

Check Point Software Technologies LTD.

How to Strip Down a Unix OS

Some suggestions to harden the stock Solaris SPARC/x86 OS. Not all things may be applicable to every installation. Use common sense. With a few changes, this is applicable to all Unix machines. No warranty is implied; standard disclaimers apply. :-)

=====

- 1) Keep the system disconnected from the network until all is ready.
 - 2) Install only the core operating system, adding only necessary packages.
-
- _____ 1. Install the latest OS version supported by CheckPoint S/W Tech.
 - _____ 2. Be sure root has a umask setting of 077 or 027 after you have fully configured the system.
 - _____ 3. Be sure root has a safe search path, as in
/usr/bin:/sbin:/usr/sbin
It helps avoid Trojan horses in the current working directory.
 - _____ 4. Generally, examine all "S" files in /etc/rc2.d and /etc/rc3.d. Any files that start unneeded facilities should be renamed (be sure the new names don't start with "S"). Test all boot files changes by rebooting, examining /var/adm/messages, and checking for extraneous processes in ps -elf output.
 - _____ 5. Make sure the to enable the "CONSOLE" line in /etc/default/login. To disable use of ftp by root, add "root" to /etc/ftpusers.
 - _____ 6. Remove /etc/hosts.equiv, /.rhosts, and all of the "r" commands from /etc/inetd.conf Do a kill -HUP of the inetd process.
 - _____ 7. Remove, lock, or comment out unnecessary accounts, including "sys", "uucp", "nuucp", and "listen". The cleanest way to shut them down is to put "NP" in the password field of the /etc/shadow file. Also consider using the noshell program to log attempts to use secured accounts.
 - _____ 8. The file /etc/logindevperm contains configuration information to tell the system the permissions to set on devices associated with login (console, keyboard, etc). Check the values in this file and modify them to give different permissions.
 - _____ 9. No file in /etc needs to be group writeable. Remove group write permission via the command chmod -R g-w /etc
 - _____ 10. By default, if a Solaris machine has more than one network interface, Solaris will route packets between the multiple interfaces. This behavior is controlled by /etc/init.d/inetinit. To turn of routing on a Solaris 2.4 (or lesser) machine, add "nnd -set /dev/ip ip_forwarding 0" at the end of /etc/init.d/inetinit. For Solaris 2.5, simply "touch /etc/notrouter". Be aware that there is a small window of vulnerability during startup when the machine may route, before the routing is turned off.
 - _____ 11. Automounter is controlled by the /etc/auto_* configuration

files. To disable automounter, remove those files, and/or disable the /etc/rc2.d/S74autofs.

- _____ 12. NFS exports are controlled by the /etc/dfs/dfstab file. Remove this file. To disable the NFS server daemon, rename /etc/rc3.d/S15nfs.server. To prevent a machine from being an NFS client, rename /etc/rc2.d/S73nfs.client. When renaming startup files, be sure to name them with a starting letter other than "S".
- _____ 13. Review all the cron jobs by reading the cron file of every system account in /var/spool/cron/crontabs. Consider logging all cron activities by setting "CRONLOG=yes" in /etc/default/cron.
- _____ 14. Machines using a dynamic route-receiving daemon like in.routed and in.rdisc are vulnerable to receiving incorrect routes. These routes can disable some or all connectivity to other networks. When possible, use static routes (routes added via the route commands in startup files, rather than the routing daemons).
- _____ 15. ARP is the protocol used to associate IP and Ethernet addresses. Machines that share a wire (and have no routers between them) know each others ARP addresses. If one machine is replaced with another, the ARP addresses are usually different. By default, Solaris machines dynamically determine ARP addresses. The arp command can be used to statically set ARP table entries and flush all other entries. This facility is best used when there are few, unchanging systems on a network and the machines need to be assured of each other's identities.
- _____ 16. rpcbind is the program that allows rpc callers and rpc service provides to find each other. Unfortunately, standard rpc is insecure. It uses "AUTH_UNIX" authentication, which means it depends on the remote system's IP address and the remote user's UID for identification. Both of these forms of identification can be easily forged or changed. Generally-purpose systems usually need rpc running to keep users happy. Special purpose systems (web servers, ftp servers, mail servers, etc) can usually have rpc disabled. Be sure to test all the facilities that you depend on to be sure they aren't affected if you turn off rpc. To disable rpc, rename /etc/rc2.d/S71RPC.
- _____ 17. /etc/utmp can be set to mode 644 without disrupting any service.
- _____ 18. Many of the setuid and setgid programs on Solaris are used only by root, or by the user or group-id to which they are set. They can have setuid and setgid removed without diminishing user's abilities to get their work done. Consider each of these programs individually as to their use on your system. Should they be run by someone other than root, their owner, or a user (running with that user's UID)?

The command to find all set-uid programs in the system is:

```
# find / -perm -4000 -print
```

```
/usr/bin/tip
```

```
/usr/bin/ct
```

```

/usr/bin/cu                /usr/bin/uuglist
/usr/bin/uuname           /usr/bin/uustat
/usr/lib/exrecover        /usr/bin/uux
/usr/lib/accton           /usr/lib/fs/ufs/ufsrestore
/usr/bin/uucp             /usr/lib/news/inews
/usr/lib/fs/ufs/ufsdump   /usr/lib/uucp/uuxqt
/usr/lib/uucp/uucico       /usr/lib/uucp/remote.unknown
/usr/lib/uucp/uusched     /usr/sbin/allocate

```

Likewise, obtain a list of set-gid files on your system via the command:

```
find / -perm -2000 -print
```

and remove the set-gid bit from appropriate files, including some of these:

```

/usr/bin/mailx            /usr/bin/netstat
/usr/bin/nfsstat         /usr/bin/write
/usr/bin/ipcs            /usr/lib/fs/ufs/ufsdump
/usr/sbin/arp            /usr/sbin/prtconf
/usr/bin/swap            /usr/sbin/sysdef
/usr/sbin/wall           /usr/sbin/dmesg
/usr/openwin/bin/wsinfo  /usr/openwin/bin/ff.core
/usr/kvm/crash           /usr/openwin/bin/mailtool
/usr/openwin/bin/xload   /usr/kvm/eeeprom
/usr/vmsys/bin/chkperm

```

Create a master list of the remaining setuid/setgid programs on your system and check that the list remains static over time.

- _____ 19. Every network on the system should be inspected to determine if the facility that it provides is appropriate for your environment. If not, disable the facility. Some of these facilities are in the system startup files, as discussed earlier. Other are started in /etc/inetd.conf. Comment out the unneeded facilities and kill -HUP the inetd daemon. Some common facilities are:

```

tftp          systat          rexd          ypupdated     netstat
rstatd       rusersd          sprayd        walld         exec
comsat       rquotad          name          uucp

```

For a very secure system, replace the standard inetd.conf with one that just includes telnet and ftp (if you need those facilities).

- _____ 20. in.fingerd has had some security problems in the past. If you want to provide the finger facility, run it as "nobody", not as "root". Or you may wish to modify your /etc/inetd.conf with this entry:

```

#finger stream tcp      nowait  nobody  /usr/sbin/in.fingerd
in.fingerd
finger stream tcp      nowait  nobody  /bin/cat      cat
/etc/drexx-pgp.txt

```

- _____ 21. By default, syslog provides minimal system logging. Modify the /etc/syslog.conf file to have syslog log more information, and separate to where the information is logged by importance. Anything related to security should be sent to a file that gets encrypted. Unfortunately, syslog must be restarted for it to read the new configuration file.
- _____ 22. Set the EEPROM to "security=command" password-protect all EEPROM commands except "boot" and continue". Set the EEPROM's password so no one else can change its modes. Unfortunately, this doesn't truly secure the machine. If someone has physical access to the machine, they can open the machine and replace its EEPROM. Replacing the machine's EEPROM also changes its hostid. Recording all the hostids of your machines and checking this list against the machines occasionally to verify that no EEPROMs have been replaced.
- _____ 23. Under Solaris, there is no way to determine if a machine's network interfaces are in "promiscuous" mode. Promiscuous mode allows the machine to see all network packets, rather than just those packets destined for the machine. This allows the machine to snoop the network and monitor all traffic. An interface should only be in promiscuous mode if the snoop program, or another network monitor program, is being run. If you aren't running such a program, and your machine's interface is in promiscuous mode, then it's likely that a hacker is monitoring your network. The public domain ifstatus command returns a machine's promiscuous state.
- _____ 24. -> Any filesystems listed in /etc/dfs/dfstab will be exported to the world, by default. Include a list of nfs clients (or a netgroup) with the "-o rw" or "-o ro" options.
-> Include the "nosuid" option to disable setuid programs on that mount where applicable
-> Don't run nfs mount through rpcbind - the mount daemon will see the request as being local and allow it. This is the source of known rpcbind vulnerabilities as reported by CERT (section 4). Use the rpcbind replacement (section 3) that does not forward mount requests through.
-> Use secure-RPC if possible. If not, you're using "AUTH_UNIX" authentication, which simply depends on the IP address of the client for identification. Any machine using the IP address of the ones in your access list can gain access to NFS.
-> Disable NFS if possible. NFS traffic flows in clear-text (even when using "AUTH_DES" or "AUTH_KERB" for authentication) so any files transported via NFS are susceptible to snooping.
-> Programs can guess the file handle of the root mount point and get any file from an NFS server, regardless of any access rights. Use fsirand to randomize inode numbers on NFS servers.
- _____ 25. With Solaris 2.x, Sun is shipping a much more modern sendmail. Still, there are new bugs reported monthly. The following can make sendmail be more secure:
- > Consider running the latest version Berkeley sendmail

(ver 8.9.x)

- > Consider using smrsh or the SMTP Security Server of FW-1.
- > Remove "decode" from /etc/aliases
- > Set /etc/aliases permissions to 644
- > Consider using a proxy-based firewall with SMTP filtering to screen out unnecessary SMTP commands.

- _____ 26. NIS is not a secure distributed name service. NIS+ is more secure when configured properly. NIS will give away all the information in its tables if its domain name is guessable. To close this hole, put trusted host/net addresses to /var/yp/securenets. Also consider using secure RPC or NIS+. Finally, don't include root and other system account information in NIS tables.
- _____ 27. Solaris 2.5 ftpd(1M) contains a good set of configuration directions, with the following exceptions:
- > cp /etc/nsswitch.conf ~ftp/etc
 - > Make sure that the filesystem containing ~ftp is not mounted with the "nosuid" option
 - > No files under ~ftp should be owned by "ftp"
 - > More detailed instructions can be found the anonymous ftp directions
- _____ 28. Making X more secure:
- > Use the SUN-DES-1 option to use Secure RPC to pass X authentication/authorization information.
 - > Use xhost +user@host when granting access
- _____ 29. Activating SUN-DES-1 authentication:
- > set DisplayManager*authorize: true
 - > set DisplayManager._0.authName: SUN-DES-1
 - > rm ~/.Xauthority
 - > add access permission for local host via xauth local/unix:0 SUN-DES-1 unix.local@nisdomain and xauth local:0 SUN-DES-1 unix.local@nisdomain
 - > Start X via xinit -- -auth ~/.Xauthority
 - > Add yourself and remove all others via xhost +user@+unix.local@nisdomain -local -localhost
- Now, to give user "foo" permission to access host "node":
- > Give "foo" permission on "node" via xhost +foo@
 - > Create appropriate xauthority for "foo" via xauth add node:0 SUN-DES-1 unix.node@nisdomain
 - > "foo" can now connect to "node": xload -display node:0
- _____ 30. Use showrev -p to list patches installed on the system. Check Sun's patch list for current security-related patches for the version you are running. Download and install all pertinent security patches. Recheck the patch list frequently. Not all security patches need be installed on every machine. But protect machines, or those with public access, should be kept up-to-date.
- _____ 31. inetd can be replaced with
ftp://qiclab.scn.rain.com/pub/security/xinetd* to add logging

facilities.

- _____ 32. ifstatus can determine if your network interfaces are in promiscuous mode.
- _____ 33. xntp is a more secure version of ntp, the network time protocol.
- _____ 34. The most recent (and usually most secure) version of sendmail is always available from Berkeley. Included in the sendmail package is smrsh, the "sendmail restricted shell" which can be used to control any programs invoked by sendmail.
- _____ 35. rpcbind can be used to replace the standard rpcbind on Solaris machines. This version includes tcpwrapper-like functionality and disables access to NFS through rpcbind.
- _____ 36. Unfortunately, passwd+ and npasswd are not yet released on Solaris. They are replacements for passwd that disallow "stupid" passwords from being used on Unix systems. The Crack program can be used to break "guessable" passwords in your /etc/shadow file. It uses a lot of compute cycles, but will generally tell you the passwords of 10% of your accounts the first time it is run.
- _____ 37. wu-ftp is a replacement for the standard ftpd daemon. It provides extensive logging and access control.
- _____ 38. noshell is a program that can be used as the shell on accounts that are never supposed to be logged into. It logs the event (and prevents the login).
- _____ 39. Allow user login only on the console, then su to root. This allows
for better user accountability, specially with multiple admins. In the file /etc/default/login :

CONSOLE=/dev/null
- _____ 40. The standard bind on Solaris has known security problems. bind fixes those problems. Also be sure to get patch1. There are also patches available from Sun to bring your system to 4.9.3. Version 4.9.4pl fixes even more security problems and should be included with Solaris 2.6.
- _____ 41. Your FireWall-1 should not trust any other machines. Remove files:
-> /.rhosts
-> ~/.rhosts
-> /.netrc
-> ~/.netrc
-> /etc/hosts.equiv
- _____ 42. Root's path should not include the current directory specified as '..'. Check files:
-> /.login
-> /.cshrc
-> /.profile

- _____ 43. Remove the "decode" alias in /etc/aliases. The file permissions for /etc/aliases should be 0644 and owned by root.
- _____ 44. The /etc/utmp file should not be world writable:
chmod 644 /etc/utmp
- _____ 45. No accounts other than root should have the user id (UID) of 0
- _____ 46. Allow no user account on the FireWall-1 machine.
-> If you must have user accounts, strictly enforce authentication (using FireWall-1) and password/account expiration.
- _____ 47. There is no need to run sendmail unless your machine need to receive incoming mail.

/etc/rc2.d/S88sendmail stop
mv /etc/rc2.d/S88sendmail /etc/rc2.d/s88sendmail

will stop the existing sendmail process and make sure that sendmail will not be started by 'init'.
- _____ 48. Use program such as tripwire, available from URL http://www.cs.purdue.edu/coast/archive/Archive_Indexing.html to monitor changes to your system and firewall-1 files.
- _____ 49. Comment out all lines in the file /etc/inetd.conf; none of the services in this file is essential to the running for FireWall-1. After you have edited /etc/inetd.conf, make sure that you send a HUP signal to the running 'inetd' process so that it will re-read the /etc/inetd.conf file.

If you are not using firewall-1 ftp/telnet authentication and want to allow telnet/ftp to your firewall-1 (Bad choice), you will need to un-comment out the telnet and ftp lines.
- _____ 50. Your firewall machine should not use NIS, either as client or master. If you already configure your firewall either as a NIS master or client, it is best to simply re-install the OS.

If you must use your firewall as an NIS master, it should not use NIS for password information. Make sure that the line

passwd: files

not

passwd: files nis

is in file '/etc/nsswitch.conf'.

If you must use your firewall as an NIS client, your firewall should bind using a list of servers (see ypinit -c) as opposed to using a broadcast to find a server.
- _____ 51. Your firewall machine should not use NFS, either as client or

master.

If you must use your firewall as an NFS server, it's exported file systems should be restricted to a particular hosts. If possible export your file system as read-only. For example, in file /etc/dfs/dfstab

```
share -F nfs -o ro=trusted_clients /logs
```

If you must use your firewall as an NFS client, always with "nosuid" options. For example:

```
mount -F nfs -o nosuid,bg trustserver:/home /trustserver_home
```

- _____ 52. Use the anti-spoofing feature of FireWall-1 to protect your network from IP spoofing.
- _____ 53. If you allow user to access internal services (telnet, ftp ...) from external hosts, you should know that information are travelled accross the Internet in cleartext (for anyone with some technical expertise to "snoop"). That includes you password and any other confidential data. You can protect your data againts snooping by using the firewall-1 to firewall-1 encryption feature. If encryption is not possible, for telnet and ftp connections, you can insist on using authentication to guard against password "snooping".
- _____ 54. You should allow ONLY authenticated telnet/ftp session TO the FireWall-1 machine.
- If your control station is different from yor inspection station, you will have to allow snmp and FW1 connections from the control station to the inspection station.
- If your firewall-1 uses encryption, you will have to allow snmp and FW1 connections from the encryption peer machine.
- _____ 55. You should allow ONLY a limited set of connections to be initiated from the FireWall-1 machine. In fact, stealthing the FW-1 will be the best thing.
- If your firewall-1 uses encryption, you will have to allow snmp and FW1 connections to the encryption peer machine.
- _____ 56. THE MACHINE SHOULD BE REBOOTED FOR ALL PATCHES TO TAKE AFFECT!!
- _____ 57. Sun security patches are available from <http://sunsolve.sun.com>