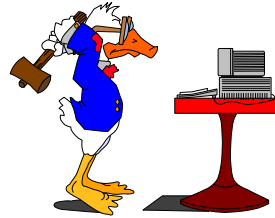


UNIX Security 101



Jaqui Lynch
Mainline Information Systems
Jaqui.lynch@mainline.com

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



1

Agenda

- Introduction
- Basics - How to secure your system
- Accounting and Logging
- Web Security
- Incident Reporting
- Helpful Sites



2

CERT Statistics

– Year	1997	1998	1999	2000	2001	2002	1H2003
– Emails	39,626	41,871	34,612	56,365	118,907	204,841	146,291
– Calls	1,058	1,001	2,099	1,280	1,417	880	380
– Vuln. Reports	311	262	419	1,090	2,437	4,129	
– Incidents	2,134	3,734	9,859	21,756	52,658	82,094	76,404
– Sites	146,484						
– Alerts Published	50	34	22	26	41	41	
– Security Notes		15	11	57	341	381	

– Please note: 2003 numbers are to June 30, 2003 so do not include Blaster, etc

Information Security Standards

- www.uscert.org.au/Information/standards.html
- ISO standard IS15408
 - <http://csrc.nist.gov/cc/ccv20/ccv2list.htm>
- E-Commerce upcoming standards
 - <http://www.ecommercestandards.com>
- Banking and Finance
 - <http://www.standards.com.au/Catalogue>

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
- W32.blaster (8/13), Nachia/Welchia (8/18), Sobig.F (8/18)
- Since 8/18 – more than 26 NEW viruses, mostly mass mailing worms

Levels & Types of Attacks

- | | |
|---|---|
| <ul style="list-style-type: none">➤ Levels<ul style="list-style-type: none">– Root access break-in– Replacement of materials– Damage done– Just looking– Theft of proprietary information– Denial of service– Worms and Trojans | <ul style="list-style-type: none">➤ Types<ul style="list-style-type: none">– 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– Buffer Overflow |
|---|---|

SANS Top 20

www.sans.org/top20/#index

1. U1 Remote Procedure Calls (RPC)
 1. Known holes in ttdbserv, cmsd, etc
2. U2 Apache Web Server
 1. Mod_ssl worm, chunk handling exploit, default cgi
3. U3 Secure Shell (SSH)
 1. Several bugs, trojan version
4. U4 Simple Network Management Protocol (SNMP)
 1. Public/private, v1 insecure
5. U5 File Transfer Protocol (FTP)
 1. Multiple exploits
6. U6 R-Services -- Trust Relationships
 1. R-services, clear text, no auth
7. U7 Line Printer Daemon (LPD)
 1. Multiple exploits
8. U8 Sendmail
 1. Buffer overflows, bad configs
9. U9 BIND/DNS
 1. DOS, buffer overflow, etc
10. U10 General Unix Authentication
 1. Accounts with No Passwords or Weak Passwords

Favorite TCP Ports

- <http://www.isi.edu/in-notes/iana/assignments/port-numbers>

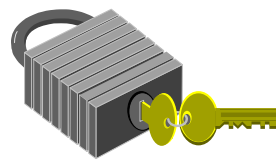
- 20 FTP (data)
- 21 FTP (control)
- 23 Telnet
- 25 SMTP (mail)
- 70 Gopher
- 79 Finger
- 80 HTTP also 8000 or 8001 or 8080
- 110 Pop3
- 119 NNTP (news)
- 143 Imap

Other TCP Ports

- 7-19 echo, discard, daytime, chargen, netstat ...
- 22 SSH
- 42 wins
- 53 dns
- 111 sun rpc
- 113 identd
- 123 ntp
- 135 loc-srv/epmap – used to attack wintel
- 137-139 netbios
- 161 snmp
- 512-517 rexec, rlogin, rsh, talk, syslog, who
- 635 mountd – Linux
- 2049 nfs
- 6670 Deepthroat
- 31337 BackOrifice

UNIX Security Basics

- Permissions
- UID
- GID
- Dangerous Accounts
- Superuser
- SUID
- Sticky bit
- Umask



File Security

- ls -l shows:
 - **-rwxr-xr-x 1 jaqui jgroup 4320 Feb 9 12:19 filename**
 - - file's type (- for file, D for directory)
 - rwxr-xr-x file's permissions
 - 1 no. of hard links the file has
 - jaqui name of the files owner
 - 4320 size of file in bytes
 - Feb 9 12:19 file's modification time
 - filename the file's name
- ls -l shows modification time for file
- ls -lu shows last accessed time
- The above two times can be changed with a command so you should check:
 - ls -lc inode last change time

Permissions

- r read
 - w write
 - x execute
 - s SUID or SGID
 - t sticky bit
-
- aaa bbb ccc i.e. **-rwxr-xr-x**
 - aaa file's owner permissions
 - bbb users who are in the file's group
 - ccc everyone else on the system (except uid 0)
 - Permissions apply to devices, named sockets, files, directories and FIFOs.



Octal Permissions

- 4000 SUID on execution
- 2000 SGID on execution
- 1000 Sticky Bit
- 0400 Read by owner
- 0200 Write by owner
- 0100 Execute by owner
- 0040 Read by group
- 0020 Write by group
- 0010 Execute by group
- 0004 Read by other
- 0002 Write by other
- 0001 Execute by other

- 755 Anyone can copy or run the program - Only the owner can change it

Umask

- Specifies the permissions you do not want given
 - by default to newly created files and directories.
 - By default:
 - New files are 666 (anyone can read/write)
 - New programs are 777 (all rwx)
 - root should be 022 and all others 077
 - **Common Umask Values**
 -
- | Umask | User | Group | Other |
|-------|------|-------|-------|
| 0000 | rwx | rwx | rwx |
| 0002 | rwx | rwx | r-X |
| 0007 | rwx | rwx | --- |
| 0022 | rwx | r-X | r-X |
| 0037 | rwx | r-X | --- |
| 0077 | rwx | --- | --- |

SUID, SGID, Sticky Bit

- SUID Sets UID to program's owner at execution
 - SGID Sets GID to program's group at execution
 - Sticky Causes program to be left in swap space after termination. Used for programs that are executed frequently - outmoded.
-
- The su command is an SUID program.
-
- To find them:
 - find / -perm -004000 -o -perm -002000 \) -type f -print
 - or ncheck -s filesystem-name

How to secure your system

- Valid accounts only
- No group, guest or dormant accounts
- All accounts should have strong passwords
- umask set to 077 except root (022)
- Set accounts such as lp or ftp that are ftp only with a shell of /dev/null or /bin/false
- Shadow Passwords
- Documentation

How to secure your system

- Recovery Lists
- Backups
- Accounting and Logging
- Limit root access - prefer su or sudo only
- Never telnet - use ssh
- No SUID, SGID or sticky bit programs
- Banner for all logins and ftp access
- NFS Exports

How to secure your system

- Clean out inetd.conf
- Use logdaemon versions of r commands or TCP wrap them
- tftpdaccess.ctl file with nothing in it
- ftpusers file
- sendmail should be at least 8.8.7 - don't run it if not needed - 8.10 is due out shortly
- Scan for .netrc, .rhosts - remove root

How to secure your system

- Check .forward files for program executions
- Add aliases to aliases file
- Ensure . is not first in root path
- Add logging to syslog.conf
- Apply all fixes for CERT advisories
- TCP Wrappers
- SSH instead of telnet
- SCP instead of ftp

How to secure your system

- Do not run finger
- NIS - run NIS+ if you must run this - see CERT & Auscert guidelines
- Use WU-FTPD for anonymous ftp if you must have it - see CERT guidelines
- Never run any services (such as ftp or web) as root

MOTD - banners

Access to the XXXXX company technological and information resources is a privilege available only to authorized individuals. This privilege requires that all users be responsible for the protection of company resources and that all use be only of a legal, ethical, moral and courteous nature.

Be advised that any attempt or any unauthorized access is a violation of both US and Massachusetts Computer Crime laws and will be addressed accordingly.

Note that in the above there is no Welcome to in this system statement

Log Facility

- Messages are sent to logs using something like mail.info or daemon.debug

- 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
- None Send nothing

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 & maillog & infolog
- Edit /etc/syslog.conf so it looks like:

➤ *.emerg, mail.none	/usr/local/logs/syslog
➤ *.alert	/usr/local/logs/syslog
➤ *.err	/usr/local/logs/syslog
➤ *.crit	/usr/local/logs/syslog
➤ mail.debug	/usr/local/logs/maillog
➤ 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

TCP Wrappers and SSH

- 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
- Do not install ssh v1

/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

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.

Advantages of WU or VS or Pro Ftp

- 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

/etc/ftpusers or ftpaccess file

bin
uucp
ingres
daemon
news
nobody
sys
adm
lpd
root
Toor
operator

List of accounts who cannot ftp
to this system

Accounting

- Last
- Lastcomm
- Start in /etc/rc
- Run daily, monthly, etc
- Ensure you clean up the pacct files as they can fill up /var

Web Security

- Create httpdsvr account (or www or similar)
- Create httpd group (or www or similar)
- httpd.conf - change user to httpdsvr & group to httpd
- Bring down the current server
- Change all directories and file from the base:
 - `chown -R httpdsvr /*`
 - `chgrp -R httpd /*`
 - `chmod -R 770 /*` makes it rwx rwx ---
- Add httpd group to accounts that need access
- Don't allow FollowSymLinks or Indexes
 - Websphere and Hostpublisher need FollowSymLinks on their directories
- UserDir DISABLED
- Fancyindexing & indexing disabled
- Protect your cgi-bin - owned by httpdsvr & rwx --- ---
- Only allow cgi-bin scripts to run from central and use cgiwrap

Web Security

- Get rid of all default cgi-bin scripts
 - Phf
 - Count.cgi
 - Test-cgi
 - Handler and so on
- Get phfscan.c & cgiscan.c and run them yourself
- Get other tools (teleport, grinder, sitedscan...)
- Known problems
 - Web site theft/copying
 - Input validation
 - Buffer Overflows
 - ASP Dot Bug (reveals ASP source code)

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

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

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.samspade.org
 - 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 sniffers

- `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`

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

Have a clear policy to protect yourself and the company

- 1998 US vs Simons
 - Rules that an employee has no reasonable expectation of privacy for internet activity at work as long as there is a clear published policy to that effect

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>

Questions



Checklist 1/3



- Individual accounts only
- All accounts must have GOOD passwords
- Disable tftp if possible
- Remove .rhost and core files nightly
- Ensure /etc/passwd can't be read anonymously by UUCP or TFTP
- Check the SU log regularly
- Only allow root to login at the console (force su or sudo)
- Set console as only trusted location for root
- Set umask to 033 or 077 (077 = rwx --- ---)
- Scan regularly for SUID/SGID files & for crack
- Change default password on all system default accounts
- Get rid of guest
- Disable dormant or temporarily inactive accounts
- Make regular backups & check restores regularly
- Export filesystems that have programs as read-only
- Check last login when you login

Checklist 2/3

- System directories - not world or group writable
- /etc/hosts.equiv should be rwx r-- r--
- Remove the + from your /etc/hosts.equiv file
- Disable finger and who and w
- Make sure fingerd is newer than 11/5/1988
- Ensure sendmail is not v5.64 or less (should be at least 8.8.7)
- Make sure ftpd is newer than 12/1988
- Ensure anonymous FTP & tftp can't get the /etc/passwd file
- Make sure /etc/ftpusers contains root, uucp, bin, etc
- Scan periodically for hidden directories (".. ")
- Check /etc/passwd for users with uid 0 regularly
- Ensure /etc/passwd is rwx r-- r--
- Check /usr/lib/preserve is not SUID
- Make sure only root can run last and lastcomm

Checklist 3/3

- User account directories should be rwx --- ---
- Set permissions on smit, sam, etc ro rwx --- ---
- Set up system logging
- Set up accounting
- Disable ntalk, rlogin in inetd.conf
- Document your install and all changes
- Create a recovery list and a list of valid uids/gids
- For tftp - create a /etc/tftpaccess.ctl file
- Ensure only root has write access to binaries
- Ensure shadow password file is not readable
- Ensure accounting files are not writable
- No binaries on NFS filesystems
- Set nodev, nosuid & noexec on NFS exported f/s
- Never export a filesystem to the world

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.sampade.org - put in ip address to find domain
- www.networksolutions.com/cgi-bin/whois/whois
- www.deja.com - deja news
- www.wiredpatrol.org
- www.sans.org/top20/#index - SANS top 20

Helpful Sites 2/2

- www.haltabuse.org
- www.scambusters.org
- www.cauce.org
- getnetwise.org
- privacyrights.org
- www.hackingexposed.com
- www.networkkice.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.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 – 1996 - 0786862106
- Stoll's The Cuckoos Egg - 0743411463
- Maximum Security - author Anonymous, 2002 by sams.net 4th edn 0672324598 - also a Linux one and one for wireless
- Hacker Proof - Klander – 1997 Jamsa Press 188413355X
- Usenet (can be read & searched at www.deja.com)
 - alt.2600, alt.crack, alt.hacker, Alt.hacking
- Hacking Exposed – McClure et al, Feb 2003 – 0072227427
 - Linux, web and java editions as well
- A Complete H@ckers Guidebook – Dr-K – 1-85868-406-4
- Removing the Spam: Email Processing and Filtering – Geoff Mulligan 1999 – 0201379570
- Anti-Hacker Toolkit – Jones et al, 2002 – 0072222824
- Well over 200 books
 - www.amazon.com
 - www.barnesandnoble.com
 - www.bookpool.com