websec.2006 World Trade Center

Febrero 15 y 16

Solaris Hardening – What's new, what's old in the world of Unix hardening…

Francisco Artes, cissp

Expectations

- **This talk's objective is to give the audience a brief overview of basic security steps that can be performed to help mitigate certain risks. This is not a complete 'hardening document', but should guard you from common hacker attacks while giving you time to read more security related material without feeling insecure.**
  - Definitions and examples of threats
  - Security from remote attacks
  - Operating system security

Definitions

- Remote compromise
- Local compromise
- Blended network compromise

What to do about blended attacks? – Hardening part 1.

- Hardening methodology
  - Step 1 - What can we harden from the installation and boot up process?
  - Step 2 - Turning off defaults & remote compromise
  - Step 3 - File system hardening
  - Step 4 - Auditing and Logging

  - We won't cover everything, but I hope this gives insight in what areas you can protect and why.

Startup & physical security controls – 2 types

- Openboot
  - Protect against physically booting to a cdrom to reset passwords.
  - Protect against what an attacker can do with Stop-A from a terminal!
- Partition Security
  - Set controls on what can be performed on certain partition spaces
    (eg nosuexec for normal user accounts)

OpenBoot Continued

- OpenBoot Security Levels

  None - no password required – this is a default

  Command – all commands except for boot and go require password, - system can boot automatically but when someone performs a stop-a, they must have a password

  Full – all commands except go (continue booting) require a password.

Openboot setup

- Setting passwords from file system
  - eeprom security-password
- Setting passwords from eeprom (stop-a)
  - ok password
- Setting security levels
  - eeprom security-mode=command
    or
  - ok setenv security-mode command

Openboot creativity

- Add some banners ☺

ok setenv oem-banner? true
ok setenv oem-banner “Stealing sucks”

In the beginning there was a partition!

- There are a large amount of attacks you can limit.

- Goal – upon install plan out your partitions.
  - Recommendations –
    - Setup separate partition for /var/, /tmp/, /usr/,/home
    - Setup nosuid on /tmp and /home

Tools you can use with partition security

- Tools
  - man mnttab
  - man mount_ufs
  - man fstab
  - Man mount_file-system-type
  - Man fsck
  - man mount
  - df -k or df -h

Useful Partition options

nosuid Do not allow set-user-identifier or set-group-identifier bits to take effect. Note: this option is worthless if a public available suid or sgid wrapper like suidperl(1) is installed on your system. It is set automatically when the user does not have super-user privileges.

ro read only file system

Secure /etc/mnttab (partition configuration)

/etc/mnttab

/dev/dsk/c0d0s7 /tmp ufs
ro,nosuid,intr,largefiles,logging,xattr,onerror=panic

Package Management: (pkgrm)

SUNWadmr
SUNWatfsr
SUNWcg6
SWUNWdtcor
SUNWkey
SUNWnisr
SUNWnisu
SUNWpcelx
SUNWpcmci
SUNWpcmcu
SUNWpcmem
SUNWpcser
SUNWpsdpr
SUNWsolnm
SUNWxwdv
SUNWxwmod

Package Management: (pkgadd -d)

SUNWdoc
SUNWfns
SUNWlibC
SUNWman
SUNWtoo
SUNWadmc
SUNWadmfw
SUNWscpu

SUNWast
--- Compiler –
SUNWarc
SUNWbtool
SUNWhea
SUNWsprot
SUNWlibm

Step 1, Fix SUID / SGID

```
find / -perm -4000 -print > /var/tmp/SUID
find / -perm -2000 -print > /var/tmp/SGID
ls -l `cat /var/tmp/SUID` > /var/tmp/SUID.long
ls -l `cat /var/tmp/SGID` > /var/tmp/SGID.long
chmod -s `cat /var/tmp/SUID`
chmod g-s `cat /var/tmp/SGID`

# Now we will put back and selectivly fix the mode on some of the files.

chmod 4555 /usr/bin/login
chmod 6555 /usr/bin/passwd
chmod 4555 /usr/bin/sparcv7/ps
chmod 4555 /usr/bin/sparcv7/uptime
chmod 4555 /usr/bin/sparcv7/w
```

More local file work:

Remove Group Write permission from /etc

chmod –R g-w /etc

Verify permissions on /var/adm/utmp and change if necessary:

Chmod 644 /var/adm/utmp

Find any world-writable directories (only tmp should have it.)

find / -perm -0002 –type d

Step 2 – Turn off remotely accessible services

- Turning off the defaults
  If you don't need it, turn it off!

  Solaris is horrible about this, they have all sorts of junk you need to turn off!

- Shutting down startup scripts

Shutting down startup scripts

- Start with /etc/rc2.d – View each startup script that starts with S*. Evaluate whether or not you _need_ these daemons running.
- Example items to turn off –
  - mv /etc/rc2.d/S47pppd /etc/rc2.d/OldS47ppd
  - mv /etc/rc2.d/S73cachefs.daemon /etc/rc2.d/OldS73cachefs.daemon

Recommended disabled services

/etc/rc2.d/S47pppd - pppd – used for dialup
/etc/rc2.d/S72slpd - p
/etc/rc2.d/S73cachefs.daemon
/etc/rc2.d/S80lp – printer services
/etc/rc2.d/S88sendmail - sendmail
/etc/rc2.d/S99dtlogin – gui login – why there is gui for a server, I don't know
/etc/rc2.d/S90wbem
/etc/rc2.d/S71rpc – rpc
/etc/rc3.d/S15nfs.server – file sharing
/etc/rc3.d/S77dmi
/etc/rc3.d/S76snmpdx – snmp (simple network hacking protocol)
/etc/rc3.d/S90samba – samba/cifs file sharing
/etc/rc3.d/S80miagent
/etc/rc2.d/S73nfs.client

Remote service

- Edit /etc/inetd.conf or simply turn off inetd.
- Turn off unneeded startup scripts
  - This can be done by
    mv /etc/rc2.d/S73cachefs.daemon
    /etc/rc2.d/Offcachefs.daemon
- Test services being off –
  - Netstat -an|grep LISTEN

    or

    ps -ef

Disable incoming syslog

- /etc/default/syslogd
  - Change
    - LOG_FROM_REMOTE=syslogd to
    - LOG_FROM_REMOTE=NO

Setting up appropriate perms on files created

- Tools
  - Umask -
    - Set /etc/profile set the umask to 027.
    - 027 = file perm 750 to be set for all files created by user x.
    - For root set umask to 077 (000)

Brief Kernel security

- Generic Buffer overflow protection (not supported in all solaris)
- /etc/system
  - set noexec_user_stack=1
  - set noexec_user_stack_log=1

Brief Kernel security

- TCP Sequence numbers
- /etc/default/inetinit
  - TCP_STRONG_ISS=2

  - This makes the system use a better randomized algorithm for generating TCP sequence numbers which can help prevent hijacking attacks.

Tune the TCP Stack: *Reboot!*

touch /etc/rc.local

Add the following lines:

```
ndd -set /dev/ip ip_respond_to_echo_broadcast 0
ndd -set /dev/ip ip_forward_directed_broadcasts 0
ndd -set /dev/ip ip_repond_to_timestamp 0
ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
ndd -set /dev/ip ip_forward_src_routed 0
ndd -set /dev/ip ip_ignore_redirect 1
ndd -set /dev/ip ip_respond_to_address_mask_broadcast 0
ndd -set /dev/ip ip_ignore_redirect 1
ndd -set /dev/ip ip_respond_to_address_mask_broadcast 0
ndd -set /dev/ip ip_ignore_redirect 1
ndd -set /dev/ip ip_send_redirects 0
ndd -set /dev/ip ip_forwarding 0
ndd -set /dev/ip ip_strict_dst_multihoming 1
ndd -set /dev/ip tcp_conn_req_max_q0 4096
ndd -set /dev/ip tcp_conn_req_max_q 1024
```

Make the file executable:
chmod 755 /etc/rc.local

---

echo "sh /etc/rc.local" >>/etc/rc2.d/S69inet

Logging & alerting

- Basic Logging
  - Kernel
    - /etc/security/bsmconv (starts bsm logging)
      - Tuning is up to you.
  - System
    - vi /etc/rc2.d/S71perf
      - Uncomment lines in this file
      - sar –A
      - Create cron script

```
#!/bin/sh
sys -c "/usr/lib/sa/sadc /var/adm/sa/sa`date +%d`"
```

BSM Readming
http://www.deer-run.com/~hal/sysadmin/SolarisBSMAuditing.html

Real world recommendations

- - Disable openssh, and enable ssh from ssh.com. The software is commercial, but is better for administrative overhead.
- - Disable syslogd and enable syslog-ng. You can do allot of cool remote syslogging options with syslog-ng.
- - Think about implementing this on your Jumpstart server.

  http://www.sun.com/software/security/jass

Now that the system is "secure"…

- Apply latest operating system patches

- download from

- ftp://sunsolve.sun.com/pub/patches

or visit

bigadmin.com

Integrity Checking

You are going to want to check if something has changed. So lets create an MD5 Hash of everything on our secure server:

```
#!/bin/sh
#
for i in `find / -name proc –prune –o type f –print`;
    do
    path_to_bin/md5sum $i >>/var/tmp/MD5SUMS
done
```

Automated Security Enhancement Tool: aset

Checks ownership and permissions of files and contents of system files.

vi /usr/aset/asetenv and comment out "noprog=false"

Create a root cron:

0 0 * * * /usr/aset/aset –l med –n admin@domain.com –u /etc/aset_users

Note: Place additional users, other then root, into the aset_users file.

Sources

- "Solaris Security" – Gregory Peter
- "Solaris System Administration Guide" – Janice Winsor
- CISECURITY – Solaris Benchmark

Thank you!

For the updated slides:

http://www.netassassin.com

My contact information:

falcor@netassassin.com