Securing your UNIX system against Hackers Part 3 Session 1746

Jaqui Lynch
Circle4 Consulting
http://www.circle4.com/
jaqui@circle4.com

The purpose of this talk is not to encourage hacking but to assist the system administrator in protecting their systems against hackers.

Agenda

- Background
- Freeware/Shareware Tools that can help
  - TCP Wrappers & Secure Shell
  - Apache, openssl, modssl, stunnel
  - Portmap
  - Secure Shell
- Incident Reporting
- Helpful Sites
- Useful scripts.

CERT Statistics

Year	1997	1998	1999	2000	1Q01
Emails	39,626	41,871	34,612	56,365	18,410
Calls	1,058	1,001	2,099	1280	410
Vuln. Reports	311	262	419	1090	633
Incidents	2,134	3,734	9,859	21,756	7,047
Sites	146,484				
Alerts Published	50	34	22	26	6
Security Notes		15	11	57	46

High Profile Hacks

- Nov 1988 Internet Worm
- 1996 CIA banner replaced with Central Stupidity Agency
- 1996 DOJ Attorney General photo replaced with one of Adolf Hitler
- 1998 Thousands of NT computers in NASA brought down by BIND bug
- 1998 teenager took over Worcester ATC
- Late 1999 - 300000 credit card numbers stolen from CD universe
- Feb 2000 – Yahoo, aol, etc – major denial of service attacks
- Past couple of months – many breakins using FTP scanners to find WU-FTP with security hole
- Gazillions of DOS attacks
- Loveletter worm

Levels & Types of Attacks

- Levels
  - Root access break-in
  - Replacement of materials
  - Damage done
  - Just looking
  - Theft of proprietary information
  - Denial of service
- Types
  - Embarrassment (replace banners, home page, etc)
  - Denial of service (syn-flood connections)
  - Ping of Death
  - Stealing proprietary code
  - Pornography
  - Harassment or threats - stalking
  - Email spam or bulk subscribes
  - Hate mail

SANS Top 10 - www.wwdsi.com

1. Bind weaknesses
   - nxt, qinv and in.named allow immediate root compromise
2. Vulnerable CGI pgms
   - Web server has Programs and CGI extensions (e.g. colddfusion) installed
3. Network Services
   - Root access allowed by rpc.statd, rpc.cmsd, rpc.ttdbserverd
4. IIS – RDS security hole in IIS
5. Sendmail & mime
   - Sendmail buffer overflow weaknesses, pipe attacks and MIME, that allow root compromise.
6. Sadmind (Solaris) & mountd
   - Buffer overflows allow root access
7. File sharing
   - Global file sharing via NetBIOS and Windows NT ports 135->139 (445 in Windows2000)
   - UNIX NFS exports on port 2049
   - Macintosh Web sharing or AppleShare/IP on ports 80, 427, and 548.
8. Weak or no passwords
9. IMAP and POP buffer overflows or poor config.
10. SNMP public/private

Useful Alert Pages

- IBM Research Hype Alerts
  - Http://www.av.ibm.com & www.ers.ibm.com
- ICSA Virus Alert
  - http://www.icsa.net/services/consortia/anti-virus/alerthoax.htm
- CERT
  - http://www.cert.org/advisories/
- Rob's Virus Myths
  - http://www.kumite.com/myths
- http://www.auscert.org.au/
- http://www.l0pht.com/advisories
- http://www.microsoft.com/security/bulletins - IE
- http://home.netscape.com/security/notes - netscape

TCP Wrappers and SSH

- TcpW - ftp.porcupine.org
- SSH – www.ssh.org
- Wrappers improve security and logging
- Reverse dns lookup can be used to disallow access
- Allows tripwires
- SSH encrypts logins
- SCP allows secure file copies
- First install the wrappers – there is a new version that can now handle IPv6
- Then configure ssh with the wrappers – I usually install v1.2.31 and then v2.4.0 (v3 is now out)

TCP Wrappers Configuration

- vi Makefile
  - STYLE = -DPROCESS_OPTIONS # Enable language extensions.
  - FACILITY= LOG_DAEMON # LOG_MAIL is what most sendmail daemons use
  - SEVERITY= LOG_INFO
  - Causes tcpd to log everything to daemon.info
- make clean
- make aix
- cp tcpd /usr/local/bin
- cp tcpd.h to ssh source directories
- cp libwrap.a /usr/local/lib
- vi inetd.conf, hosts.allow, hosts,deny
- refresh –s inetd

/etc/inetd.conf

```
ftp     stream  tcp6    nowait  root    /usr/local/bin/tcpd /usr/sbin/ftpd  -u 002 -l       ftpd

telnet  stream  tcp6    nowait  root    /usr/local/bin/tcpd /usr/sbin/telnetd       telnetd –a

exec    stream  tcp6    nowait  root    /usr/local/bin/tcpd /usr/sbin/rexecd        rexecd

dtspc   stream  tcp     nowait  root    /usr/local/bin/tcpd /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd

xmquery dgram   udp     wait    root /usr/local/bin/tcpd        /usr/bin/xmservd xmservd -p3

rlogin  stream  tcp6    nowait  root  /usr/local/bin/tcpd  /bin/false
netstat  stream  tcp  nowait  nobody  /usr/local/bin/tcpd  /bin/false
```

Delete everything else out of inetd.conf – don't just comment it out.
You should also check inetd.conf regularly

/etc/hosts.deny

ALL:ALL

Or:
ALL:ALL spawn (echo –e "\n Tcp Wrappers \: Refused \n \
By\: $(uname –n) \n Process\: %d (pid %p) \n \
Host\: %c \n Date\: $(date) \n \
" | mail –s tcpw@$(uname -n). %u@%h ->%d. admin@sys.com)

Hosts.allow Options

- Telnetd : 123.123.123.4 : options
- Options are:
  - RFC931
    - Does an ident lookup to the originator
  - BANNERS path/filename
    - Displays a banner whether service is granted or not
  - SPAWN (commands)
    - Used to execute a command such as safe_finger and then mailing the response to a security person
    - Only used for denied connections

/etc/hosts.allow

Log but don't really protect

ftpd : all
sshd : all
rshd : all
krshd : all
tftpd : all
bootpd : all
rlogind: all
krlogind: all
telnetd : all
dtspcd : all

/etc/hosts.allow

Log and protect

portmap: 123.123. 255.255.255.
ftpd : .abc.com,123.123.123.4
in.ftpd : .abc.com,123.123.123.4
sshd : all
telnetd : 123.123.123.0/255.255.255.0
xmservd : .abc.com,123.123.123.4
rexecd : LOCAL,.abc.com,123.123.123.4
dtspcd : .abc.com,123.123.123.4

Replacement portmap

- Wietse Venema
- Portmap replacement with access control
- Similar to TCP Wrappers package in style
- Used to discourage access to the NIS (YP), NFS, and other services registered with the portmapper.
- Provides NIS daemons with their own access control lists.
- "securelib" shared library (eecs.nwu.edu:/pub/securelib.tar) implements access control for all kinds of (RPC) services, not just the portmapper.
- Many vendors still ship portmap implementations that allow anyone to read or modify its tables and that will happily forward any request so that it appears to come from the local system.

Snort

- www.snort.org
- Intrusion detection tool
- Can be used as a packet sniffer like tcpdump
- Can be used as a packet logger for debugging
- Basically a network sniffer with flexible language allowing you to write rules
- Requires libpcap from www.tcpdump.org

Apache, Openssl, Modssl

- Apache
  - www.apache.org
  - Web server used by a huge number of web sites
  - Combine with openssl and modssl to add security
- Modssl & openssl
  - www.modssl.org
  - www.openssl.org
  - Provide SSL v2 and v3 implementations
  - Provide TLS (transport layer security)

Stunnel

- www.stunnel.org
- Wrapper utility for encrypting TCP sessions via SSL
- Needs openssl
- Can secure daemons
  - Imap, pop, ldap …..
  - With no changes to the daemons
- Built-in TCP wrappers support (compile)
- Can use hosts.allow format

Advantages of WU-ftpd

- logging of transfers
- logging of commands
- on the fly compression and archiving
- classification of users on type and location
- per class limits
- per directory upload permissions
- restricted guest accounts
- system wide and per directory messages.
- directory alias
- cdpath
- filename filter
- virtual host support (similar to the apache httpd server)
- Commands - ftpshut, ftpwho, ftpcount ….
- Ensure you are using 2.6.1 or have patched previous versions

Sample FTP Log - anonymous

Infolog

```
May 14 15:05:56 crobin ftpd[9504]: connect from bc151x36.circle4.com
May 14 15:05:57 crobin ftpd[9504]: USER anonymous
May 14 15:05:57 crobin ftpd[9504]: PASS guest
```

Xferlog

```
Thu May 14 14:42:10 1998 1 bc151x36.circle4.com 0 /welcome.msg a _ o a guest@circle4.com ftp 0 *
Thu May 14 14:42:18 1998 1 bc151x36.circle4.com 0 /.message a _ o a guest@circle4.com ftp 0 *
Thu May 14 14:42:23 1998 1 bc151x36.circle4.com 0 /pub/.message a _ o a guest@circle4.com ftp 0 *
Thu May 14 14:42:27 1998 1 bc151x36.circle4.com 0 /pub/README a _ o a guest@circle4.com ftp 0 *
Thu May 14 15:07:13 1998 1 bc151x36.circle4.com 0 /pub/secure/aliases a _ o a jaqui@circle4.com ftp 0
*
```

FTP AIX log (-l option)

Jul 15 22:05:57 froggy2 ftpd[13082]: connect from froggy.ne.mediaone.net

Jul 15 22:05:57 froggy2 ftpd[13082]: connection from froggy.ne.mediaone.net at Sat Jul 15 22:05:57 2000

Jul 15 22:05:57 froggy2 ftpd[13082]: FTP LOGIN FROM froggy.ne.mediaone.net, freddy

Jul 15 22:05:57 froggy2 ftpd[13082]: FTPD: EXPORT file local , remote

Jul 15 22:05:59 froggy2 ftpd[13082]: FTPD: EXPORT file local , remote

Jul 15 22:06:25 froggy2 ftpd[13082]: FTPD: IMPORT file local lcs025.gif, remote

Jul 15 22:06:25 froggy2 ftpd[13082]: FTPD: EXPORT file local , remote

Jul 15 22:07:24 froggy2 ftpd[4278]: FTPD: EXPORT file local , remote

Log Facility

- Auth — authorization systems i.e. login
- Cron — used by cron and at
- Daemon — system/network daemons
- Kern — kernel messages
- Lpr — printing
- Mail — mail system
- Mark — used for timestamps
- News — news/nntp system
- User — default – used for any program
- Uucp — reserved for uucp
- Local0…7 — local use

Log Priority

- Debug — debugging – useful if paranoid
- Info — informational msgs
- Notice — things that may require attention
- Warning — warnings
- Err — errors
- Crit — critical things like hardware errors
- Alert — deal with it NOW
- Emerg — Ouch

Possible Log Actions

- /dev/console — Log to the console
- /path/file — Write messages to file
- @loghost — Log to a central host
- Jaqui,jim — Email jaqui and jim
- * — Send messages to all logged in users

- Use swatch or logsurfer or similar to postprocess the logs looking for telltale signs

Logging

- touch /usr/local/logs/syslog & mailog & infolog
- Edit /etc/syslog.conf so it looks like:
- *.emerg /usr/local/logs/syslog
- *.alert /usr/local/logs/syslog
- *.err /usr/local/logs/syslog
- *.crit /usr/local/logs/syslog
- mail.debug /usr/local/logs/mailog
- auth.notice /usr/local/logs/syslog
- daemon.info /usr/local/logs/infolog
- *.emerg /dev/console
- *.crit /dev/console
- refresh -s syslogd or killall 1 or kill -HUP
- Note use of separate logs to allow for easier postprocessing
- Ensure logs are cycled daily and monitored

Some Hacker Tools

- Everything you use plus:
- Xscan – scans subnet for open xservers and logs all the keystrokes
- Wzap – removes a users info from wtmp
- Directories with names like " .." or " …"
- Showmount –e ipaddr - find nfs exports
- Nmap – often used for DOS attacks
- Ident scanning – to find ports owned by root
- Sam Spade
  - www.blighty.com/products/spade
  - Used to crawl and suck down your whole web site

Rootkits

- Hackers install these on the system
- Modify ps, ls, pids, logs, ifconfig, netstat …
- ps –no-headers –ef | wc
  - Should show the same result as:
- ls –d /proc /[0-9]* | wc
- If no-hdeaders does not work – remove it and subtract 1 from the total

Detecting Rootkits

- file /dev/* | grep text
- Look for things like /dev/ptyw ASCII text
- find / -perm –4000 –print (suid files)
- find / -perm –2000 –print (sgid files)
- find / -name ".*"
  - Looks for hidden directories such as ".. "

How to detect sniffer

- Ifconfig –a | grep PROMISC
- www.securitysoftwaretec.com/antisniff

- Nmap – www.insecure.org/nmap
- nmap –p 1-65535 systemname
  - Scans all ports on the system
- netstat -a

Scan yourself

- Saint
  - www.wwdsi.com
- ISS
  - www.iss.com
- Nessus
- Kane security analyst
- Nessus
- Also portsentry to monitor ports
  - www.psionic.com

Useful Scripts – syslog.cron

```
#!/bin/sh -fh
# syslog.cron
# Run this script just after midnight on every day of the month.
# -----------------------------------------------------
# 57 23 * * * /usr/local/bin/syslog.cron
# -----------------------------------------------------
  {
     machine=`uname -n`
     elog="/usr/local/logs/$machine.errptlog"
     ealog="/usr/local/logs/$machine.errptalog"
     ilog="/usr/local/logs/ infolog"
     oldilogs="/usr/local/logs/$machine.infolog"
     umask 027
     day="`/bin/date +'%d'`"
     month="`/bin/date +'%m'`"
     year="`/bin/date +'%y'`"
     set -- Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
     shift $month
     lmonth="$1"
     cat "$ilog" >>"$oldilogs.$lmonth$year"
     chown logowner "$oldilogs.$lmonth$year“
     echo >"$ilog"
  # The above is not the full script but should give you an idea
```

Useful Scripts – testlog.cron

```
#!/bin/sh
PATH=/bin:/ usr/bin:/usr/etc:/usr/ucb
day="`/bin/date +'%d'`"
month="`/bin/date +'%m'`"
year="`/bin/date +'%y'`"
set -- Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
shift $month
lmonth="$1"
cd /usr/local/logs
grep connect  *  >./$lmonth$year.connect.out
grep refuse * >./$lmonth$year.refuse.out
grep sshd * >./$lmonth$year.sshd.out
grep ftpd * >./$lmonth$year.ftpd.out
grep telnetd * >./$lmonth$year.telnetd.out
grep rshd * >./$lmonth$year.rshd.out
grep rexec *>./$lmonth$year.rexecd.out
grep rlogin * >./$lmonth$year.rlogin.out
grep tftp * >./$lmonth$year.tftp.out
grep auth * >./$lmonth$year.auth.out
sort -f -k8 -k2 -k3 -k4 -o ./$lmonth$year.refuse.sorted ./$lmonth$year.refuse.out
sort  ./$lmonth$year.connect.out >./$lmonth $year.connect.sorted
mail -s"All systems refuse list" admins@acs.neu.edu <$lmonth$year.refuse.sorted
echo end of grepit script
```

Incident Reporting

- Gathering Evidence
  - Know the legal issues
- Who to contact and how
- abuse@ your site or the attack site
- FBI
- Local Computer Crime bureau
- Police
- Have an Emergency Response Team with a clear set of policies and procedures

Gathering Evidence

- Copies of all logs (signed and dated)
- Output from last and lastcomm commands
- Output from ls -al and other commands
- If email - copy of raw headers for the messages
- Username, phone number, etc
- Email address including mail node
- http://www.haltabuse.org/header.htm

CERT

- Computer Emergency Response Team
- Mission
- Contact Information
- http://www.sei.cmu.edu/technology/cert.cc.html
- http://www.cert.org
- ftp://info.cert.org/pub/
- http://www.auscert.org.au
- Mailing List
- cert-advisory-request@cert.org

Questions

jaqui@circle4.com

Patch Information

- DEC
- http://www.service.digital.com/html/patch_service.html
- ftp://ftp.service.digital.com/public

- IBM
- ftp://software.watson.ibm.com/pub

- SGI
- ftp://sgigate.sgi.com
- ftp://ftp.sgi.com

- SUN
- ftp://ftp.uu.net/systems/sun/sun-dist
- ftp://sunsolve1.sun.com/pub/patches

Helpful Sites 1/2

- http://cs-www.ncsl.nist.gov/tools/tools.htm
- www.cert.org
- ciac.llnl.gov
- www.cs.purdue.edu/coast/
- www.defcon.org
- www.first.org
- www.iss.net/lists/ntsecurity
- www.ntbugtraq.com
- www.securityfocus.com - Bugtraq
- www.samspade.org - put in ip address to find domain
- www.networksolutions.com/cgi-bin/whois/whois
- www.deja.com - deja news
- www.cyberangels.org
- www.wwdsi.com - SANS top 10 and CVE list

Helpful Sites 2/2

- www.haltabuse.org
- www.scambusters.org
- www.cauce.org
- getnetwise.org
- privacyrights.org
- www.hackingexposed.com
- www.networkice.com
- http://www.infobin.org/cfid/isplist.htm
- http://www.usdoj.gov/criminal/cybercrime/
- http://www.dmares.com/maresware/websites.htm
- http://www.gaming.state.co.us/investigativelinks.htm
- http://www.nctp.org/weblinks.html

Some Web Pages to find Laws

- http://www.infobin.org/cfid/isplist.htm
- http://www.usdoj.gov/criminal/cybercrime/
- http://www.dmares.com/maresware/websites.htm
- http://www.gaming.state.co.us/investigativelinks.htm
- http://www.nctp.org/weblinks.html
- http://www4.law.cornell.edu/uscode
- Fedlaw - http://www.legal.gsa.gov
- http://www.findlaw.com

Reading

- Shimomura's Takedown
- Stoll's The Cuckoos Egg
- Maximum Security - author Anonymous, 1998 by sams.net 2nd edn 0-672-31341-3 - also a Linux one now
- Hacker Proof - Klander – 1997 Jamsa Press 1-884133-55-x
- Bandits on the Information Highway from ORA
- Usenet (can be read & searched at www.deja.com)
  - alt.2600
  - alt.crack
  - alt.hacker
  - Alt.hacking
- Hacking Exposed – McClure et al, 2000 – 0-07-212127-0
- Stopping Spam – Schwartz & Garfinkel – 1-56592-388-x