Global Information Assurance Certification Paper

Hp-Ux 10.20 From "Out Of The Box" To Secure

Melanie Corn

SANS Security Essentials Version 1.2e

Operating System Install

In the initial install DHCP is set to configure automatically. This needs to be disabled. under "Advanced Options" of the HP-UX Installation/Recovery window. When installing HP-UX make sure you mark the machine as not networked during the installation process. When prompted for interaction with SD-UX *swinstall* answer yes. This allows for additional software components. It is important to only install the components needed. Even a minimal system install provides services that are insecure. After the install if there are packages that you found are not needed remove them with *swremove* command.

Patch install

HP-UX patches are components of the software that are released by Hewlett-Packard. Patches perform three functions. They add functionality to the operating system or products. Support for new hardware like new types of adapters, and bug fixes to applications and the operating system. The naming convention of the patches helps to identify the different types of patches. All patches start with PH. The next two characters are the types then an underscore with the patch number. These are the following types:

CO - Command patches
KL - Kernel patches
NE - Network patches
SS - Subsystem patches. These include all other types of patches

Example of patch names is PHSS_1643, PHCO_1562, and PHKL_16189. To get a listing of currently installed patches type:

```
$ swlist –l product PH*
```

To get a starting point list of patches needed, go to http://us-support.external.hp.com/wps/bin/doc.pl/sid=935085901d233df01f. You will need to login. Select "Security Bulletins" under "HP-UX Software" Search By Keyword -10.20 Security patches. To acquire the security patches go to same location as above. All patches are distributed as "shar" files. Once they have been down loaded, the *sh* command will need to be run to unshar them.

```
$ sh PHSS_*****
```

The output of the *sh* command will be patchname.text and patchname.depot (compressed). The *.text file is the description and the *.depot file is the actual patch in SD-UX (Software Distributor) depot format.

Once the patches have been unshared a patch depot will need to be created. The depot can be stored in /var/spool/sw or /var/adm/sw/patch. To add the patches to the /var/spool/sw depot type the following:

```
$ swcopy –s PH**_****.depot PH**_**** @ /var/spool/sw
```

To install type:

```
$ swinstall –s /var/spool/sw
```

This will list the patches that are present in this depot in the swinstall window. Make the desired selection and then install.

Disabling network services

Network services are started two ways. One way is starting the service daemon at start up through "rc" run command scripts. They are located in the /sbin/init.d directory. In the /sbin/rc[0-4].d directories are links to the scripts. Each rc[0-4].d directory corresponds to a system run level. Remove any startup scripts not needed. From the /sbin/rc2.d directory make sure to remove the following: S540sendmail, S560SnmpMaster, S565SnmpHpunix, S565SnmpMib2. Also make sure all startup scripts have the following permissions.

-r-xr-xr-x 1 bin bin 8099 Jun 10 1996 net

```
$ cd /sbin/init.d
$ chmod 555 *
```

The other way is through the inetd daemon. At startup the daemon read it's configuration file /etc/inetd.conf which list the services to be served by inetd. The /etc/services file maps the service name with the corresponding port number and protocol. In each of these files comment out each service by placing a # in front of the line. The following lines should be commented out of the /etc/inetd.conf file:

```
bootps chargen comsat discard daytime echo dhcp_bootp finger name netstat
ntalk rexd rstatd rquotad rusersd shell sprayd systat talk time tftp uucp
walld /usr/sbin/rpc.rexd /usr/lib/netsvc/rstat/rpc.rstatd
/usr/lib/netsvc/rusers/rpc.rusersd /usr/lib/netsvc/rwall/rpc.rwalld
/usr/sbin/rpc.rquotad /usr/lib/netsvc/spray/rpc.sprayd
/usr/dt/bin/rpc.ttdbserver
```

In the /etc/services file comment out the following:

```
bootps bootpc chargen daytime finger ingreslock ntalk smtp snmp talk time
route tftp uucp
```

Installing TCP Wrapper

Another security precaution is installing the tcp wrapper program that allows you to monitor and filter incoming requests for services started by inetd. Download from ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.tar.gz

```
$ gunzip tcp_wrappers_7.6.tar.gz
$ tar xvf tcp_wrappers_7.6.tar
```

This will automatically create a subdirectory tcp_wrappers_7.6.

An update to the Makefile will have to be made first before building the binaries.

Replace the following line

```
FACILITY= LOG_MAIL        # LOG_MAIL is what most  sendmail daemons use
```

With the following:

```
FACILITY= LOG_DAEMON     # LOG_MAIL is what most  sendmail daemons use
```

To build the binary type the following:

```
$ make REAL_DAEMON_DIR=/usr/sbin hpux
```

After completion, copy all the programs and man pages to the correct system directories:

```
$ cp tcpd /usr/sbin
$ cp safe_finger /usr/sbin
$ cp tcpdchk /usr/sbin
$ cp tcpdmatch /usr/sbin
$ cp try-from /usr/sbin
$ cp hosts_access.3 /usr/man/man3
$ cp hosts_access.5 /usr/man/man5
$ cp hosts_options.5 /usr/man/man5
$ cp tcpd.8 /usr/man/man8
$ cp tcpdchk.8 /usr/man/man8
$ cp tcpdmatch.8 /usr/man/man8
```

Copy the library files over.

```
$ cp libwrap.a /usr/lib
$ cp tcpd.h /usr/include
```

Once the program is installed you will need to modify the inetd.conf to use the tcp wrapper daemon.

```
$ cp /etc/inetd.conf /etc/inetd.conf.bak
$ vi /etc/inetd.conf
```

Modify server_pathname in inetd.conf with /usr/sbin/tcpd for programs that support tcp wrapper.

You can configure tcp wrapper using two files /etc/hosts.allow and /etc/hosts.deny files. The man pages for hosts_options (3), hosts_options (5), and hosts_access (5) give more information. The README file that is included in the tcp_wrappers_7.6.tar file gives additional configuration and setup information.

FYI: The tcp wrapper program does not protect against all network daemons. Only those that use the TCP and UDP protocols.

Monitoring the System

On a regular basis the system should be monitor for any security violations. UNIX provides several commands, programs, and log files that can be used. The following are just some of the things to check.

The /etc/passwd file should be checked that all accounts are protected with a password.

```
$ egrep  :: /etc/passwd
```

Searching for programs and files that have the s-bit set as a permission. These are programs that allow users to execute under the owner or group of the program verses their ownership. With the *find* command a whole file system can be checked.

```
$ find  / -perm -4000 -print
```

The *ps* command shows processes that are currently active and provides a way to check to make sure nothing is running that shouldn't be.

```
$ ps -ef  | more
```

The *who* command can be used as checks on the system to see who is logged in, what times and for how long.

```
$ who
```

The *whodo* command combines the functionality of the *who* and *ps* command on a user. This will tell you how many times a user has been logged in, what terminal, and for how long. It will also tell the last input and run time consumed by its processes.

```
$ whodo
```

Enable the audit subsystem and make sure it is configured correctly.
Invoke SAM (System Administration Manager),

```
$/usr/sbin/sam
```

Select "Auditing and Security"
Select "Audited Events"
Options: admin, login, modaccess, moddac
Select "Audited Users"
Enabled for all users

Verify that syslogd daemon is running.

```
$ ps -ef | grep syslog
```

The output should be

```
root   364     1  0  Mar  4  ?         0:08 /usr/sbin/syslogd -D
```

The /etc/syslog.conf should contain:

```
mail.debug              /var/adm/syslog/mail.log
*.info;mail.none        /var/adm/syslog/syslog.log
*.alert                 /dev/console
*.alert                 root
*.emerg                 *
```

Preventive Measures

There are certain files that are used in a network environment that increase the risk of attacks. Disabling them or using them carefully will decrease the security risk.

The /etc/hosts.equiv, this file allows users to remotely login to another host without supplying a password. The /.rhosts file allows the hosts that are named in the /.rhosts file to remotely login with out a password to the host where the /.rhosts file resides. The last file /etc/hosts.lpd allows hosts to remotely log in where a printer resides.

If any of these files are needed make sure that a "+" entry is not in the file at all. A "+" in the file has the effect of making every host a trusted host. Make sure there are no comment lines or lines beginning with "!" or "#". These special characters can create vulnerabilities. The files should be owned by root and the permissions are set to read and execute for owner and not for group and world.

```
-rw-r--r--   1 root       sys            48 Nov  16 1999  /.rhosts
-rw-r--r--   1 root       sys            1034 Dec 29 13:56   /etc/hosts.equiv
```

The "r" commands (rlogin, rsh) have been a regular source of insecurities and attacks. This increases the risk of password exposure in a network. Disabling them is the most secure way, but if they are needed make sure that the latest more secure versions are running. An alternative is "ssh" in place of rlogin/rsh. It can be found at http://www.ssh.com/.

Other concerns are the use of NFS (Network File Systems). In the /etc/exports file, share the directories as read-only to make sure that the data will not be corrupted. If a file system needs to be exported with read and write privileges specify the hosts that need access. Example of /etc/exports

```
/data -access=host1:host2:host3
/home -rw=host1:host2:host3
```

After modifying /etc/exports run:

```
$ exportfs -a
```

Permissions and ownership for the /etc/exports file should be:

```
-rwxr--r--   1 root       sys            2702 Jun  6 08:31 /etc/exports
```

Backups

No one can predict an attack on a system. If data has become corrupted or lost, backups are used to recover lost data. There are three types of backups, a day-zero, a full backup, and the incremental. A day-zero backup is a complete copy of the system after initial installation. This backs up every file and program on the system. A full backup saves every file on a file system. This is the same as a day-zero backup but this is done on a regular basis. The last is the incremental backup. This saves only the files that have been modified since a particular date, usually the last full backup. The different types of backups should go hand in hand. The following backup schedule seems to work on most systems. Perform a full backup the first weekend of the month. Perform incrementals on a daily and weekly basis. Keep the weeklies for the month and the full backups (monthlies) for a full quarter or up to a year. All backups are stored on magnetic media. Usually some form of a digital tape.

There are many commands that can be used to perform backups. Each has their place. The common ones are *tar*, *cpio*, and *dump/restore*. By reading the man pages you can determine which is right for the situation. Just remember to test for recovery when the backups are implemented.

The storage location for the backups is just as important as running the backups themselves. The media should not be kept in the same location as the computer system. If the data is classified, security reasons prevent the tapes being stored just anywhere. Safes in off-site locations are the best bet. Remember to provide a safe that is designed for magnetic media.

Helpful sites

The following are helpful site to go for further information to secure the system.

HP-UX internet and security solutions	http://docs.hp.com/hpux/internet/
Cert Advisories	http://www.cert.org/advisories/
Hewlett Packard HP-UX Security Checklist	http://afcert.kelly.af.mil/hpcheck.html

References

Hewlett Packard "hp-ux 10.x operating system." 1994-2000 < http://www.docs.hp.com/hpux/os/10.x/index.html>

"Unix Security Handbook - HP-UX 10.20" <http://secinf.net/info/unix/secureHP-UX.html>

Carnegie Mellon University. "Installing, configuring, and using tcp wrapper to log unauthorized connection attempts on systems running Solaris 2.x." 2000 <http://www.cert.org/security-improvement/implementations/i041.07.html> (1 March 2000)

Carnegie Mellon University. "Disabling network services on systems running Solaris 2.X." 2000 <http://www.cert.org/security-improvement/implementations/i049.03.html> (9 January 2001)

Garfinkel, Simson, and Gene Spafford. "Practical Unix & Internet Security." Sebastpol: O'Reilly & Associates, 1996.

Rehman, Rafeeq Ur. "HP Certified HP-UX System Administration." New Jersey: Prentice Hall PTR, 2000