

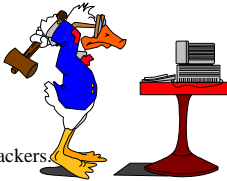
# Securing Your UNIX System Against Hackers

Jaqui Lynch

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

Session 1798 9.30am 2/27/04

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



## Agenda

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

## 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](mailto:cert-advisory-request@cert.org)

## CERT Statistics

– Year	1997	1998	1999	2000	2001	2002	2003
– Emails	39,626	41,871	34,612	56,365	118,907	204,841	542,754
– Calls	1,058	1,001	2,099	1280	1,417	880	934
– Vuln. Reports	311	262	419	1,090	2,437	4,129	3,784
– Incidents	2,134	3,734	9,859	21,756	52,658	82,094	137,529
– Sites	146,484						
– Alerts Published	50	34	22	26	41	41	32
– Security Notes		15	11	57	341	381	259

– Please note: Data taken from:  
[http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html)

# CERT

## CERT – Current Vulnerabilities and Trends

<http://www.cert.org/present/cert-overview-trends/module-5.pdf>

## Update on Cert Mailing List:

<http://www.cert.org/advisories/us-cert-announcement.html>

## Ports Associated with Known Vulnerabilities and Exploits:

[http://www.cert.org/current/services\\_ports.html](http://www.cert.org/current/services_ports.html)

# Levels & Types of Attacks

## ➤ Levels

- Root access break-in
- Replacement of materials
- Damage done
- Just looking
- Theft of proprietary information
- Denial of service
- Worms and Trojans

## ➤ 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
- Buffer Overflow

# SANS Top 20

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

- |  |   |
|--|---|
| 1. U1 BIND/DNS   | 6. U6 Sendmail                                  |
| 1. DOS, buffer overflow, etc   | 1. Buffer overflows and misconfiguration        |
| 2. U2 Remote Procedure Calls (RPC)   | 7. U7 Simple Network Management Protocol (SNMP) |
| 1. Known holes in ttdberv, cmsd, etc   | 1. Public/Private, v1 very insecure             |
| 3. U3 Apache Web Server  | 8. U8 Secure Shell (SSH)                        |
| 1. Mod_ssl worm, chunk handling exploit, default cgi                                       | 1. Several bugs, trojan version                 |
| 4. U4 General Unix Authentication  | 9. U9 Misconfiguration of NIS/NFS               |
| 1. Accounts with No Passwords or Weak Passwords  | 1. Multiple exploits                            |
| 5. U5 CLEAR TEXT SERVICES  | 10. U10 Open Secure Sockets Layer               |
| 1. Services such as telnet, imap, smtp, r*, http and ftp that send passwords in clear text | 1. Multiple exploits                            |

**Top 10 UNIX Vulnerabilities as at Oct 8, 2003**

# Tools

- TCP Wrappers and SSH
- Portmap
- Snort
- Apache, Openssl, Modssl
- Stunnel
- Logging

## 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 – do not install v1

## 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/sbin/dtspcd /usr/sbin/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

## Xinetd.conf

### /etc/xinetd.d

```
[root@biteme xinetd.d]# more telnet
# default: on
# description: The telnet server serves telnet sessions; it uses \
# unencrypted username/password pairs for authentication.
service telnet
{
    flags        = REUSE
    socket_type  = stream
    wait        = no
    user        = root
    server       = /usr/sbin/in.telnetd
    log_on_failure += USERID
    disable     = yes
}
```

## /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. 255.255.255.
##portmap    : 255.255.255.255/0.0.0.0
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.
```

## Replacement portmap

- [Wietse Venema - ftp://ftp.porcupine.org/pub/security/index.html#software](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](http://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 v2.1.1
- 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 1.3.29 or 2.0.48
    - Both have a bug if you use mod\_usertrack with the default CookieName - will be fixed in next releases
  - 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 2.8.16-1.3.29
  - [www.openssl.org](http://www.openssl.org)
    - OpenSSL 0.9.6l fixes known security holes
  - 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 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.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 “..”
- 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 tcpllist 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>

## 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/>
- Nessus
  - [www.nessus.org](http://www.nessus.org)
- Also portsentry to monitor ports
  - <http://sourceforge.net/projects/sentrytools/>
- Isuf
  - <http://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/Isuf/>
  - Use command to check for open ports
  - `Isuf | grep TCP` or `grep UDP`

## 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 Isuf
- If email - copy of raw headers for the messages
- Username, phone number, etc
- Email address including mail node
- <http://www.wiredkids.org/safety/e-mail/headers.html>

## Questions



## Patch Information

- DEC
  - [http://www.service.digital.com/html/patch\\_service.html](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](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>

## Useful Alert Pages

- IBM Research Hype Alerts
  - [Http://www.av.ibm.com](http://www.av.ibm.com) & [www.ers.ibm.com](http://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

## 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](http://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
- Hackers Challenge 2 - Mike Schiffman - 0072226307
- 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](http://www.amazon.com)
  - [www.barnesandnoble.com](http://www.barnesandnoble.com)
  - [www.bookpool.com](http://www.bookpool.com)