Global Information Assurance Certification Paper

Fernando Espinoza Salas
GSEC Practical Assignment
Version 1.2e
July 28, 2001

Securing HP-UX Services

Introduction

I found two documents about security of HP-UX on the GIAC web site:

Securing HP-UX 11 by Larry Harker
Building a Bastion Host Using HP'UX 11 by Kevin Steves

Both document show how to secure Hewlett Packard UNIX server, (disabling services). But what happen, if you need those (unsecured) services, as: NIS, FTP, TELNET and use of modems. This paper shows some procedures to improve the security of these services. And other characteristics of HP-UX 11 than help to make more secure servers.

Modem security

It is important to implement security procedures for modem. People use modems to transmit user names and password. System administrators need to ensure the modems are installed and behave properly.

Implement dial-back system

Dial-back system require the caller to enter a user name, and then immediately hang up the telephone line, The modem calls the caller back on a predefined telephone number.

Typically, an answering modem with dial-back capability responds to a call by taking the following steps:

1. Challenges incoming callers with a prompt string.
2. Accepts the input identifying the caller.
3. Hangs up the call.
4. Calls a number associated with the caller's identification.
5. Re-establishes a carrier.

You cannot use the internal modem of a HP-9000 K-class (identifies to at-commands as "MT1432HP"): because it's not callback capable.

Usually all the external modem support call back. HP use Multitech modem, you may want to look for the manual on www.multitech.com they described the call back process. ftp://ftp.multitech.com/Manuals/Text/Modems/ZDX_MAN.TXT

PPP supports the ability to maintain a connection when calling a modem that has a dial-back security feature. The Systems file chat script option \M allows this by disabling delivery of

SIGHUP to pppd. This signal usually results from loss of Carrier Detect and tells pppd to abruptly disconnect from the active session.

The calling modem might then demand the same type of identification before allowing remote data to flow through its serial interface to the local system.

Blocking SIGHUP with Chat Script \M Option
The calling system's pppd must be prepared for the temporary lack of a Carrier Detect signal from its modem during the dial-back from the remote modem. To avoid receiving a SIGHUP, pppd instructs the UNIX system's serial drivers not to deliver the signal. In other words it says, "Temporarily treat the serial interface as if it were connected to a local device like a terminal or printer, instead of a modem." pppd does this by specifying \M in the 'send' phase of a Systems chat script. See http://www.docs.hp.com/hpux/onlinedocs/B2355-90137/B2355-90137.html for more information.

Reversing Instructions with \m Option
After the disconnection period, through the 'send' phase option \m, pppd tells the system's serial drivers to reverse the first instruction and respect the modem's full variety of control. For example, to dial into a system protected by a dial-back modem, the Systems chat script might be written like this:

```
# This connects to a system protected by  a Modem callback
# modem
# with S46=2.
#
   server  Any  ACU  38400  19071234567  TIMEOUT  60  \
   ENTER\sPASSWORD:  my_modem_password\M \
   ENTER\SPASSWORD:  my_modem_password\m \
   login:  my_login_name password:  my_login_password
```

Enable Dial-up security
Dial-up security requests the user for two passwords. It can be applied to any terminal or modem port on a port-by-port basis. The first password requests the user's password, the second is a password based on the user's default shell

Determine which device files are associated with the device you wish to secure, use the command
ioscan –funC tty

Add the following lines to /etc/dialups:
/dev/tty0p0
/dev/tty0p3

Add the following lines to /etc/d_passswd:
/usr/bin/sh:"encrypted_password": Comment field.

Each line in /etc/d_passwd consist ot three fields separated by colons. The first field is the command name, matching an entry in /etc/passwd. The second field es the encrypted password to be used for dialup security for those users logging in to use that program. The third field is commentary. The colon is requires as a delimiter.

Use the following program to encrypt a password.

```
#include <stdio.h>
main )argc,argv)
int argc;
char **argv;
{
      char salt=”dp”;/ use your own salt */
      printf (“%s”, crypt (argv[1]. Salt));
}
```

Compile the program and then run it at the command line:

```
cc program_name.c –o program_name
./program_name test_password
```

Record the resulting output in the second field of /etc/d_passwd:

Log off all inactive sessions of direct connect terminals.
Use TMOUT shell variable for shell sessions.
Edit $HOME/.profile
Add the following line: TMOUT=300 #log off after 5 minutes

Dial Tone Playbacks
If you use a line for dial-in and dial-out purposes. A hacker calls to the system, he cannot get into the system and the system hangs up. The hacker does not hang up. The system decides to call out. The hacker plays a dial tone into the receiver. The system hears the dial tone, thinks it has a made a connection, and the hackers is in.

One ways to foil these kinds of attacks is to have two modems, one for dial-in and one for dial-out.

Configuring modems for hang-up
One security breach related to modems is configuring the modem with no hangup. This causes the processes running on the modem port to remain active even though the modem connection has been severed. The next time any user calls the modem port, he or she will inherit (and control) all processes on that port, even though they may have nothing to do with the user who started the process.

There are a number of test and configuration checks, which should be performed, to ensure the modem is configured properly.

By default, the getty process started on the modem port automatically performs a hang-up. If the

–h options is specified, then the modem will not hang-up and will terminate the user processes. Never use the –h option with the getty command when setting up a modem port. This option will cause processes running on the modem port to remain active even if the modem connection is broken. This means when somebody else calls the computer, they will be able to run commands as a legitimate user, without ever having to log in.

To test the modems configuration, you will need another computer or terminal with a second modem to call your computer.

1. Call your computer. Log in as usual. Type tty to verify your serial line port. Log off. The computer should hang up the phone
2. Call your computer back and log in a second time. This time, hang up the telephone by pulling the telephone line out of the originating modem. This simulates having the phone connection broken accidentally. Call the computer back on the same telephone number. You should get a new login prompt. You should not be reconnected to your old shell; that shell should have been terminated when the connection was broken.

Securing FTP

Enable the ftpd daemon to record all login attempts through FTP to the /var/adm/syslog/syslog.log file. This is done by appending the –oil option to the ftpd executable in the /etc/inetd.conf file:

```
ftp stream tcp nowait bin  /usr/lbin/ftpd ftpd –oil
```

Use the /var/adm/inetd.sec file to limit FTP access to selective hosts, and use the /etc/ftpusers file to deny FTP access to selective user accounts.

The /etc/ftpusers file should deny FTP access to all accounts that do no belong to an actual human being. Accounts like uucp, news, bin, sys, and even root should be specified in this file so hackers on remote systems cannot use these accounts to anonymously access and transfer files from the system.

Do not allow users to use the $HOME/.netrc file to store account names and passwords. Hackers will often search the system for these files and use the information stored in these files to gain further access to other systems on the network.

Periodically search user's home directories and verify that they are not using the file $HOME/.netrc.

```
ll /home/*/.netrc
```

Also you can use the following command to find all user HOME directories that are writeable by other users

```
Find `awk –F : ' {print $6}' /etc/passwd` -prune –perm –022 –exec
ls –ld ' {}' \;
```

Securing NIS

Limiting access to the NIS Master Server

By default, the master server uses /etc/passwd as the passwd map source. If all home directories are available on the master server, all users can log into the master server. If you want to restrict access to a smaller set of users than defined by the complete /etc/passwd, perform the following steps on the master server:

1. Create an alternate password file as source for the passswd map.
   cp /etc/passwd /etc/passwd.nis
2. Reduce the /etc/passwd file (i.e remove users) and add escape entries
   use the command vipw
3. Edit /etc/rc.config.d/namessvrs and modify YPPASSWDD_OPTIONS. Change to:
   YPPASSWDD_OPTIONS="/etc/passwd.nis –m passwd
   PWFILE=/etc/passwd.nis"
4. Stop and activate NIS server functionality:
   /sbin/init.d/nis.server stop
   /sbin/init.d/nis.server start
5. Edit /var/yp/make and modify PWFILE. Change to:
   DIR=${DIR:-/etc}
   PWFILE=${PWFILE:-$DIR/passwd.nis
6. Rebuild and propagate then new passwd maps
   /var/yp/ypmake passwd

Limiting Access to NIS Client

When a user logs into a NIS client running HP-UX 11.00, the /etc/nsswitch.conf file is referenced to determine the source for the user login.

The following entry in the /etc/nsswitch.conf file:

    passwd: files nis

instructs the system to search the local /etc/passwd file first for the login name, and if it is not found, to search the NIS passwd map.

Using this approach, there is no easy way to limit or restrict a certain login just to the local /etc/passwd file. Either logins receive access to the NIS passwd map, or none of the logins receive access to the map.

Previous versions of HPUX (10.XX) used a plus (+) symbol to indicate when to reference the NIS passwd map. The HP-UX 11 use the passwd entry into he /etc/nsswitch.conf file as the recommended method for managing the different password sources.

However, for backward compatibility, the plus (+) sign still can be used in the /etc/passwd file if the /etc/nsswitch.conf file contains the compat value in the passwd entry. An example of this in the /etc/nsswitch.conf file is:

    passwd: compat

The advantage of using a plus (+) sign in the /etc/passwd file is system administrator can indicate which user accounts are, and which are not to reference the NIS passwd map. This provides the

advantage of allowing all NIS logins on certain system (like a pool of shared workstations), but only certain NIS login on other system (like only the DBA accounts on the database servers).

Verifying the NIS server IP address.
One feature on HP-UX specifiec to NIS security is the /var/yp/secureservers file. This file can be used by NIS client to specify a list of valid IP addresses (i.e. NIS servers) for which the client can bind. This file helps to eliminate the threat of a client binding to unauthorized, rogue NIS servers.

The syntax of the /var/yp/secureservers file is a list of IP addresses for which the NIS client can bind.

```
cat /var/yp/secureservers
255.255.255.255 192.1.1.1       #bind to server with IP 192.1.1.1
255.255.0.0 128.1.0.0           #or any server on the 128.1 subnet
```

Excluding unauthorized clients from the domain.
Similarly, to /var/yp/secureservers the file /var/yp/securenets can be used to protect an NIS server from binding to an unauthorized NIS client.

The NIS server uses the securenets file to specify only authorized NIS client IP address. Then when the hacker system tries to bind to the NIS server, the server will reject the bind request due the hackers IP address not being listed in the /var/yp/securenets file.

The syntax of the /var/yp/securenets file is a list of authorized client IP addresses:.

```
cat /var/yp/securenets
255.255.255.255 192.1.1.1       #allow client with IP 192.1.1.1
255.255.0.0 128.1.0.0           #or any client on the 128.1 subnet
```

Other methods for improving NIS security are:
- Use NIS /etc/netgroups to manage access list of users
- Use ypbind -s on NIS client to ensure binds to secure ports
- Don't allow RPC traffic across your firewall.
- For better security, use NIS+

Telnet
If telnet is configured to display a banner, the hacker is able to gather system type, operating system name, and operating system version information.

Disable the telnet banner
Edit /etc/inetd.conf
Search for the telnet entry
Append –b to the end of the line, so the line ends witch telnetd –b
Execute the inetd –c command

Or you can replace the standard telnet welcome banner with a warning message.

vi /etc/telnet.msg
UNAUTHORIZED USE PROHIBITED!
VIOLATOR WILL BE PROSECUTED TO THE FULL EXTEND OF THE LAW

vi /etc/inetd.conf
telnet stream tcp nowait root /usr/lbin/telned telnetd –b /etc/telnet.msg

Customize the /var/adm/inetd.sec file to selectively allow or deny telnet access to various hosts on the network.
Telnet allow 128.1.*.* 128.2.1-8.* host1 host2 host3 host4

Continually monitor the syslog and /var/adm/btmp file for failed telnet login attemps.

Sendmail
The hacker uses telnet to the sendmail port, socket 25. The sendmail program responds with version information. Once a telnet connection is established, the hacker can use the vrfy command to guess user login ID's.

Disable the vrfy command of sendmail program
Edit /etc/mail/sendmail.cf
Search for the PrivacyOptions text
Add the line "O PrivacyOptions=novrfy" to disable the vrfy command
Stop the send mail daemon with /sbin/init.d/sendmail stop
Restart the sendmail daemon with /sbin/init.d/sendmail start
Verify the vrfy command has been disabled.

Finger
The hacker uses telnet to the finger socket, 79. Once connected, the hacker can enter a user ID and get the information from finger. Normally finger runs on the local system. A hacker can find out who is logged onto a remote machine by typing:
finger user@server.com

Edit /etc/inet.d.conf
Comment out the fingerd entry
Execute the inetd –c command for the change to take effect
Verify the finger command is disabled.

Or you can replace the finger executable with a shell (or command) which prints a message to the client's screen instructing them how to contac the system administrator if they need help or have questions

vi /etc/finger.msg
UNAUTHORIZED USE PROHIBITED!
TO CONTACT SOMEONE AT HP, CALL 111-1111

vi /etc/inetd.conf
Finger stream tcp nowait root /usr/bin/cat cat /etc/finger.msg

The /etc/issue file should be blank or non existent, After login, a warning message should be echoed each time a user accesses the system through any access method.

File system
Access Control List
ACL provide a mechanism in which separate file access privilegess can be defined for separate users ans separate groups.

With ACLs, in addition to being able to define file access permissions for the owner, group, and all others, an additional 13 file access permissions can be defined for other users and other groups.

Traditionally ACL only work fine with HFS file system, but with HP-UX 11 you can use ACL in JFS (journal file system). You need HP JFS 3.3 and HP Online 3.3 Veritas File System 3.3.
You can found more information in http://www.docs.hp.com/hpux/onlinedocs/B3929-90011/B3929-90011.html

The following example show how to interpret the output of the lsacl command:
lsacl myfile
(nathan.adm,rw)(monica.%,rw-)(%.users,r—)(%.%,---).

Where the above is interpreted as:
(nathan.adm,rw) nathan, while in the group adm, has read-write permission on myfile
(monica.%,rw-) monica,while in any group (%),has read-write permission on myfile
(%.users,r--) Any user (%) in group users have read permissions on myfile
(%,%,---) Any user (%) in any group (%) has no permissions for myfile.

The find command supports the -acl option, which specifies that file containing ACLs are to be found
find /home -acl opt

If you execute the ll command.:
ll myfile
-rw-----+ 1 monica users 121 Mar 15 3:33 myfile
where the plus symbol (+) show the use of ACL

The chacl command allows file permissions to be granted or restricted to specific users or groups:

chacl “(%,bio,r--)” myfile	add a ACL to myfile
chacl -d “(%.bio,r--)” myfile	delete an existing ACL
chacl -r “(%.users,r-w)” myfile	replace all existing ACLs on a file.
chacl -f myfile myfile1	copy ACL from a file to another
chacl -z myfile	zapped the ACL from myfile

IF using the chmod command on a file that has an ACL associated with it, be sure to use the -A option. IF the -A option is not used, chmod will change the mode on the file to whatever is specified and it will delete the any additional access control list.

You can found more information in http://www.docs.hp.com/hpux/onlinedocs/B3929-90011/B3929-90011.html

Verify integrity of Software.
In HP-UX the swverify command is used to verify the integrity of files installed with Software Distribuitor. An entire product can be verified, or a selected fileset, or even just a specific file.

Swverify compare file characteristics defined in the IPD database (under /var/adm/sw/products) with files in the file system.
Example:

```
swverify SecurityMon. SECURITY
tail -25 /var/adm/sw/swagent.log
```

Swverify command only verifies software installed via SD-UX (software distribution system of HP), it will not detect changes in user data files or in files associated with applications that weren't installed with SD-UX.

All changes detected by the swverify command are written to the /var/adm/sw/swagentd.log file.

Other methods of improve security in file system are:

- Use disk quotes for limited size
- Use restricted shell for operator
- Use Tripwire with a clean HP-UX system

Conclusion
Securing a system is not an easy task and network services have many security risks. To successfully secure the UNIX environment it is critical understand what service are really necessary The papers of Larry Harker and Kevin Steves are a good start point. Then only permit the services necessaries.

You need all the help that you can found. The following site are very useful:

The last security patches, are necessary. May be obtained from the following ftp site: ftp://ftp.itrc.hp.com/hp-ux_patches.

Hewlett Packard have a service of free subscriptions in internet about security breach, you can received information about Security Bulletins at http://www.itresourcecenter.hp.com/

HP have too a forum in internet, where you can found invaluable help.
http://forums.itrc.hp.com/cm

References

HP-UX Technical Documentation
URL: http://docs.hp.com/

HP-UX forum site, HP-UX and Security
URL: http://forums.itrc.hp.com/cm/CategoryHome/1,1147,155,00.html

Sys Admin
The Journal for UNIX System Administrators.
URL: http://www.sysadminmag.com/

HP-UX Specific Security Concerns
URL: http://www.adager.com/VeSoft/HpUxSecurityConcerns.html

HP-UX Computer Security Checklist
URL: http://www.idiom.com/~lorraine/securecheck.html

Building a Bastion Host Using HP-UX 11
URL: http://people.hp.stevesk/

Hacking Exposed, 2 ed.
Scambray, McClure y Kurtz, Mc Graw Hill.

UNIX System Security Tools
Seth t. Ross, Mc Graw Hill

Practical UNIX and Network Security
HP training course

HP-UX System security course
HP training course

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS