Global Information Assurance Certification Paper

Securing Unix
GCUX Practical Assignment
Version 2.2

Securing HP-UX 11i (11.11) For Use as an IDS/9000 Server

Written by: Leslie Ryan

1 Purpose of This Document

The purpose of this document is to show a systems administrator how to securely setup HP-UX 11.11. While the purpose of the server in my example is to run HP's free intrusion detection product, IDS/9000, the steps taken to secure the operating system are applicable regardless of your system's purpose. The HP-UX operating system is not secure "out of the box"; therefore it is necessary to harden any system using HP-UX. (It should be noted that no operating system is secure when using the default installation.) This paper will also show you step-by-step instructions on how to install and configure IDS/9000 to monitor Wu-FTP servers on the Internet, and how to monitor the IDS/9000 management server itself.

The IDS/9000 product is a good solution to use to monitor HP-UX servers. It actively monitors the systems, can interface with several programs that can alert you in a number of ways, and it's free. It has been developed and tested by HP and I have found that not only is it easy to configure, but it can be modified to specific needs, and it works well.

Conventions in this Paper
A command line will be indicated by the pound sign (#).
Changes to scripts will be indicated in RED.
User input will also be indicated in RED.

2 Description of the System

The purpose of this system is to serve as a monitoring server for several Wu-FTP servers that are connected to the Internet using IDS/9000. The FTP servers will have a directory that will hold software and documentation available for download to the public. This server will also use IDS/9000 to monitor itself.

2.1 Hardware

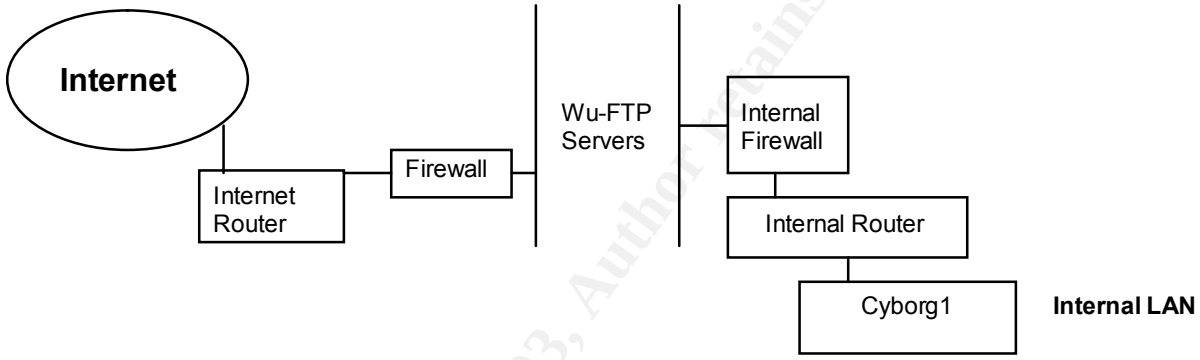
A180c HP-UX Server
166Mhz Risc Processor
2 - 4.5 GB Hard Drives
12x CD-ROM Drive
HP Surestore 4mm SCSI Tape Drive
HP PCI 10/100 Base-T Network Adapter

2.2 Infrastructure

Cyborg1 – IDS/9000 Management Server
CyFTP1 – Wu-FTP Server #1
CyFTP2 – Wu-FTP Server #2

Cyborg1 is on the internal network of an open systems development team. (They develop software and utilities that enable systems administrators to maintain secure systems and stem the tide of evil in cyberspace.) There is a firewall between it and the Wu-FTP servers that connect to the Internet.

CyFTP1, CyFTP2, etc., are on in a separate network segment that has a firewall between them and the Internet, and also a firewall between them and the internal network (Where Cyborg1 resides.) Having an Internet router/firewall between the Internet and the Wu-FTP network segment will provide added protection and will only allow traffic to port 21 (the FTP port). Allowing unnecessary access to ports just gives more opportunities to attackers. Having an internal firewall/router between the Wu-FTP network segment and the internal network will give added protection to the internal LAN in the event a malicious hacker gains access to the Wu-FTP segment. The internal firewall is configured to prevent unwanted traffic into the internal LAN.



2.3 Risk Analysis

A malicious hacker could have a multitude of different reasons for attacking a particular server. One major reason to hack Cyborg1 would be to cover up attacks on the HP-UX hosts it monitors. An attacker could try to modify or delete log files, disable the alert function in IDS/9000, or use Denial of Service attacks to make the server unstable. The biggest risks for this machine include unauthorized access and misconfigured services. To reduce the risk of misconfigured services I will eliminate unnecessary services, and securely configure necessary services. I also will enable auditing on the system so that any changes to the configuration will be tracked. To reduce the risk of unauthorized access, I will eliminate unnecessary users and implement measures to secure necessary users, which include but are not limited to, user monitoring with IDS/9000, limiting who can su to root, using strong passwords, and implementing account policies.

The services that I will need to protect on Cyborg1 are Sendmail and Secure Shell version 2. These utilize ports 25 and 21 respectively. The IDS/9000 server has a service that runs for the agent and for the admin piece. These ports are 2984 and 2985. While Cyborg1 is not meant to be accessible to the internet, if an attacker manages to do a port scan of the internal LAN both of these would show up as open. A successful buffer overflow attack on these ports could lead to root access. Another possibility is a Denial of Service (DoS) attack. This can occur against both the daemons running on Cyborg1

and the network itself. This would render the server useless and would offer a prime time to attack the servers it monitors. A good configuration for our Internet router and firewall will help minimize external attacks.

.
A recent study by the FBI and the Computer Security Institute shows that 60% of attacks originate internally. The motivation for such attacks can range from a disgruntled employee to a consultant trying to gain information about the company. The vulnerabilities from internal attacks on Cyborg1 include exploiting SSH vulnerabilities, password cracking, and unauthorized access to the data center. I will be using SSHv2 to avoid known problems with SSHv1, and I will not configure backwards compatibility in SSHv2 for clients requesting a connection using SSHv1. The accounts on Cyborg1 will be required to change passwords every 60 days, will require 8 characters with at least one number, and only certain users will be allowed to su to root with root not being able to directly log in. I also will enable auditing on the system so that any changes to the configuration will be tracked. The data center is equipped with secured doors that require an assigned key-card to enter. This will facilitate the tracking of any access to the room.

The Wu-FTP servers Cyborg will be monitoring will be especially vulnerable since they will be available on the Internet. A malicious attacker could attempt to break into these machines and upload their own files for public distribution. Those uploads could be illegal in nature, making us an unwilling accomplice in an attacker's crimes. Also, if the Wu-FTP servers are compromised, they could be used as a segue into the internal LAN. This makes it necessary to use Cyborg1 as an IDS server to watch over them.

3 Step-by-Step Guide

3.1 Installing HP-UX

- Insure the server is not connected to the network. This will prevent any tampering via the network until the system is hardened.
- Insert HP-UX 11i core os CD 1 in the CD-ROM drive and boot up the server.
- The Main Menu will appear. Type in SEA to search for all of the boot paths.
- Find the CD-ROM drive and enter: BO P2 (P2 on this machine is the CD-ROM Drive.)
- You will be prompted to interact with IPL, enter N for no:

```
# Interact with IPL? N
```

The following sections deal with the installation options for HP-UX. Use the Tab key and Tab + Shift to navigate the menu items. When the option you want is highlighted, hit Enter to make the selection. It is also possible to type the underlined letter of an option as a shortcut. I will highlight the recommended option(s) in gray.

First you will see a screen titled “Welcome to the HP-UX Installation/Recovery Process” with the following options:

[Install HP-UX]
[Run a Recovery Shell]
[Advanced Options]

At the User Interface Media Options Screen, choose:

Source Location Options:
[*] Media only installation
[ ] Media with Network enabled (allows use of SD depots)
[ ] Ignite-UX server based installation

User Interface Options:
[ ] Guided Installation (recommended for basic installs)
[*] Advanced Installation (recommended for disk and filesystem management)
[ ] No user interface – use all the defaults and go

Tab to [OK] and hit Enter

The /opt/ignite/bin/tool screen has different sections that can be navigated by using the Tab key and Shift+Tab. As with all of the screens in setup, there are underlined shortcut keys that can be used to navigate to each section. The sections on this screen include Basic, Software, System, File System and Advanced. We will only be using the Basic, Software, and File System sections.

Software

/opt/ignite/bin/itool ()			
Category	Marked?	Product	Description
All	No	100BASEt-00	EISA 100BaseT;Suppt
OrderedApps	No	100BASEt-01	EISA 100BaseT;Suppt
HPUXAdditions	No	ATM-00	PCI ATM;Supptd HW=A
Uncategorized	No	ATM-01	HSC ATM;Supptd HW=J
	Yes	BUNDLE11I	Required Patch Bun
[Show Summary…]		[Reset Configuration]	
[Go!]	[Cancel]		[Help]

The only additional software I am going to mark right now will be Ignite-UX 11-11.

File System

/opt/ignite/bin/itool ()				
Mount Dir	Usage	Size	% Used	Group
/stand	HFS	300	7	vg00
primary	SWAP+D	1024	0	vg00
/	VxFS	200	32	vg00
/tmp	VxFS	200	0	vg00
/home	VxFS	**500**	0	vg00
/opt	VxFS	**1800**	69	vg00
/usr	VxFS	948	13	vg00
/var	VxFS	**1524**	13	vg00
[Show Summary…]			[Reset Configuration]	
[Go!]		[Cancel]		[Help]

I have increased the size of /home to 500MB to give the users some more space in their home directories, increased /opt to 1800 MB due to the additional software I will be installing such as IDS/9000, and I increased /var to 1500 MB to store some patches. My changes are indicated in RED.

Basic

/opt/ignite/bin/itool ()				
Configurations [HP-UX B.11.11 Default →]		[Description…]		
Environments: [HP-UX 11I OE-32bit →]		(HP-UX B.11.11)		
[Root Disk…] SEAGATE ST93173N, 8/16/5.6.0, 8678 MB				
File System: [Logical Volume Manager (LVM) with VxFS →]				
[Root Swap (MB…)] 1024 Physical Memory (RAM) = 512 MB				
[Languages…] English	[Keyboards…]	[Additional…]		
[Show Summary…]			[Reset Configuration]	
[Go!]		[Cancel]		[Help]

For this machine I will be using an internal disk for installing the kernel. I will use the second internal disk to mirror vg00 for fault tolerance. You may choose either the 32-bit or 64-bit versions of the operating environment based upon your individual need. I am able to use 1024 MB for the Root Swap since this machine has only 512 MB of RAM. If your machine has more RAM, you will need to determine how much disk space you can dedicate to swap. The more swap you have, the more information you will be able to obtain after a core dump. You may also choose to set other options under "Additional". Choose "Go" to proceed.

itool Confirmation
All data will be destroyed on the following disks:
Address of disk you have chosen
The results of the pre-install analysis are:
If you are overwriting a disk with a previous installation, it will warn you that it contains a file system and boot area.

```
[ Go! ]                    [ Cancel ]                    [ Help ]
```

The system will then begin to create vg00 and install the operating system. (This will take several minutes.)

USER INTERACTION REQUIRED:
To complete the installation you must now insert the "B3920 11I Operating Environment: Disk 2" CD
Once this is done, press the <Return> key to continue:

The system will continue installing the HP-UX 11i operating system. (This will take several more minutes.)

Once all software is installed from the Core OS CD's, the system will reboot and prompt you to hit <Enter> if you would like to stop the boot process. Do not hit <Enter> but allow the system to continue to boot. You will get the following prompts with the recommended response:

```
# Are you ready to link this system to a network?
Press [y] for yes or [n] for no, then press [Enter] n
```
Hit <Enter>

```
# Do you wish to continue (answering no will HALT the system) ?
Press [y] for yes or [n] for no, then press [Enter] y
```
Hit <Enter>

```
# Enter the system name, then press [Enter]. Just pressing [Enter]
will keep the (not recommended) name "unknown": CYBORG1 (or your host
name)
```
Hit <Enter>

```
# You have chosen CYBORG1 as the name for this system.
Is this correct?
Press [y] for yes or [n] for no, then press [Enter] y
```
Hit <Enter>

Note: *The next three screens ask for the country, time zone, and system time. These sections are self-explanatory and will not be outlined in this paper.*

```
# This section enables you to set the "root" password for the
system. Do you want to set the root password at this time?
Press [y] for yes or [n] for no, then press [Enter] y
```
Hit <Enter>

Note*: You should use a strong password for the root account. You should include both uppercase and lowercase letters, and at least one number. It should not be a common word or name as these can be cracked using a password crack program. Use at least eight characters.*

```
# New Password: <a good admin never reveals this>
# Re-enter New Password: <a good admin never reveals this even when
threatened!>
```

If your password is accepted, the system will advise you of the total amount of unallocated disk space. After the system has finished starting up you can configure this space using the Logical Volume Manager commands or SAM (not recommended.)

Hit <Enter>

The system will verify that you have configured a standalone system and the host name you chose, and will complete the boot process and allow you to login as "root".

Hit <Enter>

Once you have logged in as root, the system may give you the following error:

```
INIT: Command is respawning too rapidly.
Will try again in 5 minutes.
Check for possible errors.
id:samd "/usr/sam/lbin/samd  # system mgmt daemon"
```

This error is being generated because the system was installed as a standalone, without configuring the network card or network settings. The SAM daemon (samd) is not able to resolve the hostname and network configuration.

The error can be stopped by commenting out the "`samd`" line in the /etc/inittab file until the lan/networking information is configured.

```
# ups::respawn:rtprio 0 /usr/lbin/ups_mond -f /etc/ups_conf
# samd:23456:respawn:/usr/sam/lbin/samd  # system mgmt daemon
ems1::bootwait:/sbin/rm -f /etc/opt/resmon/persistence/runlevel4_flag
ems2::bootwait:/sbin/cat /etc/opt/resmon/persistence/reboot_flag
ems3:3456:wait:/usr/bin/touch \
/etc/opt/resmon/persistence/runlevel4_flag
ems4:3456:respawn:/etc/opt/resmon/lbin/p_client
```

Note: Modified line is in RED.

The `init q` command must be issued for the changes to the /etc/inittab file to be re-read and to take effect.

3.2 Installing Additional Software

`

At this point you can begin installing additional software. I will install the following:

- OnlineJFS (Codeword needed)
- MirrorDisk/UX (Codeword needed)
- C Compiler (needed for IDS/9000 software and will be removed after installation.)
- Ignite-UX
- Diagnostic Tools
- Java SDK (needed for IDS/9000)
- Perl 5.6.1 (needed for Security Patch Check later)

Some of the above software requires a license and codeword from HP to install. These will need to be purchased from HP. The remaining software is included on the HP-UX application disks and they do not require a codeword.

We will use the swinstall utility to install the additional software. I will first bring up the swinstall GUI and then highlight the software I want to install:

```
# swinstall
```

The GUI interface will appear. You can use the Tab key to navigate to the menu bar or software list. To choose a software package use the space bar to highlight it and mark it for install. You can use the Tab and arrow keys to highlight the menu bar choices or the underlined shortcut keys.

Tab to the software display are and use the spacebar to highlight and mark the software packages listed above.

Once all of the software packages are marked for install, tab to the menu bar and choose **Actions → Install**

Swinstall will bring up a dialog box and will analyze the packages to be installed to ensure there is enough disk space available and to check for dependencies. Once the analyzation is done, use the Tab key to navigate to "Log File" and hit Enter.

Review the log file for any errors or warnings; you should see a message at the bottom that says "No errors or warnings". Tab to "OK" and hit Enter, this will take you back to the install dialog box.

Tab to "Install" and hit Enter; swinstall will now install the marked software that passed analysis.

Once the install finishes you must Tab to "Log File" and hit enter to review the log file. You should see this message at the bottom of the log file:

```
* Summary of Execution Phase:
        * 8 of 8 filesets had no Errors or Warnings.
        * The Execution Phase succeeded.
```

Tab to “OK” and hit enter. Hit “OK” again, then Tab to the menu bar and choose **File** → **Exit**.

The software is now installed.

3.2.1 Patching the Operating System

We will need to install the General Release Patch Bundle:

```
# swinstall -s hpovnnm1:/SD_CDROM/XSWGR1100 -x patch_match_target=true
-x autoreboot=true
```

Also install the Critical Release Patch Bundle:

```
swinstall -s hpovnnm1:/SD_CDROM/XSWHWCR1100 -x patch_match_target=true
-x autoreboot=true
```

Check the patch install with the following command:

```
# swlist -l fileset
```

3.3 Additional Configurations

3.3.1 Volume Group Creation

I am going to create a special volume group that I will use for two IDS/9000 logical volumes later. It will need to be 200MB. To create this I will take the following steps:

```
# cd /dev
# mkdir vgsecurity
# cd vgsecurity
# mknod group c 64 0x020000
# vgcreate /dev/vgsecurity
```

Now I will see if the volume group was created:

```
# vgdisplay vgsecurity

--- Volume groups ---
VG Name                     /dev/vgsecurity
VG Write Access             read/write
```

```
VG Status                     available
Max LV                          255
Cur LV                            0
Open LV                           0
Max PV                           16
Cur PV                            1
Act PV                            1
Max PE per PV                  2500
VGDA                              4
PE Size (Mbytes)                  4
Total PE                         50
Alloc PE                         50
Free PE                          50
Total PVG                         0
```

3.3.2 Network Configuration

- Edit the /etc/rc.config.d/netconf file and configure the IP address and Gateway for the network card. I will enter the following information for Cyborg1's network:

```
HOSTNAME="cyborg1"
OPERATING_SYSTEM=HP-UX
LOOPBACK_ADDRESS=127.0.0.1

INTERFACE_NAME[0]="lan0"
IP_ADDRESS[0]="10.1.1.50"
SUBNET_MASK[0]="255.255.255.0"
BROADCAST_ADDRESS[0]=""
INTERFACE_STATE[0]=""
DHCP_ENABLE[0]=0

ROUTE_DESTINATION[0]="default"
ROUTE_MASK[0]=""
ROUTE_GATEWAY[0]="10.1.1.1"
ROUTE_COUNT[0]="1"
ROUTE_ARGS[0]=""
```

- Save your changes and then run netstat –rn to see the gateways configured for each IP address.

- You also will have to uncomment the samd line in /etc/inittab we commented out earlier. I realize it seems like we just disabled this, but the error is extremely annoying and can print on the screen even when you're using vi.

```
# ups::respawn:rtprio 0 /usr/lbin/ups_mond -f /etc/ups_conf
samd:23456:respawn:/usr/sam/lbin/samd  # system mgmt daemon
ems1::bootwait:/sbin/rm -f /etc/opt/resmon/persistence/runlevel4_flag
```

```
ems2::bootwait:/sbin/cat /etc/opt/resmon/persistence/reboot_flag
ems3:3456:wait:/usr/bin/touch \
/etc/opt/resmon/persistence/runlevel4_flag
ems4:3456:respawn:/etc/opt/resmon/lbin/p_client
```

Note: Modified line is in RED.

- Once again, you have to issue the `init q` command for the above changes to take effect.

3.4 Hardening the Operating System

3.4.1 Services

Turn off any services that are not needed in /etc/inetd.conf. Many of these services can be used for Denial Of Service attacks.

To see what services are currently running issue the command:

```
# netstat -af inet
```

It will look something like this:

```
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp        0      0  *.dtspc                *.*                    LISTEN
tcp        0      0  *.discard              *.*                    LISTEN
tcp        0      0  *.echo                 *.*                    LISTEN
tcp        0      0  *.chargen              *.*                    LISTEN
tcp        0      0  *.kshell               *.*                    LISTEN
tcp        0      0  *.klogin               *.*                    LISTEN
tcp        0      0  *.diagmond             *.*                    LISTEN
tcp        0      0  *.49181                *.*                    LISTEN
tcp        0      0  *.49183                *.*                    LISTEN
tcp        0      0  *.49189                *.*                    LISTEN
tcp        0      0  *.exec                 *.*                    LISTEN
tcp        0      0  *.ident                *.*                    LISTEN
tcp        0      0  *.printer              *.*                    LISTEN
tcp        0      0  *.daytime              *.*                    LISTEN
tcp        0      0  *.time                 *.*                    LISTEN
tcp        0      0  *.telnet               *.*                    LISTEN
tcp        0      0  *.ftp                  *.*                    LISTEN
tcp        0      0  CYBORG1.22             main_pc.1345           ESTABLISHED
tcp        0      0  *.shell                *.*                    LISTEN
tcp        0      0  *.login                *.*                    LISTEN
tcp        0      0  *.49159                *.*                    LISTEN
tcp        0      0  *.time                 *.*                    LISTEN
tcp        0      0  *.telnet               *.*                    LISTEN
tcp        0      0  *.ftp                  *.*                    LISTEN
tcp        0      0  CYBORG1.22             main_pc.1345           ESTABLISHED
tcp        0      0  *.shell                *.*                    LISTEN
```

```
tcp        0      0  *.login                *.*                    LISTEN
tcp        0      0  *.49159                *.*                    LISTEN
tcp        0      0  *.22                   *.*                    LISTEN
tcp        0      0  *.http                 *.*                    LISTEN
tcp        0      0  *.2121                 *.*                    LISTEN
udp        0      0  *.*                    *.*
udp        0      0  *.chargen              *.*
udp        0      0  *.instl_bootc          *.*
udp        0      0  *.2121                 *.*
udp        0      0  *.syslog               *.*
udp        0      0  *.1710                 *.*
udp        0      0  *.bootpc               *.*
udp        0      0  *.echo                 *.*
udp        0      0  *.discard              *.*
udp        0      0  *.tftp                 *.*
udp        0      0  *.177                  *.*
udp        0      0  *.daytime              *.*
udp        0      0  *.ntalk                *.*
```

This gives you an idea of how many services startup by default. Many of these aren't necessary and their presence pose ample opportunity for exploitation. If you read through the purposes for the daemons I am disabling, you will see how many of them create the risk for a port to be flooded with traffic. Here is a list of the services I am going to disable by putting # at the beginning of the service in /etc/inetd.conf. Be sure to comment out **both** UDP and FTP services:

Service	Description
ftp	File transfer protocol. Could be hacked and used to obtain files.
telnet	Insecure way to connect to the server. Turn this off **after** installing SSHv2.
tftp	Trivial file transfer protocol. This is connectionless and quite insecure.
login	rlogind – totally insecure. We'll be using SSHv2.
shell	remshd – insecure. Will be replaced by SSHv2
exec	rexecd – insecure. Will be replaced by SSHv2
ntalk	A tool used to talk to other users. Not necessary.
ident	TCP authentication protocol server.
daytime	Used in testing. Will send the date in a datagram in ASCII format. Don't need it.
time	rdate daemon. Not necessary.
echo	A debugging tool that uses port 7 to send datagrams back to the original source.
discard	Another unneeded debugging tool. Sends data using port 9.
chargen	Character generator. Used to find the cause of dropped packets.
printer	Remote print spooler. Don't need it.
kshell	Kerberos remshd
klogin	Kerberos rlogind

To get the system to reread the inetd.conf file issue the following command:

```
# inetd -c
```

Let's see what services are running now:

```
# netstat -af inet

Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp        0      0  *.registrar            *.*                    LISTEN
tcp        0      0  *.dtspc                *.*                    LISTEN
tcp        0      0  *.diagmond             *.*                    LISTEN
tcp        0      0  *.49181                *.*                    LISTEN
tcp        0      0  *.49183                *.*                    LISTEN
tcp        0      0  *.49189                *.*                    LISTEN
tcp        0      0  *.49255                *.*                    LISTEN
tcp        0      0  CYBORG1.22             main_pc.1345           ESTABLISHED
tcp        0      0  *.49159                *.*                    LISTEN
tcp        0      0  *.22                   *.*                    LISTEN
tcp        0      0  *.http                 *.*                    LISTEN
tcp        0      0  *.2121                 *.*                    LISTEN
tcp        0      0  CYBORG1.49374          CYBORG.registrar       TIME_WAIT
udp        0      0  *.instl_boots          *.*
udp        0      0  *.49153                *.*
udp        0      0  *.instl_bootc          *.*
udp        0      0  *.2121                 *.*
udp        0      0  *.syslog               *.*
udp        0      0  *.1710                 *.*
udp        0      0  *.bootpc               *.*
udp        0      0  *.*                    *.*
udp        0      0  *.177                  *.*
```

Okay, this is looking much better. Many of those unneeded services are now gone.

3.4.2 Disable Unnecessary Scripts in /sbin/init.d

Some services use a script in /sbin/init.d to start at boot time. The script includes startup and shutdown commands for the service. The services are started and shutdown at designated run levels. The files that tell the system the run level for a service to be started or shutdown are located in /sbin and are named rc2.d, rc3.d, and rc4.d. Just like the services in /etc/services file, it is necessary to disable these services since they present the opportunity of Denial Of Services attacks. The scripts can be disabled either by renaming the file so there is no K or S at the beginning or by issuing the following command to remove the execute bit:

```
# chmod 440 script_name
```

In /sbin/rc2.d I am issuing the above command for the following scripts:

K100dtlogin.rc	K200tps.rc	S530rwhod
K900nfs.server	S370named	S006hpfc
S400nfs.core	S540sendmail	S406nisplus.server
S710hparray	S408nisplus.client	S560SnmpMaster
S720lp	S410nis.server	S420nis.client

S565SnmpHpunix	S430nfs.client	S565SnmpMib2
S740supprtinfo	S440comsec	S565SnmpTrpDst
S570dce	S770audio	S490mrouted
S590Rpcd	S780slsd	S230ptydaemon
S600iforls	S510gated	S870swagentd
S620xfs	S900hpfcms	S522ppp
S630vt		

In rc3.d I will chmod the following:

S825apache
S100nfs.server

The changes will take affect after the next reboot and can be verified by running:

```
# netstat -af inet
```

3.4.3 Disable Unnecessary System Services /etc/rc.config.d

This directory holds files that contain environment variables. These files are referenced by startup scripts and determine if a service should be started and how it should run. Here are a list of changes that should be made to certain services:

File	Parm Setting	Purpose
mailservs	export SENDMAIL_SERVER = 0	Disables Sendmail Server
netdaemons	INETD_ARGS = -l	Enables inetd logging
nfsconf	NFS_CLIENT = 0 NFS_SERVER = 0	Disables Network File System Client Disables Network File System Server
syslogd	SYSLOGD_OPTS = "-DN"	Adding "N" Disables logging from remote systems

These changes will occur at the next reboot.

3.4.4 Permissions

- Restrict access to the Software Distributor Suite to the local root user. This will prevent hackers and users from viewing patch levels and installing unauthorized software.

```
# swacl -l root -D any_other
```

Verify that no entries with "any_other" is listed:

```
# swacl -l root

##############################################
# swacl    Installed Software Access Control List
#
```

```
# For host:  cyborg1:/
#
# Date:  Thu Feb 13 15:31:19 2003
#

# Object Ownership:  User= root
#                    Group=sys
#                    Realm=cyborg1
#
# default_realm=cyborg1
object_owner:crwit
group:swadm:crwit
any_other:

##########################################
```

As you can see, there is nothing listed after the `any_other` entry. If you see an entry like `--r--t` after this line, that means "other" users are allowed to read product files using swinstall, swcopy, and swlist. If a malicious attacker can execute the command "swlist –l product" this will show the patch level of the system, possibly revealing vulnerabilities that have not been fixed with a patch. The attribute "t" means any user can perform access checks and list the ACL for the sw commands. An ACL (Access Control List) is a table that tells the operating system who has access to a file or directory. If a malicious attacker knows who has access to these commands, he or she could attempt to access that account to use the sw commands.

- Set the permissions of /tmp/wtmp.out and /var/adm/wtmp to 700
  The /var/adm/wtmp file shows successful login attempts. This can give a malicious hacker account names that they can attempt to hack. The /tmp/wtmp.out file is simply the overflow file.

  ```
  # chmod 700 /var/adm/wtmp

  # chmod 700 /tmp/wtmp.out
  ```

- Set the permissions of /tmp/btmp.out and /var/adm/btmp to 700
  The /var/adm/btmp file shows bad login attempts. An attacker could obtain valid account names here also. If SSH is not functioning, it would even be possible to see a user's password if they accidentally entered it where their user name belongs at the login screen. The /tmp/btmp.out file is the over flow file.

  ```
  # chmod 700 /tmp/btmp.out

  # chmod 700 /var/adm/btmp
  ```

- Remove read access from "others" for files in /etc/rc.config.d

This directory contains files that tell the system to start service daemons at startup. If a malicious hacker can see which daemons are started, he or she can try to attack the services with Denial of Service attacks or buffer overflow attempts.

```
# chmod 700 /etc/rc.config.d
```

- Make sure that "." is not in root's search path.
  If "." is in root's search path, especially at the beginning, it will search the current directory first. If a common command such as ls has been replaced with a Trojan Horse and placed in a commonly accessed directory such as root (/) then the evil ls command will be run rather than the /sbin/ls command.

  ```
  # cd  /
  # vi .profile
  ```

  If "." is in the PATH= line, remove it and save your changes.

- Set the permissions for /stand/vmunix to 744 (owner should be root.)
  There is no need for a user to execute anything in the system kernel. This can only lead to trouble with Trojan Horse attacks.

  ```
  # chmod 744 /stand/vmunix
  ```

- Change the permissions on /etc/inetd.conf to 700 (owner root).
  We don't want a hacker being able to see what services we may have configured to run. This might give them information on what services to attack.

  ```
  # chmod 700 /etc/inetd.conf
  ```

- Change the owner of /etc/services to root and chmod to 700
  Again, there is no need to give hackers any information on services, or what ports they are using.

  ```
  # chmod 700 /etc/services
  ```

- Change the permissions on root's crontab to 700 (/usr/bin/crontab)
  You don't want non-root users being able to execute commands from root's cron file. They could attempt to start a shell with elevated permissions.

- Set the sticky-bit on any public directories, including:
  This will prevent unauthorized users from deleting or replacing files that they do not own and possibly executing malicious code.

  /tmp
  /var/tmp

  ```
  # chmod o+t /tmp
  ```

```
# ll -d /tmp
# drwxrwxrwt 5 bin  bin   1024  Jan 31 10:20  /tmp

# chmod o+t /var/tmp
# ll -d /var/tmp
# drwxrwxrwt 5 bin  bin   1024  Jan 31 10:20  /var/tmp
```

- Make root the owner on the following directories:
  This will prevent malicious attackers from trying to use accounts like bin for accessing data.

/etc	/usr/etc
/bin	/usr/bin
/sbin	/usr/sbin
/tmp	

Use the following syntax for each directory to change the owner to root:

```
# chown root /etc
```

3.4.5 Group and World-writable Directories

A world-writable directory could be exploited by an attacker inserting malicious code or filling up a mount point.

```
# /bin/find / -type f \( -perm -2 -o -perm -20 \) -exec ls -lg {} \;
# /bin/find / -type d \( -perm -2 -o -perm -20 \) -exec ls -ldg {} \;
```

3.4.6 SUID/SGID

I want to keep track of any files with SUID or SGID permissions set. A hacker could insert malicious code into one of these files and it would be executed as root. I'll use the following command to find these files:

```
# find / -user 0 \( -perm -4000 -o -perm -2000 \)-exec ls -ld {} \;
```

I will keep a copy from the output of this in a read-only file system. To do this I will need to create a small logical volume to which I can write the data:

```
# lvcreate -n lvnowrite vg01
# lvextend -L 100 /dev/vg01/lvnowrite
# newfs -F vxfs /dev/vg00/rlvtest
# cd /
# mkdir /nowrite
# mount /dev/vg01/lvnowrite /nowrite
```

Run the command again and direct the output to a file on the new mount point:

```
# find / -user 0 \( -perm -4000 -o -perm -2000 \)-exec ls -ld {} \; >
/nowrite/suid-sgid.orig
```

Then I will unmount the file system and remount it as read-only to protect the data from being overwritten or deleted:

```
# cd /
# umount /nowrite
# mount -r /dev/vg01/lvnowrite /nowrite
```

Take a look at the permissions for the /nowrite directory:

```
# ll -d /nowrite
drwxr-xr-x   3 root       root            96 Nov 29 19:13 /nowrite
```

Now let's try to write to the directory to test it:

```
# touch /nowrite/test.file
touch: /nowrite/test.file cannot create
```

Now that we know that we can't write to the directory, we need to edit the /etc/fstab to mount the directory as read-only at boot time (added line is in RED):

```
# vi /etc/fstab

#####################################################
# System /etc/fstab file.  Static information about the file systems
# See fstab(4) and sam(1M) for further details on configuring devices.
/dev/vg00/lvol3 / vxfs delaylog 0 1
/dev/vg00/lvol1 /stand hfs defaults 0 1
/dev/vg00/lvol4 /tmp vxfs delaylog 0 2
/dev/vg00/lvol5 /home vxfs delaylog 0 2
/dev/vg00/lvol6 /opt vxfs delaylog 0 2
/dev/vg00/lvol7 /usr vxfs delaylog 0 2
/dev/vg00/lvol8 /var vxfs delaylog 0 2
/dev/vg01/lvnowrite /nowrite vxfs ro 0 2
#####################################
```

Having this data available on the read-only mount point will allow me to run the same command at anytime and compare the output to the original file. I will also burn the original file onto a CD and store it in a safe place for a backup. In addition to this, IDS/9000 will monitor this machine and I will configure it to alert me when any files are created with the SUID or SGID permissions set. *(See Appendix B)*

3.4.7 Delete Unnecessary Users

Experienced hackers often try to log in using an operating system's default accounts. If the accounts are not needed, it is best to delete them and reduce this risk. The only accounts necessary for this server are: ids (IDS/9000 admin account), three system

administrators, and root. Root will not have direct access and only the three system administrators have the special privilege to su to root. Below are the default accounts in HP-UX that SAM cannot delete. Use the following command to remove the accounts:

```
# Userdel account_name
```

Use the above command for each of these accounts:

```
lp
nuucp
uucp
hpdb
```

3.4.8 Delete Unnecessary Groups

These default groups are not needed either. Use the following command:

```
# groupdel group_name
```

to delete the following groups:

lp
nuucp
daemon

3.4.9 Allow only certain users to su to root

Any user can attempt to su to root by default. If an attacker gains entry via a lower level account, he or she could attempt to gain root privileges by doing this. We can restrict the ability to attempt this to a certain group of users. First create the /etc/default/security file:

```
# touch /etc/default/security
```

Edit the file and add the following line:

```
SU_ROOT_GROUP=su
```

I'm also going to add another line to this file. If a user does not have a home directory, HP-UX will allow the user to login in at "/ " by default.

```
ABORT_LOGIN_ON_MISSING_HOMEDIR=1
```

If an attacker gains entry to a server they often will create a backdoor account for later use. Since they may not bother to create a home directory for the user, this could prevent the backdoor account from working.

Add the su group to the system and add only the users you want to be able to su to root. In this case, I am going to add our three system administrators affectionately known as Larry, Curly, and Moe:

```
# sam
```

The SAM interface will appear, choose:

1. Accounts and Groups → Groups
2. Tab to the menu and highlight Actions using the space bar and hit <ENTER>
3. Highlight Add and hit <ENTER>
4. Enter the group name (I'll call it "suers")
5. Highlight the users you want to add using the space bar
6. Tab down to OK and hit <ENTER>
7. Exit SAM by using tab to navigate to the Menu Bar
8. "File" should be highlighted
9. Hit the "f" key
10. Hit the "e" key for Exit
11. Repeat steps 7 – 10 to exit completely.

The suers group is now setup with the appropriate users.

3.4.10 mask

The result of converting to a trusted system is that the umask of root is set to 077. This is desired and no change is needed.

3.4.11 netd Logging

Since inetd will be running I will enable logging for this daemon. Add –1 to the /etc/rc.config.d/netdaemons as follows:

```
Export INETD_ARGS= -1
```

3.4.12 rotecting Programs from Illegal Execution

A new kernel parameter was added to HP-UX 11.11 called the "executable_stack". When set to 1 it will prevent an attacker from successfully getting a program to execute malicious code from its program stack when using a buffer overflow attack.

The executable_stack parameter is set to 0 by default for backwards compatibility. We will set this to 1 using SAM. (If an older program does need to execute from its stack use the chatr +es command to enable this.)

1. Run SAM by typing at the command line: sam
2. Choose Kernel Configuration
3. Choose Configurable Parameters
4. Highlight executable_stack with the spacebar
5. Tab to the top and choose Actions/Modify Configurable Parameter

6. In the Formula/Value field enter: 1
7. Choose OK and exit SAM

3.5 Convert Machine to a Trusted System

When a machine is converted to a Trusted System, the encrypted passwords are put into a protected password database readable only by root. It also restricts terminal and serial port access, enables auditing, and allows password aging. Before the conversion, be sure you have applied the latest patches. Also, once the system is converted, it is very important to try logging in on another session before logging off. That way you can fix the problem with the current session.

You can convert a machine using the command line or with SAM. For this paper I will use SAM:

1. Run SAM by typing at the command line: sam
2. Choose "Auditing & Security"
3. Then choose "System Scurity Policies"
4. Select YES at the dialogue box to continue
5. The system will begin conversion, which will take a few minutes. The length of time it takes is determined by the number of users in the /etc/passwd file.
6. A dialogue box will say "Successfully converted to a trusted system. Press OK to continue." Press OK.

CAUTION: Before we go any further, make sure you telnet into the server from another session and can su to root, or log in as root at the console. After you are sure you can still log in, you can continue to setup the Trusted System parameters.

All of the policy settings below apply to all users unless user-specific policies are set in Users/Groups functional area.

- **Password Format Policies:** This is where you can choose what format a user can have for their password. I will take the defaults, which includes requiring an 8 character password.

- **Password Aging Policies:** This is disabled by default. Since this system only has administrator accounts and system accounts I won't set this but instead rely on my root password policy. If there were several users logging into this machine, I would enable this function and require the user to change their password at least every 90 days.

- **General User Account Policies:** This section allows you to lock inactive accounts. I will enable this feature and set the time limit to 7 days. I will also keep the default for unsuccessful login tries allowed to 3.

- **Terminal Security Policies:** This allows you to set the number of times a user can attempt to login from all terminals that are connected directly or through modems, to a serial or MUX port on the system. (This does not include remote terminals.) We will keep the defaults since anyone accessing the terminal will be in front of the server and on site at the data center.

Once the security policies are set, select OK and then a dialogue box will appear saying you have successfully changed the security policies. Select OK again. You can now exit SAM.

3.6 Security Banner

Another step we want to take is to change the banner that display at login. Doing this will warn potential intruders that this system is private and only authorized users are allowed in. While this may seem obvious to most, this step makes the lawyers happy. Having a "welcome" message could be interpreted as welcoming anyone onto our system. We will also scrub the login prompt of any indicators about the operating system. There is no point in giving attackers too much information.

- Move the /etc/copyright file:

```
# mv copyright copyright.old
```

- Then modify /etc/issue and remove the following line:

```
GenericSysName [HP Release B.11.11] (see /etc/issue)
```

- Then add the following text to give adequate warning at the login prompt:

```
WARNING: This is a private system owned by Cyborg, Inc. You must have
proper authorization from Cyborg, Inc. to log in and use this system.
Unauthorized access will be prosecuted to the fullest extent of the
law.
```

- Link /etc/issue to /etc/copyright so that console users will be able to see the banner:

```
# ln -s /etc/issue /etc/copyright
```

- Now link /etc/issue to /etc/motd. This will allow users not using protocol 2 to be able to see the warning after login. Unfortunately, most users will have to see the banner twice, but at least everyone will see it.

```
# ln –s /etc/issue /etc/motd
```

3.7 TCP Wrappers and HP Secure Shell (SSH)

It is a good idea to install TCP Wrappers to protect network services. When a client connects to the host and requests a service, the inetd daemon launches the appropriate service from /etc/inetd.conf, then continues to wait for other connections. With TCP Wrappers, inetd launches tcpd rather than the requested service. Tcpd then reads the /etc/tcpd.conf file for access parameters for each service. This gives us a centralized place to control access for network services or daemons, rather than using each daemon's control file. It is also gives us more access control than SSH offers. I will use TCP Wrappers in conjunction with SSH. HP's Secure Shell software has the TCP Wrapper program included so I will install and configure it and then configure TCP Wrappers

The Secure Shell program will help protect from unauthorized access by encrypting the passwords rather than sending them in clear text. SSH should be used in place of telnet, FTP and rsh, rcp, and rlogin as these send data unencrypted. I am using HP Secure Shell ver. A.3.10.002. HP's SSH is based on SSHv2. SSHv1 has been shown to have a vulnerability that allows an attacker to recover a SSH connection's session key and decrypt all communications from the connection. For this reason, I will not enable my installation of SSHv2 to allow SSHv1 connections. The system administrators who will be accessing this server only use SSHv2 clients. The software can be downloaded free from HP's website at: www.software.hp.com/ISS_products_list.html.

SSH works similar to renting a safety deposit box at a bank. The bank holds one key, and you hold another. The box cannot be opened with only your key, nor can it be opened with only the bank's key. Instead, you must have both keys to open the box. In this instance, our server has the private key or host key and also a method to distribute the public key. However, we must protect the private host key with directory permissions. We don't want to give someone access to our private key anymore than a bank wants to give access to their private key:

- The file system permissions for /opt/ssh/etc should be:

```
drwxr-xr-x   2 bin        bin       1024 Aug  8 08:50 /opt/ssh/etc
```

- The file system permissions for the public/private host keys in /opt/ssh/etc should be:

```
-rw-------   1 root       sys        526 Aug  8 08:49 ssh_host_key
-rw-r--r--   1 root       sys        330 Aug  8 08:49 ssh_host_key.pub
```

- The /opt/ssh/etc directory holds two pairs of the keys that are encrypted with different kinds of algorithms. There are two different sets so that a common algorithm can be used between client and host. The file permissions for these sets should be as follows:

```
-rw-------   1 root       sys      668 Aug  8 08:50 ssh_host_dsa_key
-rw-r--r--   1 root       sys      601 Aug  8 08:50 ssh_host_dsa_key.pub

-rw-------   1 root       sys      883 Aug  8 08:50 ssh_host_rsa_key
-rw-r--r--   1 root       sys      221 Aug  8 08:50 ssh_host_rsa_key.pub
```

These permissions are set by default, but in the event of a system intrusion you should know how these keys should be protected.

The keys were created when I installed HP SSH so this process is done. will need to generate public/private keys to login. There are different authentication protocols you can use; I will be using RSA1. Run the following for each user:

```
# /opt/ssh/bin/ssh-keygen -t rsa1
Generating public/private rsa1 key pair.
Enter file in which to save the key (/home/curly/.ssh/identity):
Enter passphrase (empty for no passphrase): [enter passphrase here]
Enter same passphrase again: [enter it again!]
Your identification has been saved in /home/curly/.ssh/identity.
Your public key has been saved in /home/curly/.ssh/identity.pub.
The key fingerprint is:
f6:0d:b6:b5:73:57:cd:9b:56:d2:2c:49:f9:20:2e:d5 curly@CYBORG1
```

If I go to the /home/sysadmin1/.ssh directory I will see the identity.pub and identity files:

```
# cd /home/sysadmin1/.ssh
-rw-------   1 curly    adm          527 Nov 30 20:09 identity
-rw-r--r--   1 curly    adm          331 Nov 30 20:09 identity.pub
-rw-------   1 curly    adm         1024 Nov 30 20:09 prng_seed
```

- I will need to copy the configuration files that SSH uses to the appropriate directories and then configure them:

```
# cp /opt/ssh/newconfig/etc/rc.config.d/sshd /etc/rc.config.d
# cp /opt/ssh/newconfig/opt/ssh/etc/ssh_config /etc
# cp /opt/ssh/newconfig/opt/ssh/etc/sshd_config /etc
```

- Edit the /etc/sshd_config file as follows:

```
ForwardAgent yes
ForwardX11 yes          (Need this to see IDS/9000 GUI)
PermitRootLogin no      (This prevents root login over the network)
PrintMotd yes           (Uncomment this)
Banner /etc/issue       (uncomment So users can see security banner)
```

Make sure that any client used to connect to this server has the above settings.

- I will create a directory in which to store a copy of the original binaries for rsh, rlogin, rcp, and ftp in the event I would need to uninstall SSH:

```
# cd /usr
# mkdir rbin
```

- I will also create symbolic links to the SSH binaries so that if the "r" commands are used they will execute the SSH commands instead:

```
# ln -s /opt/ssh/bin/sftp /usr/bin/ftp
# ln -s /opt/ssh/bin/slogin /usr/bin/rlogin
# ln -s /opt/ssh/bin/scp /usr/bin/rcp
# ln -s /opt/ssh/bin/ssh /usr/bin/rsh
```

- Now I need to compile the TCP Wrappers program that is included with SSH:

```
# cd /opt/ssh/src/tcp_wrappers_7.6
# chmod Makefile 700
```

- Edit the Makefile and under the Easy Installation section uncomment the following line:

```
# HP-UX SCO Unicos
REAL_DAEMON_DIR=/usr/lbin/
```

The "easy installation" will move the rsh, rlogin, rcp and ftp daemons to the /usr/lbin/wrapper directory and the tcpd wrapper daemons fill the holes that are left.

- Edit the /etc/inetd.conf file and add the following line to wrap ssh in tcpd (TCP Wrappers daemon):

```
ssh    stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/sshd -I
```

- Be sure to restart inetd for the changes to take place:

```
# inetd -c
```

- Configure the access files that TCP Wrappers uses which are located in /etc. The files are in search order:

File	Entry
hosts.allow	If a client and daemon pair are here, the client is granted access.
hosts.deny.	If a client and daemon pair are here, the client is denied access
No entry	If the client is not in either then access is granted by default.

- I will configure the server to deny everything by default by adding the following line in /etc/hosts.deny:

```
ALL:ALL
```

- Then I will allow specific hosts in /etc/hosts.allow by adding two lines. In this instance I'm only going to allow the servers that this host is monitoring, an

administration machine I use to administrate my servers, and the system administrator's machines. They will only be able to connect using SSH:

```
sshd: 10.1.1.40, 10.1.1.20, 10.1.1.21, 10.1.1.22
sshd: 192.168.19.0/255.255.255.0
```

- Now I will test the tcp wrappers configuration by running tcpdchck. This will examine the /etc/hosts.allow and /etc/hosts.deny files against the entries in /etc/inetd.conf:

```
# tcpdchk -i /etc/inetd.conf –v

>>> Rule /etc/hosts.allow line 1:
daemons:  sshd
clients: 10.1.1.40, 10.1.1.20, 10.1.1.21, 10.1.1.22,
         192.168.19.0/255.255.255.0
access:   granted
```

3.8 NTP

It is important to have the correct time on your servers. The timestamps on all files, especially log files, depend on this. It is equally as important that your servers are in sync with each other and other machines, as the firewall. In the event of a compromise on a system, you will be able to coordinate log files on the server as well as the firewall and other network appliances. It is also necessary for the forensics team to have reliable dates as legal evidence in the prosecution of malicious hackers. This server is an internal time server that is a peer with the three central time servers in this environment. The three central time servers are connected to the internet and have separate sources for synchronizing the time. Cyborg1 will ignore any sync requests outside of the network parameters in the configuration file.

- Create the ntp.conf file

```
# touch /etc/ntp.conf
```

- Add the following lines to /etc/ntp.conf:

```
driftfile   /etc/ntp.drift       #  drift file

server xxx.xxx.xxx.xxx     # ntp internal server 1
server xxx.xxx.xxx.xxx     # ntp internal server 2
server xxx.xxx.xxx.xxx     # ntp internal server 3

server 127.127.1.1 prefer  # Allows for internal sync but not external
```

- Now edit the xntp lines in /etc/rc.config.d/netdaemons as follows:

```
XNTPD=1
NTPDATE_SERVER="time_server1 time_server2"
```

Setting the *XNTPD* variable to "1" will cause the daemon to be started automatically when the system makes the transition from run level 1 to 2. NTPDATE_SERVER tells xntpd which internal servers to sync with on bootup.

- Change the permissions for the /etc/ntp.conf file:

```
# chmod 444 /etc/ntp.conf
```

Reboot the machine and the xntpd will now run as a daemon.

3.9 Sendmail

Sendmail can be a vulnerability in a networked environment. If Sendmail is set with the defaults, it is ripe for being exploited to propagate a virus. For example, port 25 is a common port used on mail servers, if a virus scans for that port Sendmail will respond. This will cause unnecessary network traffic and could affect not just the server but the entire segment.

- Since I will be using Sendmail to send alerts from IDS/9000 I cannot disable it, however, I can configure it to start only when needed and then let it die when no longer needed. Stop the Sendmail daemon if it is running:

```
# /usr/sbin/sendmail stop
```

- Then set the SENDMAIL_SERVER line to 0 in /etc/rc.config.d/mailservs:

```
########################################
# Mail configuration.  See sendmail(1m) #
########################################
#
# @(#)B.11.11_LR
#
#  BSD's popular message handling system
#
# SENDMAIL_SERVER:      Set to 1 if this is a mail server and should
#                       run the sendmail daemon.
# SENDMAIL_SERVER_NAME: If this is not a mail server, but a client
#                       being served by another system, then set this
#                       variable to the name of the mail server system
#                       name that site hiding can be performed.
#

export SENDMAIL_SERVER=0
export SENDMAIL_SERVER_NAME=

#########################################################
```

This will prevent the sendmail server from starting at bootup.

- To stop Sendmail from running as a daemon listening on port 25 change the following line in /sbin/init.d/sendmail:

```
/usr/sbin/sendmail -bd -q30m && echo "sendmail"
```

remove –bd to make the line look like:

```
/usr/sbin/sendmail -q30m && echo "sendmail"
```

This configuration will stop the Sendmail daemon from running and actively listening on port 25. We can rely on the mailx command to send mail by starting Sendmail as needed (for alerts) then die once the task is completed.

- For additional security, I want remove ($v/$Z) from each of the following lines in /etc/mail/sendmail.cf as this causes the version and patch levels of Sendmail to be indicated in sent messages.
  - `Received: $?sfrom $s $.$?_($?s$|from $.$_) $.by $j ($v/$Z)$?r with $r$. id $i$?u for $u; $|; $.$b`
  - `SmtpGreetingMessage=$j Sendmail $v/$Z; $b`
- I will have Cyborg's root email sent to the system administrator's address by configuring the /etc/mail/aliases file:

```
##
#  Sendmail Alias File
#  @(#)B.11.11_LRaliases $Revision: 1.1.212.1 $ $Date: 99/09/13
15:13:16 $
#
#  Mail to an alias in this file will be sent to the users, programs,
or
#  files designated following the colon.
#  Aliases defined in this file will NOT be expanded in headers from
#  mailx(1), but WILL be visible over networks and in headers from
#  rmail(1).
#
#    >>>>>>>>>>  The program "/usr/sbin/newaliases" must be run after
#    >> NOTE >>  this file is updated, or else any changes will not
be
#    >>>>>>>>>>  visible to sendmail.
##

# Alias for mailer daemon
MAILER-DAEMON   : root

# RFC 822 requires that every host have a mail address "postmaster"
postmaster      : root

# Aliases to handle mail to msgs and news
nobody          : /dev/null
```

```
# System Administration aliases
operator        : root
uucp            : root
daemon          : root

# Ftp maintainer.
ftp-bugs        : root

# Local aliases
root       : sysadmin@cyborg.com

#####################################################
```

My addition is in RED

- Run /usr/sbin/newaliases to update the /etc/mail/aliases.db file after making any changes to the aliases file:

```
# /usr/sbin/newaliases
/etc/mail/aliases: 7 aliases, longest 9 bytes, 88 bytes total
```

Note that if you are not using DNS and do not have a fully-qualified host name as the first entry in the /etc/hosts file (i.e. – cyborg1@cyborg.com) you will get the following error when running the newaliases command:

```
WARNING: local host name (sys1) is not qualified; fix $j in config
file
```

To fix this you must modify the following line in /etc/mail/sendmail.cf so that Sendmail can resolve your domain name:

Change the line:

```
#Dj$w.Foo.COM
```

to

```
Dj$w.my_domain.com
```

4 Installing & Configuring IDS/9000 2.1

HP's IDS/9000 is a host-level intrusion detection system. It continuously monitors activity on configured hosts for patterns that could indicate an intrusion. It can detect multiple failed login attempts, repeated failed su attempts, changes to key files, and more. It is also possible to capture the alerts generated by the IDS/9000 agent and use a number of tools to process them according to the severity level. In the following instructions I will use Sendmail to send the system administrator a page for high level alerts. Oh, and the beauty of it is that it's free. You can download it at www.software.hp.com.

The purpose of Cyborg is to use IDS/9000 to monitor several FTP servers that are used on the internet for the public to download software and documentation. I also will configure IDS/9000 to monitor Cyborg1 itself.

4.1 Installation

- Dependencies
  - You must have Java SDK or RTE 1.3.1 (version 1.3.1.00) and all the corresponding Java patches.
  - You also must install a critical patch that was released for 11i: `PHKL_26074 s700_800 11.11 libaudit.a cumulative patch`. This patch requires a reboot.

- Download the latest version of IDS/9000 from http://software.hp.com and copy it to a secure medium.

- Then create the directory: /var/tmp/idsprod and copy J5083AA_1111.depot to this directory.

- I need to create an agent depot from which the monitored systems can install the software:

```
# swcopy -s /var/tmp/idsprod/J5083AA_1111.depot IDS.IDS-Agent \
IDS.IDS-Doc @ /var/depot/ids_11i_agent
```

- I also need to create an admin depot since this will be our admin server:

```
# swcopy -s /var/tmp/idsprod/J5083AA_1111.depot IDS.IDS-Admin \
IDS.IDS-Doc @ /var/depot/ids_11i_admin
```

- Now I'll install both the admin and agent on this server since we will also be monitoring this server:

```
# swinstall -x autoreboot=true -s /var/depot/ids_11i_admin+agent \*
```

- After install run:

```
# /opt/ids/bin/IDS_checkInstall
```

You should receive a message similar to the following:

```
WARNING: The idds driver is configured into the kernel but IDDS is not
enabled.
         You will need to do the following to enable IDDS:
         # /usr/sbin/kmtune -s enable_idds=1
         # mk_kernel
         # kmupdate
         # reboot.
CYBORG is not an HP-UX 11.00 system. No need to check patches
Install check successful!
```

- Before I move on, I want to change the kernel parameter `max_thread_proc`. By default this parameter is set to 64, which will allow us to monitor 23 agents. At some point I may want to add more agents so I will bump this parameter up to 128, which should allow me to have 46 agents. We will do this through SAM:

  - At the command line type: sam
  - Choose Kernel Configuration
  - Choose Configurable Parameters
  - Highlight max_thread_proc using the space bar
  - Tab up to Actions, and choose Modify Configurable Parameter
  - Enter the new value in the Formula/Value box
  - Choose OK

This will require a new kernel to be built. Go ahead and allow SAM to do this and reboot the machine. Once the system comes back up the new value will be set.

4.1.1 Certificate Creation

The group “ids” and the user “ids” has been added to the system, along with two services in the /etc/services file: hpidsadmin and hpidsagent. I will now reboot the system as this is required after installing IDS/9000.

- Login as the user “ids”:

```
# su - ids
```

- Then export the PATH and SH_LIBPATH as follows:

```
# export PATH=/opt/ids/bin:$PATH
# export SHLIB_PATH=/opt/ids/lib:$SHLIB_PATH
```

- A secure method of communication must be setup between the IDS/9000 agent process on each client server and the System Manager process on the IDS Admin server. Each must have a X.509 certificate associated with it or the System Manager process on the Admin server will not start. The following steps will create the necessary certificates:

```
# cd /opt/ids/bin

# IDS_genAdminKeys
```

This generates administration certificate and the Root Certification Authority (Root CA).

```
Generating a certificate request for IDS Root CA...
Generating a self-signed certificate for IDS Root CA...
Generating a certificate for the IDS/9000 System Manager...
Generating cert signing request for IDS/9000 System Manager...
Signing the IDS/9000 System Manager certificate request...
Importing IDS Root CA certificate...
Importing the IDS/9000 System Manager certificate...

************************************************************
* Successfully created certificates for IDS Root CA and for
* the IDS/9000 System Manager.
* Certificate public keys are valid for 700 days and are
* 1024 bits in size.
*
* Now you need to create keys for each of the hosts on which
* the Agent software is installed by running the script
* 'IDS_genAgentCerts'.
************************************************************
```

- Then generate keys for each client:

```
# IDS_genAgentCerts

Generate keys for which host? cyborg1
Generating key pair and certificate request for IDS Agent
on myhost1....
Signing certificate for IDS Agent on cyborg1...
Certificate package for IDS Agent on cyborg1 is
/var/opt/ids/tmp/cyborg1.tar.Z

Next hostname (^D to quit)? cyftp1
Generating key pair and certificate request for IDS Agent
on cyftp1....
Signing certificate for IDS Agent on cyftp1...
Certificate package for IDS Agent on cyftp1 is
/var/opt/ids/tmp/cyftp1.tar.Z

Next hostname (^D to quit)? cyftp2
```

```
Generating key pair and certificate request for IDS Agent
on cyftp2....
Signing certificate for IDS Agent on cyftp2...
Certificate package for IDS Agent on cyftp2 is
/var/opt/ids/tmp/cyftp2.tar.Z

Next hostname (^D to quit)? Ctrl-D
************************************************************
* Successfully created agent certificates for the following
* hosts:
*    cyborg1
*    cyftp1
*    cyftp2
*
* Certificate public keys are valid for 700 days and are
* 1024 bits in size.
*
* They are stored in /var/opt/ids/tmp as hostname.tar.Z
*
* You should now transfer the bundles via a secure channel
* to the IDS agent machines.
*
* On each agent you will need to run the IDS_importAgentKeys
* script to finish the installation.
************************************************************
```

The agent certificate bundles are generated and stored in the files:

```
/var/opt/ids/tmp/cyborg1.tar.Z
/var/opt/ids/tmp/cyftp1.tar.Z
/var/opt/ids/tmp/cyftp2.tar.Z
```

- I will need to transfer the certificates from the Admin Server to the agents in a secure way. There are several ways to do this depending on your environment. I will do this by copying the /var/opt/ids/tmp/*host_name*.tar.Z file onto a local tape drive and loading them onto the agent:

```
# cd /var/opt/ids/tmp/
# tar cvf /dev/rmt0 agent_name.tar.Z
```

On the agent, extract the key in the /var/opt/ids/tmp directory:

```
# cd /var/opt/ids/tmp
# tar xvf /dev/rmt0 agent_name.tar.Z
```

- Once I have transferred the keys onto the agent hosts I do the following on the ***agent***:

```
# su - ids
```

```
# cd /opt/ids/bin
```

- We've stored the key bundle in the directory `/var/opt/ids/tmp` so now import the key bundle:

```
# IDS_importAgentKeys /var/opt/ids/tmp/agent_name.tar.Z adminsys
```

agent_name is the name you entered for this agent on the Admin Host and *adminsys* is the host name or IP address of the administration system.

The Root Certificate Authority and the certificate for the agent are now extracted and installed in /etc/opt/ids/certs/agent

Here is an example of the type of message you should get:

```
Extracting key pair and certificates...
Modifying the configuration file /etc/opt/ids/ids.cf to use
myadmin as the IDS Administration host...

************************************************************
* Keys for IDS Agent were imported successfully.
*
* You can now run the idsagent process on this machine and
* control it from the IDS/9000 System Manager.
************************************************************
```

4.1.2 Permissions

I would like to note that IDS/9000 has very strict permissions and only the user *ids* can execute programs in it or access configuration files. Not even root has these privileges. Be sure to su – to the ids user when you need to administrate IDS/9000.

4.1.3 Starting the Agent

When you log into each agent host for the first time, you will not be able to log in directly as the ids user, you will have to log in as root and use the passwd command for the ids user.

- Now I will su – to the ids agent on **CyFTP1** and start the agent program:

```
# /opt/ids/bin/idsagent
```

Then I will log back into Cyborg (our admin host) and start the System Manager Program: Remember to use the passwd command to set the password for the ids user

```
# su - ids
# /opt/ids/bin/idsgui
```

The license agreement will pop up, click on *Accept*.

4.1.4 Log Files

One change that I made was to store the alert, error and log files to a separate mount point. I have created a logical volume mounted in /security for this purpose. I did this because I did not want the /var mount point to fill up. In the /etc/opt/ids/ids.cf file change the following lines to store these files on the /security mount point:

```
IDS_ALERTFILE                   /security/ids/alert.log
IDS_ERRORFILE                   /security/ids/error.log
IDS_LOGFILE                     /security/ids/kernelaudit.log
```

Create the logical volume and mount point ids:

```
# lvcreate -n lvids vgsecurity
# lvextend -L 500 /dev/vgsecurity/lvids
# newfs -F vxfs /dev/vgsecurity/lvids
# cd /security
# mkdir /ids
```

Modify /etc/fstab so that this will mount at boot time:

```
# vi /etc/fstab

#####################################################
# System /etc/fstab file.  Static information about the file systems
# See fstab(4) and sam(1M) for further details on configuring devices.
/dev/vg00/lvol3 / vxfs delaylog 0 1
/dev/vg00/lvol1 /stand hfs defaults 0 1
/dev/vg00/lvol4 /tmp vxfs delaylog 0 2
/dev/vg00/lvol5 /home vxfs delaylog 0 2
/dev/vg00/lvol6 /opt vxfs delaylog 0 2
/dev/vg00/lvol7 /usr vxfs delaylog 0 2
/dev/vg00/lvol8 /var vxfs delaylog 0 2
/dev/vgsecurity/lvsecurity /security vxfs rw,suid,delaylog,datainlog 0 2
/dev/vgsecurity/lvids /security/ids vxfs rw,suid,delaylog,datainlog 0 2
/dev/vg01/lvnowrite /nowrite vxfs ro 0 2

#######################################
```

Now mount the new file system:

```
# mount -a
```

Make sure the file system mounted:

```
# bdf

   Filesystem              kbytes    used    avail   %used Mounted on
   /dev/vg00/lvol3         204800    71929   124620   37%  /
   /dev/vg00/lvol1         299157    41577   227664   15%  /stand
   /dev/vg00/lvol8         1560576  1003327 523472   66%  /var
   /dev/vg00/lvol7         970752    848414  114700   88%  /usr
```

```
/dev/vg00/lvol4             204800   93911   103967  47%  /tmp
/dev/vg00/lvol6             1812480  882925  871501  50%  /opt
/dev/vg00/lvol5             512000   1780    478645   0%  /home
/dev/vgsecurity/lvsecurity 512000   1780    478645   0%  /security
/dev/vgsecurity/lvids       512000   1780    478645   0%  /security/ids
/dev/vg01/lvnowrite         204800   1157    190916   1%  /nowrite
```

We can see that the /security/ids mount point has been mounted.

4.1.5 IDS User

- Put /opt/ids/bin in the ids user's path so that the commands can be run while in any directory.
- I am going to modify the agent configuration file since I will be using IDS/9000 to monitor this server also. (See Appendix B for monitoring configuration for Cyborg.)
- Make the ids.cf agent configuration file writable:

```
# su - ids
# chmod u+w /etc/opt/ids/ids.cf
```

- Edit /etc/opt/ids/ids.cf file to reflect the following changes:

```
REMOTEHOST
```

becomes

```
REMOTEHOST 10.1.1.50
```

- Change the ids.cf agent configuration file to be read and execute only for user ids:

```
# chmod u=r /etc/opt/ids/ids.cf
```

- If the agent process is running, force it to reread the configuration file:

```
# kill -HUP $(cat /var/opt/ids/idsagent.pid)
```

This will cause the ids agent process to reread the configuration and reactivate any current surveillance schedule.

4.2 Intrusion Detection Configuration Section

Components

The IDS/9000 product has three different components that work together to raise an alert for an event. In the next few pages I will be configuring these components to

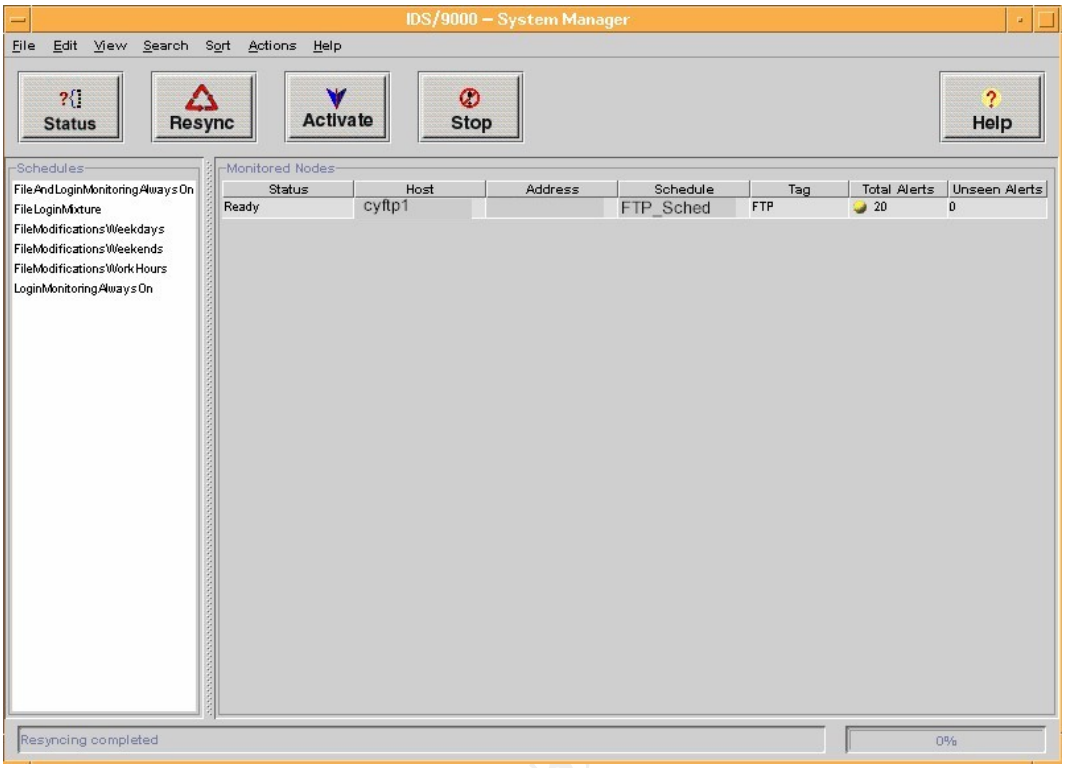
monitor the FTP server(s). The following explanation will outline how these components fit together.

Detection Templates
HP provides a set of pre-configured templates that identify certain system activity and attacks commonly seen in a network environment. Each template has customizable values that can be adjusted for each environment.

Surveillance Groups
A surveillance group contains related detection templates, such as file system attacks or login attacks. Surveillance groups are saved as
`var/opt/ids/gui/SurveillanceGroups/`*`groupname`*`.grp`

Surveillance Schedules
A surveillance group can be scheduled to run on one or more host agents on a regular weekly basis. More than one schedule can run a host, and more than one host can use one surveillance schedule. Surveillance schedules are saved as
`/var/opt/ids/gui/SurveillanceSchedules/`*`schedname`*`.schedule.`

A screen shot of the IDS/9000 System Manager:



Scheduling

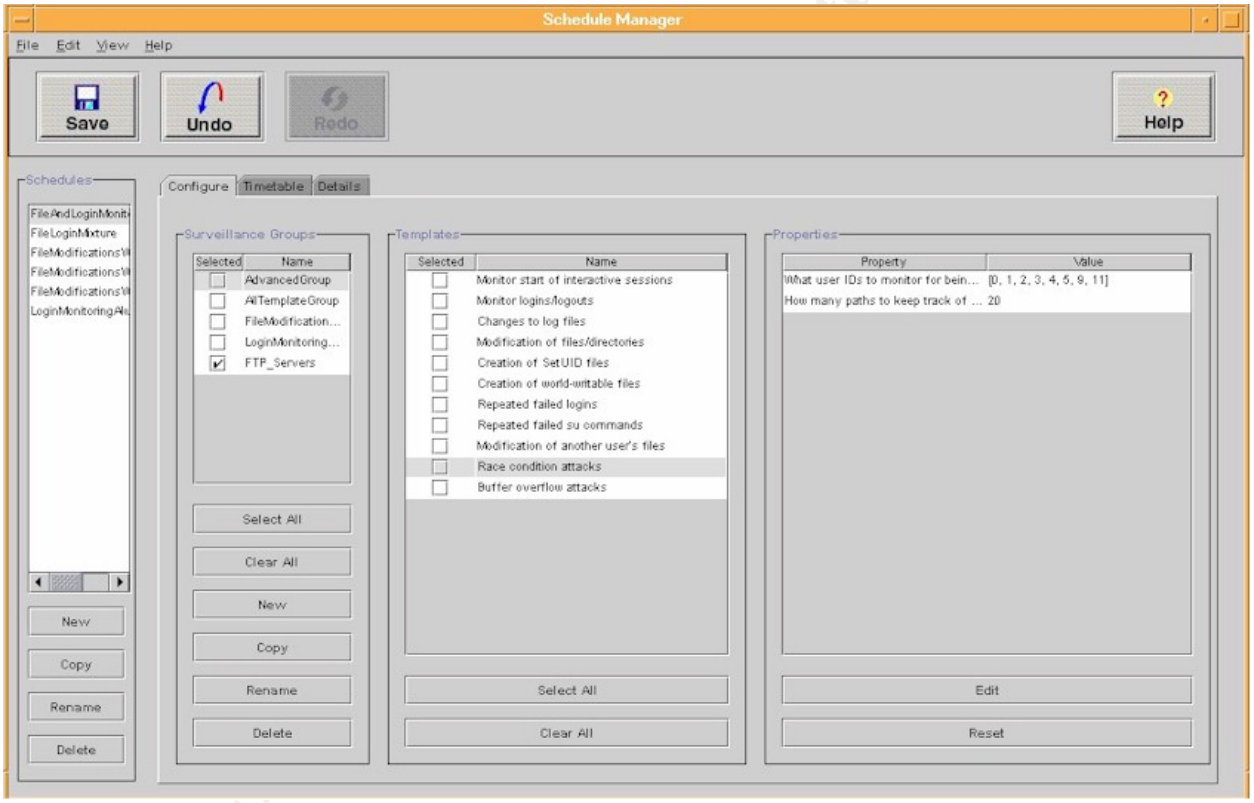
There are pre-defined schedules provided with IDS/9000. I wouldn't want to use the schedules that limit monitoring to just weekdays or weekends since the FTP servers I'm monitoring will be available 24/7. The schedule I will use to copy is FileandLoginMonitoringAlwaysOn. I also prefer to create my own Surveillance Groups and group them by the type of server(s) I am monitoring.

Step-by-Step:

1. From the System Manager screen choose Edit/Schedule Manager from the menu.
2. Click on and highlight FileandLoginMonitoringAlwaysOn under Schedules.
3. Click on the Copy button
4. Enter the name of the new schedule "FTP_Sched"
5. Click OK
6. Highlight FTP_Sched

7. Under Surveillance Groups click on the New button.
8. I will call this Surveillance group “FTP_Servers”
9. Click OK
10. Uncheck any other Surveillance Groups
11. Check the new Surveillance group “FTP_Servers”
12. Highlight FTP_Servers

The following sections will cover each template and which values we will assign to them. Since we have our new surveillance group “FTP_Servers” checked, we can then check each template we want to activate. While that template is highlighted, edit the value(s) under the Properties section on the right. Below is a screen shot of the Schedule Manager for reference:



Monitoring the Wu-FTPD Servers

The group of servers that I am monitoring are public servers that hold files available for download by anonymous ftp. No uploads are permitted. All of the servers are setup identically. They run the WU-FTPD 2.6.1 release from Hewlett Packard. WU-FTPD is a secure FTP daemon for Unix that was developed by Washington University.

The FTP servers have been setup according to www.cert.org guidelines, adapted to the HP-UX environment. The biggest security risk with anonymous FTP lies with directory permissions and ownership. If a malicious user can manage to write to the ftp directory structure, then the server could be used for all sorts of purposes, such as a depot for unlicensed software (warez site), or worse.

A chroot'ed directory has been setup for the ftp download area that will appear to the anonymous user as "/". In reality, the directory is: /secure/ftp/. It is also mounted on its own logical volume. Since these servers are only for downloading files, no write permissions will be allowed. The user/group *ftpuser:ftpgroup* was created on the systems for anonymous FTP. No directories will be owned by this user. The directory structure is as follows:

Directory	Owner	Group	Permissions
/secure/ftp	root	other	555
/secure/ftp/dist	root	other	555
/secure/ftp/etc	root	other	555
/secure/ftp/usr	root	other	555
/secure/ftp/usr/bin	root	other	555

Since the commands need to navigate within the chroot'ed area (i.e. – ls) /usr/bin commands have copied into /secure/ftp/usr/bin. This is in keeping with the HP-UX directory structure. No system commands are found here.

In light of the purpose of these servers and the above directory structure, the strategy to protect the servers will involve:

- Monitoring the secure ftp area for unauthorized modification or file creation.
- Monitoring directory and file ownership and permissions.
- Monitoring the account *ftpuser* for suspicious commands.

The template defaults will be listed, as well as any additions necessary to protect the systems in an FTP environment.

Templates

Buffer Overflow Attacks

This template monitors programs executed with setuid. This means that a program or script is run with the owner's permissions instead of the user executing the program. The template will give an alert if a suid program execute another program, or a program unexpectedly gains user ID 0 privileges.

The default users that are monitored are: root, daemon, bin, sys, adm, uucp, lp, and nuucp. We will add the user ftpuser.

1. Check template: Buffer Overflow Attacks
2. Highlight Property: What user ID's to monitor for being attacked
3. Click on the Edit button
4. The Edit Property Dialog box will pop up
5. Click the Add button
6. Enter the user number for the user you want to add.
7. Click OK
8. Click OK again

Changes to Log Files

This template monitors log files for any attempt to do anything but append them. Many attackers will modify or delete log files to cover their tracks. Below is a list of log files that are monitored by default.

- Files that log login attempts:

/var/adm/btmp	/var/adm/wtmp
/var/etc/bmp	/etc/wtmp

- Syslog files:

/var/adm/messages	/var/adm/syslog/mail.log
/var/adm/syslog/syslog.log	

- The file that tracks commands that a user executed and the timestamp:

/var/adm/pacct

- The file that tracks the su command and the timestamp:

/var/adm/sulog

My Additions:

This is the log file I have setup in syslog.conf to monitor any FTP activity:

/var/adm/syslog/ftpd.log
/var/opt/ids/alert.log *– Log file for ids alerts*

1. Check template: Changes to log files
2. Highlight Property: Files which should only be appended to

3. Click on the Edit button
4. The Edit Property Dialog box will pop up
5. Click the Add button
6. Enter the full path of the file
7. Click OK
8. Click OK again

Creation of World-Writable Files

Any user can modify a world-writable file. If a file is world-writable, owned by a system user, and is a system file, it could be exploited by a regular user. This template will monitor a file that has been modified by setting the world-writable bit, changing the owner of a file that is world-writable and is owned by a user on a pre-determined list, and creation of a file that is world-writable and is owned by a user on that list.

The default list is as follows:

root	daemon
bin	sys
adm	uucp*
lp*	nuucp*

**Red Indicates deleted users.*

My Additions:

I am going *to* add *ftpuser* since this user should not own any files.

1. Check template: Creation of world-writable files
2. Highlight Property: List of critical user ID's to be monitored
3. Click on the Edit button
4. The Edit Property Dialog box will pop up
5. Click the Add button
6. Enter the user number for the user you want to add.
7. Click OK
8. Click OK again

Modification of Another User's Files

This template will send an alert when a user modifies a file not belonging to them. An attacker could try to change files by using a system program, since most daemons are run by a certain user, having warning of any changes could alert us to this attack.

There are only three defaults to this template. They are as follows:

- Property: `Ignore changes to these files (full path)`
  Default: `/dev/null`

  Adding files to this list allows specific files to be modified without generating alerts. These need to have exact, full path names.

- Property: `Ignore changes to these directories (full path)`
  Default: empty.
  Adding directories to this permits anything in or below that directory to be modified without generating an alert. These should be full path names, but need not be exact. For instance "/tmp/a" will match "/tmp/apple". If you want to specify a specific directory, be sure to append a trailing "/".

- Property: `List of user IDs to be ignored`
  Default: empty.

  Adding user ID numbers to this list will cause those users to be ignored by this template. It is recommended that this be left blank unless specifically needed.

- Property: `Files modified by Program List x`

- Property: `Program List x`

  There are three pairs of lists, with *x* values of 1, 2, and 3.

  Default: all lists empty.

  If a program in "`Program List x`" modifies a file in "`Files modified by Program List x`", the event does not generate an alert.

My Additions:
None. All files should be monitored for changes by a non-owner.

Modification of Files/Directories

This template tracks changes or deletions made to specified files or directories. It also monitors specified files for owner or permission changes.

Note: The template does not monitor the actual contents of a file, it only knows that a change was made.

There are four properties for configuring the filtering system:

- Watch these files for modification/creation
- Ignore these files
- Watch these directories for modification
- Ignore these directories

The defaults for this template are as follows:

- Property: `Watch these files for modification/creation`

- System Kernel and Configuration Files:

/stand/vmunix	/stand/kernel
/stand/bootconf	

- Files Pertaining to Users:

/etc/passwd	/etc/group

- Network Services:

/etc/inetd.conf

- Files Pertaining to Remote Root Access:

/.rhosts	/.shosts
/etc/hosts.equiv	

- Property: `Ignore these files`

- Temporary files pertaining to vipw but are not used in system configuration:

/etc/.pwd.lock	/etc/ptmp
/etc/utmp	/etc/utmpx

- Property: `Watch these directories for modification`

- Directories that contain system binaries:

/lib

- Software package directory:

/opt

- System configuration files:

/etc

- Kernel configuration files:

/stand

My Additions for <u>Directories</u> to Monitor:

/secure/ftp	/secure/ftp/dist
/secure/ftp/etc	/secure/ftp/usr
/secure/ftp/usr/bin	/etc/ftpd
/home/ftpuser	/tcb *(trusted system directory)*

My Additions for <u>Files</u> to Monitor:

/usr/bin/false – *(used in /etc/passwd for ftpuser to prevent shell access)*

1. Check template: Modification of files/directories
2. Highlight Property: Watch these files for modification/creation
3. Click on the Edit button
4. The Edit Property Dialog box will pop up
5. Click the Add button
6. Enter the full path of the file
7. Click OK
8. Click OK again
9. Highlight Property: Watch these directories for modification
10. Click on the Edit button
11. The Edit Property Dialog box will pop up
12. Click the Add button
13. Enter the full path for the directory
14. Click OK
15. Click OK again

<u>Monitor Logins/Logouts</u>

This template monitors users that log in and out of the system.

The only property in this template is to ignore specific users. Since we will be monitoring all users, we will not add any values.

<u>Monitor Start of Interactive Sessions</u>

This template will monitor any interactive session including FTP sessions, remote logins, and whenever the su command is invoked. There are certain accounts that should only be used by the system. If an interactive session is started by one of these accounts this template will send an alert.

The defaults for this template are as follows.

- Property: `Notify when these users begin a session`
- Login accounts:

root	ids
news	www
adm	bin
daemon	hpdp
lp	nuucp
sys	uucp

My Additions

ftpuser

1. Check template: Monitor logins/logouts
2. Highlight Property: Ignore these users
3. Click on the Edit button
4. The Edit Property Dialog box will pop up
5. Click the Add button
6. Enter the user number for the user you want to add
7. Click OK
8. Click OK again

Race Condition Attacks

A race condition is a type of attack that uses the time between a program checking to see if a file exists and a program using that file. If an attacker can change the file during this time, malicious code could be executed by the program.

The defaults for this template are as follows.

- Property: `What user IDs to monitor for being attacked`

root	bin
adm	hpdp
daemon	nuucp
lp	uucp
sys	

My Additions:

lds	ftpuser

1. Check template: Race Condition Attacks
2. Highlight Property: What user ID's to monitor for being attacked
3. The Edit Property Dialog box will pop up
4. Click the Add button
5. Enter the user number for the user you want to add
6. Click OK
7. Click OK again

- Property: `How many paths to keep track of per process (0 is all)`
  Default: `20` *`(this is the number of file accesses to store per process)`*

Note: Increasing this number will give a larger view of a user's actions, but it will slow down the response time of this template and require more memory.

I will not increase the number of paths.

Repeated Failed Logins

This template monitors failed login attempts and will send an alert after a pre-defined number of attempts.

The defaults for this template are as follows.

- Property: Number of failures to exceed
  Default: 2

- Property: Time span to detect failures over (in seconds)
  Default: 10

- Property: Suppression period for reporting (in seconds)
  Default: 30

My Changes:
I am going to change the "Number of Failures to Exceed" to 3

1. Check template: Repeated failed logins
2. Highlight Property: Number of failures to exceed
3. Click on the Edit button
4. The Edit Property Dialog box will pop up
5. Delete the current value and enter 3
6. Click OK

Repeated Failed su Commands
This template sends an alert for su attempts after a pre-determined threshold.

The defaults for this template are as follows.

- Property: Number of failures to trigger on
  Default: 2

- Property: Time span to detect failures over (in hours)
  Default: 24

My Changes:
The default settings will cause an alert to be generated if two or more su failures by a user occur within one day. Since we will be monitoring FTP servers that are accessed often, I will change the default to 2 hours.

1. Check template: Repeated failed su commands
2. Highlight Property: Time span to detect failures over
3. Click on the Edit button
4. The Edit Property Dialog box will pop up
5. Delete the current value and enter 2
6. Click OK

Creation of SetUID Files
This template monitors creation of setuid files from a list of users. A setuid file runs with the owner's permissions instead of the user executing the program. A common attack is for an intruder to run a copy of the /bin/sh program with a setuid of root. This will allow the intruder to have a shell with root privileges.

The defaults for this template are as follows:

root	daemon
bin	sys
adm	uucp
lp	nuucp

My Additions:

ids	ftpuser

1. Check template: Creation of SetUID files
2. Highlight Property: List of critical user ID's to be monitored
3. Click on the Edit button

4. The Edit Property Dialog box will pop up
5. Click on Add
6. Enter the user ID
7. Click OK
8. Click OK again

Do this for each user to be added.

4.3 Alerting System Administrator to Attacks

Monitoring the systems accomplishes nothing if the system administrator is not alerted to critical attacks. IDS/9000 is designed to work with different alert programs, from shell scripts to HP's OpenView product. In this environment, there is a pager gateway on another platform. I will utilize this gateway to send critical (level 1) alerts to the system administrator's pager. Any lower level alerts (levels 2 and 3) I will have emailed to the root account.

IDS/9000 provides the following arguments for response programs:

Argument	Data Type	Name	Description
`argv[0]`	String	Program	Name of the executable.
`argv[1]`	Integer	Code	Code assigned to the detection template. Three digits with leading zeros, as in 005 and 027.
`argv[2]`	Integer	Version	Version of the detection template.
`argv[3]`	Integer	Severity	A number from `1` to `3` indicating the general severity of the alert as follows: 1. Critical: Can provide root access to an attacker. 2. Severe: Can compromise the operation of the system, overwrite or delete files, attempt to gain privileged access, etc. 3. Alert: Information about actions that might be used to attack the system.
`argv[4]`	String	UTC Time	The UTC date, formatted as *YYYYMMDDhhmmss*, where *YYYY* is the year, *MM* is the month (`01` to `12`), *DD* is the day (`01` to `31`), *hh* is the hour (`00` to `23`), *mm* is the minute (`00` to `59`), and *ss* is the seconds (`00` to `59`).
`argv[5]`	String	Attacker	The "initiator" of the action, if known.
`argv[6]`	String	Target ID	A two-digit code followed by a label, indicating the general computer subsystem affected by this action. For example, `02:FILESYSTEM`.
`argv[7]`	String	Attack Type	A brief summary of the alert.
`argv[8]`	String	Details	Detailed information on the alert.

Using the above arguments, I have modified the sample shell program provided with IDS/9000 to send email or pager alerts to the system administrator depending on the severity of the attack:

```
#!/usr/bin/sh
#
# IDS/9000 alert response script for sendmail
#
# Send an email via the pager gateway to the SysAdmin's pager if # a
severity 1 alert is received
#
# Send an email to root's address if a severity 2 or is received
#

IDS_BASE="/opt/ids"
IDS_ETC="/etc/opt/ids"
IDS_VAR="/var/opt/ids"
RESPONSE_BASE=$IDS_BASE/response

# This is the pager gateway address for root
PAGEROOT = sysadm_pager@cyborg.com

# This is the local email for root
ROOT = "root"

# Setting the umask to a "sane" value
umask 077

# If we have a severity 1 alert then send the details in email
if [ $3 = "1" ]
then
        echo "$8" | /usr/bin/mailx -s "$7" ${PAGEROOT}

else

     echo "$8" | /usr/bin/mailx -s "7" ${ROOT}

fi

# Exit with no error
exit 0
```

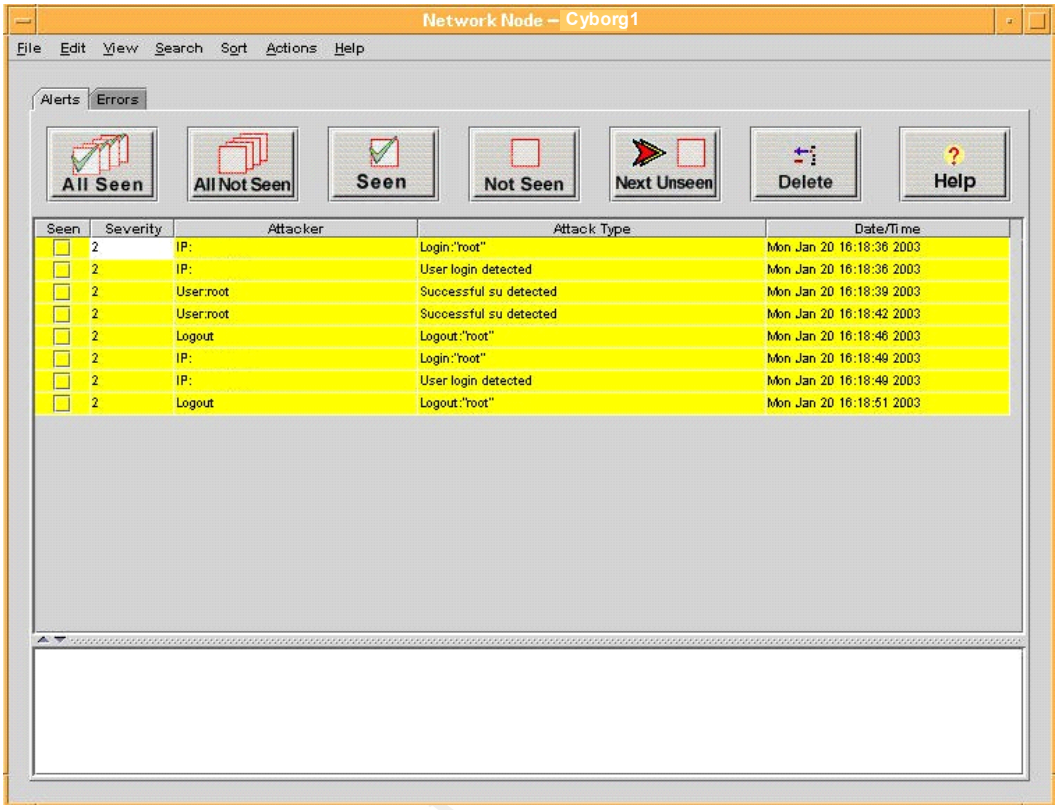
The system administrator will now be notified about any suspicious activity IDS/9000 detects. The sys admin can then investigate the issue and take appropriate action.

4.4 If FTP Servers are Compromised

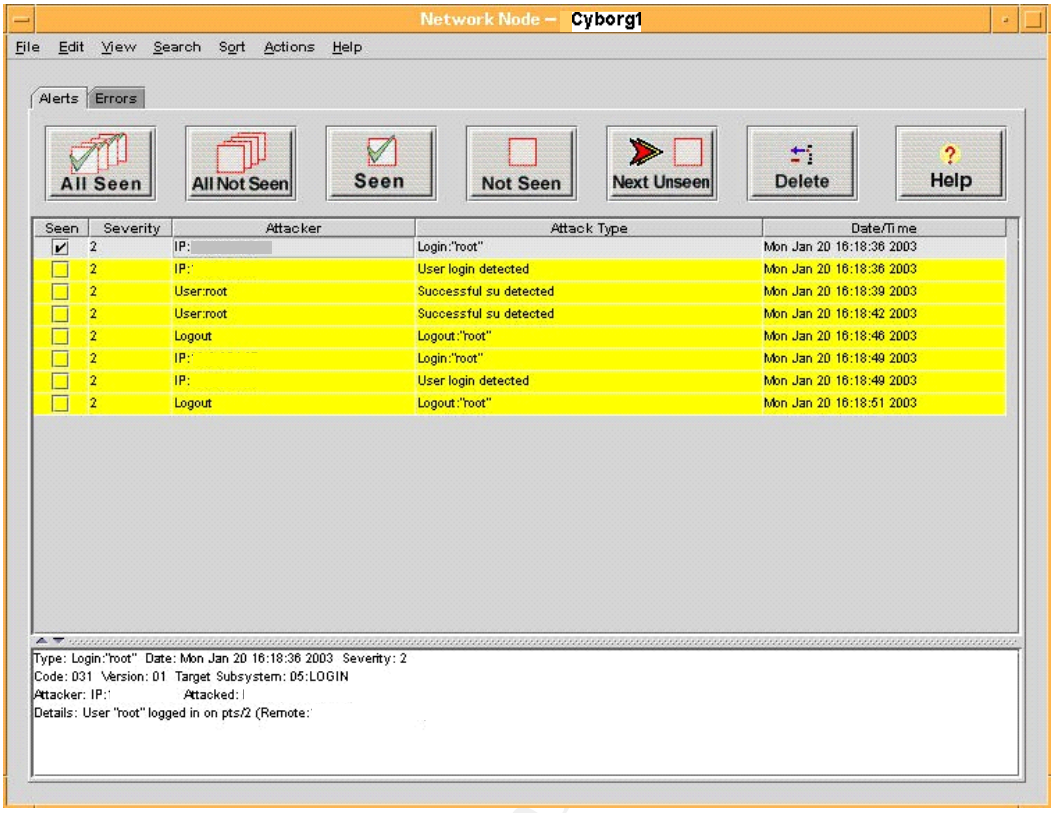
The FTP servers have been thoroughly documented, and an Ignite-UX backup will be created after all security checks are done. In the event the servers get compromised, they can be restored to the original configuration.

4.4.1 Network Node Screen

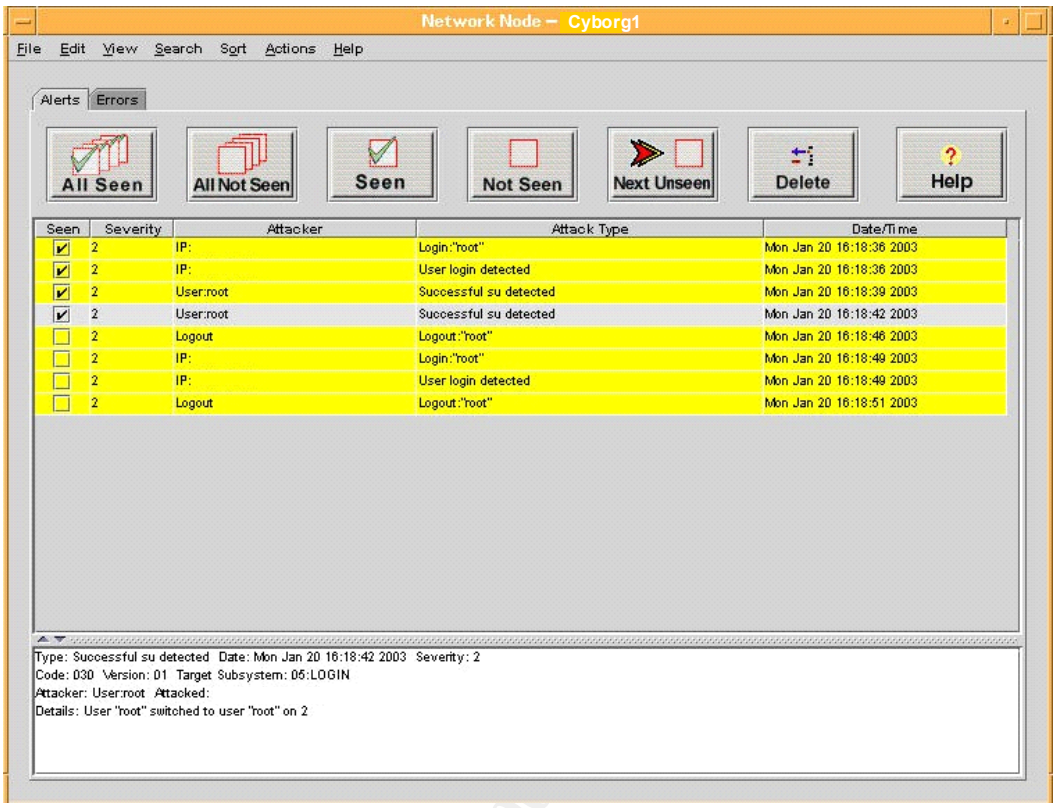
The Network Node Screen tells you what alerts you have for a host. In this screen you can view the details of alerts and then clear the alerts after they have been investigated. To view the alerts for a particular system, double-click on the host name in the System Manager, this will bring up the Network Node Screen for that host:



To see the details for an alert, highlight the alert by clicking on it once and then read the details at the bottom of the Network Node Screen:



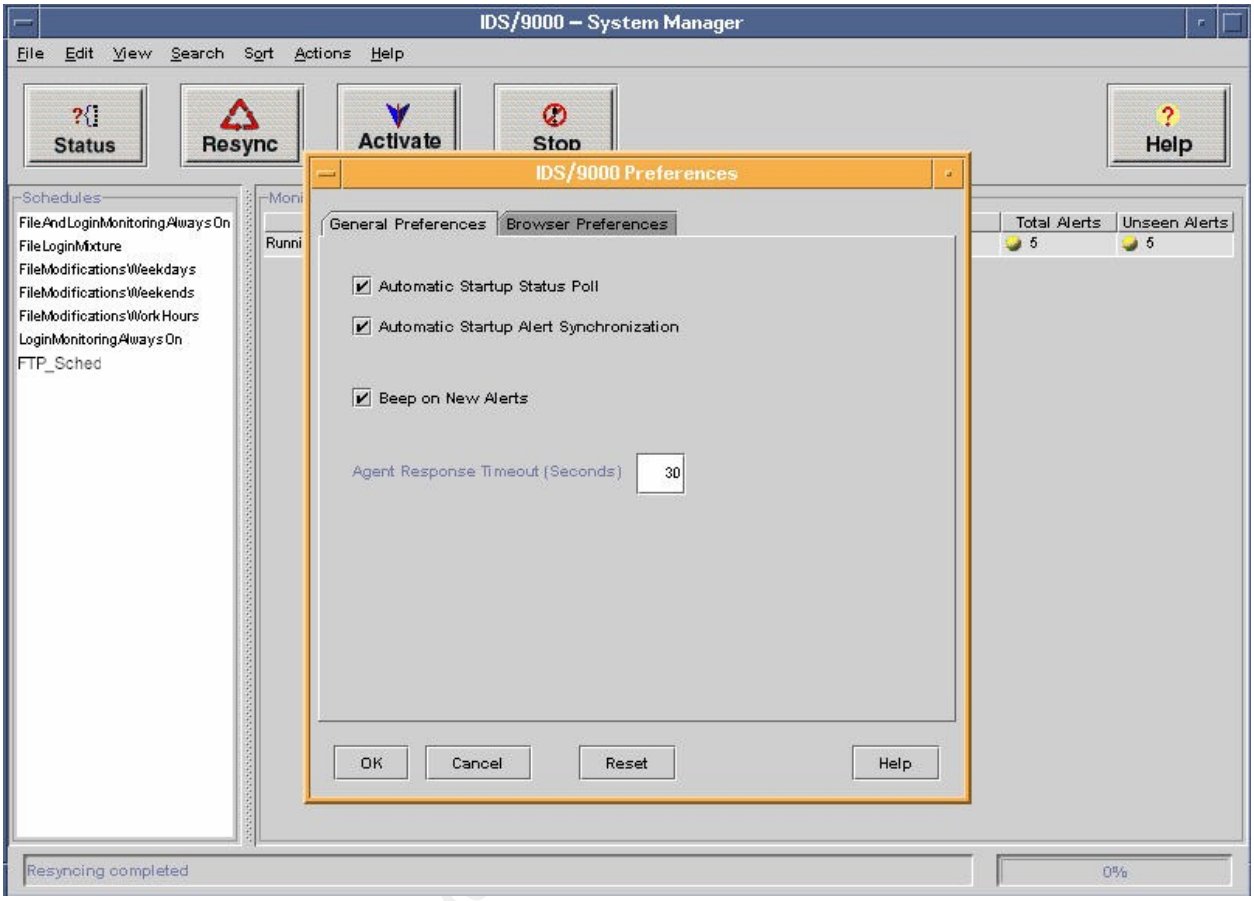
When you have investigated the alert and want to clear it, simply check the box beside the alert and click the Delete button. If you want to keep the alert but mark it as seen but don't want to delete it, check the box and click the Seen button.



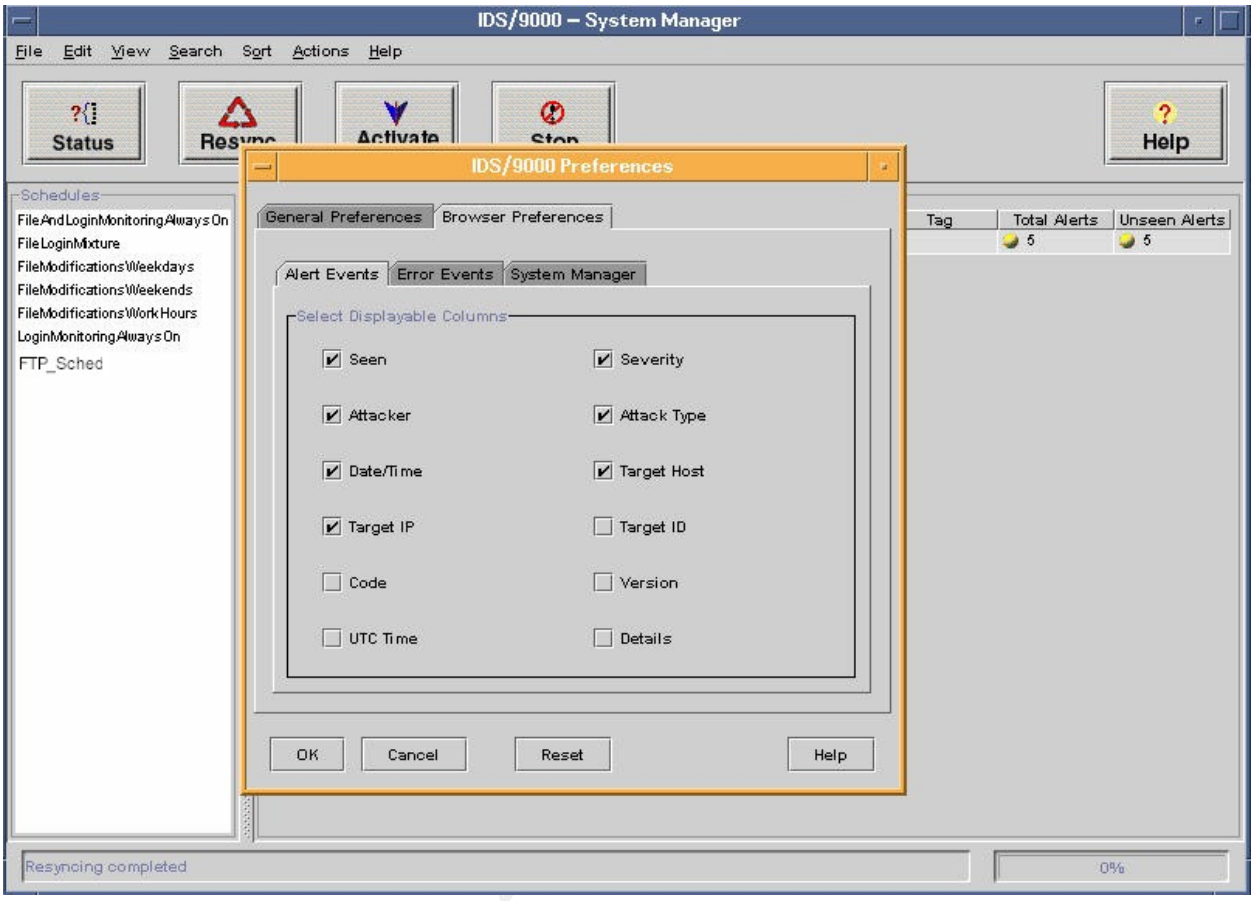
When you are finished you can choose File, Close on the menu bar. This will take you back to the System Manager.

Preferences

You can change the preferences for Event Alerts, Error Events, and the System Manager displays. In the System Manager choose Edit, Preferences from the menu bar.



Then select the Browser tab. You can then choose what events you want displayed on these three displays.



Once you have made the desired changes, click OK.

5 Checking the Configuration

The system was tested for performance and security to minimize risk and ensure functionality. Anytime a kernel change is made to the system I will retest the system. Other tools can be utilized for this purpose:

5.1 Nmap

Nmap is an open-source utility that will scan a network to determine what hosts are available, what services they have available, what operating system and version they are running, and other information. It is a good tool for finding what ports and/or services your system is running and where any vulnerability may lie. You can download this utility at: http://www.insecure.org/nmap/nmap_download.html

I first ran Nmap using "Syn Stealth"

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on  (10.1.1.50):
(The 1595 ports scanned but not shown below are in state: closed)

Port       State       Service
22/tcp     open        ssh
1508/tcp   open        diagmond
2984/tcp   open        hpidsadmin
2985/tcp   open        hpidsagent
6000/tcp   open        X11
6112/tcp   open        dtspc

Remote operating system guess: HP-UX 11 or Apple Mac OS 9.04 or HP-UX
B.11.00
Uptime 0.479 days (since Sun Mar 02 12:22:50 2003)
Nmap run completed -- 1 IP address (1 host up) scanned in 8 seconds
```

These ports are necessary to have open, ssh is our Secure Shell, diagmond is the the Support Tools daemon, X11 is the daemon for dtspc is the daemon for the CDE Subprocess Control service, the X11 daemon is a graphical interface that we need for the IDS/9000 GUI interface, dtspc is the daemon for the CDE Subprocess Control service in response to a CDE client requesting a process to be started on the daemon's host, and the hpidsadmin and hpidsagent are for IDS/9000.

5.2 SUID and SGID Files

I will check to see if any SUID or GUID files are present that don't match what I mounted on my read-only directory:

First run the command and create a file for today's outcome:

```
# find / -user 0 \( -perm -4000 -o -perm -2000 \) -exec ls -ld {} \; >
/var/adm/suid-sgid.today
```

Now compare today's file with the original file:

```
# diff /var/adm/suid-sgid.today /nowrite/suid-sgid.orig
```

There are no differences between today's file and the original file!

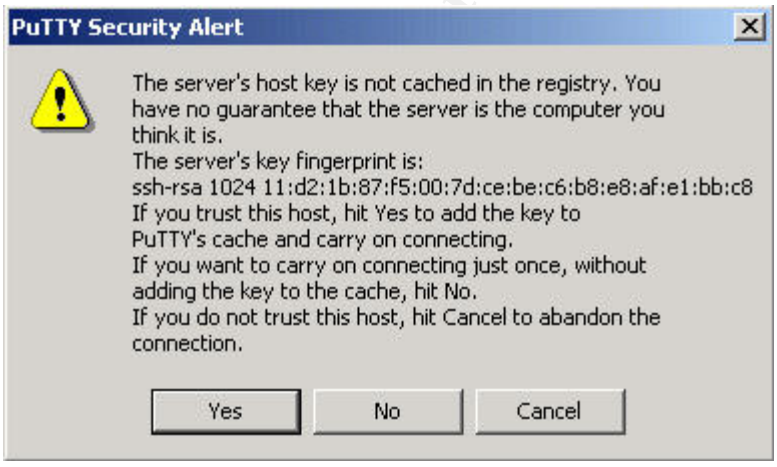
5.3 Connect With SSHv2 Authorized Client

5.3.1 Connecting with SSHv2 Client

First I'll test a valid SSHv2 client. I am using PuTTY for my SSHv2 connection **and** Hummingbird Exceed as my Xclient. Several different PuTTY clients can be downloaded for free from http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

- The PuTTY client is configured to use SSHv2 and X11 forwarding is enabled. (This matches the SSH configuration on Cyborg1.)
- Hummingbird Exceed is configured to use Passive communication.

- I open PuTTY to connect to Cyborg1. The first time I connect I am asked if I want to cache the Security Key:



- I click Yes.

- ✓ The login prompt appears and I login. This is successful; however, I want to make sure I can export the display to my local machine (a Windows 2000 Professional workstation). This feature is needed for IDS/9000 administration.

- I open Exceed and it runs in the background.

- I switch back to PuTTY and export the display to my local machine:

```
# export DISPLAY=10.1.1.40
```

- To test this I will bring up the xclock:

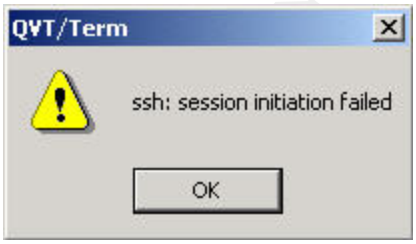
```
# xclock &
```

- ✓ After impatiently waiting a few seconds, the very modern looking xclock displays on my local desktop!

6.3.2

To further test my configuration, I attempt to connect with a QVT/Term SSHv1 client.

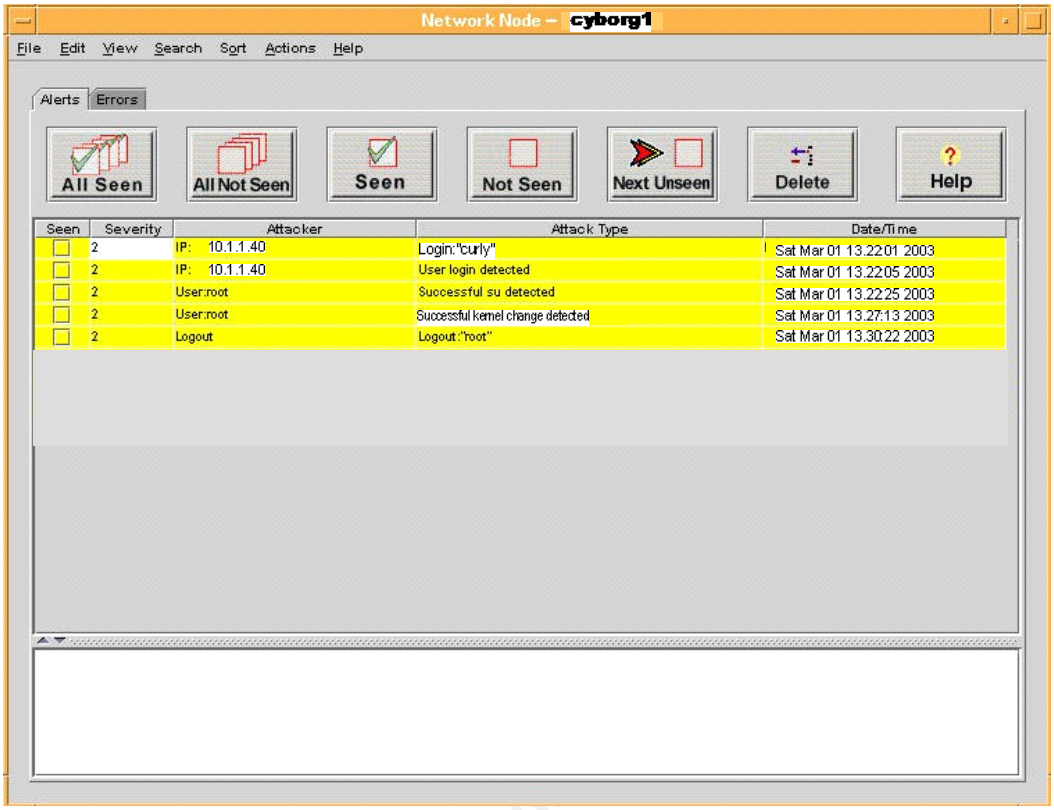
- After attempting to log in I get the following error:



- ✓ This is what I wanted to see, my SSH configuration did not allow a SSHv1 client connect.

5.4 Does IDS Catch a Change in Kernel Binary on CYBORG1

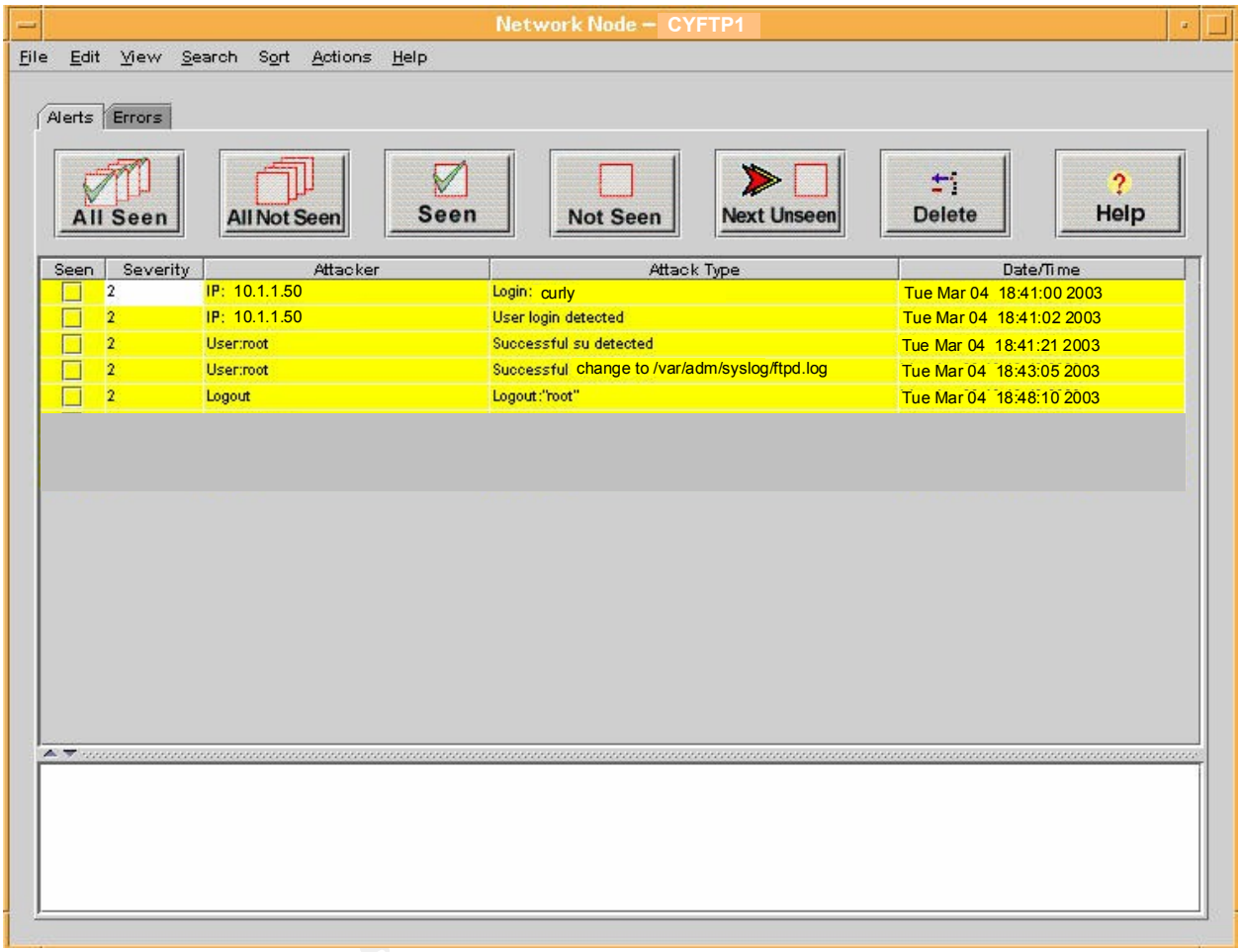
I used SAM on Cyborg1 to change the kernel parameter maxusers from 128 to 200, then checked the Network Node screen in IDS/9000:



✓ IDS/9000 shows a kernel parameter was successfully changed!

5.5 Does IDS See Events on FTP Servers?

To test the IDS/9000 alerts for Cyftp1, I edited the log file /var/adm/syslog/ftpd.log. IDS/9000 has been set to send an alert if this log file is changed rather than appended.



✓ IDS/9000 caught the change and sent an alert!

6 Ongoing Maintenance

6.1 Ignite-UX Backup

Now that the system is configured and secured, run an Ignite-UX recovery backup of vg00. This tape should be put aside in a secure spot, either in a vault or off-site. It can be used to quickly restore the system to its original state after a hardware failure or malicious attack. I also will setup a cron job to run an Ignite back up once a week, using a tape rotation. Here is the command I will use to run the backup and will use for my cron job:

```
# /opt/ignite/bin/make_recovery –A –i /dev/rmt
```

-A This creates a complete bootable backup of the disk or volume group.
-i Causes the recovery process to be interactive during bootup so configuration changes can be made during recovery.

6.2 Physical Security

Critical equipment should be stored in a secure area that is monitored for access, with only authorized personnel allowed. The ideal place would be a dedicated data center that has climate control as well as power redundancy. If at all possible, the data center should not be on the lower level of a building since flooding is a common natural disaster. By simply putting the data center on the second or third floor of a building you can avoid equipment damage from natural flooding.

6.3 Social Engineering

Another issue that needs to be addressed in any business is the concept of “Social Engineering”. This is a term that describes how malicious attackers attempt to gain sensitive information about systems by tricking an employee into giving out the information. For instance, if a person calls the help desk and claims to be a vice president that forgot his or her password, he/she could bully the person into resetting it. Training will help eliminate this problem, as well as a security policy that prohibits resetting passwords based upon a verbal request.

6.4 User Training

Users should receive training in the area of data security, using a well-documented security policy that is supported by the company’s officers. This training should include creating strong passwords, keeping passwords private (e.g. – not writing it on a post-it note attached to their monitor), confidential data security, and acceptable usage of the company’s equipment. Having them sign off on a policy that has been reviewed by the company’s legal council will deter unacceptable usage and help in prosecution should a security breech occur.

6.5 Log Rotation

It is important to implement a log file rotation so that they can be studied in the event of a system problem or compromise. I will run the following script in cron for every night at 11:59pm. This will preserve each day's syslog file with the date appended onto the end.

```
#########################################################
#!/bin/ksh
#Script to save the syslog file for each day
#
#
cp /var/adm/syslog/syslog.log /var/adm/syslog/syslog.log_`date '+%d.%m.%y_%H:%M'`
#
#########################################################
```

These should be cleaned out on a regular basis so as not to fill up /var. I am not going to setup a cron job to delete the files regularly since I will be routinely checking these anyways and will do that manually.

6.6 Subscribe to hp-ux security mailing list or SANS

SANS offers a weekly Critical Vulnerability Analysis Newsletter that alert systems administrators on three to eight critical vulnerabilities and what damage they do. You can sign up at http://server2.sans.org/sansnews

I would also recommend signing up for the CERT/CC Current Activity mailing list and the CERT Advisories mailing list. The CERT/CC Current Activity is a regularly updated summary of the most frequent, high-impact types of security incidents and vulnerabilities currently being reported to CERT. CERT Advisories address Internet security problems. They offer an explanation of the problem, information that helps you determine if your site has the problem, as well as fixes or workarounds, and vendor information. You can sign up for both at: http://www.cert.org/nav/alerts.html#advisories

To receive HP Security bulletins you can go to http://itrc.hp.com and register. Under the Maintenance and Support menu click on "more…" then under Notifications near the bottom choose Support Information Digests.

6.7 Regular Security Patch Checks

The Security Patch Check tool from HP will analyze the system for vulnerabilities that have not already been fixed by other patches on the system. It will generate a report of recommended security patches to install and will warn you about recalled patches that are currently on the system. This tool should be run at least weekly.

1. Download the Security Patch tool (B6834AA) from http://software.hp.com

2. Install the software:

 # SWINSTALL –S CYBORG:/TMP/B6834AA.DEPOT

3. Download the security catalog from: ftp://ftp.itrc.hp.com/export/patches/security_catalog and put it into /opt/sec_mgt/spc/security_catalog directory.

4. Now run the patch check script:

**# /OPT/SEC_MGMT/SPC/BIN/SECURITY_PATCH_CHECK –C **
/OPT/SEC_MGMT/SPC/SECURITY_CATALOG

You should see something similar to the following:

```
*** BEGINNING OF SECURITY PATCH CHECK REPORT ***
Report generated by: /opt/sec_mgmt/spc/bin/security_patch_check.pl,
run as root
```

ANALYZED LOCALHOST (HP-UX 11.11) FROM CYBORG

```
Security catalog: ./security_catalog
Security catalog created on: Sat Nov 23 14:52:48 2002
Time of analysis: Sun Nov 24 21:22:01 2002

List of recommended patches for most secure system:

#  Recommended  Bull(s) Spec? Reboot? Pdep? Description
Security patches are up to date with the security patch catalog used
*** END OF REPORT ***
```

If patches are recommended, download the patches and install them as soon as possible. If patches have been recalled, remove them if it presents a security vulnerability or system stability problem.

The following table shows the recommended patch schedule from HP:

If you want to:	You should Install:	Updated:
Update or install diagnostics and hardware monitors required for supported hardware	Diagnostic bundle: `OnlineDiag`	Quarterly
Install defect fixes for the core OS or the network or graphics drivers included on the OE	Gold Base bundle: `GOLDBASE11i`	Every six months
Install defect fixes for HP-UX OE application software	Gold Applications bundle: `GOLDAPPS11i`	Every six months
Enable new hardware or add-on hardware	Hardware Enablement bundle: `HWEnable11i`	Quarterly
Prepare your server to use new iCOD functionality	iCOD Client Product (from the `OnlineDiag` depot, `B9073AA` bundle)	As needed

WARNING: You should ALWAYS do an Ignite backup of vg00 before applying patches. If a patch causes a problem, you can ignite the system with the backup and restore it to its original state.

6.8 Documentation

A log book should be kept with any changes made to the system configuration. This will aid in troubleshooting, and can help other systems administrators to be able to pick up where someone else left off. It can also help in restoring a system after a disaster or security breech.

The End!

Appendix A

References

The references below were used for the following subjects as well as other parts of this paper.

INIT: Command is respawning too rapidly.

- http:/itrc.hp.com - document id:USAMKBRC00007275

Delete Unnecessary Groups

- http://rr.sans.org/unix/HP-UX11.php

Protecting Programs from Illegal Execution

- Managing Systems and Workgroups: A guide for HP-UX Systems

HP Secure Shell (SSH)

- www.cert.org/advisories/CA-2002-18.html
- http://www.docs.hp.com/hpux/onlinedocs/T1471-90002/T1471-90002.html
- Maarteen Hartsuijker - Securing Unix Step By Step – Secure mail gateway

Security Banner

- Building and Installing OpenSSH on HP-UX by Kevin Steves http://www.atomicgears.com/papers/osshhpux.html)

Sendmail

- Walt Jones – HP Security Engineer, CISSP
- http://www.cert.org/tech_tips/usc20.html#8.1

Installing & Configuring IDS/9000

- HP Intrusion Detection System/9000 Administrator's Guide: www.docs.hp.com
- HP Intrusion Detection System/9000 Release 2.1 Release Notes

Wu-FTP

- Chris Wong book

Regular Security Patch Checks

- http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA

Securing the OS Checklist:

- http://www.cert.org/tech_tips/intruder_detection_checklist.html
- http://www.cert.org/tech_tips/usc20_essentials.html

Trusted System

- http://docs.hp.com/cgi-bin/fsearch/framedisplay?top=/hpux/onlinedocs/B2355-90742/B2355-90742_top.html&con=/hpux/onlinedocs/B2355-90742/00/00/60-con.html&toc=/hpux/onlinedocs/B2355-90742/00/00/60-toc.html&searchterms=hp-ux%7csecurity&queryid=20020909-204153

SSH

- HP-UX 11i Security, by Chris Wong
- http://newfdog.hpwebhost.com/bookupdates/article.nhtml?uid=10010

TCP Wrappers

- HP doc: 5969-4315.pdf

Monitoring the FTP Machines:

- http://www.cert.org/tech_tips/anonymous_ftp_abuses.html
- http://www.cert.org/tech_tips/usc20.html#6.0

John the Ripper

- HP-UX 11.0 Installation and Security Verification, by Theodore Ellis

HP Patch Schedule

- www.docs.hp.com/hpux/pdf/5967-3578.pdf

Appendix B

IDS/9000 Configuration for Cyborg1

Buffer Overflow Attacks

Changes to Log Files

/var/adm/btmp	/var/adm/wtmp
/var/etc/bmp	/etc/wtmp

Syslog files:

/var/adm/messages	/var/adm/syslog/mail.log
/var/adm/syslog/syslog.log	

The file that tracks commands that a user executed and the timestamp:

/var/adm/pacct

The file that tracks the su command and the timestamp:

/var/adm/sulog

Creation of World-Writable Files

root	daemon
bin	sys
adm	uucp
lp*	nuucp

* *Users in RED indicate deleted users*

Modification of Another User's Files

All files are tracked by default, no changes here.

Modification of Files/Directories

System Kernel and Configuration Files:

/stand/vmunix	/stand/kernel
/stand/bootconf	

Files Pertaining to Users:

/etc/passwd	/etc/group

Network Services:

/etc/inetd.conf

Files Pertaining to Remote Root Access:

/.rhosts	/.shosts
/etc/hosts.equiv	

Property: `Ignore these files`

Temporary files pertaining to vipw but are not used in system configuration:

/etc/.pwd.lock	/etc/ptmp
/etc/utmp	/etc/utmpx

Property: `Watch these directories for modification`

Directories that contain system binaries:

/lib

Software package directory:

/opt

System configuration files:

/etc

Kernel configuration files:

/stand

My Additions:

/tcb – *(created when converting to a trusted host)*

Monitor Logins/Logouts

All users are monitored by default – no changes.

Monitor Start of Interactive Sessions

root	ids
news	www
adm	bin
daemon	hpdp
lp	nuucp
sys	uucp

Race Condition Attacks

root	bin
adm	hpdp
daemon	nuucp
lp	uucp
sys	

My Additions:

Added user *ids* to the list.

Repeated Failed Logins

Property: Number of failures to exceed
Default: 2

Changed Default to 3

Repeated Failed su Commands

Keep defaults

Creation of SetUID Files

root	daemon
bin	sys
adm	uucp
lp	nuucp

My Addtions:

idsuser

Monitor Start of Interactive Sessions

root	ids
news	www
adm	bin
daemon	hpdp
lp	nuucp
sys	uucp