Hardening Solaris

Sun Microystem's Solaris Operating system is reasonably secure as delivered, but does have vunerablilities. This session will discuss how to remove those issues, and harden the Operating System to prevent attacks.

What Version of Solaris?

- Three Paths Available
- Solaris Operating System
- Solaris SE
- Trusted Solaris

Solaris Operating System

- Used by majority of Sun's Customers
- Can be hardened with reasonable effort
- Currently at Version 9 (SunOS 2.9)

But for those who want to be Certified...

Solaris 2.6SE

- Solaris 2.6SE has been evaluated at the ITSEC E3/F-C2 level.
- The evaluated configuration consists of Solaris 2.6 5/98 and a small set of standard Solaris 2.6 patches.
- Information about it can be found at:

  http://wwws.sun.com/software/security/securitycert/2.6.html

Trusted Solaris

- Trusted Solaris is Sun's product for those who are looking for the ultimate in commericial OS Security.
- Trusted Solaris 8 has entered evaulation under Common Criteria EAL4.
- Trusted Solaris 2.5 was ITSEC certified E3/F-B1 and E3/F-C2 in September, 1998.
- More information on Trusted Solaris is at: http://wwws.sun.com/software/solaris/trustedsolaris

Configuring Solaris

This section covers changes in Kernel, Filesystems, Permissions, Network Configuration to improve Solaris Security

Kernel Configuration Changes

- Add the following to */etc/system* to prevent and log stack buffer overflows attacks

  set noexec_user_stack=1
  set noexec_user_stack_log =1

Root User Configuration

- Ensure root has a umask setting of 077 or 027.
- Ensure root has a safe search path, as in */usr/bin:/sbin:/usr/sbin*

Securing the files in /etc

- Remove group write from all files in /etc.
- This can be done with the command **chmod -R g-w /etc**
- */etc/utmp* can be set to mode 644 without disrupting services**.**

Review all Startup Files

- Examine all startup files in */etc/rc2.d* and */etc/rc3.d*. (They start with an “S”)
- Rename any unnecessary startup files so they don't start with “S”
- Test by rebooting, and examining */var/adm/messages*
- Check for extraneous processes with **ps -elf** command.

Lock all Administrative Accounts

- Lock, or comment out unnecessary accounts
- Don't forget "sys", "uucp", "nuucp", and "listen".
- The easy way is to put "*LK*" in the password field of the */etc/shadow* file.
- Use the **noshell** program to log attempts to use secured accounts.
  - **Noshell** is part of **Titan**, which can be found at: http://www.fish.com/titan

Securing Devices

- Examine the file */etc/logindevperm*.
- It contains the configuration information for what permissions to set on devices associated with login (console, keyboard, etc).
- Modify them to give different permissions as needed.

Securing Removable Devices

- The Basic Security Module (BSM) can provide allocate and deallocate commands to ensure that only a single user can access removable media (such as tapes) at any one time.
- You can find a BSM Guide at:

  http://www.sans.org/rr/paper.php?id=403

Diasble the Automounter

- Automounter is controlled by the */etc/auto*_* configuration files.
- Remove those files, and/or disable the */etc/rc2.d/S74autofs*.

Don't forget the Cron Jobs

- Review the cron jobs of every system account in */var/spool/cron/crontabs*.
- Log all cron activities by setting "CRONLOG=yes" in */etc/default/cron*.

Remove setuid/setgid from Programs

- Find them with **find / -perm -4000 -print**
- Most are run by root or the user or group that owns them
- They can have the setuid and setgid bit removed
- Periodically check and make sure the list remains static

Network Configuration Changes

This Section details changes to Network Configuration files to improve Security

Disable Network root logins, rlogin and rsh

- Enable the "CONSOLE" line in */etc/default/login*.
- Remove */etc/hosts.equiv*, */.rhosts*
- Remove the "r" commands from */etc/inetd.conf*
- Refresh the inetd process with
  kill -HUP [inetd process id].

Don't let your machine be a router...

- Solaris will route packets if it has multiple network interfaces.
- This behavior is controlled by */etc/init.d/inetinit*.
- Add **ndd -set /dev/ip ip_forwarding 0** at the end of */etc/init.d/inetinit*. (Solaris 2.4 and below).
- Touch */etc/notrouter* (Solaris 2.5 and above).
- A small window of vulnerability exists during startup before the routing is turned off.

Prevent TCP Sequence Prediction Attacks

- Modify the variable **TCP_STRONG_ISS to be set to 2** in */etc/default/inetinit*

Disable NFS Services

- Remove the */etc/dfs/dfstab* file. This disables NFS exports.
- Disable the NFS server daemon by renaming */etc/rc3.d/S15nfs.server*.
- To prevent becoming an NFS client, rename */etc/rc2.d/S73nfs.client*.
- Be sure to name them with a starting letter other than "S".

Use Static Routes whenever possible

- Dynamic routing (**in.routed,in.rdisc**) is vulnerable to receiving incorrect routes.
- Use static routes to prevent this from happening.

Use Static ARP

- Solaris machines dynamically determine ARP by default.
- Use the **arp** command to statically set ARP table entries and flush other entries.
- Best used when there are few, unchanging systems on a network with no router between machines, and machines need to be assured of each other's identities.

Hardening System Services

This next section will address what can be removed or modified to increase Security

Disabling INETD Services

- Comment out the entries in the */etc/inetd.conf* file, except for **telnet** and **ftp**.
- If using **ssh** for network access, you can remove them as well.
- If needed, use **xinetd** instead of **inetd** to add logging facilities.

Sendmail

- The current version of sendmail is always available from Berkeley.
- Note: Sun specific modifcations that will be lost if you move to a Berkley sendmail.
- Sun sendmail patches have a tendency to replace Berkeley sendmail with Sun's sendmail.
- Check that the sendmail version that you want to run is still in place after installing patches.

BIND

- Bind on Solaris has known security problems (Just check www.cert.org).
- The problems do get patched, but Solaris bind is generally behind on patches.
- The current standard bind release is always available at ftp://ftp.isc.org/isc/bind

FTP

- **wu-ftp** is a replacement for the standard ftpd daemon. It has extensive logging and access control.
- You can find it at: http://www.wu-ftpd.org/wu-ftpd-faq.html

Patches

- According to CERT, many systems are compromised by exploiting known bugs for which patches exist. Simply keeping patches up-to-date, especially on "exposed" machines, will greatly decrease the chance of a break-in. You can get recommended and security patches at: http://sunsolve1.sun.com.

Tools Available

Summary of Tools available to help secure Solaris

Tools to help Secure Solaris

- Fix-modes was created by Casper Dik to adjust the permissions of several files and directories in Solaris, for the purpose of improving security. It is available from ftp://ftp.wins.uva.nl/pub/solaris/fix-modes.tar.gz.
- The Titan toolkit was created by Brad Powell to fix or tighten potential security holes in UNIX (Solaris, Linux and FreeBSD). It's available from http://www.fish.com/titan.

Tools to help Secure Solaris(cont.)

- The Solaris Security Toolkit “Jass” is designed to assist in the development, deployment, and maintenance of secured Solaris Operating Environment systems. Jass is a set of scripts and directories implementing the recommendations of the security-related Sun BluePrints OnLine articles. Documentation is available from http://www.sun.com/blueprints/browsesubject.htm

Tools to help Secure Solaris(cont.)

- **Yassp** stands for “Yet another Solaris Security Package”. It was written by Jean Chouanard. It automates a large majority of the sercurity changes that were detailed in this presentation. You can find it at: http://www.yassp.org

SunScreen

- One of the bigest additions of Solaris 9 is the inclusion of SunScreen, Sun's previously commericial firewall.
- SunScreen is a full-featured firewall. It has an extensive feature set and provides the bulk of the features found in other major firewalls. It is stateful and dynamic, and at its core is a packet-filtering system like Checkpoint Firewall-1.

Solaris Website Resources

- http://www.sun.com/bigadmin/faq/indexSec.html - Sun's Big Admin Security Resources
- **http://www.wins.uva.nl/pub/solaris/solaris2** - The excellent Solaris FAQ
- sunsolve.Sun.COM/pub-cgi/show.pl?target=home - SUN Recommended & Security Patches
- www.sunhelp.org - An excellant Sun Resource
- web.mit.edu/kerberos/www - Kerberos home page

Sun Web Resources(Cont.)

- www.auscert.org.au - Australian Computer Emergency Response Team
- www.cert.org - CERT Coordination Center
- www.cisecurity.com - The Center for Internet Security
- www.fish.com - Dan Farmer's web site with lots of computer security related stuff
- www.ibiblio.org/pub/solaris/sparc - Solaris Package Archive (SUNSite)

Sun Web Resources(Cont.)

- www.infrastructures.org/cfengine - Cfengine
- www.rootprompt.org - Root Prompt -- Nothing but Unix
- www.sabernet.net/papers/Solaris.html - Solaris Security Guide
- www.sans.org - SANS Institute
- www.securityfocus.com - SecurityFocus
- www.solarisguide.com - SolarisGuide.com

Sun Web Resources(Cont.)

- www.sun.com/bigadmin - Sun Large System Administration
- www.sun.com/blueprints - SUN Blueprints
- www.sun.com/security/blueprints - SUN Security Blueprints
- www.sun.com/security/jass - Additional information on the SUN JASS toolkit
- www.sunfreeware.com - Sunfreeware

References

- http://www.itworld.com/Comp/2377/security-faq
- http://www.accs.com/p_and_p/SolSec/index.html
- http://www.sun.com/bigadmin/faq/indexSec.html
- http://www.samag.com/documents/s=7667/sam0213l/0213l.htm
- http://www.samag.com/documents/s=7667/sam0213d/0213d.htm
- http://www.boran.com/security/sp/hardening_solaris_%20resources.txt