

Audit and Security of UNIX

By

Rodney Kocot

**President
Systems Control and Security**

Copyright ©1999, 2001 Rodney Kocot, All rights reserved

Outline Part 1

Physical Security

Security Utilities

User Administration Files and Programs

- File Formats And Unix Programs Used To Manipulate Them
- User Attributes
- Crack Programs

Resource Protection and Management

- Types Of Files
- Protections For Types Of Files
- Resource Administration

Privileged Programs

- Setuid And Setgid Programs
- Programs Executed At Startup And In Other Privileged Situations

Outline Part 2

Schedulers

System Startup and Shutdown

Network Security

- File Formats
- Services, Their Uses And Abuses
- Scanning Software

Logging And Monitoring

- Common Logs And Their Formats
- Reporting And Review Procedures

Patch Management

Common Findings

Audit Approach

Scripts and Utilities

Sources Of Information

Pre-Test Part 1

1. Can you do an independent audit of a \$1,000.00 cash box by interviewing the manager of the cash box and not count the cash?
2. Can you perform an independent audit of a Unix operating system by interviewing the system manager?
3. In a Unix environment what command provides a list of files and their attributes?
4. What is the name of the most powerful userid on a Unix system?
5. What is the batch job scheduler on most Unix systems?
6. What is TFTP?
7. What command would you use to get a list of all the processes on a Unix system?
8. In a Unix system what is the file that contains the list of userids on the system and how many fields does it contain?

Pre-Test Part 2

9. In a Unix system which field is the password field?
10. Should the first line in `/etc/hosts.equiv` contain only a plus sign (“+”)?
11. In a Unix system should users be allowed to create their own `$HOME/.rhosts` file?
12. In a Unix system what does the “`pwd`” command display?
13. In a Unix system what does a `umask` of `077` mean?
14. In a Unix system what will the command “`find . -perm -4000`” show?
15. In a Unix system what information does the “`uname -a`” command provide?
16. In a Unix system how many terminals defined in `/etc/ttys:*` should have the secure key word specified?
17. If your systems are connected to internet what should be used to prevent unauthorized access?

Pre-Test Part 3

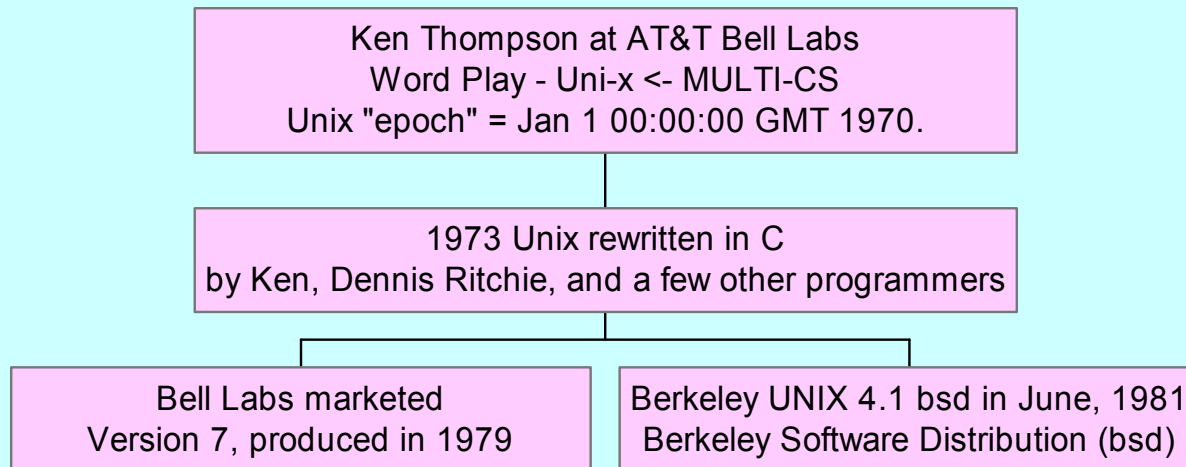
18. What public domain utilities are available to assist in maintaining and monitoring the security of Unix systems?
19. In a Unix system which users can set the sticky bit?
20. In a Unix system what startup shell scripts do users execute when they logon?

Introduction Part 1

This session will describe how to perform an audit of, and hack a Unix operating system. The listings and steps described are a compilation of numerous Unix operating system and penetration audits and include only security and management of the system. Sample listings will be reviewed. A generic audit program and utilities will be provided.

Introduction Part 2 - Unix History

Unix 25th Anniversary new-years-midnight GMT, January 1, 1995



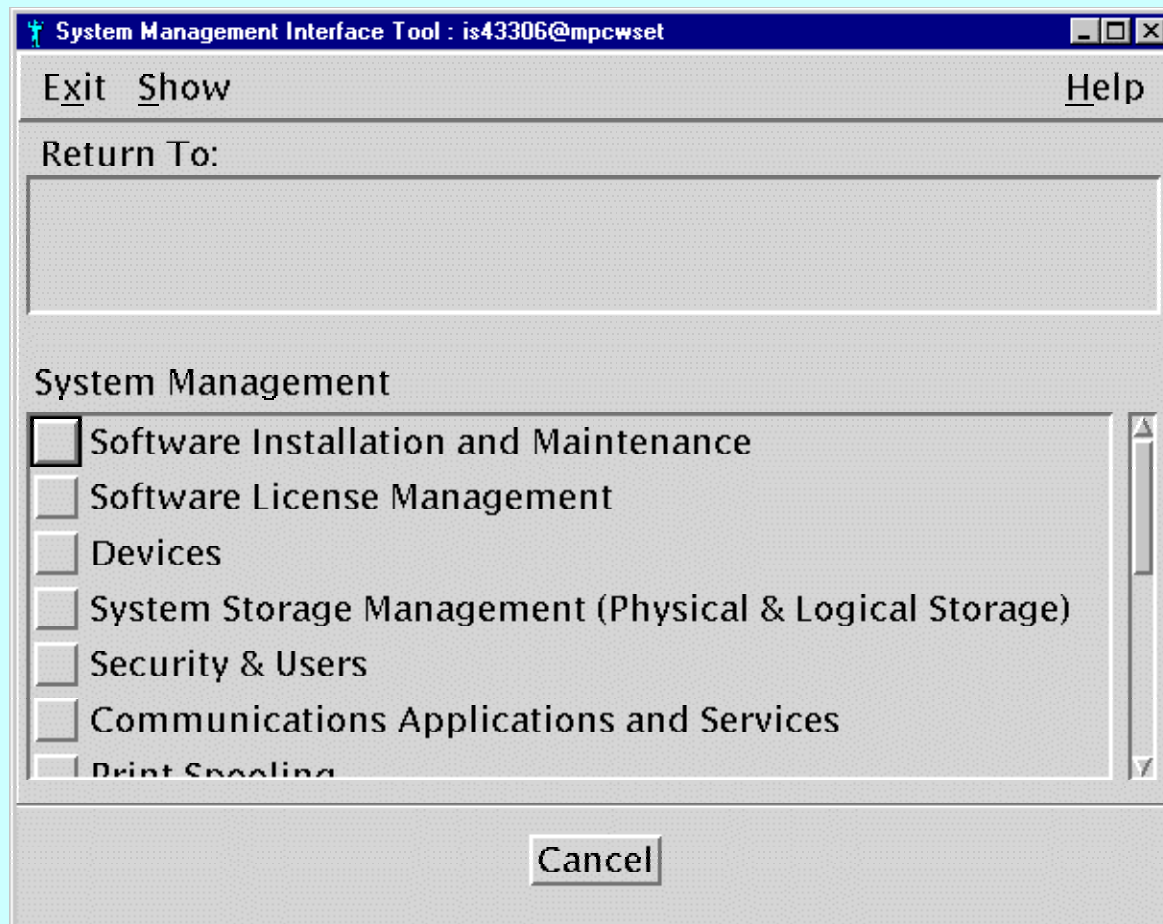
Physical Security

- Every person with physical access to the CPU, disk, and peripheral cabinets can compromise the security of the system.
- Every person in your building has the ability to force you to implement your contingency plan.
- Every person in the community around the building where your system is located can perform denial of service attacks.
- Every person on the network that your system is on can use the latest and greatest exploits available from the Internet.

System Management Utilities

- **AIX - System Management Interface Tool (SMIT)**
- **HPUX - System Administration Management (SAM)**
- **Solaris - Automated Security Enhancement Tool (ASET)**
- **Each implementation of Unix has numerous unique utilities. The best way to identify utilities for audit use is to review the system and security management manuals and man pages for the specific operating system and version you are reviewing.**

System Management Utilities - AIX, SMIT



System Management Utilities

- uname, motd

- AIX `uname -a`

```
AIX prod01 2 4 000073178200
```

- Solaris `uname -a`

```
uname SunOS dev01 5.5 Generic_103093-08 sun4d  
sparc SUNW,SPARCcenter-2000
```

- HPUX `uname -a`

```
HP-UX ub-hp755 A.09.05 E 9000/755 2010078180 8-  
user license
```

- **/etc/motd** - contains the message of the day

System Management Utilities

- df

```
$ df
Filesystem      512-blocks      Free %Used      Iused %Iused
  Mounted on
/dev/hd4         253952         95296   63%       1758     6% /
/dev/hd2        2662400        140864   95%      31828    10% /usr
/dev/hd3         204800        143336   31%        205     1% /tmp
/dev/hd1         106496         59072   45%        311     3% /home
/dev/hd10        319488         1024  100%         24     1%
  /usr/sys/xxxx
df: /xxx/local/oracle/controll: The file access permissions do
not allow the specified action.
$
```

System Management Utilities

- ps

```
$ ps # Process Status
```

```
  PID  TTY  TIME CMD  
53388 pts/2 0:00 ps  
56198 pts/2 0:00 -sh
```

```
$
```

```
$ ps -e
```

```
  PID  TTY  TIME CMD  
    1  - 11:17 init  
 2184  - 4:20 syncd  
 2628  - 0:00 srcmstr  
 2962  - 0:00 errdemon  
 3160  - 0:01 syslogd  
 3428  - 0:00 portmap  
 3934  - 0:00 sendmail  
 4458  - 0:00 inetd
```

System Management Utilities

- who, users, ...

```
$ users
```

```
guest root root root root
```

```
$ who
```

```
root      tty0      Mar 29 10:46
root      xdm/mpfncon Apr 06 16:23 (dev01)
root      pts/0     Apr 06 16:24 (dev01)
root      pts/1     Apr 06 16:24 (dev01)
guest     pts/2     Apr 06 19:29 (1.1.1.1)
```

```
$
```

User Administration

- Utilities
- File Formats
- Threats
- Controls
- Tests

User Administration - Utilities

- AIX - System Management Interface Tool (SMIT)
 - /usr/bin/pwdadm - administers users passwords
 - /usr/bin/passwd - changes a users password
 - /usr/bin/chfn - changes user information
 - /usr/bin/chsh - changes users shell
 - /usr/bin/login - initiates a user session
 - /usr/bin/pwdck - verifies local authentication information
 - ...
- HPUX - System Administration Management (SAM)
- Solaris - Automated Security Enhancement Tool (ASET)

User Administration - File Formats

- `Passwd` - basic user attributes
- `Security Passwd` - actual passwords and security information
- `Group` - groups and users assigned
- `Security Group` - passwords for groups
- **Additional AIX files:**
 - `/etc/security/user` - extended attributes of users.
 - `/etc/security/login.cfg` - configuration information and password restrictions

User Admin - File Formats - /etc/passwd

```
cat /etc/passwd
root:!:0:0:/:/bin/ksh
daemon:!:1:1::/etc:
bin:!:2:2::/bin:
sys:!:3:3::/usr/sys:
adm:!:4:4::/var/adm:
uucp:!:5:5::/usr/lib/uucp:
guest::100:100:~/home/guest:
nobody:!:4294967294:4294967294:~/:
lpd:!:104:-2:~/:
kocotr*:80:80:Rodney Kocot 8189510761:~/usr/rlk:~/bin/ksh
oracle:!:81:81:~/usr/oracle:~/bin/ksh
operator::203:1:~/usr/ops:~/bin/ksh
```

Username:Password:UID:GID:Comment:Directory:Shell

User Admin - File Formats - /etc/passwd

Common shells and initial scripts:

- Bourne - prompt \$
 - /etc/profile
 - /usr/lib/profile
 - \$HOME/.profile
 - Korn - prompt \$
 - /etc/profile
 - /usr/lib/profile
 - \$HOME/.profile
 - C shell - prompt %
 - /etc/cshprofile or
 - /etc/login or
 - /etc/cshrc
 - \$HOME/.cshrc and .login
- (root/administrator prompt #)

User Admin - File Formats - AIX /etc/security/passwd

```
cat /etc/security/passwd
```

```
root:
```

```
password = VWhzFJXLdCd/2    <= encrypted password  
lastupdate = 905314541      <= seconds since 1/1/1970  
flags =
```

```
daemon:
```

```
password = DIqv0Eh/DKSr2  
lastupdate = 798126276  
flags = ADMCHG                <= ADMIN  
                                ADMCHG -  
bin:                            NOCHECK - No password
```

```
password = TImG7Uy9NX8es  
restrictions  
lastupdate = 798126287  
flags = ADMCHG
```

User Admin - File Formats - Solaris /etc/shadow

```
cat /etc/shadow
root:Nrcq25BOBkOZ2:10119::::::
daemon:NP:6445::::::
bin:NP:6445::::::
sys:NP:6445::::::
adm:NP:6445::::::
lp::6445::::::
smtp:NP:6445::::::
tcp:YCCNwQD2JghBA:9957::::::
listen:*LK*::::::
nobody:NP:6445::::::
noaccess:NP:6445::::::
oracle:CQhRyU9sXfYOM:9757::::::
operator:IYhCDIkntqAGM:9965::::::
```

User Admin - File Formats - HP Group File

- `root::0:root,bob`
- `other::1:root,hpdb`
- `bin::2:root,bin`
- `sys::3:root,uucp,ray,supjamie,rmt`
- `adm::4:root,adm`
- `daemon::5:root,daemon`
- `mail::6:root`
- `lp::7:root,lp`
- `users::20:root,ray,guest,au007`
- `nogroup:*:-2:guest`
- `rmt*:200:rmt,au007,bob`
- `informix*:201:informix`

User Admin - File Formats - Other User AIX Files - login.cfg Part 1

`/etc/security/login.cfg` defines the following port attributes:

- `Herald` - message displayed when `getty` or `login` prompts for a login name.
- `Logindelay` - The delay (in seconds) between unsuccessful login attempts.
- `Logindisable` - The number of unsuccessful login attempts before port is locked. Used in conjunction with `logininterval`.
- `Logininterval` - The number of seconds during which `logindisable` unsuccessful login attempts must occur for a port to be locked.

User Admin - File Formats - Other User AIX Files - login.cfg Part 2

- `logindisable` unsuccessful login attempts must occur for a port to be locked.
- `Loginreenable` - The number of minutes after a port is locked that it will be automatically unlocked. Setting `Loginreenable` to 0 will cause the port to remain locked.
- `Logintimes` - Defines the times a user can use this port to login.
- `sak_enabled` - Defines whether users are allowed to access the trusted path through this port through the use of the secure attention key sequence (`ctrl-x ctrl-r`).
- `synonym` - Defines the set of ports which are synonyms for the given port; ...

The default stanza contains the default values used if no stanza appears for a given port.

User Admin - Other User AIX Files - etc/security/user

```
default:
  admin = false
  login = true
  su = true
  daemon = true
  rlogin = true
  sugroups = ALL
  ttys = ALL
  auth1 = SYSTEM
  auth2 = NONE
  tpath = nosak
  umask = 022
  expires = 0
  SYSTEM = "compat"
  logintimes =
  pwdwarntime = 0
  account_locked = false
  loginretries = 0
  histexpire = 0
```

```
  histsize = 0
  minage = 0
  maxage = 0
  maxexpired = -1
  minalpha = 0
  minother = 0
  minlen = 0
  mindiff = 0
  maxrepeats = 8
  dictionlist =
  pwdchecks =
  admgroups =
  dce_export = false
```

```
root:
  admin = true
  SYSTEM = "compat"
  loginretries = 0
  account_locked = false
```

User Admin - File Formats - Other Solaris Files

- **/etc/default/login** Controls system login policies, including root access. The default is to limit root access to the console.
- **/etc/default/passwd** Controls default policy on password aging
- **/etc/default/su** Controls which root (su) access to system will be logged and where it will be displayed!!!!!!!!!!!!
- groupadd
- groupdel
- groupmod
- useradd
- userdel
- usermod
- ...

User Admin - Application Users

```
Name: Oper: BANK_SF: App11
Id: 13
Password: oper
Administrative group: SysAdminG: BANK_SF: App11
Comment: App11 Operator account
Primary group: OperatorG: BANK_SF: App11
Creation time: Wed Apr 19 08:20:25 1995
Logon times: From *,*:* to *,*:*
Expiration time: No expiration
Last successful logon time: Fri Apr 2 21:33:05 1999
Last successful logon location: 1.1.1.1: BANK_SF: App11
Last failed logon time: Sun Apr 4 21:08:53 1999
Last failed logon location: 1.1.1.1: BANK_SF: App11
Last Failed Logon Error: <92,2,2>
Logon tally: 4381
Override system defaults: Yes
Maximum concurrent sessions: 10
Device security: No
Log successful logons: No
Log failed logons: No
Log security updates: No
```

User Administration - Threats

- Poor user administration resulting in:
 - Unauthorized and inappropriate userids
 - Easily guessable passwords, no passwords, or distribution passwords
 - Excessive root access
 - Shared userids

User Administration - Controls

- Formal user administration procedures exist and are followed
- Userids are disabled and removed after a period of inactivity
- The passwd file is periodically reviewed for easily guessable, null, and distribution passwords
- Users are forced to periodically change passwords
- Password requirements are defined in standards and users are forced to comply by system parameter settings
- Root access is restricted to the minimum number of trusted employees possible
- Shared userids are not allowed

User Administration - Tests

Part 1

- **Review the password and shadow password files for users that do not require a password.**
- **Run a password cracker to identify all weak passwords.**
- **Verify all passwords comply with company standards and that operating system controls are implemented to force compliance:**
 - **Password expiration,**
 - **Password minimum length, and**
 - **non-guessable**
- **Verify that unused userids are removed from the system.**
- **Verify that root and root equivalent userids are well controlled.**

User Administration - Tests

Part 2

- **If enhanced security is used ensure that administrator access is restricted.**
- **Identify sensitive groups and determine whether user groupings are appropriate.**
- **Interview all users with root access to determine level of security awareness**
- **Determine whether userids and passwords are shared.**
- **Verify that periodic self-audits are performed.**

Resource Protections

- ls Command
- Types of Resources
- Protection Bits
- umask
- ACLs
- Sensitive Files
- Threats
- Controls
- Tests

Resource Protections - ls Command

```
ls -albiR
Directory Tree
.:
total 4864
  2 drwxr-xr-x  38 root    root    1024 Oct  3 17:57 .
  2 drwxr-xr-x  38 root    root    1024 Oct  3 17:57 ..
264 -rw-r--r--   1 root    other   175 Dec 21 1996 .OWdefaults
995 -rw-----   1 root    other    0 Sep 17 20:28 .Xauthority
276 -rw-r--r--   1 root    other   186 Oct 31 1996 .ab_library
232 -rw-r--r--   1 root    other   204 Feb 29 1996 .cshrc
249 -rw-r--r--   1 root    other  1017 Mar 26 1997 .desksetdefaults
27255 drwx-----  2 root    other   512 Feb 29 1996 .fm
 233 -rw-r--r--   1 root    other   594 Feb 29 1996 .login
 231 -rw-r--r--   1 root    other   963 Jun 17 07:36 .profile
 252 -rw-r--r--   1 root    other    99 Oct  3 17:57 .rhosts
 250 -rw-----   1 root    other  3310 Oct  9 07:55 .sh_history
 248 drwxr-xr-x   2 root    other   512 Feb 29 1996 .wastebasket
   4 lrwxrwxrwx   1 root    root     9 Feb 29 1996 bin -> ./usr/bin
 226 drwxr-xr-x   7 root    nobody  512 Mar 17 1997 cdrom
```

inode, mode, links, owner, group, size, last mod date, file name

Resource Protections - Types of Resources

- **d** - directory.
- **b** - block special file.
- **c** - character special file.
- **l** - symbolic link,
- **p** - first-in,first-out (FIFO) special file.
- **s** - local socket.
- - - The entry is an ordinary file.

Resource Protections - Protection Bits

File Mode: -rwxrwxrwx+

- file type**
- r owner read**
- w owner write**
- x owner execute, s=SUID with x, S=SUID no x**
- r group read**
- w group Write**
- x group execute, s=SGID with x, S=SGID no x**
- r other read**
- w other write**
- x other execute, t=sticky bit with x, T=sticky no x**
- + ACL or TCB +=active, -=not active**

Resource Protections - umask

The default umask is 022. Umask is expressed in octal. Default permissions are derived by subtracting umask from the following permissions:

```
                421421421 <=bit values
directory      - rw-rw-rw-      bits=(42-42-42-) = 666
normal files   - rwxrwxrwx      bits=(421421421) = 777
```

```
directory      - 666 - 022 = 644 = rw-r--r--
normal files   - 777 - 022 = 755 = rwxr-xr-x
```

```
special        owner   group   other
421            421     421     421
```

```
4 = suid
2 = sgid
1 = sticky
```

find . -perm -4000

Resource Protections - Solaris ACLs

- ACLs are identified by a plus sign (+) to the right of the mode (protection) when using the "ls -l" command
- "getfacl" is used to display ACL entries. Use the -a option which displays the filename, owner, group, and ACL for the file

Resource Protections - Solaris ACLs For Directories

Valid formats for a Solaris directory ACL are:

- default:user::Permission
- default:group::Permission
- default:other::Permission
- default:mask::Permission
- default:user:UID:Permission
- default:group:GID: Permission

Resource Protections - Solaris ACLs For Files

Valid formats for a Solaris file ACL are:

- user::Permission
- group::Permission
- other::Permission
- mask::Permission
- user:UID or user name:Permission
- group:GID or group name: Permission

Resource Protections - Sensitive Files

- Identify all sensitive files and directories
- Determine appropriate security for all sensitive files
- Periodically review the protection for sensitive files

Privileged Programs - suid and guid

- **setuid** - A program with suid will run under the authority of the UID of the owner of the file. Only the owner of a file or root can set the suid bit using the **chmod** command.
- **setgid** - A program with sgid will run under the authority of the GID of the owner of the file. Only the owner of a file or root can set the sgid bit using the **chmod** command.
- **Usage Notes:**
 - **AIX ignores suid and sgid bits when executing shell scripts.**
 - **In some types of Unix the sgid bit on a directory determines how group ownership is assigned for files created in the directory.**

Privileged Programs - Sticky Bit

- **Sticky Bit:**
 - **In early versions of Unix the sticky bit was used to keep a program in memory for performance purposes**
 - **In AIX if a directory has the sticky bit then only the owner of the directory, root, or the owner of a file in the directory, can move or remove the file. Used to control access to files in unprotected directories.**

Schedulers - cron Part 1

`cron` is the Unix batch scheduler

- `cronadm` command lists or removes crontab or at jobs.
- `crontab` command is used to submit, edit, list, or remove cron jobs, crontab file format:

`minute hour day_of_month month weekday command`

- `/var/adm/cron/cron.allow` and `/var/adm/cron/cron.deny` specify users that can and can not use crontab. If neither of the above files exist only root can use crontab.

Schedulers - cron Part 2

- `/var/adm/cron` - main cron daemon directory
- `/var/spool/cron/atjobs` Indicates the spool area.
- `/var/adm/cron/log` Specifies the accounting information.
- `/var/adm/cron/queuedefs` file defines how the system handles different cron daemon events types.
- `/var/adm/cron/log` - accounting information.

Schedulers - at

`at` - allows users to specify, list, and delete jobs to be run at a later time. Files associated with `at`:

- **`/usr/bin/at` - at command.**
- **`/var/adm/cron/at.allow` and `/var/adm/cron/at.deny` files control who can use the `at` command, root users can create, edit, or delete these files.**
- **`var/adm/cron/FIFO` - sends messages to the cron daemon when new jobs are submitted with the `crontab` or `at` commands.**
- **`/var/adm/cron` - main cron directory.**
- **`/var/spool/cron/atjobs` - spool area directory for `at`.**

Schedulers - batch

batch runs jobs when the system load level permits.

- `usr/bin/batch` - batch command
- `/bin/batch` - symbolic link to the batch command

System Startup and Shutdown

- Each Unix vendor has implemented their own startup and shutdown processes. Refer to the System Management manuals and man pages for the version of Unix you are auditing to identify the appropriate commands, utilities, files, and controls for review. In general, most Unix systems use:
 - **/sbin/init** - creates processes defined in /etc/inittab
 - **/etc/inittab** - defines initial processes to be started
 - **/etc/telinit** - changes init's run level (single vs multi-user)
 - **shutdown** - used when multiple users are on the system
 - **reboot** - used when system is in single user mode
 - **/var/adm/wtmp** usually contains shutdown records

System Startup and Shutdown

- AIX

In addition to the files identified above, AIX uses the following files and many others. Checkout the manuals and man pages for details regarding the startup and shutdown processes.

- **fastboot** - restarts the system by calling reboot
- **/etc/rc.boot** - controls the machine boot process
- **/usr/lib/boot/ssh** calls the **rc.boot** file

- **lsattr -D -l sys0** - shows the value of the autorestart parameter
- **chdev -l sys0 -a autorestart=true** - the value of the autorestart parameter to true

Network Security

- Network Filtering
- Commands
- Files
- Network File System
- Audit Program

Network Filtering (Part 1)

If the following services are not required from outside your domain then filter them out at the router:

•Name	Port	Protocol
•echo	7	TCP/UDP
•sysstat	11	TCP
•netstat	15	TCP
•bootp	67	UDP
•tftp	69	UDP
•link	87	TCP
•supdup	95	TCP
•sunrpc	111	TCP/UDP
•NeWS	144	TCP
•snmp	161	UDP
•xdmcp	177	UDP
•exec	512	TCP

Network Filtering (Part 2)

If the following services are not required from outside your domain then filter them out at the router:

- login 513 TCP
- shell 514 TCP
- printer 515 TCP
- biff 512 UDP
- who 513 UDP
- syslog 514 UDP
- uucp 540 TCP
- route 520 UDP
- openwin 2000 TCP
- NFS 2049 UDP/TCP
- X11 6000 to 6000+n TCP (where n is the maximum number of X servers you will have)

Network Security - Commands

Following are only a few of the network commands available:

- **tftp -**
- **ftp -**
- **login -**
- **rcp -**
- **rexec -**
- **rsh -**
- **telnet -**
- **...**

Network Security - Commands

Disable all "r" commands unless specifically required:

- **rlogin,**
- **rsh,**
- **...**

- **If r commands are required then:**
- **Filter ports used by "r" commands**
- **Use secure versions of "r" commands**
- **Use tcp wrappers so a small number of ports are exposed**

Network Security - Files - inetd.conf - Part 1

- `inetd.conf` -

```
ftp      stream  tcp      nowait  root    /usr/sbin/ftpd      ftpd
telnet   stream  tcp      nowait  root    /usr/sbin/telnetd   telnetd
shell    stream  tcp      nowait  root    /usr/sbin/rshd      rshd
login    stream  tcp      nowait  root    /usr/sbin/rlogind   rlogind
exec     stream  tcp      nowait  root    /usr/sbin/rexecd    rexecd
#uucp    stream  tcp      nowait  root    /usr/sbin/uucpd     uucpd
## Finger, systat and netstat give out user information which may be
## valuable to potential "system crackers."  Many sites choose to disable
## some or all of these services to improve security.
##
#finger  stream  tcp      nowait  nobody  /usr/sbin/fingerd   fingerd
#systat  stream  tcp      nowait  nobody  /usr/bin/ps          ps -ef
tftp     dgram   udp      wait    nobody   /usr/sbin/tftpd     tftpd -n
#talk    dgram   udp      wait    root    /usr/sbin/talkd     talkd
ntalk    dgram   udp      wait    root    /usr/sbin/talkd     talkd
#
# rexd uses very minimal authentication and many sites choose to disable
# this service to improve security.
#rexid   sunrpc_tcp  tcp  wait  root  /usr/sbin/rpc.rexd  rexd 100017 1
```

Network Security - Files - inetd.conf - Part 2

Several vendors have implemented secure TCP/IP options. In the AIX TCP/IP security enhancement, the following programs are not allowed to execute on a secure system:

TFTP=/usr/bin/tftp
UTFTP=/usr/bin/utftp
TFTPD=/usr/sbin/tftpd
RCP=/usr/bin/rcp
RLOGIN=/usr/bin/rlogin
RLOGIND=/usr/sbin/rlogind
RSH=/usr/bin/rsh
RSHD=/usr/sbin/rshd

Many of the above services also have their own security features. For example, in AIX, **/etc/tftpaccess.ctl** can be used to restrict the directories that TFTP can use.

Network Security - Files - hosts.equiv

- `hosts.equiv` - this file and a local user's `$HOME/.rhosts` file, identifies users on remote hosts who are permitted to remotely execute commands on this host:

```
dev01
laprod1    user1
-laprod1   auditor
```

- + - any host on the network is trusted.
- HostName - host is trusted
- -HostName - host is not trusted
- HostName UserName - user on host is trusted
- -HostName UserName - user on host is not trusted
- +@NetGroup - all hosts in netgroup are trusted
- -@NetGroup - no hosts in netgroup are trusted

Network Security - Files - .rhosts

`$HOME/.rhosts` and user `.rhosts` files -

- support the following hostname entries:
 - +
 - *HostName*
 - *-HostName*
 - *:@NetGroup*
 - *-@NetGroup*
- support the following username entries:
 - +
 - *UserName*
 - *-UserName*
 - *:@NetGroup*
 - *-@NetGroup*

Network Security - Files - .rhosts

```
$ for i in $(find /usr -name .rhosts)
> do
>     ls -l $i
>     cat $i
>     print
> done
find: 0652-081 cannot change directory to </usr/lost+found>:
: The file access permissions do not allow the specified action.
-rw-----  1 usr1  usr1          84 Mar 27 15:51 /usr/usr1/.rhosts
cat: 0652-050 Cannot open /usr/usr1/.rhosts.

$ who am i
guest          pts/2          Apr 04 18:52   (1.1.1.1)
```

Network Security - Files - .rhosts

```
# for i in $(find . -name .rhosts)
> do
>         ls -l $i
>         cat $i
>         print
> done > rhost.out
# cat rhost.out
-rw-----  1 root  system      84 Jun 06 1995  /usr/usr1/.rhosts
dev01 root
prod01 usr1
prod01 root
-rw-----  1 root  system     113 Jan 13 1998  /.rhosts
dev01 root
prod01 usr1
prod01 root
test root
```

(Ask the system manager to use root for running listings that might need to access all the files on the system. Otherwise, as shown on the previous page, files will be missed.)

Network Security - NFS

Network File System (NFS)

- **Lsnfsexp** - Displays the characteristics of directories that are exported with NFS.
- **Lsnfsmnt** - Displays the characteristics of mounted NFS systems.

```
$ lsdfsexp
/cdrom          -ro
/upgrade       -rw
/usr/netstation -ro
/usr/sys/inst.images -rw
$
```

Network Security - Audit Program - Part 1

- With assistance from the system and network administrators identify and copy or print all network configuration files including but not limited to the following:
 - Network File System (NFS) files
 - Network Information Service (NIS) files
 - /etc/inetd.conf
 - /etc/hosts.equiv
 - \$HOME/.rhosts
 - All .rhosts files in user directories
 - /etc/netgroup
 - /etc/ftpusers
 - /etc/services
 - /etc/protocols
 - /etc/syslog.conf

Network Security - Audit Program - Part 2

- Review the listings for appropriate settings
- Determine whether any trusted relationships are appropriate
- Discuss the network implementation with the system and network administrators
- Determine whether all running services are appropriate
- Determine whether exported directories or devices are appropriate
- Test services from the network

Logging and Monitoring

- Log Files
- Log Utilities
- Log Formats
- Audit Program

Logging and Monitoring - Log Files - Generic

- **/etc/utmp** - users logged into the system
- **/var/adm/wtmp** - connect accounting information
- /var/adm/loginlog - login failures
- **/var/adm/sulog** - su attempts
- **/etc/default/su** - su logging options
- **/usr/adm/messages** or **/var/adm/messages** - system console messages

Logging and Monitoring - Log Files - AIX

- **/usr/sbin/acct** - directory containing programs for the accounting system
- **/var/adm** - directory containing data, report and summary files.
- auditing system configuration files:
 - **/etc/security/audit/config**
 - **/etc/security/audit/events**
 - **/etc/security/audit/objects**
 - **/etc/security/audit/bincmds**
 - **/etc/security/audit/streamcmds**
- **/usr/sbin/acct/lastlogin** - provides a report showing the last date each user logged in.
- **/etc/security/failedlogin** Contains invalid login attempts

Logging and Monitoring - Audit Program

- **Determine whether standards and procedures for logging and monitoring have been formalized.**
- **Determine whether standards and procedures for logging and monitoring are appropriate and at a minimum include:**
 - **logging of all logins and logoffs**
 - **monitoring login failures**
 - **monitoring accesses to sensitive files**
 - **monitoring network services activity**
 - **identification of shared passwords**
 - **excessive and/or unusual access**
 - **application users performing system commands**
 - **follow-up of security violations and break-ins**
- **Determine whether standards for logging and monitoring are implemented.**

Patch Management

- Policy
- Procedures
- Identify recent vendor patches and determine whether patches are installed according to formalized policies and procedures.

Audit Approach

- **Identify Key Resources**
 - **Identify knowledgeable Individuals**
 - **Locate Documentation**
- **Obtain Access (non-root!) Ask root to execute commands.**
- **Obtain Tools - ISS, ...**
- **Run Script**
- **Process Script**
- **Identify and Document Issues**
- **Discuss and Distribute Issues**
- **Write and Distribute Report**
- **Get Out of Dodge!**

Scripts and Utilities

- Password Crackers
- Command Lists
- AuditUnix.MDE
- Internet Security Scanner
- Trinux

Scripts and Utilities - Password Crackers

```
Crack, Dr. Jacks Crack, ... (www.rootshell.com)
```

```
=====
```

```
PWfile      : passwd.txt
```

```
Wordfile    : goodword.w
```

```
-----
```

```
inick:::216:200:::/ho:/bin/ksh
```

```
adm:adm:4:4::/usr/adm:
```

```
scottb:scott:200:200::/home/scott:/bin/ksh
```

```
test:test:235:200::/home/test:/bin/ksh
```

```
-----
```

```
Encryption/Comparisions: 23262
```

```
Time Elapsed In Seconds: 21
```

```
Mean Encryptions/Second: 1107.71
```

```
=====
```

Scripts and Utilities - Command Lists

```
# script script.log
```

```
echo "\n\n*****" >> $1
```

```
echo "uname -a" >> $1
```

```
uname -a >> $1
```

```
echo "\n\n*****" >> $1
```

```
echo " cat /etc/passwd" >> $1
```

```
cat /etc/passwd >> $1
```

```
echo "\n\n*****" >> $1
```

```
echo " cat /etc/security/passwd" >> $1
```

```
cat /etc/security/passwd >> $1
```

```
echo "\n\n*****" >> $1
```

```
echo " cat /etc/group" >> $1
```

```
cat /etc/group >> $1
```

Scripts and Utilities - Command Lists

```
echo "\n\n*****" >> $1
echo " cat /etc/security/group" >> $1
cat /etc/security/group >> $1
echo "\n\n*****" >> $1
echo "cat /etc/security/login.cfg" >> $1
cat /etc/security/login.cfg >> $1
echo "\n\n*****" >> $1
echo "cat /etc/security/user" >> $1
cat /etc/security/user >> $1
echo "\n\n*****" >> $1
echo "cat /etc/security/config" >> $1
cat /etc/security/config >> $1
echo "\n\n*****" >> $1
...
```

Scripts and Utilities - AuditUnix.MDB

Microsoft Access can be used to import many of the files and listings from a Unix system. Queries can be developed and reused audit after audit.

Scripts and Utilities - Internet Scanner

Internet Security Systems Inc (ISS)

Contact: Ashley Hanway

6600 Peachtree Dunwoody Road 300 Embassy Row

Atlanta, Georgia 30328 USA

Tel: 678-443-6000

Fax: 678-443-6477

E-mail: info@iss.net

Web: www.iss.net

Internet Scanner

Proactively performs comprehensive vulnerability detection. Can be used to automatically review network communication services, operating systems, key applications, firewalls and routers.

Common Findings - Part 1

- System wide issues
 - policies and standards are not formalized or implemented
 - responsibility for security administration is not assigned
- User Administration
 - periodic review of user profiles is not performed
 - unused userids exist
 - easily guessable passwords
 - password controls such as minimum password length and expiration dates not implemented
 - excessive root access
 - shared userids
 - application users have command line access

Common Findings - Part 2

- Resource Protections
 - sensitive files are not identified and periodically reviewed
 - sensitive files not protected appropriately
 - xx% of all the files on the system are unprotected
- Privileged Programs
 - suid and sgid files are not periodically reviewed
 - there is no list of authorized suid and sgid programs
 - suid or sgid programs provide excessive access
- Schedulers
 - scheduler configuration allows any user to submit jobs as any other user including root

Common Findings - Part 3

- Network Security
 - inetd.conf is configured to start insecure services
 - TFTP is running and not restricted to a specific directory
 - excessive and inappropriate trusted relationships exist
 - secure sockets are not used
 - exported file systems are inappropriate
- Logging and Monitoring
 - logging is not enabled
 - inadequate logging is being performed
 - logs are not periodically reviewed

Other Sources of Information

- Vendor Manuals!
- Internet search on the the following key words:
 - “Unix Security”, “AIX Security”, “Solaris Security”, ...
 - “Unix Management”, ...
 - Specific files and commands (passwd, aset, ...)
- The following sites have useful information:
 - Unix Tutorials - [//www.cs.canisius.edu/onlinestuff.html](http://www.cs.canisius.edu/onlinestuff.html)
 - AIX Manuals - [//www.austin.ibm.com/](http://www.austin.ibm.com/)
 - HPUX Man Pages - [//gto.ncsa.uiuc.edu/usail/man/hpux/](http://gto.ncsa.uiuc.edu/usail/man/hpux/)
 - AIX Security Checklist - <http://consort.cc.vt.edu/aix.security.html>
 - rootshell.com
 - ...
- Magazines

Other Sources of Information

- Information Security and Systems Programming must have a process in place to periodically receive and/or obtain information regarding new exploits and patches.
 - <http://www.cert.org/> - CERT® Coordination Center
 - <http://ciac.llnl.gov/ciac/CIACHome.html> - Computer Incident Advisory Capability
 - <http://www.cerias.purdue.edu/> - Center for Education and Research in Information Assurance and Security
 - Vendors
 - Hacker Sites

Post Test

- Are your Unix systems secure?