Global Information Assurance Certification Paper

Secure Intranet Host Setup Checklist

Author: Joe Callis
GIAC USERID: callis001

GCUX Practical Version 1.6d

August 22, 2001

Secure Intranet Host Setup Checklist

This checklist is to be used by all administrators and operators setting up Solaris 8 hosts that are deemed to be "secure" servers. A secure server is one that will either sit on a screened network, at a client site, or even sit on the intranet, if the machine contains sensitive information. The point of this checklist is to show how to setup a machine so that access is restricted to only those allowed access and to limit the number of potential vulnerabilities. It should be noted here, that security is not a single step, but rather an on-going process. This list may have to be adjusted or modified to take into account new security concerns.

The host to be built is going to reside on the company intranet. The hardware used in this setup is a Sun Netra T1 AC200 with two 18 Gb internal drives. The machine has a 500 MHz processor with 512 Mb of RAM. An internal cdrom drive can be put in the machine for installation only, and then must be removed before putting the system into production. If an internal cdrom drive is not available, an external will need to be used. (This setup assumes that an internal drive is being used.) The only other equipment needed is a RJ-45 cable with a Netra t term connector and of course, the Solaris 8 cd as well as the internal applications cd.

Console Access

Since initial access to the machine will be through console only, that will need to be setup. Netra T1s require a special T-term connector between the RJ-45 cable and the RS-232 port on the switch box (if a switch box is not available, you will need a cross-over cable). This is shipped with the hardware and should be labeled accordingly. Once wiring is completed and the power connected (Note, the machine should NOT be connected to the network at this time), you will need to login to a unix host, pull up a terminal window.

Type: **/usr/local/bin/sudo /usr/local/bin/kermit**, and enter your password. At the kermit prompt, type the following:

____ **set line /dev/ttya** (tells kermit which serial port to use)
____ **set carrier-watch off** (tells kermit not to expect a carrier detect signal)
____ **c** (tells kermit to connect to the remote system)

Since Netra's come with a lights-out management feature, which enables remote power up and power down functionality, the prompt that you will see will be the "lom" prompt:
lom>
At the lom prompt, type in

____ **poweron**

Once the machine is up and you are at the "ok" prompt, the OS installation can begin.

PROM Settings

The decision of whether or not to set an Open boot PROM (obp) password depends on a couple of factors. Is the machine sitting in a potentially hostile environment out of our physical control? One example might be a machine sitting at a client-site. Another example is a machine on our own intranet with enough sensitive information to warrant the added security measure.

A major caveat about setting an obp password; if the password is lost, it cannot be recovered. Sun has to send a replacement PROM chipset in order to recover the box. If a password is to be used, follow all password rules and do NOT use the root password. Assuming that the machine is still at the "ok":

____ **setenv security-mode** *command*
____ **setenv security-password** *password*

It is important to check the auto-boot variable. If the system loses power, or reboots for any reason, you want to make sure it comes back up, otherwise you might be making an office visit at 2am.

____ **setenv auto-boot? true**

Operating System Installation

One of the quirks of the AC200 Netra's, is they need to use Solaris 8 4/01 cd or later. If an earlier release of 8 is required, you will need to get the cds that shipped with the system. For bookkeeping sake, please note the version of Solaris 8 used:

_____

Place the cdrom in the drive and boot:

____ **boot cdrom**

Once the system loads the cdrom, you will be asked several questions. Please use the following in answering the questions:

____ Format /dev/dsk/c1t0d0
____ Swapsize should be 1024 Mb
____ Yes, swap space can begin at the beginning of the disk
____ Yes, erase entire disk

Solaris will now setup the swap space and install a mini-root on the disk. Please note, that if you make a mistake specifying the swap space size and do not realize it until later, you will need to restart from the beginning.

____ Is system networked? The system should not be on the network, but say "yes" anyway. This way we can setup the ip address, etc.
____ DHCP will not be used
____ Enter hostname. Please record here: _____
____ Enter IP address. Please record here: _____
____ Enter netmask. Please record here: _____
____ Do not enable Ipv6.
____ Enter "None" for Name Service
____ Enter default route. Please record here: _____
____ Select timezone from geographic area. Please record here: _____
____ Do not worry about setting the exact time, NTP will adjust it, once the machine is networked.
____ Enter the root password. Please do not write down or email the password

Please confirm the information just entered with the information recorded on the checklist. If any discrepancies are found, please select "**n**" and redo the system configuration section.

Software Installation

The software will be installed from the Solaris 8 Software disks 1 and 2. The system will prompt you for the type of media (select "cd") and will ask you to insert the Software 1 cd into the drive.

____ Select "Custom Install." This will enable us to eliminate several packages that we do not want.
____ Accept the default settings for the regional questions.
____ Toggle "off" the Documentation packages.
____ Under "Solaris Software 2 of 2" toggle "on" the Disksuite 4.2.1 (for mirroring the disks).
____ Toggle "off" the "Solaris Supplemental Software."
____ Select "none" for additional products.

____ Select both 64-bit and 32-bit support.
____ Select the “End User Software Group.”
____ Select the default installation.

File System Layout

For the file system layout, we are limited to seven partitions. One is used for swap (setup earlier) and another is for disksuite (needs to be partition 4), so we are limited to five partitions for our own use. We typically will setup /, /usr, /var, /opt and a hostname partition with the remainder of the disk space. A couple of caveats about setting up the partitions, make /usr large enough so that it can be patched, if and when necessary. Sun’s recommended size of 683 Mb is sufficient, but to allow a bit more breathing room, it can be increased to 800 Mb. Be careful about making /var too small as well. Nothing is more frustrating that having to reformat a drive because /var is not sufficient. It is recommended to make it around 1 Gb.
Since most of our software is placed in the hostname partition, /opt can be minimally sized. Home directories, additional logging and configuration directories will be placed in the hostname partition.
In order to make a single cylinder partition, you will need to setup the entire disk and when done, go into “cylinder”mode and modify partition 5 so that the starting cylinder is one higher.
Please record the final partition setup.

Slice	Mount Point	Size (Mb)
0	_____	_____
1	swap	1024
3	_____	_____
4	metastate db	~6 (1 cylinder)
5	_____	_____
6	_____	_____
7	_____	_____

When finished, select done, confirm the software installation and start the installation.

Patch Cluster Installation

The best way to get the latest patches on the system (which is still not connected to the network) is by downloading them from an internet-connected machine and putting them on an external scsi disk that can be hung off of our secure system. The best way to get the patch cluster and checksums is to go to http://sunsolve.Sun.COM/pub-cgi/show.pl, and download via ftp. While you are on this page, download the README file and checksum data, so that you can confirm that the patches have not been tampered with or corrupted.

While the patches are downloading, it is a good idea to read through the README file, to look for special instructions, dependencies and potential conflicts.

Once the download has completed, run an md5sum on the zipped patch file. Confirm the signature matches that contained in the checksum file.

____ Mount the external disk onto the new Netra.
____ Create a directory in the hostname partition called "patches".
____ Copy the patches into the /hostname/patches directory.
____ Unzip the file: **unzip 8_Recommended.zip**.
____ Install the patch cluster by running the install script.
____ Once the install has completed, reboot.

Setting up / (root filesystem)

Often times administrators have several windows open to different hosts. To alleviate the chances of an admin running "init 6" on the wrong machine, it is recommended creating /.profile with prompt information, as well as information you do not want to rely on getting from the system default profile.

____ **vi /.profile**
____ Enter the following information:

PATH=/usr/bin:/usr/sbin; export PATH
umask 022
stty erase <^v><bkspace>
EDITOR=vi;export EDITOR
PS1="<hostname>*# ";export PS1*
TERM=vt100;export TERM
____ Save and exit.
____ Change mode to 0500 and check to make sure ownership is root:root.
____ **. /.profile** (to source the .profile)

Create a bogus .rhosts file to trip up anyone attempting to create one.

____ **touch /.rhosts**
____ **chmod 000 /.rhosts**
____ **chown root:root .rhosts**

Securing Networking

In order to prevent different types of network-based attacks the following parameters should be added to the end of /etc/init.d/inetinit

____ **ndd –set /dev/tcp tcp_conn_req_max_q0 10240**
____ **ndd –set /dev/arp arp_cleanup_interval 60**
____ **ndd –set /dev/ip ip_ignore_redirect 1**
____ **ndd –set /dev/ip ip_send_redirects 0**
____ **ndd –set /dev/ip ip_ire_arp_interval 60000**
____ **ndd –set /dev/ip ip_forward_directed_broadcasts 0**
____ **ndd –set /dev/ip ip_forward_src_routed 0**
____ **ndd –set /dev/ip ip_forwarding 0**
____ **ndd –set /dev/ip ip_strict_dst_multihoming 1**

Sun announced in early 2001 that the default setting for the TCP initial sequence number generation was not as random as was originally thought and recommended that the setting be changed to RFC 1948 sequence number generation.

____ Edit /etc/default/inetinit
____ Change *TCP_STRONG_ISS* to "*2*"

Eliminating Unwanted Services

Solaris ships with quite a number of services turned on at boot time. Some of these services make life easier (vold, CDE, etc.) but most are not used and some pose a very serious security threat (nfs, nis, rpc, etc.). This section will go through each startup directory and remove the files from the startup sequence. I will give the entire command sequence for the first one, and after that will just name the files that should be changed.

____ **cd /etc/rc3.d**
____ **for i in S15nfs.server S76snmpdx S77dmi<**return>
do<return>
mv $i _$i<return>
done<return>
____ Now do a listing (**/usr/bin/ls**) and it should look like this:

 # ls /etc/rc3.d
_S15nfs.server _S76snmpdx _S77dmi S25mdlogd

This disables nfs.server, snmpdx and dmi from starting at boot up, but allows mdlogd to start up. A more secure method would be to delete the files entirely. Since this system will be an intranet system, we will keep the files around, in case we decide at a later time that we need to enable some of these features.

____ **cd /etc/rc0.d**

____ rename files K07dmi K07snmpdx K10dtlogin K28nfs.server K33audit K35volmgt K36sendmail K36wbem K37power K39lp K39spc K41rpc K52llc2
____ **cd /etc/rcS.d**
____ rename files K07dmi K07snmpdx K10dtlogin K28nfs.server K33audit K35volmgt K36sendmail K36wbem K37power K39lp K39spc K40nscd K41autofs K41ldap.client K41rpc K41slpd K52llc2
____ **cd /etc/rc1.d**
____ rename files K07dmi K07snmpdx K10dtlogin K28nfs.server K33audit K35volmgt K36sendmail K36wbem K37power K39lp K39spc K40nscd K41autofs K41ldap.client K41rpc K41slpd K52llc2
____ **cd /etc/rc2.d**
____ rename files K07dmi K07snmpdx K28nfs.server S40llc2 S71ldap.client S71rpc S72slpd S73cachefs.daemon S73nfs.client S74autofs S76nscd S80lp S80spc S85power S88sendmail S90wbem S92volmgt S99audit S99dtlogin
____ **vi /etc/init.d/inetsvc**
____ Go to the last line, where inetd is started and add a "-t". This will turn on logging for all inetd processes. Save and exit the file.
____ **vi /etc/init.d/sendmail**
____ Look for where sendmail is started. The command should look like "/usr/lib/sendmail –bd –q10m". Remove the "-bd". We have disabled sendmail at startup, but just in case, we need to start it manually, the smtp port will not be opened.

Crontab Modifications

As cron is a good place to hide things, we want to run as few as possible. Solaris 8 comes with three crontab files: root, adm and lp. Root is the only one that is needed.

____ **crontab –r adm**
____ **crontab –r lp**
____ **crontab –e**
____ Remove the entries for nfsfind and gsscred_clean
____ Add an entry for sendmail:
____ **0,10,20,30,40,50 * * * * /usr/lib/sendmail –q**

This last entry will start up sendmail (every 10 minutes), empty the mail queue, and stop sendmail.

Before you get much further it is a good idea to reboot the machine, just to confirm that everything comes up as expected.

Installing TCP Wrappers

TCP Wrappers provides nice functionality, is easy to compile and install. Basically, tcp wrappers will listen on all inetd ports. As connections come in, tcpd (the binary) logs the incoming connection, does a reverse lookup, confirm that it is not a spoofed address and then makes a call to the daemon requested. If the host requesting service is not allowed access, a prompt is never issued to the remote client, thus preventing brute force attacks. Since this machine is going to sit on the intranet, we want to ensure that only certain machines are allowed access. The allowed hosts should not be on NIS/NIS+. This will prevent anyone from logging into the "jump-off" host and subsequently attempting to telnet to the secure host.

Solaris 8 requires a Ipv6 version of 7.6 TCP Wrappers. The version that works with Solaris 8 is available from ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6-ipv6.tar.gz. Because there is not have a compiler (or gzip for that matter), tcp wrappers will need to be compiled on a similar Solaris 8 machine. Once compiled, the binaries and libraries can be put on removable media and transferred to the new host.

____ Download tcp wrappers
____ Check pgp signature with the gzipped tar file
____ **gzip –cd tcp_wrappers_7.6-ipv6.tar.gz |tar xvf –**
____ **cd tcp_wrappers_7.6-ipv6**
____ **vi Makefile**
____ Remove the comment from the line REAL_DAEMON_DIR for Solaris 2.x
____ Remove the comment on the line "IPV6 = -DHAVE_IPV6."
____ Insert "CC=gcc" at the top of the script
____ Change FACILITY to LOG_AUTH
____ Save and exit. Now run the make: **make sunos5**
____ Copy tcpd, tcpdmatch, try-from, libwrap.a,tcpd.h and tcpdchk onto removable media. You can also copy safe_finger, but it will not be used during the course of this setup. Make sure that the files are owned by root. The group should be daemon.
____ Mount the disk onto the secure host
____ Create the appropriate directories: **mkdir –p /hostname/local/sbin /hostname/local/lib /hostname/local/include**
____ Copy the binaries (tcpd, tcpdmatch, try-from and tcpdchk) to/hostname/local/sbin. Change their permissions to 0555.
____ Copy libwrap.a to /hostname/local/lib and tcpd.h to /hostname/local/lib.
____ Create a symbolic link: **ln –s /hostname/local /usr/local**.

Trimming Down inetd.conf

Unfortunately, Solaris has quite a few processes turned on by default in the inetd.conf file. Some of these processes have been the cause of remote root exploits, internal root exploits as well as providing aid to malicious users trying to glean information from a system. The inetd daemon can be turned off entirely, by simply commenting out the last

line in the /etc/init.d/inetsvc script. In the case of this server (it is going to sit on the intranet), we can leave telnet and ftp enabled. All other lines should be deleted.

____ **vi /etc/inet/inetd.conf**
____ Remove all lines, except telnet and ftp
____ Now is tcp wrappers are installed. In place of the /usr/sbin/in.telnetd and /usr/sbin/ftpd, put /usr/local/sbin/tcpd. This will invoke tcpd first, which will make the call to telnetd.
____ Save and exit.
____ kill –HUP the inetd daemon.

Adding Access Control

Now that tcp wrappers have been added and the appropriate lines have been modified in the /etc/inetd.conf file, access control can now be added. The tcp wrappers access control allows for hosts to be allowed or denied access to either specific daemons or all daemons. One caveat about the access control files, the hosts.allow file is checked first. If the host/service is allowed, then no further checking occurs. If there is not a specific rule in place, the deny rule is checked. If there is still not a match, the host is allowed access.

____ **cat ALL:ALL >/etc/host.deny**
____ **cat telnetd:**{enter hostname(s) of allowed host(s)} **>/etc/hosts.allow**
____ **cat ftpd:**{enter hostname(s) of allowed host(s)}**>>/etc/hosts.allow**

Tweaking Logging

As logs are the only way of keeping watch over the system, it is quite important that as much information is logged as possible. One important bit of information that Solaris does not log by default, is failed login attempts. While the average user will mistype a password every once in a while, a consistent pattern of failures points to someone trying to brute force crack an account. TCP Wrappers provides a nice logging feature, but it has to be enabled in /etc/syslog.conf first.

____ **vi /etc/syslog.conf**
____ At the bottom of the file, add *auth.info*<tab over>*/var/log/wrap_log* (NOTE: It is very important that the columns be separated by a tab, not a space.
____ If a logging server is used, *add auth.info*<tab over>*@loghost*
____ **touch /var/log/wrap_log**
____ **touch /var/log/loginlog** (This log file will monitor failed login attempts).
____ Change ownership of the two files to root:sys. The permissions should be 600.
____ **kill –HUP `/usr/bin/cat /etc/syslog.pid`**

Enabling NTP

In thinking about enterprise network and systems security, it is important that all systems be synchronized to the same time. In computer time, a few seconds difference make logs much less useful and effective.
Since the machine is not connected to the network, ntp will not be started yet. However, at the next reboot, ntp will start (the startup script looks for the presence of /etc/ntp.conf as its signal to start).

____ Copy /etc/ntp.client to /etc/ntp.conf
____ Edit /etc/ntp.conf, adding (to the end of the file): **server <IP address>**. Save and exit.

Modifying the /etc/hosts File

Solaris was not told anything about our fully qualified domain name (FQDN) when the OS was installed, so we can add that information, as well as the name of our logging server (if appropriate). In a screened network environment, it would be necessary to put all hosts that our host needs to know about in this file. This host will be using DNS for its name resolution, so this is not necessary.

____ **vi /etc/hosts**
____ Add the FQDN to the line with the IP address and hostname. The format should be: IP address<white space>FQDN<white space>unqualified hostname
____ If a separate logging server is used, add its information here (in the same format), add an unqualified hostname of "loghost" at the end. If a separate logging server is not used, put "loghost" at the end of the "localhost" entry.
____ Save and exit.

Log Rotation

After adding the logs for tcp wrappers and failed logins, the logs need to be configured to rotated on a regular basis. This prevents the files from growing too large and filling up the /var partition. This also makes looking through the files easier.

____ **vi /usr/lib/newsyslog**
____ Copy one of the entries for another log (syslog for instance), paste it twice.
____ Modify each (one for loginlog, the other for wrap_log).
____ The syslog template will keep the log around for 8 weeks. If this is not sufficient (or is too long), modify accordingly.
____ Save and exit.

Passwd/Shadow File

As with many things, Solaris comes with extraneous accounts in the passwd/shadow file. Some of the accounts (nobody4) date back to sunos4.x and are kept around for compatibility issues. One vulnerability announced shortly before the writing of this checklist found that all accounts with a two character password could allow someone to log into a machine with a trivial (or no) password. This vulnerability was using a third-party software, but does highlight the problem with having extra accounts with "NP" as the password.

____ Edit the /etc/passwd file. Make sure that none of the accounts have a real shell (except for root). If a bogus shell is needed, do not use /bin/false, use /dev/null.
____ Save and exit. Run **pwconv**
____ Edit the /etc/shadow file.
____ (in "vi") **:1,$s/:NP:/:*LK*:/** (find/replace replacing all ":NP:" with ":*LK*:")
This does two things, it prevents the vulnerability mentioned above from being effective, but also, it puts an illegal password character in the password field, thereby rendering the account completely useless.
____ Save and exit.

If user accounts are going to exist on the machine, password aging should be used. The minimum and maximum password age can be set in /etc/default/passwd. This value should be set based on current security policy.

____ Edit /etc/default/passwd
____ Set MAXWEEKS=13
____ Set MINWEEKS=2
____ Set WARNWEEKS=1. Save and exit.

It is important to set up certain default login settings, to prevent potential abuse by either malicious or uneducated users. The /etc/default/login file is a good place to do that.

____ Edit /etc/default/login
____ Uncomment TIMEOUT variable
____ Uncomment UMASK variable
____ Add "**umask 022**" to /etc/skel/local.* and /etc/.login and/etc/.profile.

If user accounts need to be created on this machine, those accounts can be created at this time. The safest way to do that is via the useradd command.

____ **mkdir /hostname/home**, change permissions to 0555 and owned by root:root
____ **ln –s /hostname/home /home**
____ **/usr/sbin/useradd –c <***full name***> -u** <*userid #*> **-g <***groupid #*> **-d /home/**<*login*> **-m –s** <*shell*> <*login*>
____ Check the /etc/shadow file, to confirm that password aging parameters were set.

DNS Configuration

For the DNS configuration, no more than three IP addresses of DNS servers (preferably secondary servers) are needed. If the system is sitting on a screened network, this step can be ignored, since the host will probably not be able to talk to local or remote DNS servers.

____ Edit /etc/resolv.conf. The first line needs to be **domain <***domain name***>**. After which the DNS servers can be listed, one per line.
____ Save and exit.
____ **cp /etc/nsswitch.dns /etc/nsswitch.conf**

Banners

A lot of UNIX systems like to advertise themselves through their banners. This is the most common way for malicious users to determine the OS and version of a host they do not have access to. Because of this, it is advisable to replace the OEM banners with ones that basically tell the user nothing. Check with current security policy, so as to ensure that the banners comply with all legal requirements.

____ Edit /etc/default/telnetd
____ Add a line similar to the following:
BANNER="\n\nAuthorized Users only. All system activity is monitored.\n\n\n"
____ Save and exit.
____ Do the same for /etc/default/ftpd.

Kernel-level Changes

Be very careful about making changes to the /etc/system file. Bad/misspelled entries can cause system problems. Kernel level changes are useful for setting the system stack non-executable or for hard-coding network speed and duplexity.
____ Edit /etc/system
____ Add **set noexec_user_stack=1** (to set stack non-executable).
____ Add **set noexec_user_stack_log=1** (to set stack non-executable).

Since an attacker can use a core file as a DOS tool (by filling up disk space), this feature should be nixed as well

____ Add **set sys:coredumpsize=0** (to turn off the systems ability to dump a core file).

These lines set up the network speed and duplexity. Unless networking has a policy in place that states otherwise, always try to have the switch hard-coded to speed and duplexity (as compared to auto negotiated).

____ Add the following lines:
set hme:hme_adv_autoneg_cap = 0
set hme:hme_adv_100fdx_cap = 1
set hme:hme_adv_100hdx_cap = 0
set hme:hme_adv_10fdx_cap = 0
set hme:hme_adv_10hdx_cap = 0

Just to complete the changes we have made up to this point, reboot the system. This will apply our changes, clean out the proc table, etc. and get the system in a stable state, before we start setting up mirroring. Be sure watch during the reboot, so that you can determine if you made any misspellings in the /etc/system file.

____ **/usr/sbin/init 6**

Disk Mirroring

One method of introducing fault tolerance into our system is to mirror the root disk. During the installation, we installed Disksuite 4.2.1 on the system. One patch needs to be added before beginning. Use the url above to download it.

____ Apply patch number 108693-04

Format the second disk and partition it like the first.
____ **prtvtoc /dev/rdsk/c1t0d0s2 | fmthard -s - /dev/rdsk/c1t1d0s2**

Configure the metastate database. (-a= attach, -f=create initial state db, -c=# of replicas/slice)
____ **/usr/sbin/metadb -a -f -c 2 /dev/rdsk/c1t0d0s4 /dev/rdsk/c1t1d0s4**
____ **/usr/sbin/metadb –i** (to confirm creation and proper configuration)

Create one-way concatenations for partitions that are to be mirrored. The concatenations are not created for the backup slice (slice 2) or the metastate db slice (slice 4).

____ **/usr/sbin/metainit -f d0 1 1 c1t0d0s0** (-f=force creation, d0=metadevice name, "1 1" = number of stripes and number of slices/stripe respectively)
____ **/usr/sbin/metainit –f d1 1 1 c1t0d0s1**
____ **/usr/sbin/metainit –f d3 1 1 c1t0d0s3**
____ **/usr/sbin/metainit –f d5 1 1 c1t0d0s5**
____ **/usr/sbin/metainit –f d6 1 1 c1t0d0s6**
____ **/usr/sbin/metainit –f d7 1 1 c1t0d0s7**
____ **/usr/sbin/metainit –f d10 1 1 c1t1d0s0**
____ **/usr/sbin/metainit –f d11 1 1 c1t1d0s1**
____ **/usr/sbin/metainit –f d13 1 1 c1t1d0s3**
____ **/usr/sbin/metainit –f d15 1 1 c1t1d0s5**
____ **/usr/sbin/metainit –f d16 1 1 c1t1d0s6**

____ **/usr/sbin/metainit –f d17 1 1 c1t1d0s7**

Submirrors are created for the root disk only (c1t0d0).

____ **/usr/sbin/metatinit d100 –m d0**
____ **/usr/sbin/metatinit d101 –m d1**
____ **/usr/sbin/metatinit d103 –m d3**
____ **/usr/sbin/metatinit d105 –m d5**
____ **/usr/sbin/metatinit d106 –m d6**
____ **/usr/sbin/metatinit d107 –m d7**
____ Make a backup copy of /etc/vfstab file
____ Modify the /etc/vfstab file, referencing the mirrors. Example:

/dev/md/dsk/d100 /dev/md/rdsk/d100 / ufs 1 no logging

____ Make a backup copy of /etc/system.
____ **/usr/sbin/metaroot d100** (this is only done for the root filesystem (c1t0d0s0)
____ Flush file lock transactions: **lockfs –fa**
____ Confirm sane entries in /etc/system and /etc/vfstab prior to rebooting
____ **init 6**

Now that the partitions are set up for mirroring, the mirrors need to be attached and synced. Do not reboot during the sync period. For an 18 Gb disk with 6 partitions, the mirroring might take as long as 1 hour to complete.

____ **/usr/sbin/metattach d100 d10**
____ **/usr/sbin/metattach d101 d11**
____ **/usr/sbin/metattach d103 d13**
____ **/usr/sbin/metattach d105 d15**
____ **/usr/sbin/metattach d106 d16**
____ **/usr/sbin/metattach d107 d17**

The progress of the sync can be monitored using the /usr/sbin/metastat command.

Physical Security and Wrap-Up

____ After mirrors have completed syncing. Power down the host (**init 5**).
____ Remove the removable media and internal cdrom (if applicable).
____ If a test lab exists, install host in test lab and run nmap, nessus, saint, etc. against the machine. Do NOT run these tools on the production network, **EVER**! Nmap can clog the network or worse, bring down switches, routers and even systems.
____ Observing all data center rules regarding installing machines during production hours, rack mount the machine in secured data center.
____ Ensure that all cables (power, network and console) are in no danger of being pulled out or pinched accidentally (routed through proper cable channels.
____ Once switch is setup, run the appropriate cables and power up the host.

____ Ensure that you can connect to the console and ensure that you can connect from your "jump-off" host. It is a good idea to try connecting from other hosts, just to confirm tcp-wrappers are working and logging properly.
____ Do a time check to ensure that NTP is syncing up properly with the timeserver.
____ Inform the client that the host is ready for production testing.
____ Sign, date and hand carry this form to security for audit and review.

_____
signature date installed

Problems encountered during build and resolution (please be specific):

References

Campione, Jeff. Solaris 8 Installation Checklist. Available from http://www.sans.org/y2k/practical/Jeff_Campione_GCUX.htm, 2000.

Gregory, Peter H. Solaris Security. Upper Saddle River, NJ: Prentice Hall PTR, 2000.

Pomeranz, Hal, ed. *Solaris Security Step by Step*. SANS Conference notes. SANS Institute, 2001.

Pomeranz, Hal, ed. Solaris Security Step by Step: Version 2.0. SANS Institute, 2001.

Solstice DiskSuite 4.2.1 Collection. Available from http://docs.sun.com, 2001.