Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Solaris 2.6 Installation Checklist

This is the administrative checklist for installing Solaris 2.6 as securely as possible on a Sun Ultra 5. The machine will be used as a Sybase database server providing limited shell access to remote users accessing via an internal LAN. Users will not be able to compile software on this machine, but can execute their own shell scripts and SQL statement via isql, all which will be into personal data space. Users will not receive mail on this host, but mail will be relayed to others. The host will be a DNS client, and will otherwise retrieve network services information from local files. Filesystems are local and not exported. User will be able to telnet into this host and ssh will be installed. You will need an external tape drive to copy scripts and other compiled packages.

Please place the date and time in the space provided for each step. This machine should not be on the network until all steps have been completed.

Install OS

From the OK prompt type boot cdrom and you will be asked a few questions.

1. _____ Select USA-English(ASCII only)
2. _____ Hostname: dbserv
3. _____ Networked: Yes
4. _____ IP Address: <IPADDRESS>
5. _____ Name Service: None
6. _____ Part of a subnet: yes
7. _____ Netmask: 255.255.255.0
8. _____ Geographic region: United States and Eastern
9. _____ Date and Time: set to current date and time.
10. _____ Select Initial install.
11. _____ Select core System Support
12. _____ Select Autolayout select /, /opt, /usr,/var
13. _____ Select customize to change sizes of each slice.
14. _____ Set to the following sizes

1	/	256 mb
2	/var	2 gb
3	swap	148 mb
4	/usr	2 gb
5	unassigned	3.5 gb
6	unassigned	400 mb
7	unassigned	200 mb

Slice 5 will be used for a local FS while 6 and 7 will be raw partitions for sybase.

15. _____ Select continue to install OS from cd.

© SANS Institute 2000 - 2002, Author retains full rights.

Add additional Packages

Install 5 additional packages SUNWntpr and SUNWntpu for NTP, SUNWlibm and SUNWlibms for Perl, and SUNWdoc for online man pages.

```
/bin/mkdir /mnt/cdrom
/etc/mount -r -F hsfs /dev/dsk/c0t2d0s0 /mnt/cdrom
cd  /mnt/Solaris_2.6/Product
/usr/sbin/pkgadd -d .  SUNWntpr SUNWntpu SUNWlibm  \
      SUNWlibms SUNWdoc
/bin/cd /
/etc/umount /mnt/cdrom
```

1. _____

Sun Recommended and Security Patch Cluster

1. _____. Download the 2.6_Recommended.zip from sunsolve.sun.com.
2. _____. Download CLUSTER README for 2.6_Recommended.zip
3. _____. Download ftp://sunsolve.sun.com/pub/patches/CHECKSUMS.
4. _____. Run md5sum 2.6Recommended.zip and verify that it matches what is listed in CHECKSUMS.
5. _____. Read CLUSTER README for special instructions.
6. _____. Copy 2.6_Recommended.zip to removable media which is readable by the target machine.
7. _____. Mount the removable media on the target machine.
8. _____. Copy 2.6_Recommended.zip into /local and /bin/cd /local
9. _____. Uncompress 2.6_Recommended.tar.z
10. _____. Tar –xvf 2.6_Recommended.tar
11. _____. Cd to 2.6_Recommended and Execute its install script "./install_cluster".

Some patches will not install; these are for packages which were not installed.

Copy Scripts from Tape into a temporary directory

1. _____. Create temporary directory to put scripts. "Mkdir /tempdir"
2. _____. Cd to /tempdir
3. _____. Tar –xvf /dev/rmt/0

The following scripts will put in /tempdir

CHECK_NET_SETTINGS:

```
echo tcp_conn_req_max_q0
ndd -get /dev/tcp tcp_conn_req_max_q0
echo tcp_ip_abort_cinterval
ndd -get /dev/tcp tcp_ip_abort_cinterval
echo ip_ignore_redirect
ndd -get /dev/ip ip_ignore_redirect
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
echo ip_send_redirects
ndd -get /dev/ip ip_send_redirects
echo ip_ire_flush_interval
ndd -get /dev/ip ip_ire_flush_interval
echo arp_cleanup_interval
ndd -get /dev/arp arp_cleanup_interval
echo ip_forward_src_routed
ndd -get /dev/ip ip_forward_src_routed
echo ip_forward_directed_broadcasts
ndd -get /dev/ip ip_forward_directed_broadcasts
echo ip_forwarding
ndd -get /dev/ip ip_forwarding
echo ip_strict_dst_multihoming
ndd -get /dev/ip ip_strict_dst_multihoming

NET_SETTINGS
ndd -set /dev/tcp tcp_conn_req_max_q0 8096
ndd -set /dev/tcp tcp_ip_abort_cinterval 60000
ndd -set /dev/ip ip_ignore_redirect 1
ndd -set /dev/ip ip_send_redirects 1
ndd -set /dev/ip ip_ire_flush_interval 60000
ndd -set /dev/arp arp_cleanup_interval 60000
ndd -set /dev/ip ip_forward_src_routed 0
ndd -set /dev/ip ip_forward_directed_broadcasts 0
ndd -set /dev/ip ip_forwarding 0
ndd -set /dev/ip ip_strict_dst_multihoming 0


RmRC2.dFiles:
cd /etc/rc2.d
mv S30sysid.net NOS30sysid.net
mv S71sysid.sys NOS71sysid.sys
mv S72autoinstall NOS72autoinstall
mv S71rpc NOS71rpc
mv S76nscd NOS76nscd
mv K60nfs.server NOK60nfs.server
mv S73cachefs.daemon NOS73cachefs.daemon
mv S93cacheos.finish NOS93cacheos.finish
mv S80PRESERVE NOS80PRESERVE
mv S88sendmail NOS88sendmail
mv S73nfs.client NOS73nfs.client
mv S74autofs NOS74autofs
cd /etc/rc3.d
mv S15nfs.server NOS15nfs.server
echo 'umask 022' > /etc/init.d/umask.sh
chmod 744 /etc/init.d/umask.sh
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
for dir in /etc/rc?.d
do
      ln -s ../initd/umask.sh $dir/S00umask.sh
done
```

Stopping Unnecessary Boot Processes

1_____. Cd to /tempdir and Run the RmRC2.dFiles script copied to /tempdir above.

Tightening Networking

1_____. Cat NET_SETTINGS file to /etc/init.d/inetinit.
"cat NET_SETTINGS >> /etc/init.d/inetinit"

TCP_STRONG_ISS sets the TCP initial sequence number generation parameters. Setting the value to 2 enables RFC 1948 sequence number generation, unique per connection ID. This makes it more difficult to hijack a session by predicting TCP sequencing.

2. _____ Set TCP_STRONG_ISS=2 in /etc/default/inetinit.

File System Configuration

1_____. Change the rw option in the last column of the /usr entry to ro.
2_____. Change the rw option in the last column of the /opt entry to nosuid,ro.
3_____. Change the rw option in the last column of the /var entry to nosuid.
4_____. Change the rw option in the last column of the / entry to remount,nosuid.

There are two levels of protection which you want to enforce here. First, you want to prevent trojan horse programs from replacing system binaries in /usr and /opt. So you mount them read-only. Second, you want to prevent set-uid scripts from executing on any of these filesystems. This was not possible because of the need for 2 raw partitions for sybase. We would need another drive to make this possible. You could make it possible by installing another drive for the raw partitions and creating /dev and /devices filesystems on these slices. Mounting a filesystem nosuid also prevents devices from operating, so you need those to be separate filesystems from the root directory in order to mount / nosuid.

© SANS Institute 2000 - 2002, Author retains full rights.

Administrative Accounts

Several of the accounts in /etc/passwd are unneccessary, but to ensure that older programs do not break, you will just effectively disable them. You also should ensure that these accounts cannot use ftp, cron or at.

1. _____ Make /dev/null the default shell for all users other than root or sys in /etc/passwd.
2_____ Make /sbin/sh the default shell for root and sys.
3. _____ Issue /bin/passwd -l <user> for every user in /etc/passwd other than root. This will lock out the accounts. (Replaces "NP" in the shadow file with "*LK*".)
4. _____ Remove crontab entries in /var/spool/cron/crontabs for all users except root and sys.
5. _____ Add adm, lp, uucp and nobody4 to /usr/lib/cron/at.deny.
6. _____ Add adm, lp, uucp and nobody4 to /usr/lib/cron/cron.deny.
7. _____ Create an /etc/ftpusers file containing all users in /etc/passwd.
8. _____ /bin/chown root:root /etc/ftpusers
9. _____ /bin/chmod 600 /etc/ftpusers

Remaining Network Services

Not many. But the host needs to be a DNS client and should reference local files for password and group information. Let IPADDRESS be the IP address of the trusted DNS server, and GATEWAY be the IP address of the default router.

1. _____ IPADDRESS?
2. _____ /bin/touch /etc/resolv.conf
3. _____ /bin/echo 'nameserver <IPADDRESS>' > /etc/resolv.conf
4. _____ /bin/chown root:root /etc/resolv.conf
5. _____ /bin/chmod 644 /etc/resolv.conf
6. _____ Set every entry in /etc/nsswitch.conf to be "files", except "hosts: files dns".
7. _____ GATEWAY?
8. _____ /bin/touch /etc/defaultrouter
9. _____ /bin/echo '<GATEWAY>' > /etc/defaultrouter

Sendmail

We removed the start up script that starts senmail earlier. You should replace Sun's sendmail binary with one built from source. You will need to do this on a separate host

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

which has compilers installed and then move the binaries and libraries over to this machine. From the compiler machine:

1. _____ Download ftp://ftp.sendmail.org/pub/sendmail/sendmail-8.9.3.tar.gz
2. _____ Unpack: gzip -dc sendmail-8.9.3.tar.gz | tar xvf -
3. _____ cd sendmail-8.9.3/BuildTools/OS
4. _____ In the SunOS.5.8 file, change the line define(`confENVDEF', `-DSOLARIS=20800 ') to define(`confENVDEF', `-DSOLARIS=20800 -DUSE_VENDOR_CF_PATH')
5. _____ cd ../../src
6. _____ sh Build
7. _____ cd obj.SunOS.5.8.sun4 and mkdir ./usr/lib and copy the sendmail file to that directory. Set permission of /usr/lib/sendmail to 6551 owned by root:root.
8. _____ mkdir ./etc/mail and copy sendmail.cf into ./etc/mail
9. _____ create sendmail.cf with the following lines

```
include(`../m4/cf.m4')
include(`../ostype/solaris2.m4')
FEATURE(`nullclient',`mailhub')
```

And copy it to ./etc/mail

Now you should move the new sendmail files to the target host:

10. _____ On compiler host tar –cvf /dev/rmt/0 ./usr ./etc
11. _____ On target host tar –xvf /dev/rmt/0

Installing TCP Wrappers

You want to force all remote connections to this machine to be made via SSH and through TCP Wrappers. Once again you will need to build from the source on a separate host which has compilers installed and then move the binaries and libraries over to this machine.
From the other machine:

1. _____ Download ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.tar.gz
2. _____ Unpack: gzip -dc tcp_wrappers_7.6.tar.gz | tar xvf -
3. _____ cd tcp_wrappers_7.6 ; chmod 644 Makefile

4. _____ Edit Makefile by uncommenting the instance of REAL_DAEMON_DIR
which appears after the comment # SysV.4 Solaris 2.x OSF AIX. Also set FACILITY = LOG_AUTH.
5. _____ make sunos5

After TCP Wrappers builds, you can move it from the compiler host to the target host:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1. _____ On the compiler host mkdir ./usr/local/sbin ./usr/local/include ./usr/local/lib, ./usr/man/man3, ./usr/man/man5 and copy safe_finger, tcpd, tcpdchk, tcpdmatch, try-from to ./usr/local/sbin, libwrap.a to ./usr/local/lib.
2. _____ On the Compiler host set each permissions of each file in ./usr/local/sbin to 0555. Make root the owner and daemon the group.
5_____ On the Compiler host set permissions of tcpd.h in ./usr/local/include to 0444 and make root the owner and daemon the group.
6. _____ On the Compiler host set permissions of libwrap.a ./usr/local/lib to 0555 and make root the owner and daemon the group.
3. _____ On the compiler host type tar –cvf /dev/rmt/0 ./usr
4. _____ On the target host cd / and tar –xvf /dev/rmt/0.
5_____ Check Permissions of all files installed.

Installing OpenSSH

Now that TCP Wrappers is built, you can build SSH with TCP Wrappers support. The instructions here show you how to build OpenSSH, which is ported to other Unices from the SSH implementation in OpenBSD. OpenSSH is a little harder to build, but is preferable because it has a strong base of ongoing support, and is capable of communicating with commercial products using the SSH 2.0 protocol and therefore more flexible for your users. As before, you will need to build from the source on a separate host which has compilers installed and then move the binaries and libraries over to this machine. OpenSSH requires Zlib (which you should have added as a package above and which obviously needs to be installed on the compiling machine) and OpenSSL, which you will build here first. From the other machine:

1. _____ Download ftp://ftp.openssl.org/source/openssl-0.9.6.tar.gz
2. _____ Unpack: gzip -dc openssl-0.9.6.tar.gz | tar xvf -
3. _____ cd openssl-0.9.6
4. _____ ./config
5. _____ make && make test
6. _____ make install (You need the libraries in the right place to compile OpenSSH.)
7. _____ Download ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-2.3.0p1.tar.gz
8. _____ Unpack: gzip -dc openssh-2.3.0p1.tar.gz | tar xvf –
9. _____ cd openssh-2.3.0p1
10. _____ /configure --with-ssl-dir=/usr/local/ssl --sysconfdir=/etc/ssh --with-tcp-wrappers --with-ipv4-default
11. _____ make
12. _____ make install

With both OpenSSL and OpenSSH built, you can transfer the files to the target host:

1. _____ On the compiler host cd to / and tar –cvf /dev/rmt/0 ./usr/local/lib/libssl.a ./usr/local/lib/libcrypto.a ./usr/local/include/openssl ./etc/ssh ./usr/local/bin/ssh* ./usr/local/sbin/ssh*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2. _____ On the target host cd / and tar –xvf /dev/rmt/0

Configuring TCP Wrappers
Your users may connect from anywhere, but you must ensure that they only use SSH. You should also be notified when connection attempts are made and rejected. Let ADMIN_EMAIL be the appropriate email address for such messages to go on your site.

1. _____ /bin/touch /etc/hosts.allow
2. _____ /bin/chown root:root /etc/hosts.allow
3. _____ /bin/chmod 600 /etc/hosts.allow
4. _____ /bin/echo 'ssh: ALL' > /etc/hosts.allow
5. _____ /bin/touch /etc/hosts.deny
6. _____ /bin/chown root:root /etc/hosts.deny
7. _____ /bin/chmod 600 /etc/hosts.deny
8. _____ /bin/echo 'ALL: ALL: /usr/bin/mailx -s "%s: connection attempt from %a" <ADMIN_EMAIL>' > /etc/hosts.allow

Configuring SSH

1. _____ Modify /etc/ssh/sshd_config to look like this:

```
Port 22
ListenAddress 0.0.0.0
SyslogFacility AUTH
LogLevel INFO

HostKey /etc/ssh_host_key
ServerKeyBits 1024
KeyRegenerationInterval 900

CheckMail no
UseLogin no
PrintMotd no
KeepAlive no

PermitRootLogin no
IgnoreRhosts yes
RhostsAuthentication no
RhostsRSAAuthentication no
RSAAuthentication yes
PasswordAuthentication yes
PermitEmptyPasswords no
StrictModes yes
UseLogin no
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
LoginGraceTime 180
```

2. _____ /bin/chown root:root /etc/ssh/sshd_config
3. _____ /bin/chmod 600 /etc/ssh/sshd_config
4. _____ Create a startup script /etc/init.d/sshd which looks like this:

```
#!/bin/sh -
#
#
PIDFILE="/etc/sshd.pid"
SSHD=/opt/slocal/sbin/sshd

case $1 in
  start)
test -f $SSHD || exit 0
$SSHD
;;
  stop)
test -f $PIDFILE || exit 0
PID=`cat $PIDFILE`
test "$PID" && kill "$PID"
> $PIDFILE
;;
   *)
echo "Usage /etc/init.d/sshd {start | stop)";;
esac
exit 0
```

5. _____ /bin/chown root:sys /etc/init.d/sshd
6. _____ /bin/chmod 744 /etc/init.d/sshd
7. _____ /bin/ln /etc/init.d/sshd /etc/rc2.d/S75sshd
8. _____ Start SSHD: /etc/init.d/sshd start (Note: this will generate the server key.)

Modify inetd.conf

1. _____ Comment out all line in inetd.conf except for the line with telnetd.
2. _____ **Replace the telnet line with**

```
telnet   stream tcp       nowait root     /usr/sbin/tcpd  in.telnetd
```

You can now control who can telnet in using /etc/hosts.allow and /etc/hosts.deny files. Telnet should be disabled when all users are able to use ssh.

© SANS Institute 2000 - 2002, Author retains full rights.

Configuring NTP

You installed the Solaris NTP package earlier, which created the startup scripts and stored the binaries and configuration file. But you still need to modify that file.

1. _____ Go to the list of public NTP servers at http://www.eeics.udel.edu/~mills/ntp/servers.htm and find three secondary servers and their administrative contact infomation.
2. _____ Contact the administrator for each of these three sites and ask for permission to connect.
3. _____ Once you have permission for three servers, add each server's IP address to /etc/ntp.conf in the form: server IPADDRESS

Modify /etc/system

Make the system stack non-executable and do not allow core files to be created userid and passwords can sometimes be seen in core files. This may cause problems for developers to debug their code with this set. This is not an issue on this system. Also set shminfo_shmmax for sybase.

1. _____ Append to /etc/system: set noexec_user_stack = 1.
2. _____ Append to /etc/system: set noexec_user_stack_log = 1.
3. _____ Append to /etc/system: set sys:coredumpsize = 0
4. _____ Append to /etc/system: set shmsys:shminfo_shmmax = 300000000

Password aging is annoying, but some companies require users to change their password every three months.

1. _____ Set MAXWEEKS=13 in /etc/default/passwd.

Root should not be able to login directly, either remotely or at the console. This forces any legitimate attempt at a root shell to be via su and therefore logged. Actions can be traced back to the original user, or if the original user cannot be found in the log, you will know the action is malicious.

1. _____ Change "CONSOLE=/dev/console" to "CONSOLE=" in /etc/default/login. (Note: the former prevents remote logins as root, the latter will deny root the ability to log in even at the console.)

Set a fairly restrictive umask for all users:

1. _____ Uncomment UMASK=022 in /etc/default/login.
2. _____ Add umask 022 to /etc/profile and /etc/.login.

Create an account for sybase and yourself, so that you can login at the next reboot:

1. _____ /bin/touch /home/<username>
2. _____ /usr/sbin/groupadd -g <gid> <group>

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3. _____ /usr/sbin/useradd -u <uid> -g <gid> -d <home dir> -s <default shell> -c <full name> <loginid>
4. _____ /bin/passwd <loginid>
5. _____ give ownership of to the raw devices /dev/rdsk/c0t0d0s6 and /dev/rdsk/c0t0d0s7.
6. _____ Create the local filesystem. Newfs /dev/rdsk/c0t0d0s6
7. _____ Mount the file system mount /dev/dsk/c0t0d0s6 /local
8. _____ Create directory /local/sybase
9. _____ Add line to /etc/vfstab for /local with nosetuid option.

Install Sybase

You will need to install the sybase binaries on a machine with openwin installed and tar the $SYBASE directory to tape

1. _____ On source host cd $SYABSE and tar –cvf /dev/rmt/0 ./*
2. _____ On target host cd $SYBASE and tar –xvf /dev/rmt/0
3. _____ On target host cd $SYABSE/bin/srvbuildres –r my.rs. Using the resource file will not require a GUI which would not run on this machine.

   my.rs should contain:
   sybinit.release_directory: /local/sybase
   sybinit.product: sqlsrv
   sqlsrv.server_name: dbserv_db
   sqlsrv.new_config: yes
   sqlsrv.do_add_server: yes
   sqlsrv.network_protocol_list: tcp
   sqlsrv.network_hostname_list: dbserv
   sqlsrv.network_port_list: 4100
   sqlsrv.master_device_physical_name: /dev/rdsk/c0t0dos7
   sqlsrv.master_device_size: 200
   sqlsrv.master_database_size: 150
   sqlsrv.errorlog: USE_DEFAULT
   sqlsrv.do_upgrade: no
   sqlsrv.sybsystemprocs_device_physical_name: /local/sybase/data/sysprocsdev.dat
   sqlsrv.sybsystemprocs_device_size: 200
   sqlsrv.sybsystemprocs_database_size: 150
   sqlsrv.sybsystemdb_device_physical_name: /local/sybase/data/tempdb.dat
   sqlsrv.sybsystemdb_device_size: 50
   sqlsrv.sybsystemdb_database_size: 45
   sqlsrv.default_backup_server: dbservBAK_db

4. _____ Create Sybase startup file in /etc/init.d and create link in rc3.d.

Also, the message in /etc/motd, /etc/issue, and /etc/default/telnetd “BANNER” needs to warn users that unauthorized activity is prohibited, that access may be logged, that users on the system consent to logging, and possibly that logs might be turned over to law

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

enforcement if criminal activity is found. The wording and the rules themselves must be exact and carefully chosen. You will need to warn those who access your system, but that warning must be precise. Get it approved by your legal counsel and policy makers before you apply it.

1. _____ /etc/motd and /etc/issue approved by legal.
2. _____ /etc/motd and /etc/issue installed on the system.
5. _____ Banner in /etc/default/telnetd.

Other Things to do

You may want to write some scripts to run from cron that will monitor sulog for su to root and loginlog for failed logins. The script should forward all event to another system via ssh to will alert an operator or possibly page the person on call.
Failed login attempts will be logged to /var/adm/loginlog if the file exists.
1._____ touch /var/adm/loginlog
2._____ chown root:sys /var/adm/loginlog
3._____ chmod 600 /var/adm/loginlog

Physical Security

If a machine is not physically secure, it is not secure. Anyone who has access to the hardware can bring down the system or manipulate the disk.
1. _____ The system should be installed in a climate controlled data center environment.
2. _____ The data center should not be accessable to unauthorized personnel.
3. _____ The data center should have card swipes and cameras installed to monitor and record all actions inside.
4. . _____ The persons who are authorized to access this machine must be trained and trusted.

Have a supervisor sign here to testify that he or she has checked the qualifications and backgrounds of all authorized persons:

Printed Name:_____
Signature:_____
Date:_____

Testing

Bring the machine online and test connectivity and for the desired results from the restrictions you imposed. If any test fails, bring the machine offline immediately and repair.

1.___ Cannot boot from CD-ROM without obp_password.
2.___ Cannot write to /usr or /opt.
3.___ Cannot execute set-uid scripts from /opt or /var.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

4.___ Cannot execute sys-unconfig.
5.___ Cannot mount NFS volumes.
6.___ Cannot export NFS volumes.
7.___ Can SSH out to another machine.
8.___ Can SSH into this machine.
9.___ Ensure that you cannot rlogin/rsh/ftp into this machine.
10.___ Cannot login as root via SSH.
11.___ Cannot login as root to the console.
12.___ Correct /etc/motd appears at login.
13.____ /etc/default/telnetd with the correct BANNER
14.___ RPC processes are not running.
15.___ NFS/autofs/cachefs are not running.
16.___ Run nmap and nessus against the new host.

Backup

The system should now be fairly secure. With the OS disk in this wonderful pristine state, back it up.

```
for FS in `mount |grep /dev/dsk |awk '{print $1}'`
do
      echo Backing up $FS
      # do level 0 ufsdump
      /usr/sbin/ufsdump 0uf /dev/rmt/0 $FS
done
```

Verify the images on the tape

```
ERROR=0
mt -f /dev/rmt/0 rew
while [ $ERROR -eq 0 ]
do
        FILENUM=`mt -f /dev/rmt/0 status |grep file |awk '{print $3}' `
        echo "\nFile: `expr ${FILENUM} + 1` "
        echo "quit\c"|ufsrestore -ivf /dev/rmt/0 2>/dev/null |grep "ump"
        ERROR=$?
done
echo "EOM"
mt -f $TAPE rewoffl
```

Restore Backup

Replace system disk with new disk and restore backup to it.
Boot to cdrom and format disk with the same patitions as the same as original.

1. _____ cd / and ufsresore –s 1
2. _____ cd /var and ufsresore –s 2
3. _____ cd /usr and ufsresore –s 3

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

4. _____ cd /local and ufsresore –s 4
Reboot the system.

Boot system and make sure sybase starts up. Run the same test as before.

Printed Name:_____

Signature:_____
Date:_____

© SANS Institute 2000 - 2002, Author retains full rights.