Global Information Assurance Certification Paper

SANS Security Essentials
GSEC Practical Assignment
Version 1.2d

Securing HP-UX 11
Larry Harker
May 2001

Introduction

As I looked through the documents on the GIAC web site to research what I would do my practical on I noticed that no one has yet attempted to tackle HP-UX. There were several papers on Solaris, Linux, NT, and even AIX, but there were no papers on HP. I was rather surprised, as HP owns approximately 40% of all UNIX hardware sold today. With that being said, the goal of this paper is to discuss the necessary steps that it takes to secure the 11.0 operating system. HP-UX 11.0 is NOT a secure platform in an "out-of-the-box" configuration. It has several security holes that will be discussed in the following paragraphs.

To successfully secure the UNIX environment it is critical that a thorough understanding of what it is that your host is attempting to accomplish exists. For example, is the server going to be a mail server, firewall, database, web host, or application server? Understanding the functionality of the system being configured will allow the system administrator to securely configure the many services that are available within the HP-UX Operating System. This paper will start with physical security and walk through the minimum steps that should be followed to secure the HP-UX operating system.

Physical Security

Something that is often overlooked when talking about security is physical security. In many offices around the country any person may walk up to a server and do anything they want with a machine. There is no need for this person to have a logon, he or she can simply power-off the machine or do physical damage to the box. It is important therefore to have a server in a room that is secure with locks on all entry points. Not only a secure room, but also one with limited access. Only administrators should have access to the servers.

Installing the O.S. & Loading Patches

This paper assumes that the reader understands how to perform a default installation of HP-UX. Therefore the initial activity discussed here is to get the system up-to-date by installing the latest Hardware Enablement, and Software Patches. These may be obtained from the following web site:
http://us-support.external.hp.com
The system administrator should follow the web links to the area where the "Standard Patch Bundles" are hosted. Once there the system administrator can either logon to the

HP Resource Center (if a support contract exists) or put in the version of O.S. and the web site will ensure that the right patch bundle is obtained.
For this paper the security patches are of special interest. There are 10's of security patches for HP-UX 11.0 as of this writing. And the latest security patches are listed on the following ftp site:
ftp://ftp.itrc.hp.com/export/patches/hp-ux_patch_matrix.
All of the security patches may be obtained from the following ftp site:
ftp://ftp.itrc.hp.com/hp-ux_patches/
Make sure that you obtain the patches as they relate to the class of machine that you are installing. i.e. S700 or S800 for HP-UX capable hardware.
Once the patches are installed the following paragraphs address the required steps to ensure that the HP-UX operating system is secure. Some modifications to these procedures will need to be made depending on what your system is installed to perform.

Converting the system into a "Trusted System"
Use the supplied tsconvert command to convert the system into a trusted system. A sample output is provided. Immediately after converting… change the root password as the tsconvert command ages all passwords. The output of the tsconvert command follows:

/usr/lbin/tsconvert

```
Creating secure password database...
Directories created.
Making default files.
System default file created...
Terminal default file created...
Device assignment file created...
Moving passwords...
secure password database installed.
Converting at and crontab jobs...
At and crontab files converted
```

After converting the system I always stop root access from any other place than the console. This goes hand-in-hand with the physical security of the machine. If unauthorized individuals don't have physical or "virtual" access to the machine, the less damage that that person can deliver. To eliminate the root access simply touch the file /etc/securetty and chmod that file to 400.

Startup Scripts
The default installation of HP is very powerful and provides many useful services. However, most of these services are unneeded and pose a potential security risk for an organization. The first place to start is the startup scripts. Ensure that only necessary files are in /sbin/rc2.d, /sbin/rc3.d, and /sbin/rc4.d. These files are hard links to /sbin/init.d. Let's start with /sbin/rc2.d. By default there are many startup scripts. Remove those that have strike-through marks.

~~K100dtlogin.rc~~	S333hpsppci100	S525rarpd	S660xntpd
~~K200tps.rc~~	S340net	~~S530rwhod~~	S700acct
~~K900nfs.server~~	~~S370named~~	S535inetsvcs	S705pwgr
~~S006hpfc~~	~~S400nfs.core~~	~~S540sendmail~~	
~~S710hparamgr~~			
S008net.init	~~S406nisplus.server~~	S550ddfa	~~S710hparray~~
S100swagentd	~~S408nisplus.client~~	~~S560SnmpMaster~~	~~S720lp~~
S120swconfig	~~S410nis.server~~	S565OspfMib	S722pd
S200clean_ex	~~S420nis.client~~	~~S565SnmpHpunix~~	S730cron
S202clean_uucp	~~S430nfs.client~~	~~S565SnmpMib2~~	
~~S740supprtinfo~~			
S204clean_tmps	~~S440comsec~~	~~S565SnmpTrpDst~~	
S760auditing			
S206clean_adm	S462maclan	~~S570dce~~	~~S770audio~~
S220syslogd	~~S490mrouted~~	~~S590Rpcd~~	~~S780slsd~~
~~S230ptydaemon~~	S500inetd	~~S600iforls~~	S800spa
S300nettl	~~S510gated~~	S610rbootd	
~~S870swagentd~~			
S320hpether	S520rdpd	~~S620xfs~~	~~S900hpfcms~~
S323hpbase100	~~S522ppp~~	~~S630vt~~	

Also remove everything in the /sbin/rc3.d, and /sbin/rc4.d directories.

Remove unnecessary users and groups

Hackers over the years have developed some very sly ways of compromising a system. Some of these exploits involve logging onto a box with one of the default accounts. By default HP has several accounts that may allow this to happen. In order to eliminate this possibility simply remove those users and groups in question. With HP-UX 11 the following users and groups should be deleted:

USERS	GROUPS
uucp	lp
nuucp	nuucp
lp	daemon
hpdb	
www	
daemon	

Controlling Network Services

HP-UX uses the /etc/inetd.conf file to tell the system which services to startup. If no services are needed simply remove the startup script that is referenced in the Startup Scripts section of this document. Otherwise simply "pound" out all unnecessary services. A sample section of a typical HP-UX inetd.conf file follows:

```
##
ftp          stream tcp nowait root /usr/lbin/ftpd      ftpd -l
telnet       stream tcp nowait root /usr/lbin/telnetd  telnetd

# Before uncommenting the "tftp" entry below, please make sure
```

```
# that you have a "tftp" user in /etc/passwd. If you don't
# have one, please consult the tftpd(1M) manual entry for
# information about setting up this service.

#tftp        dgram  udp wait   root /usr/lbin/tftpd    tftpd
#bootps      dgram  udp wait   root /usr/lbin/bootpd   bootpd
#finger      stream tcp nowait bin  /usr/lbin/fingerd  fingerd
login        stream tcp nowait root /usr/lbin/rlogind  rlogind
shell        stream tcp nowait root /usr/lbin/remshd   remshd
exec         stream tcp nowait root /usr/lbin/rexecd   rexecd
#uucp        stream tcp nowait root /usr/sbin/uucpd    uucpd
ntalk        dgram  udp wait   root /usr/lbin/ntalkd   ntalkd
ident        stream tcp wait   bin  /usr/lbin/identd   identd
```

This list shows how many unnecessary services are running on the default installation of the O.S. To verify which services are running, use the netstat command. A partial netstat output is provided below:

```
#netstat -af inet
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp        0      0  *.4045                 *.*                    LISTEN
tcp        0      0  *.6000                 *.*                    LISTEN
tcp        0      0  b1000.6000             b1000.49156        ESTABLISHED
tcp        0      0  *.portmap              *.*                    LISTEN
tcp        0      0  *.2121                 *.*                    LISTEN
tcp        0      0  *.smtp                 *.*                    LISTEN
```

Another useful tool to determine what is running on you server is lsof. This tool can be obtained from ftp://ftp.cerias.com/pub/tools/unix/sysutils/lsof/

How does one determine which services are needed on a given server? The answer to this question goes back to the statement made in the introduction of this paper. A system administrator must know what the system is designed to accomplish. If this server is a mail server, and only a mail server, you need the smtp service but you do not need ftp, telnet or any of the other services that start by default. I usually take the approach as if I were a firewall administrator. Start with an operating system that has no services running. Then open up only those services that are needed as it relates to the determined function of the server. This will eliminate the possibility of any "extra" services running on the box.

File Permissions / Access

Determine what files have the set-gid by executing the following command.
find -perm -4000 -o -perm –2000 –print
Remove set-gid bit for the files as they apply to how the host will be used. Once files to be changed have been determined create a master list with the above commands and ensure that this list does not change over the life of the system.

If this server is to be an ftp or telnet server, create the /etc/ftpusers file to disable ftp services for all users in the /etc/passwd file. One should also install the tcpwrapper program. This will allow the host to authenticate and log the above two mentioned services. This can be obtained from the following site:
ftp://ftp.porcupine.org/pub/security/index.html
After installing the wrapper program edit the inetd.conf file with the following modifications:

```
ftp     stream tcp nowait root /usr/sbin/tcpd /usr/lbin/ftpd
telnet       stream tcp nowait root /usr/sbin/tcpd  /usr/lbin/telnetd
```

In conjunction with the tcpwrappers, one should also install a secure shell. One that I have successfully used is the openssh provided at the following web site:
www.openssh.org
This provides a secure tunnel for ftp, telnet, and many other services including X window applications. As a note to the above statement, you must also install zlib and openssl to ensure that the openssh compiles correctly. These programs can be found at the following web sites:

http://www.openssl.org
http://www.freesoftware.com/pub/infozip/zlib

Disabling unnecessary IP functions
With the onset of HP-UX 11 it has become very easy to modify the way that ip, tcp, udp, and arp perform. The ndd command-set has been added. To get a list of the modifiable options simply use the –h option. i.e. ndd –h. If you issue the ndd –c command it reads the /etc/rc.config.d/nddconf file and makes the necessary adjustments to the previously mentioned protocols. To secure a host minimally you at least want to disable ip_forwarding. A sample nddconf is shown below.

```
TRANSPORT_NAME[1]=ip
NDD_NAME[1]=ip_forwarding
NDD_VALUE[1]=0

TRANSPORT_NAME[2]=ip
NDD_NAME[2]=ip_forward_directed_broadcast
NDD_VALUE[2]=0

TRANSPORT_NAME[3]=ip
NDD_NAME[3]=ip_forward_src_routed
NDD_VALUE[3]=0

TRANSPORT_NAME[4]=ip
NDD_NAME[4]=ip_respond_to_echo_broadcast
NDD_VALUE[4]=0
```

Conclusion

As one can see securing a system is by no means an easy task, and sometimes it is one that is ignored because we sometimes take the mindset of "If it works, Don't Touch It". This can be very dangerous as has been demonstrated in the above paragraphs…What you don't know can KILL. The many services that run "out-of-the-box" pose many security threats that have to be looked at very carefully in order to successfully thwart the many hackers and vandals that are out in the world.

One must first secure the server physically to insure that no unauthorized individuals have access to the machine. Then by first determining what a servers "task" or "tasks" will be, one can successfully "secure" a server by following the above outlined procedures.

References:

1. "HP-UX Computer Security"
URL: http://www.vennerable.com/security.html

2. "Securing Unix Part 1"
URL: http://www.boran.com/security/unix1.html

3. "Securing Unix Part 2"
URL: http://www.boran.com/security/unix2.html

4. "Building a Bastion Host Using HP-UX 11.0"
URL: http://people.hp.se/stevesk/bastion11.html

5. "HP-UX Security Guide"
URL: http://www.sabernet.net/papers/hp-ux10.html