

# AIX Security

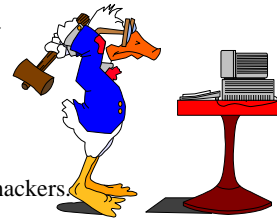
Jaqui Lynch

Mainline Information Systems  
Email – jaqui.lynch@mainline.com

Useblue 3/14/05

<http://www.circle4.com/papers/ubsec05.pdf>

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



1

## Agenda

- Basics
  - Security Types
  - Permissions
- Freeware/Shareware Tools that can help
  - TCP Wrappers & Secure Shell
  - Apache, openssl, modssl, stunnel
  - Portmap
  - Snort
  - Ftp
- Logging, finding Rootkits
- Scanners and Tools
- Questions



2

## Security Types

- Physical
- Local
  - Keep system patched!!!
- Files and filesystems
- Passwords
- Kernel
- Network

## Levels & Types of Attacks

- |   |   |
|---|---|
| <ul style="list-style-type: none"><li>➤ Levels<ul style="list-style-type: none"><li>– Root access break-in</li><li>– Replacement of materials</li><li>– Damage done</li><li>– Just looking</li><li>– Theft of proprietary information</li><li>– Denial of service</li><li>– Worms and Trojans</li></ul></li></ul> | <ul style="list-style-type: none"><li>➤ Types<ul style="list-style-type: none"><li>– Embarrassment (replace banners, home page, etc)</li><li>– Denial of service (syn-flood connections)</li><li>– Ping of Death</li><li>– Stealing proprietary code</li><li>– Pornography</li><li>– Harassment or threats - stalking</li><li>– Email Spam or bulk subscribes</li><li>– Hate mail</li><li>– Buffer Overflow</li></ul></li></ul> |
|---|---|

# SANS Top 20

[www.sans.org/top20/#threats](http://www.sans.org/top20/#threats)

1. U1 BIND/DNS
  1. DOS, buffer overflow, etc
2. U2 Apache Web Server
  1. Mod\_ssl worm, chunk handling exploit, default cgi
3. U3 General Unix Authentication
  1. Accounts with No Passwords or Weak Passwords
4. U4 Version Control Systems
  1. Anonymous access via port 2401 t0 repository
5. U5 Mail Services
  1. Buffer overflows and misconfiguration
6. U6 Simple Network Management Protocol (SNMP)
  1. Public/Private, v1 very insecure
7. U7 Open Secure Sockets Layer
  1. Multiple exploits
8. U8 Misconfiguration of NIS/NFS
  1. Multiple exploits
9. U9 Databases
  1. Multiple vulnerabilities in Oracle and MYSQL
  2. SQL Injection Vulnerabilities in Oracle E-Business Suite
10. 10 Kernel
  1. Icmp attacks can cause kernel to loop

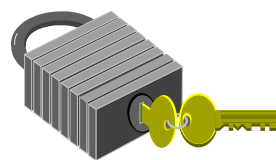
**Top 10 UNIX Vulnerabilities as at Feb 22, 2005**



5

# UNIX Security Basics

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



6

# File Security

- ls -l shows:
- -rwxr-xr-x 1 jaqui jgroup 4320 Feb 9 12:19 files
- - 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
- files 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
- 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 on most systems:
    - 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  
Also used to share files in a directory  
All files and subdirectories will inherit the group
- Sticky                    Causes program to be left in swap space after termination. Used for programs that are executed frequently - outmoded.  
If set on a dir then only root or owner can delete or rename (see /tmp drwxrwxrwt)
  
- The su command is an SUID program.
  
- To find them:
  - find / -perm -004000 -o -perm -002000 \) -type f -print
  - or ncheck -s filesystem-name

## Files to Clean Out

- /etc/services
- Password and group files
- /etc/inetd.conf
- /etc/inittab
- /etc/rc.local and other rc files

## 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 and hosts.lpd should be rwx r-- r--
- Remove the + nd all comments from your /etc/hosts.equiv and lpd files
- Disable finger and who and w
- Make sure fingerd is recent and disabled
- Ensure sendmail or Postfix is at latest version
- Make sure ftpd is current and disabled
- 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--
- Make sure only root can run last and lastcomm
- Turn on password aging

## Checklist 3/3

- User account directories should be rwx --- ---
- Set up system logging
- Set up accounting
- Disable ntalk, rlogin in /etc/xinetd.d and /etc/services
- 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
- NFS export files to fully qualified names or ips

## Tools

- SUDO
- TCP Wrappers 7.6-ipv6-4
- SSH 3.2.9.1
- Portmap 4
- Snort 2.3.0
- Apache, Openssl, Modssl
- Stunnel
- Logging

## TCP Wrappers and SSH

- TcpW - [ftp.porcupine.org](http://ftp.porcupine.org)
- SSH – <http://ftp.ssh.com/pub/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 v1 of ssh

## 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

## 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      : 192.168.1. 192.168.5.3
vsftpd       : LOCAL, 192.168.1.
in.ftpd, ftpd : .abc.com,192.168.1.4
sshd         : all
dtspcd       : 192.168.1.0/255.255.255.0
xmservd      : .abc.com,123.123.123.4
rexecd       : LOCAL,.abc.com,123.123.123.4
rexecd, telnetd : LOCAL, 192.168.1.
smtpd        : LOCAL, 192.168.1.
sendmail     : LOCAL, 192.168.1. EXCEPT 192.168.1.4
```

## Replacement portmap

- Wietse Venema - <ftp://ftp.porcupine.org/pub/security/index.html#software>
- 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.
- Now included in most Linux and Unix distributions

## Snort

- [www.snort.org](http://www.snort.org)
- Latest version is v2.3.0
- 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](http://www.tcpdump.org)

## Apache, Openssl, Modssl

- Apache
  - [www.apache.org](http://www.apache.org)
    - Latest is 1.3.33 or 2.0.53
  - Web server used by a huge number of web sites
  - Combine with openssl and modssl to add security
- Modssl & openssl
  - [www.modssl.org](http://www.modssl.org)
    - For Apache 1.3
    - Latest version is 2.8.22-1.3.33
  - [www.openssl.org](http://www.openssl.org)
    - OpenSSL 0.9.7d fixes known security holes
    - 0.9.7e is available – have had problems compiling it
  - Provide SSL v2 and v3 implementations
  - Provide TLS (transport layer security)

## Stunnel

- [www.stunnel.org](http://www.stunnel.org)
- Latest version is 4.05
- 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

## Log Facility

auth.notice            /usr/local/logs/syslog  
facility.priority      action

- 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 & maillog & 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/maillog
  - auth.notice /usr/local/logs/syslog
  - daemon.info /usr/local/logs/infolog
  - \*.emerg /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
- Move logs out of default /var location to own filesystem

# 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.samspace.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 -l`
  - Should show the same result as:
- `ls -d /proc /[0-9]* | wc -l`
- If no-headers 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 ".. "
- try du, ls, ps, and netstat with the -/ option
  - If this works then a rootkit has probably been installed
- Use safe (saved to cd) copied of top, lsof and tcplist to check the system
- Look for binary zeroes in utmp & wtmp & lastlog to see if someone used zap

## Articles worth Reading

- Article on rootkits
  - <http://www.cs.wright.edu/people/faculty/pmateti/Courses/499/Fortification/obrien.html>
- SANS Analysis of the T0rn rootkit
  - <http://www.sans.org/y2k/t0rn.htm>
- Analysis of the Knark Rootkit
  - <http://www.securityfocus.com/guest/4871>
- <http://www.linuxsecurity.com>
  - Security Quick Reference Guide

## How to detect sniffers

- `ifconfig -a | grep PROMISC`
- [www.securitysoftwaretec.com/antisniff](http://www.securitysoftwaretec.com/antisniff)
- Nmap – [www.insecure.org/nmap](http://www.insecure.org/nmap)
  - `nmap -p 1-65535 systemname`
  - Scans all ports on the system
- `netstat -a`

## Scan yourself

- Saint
  - <http://www.saintcorporation.com/>
- ISS (Internet Security Systems)
  - <http://xforce.iss.net/>
- Nmap
  - `nmap -sTU <remote host>`
- Nessus
  - [www.nessus.org](http://www.nessus.org)
- Also portsentry to monitor ports
  - <http://sourceforge.net/projects/sentrytools/>

## Finding active network ports

- Isof
  - <http://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/Isof/>
  - Use command to check for open ports
  - `Isof | grep TCP`      or `grep UDP`
- `netstat -tulp`

## 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

- CHAIN OF CUSTODY
- Copies of all logs (signed and dated)
- Output from last and lastcomm commands
- Output from ls -al and other commands
- Output from lsof
- If email - copy of raw headers for the messages
- Username, phone number, etc
- Email address including mail node
  - See next slide

## Obtaining Email Headers

- Instructions for most clients are at:
  - <http://www.spamcop.net/fom-serve/cache/19.html>
  - <http://www.haltabuse.org/help/headers/index.shtml>
  - <http://www.wiredkids.org/safety/e-mail/getheaders.html>
- Info on Email Headers in general:
  - <http://www.stopspam.org/email/headers.html>
  - <http://tgos.org/newbie/xheader.html>

## Questions



## Helpful Sites 1/2

- <http://cs-www.ncsl.nist.gov/tools/tools.htm>
- [www.cert.org](http://www.cert.org)
- [ciac.llnl.gov](http://ciac.llnl.gov)
- [www.cs.purdue.edu/coast/](http://www.cs.purdue.edu/coast/)
- [www.defcon.org](http://www.defcon.org)
- [www.first.org](http://www.first.org)
- [www.iss.net/lists/ntsecurity](http://www.iss.net/lists/ntsecurity)
- [www.ntbugtraq.com](http://www.ntbugtraq.com)
- [www.securityfocus.com](http://www.securityfocus.com) - Bugtraq
- [www.sampade.org](http://www.sampade.org) - put in ip address to find domain
- [www.networksolutions.com/cgi-bin/whois/whois](http://www.networksolutions.com/cgi-bin/whois/whois)
- [www.deja.com](http://www.deja.com) - deja news
- [www.wiredpatrol.org](http://www.wiredpatrol.org)
- [www.sans.org/top20/#index](http://www.sans.org/top20/#index) - SANS top 20

## Helpful Sites 2/2

- [www.haltabuse.org](http://www.haltabuse.org)
- [www.scambusters.org](http://www.scambusters.org)
- [www.cauce.org](http://www.cauce.org)
- [getnetwise.org](http://getnetwise.org)
- [privacyrights.org](http://privacyrights.org)
- [www.hackingexposed.com](http://www.hackingexposed.com)
- [www.networkkice.com](http://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>
- <http://www.linuxsecurity.com>