids.openbsdservers.com/>

Snort web site

- <http://www.snort.org/>
- http://www.snort.org/docs/snort_htmanuals/html_nual_233/node16.html

I hate spam!



- After one week of vacation, my ucdavis.edu account had:
 - 208 good e-mail messages
 - 3555 pieces of spam

MailDroid



- OpenBSD 3.7
- Sendmail 8.13.3 (chrooted)
 - Standard OpenBSD patched sendmail
- smtp-vilter 1.1.9 (chrooted)
 - Connect milters to filter incoming mail
- spamassassin 3.0.2
- Cyrus-sasl 2.1.20
 - SASL2 authentication daemon to use with sendmail
- Clamav 0.85.1 (chrooted)
 - Open source anti-virus milter
- Squirrelmail 1.4.4
 - SSL web mail front-end using internal IMAP server
- Spamd
 - E-mail tarpit to trap spammers, now with greylisting
- Pop3s
 - TLS based POP
- Pf
 - Integrated with firewall ruleset
- Chrooted Apache, named, PHP4.3.10

spamd

- Fake sendmail-like daemon which rejects false mail by returning error code 450 (default) or 550 for Blacklisted hosts (known bad)
- Very efficient - doesn't slow receiving machine
- Greylisted hosts get innocuous 451 Temporary Failure
- If they retry later, they get Whitelisted
- If they try to deliver another message, they get Blacklisted
- Pf can be used to redirect port 25 requests for Whitelisted hosts to real MTA:

```
table <spamd> persist
```

```
table <spamd-white> persist
```

```
rdr pass inet proto tcp from <spamd> to any \  
  port smtp -> 127.0.0.1 port 8025
```

```
rdr pass inet proto tcp from !<spamd-white> to any \  
  port smtp -> 127.0.0.1 port 8025
```

MailDroid Hints

- Make sure maildroid37.tgz is selected
- I prefer to start ntpd by default
- No to X Windows
- No to com0 console
- Select external interface as firewall interface
- Webadmin panel password doesn't do anything (yet)
- Halt, remove CD, reboot, login as root, and run ./setup

Troubleshooting MailDroid



Consider making just one large partition to ensure all subdirectories have enough room (don't do this on production!)

- <http://www.artran.co.uk/computers/sendmailBSD.html>
- http://www.aei.ca/~Pmatulis/pub/obsd_mfg-1.html
- <http://spamassassin.apache.org/>
- <http://www.elwood.net/greyspamd.html>
- <http://www.devguide.net/books/openbsd-fw-02-ed/spamd-02.pdf>

MailDroid Resources



MailDroid website

- <http://www.maildroid.org/download.html>

Spamd info

- <http://www.openbsd.org/cgi-bin/man.cgi?query=spamd&apropos=0&sektion=0&manpath=OpenBSD+Current&arch=i386&format=html>

Clam AntiVirus

- <http://www.clamav.net/>

SpamAssassin

- <http://spamassassin.apache.org/>

Smtp-vilter

- <http://freshmeat.net/projects/smtp-vilter/>

Cyrus-SASL

- <http://www.sendmail.org/~ca/email/cyrus/sysadmin.html>

SquirrelMail

- <http://www.squirrelmail.org/>

Pop3s

- <http://sharkysoft.com/tutorials/linuxtips/pop3s/>

Questions?

A horizontal line with a color gradient from dark blue on the left to yellow on the right, ending in a teardrop shape. The line is set against a black background.

Defending Your Network



Adam Getchell

College of Agricultural &
Environmental Sciences Deans'
Office

ACGetchell@ucdavis.edu

IT Security Symposium

June 22-24, 2005