Server management and security

Cctld workshop
Amsterdam, 19-22 june 2004
aalain@trstech.net
Table of contents

• Before we start
• Security basics
• Unix / Linux sever security
• System setup guide
• Detection
Module 1: Before we start
Welcome to wild Internet!

- Quote from Crypto-Gram (June 15, 2001)

A random computer on the Internet is scanned dozens of times a day. The life expectancy of a default installation of Red Hat 6.2 server, or the time before someone successfully hacks it, is less than 72 hours. A common home user setup, with Windows 98 and file sharing enabled, was hacked *five times in four days*. Systems are subjected to NetBIOS scans an average of 17 times a day. And the fastest time for a server being hacked: *15 minutes after plugging* it into the network.
No system is ever perfectly secure.
But, still we need security.

- Any number of toolkits exist that allow total amateurs to become holy terrors.
- The good news is that if you can beat the popular intrusion toolkits, 90 percent of the bad guys will go bother somebody else who's less secure.
System security in a page

• The Seven Most Deadly Sins
  – Weak Passwords
  – Open Network Ports
  – Old Software Version
  – Poor Physical Security
  – Insecure CGIs
  – Stale and Unnecessary Accounts
  – Procrastination
Module 2 : Security basics
Security requirements

- Confidentiality
- Integrity
- Authentication
- Non-repudiation
- Availability
- Access control
- Combined
  - User authentication used for access control
  - Non-repudiation combined with authentication
Some terminologies

• System security / network security
• Passive attack / active attack
  – sniffing / spoofing
• Two models
  – Access control
    • discretionary access control vs. mandatory access control
  – Audit
Module 3: Unix / Linux server security

- Password
- Superuser
- File system
- Account
- Integrity
- Log and Audit
- TCP/IP
Module 3-1: Password
Bad passwords

- Your name, spouse’s name, partner’s name, pet’s name, child’s name, friends’ name, boss’s name
- Operating system, hostname, username
- Phone number, license plate number, birth date, social security number
- Words in the dictionary
- Simple patterns of letters on the keyboard (qwerty)
- Passwords of all the same letter
- Any of above spelled backwards
- Any of above followed or prepended by a single digit
Good passwords

- Have both uppercase and lowercase letters.
- Have digits and/or punctuation characters as well as letters.
- May include some control characters and/or spaces.
- Are easy to remember, so they do not have to be written down.
- Are seven or eight characters long.

Password
Methods of Authentication

WHO are you?  What credentials do you give?

Weak

No username/password
Static username/password
Aging username/password
One-Time Password (OTP)
  S/Key—OTP for terminal login
  PAP—OTP for PPP
  Token cards/soft tokens (OTP)
  Enigma Logic, DES Card, Security Dynamics

Strong

Password
The Thompson Test

- Devised by Ken Thompson
- Cracking algorithm
  - One to six ASCII characters
  - Seven or eight lowercase letters
  - Any word from a large dictionary such as hangman-words, or a word spelled backward or with the digit “1” instead of the letter “l”, with the digit “0” instead of the letter “o”, or with the digit “3” instead of the letter “e”.
  - Any pair of words from a large dictionary or words spelled backwards.
Module 3-2 : Superuser
Who is superuser?

• UID of 0
• Any username can be the superuser.
• Normal security checks and constraints are ignored for the superuser.
• Superuser is not for casual use.
  – Do not login as superuser, use ‘/bin/su’ with “-” option instead.
Module 3-3 : File system
File permission

File type
- : plain file
d : directory
c : character device (tty, printer)
b : block device (disk, CD-ROM)
l : symbolic link
s : socket
=: , p : FIFO

Access granted to owner
r : read / w : write / x : execute

Access granted to group member

Access granted to others

File system
SUID/SGID/sticky bits

• SUID (set uid)
  - Processes are granted access to system resources based on user who owns the file.

• SGID (set gid)
  - (For file) Same with SUID except group is affected.
  - (For directory) Files created in that directory will have their group set to the directory's group.

• sticky bit
  - If set on a directory, then a user may only delete files that the he owns or for which he has explicit write permission granted, even when he has write access to the directory. (e.g. /tmp )

File system
File system tips

• Finding SUID and SGID Files
  # find /\( -local -o -prune \) \( -perm -004000 -o
  -perm -002000 \) -type f -print
  ( xdev can be used in place of local/prune)

• Files without associated owner/group can be a signal of compromise.
  # find / -nouser -o -nogroup -print

• Users are not allowed to have .rhosts file.
  # find /home -name .rhosts -print
File system tips (continued)

• Turning off SUID / SGID in mounted file system
  – use nosuid (and nodev if possible) when mounting remote file system or allowing users to mount floppies or CD-ROMs

• Device file can be created as a backdoor after compromise.
  # find / \( -local -o -prune \) \( -type c -o -type b \) -exec ls -l \{ \};
Critical system files

- These files should be backed up and compared with saved version frequently.
  - /etc/passwd, /etc/shadow, /etc/group
  - /etc/rc*
  - /etc/tty*, /etc/ttytab, /etc/inittab
  - /usr/lib/crontab, /usr/spool/cron/crontabs/, /etc/crontab
  - /usr/lib/aliases
  - /etc/exports, /etc/dfs/dfstab
  - /etc/netgroups
  - /etc/fstab, /etc/vfstab
  - /etc/inetd.conf
  - UUCP related files
Module 3-4 : Account
Dangerous accounts

• Accounts without passwords
  # cat /etc/passwd | awk -F: 'length($2)<1 {print $1}'

• Default accounts
  - Just remove them!

• Shared accounts
  - Less accountability, less security.
  - Create several accounts in a group.

• e-mail ID and account
  - Do not use e-mail ID as an account, utilized alias feature instead.
Dormant account

• Risks
  - Intruder can use dormant account without being noticed.
  - Owner of dormant account cannot follow your policy or order. (e.g. Dear every users, please change your passwords right now.)

• How to handle
  - Disabling dormant account automatically (SVR4)
    • `usermod -f 10 newcat` (locked if no login in 10 days)
  - Freeze it
    • Put “*” in password field
    • `chmod 0 /home/newcat`
    • `find / -user newcat -ls`
Module 3-6 : Log and audit
Basics

- Consider remote logging to secure log data.
- List of log files
  - acct / pacct : Commands run by users
  - aculog : Dial-out modem (acu : automatic call unit)
  - lastlog : Most recent login success/fail times
  - loginlog : Bad login attempts
  - messages : Console / syslog facility
  - sulog : su command
  - utmp / utmpx : Each user currently logged in
  - wtmp / wtmpx : Login/out, shutdown/startup
  - xferlog : FTP access

Log and audit
Files and commands

• lastlog file
  - lastlog (Linux only)
    • Displays last login time and location.

• u/wtmp file
  - last
    • Displays login and logout information about users and terminals

• acct/pacct file
  - (Solaris 5.8) /usr/lib/acct/[startup, shutacct]
    • Starts or stop accounting.
  - (Solaris 5.8) acctcom, lastcom
    • Displays the recent commands executed.

Log and audit
Monitoring logs

• logcheck (logsentry)
  – Extracts anything that might indicate a security violation or other abnormality, and informs via e-mail.
Module 3-8 : TCP/IP
Vulnerabilities

• ftp
  – Passwords are sent in plain text.
  – /etc/ftpusers
    • List of accounts that are NOT allowed to use ftp.

• telnet
  – Passwords are sent in plain text.
  – Attacker can hijack the session.
Vulnerabilities (continued)

- smtp (sendmail)
  - Must be upgraded 8.9.3 or higher. Current version is 8.12.6.
  - Check permission of /var/spool/mqueue, sendmail.cf, /etc/aliases*, /etc/mail/mailertable* (owned by root, writable by owner only)
Vulnerabilities (continued)

• Sun RPC portmapper
  - Assigns the TCP/UDP ports used for RPC.
  - To improve security, turn it off if possible. Or,
    • Replace it with Wietse Venema’s version.
    • Block packets on port 111.

• rexec, rsh, rlogin
  - Executes remote program or login.
  - rexec transmits plain text password and rsh/rlogin use “trusted host/user” concept.
  - Disable rexec, and replace rsh/rlogin with ssh.
Vulnerabilities (continued)

• web
  – Yet another BIG topic. See references;
    • Lincoln D. Stein’s WWW Security FAQ
    • Paul Phillips CGI security FAQ
      – http://www.primus.com/staff/paulp/cgi-security
    • NCSA’s CGI security documentation
      – http://hoohoo.ncsa.uiuc.edu/cgi/security.html
Vulnerabilities (continued)

• NFS
  - Limit exported and mounted file systems
  - Export read-only and use root ownership
  - Remove group-write permission for files and directories
  - Do not export server executables and home directories
  - Do not allow users to log into server
  - Use fsirand and set the portmon variable
  - Use showmount –e
  - Use secure NFS
Vulnerabilities (continued)

• tftp (UDP 69)
  – No security at all.

• finger (79)
  – Provides user information.

• POP (109, 110)
  – Username/password is sent in plain text.
Module 4:
System setup guide
Useful links for system setup

• Solaris
  – Solaris/Unix Security Checklist Version 1.0
    • http://www.geocities.com/losttoy2000/solarissec
      rtf
  – The Solaris Security FAQ
    • http://www.itworld.com/Comp/2377/security-faq/

• Linux
  – Securing Debian Manual
    • http://www.debian.org/doc/manuals/securing-
      debian-howto/
System setup steps (1/2)

1. Disconnect system from network.
2. Install a minimal Operating System.
3. Install the recommended patches.
4. Use BIOS/EEPROM security.
5. Securing root account
   1. Force root to login through su.
   2. Check environments
      1. default mask (027), PATH
5. Apply hardening script if available.
6. Direct syslog to loghost
System setup steps (2/2)

1. Create minimal accounts and disallow login.
2. Let minimal services run;
   1. /etc/rc*, /etc/inet.d
3. Use tcpwrapper for network services.
4. Install Secure Shell and encourage its use.
5. Install integrity checker (e.g. Tripwire).
6. Test it periodically
   1. e.g. Nessus, COPS, Tiger, ...
7. Monitor it forever
   1. Check logs, login/outs, commands
Module 5: Detection

- Monitoring
- Scanning
- Handling
Monitoring (1/2)

• Log (logcheck)
  – Propagate it using loghost and e-mail.
  – Check it.

• Network port (netstat)
  – Trojan horse may use network ports.

• Network (tcpdump)
Monitoring (2/2)

• Process (ps)
  – Check suspicious processes, e.g. compiler.
  – Record typical size of daemons and important programs to detect Trojan horse.

• Load (uptime)
Scanning

• Find suspicious files.
• Run Tripwire.
• Detect promiscuous network interfaces.
  – (see next page)
Perl script to detect sniffer

#!/usr/bin/perl
my $ifconfig = "/sbin/ifconfig";
my $recips = admin@my.admin.host;
my %PROMISC = ();
my $interface = "";
open( IFCONFIG, "$ifconfig" ) || die( "Error: cannot run ifconfig!" );
while( <INCONFIG> ) {
    $interface = $1 if m/^\s+$/;
    $PROMISC{$interface} = 1 if m/promisc/;
}
close( IFCONFIG );
if( %PROMISC ) {
    open( MAIL, "|Mail -s 'Promisc mode' $recips" ) || die( "Error: cannot send mail"
    );
    print MAIL "Interfaces in Promisc mode: 
    , join( " ", sort keys %PROMISC), 
    close MAIL;
}
Handling incidents

• Don’t panic
  – Is it really a security incident?
  – Was any damage really done?
  – Evidence or normal operation, that is the question.

• Document
  – Write down everything you find, always noting the date and time.

• Plan ahead !!!