# HARDENING SOLARIS INSTALLATIONS

CHRIS HURLEY

DEFCON 10

© 2002, Security Horizon

# INTRODUCTION

The purpose of this presentation is to present a step by step guide to hardening a Solaris installation. Focusing primarily on Solaris 8 but with concepts that apply to all Solaris/Unix installs, I will focus on the steps that need to be taken to lock down a Solaris installation. While recognizing the best practice of pre-deployment hardening, the concepts presented also apply to already live Solaris installations. Rather than focusing on known attacks and reacting to them, this presentation will better equip system/security administrators to proactively reduce the risk of a successful attack against their systems.

© 2002, Security Horizon

# WHAT WILL BE COVERED

- INSTALLATION
- OPEN BOOT
- SCREEN AUTOLOCK
- SERVICES
- DISK QUOTAS
- ACCESS CONTROL LISTS
- SET UID/SET GID FILES
- PERMISSIONS
- PATHS
- ALIASING
- SYSTEM IDENTIFICATION
- GROUPS, ACCOUNTS AND PASSWORDS
- LOGGING

© 2002, Security Horizon

# WHAT WILL BE COVERED

**CRON AND AT JOBS**

**IF YOU MUST USE…**

**THE NDD's (aka The /etc/init.d/inetinit)**

**MISCELLANEOUS**

**AT THE BORDER**

© 2002, Security Horizon

# WHAT WILL NOT BE COVERED

DNS (BIND)
NIS/NIS+
NFS
SERVICE SPECIFIC/3rd PARTY SOFTWARE

© 2002, Security Horizon

# INSTALLATION

Load Solaris from an official CD.

Set up partitions large enough to accommodate patches and upgrades.

Do not load entire distribution. Load only needed packages.

Apply all appropriate security patches.

http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-license&nav=pub-patches

Maintain 2 current system backups, one on site, one off site.

© 2002, Security Horizon

# OPEN BOOT

Set OpenBoot Security level to command or full:

Command:

From root prompt (#):

#eeprom security-mode=command

From OpenBoot prompt:

ok setenv security-mode command

Full:

From root pormpt (#):

#eeprom security-mode=full

From OpenBoot prompt:

ok setenv security-mode full

© 2002, Security Horizon

# OPEN BOOT

Set OpenBoot password:

From root (#) prompt:

```
# eeprom security-password
```

From OpenBoot prompt:

```
ok password
```

Set OpenBoot Banner:

```
ok setenv oem-banner? true
ok setenv oem-banner “This system property of…”
```

© 2002, Security Horizon

# SCREEN AUTOLOCK

Enable screen autolock on GUI enabled systems

For CDE:

Right click on desktop and choose “Desktop Controls”

Open the “Screen Style Manager”

Choose the “On” radio button for screen lock and slide the “Start Lock” slide all the way to the left (1 minute).

© 2002, Security Horizon

# SCREEN AUTOLOCK

For OpenWindows:

Right click on desktop and choose “Properties”

Select “Miscellaneous”

Set screen saver to auto and fill in the number of minutes.

© 2002, Security Horizon

# SERVICES

DISABLE ALL UNNEEDED SERVICES:

Edit /etc/inetd.conf

Comment out all lines except those needed for operations.

Change names of startup and kill scripts in /etc/rc2.d and /etc/rc3.d

Ex.: #mv S76snmpdx s76snmpdx

HINT: To disable the GUI interface, but allow it to be easily started for administration purposes:

# mv S71rpc s71rpc

When GUI is needed:

# s71rpc start

© 2002, Security Horizon

# SERVICES

Make sure to disable sendmail if this is not a mail server.

```
# mv /etc/rc2.d/S88sendmail s88sendmail
```

If this is a mail server, configure it to prevent message source routing by commenting the following lines out of /etc/mail/sendmail.cf

```
R$+%$+              $@$>3$1@2                    user%host
R$*<@$%y.LOCAL      $#ether $@$2 $:$1<@$2>$3     user@host.your.domain
R$*<@$%x.LOCAL      $#ether $@$2 $:$1<@$2>$3     user@host.your.domain
R$*<@$%y>$*         $#ether $@$2 $:$1<@$2>$3     user@etherhost
R$*<@$%x>$*         $#ether $@$2 $:$1<@$2>$3     user@etherhost
R$+%$+              $@$>30$1@$2                  turn % => @, retry
```

© 2002, Security Horizon

# SERVICES

Also disable SMTP EXPN (expand) and VRFY (verify) by adding the following 2 lines to /etc/mail/sendmail.cf:

Opnoexpn

Opnovrfy

Install and configure Secure Shell (SSH) to replace clear text services FTP and Telnet with an encrypted tunnel service.

© 2002, Security Horizon

# DISK QUOTAS

Implement User Quotas:

Edit /etc/vfstab adding the mount option quota.

```
/dev/dsk/c0t0d0s7   /dev/rdsk/c0t0d0s7   /export/home   ufs   2   yes   quota
```

Create a file called quotas in the root directory of the filesystem (ex: /export/home

```
# touch /export/home/quotas
```

Set up a prototype quota entry using the edquota command

```
# edquota protouser
```

© 2002, Security Horizon

# DISK QUOTAS

Edit the number of hard and soft blocks and inodes

fs /export/home blocks (soft = 10000, hard = 12000) inodes (soft = 1000, hard = 1200)

2000 blocks is 1 MB. In this example the user has a soft quota (warning is issued) of 5 MB and a hard quota (user can no longer create files) of 6 MB. Inodes refers to the number of files a user may own.

This prototype must be replicated for all users.

```
# edquota –p protouser joeuser1 joeuser2
```

Activate quotas with the quotaon command

```
# quotaon /export/home
```

© 2002, Security Horizon

# DISK QUOTAS

The quotacheck command will build statistics

```
# quotacheck -a
```

The repqota command will create and display a report of active quotas:

```
# repquota –a
```

/dev/dsk/c0t0d0s7 (/export/home):

| | Block limits | | | | File limits | | | |
|---|---|---|---|---|---|---|---|---|
| User | used | soft | hard | timeleft | used | soft | hard | timeleft |
| Protouser -- | 50 | 10000 | 12000 | | 50 | 1000 | 12000 | |
| joeuser1 -- | 50 | 10000 | 12000 | | 50 | 1000 | 12000 | |
| joeuser2 -- | 50 | 10000 | 12000 | | 50 | 1000 | 12000 | |

© 2002, Security Horizon

# ACCESS CONTROL LISTS

Implement Access Control Lists

Use setfacl command to set access controls on individual files.

```
# ls –al accessfile
 -rw-rw--- 1 churley admins     31337 May 6 2002  accessfile
```

© 2002, Security Horizon

# ACCESS CONTROL LISTS

```
# getfacl accessfile
# file: accessfile
# owner: churley
# group: admins
user::rw-
group::rw-                    #effective:r--
mask:r--
other:---
```

© 2002, Security Horizon

# ACCESS CONTROL LISTS

```
# setfacl –m user:russ:rw- accessfile
# getfacl accessfile
# file: accessfile
# owner: churley
# group: admins
user::rw-
user:russ:rw-            #effective:rw-
group::rw-               #effective:r--
mask:r--
other:---
```

© 2002, Security Horizon

# SET UID/SET GID FILES

Find all SetUID and SetGID files

```
# find / -type f –perm –4000 –print >SUIDFiles
```

```
# find / -type f –perm –2000 –print >SGIDFiles
```

Find all world writable files

```
# find / -type f –perm –o+w –print >WorldWrites
```

© 2002, Security Horizon

# PERMISSIONS

Set root umask to 027 or 077.

Edit the /etc/default/login file to set a root umask of 077

Check system device permissions.

The initial install permissions are correct.
Under no circumstances should the permissions of a disk or device be changed.

Check permissions of /var/adm/utmpx

Ensure permissions of 644 ( -rw-r--r--)

© 2002, Security Horizon

# PERMISSIONS

Verify permissions of /etc/passwd are 644 (-rw-r--r--)

#ls –l /etc/passwd

-rw-r--r-- 1 root sys 468 Mar 22 16:51 /etc/passwd

Verify permissions of /etc/shadow are 400 (-r-------)

#ls –l /etc/shadow

-r-------- 1 root sys 301 Mar 22 16:53 /etc/shadow

© 2002, Security Horizon

# PERMISSIONS

Delete or restrict the /etc/hosts.equiv, /etc/.rhosts, and /etc/.netrc files

```
# touch /etc/hosts.equiv /etc/.rhosts /etc/.netrc
# chmod 0 /etc/hosts.equiv /etc/.rhosts /etc/.netrc
# ls –al /etc/hosts.equiv /etc/.rhosts /etc/.netrc
----------   1 root  other          0 Jun 14 15:56 /etc/hosts.equiv
----------   1 root  other          0 Jun 14 15:56 /etc/.rhosts
----------   1 root  other          0 Jun 14 15:56 /etc/.netrc
```

Restrict execute privileges on snoop to root:

```
# ls –al /usr/sbin/snoop
-r-x-r-x-r-x-          1 root bin  300352 Jan 5 2000 /usr/sbin/snoop
# chmod 500 /usr/sbin/snoop
# ls –al /usr/sbin/snoop
-r-x------     1 root bin  300352 Jan 5 2000 /usr/sbin/snoop
```

© 2002, Security Horizon

# PATHS

Set the root user path

Edit the /.profile to show the following:
PATH=/usr/bin:/sbin:/usr/sbin

Ensure that no user has “.” in his PATH

```
# su - joeuser1
$ echo $PATH
/usr/bin:
$
```

This should be done for each user. Alternatively, it can be scripted with the output sent to a file for later analysis.

© 2002, Security Horizon

# ALIASING

Alias the ls command to use the –a and –b options and
Alias the rm command to use the –i option

Edit each users login script to which the alias will apply:

C shell

Add the following to the .login file:

alias ls ‘/usr/bin/ls –a –b \!*’

alias rm ‘/usr/bin/rm –i \!*’

Bourne and Korn Shell

Add the following to the .profile file:

ls() { /usr/bin/ls –a –b $* ; }

rm() { /usr/bin/rm –i $* ; }

bash shell

Add the following to the .bashrc file:

ls() { /usr/bin/ls –a –b $* ; }

rm() { /usr/bin/rm –i $* ; }

© 2002, Security Horizon

# SYSTEM IDENTIFICATION

Include the system name in root and admins shell prompt.

C shell

Add the following to the .login file:

set prompt="'uname –n' # "

Bourne and Korn Shell

Add the following to the .profile file:

PS1="`uname –n` # "

export PS1

bash shell

Add the following to the .bashrc file:

PS1="`uname –n` # "

export PS1

© 2002, Security Horizon

# GROUPS, ACCOUNTS AND PASSWORDS

Require users to use the newgrp command to change groups.

1. Do not have any users assigned to groups other than staff.
2. Choose a strong group password.
3. Change the password of a normally locked account (ex. lp)

```
# passwd lp
New password: ********
Re-enter new password ********
#
```

© 2002, Security Horizon

# GROUPS, ACCOUNTS AND PASSWORDS

4. Extract the password string from /etc/shadow
5. Insert the string into the password field for the selected group in /etc/group. For example for the admins group:

admins:ijexo17Cu5tg:14:

6. Return the lp group to a locked state by editing the /etc/shadow

© 2002, Security Horizon

# GROUPS, ACCOUNTS AND PASSWORDS

Restrict use of su command.

Create an admins group

```
# echo admins::101:root >>/etc/group
```

Assign a password to the admins group.

```
# chgrp admins /usr/bin/su
# chmod o-rwx /usr/bin/su
```

Anyone wishing to execute the su command must now use the newgrp command to change to the admins group, provide the group password, and then execute the su command.

© 2002, Security Horizon

# GROUPS, ACCOUNTS AND PASSWORDS

Lock system accounts
Edit the /etc/shadow file to lock the daemon, lp, bin, sys, adm, uucp, nuucp, listen, nobody, and noaccess accounts.
A locked account looks like this:

```
#more /etc/shadow |grep lp
lp:*LK*:11771::::::
```

Lock sysadmin and sys groups
Edit the /etc/group file to lock the sysadmin and sys groups.
A locked group looks like this:

```
#more /etc/group |grep sys
sys:*LK*:3:root,bin,sys,adm
sysadmin:*LK*:14:
```

© 2002, Security Horizon

# GROUPS, ACCOUNTS AND PASSWORDS

Edit the /etc/default/passwd file to require password changes every 8 weeks with 1 week interval between changes and a minimum of 8 character length passwords. A properly configured /etc/default/passwd file will look like this:

```
# more /etc/default/passwd
#ident  "@(#)passwd.dfl 1.3   92/07/14 SMI"
MAXWEEKS=8
MINWEEKS=1
PASSLENGTH=8
#
```

© 2002, Security Horizon

# GROUPS, ACCOUNTS AND PASSWORDS

Run pwck to check for password file inconsistencies. This checks the field number, login name, UID, GID, and where the login directory and shell exist.

Run grpck to check for group inconsistencies. This checks the field number, group name, GID, whether any login names belong to more than the maximum allowable group memberships, and that all login names appear in the password file.

Verify permissions of /etc/group are 644 (-rw--r--)

```
#ls –l /etc/group
-rw-r--r--        1 root   sys       286      Mar 25 16:51 /etc/group
```

© 2002, Security Horizon

# LOGGING

Log all su attempts

Verify that /etc/default/su exists and provides a path to the sulog.

```
# grep SULOG /etc/default/su
SULOG=/var/adm/sulog
# more /var/adm/sulog
SU 03/22 18:19 + pts/4  joeuser1-root
```

© 2002, Security Horizon

# LOGGING

Log failed login attempts to loginlog.

```
# touch /var/adm/loginlog
# chown root:sys /var/adm/loginlog
# chmod 600 /var/adm/loginlog
```

Failed attempts logged to loginlog will look like this:

```
hax0r:/dev/pts/7:Fri Jun 14 12:12:12 2002
```

This indicates that on Friday June 14th at 12:12 a user attempted to log in as hax0r on /dev/pts/7 and failed.

© 2002, Security Horizon

# LOGGING

Turn on inetd connection tracing to attempt to trace all incoming TCP services. This will be logged to syslog.

Edit /etc/init.d/inetsvc and add –t to the inetd start line: /usr/sbin/inetd –s –t &

Reboot or kill and restart the inet daemon manually:

```
# ps –ef|grep inetd
        root 666 602 0 06:06:06 pts/4    0:00 grep inetd
        root  89     1 0 01:01:02 ?              0:00 /usr/sbin/inetd –s
# kill 89

# /usr/sbin/inetd –s -t
```

© 2002, Security Horizon

# LOGGING

Configure /etc/system to prevent stack based buffer overflow attacks.

Add the following lines to /etc/system:

set noexec_user_stack=1

set noexec_user_stack_log=1

This will help prevent attempts to execute code on the program stack. Additionally, it will log any attempts to do so in syslog.

Because some software uses the stack for program execution, this can cause some applications to fail. On operational systems, it is recommended to turn the logging on (set noexec_user_stack_log=1) for a couple of weeks of normal operation. If no attempts occur, add the other line.

© 2002, Security Horizon

# CRON AND AT JOBS

Check cron and at jobs for validity

```
# crontab -l
# at -l
```

Place the userids of users allowed to create cron jobs in the /etc/cron.d/cron.allow file

Place the userids of users allowed to create at jobs in the /etc/cron.d/at.allow file

Place the userids of users not allowed to create cron jobs in the /etc/cron.d/cron.deny file

Place the userids of users allowed to create cron jobs in the /etc/cron.d/at.deny file

© 2002, Security Horizon

# CRON AND AT JOBS

It is important to verify that all cron jobs are legit both before and after adding a user to cron.deny because cron.deny and at.deny only disallow users from creating future jobs. Already scheduled jobs will continue to run.

Also ensure that scripts and programs launched by cron and at are readable only by the owner

Ex. If /export/home/chris/mailrun.pl is scheduled to run daily in the crontab, it should look like this:

```
# ls –al /export/home/chris/mailrun.pl

-rwx------   1 chris staff   1024 May 5 19:37 mailrun.pl
```

© 2002, Security Horizon

# IF YOU MUST USE…

If FTP must be used, enable logging and debugging by editing the/etc/inetd.conf file and adding the –dl switches:

ftp stream tcp nowait root /usr/sbin/in.ftpd in.ftpd -dl

Make sure that root, uucp, bin, and anonymous are in the /etc/ftpusers file to prevent ftp access:

```
# more /etc/ftpusers
root
daemon
bin
sys
adm
lp
listen
nobody
noaccess
nobody4
anonymous
```

© 2002, Security Horizon

# IF YOU MUST USE…

Configure /etc/default/ftpd to remove the OS banner:

```
# touch /etc/default/ftpd
# echo BANNER=‘‘‘‘‘>/etc/default/ftpd
```

If Telnet must be used, edit the /etc/issue to issue a warning banner:

```
# touch /etc/issue
# echo “AUTHORIZED ACCESS ONLY, OTHERS WILL PERISH”>/etc/issue
```

Configure /etc/default/telnetd to remove the OS banner:

```
# touch /etc/default/telnetd
# echo BANNER=‘‘‘‘‘>/etc/default/ftpd
```

© 2002, Security Horizon

# THE NDD's (aka The /etc/init.d/inetinit)

Add the following lines to /etc/init.d/inetinit

If the system is not being used as a router, disable IP Forwarding and Directed Broadcasts:

```
# ndd –set /dev/ip ip_forwarding 0
# ndd –set /dev/ip ip_forward_directed_broadcasts 0
```

Configure the system to ignore redirects, and disable forward source routing:

```
# ndd –set /dev/ip ip_ignore_redirect 1
# ndd –set /dev/ip ip_forward_src_routed 0
```

© 2002, Security Horizon

# THE NDD's (aka The /etc/init.d/inetinit)

Configure the system not to repsond to address mask broadcast, echo boradcast, timestamp, and timestamp broadcast:

```
# ndd –set /dev/ip ip_repsond_to_address_mask_broadcast 0

# ndd –set /dev/ip ip_repsond_to_echo_broadcast 0

# ndd –set /dev/ip ip_repsond_to_timestamp 0

# ndd –set /dev/ip ip_repsond_to_timestamp_broadcast 0
```

© 2002, Security Horizon

# MISCELLANEOUS

Limit root login to console or preferably disallow direct root login.

Console only access:

Edit CONSOLE= setting in /etc/default/login to read:

CONSOLE=/dev/console

Disable direct root login:

Edit CONSOLE= setting in /etc/default/login to read:

CONSOLE=/dev/null

This will require anyone wishing root access to login as a normal user and su to root.

© 2002, Security Horizon

# MISCELLANEOUS

Prevent TCP sequence predictability by setting the initial sequence to 2 in /etc/default/inetinit:

TCP_STRONG_ISS=2

Edit /etc/profile and set the ulimit to 0 to restrict the generation of core files.

© 2002, Security Horizon

# MISCELLANEOUS

Randomize filesystem inode numbers using fsirand

Randomizing inode numbers for /, lost+found, and other filesystem files reduces the risk of an attacker altering files by inode number instead of by name.

A filesystem MUST be unmounted before fsirand can be run. Filesystems to be altered by fsirand should be backed up and fsck'd first.

WARNING: THIS CAN BE DANGEROUS. USE WITH CAUTION!!

© 2002, Security Horizon

# MISCELLANEOUS

Install and configure Tripwire and logcheck to monitor file and system integrity.

Install and configure an Intrusion Detection System such as Snort (www.snort.org) to monitor attempted intrusions.

© 2002, Security Horizon

# AT THE BORDER

Stop auth (identd) traffic at the border by blocking TCP and UDP port 113 traffic inbound.

Block ICMP type 17 (MASKREQ) traffic at the border.

Allow access through the firewall only to necessary ports on specific machines.

© 2002, Security Horizon

# CONCLUSION

While implementing the measures presented here will not guarantee that your server will not be compromised, it will enable you go beyond the current practice of patching after an exploit has been discovered.

Patches should still be applied, and other good security practices should still be followed. Users will continue to be the number one weakness and poor passwords/authentication practices must be followed

© 2002, Security Horizon

# REFERENCES AND FURTHER INFORMATION

http://www.sans.org/newlook/resources/hard_solaris.htm

http://www1.securityfocus.com/frames/?focus=sun&content=/focus/sun/articles/harden1.html

http://ist.uwaterloo.ca/security/howto/2000-09-19/

Solaris Security by Peter H. Gregory

ISBN 0-13-096053-5

Practical UNIX & Internet Security by Simson Garfinkel and Gene Spafford

ISBN 1-56592-148-8

© 2002, Security Horizon