# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

## Interested in learning more?

Check out the list of upcoming events offering
"Securing Linux/Unix (Security 506)"
at http://www.giac.org/registration/gcux

# PRACTICLE FOR ROBERT E. LAUGHLIN

AUGUST 15, 2000

## 1. EXECUTIVE SUMMARY

Here at the center there is a computer system that runs on a HP-743i PA-RISK single board computer in a VME chassis. The operating system that is used is Hewlett Packard's (HP) HP-RT, a real time operating system. This machine is used to test real time software applications for later use in larger systems. This system must be connected to the Internet to allow the developers to have access to it.

The HP-RT operating system, as it comes from the vendor, is not secure. (Almost all operating systems as delivered are not secure.) It is wide open to any one that might want to enter. The only saving grace is that because HP-RT is a relatively obscure operating system it is not likely to be used to run dangerous packages.

HP has the policy of not providing patches to it's HP-RT customers unless they have a support contract. The center does not have such a support contract. Therefore there are no vendor patches available, at this time, to correct the security holes. Center personnel must implement all of the corrections for the security problems.

Most of the corrections that are needed to improve the security level of the system require retrieving the source code for software packages from the Internet. These packages then must be ported to HP-RT, installed, and tested. Most of these are to close security holes that are known to exist in HP-RT, wu-ftp and TCP-wrappers are examples. Some of these packages are needed to run on the system to check for internal security problems, such as permission bits being set incorrectly.

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

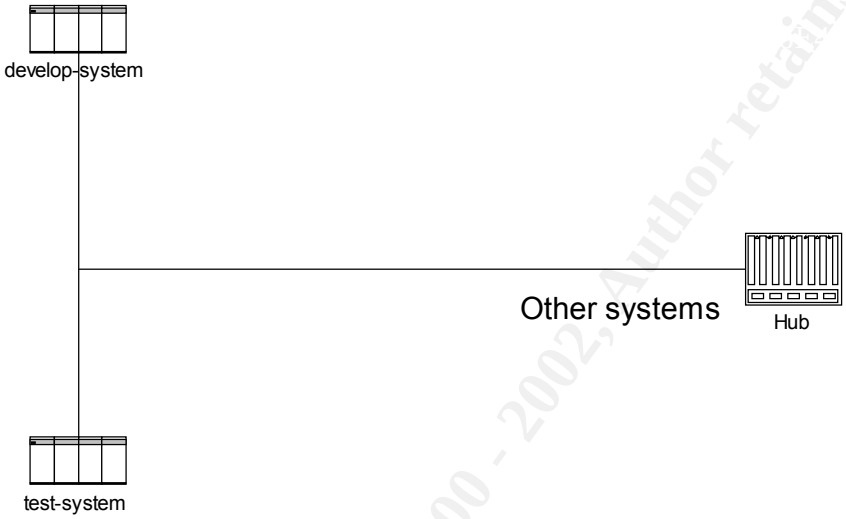


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

## 2. SYSTEM DESCRIPTION

The system that was examined, test-system.nowhere.vil, runs the HP-RT Operating System. Test-system runs on a HP-743i PA-RISK single board computer in a VME chassis. It has a 1.05 Gigabyte, SCSI hard drive, a built-in 10 MHz Ethernet port, and two serial ports.

The HP-RT development package does not run on the HP-RT operating system. It must be run on a HP-UX operating system. Therefore somewhere there must be a HP-UX machine that has the HP-RT development package installed. In the drawing below develop-system.nowhere.vil is such a system. It has all of the software tools required to develop HP-RT software. Develop-system is connected to test-system via an Ethernet.




This drawing represents the physical connections involved in the local configuration. The connections between the two systems shown and the hub use a 10 MHz Ethernet cable. The reason for this is because the rest of the connections at this location use 100 MHz Ethernets. The hub also serves as the gateway to translate from 10 MHz to 100 MHz. (HP's PA-RISC hardware of the vintage in use only supports 10 MHz.)

Modification of the HP-RT operating system kernel and the generation of executable software to run on a HP-RT operating system must all be done on a system such as develop-system. The resultant binaries, libraries, etc. are then transferred via the Ethernet (the method preferred by HP) or via a four-millimeter DAT tape to the target system. Because the use of a DAT tape is extremely inconvenient and because test-system does not have a tape drive we use the Ethernet here to transfer files to test-system and to install an updated operating system on test-system. Unfortunately this method of installation is vulnerable to several methods of attack from the Internet. For this reason we disconnect the 100 MHz side of the hub from the Internet during the installation of the HP-RT operating system or upgrading of software on test-system.

Develop-system has already been hardened by the installation of the most recently available of HP's security patches, as well as the installation of several extra software packages, such as TCP-wrappers and ssh. Develop-system is not the system being examined here, test-system is.


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

Test-system is needed as a test bed for the development of application software for a larger system and as such must be available for developers to access from the Internet. At the same time it should not be available for use in attacking other sites.

"Lynx Real-Time Systems, Inc." originally wrote what is now HP-RT as their own proprietary real time operating system, Lynx-os. HP paid Lynx to port the Lynx-os to the HP PA-RISC machines as HP-RT. Lynx-os and of course HP-RT operating system is a direct descendent of a version of BSD that dates from before the time that the University of California at Berkeley stopped supporting it. The present version of HP-RT, 3.02, has been installed in Test-system since 1998. HP does not provide access to ANY patches for HP-RT unless you have a support agreement with them. The result is that some of the binaries and libraries that come with the HP-RT software package are over twelve years old and have a lot of security holes that have not been fixed, for example the installed version of ftpd dates from 1988.

HP-RT operating system delivered directly from HP includes support for the following networking services; ftp, telnet, rlogin, remsh, rcp, NFS, XNTP, and Berkeley sockets. It does not support; SMTP, sendmail, rwho, ruptime, and the secure sockets layer (SSL).

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



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

## ANALYSIS

At this time a HP-RT machine can only be tested from the outside, because no one has ported system integrity and vulnerability testing software, such as cops, crack, and tiger, to HP-RT. A lot of people write "real time applications" for HP-RT, but apparently no one, to date, has worried about security for a HP-RT machine.

### *1) Operating System Vulnerabilities*

Some of the operating system vulnerabilities are built into the binaries and packages that the operating system contains. Quite often a system includes executable packages that have not been updated to remove security holes even when the security problems have been known and publicized for many years.

a) System installation is done over the network. This leaves the installation vulnerable to man in the middle attacks.

b) The HP-RT password command does not support a shadow password file. This leaves the system with a with a password file that can be read and captured for later processing.

c) The HP-RT password command uses an older less capable encryption algorithm.

d) The HP-RT password command does not support checking for a "good" or "bad" password.

e) The HP-RT password command does not support password aging.

f) The version of xntp that is supplied with HP-RT is at least three years out of date. It is version 3.4. The present version is 3-5.93. If the time mechanism can be spoofed then the forensics after a break in is much more difficult and likely to stand up in court.

g) The ftpd version is 12 years out of date. It has not been corrected for the many known security holes in ftp software packages.

h) NFS is at least four years out of date and by default is installed and enabled during the operating system installation.

### *2) Configuration Vulnerabilities*

Not only do most operating systems include executables that are vulnerable, but they are also usually configured such that the vendor's engineers can easily enter and modify them, of course these vulnerable configurations are well know to hackers. This is exactly the opposite of the configuration that is needed to keep unauthorized visitors out of a system. These problems need to be corrected as soon as possible.

a) Snmp has its community strings set to public in snmpd.conf and the snmpd is started by default. It may not be needed in this installation.

b) NFS is installed and enabled by default.

c) Ps, hostname, sync, and shutdown are setup as accounts that perform the command that is named.



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

d) There is a guest account set up with a home directory.

e) Root access from the Internet, to test-system, is enabled.

f) .Rosts files are allowed and present.

g) Xntpd is configured to use the hardware clock and is not synchronized to remote sites.

h) Inetd.conf contains the following:

```
#
# $Date: 94/06/03 14:06:11 $
# $Revision: 200.0 $
#
shell    stream tcp      nowait root    /bin/rshd       rshd
login    stream tcp      nowait root    /bin/rlogind    rlogind
ftp      stream tcp      nowait root    /etc/ftpd       ftpd
telnet   stream tcp      nowait root    /bin/telnetd    telnetd
ntalk    dgram  udp      wait    root    /etc/talkd      talkd
tftp     dgram  udp      wait    root    /bin/tftpd      tftpd
bootps dgram  udp      wait    root    /bin/bootpd     bootpd
exec   stream  tcp    nowait  root   /bin/rexecd    rexecd
#smtp  stream tcp      nowait root    /usr/local/smtpd        smtpd
#
#------< Ptrace Server - ngc 910991
#
rt_ptrace stream tcp    nowait  root    /etc/pt_svr pt_svr /dev/console
#
#------< network performance server
#
netperf stream tcp nowait root /usr/etc/net_perf/netserver netserver
```

Most of these should be commented out or removed. The ones that are kept should be at least be controlled by TCP_wrappers.

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



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

### 3) Risks from installed third-party software

The installation of third party software, that is software that was not developed by the system owner or by the operating system vendor, can cause a great deal of trouble because the system owner does not know for sure how many problems still remain in the third party's software.

a) The only risks at this location are from the software under test and the packages that came with the HP-RT system. The only third party software packages installed on this machine at this time are those that are under test.

### 4) Administrative Practices

Any institution that has computers should have policies about the administration of the computers and the implementation of security practices.

a) This organization has policies about what constitutes an acceptable password.

b) This organization has policies about password aging.

c) This organization has policies about who can get access to a computer.

d) This organization has policies about accessing in-house computers from off site.

- Several of the ports used to remotely access computers are blocked from outside of the center's networks.

### 5) Backup Policies, Disaster Preparedness

Normally a system should be backed up on to tape, or other such medium.

a) Backups are performed daily on develop-system. Because everything is reloaded almost every day from develop-system to test-system no backup is required for test-system.

b) HP-UX has a package called make_recovery. This generates a self-booting tape that can be used to rebuild the hard disks as needed, including all of the data on the disks.

c) Copies of the backup tapes and the make_recovery tapes are kept off site.

### 6) Other issues

There are other things that the administrators need to make sure of. This list is by no means complete.

a) Both systems and their console keyboards and monitors are kept in a locked room. Only three people have keys to access them physically.

b) The circuit breaker rooms are kept locked.

c) There is a document that lists which circuit breakers are associated with these machines.

d) There is a document that lists where the network connections for these machines go to.



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

e) All software development access is via the network.

## 4. PRIORITIZED LIST OF VULNERABILITIES

This list of vulnerabilities is ordered in decreasing likely hood of causing problems.

1) Root access from the net should be denied.
2) NFS should not be turned on or installed.
3) Extra accounts are present on the system that should not be there.
4) The password command does support a shadow file.
5) The password command does not support any of the better cryptographic algorithms.
6) A mechanism is needed to support the password aging
7) A mechanism is needed to check for bad passwords.
8) TCP_wrappers should be used to control access to the commands that must be in the inetd.conf file.
9) Password strings are transmitted in the clear during remote access to the system. Ssh should be used instead of rlogin, as is used now.
10) The snmp daemon community strings being set to public allows any one with an snmp browser to access the system.
11) The snmp daemon binary is at least three years out of date and does not have the latest fixes. If snmpd must be used a newer version should be installed.
12) The ftp daemon does not have any of the modern fixes. This allows an unauthorized user to get root privileges with out much trouble.
13) Xntpd is out of date and does not have the latest fixes.

## 5. RECOMMENDED FIXES

The majority of the recommended fixes require porting and installation of software from retrieved from Internet sites. Software such as Perl, ssh, lsof, trip-wire, TCP_wrappers, etc. must be ported to HP-RT.

Porting software downloaded from the Internet poses some interesting problems. The major difficulty is because the configuration mechanism supplied with most of them does not provide, correctly, for cross compiling. Cross compilation is required, here, because the development system runs on HP-UX a SYSV machine and HP-RT is a BSD machine. Software compiled using the libraries for one operating system will not run on the other one. The configuration mechanism for most of these packages tries to check to see if the compiler works correctly by compiling and running a program, in this environment that will not work. Perl is the only software package that explicitly states (on their web site) that it does not support cross compiling. The perl people call that making a non-native binary. Experience teaches that some of the other packages have the same problem, sshd is one example.


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

The development directory tree, for HP-RT on develop-system, contains all of the information that will be installed on test-system during a HP-RT installation. When a fix is implemented and tested it will be installed on both the test-system and in the development directory tree on develop-system. From then on when a reinstallation of the operating system is performed all of the new software will also will be installed.

Two additional software packages, lsof and trip-wire, should be installed. They will help in detecting when an intrusion has occurred. TCP-wrappers helps to detect attempted break-ins, but it will not catch all of them, and any one that is smart enough to avoid detection by TCP-wrappers is probably smart enough to remove any immediately accessible evidence may do a successful attack. Therefore the system will need to be configured to send any log files to an independent machine with flags to call attention to attempted intrusions. These log files need to have date time information that is consistent with the rest machines. That mandates that xntpd use external clock sources, more than two.

### *1) Fixes to be implemented*

(a) Build a HP-RT operating system that does not include NFS. This will require the generation of a new kernel.

(b) Remove the ps, hostname, shutdown, and guest user entries from /etc/passwd.

(c) Remove "guest" users home directory.

(d) Port, install, test, and use the shadow password suite from one of the open software packages.

- Enable the shadow password file.
- Enforce password aging.
- Enforce the policies about proper passwords.
- Set it up to use one of the better encryption algorithms

(e) Port, install, and test TCP_wrappers.

(f) Configure inetd.conf such access to all commands that must be used via inetd must first be filtered by TCP_wrappers. All of the rest of the commands will be removed from the inetd.conf file and the associated binaries will be removed from the system.

(g) Add hosts.allow and hosts.deny to /etc for TCP-wrapper.

- Configure them such that root access is denied from all hosts.
- Configure them such that only hosts with in the local subnet can access test-system.
- Configure them such that only selected users on selected hosts are allowed to access test-system.

(h) Port and install perl to HP-RT

- Needed for parts of the ssh package.


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

(i) Port, install, and use sshd to HP-RT.

- Build sshd to use RSA, for encryption.
- Disable the uses of .rhosts or .shosts files
- Use the AllowUsers and DenyUsers configuration to control who can login remotely.
- Set PermitRootLogin to no.
- Set IgnoreRhosts to yes

(j) Once sshd is ported, installed, and tested disable and remove all of the remote commands in inetd.conf, such as rlogin, rcp, remsh,

(k) Port, install, and test the latest version of WU-Ftp.

(l) Port, install, and test a new xntpd.

- Configure xntpd to use three clock sources. That way if one is wrong the internal voting mechanism in xntp will keep the local machine near to the correct time.
- Make sure to use the undocumented flag, -g, so that xntpd will not die when it finds that the local clock is more than 15 minutes off. (Presently if the clock error is larger than 15 minutes it will die.)

(m) Port, install, test, and run the latest version of snmpd.

(n) Port, install, test, and run crack periodically to make sure that "good" passwords are being used.

(o) Port, install, test, and run tiger.

- Correct any configuration problems that it reveals. This step is an iterative process.

(p) Port, install, and test lsof on test-system.

(q) Port, install, and test trip-wire on test-system.

© SANS Institute 2000 - 2002 Author retains full rights.



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

### *2) Estimated costs of the fixes*

Some of these fixes involve configuring the system generation commands on develop-system. Some of them involve adjusting the contents of files that are read by HP-RT daemons when test-system starts up. Some of these fixes require porting software where the configure script can figure every thing out correctly (tcp-wrappers for example) and running the make file. There are others (perl and sshd) that require finessing the configure script to get around the need that the script has for using binaries that it generates on the development host. On average I believe that it will take six work days to port, install, and test each of these packages. Some of them will take more time and some less.

| | |
|---|---|
| (a) Building new kernel; | $ 640 |
| (b) Remove ps, sync, shutdown, and guest from /etc/passwd | $ 640 |
| (c) Remove the "guest" home directory. | $ 640 |
| (d) Find, port, test, and installing the "shadow" suite | $7,680 |
| (e) (f) (g) Port, test, and install TCP_wrappers | $ 640 |
| (h) Port, install, and test perl | $3,840 |
| (i) Port, install, and test sshd | $3,840 |
| (j) Remove the replaced commands from inetd.conf | $ 640 |
| (k) Port, install, and test WU-Ftp | $3,840 |
| (l) Port, install, and test xntpd | $3,840 |
| (m) Port, install, and test snmpd | $3,840 |
| (n) Port, install, and test crack | $3,840 |
| (o) Port, install, and test tiger | $3,840 |
| (p) Correct the problems that tiger reveals (iterative process) | $7,680 |
| (q) Port, install, and test lsof | $3,840 |
| (r) Port, install, and test trip-wire | $3,840 |

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



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

## 6. REFERENCES

Book List


HP-RT System Administration Tasks; HP Part No. B5487-90002

Unix System Administration Handbook, Second Edition, Evi Nemeth, et. all

Essential System Administration, Second Edition, Aeleen Frish

The Documents from the SANS DC2000 Unix Security Course


The following is a list of web pages for getting the software mentioned in this document.

http://www.perl.com

http://www.linuxdoc.org/HOWTO/Shadow-Password-HOWTO.html

ftp://ftp.cs.hut.fi/pub/ssh

ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.tar.gz

ftp://net.tamu.edu/ftp/security/TAMU/tiger-2.2.4pl1.tar.gz

ftp://coast.cs.purdue.edu/pub/tools/unix/crack/crack5.0.tar.gz

ftp://vic.cc.purdue.edu/pub/tools/unix/lsof

ftp://ftp.wu-ftdp.org/pub/wu-ftpd/

ftp://ftp.icm.edu.pl/pub/Linux/shadow/shadow-current.tar.gz

http://www.net.cmu.edu/groups/netdev/software.html

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



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

Last Updated: May 28th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| **SANS London July 2017** | **London, United Kingdom** | **Jul 03, 2017 - Jul 08, 2017** | **Live Event** |
| **SANSFIRE 2017** | **Washington, DC** | **Jul 22, 2017 - Jul 29, 2017** | **Live Event** |
| **SANS Network Security 2017** | **Las Vegas, NV** | **Sep 10, 2017 - Sep 17, 2017** | **Live Event** |
| **SANS OnDemand** | **Online** | **Anytime** | **Self Paced** |
| **SANS SelfStudy** | **Books & MP3s Only** | **Anytime** | **Self Paced** |