# Unix Systems Security Fundamentals

Training Course Workbook

Published by and copyright Reference-Systems.Com
http://www.reference-systems.com/

Winter 2005

## Course Prerequisites

- Knowledge of use of Unix as an end user. No basic Unix skills will be covered in this course. Knowledge of Unix utilities, such as, ls, df, vi, is assumed.

- Knowledge of basic Unix system administration tools and techniques is required. Knowledge of administration utililities, such as, ifconfig, traceroute, ping and nmap are assumed.

- Experience building Unix based applications with a high-level language would also be helpful, but is not a requirement.

## Required Course Materials

- *Practical Unix and Internet Security*, 3rd Edition, Simson Garfinkel and Gene Spafford, , O'Reilly & Associates, Inc., Feb 2003, ISBN 0596003234 (PUIS).

- The Unix Systems Security Fundamentals training course workbook.

- Defense-In-Depth: Information Assurance white paper

- Access to the Internet to view web pages at http://www.reference-systems.com and http://www.reference-systems.com/USSF

- Access to a computer running Linux. This system must provide access to a C compiler, *make* utility, and *gpg* (the gnu version of Pretty Good Privacy encryption and digital signature tool). Red Hat version 9, Red Hat Enterprise Linux 3 or equivalent provides an adequate environment.

# Instructor Profile

Victor Hazlewood, B.S., CISSP, has over 15 years experience with Unix and Windows systems and over ten years experience with information technology security. Victor received his Certified Information Systems Security Professional credential (#35556) in August of 2002. Victor spent six years working with high performance computing systems running Unix at Texas A&M University, seven years at the San Diego Supercomputer Center (SDSC) as the Manager of the High Performance Computing Systems group at SDSC, about two years as Director of Information Assurance with Strategic Data Systems in San Diego working on commercial and U.S Navy projects, and, most recently, one year as the Manager of Security Technologies and Information Security Officer of SDSC. Victor worked with a variety of system administrators and security professionals in auditing and securing Unix and Windows computing systems from desktops to supercomputers. He also has over six years experience teaching Unix system administration and Unix security courses for the UCSD Extension where he received the Outstanding Instructor Award in 2000. Victor has had numerous system administration and security articles published in conference proceedings and in the SysAdmin magazine.

Course Overview

| Module | Description | PUIS Chapters |
|---|---|---|
| Module 1 | Intro to Computer Security<br>Defense-In-Depth strategy<br>Roles and Responsibilities<br>Security policy and planning | 1, 2, 3<br><br>Defense-In-Depth white paper |
| Module 2 | Unix authentication and password overview<br>Eliminating plaintext passwords<br>File permissions<br>Super user (root) privileges<br>Encryption<br>Digital Signatures<br>Pretty Good Privacy (PGP/gpg)<br>*Hands on: PGP/gpg lab* | 4, 5, 6, 7 |
| Module 3 | Auditing and logging<br>Networking and network services<br>Using TCP wrappers<br>*Hands on: Building TCP wrappers* | 21, 11, 12, 13 |
| Module 4 | Backups<br>*Hands on: Using dump and restore*<br>Performing a security audit<br>Intrusion detection<br>Examining a compromised system:<br>*lilred t0rn rootkit demonstration*<br>*suckit kernel rootkit demonstration* | 18, 22<br>Appendix A |
| Module 5 | Web server security<br>Automated threats<br>Writing secure Setuid and other programs<br>Denial of Service attacks<br>Data integrity assurance with Tripwire<br>*Tripwire demonstration* | 16,. 23, 24 |
| Module 6 | Vendor security patches<br>Security awareness<br>Security information resources<br>Computer crime<br>Review of security tools | 25<br>Appendix D and E |

## Module 1 Exercises

1. Read PUIS chapters 1, 2, and 3.

2. Read the Defense-In-Depth white paper

3. Name the four categories of the Defense-In-Depth strategy

4. Name the three components of each Defense-In-Depth category.

5. Name six threats to information systems.

6. Name the eight information systems roles described in Module 1.

7. Name the six components of security needs planning and put them in order of importance for your organization?

8. Describe the difference between policies, standards and guidelines.

## Module 2 Exercises

1. Read PUIS chapters 4, 5, 6, and 7.

2. Read the man page for the password (/etc/passwd) and shadow (/etc/shadow) file formats. Become familiar with the details of each file format.

3. Read the ssh and ssh-keygen man pages for Secure Shell. Determine how to generate RSA key pairs for Secure Shell authentication. Generate key pairs, install in your home directory and log in using ssh with RSA authentication.

4. Why is the /etc/passwd file world readable?

5. Why is the /etc/shadow file readable only by root?

6. If the /etc/shadow file is only readable by root, how does the passwd program work to change a users password?

7. Use find to catalog all setuid root programs on your Linux system. How many setuid root programs are there on your Linux system?

8. What permissions does the /tmp directory have and why?

9. Thinking like a black hat hacker, how would you go about sniffing or stealing username and password credentials? Describe at least two ways to capture passwords after root compromising a system.

10. Name six example private key encryption algorithms.

11. Name four example public key encryption algorithms.

12. Use gpg on your Linux system. First, read the gpg man page and then use the following instructions:

```
1.   Set up a gnupg directory
      % cd
      % rm -r .gnupg
      % mkdir .gnupg

2.   Create your key pair:
      % gpg --gen-key

3.   Check your key:
      % gpg --list-keys
      % gpg --list-sigs
```

4. Extract a copy of your key from your keyring in ascii to make it available for others

   ```
   % gpg --export -a > /tmp/my.gpg.key.asc
   ```

5. Get my key and add it to your keyring
   Save the contents of http://www.sdsc.edu/~victor/mykey.html to a file and import the key into your keyring.

6. Check a test message

   ```
   % mkdir /tmp/(yourlastname)
   ```

   Copy the below test message to the directory you just created and check the signature.

   ```
   % gpg test.gpg
   ```

7. Be familiar with how to encrypt and decrypt a message and how to create and check digital signatures. gpg commands to try:

   ```
     encrypt a message (You must have the recipients public key)
     Create a digital signature
     Create a digital signature and include the text
     Create an encrypted message and add a digital signature:
   ```

The test message:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1


This is a test.

- -Victor Hazlewood

-----BEGIN PGP SIGNATURE-----
Version: PGP 8.0.3

iQA/AwUBQQlUAjxANmybuZVIEQL+OQCbBiP9k1eYu8FH2rRXMRAHsM6eAxIAoJLZ
KBLhL5URGQDx4T921pUphuAY
=G64P
-----END PGP SIGNATURE-----
```

## Module 3 Exercises

1. Read PUIS chapters 1, 2, and 3.

2. Locate the utmp/utmpx and wtmp/wtmpx files on your system. Convince yourself these are binary files. Use who and last to read the contents of your utmp/utmpx and wtmp/wtmpx files.

3. Enable process accounting with *accton* and watch the pacct file grow each time a process ends on your system. Use acctcom or lastcomm to read the pacct file. Familiarize yourself with the output of acctcom or lastcomm.

4. Locate the syslog configuration file, read its contents and determine where all log messages are being logged. Is there a syslog log file that records all syslog messages? That records mail log entries? That records authentication log messages?

5. Use nmap to port scan your entire service port range. What ports are listening? Use the "-sV" option to attempt to determine more about what program is actually listening to the port. Configure your system to only run the secure shell daemon and nothing else. Port scan your system again to prove to yourself that you are only running the Secure Shell daemon.

6. Download TCP wrappers from the author's (Wietse Venema) website at

   http://www.porcupine.org/
     -> Tools and Papers
     -> TCP Wrapper

   Validate the PGP signature that goes along with this tarred and gzipped file. If the signature checks out then attempt to compile the software for your system. Just attempt to compile it. You do not have to install it. Odds are it is already installed on your Linux system by default.

## Module 4 Exercises

1. Read PUIS chapters 18, 22, and Appendix A.

2. Create an empty directory in your home directory. Use tar to backup all the files in your home directory. Check the tarfile to see how your system handles tarring up empty directories. Use tar to back all the files in the /dev directory. Restore these files into /tmp. Check the behavior of your system in restoring device files with tar.

3. Use dump to backup the smallest file system on your Linux system. Check the dumpdates file after your backup completes successfully. Use restore –i to attempt to recover a single file from the backup.

4. What find command(s) would you use to check the entire file system for setuid root programs?

5. How would you check your Linux system for Trojan horse programs, such as, a trojaned ssh client or daemon. Hint: rpm has an interesting feature that helps with this.

6. Identify where you could obtain the following tools
   cfengine
   Nessus
   Tripwire
   bro
   TCP Wrappers

## Module 5 Exercises

1. Read PUIS chapters 18, 22, and Appendix A

2. Start a web server on your Linux system. Where are the httpd.conf and srm.conf files located. Based on the contents of these configuration files, where are the access and error log files going to be placed on your system?

3. Name two tools that can be used to probe your system remotely for port and/or vulnerability information.

4. Name two general programming tips for writing secure applications.

5. Name two tips for writing secure setuid and/or setgid applications.

6. Describe how you might defend yourself against a service overload attack.

7. Review the commercial Tripwire site, specifically the Tripwire for Servers product. Describe the capabilities of this data integrity assurance tool.

## Module 6 Exercises

1. Read PUIS chapter 25, and Appendices D and E.

2. What important practice should be performed before connecting a newly installed computer system to the Internet?

3. Name five computer security resources on the Web.

4. Review the list of tools we have discussed and be familiar with there function.