Global Information Assurance Certification Paper

OneMore.Com Security Consulting
1024 Megabyte Drive
Linuxville, CA 98000

GIAC Enterprises

Security Audit Report

November 15, 2000

Consultant: Jason M. Frey

1. Introduction

As the leader in online fortune cookie saying sales, **GIAC Enterprises** realizes the need to ensure security in their network. This preliminary audit is the first step towards that goal. This document outlines the findings of the security audit conducted by **OneMore.Com Security Consulting**.

The audit focuses on several key areas.

- Administrative Practices
- Physical Security
- Operating System and Configuration
- Third-Party Applications
- Data Encryption
- Disaster Recovery and Backups

Some issues may be repeated in the document if their vulnerabilities cross key areas.

Details on how to secure the item in the form of a "step-by-step" checklist will not be provided in this document. Where necessary examples will be given. It is the expectation of **OneMore.Com Security Consulting** that **GIAC Enterprises** will perform all the necessary actions to secure the system. **OneMore.Com Security Consulting** does, however, extend an offer to provide such level of support at standard cost if **GIAC Enterprises** requests such support. This level of support is included with our **GOLD Security** package.

1.1. Infrastructure Overview

GIAC Enterprises current development infrastructure consists of four servers. Four servers are all running the same operating system on the same platform. A single server is being audited for this preliminary review. The systems are run on a switched network with no connectivity to the Internet. There are three developers and a two system administrators with privileges to access these systems.

1.2. Target System

Server Name:	jester.giac.com
Operating System:	RedHat Linux 6.2
Kernel Version:	2.2.14-5.0smp
Platform:	Intel
Function:	Internal development and web server
Service:	Apache 1.3.12

2. Executive Summary

OneMore.Com Security Consulting has determined that the target system audited for **GIAC Enterprises** poses a **High Risk** to the security of the network infrastructure.

2.1. Summary of Major Findings

The major findings for each key area are outlined below.

Administrative Practices – High Risk

- There are no security policies in place at this time.
- Lack of standard practices (builds, updates, etc…)
- Super-User Logins are common practice
- Telnet and FTP are used for administration
- Logs are not inspected on a regular basis nor rotated

Physical Security – Low Risk

- Physical access security is sufficient
- Tape Storage is sufficient

Operating System and Configuration – High Risk

- Unnecessary accounts with valid shells
- 60% password cracking success rate
- World-writeable files exist
- Unnecessary and vulnerable services running
- X-Windows and other "workstation" applications installed
- Operating system not current with latest security patches
- Kernel not current and not configured

Third-Party Applications – High Risk

- Apache web server not updated nor optimally configured

Data Encryption – High Risk

- Secure Shell is not utilized to protect remote session data
- SSL is not being used to secure http transactions

Disaster Recovery and Backups – Low Risk

- Backup / Restore plan is sufficient and tested
- System redundancy and load balancing do not exist

3. Administrative Practices

It is determined that administrative practices pose a serious risk to the security of all networked systems within the **GIAC Enterprises'** infrastructure. It is the administrative practices that provide the basis for a solid security plan. Having a sound security plan will assist the company in raising their security posture to an appropriate level.

3.1. Security Policies

The audit found that there are currently no security policies in place. Security policies provide the limits and restrictions required to maintain a good security posture. They are also vital should a company decide to prosecute an attacker.

At a minimum, the following policies should be drafted and published:

- **Acceptable Use Policy** – defines what constitutes acceptable use of the networked systems and services by company employees
- **Privacy Policy** – defines the policy with regards to personal/corporate confidentiality covering topics as monitoring and email privacy
- **Access Policy** – defines the process for authorizing physical access and privileged login ability to networked systems

Examples of these policies can be found at the SANS website – http://www.sans.org/newlook/resources/policies/policies.htm

3.2. Administrative Standards

There are no published or adhered to standards for the administration of the networked systems. Interviewing the administrator, it was discovered that different personnel built each of the four servers. The administrator admitted that he was only aware of the details of one server – the target system. Also, responsibility for updating the software on these systems has passed through several personnel.

Lack of standards creates an unpredictable computing atmosphere. It is recommended that the following standard practices be implemented to ensure a secure networked environment.

- **Kickstart** – Develop a standard bare-bones server installation of RedHat 6.2 utilizing the **Kickstart** utility, which creates a snapshot profile of a built system that can be used to build subsequent identical systems. **Kickstart How-To** documentation can be found at http://www.redhat.com/mirrors/LDP/HOWTO/KickStart-HOWTO.html.
- **Configuration Utility** – Utilize a configuration utility such as **cfengine** to provide consistent configurations across systems. Utilities such as these are used to

ensure that patches and updates are performed across multiple systems defined by the administrator. Information on **cfengine** can be obtained from http://www.iu.hioslo.no/cfengine/.

- **Responsibility Matrix** – Develop a responsibility matrix that outlines who is responsible for what administrative duties. Publish this matrix so that all know their responsibilities and others know whom to turn to for issues.
- **Standard Procedures** – Standardize procedures that are repetitive and document those procedures. Create scripts where possible to automate the procedure.

3.3. Super-User Logins

The system administrators often perform all of their administration while logged in as the super-user (root). Sometimes they login as "root" from the console, but more often administration is performed remotely via telnet.

Logging in as the super-user is not recommended practice. It offers no ability to log which employee is actually logged in and performing administrative actions. It also provides a greater risk of causing harm to the system in the event a typographical mistake is made when using destructive commands. Many administrative tasks do not require super-user privileges.

It is recommended that administrators set up **sudo** to provide logged access to those commands that require super-user privileges. This is done by editing the **/etc/sudoers** file.

The other possibility is to have administrators login as themselves and **su** to the root user to perform those actions. This still presents some risks, but will provide a log of which administrator performed the action.

3.4. Telnet and FTP Sessions

The majority of the administration tasks are carried out remotely. The greatest security risk with this administrative practice is the lack of security of the transferred information. Since telnet and FTP do not encrypt session data, they offer attackers a visual window to the session data. Attackers equipped with packet sniffers and access to the network can easily capture usernames and passwords for those sessions.

Since the administrators usually log in as the super-user via telnet, they are exposing the super-user password to any individual with a packet sniffer.

The solution to this problem is a simple one and is discussed in the **Data Encryption** section that follows.

3.5. Logging

The use of logs should be improved on the target system. Logs are not checked on a regular basis. The administrators currently only use the logs to troubleshoot system problems as they occur.

Consistent inspection of the log files will keep the administrator informed of the baseline operations of the system. Items out of the ordinary will alert the system administrator and possibly allow quicker reaction times.

3.5.a. Logs to Maintain

Logging should be increased to include all warning, error and kernel messages. The warning and error messages should be directed to **/var/log/syslog** and the kernel messages to **/var/log/kernel**. The administrator should edit the **/etc/syslog.conf** file and make the appropriate changes. Also, the two log files will need to be created and permissions set on those files to secure them.

3.5.b. Log Rotation

Logs should be rotated periodically. The interval for log rotation is dependent upon the traffic the system receives and the amount of messages created. At a minimum a monthly rotation is recommended. The administrator should edit the **/etc/logrotate.d/syslog** and **/etc/logrotate.conf** files to make this change.

3.5.c. Logchecker

An improved method of checking the files will likely increase the inspection of the logs. The application **logchecker** can be used to send an email that compiles the logs into a nice format for the administrator to inspect.

4. Physical Security

Physical security of the systems was found to be sufficient.

4.1. System Security

All systems are located within a small data center with access controlled by a cipher-lock. The cipher lock is activated through the employees' identification badge. Only the Director of Operations has the ability to authorize access to this room. Deactivation upon employee termination is automatic.

A closed circuit camera monitors the room at all times and is broadcast the security office (also controlled by a cipher lock). A security guard is present in the room at all

times. The front portion of the room is a glass wall that allows visual inspection of the room from the outside.

A single terminal is connected to the target system (monitor, keyboard and mouse). The monitor screen is not visible from the window. If an unauthorized individual were to gain access to the room, they would have direct console access. This threat is considered minimal given the physical and visual security of the room.

The systems have power and reset switches accessible from the front of the machine, which could intentionally or inadvertently get pressed. The power switch is set so that it must be depress for five seconds before it will instantly shutdown the system.

The reset button does not have this feature. It is possible that accidentally bumping the switch would cause the system to instantly recycle. The potential of data loss/corruption as a result of this is high. It is recommended that this switch be disconnected from the motherboard to prevent such an event.

4.2. Tape Storage

Backup tapes are maintained in a separate cipher–locked controlled room for a period of thirty days. After which time the tapes are moved offsite. Tapes that are sent offsite are locked in a steel fireproof container before being handed to the offsite storage courier. The bonded courier delivers the tapes and stores them in a locked room offsite.

The offsite storage facility utilizes guards, access badges, and closed-circuit cameras to ensure the security of the stored tapes. A halon fire system is activated in the case of a fire emergency.

5. Operating System and Configuration

5.1. Accounts

Running the Tiger utility shows the following accounts on the system that are disabled, but still have valid shells. The following accounts are default accounts setup by RedHat Linux and are unnecessary on this machine. Changing the shells for these accounts to **/dev/null** would reduce the threat potential of these accounts. The accounts may also be removed completely so as to not be inadvertently reactivated.

```
Login ID adm is disabled, but still has a valid shell  (/bin/sh).
Login ID bin is disabled, but still has a valid shell  (/bin/sh).
Login ID daemon is disabled, but still has a valid shell  (/bin/sh).
Login ID ftp is disabled, but still has a valid shell  (/bin/sh).
Login ID games is disabled, but still has a valid shell  (/bin/sh).
Login ID gdm is disabled, but still has a valid shell  (/bin/bash).
Login ID gopher is disabled, but still has a valid shell  (/bin/sh).
```

```
Login ID lp is disabled, but still has a valid shell  (/bin/sh).
Login ID mail is disabled, but still has a valid shell  (/bin/sh).
Login ID news is disabled, but still has a valid shell  (/bin/sh).
Login ID nobody is disabled, but still has a valid shell  (/bin/sh).
Login ID operator is disabled, but still has a valid shell (/bin/sh).
Login ID uucp is disabled, but still has a valid shell (/bin/sh).
```

5.2. Account Passwords

Using the password cracking utility, **John the Ripper**, 60% of the accounts were successfully cracked within five minutes. No super-user accounts were compromised through the use of this utility.

Initiating password aging and recycling mechanisms and periodic audits should sufficiently enforce password security. It is recommended that users change their passwords every six months. Privileged accounts should be changed every quarter.

Educating the users in password security requirements is necessary if the administrator expects them to adhere to a policy.

5.3. File Permissions

5.3.a. World-Writeable Files

World-writeable files present a serious risk to security of a system. If the file is also executable anyone with access to the system can alter the file and insert malicious code. If the file is later executed by a user logged in as super-user it could cause serious irreversible damage.

The Tiger tool identified an alarming number of world-writeable files. This was likely caused by an administrative error associated with changing the file permissions for apache directory. A recommendation in section 7.1 – Apache Web Server will address the best solution to this problem.

Appendix A lists the files that are world writeable.

5.3.b. User/Group Ownership and Permissions

The complete **/usr/local/apache** file tree has undefined group ownership. This may have been caused by an unexpected administration error. A recommendation in section 7.1 – Apache Web Server will address the best solution to this problem.

The Tiger utility identified the following problem areas, with regards to group permissions, that should be attended to by the administrator:

```
# Performing check of system file permissions...
--WARN-- [perm006w] /root/.bashrc should not have group read.
--WARN-- [perm006w] /root/.bashrc should not have world read.
--WARN-- [perm006w] /root/.cshrc should not have group read.
--WARN-- [perm006w] /root/.cshrc should not have world read.
--FAIL-- [perm007f] /etc/aliases should not have group read.
--FAIL-- [perm007f] /etc/aliases should not have world read.
--FAIL-- [perm007f] /etc/aliases.db should not have group read.
--FAIL-- [perm007f] /etc/aliases.db should not have world read.
--WARN-- [perm008w] /etc/exports should not have group read.
--WARN-- [perm008w] /etc/exports should not have world read.
--WARN-- [perm003w] /etc/fstab should not have group read.
--WARN-- [perm003w] /etc/fstab should not have world read.
--WARN-- [perm012w] /etc/inetd.conf should not have group read.
--WARN-- [perm012w] /etc/inetd.conf should not have world read.
--FAIL-- [perm015f] /etc/rc.d should not have group read.
--FAIL-- [perm015f] /etc/rc.d should not have group search.
--FAIL-- [perm015f] /etc/rc.d should not have world read.
--FAIL-- [perm015f] /etc/rc.d should not have world search.
--WARN-- [perm017w] /var/run/utmp should not have group write.
--WARN-- [perm021w] Disk device /dev/sda1 has read/write access for group
disk.
--WARN-- [perm021w] Disk device /dev/sda8 has read/write access for group
disk.
--WARN-- [perm021w] Disk device /dev/sda9 has read/write access for group
disk.
--WARN-- [perm021w] Disk device /dev/sda5 has read/write access for group
disk.
--WARN-- [perm021w] Disk device /dev/sda6 has read/write access for group
disk.
```

5.3.c. SetUID/SETGID Files

No setuid/setgid files were identified by the Tiger utility. It is recommended that scripts are not set to setuid as they present a security risk if compromised.

5.4. Running Services

Utilizing Nessus, the following ports were identified. Ports listed in bold italics are services deemed unnecessary and should be turned off.

List of open ports :

telnet (23/tcp)	***sunrpc (111/tcp)***
ftp (21/tcp)	***linuxconf (98/tcp)***
smtp (25/tcp)	***printer (515/tcp)***
www (80/tcp)	***shell (514/tcp)***
finger (79/tcp)	***login (513/tcp)***
auth (113/tcp)	***ntalk (518/udp)***

5.4.a. Telnet

As discussed earlier, this service transmits data in clear text and should not be used. Use Secure Shell, as outlined in the **Data Encryption** section that follows. Comment this out in the **/etc/inetd.conf** file and recycle **inet** to turn it off.

5.4.b. FTP

FTP also is a non-secure protocol and should not be used. Use **scp** or **rsync** with Secure Shell option in its place. Comment the ftp line out in the **/etc/inetd.conf** file and recycle **inet** to turn it off.

5.4.c. SMTP

Sendmail 8,9 was found running on this system. Sendmail has a number of vulnerabilities associated with it. Since this system performs no mail functions, Sendmail should not be run in daemon mode.

5.4.d. Finger

Finger should also be disabled in **/etc/inetd.conf**. It can provide information that is useful to an attacker and offers no valuable features to the server.

5.4.e. Auth

This is the IDENT user identification protocol server. Disable this as well.

5.4.f. Sunrpc

This is Sun's version of the Remote Procedure Protocol. If **sunrpc** is running, an intruder will attempt to query which RPC services are running. After obtaining the correct version number of the services running, the hacker can then attempt to attack known vulnerabilities.

RPC is not required for this system and should be removed. Since **sunrpc** is a service run by **init** it will need to be disabled from the **/etc/rc.d/init.d** directory byf first using the **stop** option and then remove the package.

5.4.g. Linuxconf

Linuxconf is a configuration utility for Linux. It is not required by the system and should not be enabled in **/etc/inetd.conf** to provide access to it via http. Disable this service.

5.4.h. Printer

Printing is not required by the target system. Remove the **lpd** service from the system. This is a service run from **init**.

5.4.i. Shell and Login

The are the dreaded "R-Services." They were designed to provide remote shell capabilities. They are just as non-secure as telnet and should be replaced with the Secure Shell application. These can be disabled in **/etc/inetd.conf**.

5.4.j. Ntalk

This allows remote users to us the **talk** command to conduct real-time conversations with a user on the host. This is not necessary for the target system and is considered a security hazard. Disable this in the **/etc/inetd.conf** file.

5.5. Disabling inet

The target system has no need for any of the services offered through **/etc/inetd.conf**. It is recommended that **inet** be disabled altogether.

5.6. X-Windows and Workstations Applications

The target system was originally setup using the "Custom" option from the RedHat installation cd-rom. This resulted in a combination server/workstation configuration. The more applications you have on your system, the greater the chance for a vulnerability to be discovered.

All workstation applications, including X-Windows, should be removed from this system. This will reduce the overall number of potential vulnerabilities that will require administrative attention.

Appendix A lists all the applications that should be removed from the system. This should leave you with a system containing only those server elements required to perform the server's function.

5.7. Security Patches

The target system has not been updated with any of the security fixes for RedHat 6.2. There are currently eighty-two security patches listed on the RedHat web site (see resources). The packages above should be removed prior to deciding what security patches are necessary.

5.8. Outdated Kernel

The target system is running kernel version 2.2.14-5.0smp (a stable version). The current version (2.2.16-3), which provides a security update to prevent compromise of the root account, should be installed. The current kernel can be obtained from RedHat's web site (see resources).

The administrator may also want to consider compiling the kernel to meet their specific needs. This is only recommended if the administrator is experienced in compiling kernels specific to a system and function.

6. Third-Party Applications

6.1. Apache Web Server

The Apache installation is severely flawed. It is also an outdated version and should be upgraded. As mentioned previously, the entire **/usr/local/apache** tree has been made world-writeable. It is recommended that a completely new build of Apache be installed.

6.1.a. Education and Configuration

The administrators are not familiar with the Apache product and have, therefore, not altered the configuration files beyond the basic configuration. It is recommended that the administrators receive training on this server application before attempting to configure it securely.

A good article on securing Apache's web server exists at the Apache web site (see resources). Also there is an excellent article, **Security and Apache: An Essential Primer** located at http://www.linuxplanet.com/linuxplanet/print/1527/.

6.1.b. New Build

Administrators should remove the current package and build Apache fresh from the source, using the latest stable version. Building Apache with the **mod_ssl** module is recommended to add Secure Socket Layer functionality.

6.1.c. Configuration Directives

A thorough understanding of the configuration directives is necessary to ensure that the appropriate security mechanisms are being utilized. It is also essential to prevent one directive from overriding another's security. A complete explanation of the directives is outside the scope of this report. Administrators should seek training in this area or obtain a comprehensive book. Check the Apache web site (see resources) for further information.

Following are some key areas with regards to configuration. These areas at a minimum should be checked for security issues.

Server Side Includes

It has not been determined whether the company requires this feature. It should not be enabled unless a determination is made to use it.

ScriptAlias CGI

GIAC Enterprises' developers write and test a large number of CGI scripts. These scripts should be limited to special directories that the administrators control. The **ScriptAlias** directive tells Apache that a particular directory is used for CGI scripts. All files in this directory will be executed as a script when the client requests it. All CGI scripts should be restricted to ScriptAlias'ed directories.

Overriding System Settings

Do not allow users to create **.htaccess** files that can override security settings the administrator has implemented. Use the **AllowOverride** directive with the **None** option.

Default "Deny All"

Use the following directive to protect the file system from prying eyes. This directive prevents access to file system locations. The administrator will need to create specific **<Directory>** sections for those directories where access is to be granted.

```
<Directory />
      Order Deny, All
      Deny from all
</Directory>
```

7. Data Encryption

Currently there is no means of data encryption in use on the target system. There is no requirement for encryption of data stored on the system. The information that is transferred as part of a telnet session, however, poses a serious risk to the security of the target and other systems on the network.

Administrators accessing the target system through telnet or FTP send information in clear-text over the network. This information is susceptible to packet sniffing tools, thus intruders easily obtain any passwords sent as part of the login process.

7.1. Secure Shell

Secure Shell (SSH) should be installed as a secure replacement for the r-services, telnet and FTP. Secure Shell provides data encryption of session data, including login information, to prevent the information from being "sniffed".

SSH also provides the capability to transfer data from system to system using the **scp** (secure copy) command. This is preferred over the use of FTP and eliminates one more service to check for vulnerabilities.

7.2. Secure Socket Layer

The requirement for Secure Socket Layer (SSL) protection of web traffic is not of high priority, but would provide an added layer of security to the web server function of the target system. It is recommended that SSL be installed on the target system for added protection.

7.3. Virtual Private Networking

Virtual Private Networking (VPN) allows remote connections from the Internet through a secure encrypted tunnel. If remote connections outside of the local area network are required, VPN should be implemented. VPN can either be software-based running on a networked server or integrated with a firewall. Budget and feature requirements will dictate which option is best.

8. Disaster Recovery and Backups

Disaster Recovery and Backups refer to the company's ability to resume operation in a timely manner so as to affect the least number of people for the smallest period of time.

8.1. Backup / Restore Plan

The backup and restoration plan in place was found sufficient.

8.1.a. Backup Schedule

Full backups are performed weekly on Saturdays. This is ideal as there is no traffic on the weekends.

Incremental backups are performed daily every evening at 10:00pm.

8.1.b. Restoration

Administrators have tested the restoration plan without any problems. During their tests, they tracked the time it took to restore the data and tested the integrity of the restored information.

8.1.c. Tape Rotation

Tapes are rotated to an offsite facility monthly. A contact exists between the offsite storage facility and the company to allow delivery of offsite tapes within one hour. Contact information is accurate and readily available. Complete procedures are drafted and accessible.

8.2. System Redundancy

There is no redundancy for the target system. If the system were to fail it would have to be rebuilt. The company has no plans to add redundancy for this system as it serves internal users only.

8.3. Load Balancing

There is no need for load balancing the target system. The user-base is limited and there are no expected bandwidth problems.

9. Recommendation Overview

9.1. Rebuild System

Due to the vast number of potential vulnerabilities, it is highly suggested that this server is rebuilt from the ground up. The rebuild method should take into account the server's function and install only those items necessary. In the event that this course of action cannot be carried out promptly, then the following ordered list should be carried out to improve the security of the target system.

Importance or impact on the security of the system prioritizes the list. In either case, a full backup of the system should be performed prior to performing a rebuild or carrying out the below tasks. To assist with carrying out the below tasks, it is recommended that you order a copy of **Securing Linux – Step-by-Step** from **SANS** (see resources – Appendix B).

9.2. Prioritized Task List

1 Install Secure Shell
   - Install secure shell to provide encryption of session data and file transfers (using scp)
     - Requires OpenSSL package (used for Apache also)

2 Accounts and Passwords
   - Change all passwords on the system; especially **root** since the use of telnet may have allowed these accounts to be compromised.
   - Implement password aging and password recycling mechanisms
   - Change default shell for disabled accounts to **/dev/null** or remove them

3 Disable Unnecessary Services
   - Disable inet altogether
   - Disable Sunrpc
   - Disable Sendmail daemon
   - Disable lpd daemon

4 Remove Unnecessary Packages listed in **Appendix A**

5 Update Remaining Packages to Latest Versions - http://www.redhat.com

6 Update kernel to latest "secure" release

7 Correct file system issues
   - Eliminate world writeable files
   - Correct group/world readable files listed in **Section 5.3.b**

8 Reinstall Apache Web Server with latest version - http://www.apache.org
   - Build Apache with mod_ssl
   - Disable Server Side Includes
   - Use ScriptAlias'ed CGI directories
   - Implement security through directives

9 Improve logging

- Edit **/etc/syslog.conf** to add logging for the following (use tabs – not spaces)
  - Edit kernel.* line to send messages to **/var/log/kernel** (don't forget to create the file)
  - Add lines to send warning and error messages to **/var/log/syslog** (don't forget to create the file)
- Configure log rotation to occur at prescribed intervals using **logrotate**.
- Install and configure **logcheck** to receive log updates via email

10 Draft and publish policies, procedures and standards for operation
11 Educate users in security

10. Appendix A – File Listings

10.1. Unnecessary Packages

The following packages were found installed on the target system. These packages are unnecessary for the target system to perform its function. These packages should be removed to reduce the number of potential vulnerabilities.

arpwatch-2.1a4-19
audiofile-0.1.9-3
audiofile-devel-0.1.9-3
autoconf-2.13-5
automake-1.4-6
bind-8.2.2_P5-9
bison-1.28-2
bug-buddy-0.7-1
byacc-1.9-12
cdecl-2.5-10
control-center-1.0.51-3
control-center-devel-1.0.51-3
control-panel-3.13-1
cproto-4.6-3
ctags-3.4-1
cvs-1.10.7-7
desktop-backgrounds-1.1-1
dev86-0.15.0-2
diffstat-1.27-2
dump-0.4b15-1
ee-0.3.11-1
ElectricFence-2.1-3
elm-2.5.3-6
enlightenment-0.15.5-48
enlightenment-conf-0.15-9
esound-0.2.17-2
esound-devel-0.2.17-2
exmh-2.1.1-3
expect-5.28-35
extace-1.2.15-1
fetchmail-5.3.1-1
flex-2.5.4a-9
fnlib-0.4-10
fnlib-devel-0.4-10
fortune-mod-1.0-11
fvwm2-2.2.4-4
fvwm2-icons-2.2.4-4
gd-devel-1.3-6
gdb-4.18-11
gdbm-devel-1.8.0-3
gdm-2.0beta2-23
gedit-0.6.1-3
gettext-0.10.35-17
gftp-2.0.6a-3
git-4.3.19-2
glade-0.5.5-4
glib-devel-1.2.6-3
glib10-1.0.6-6
gmc-4.5.42-10
gnome-audio-1.0.0-8
gnome-audio-extra-1.0.0-8
gnome-core-1.0.55-12
gnome-core-devel-1.0.55-12
gnome-games-1.0.51-4
gnome-games-devel-1.0.51-4
gnome-libs-1.0.55-12
gnome-libs-devel-1.0.55-12
gnome-linuxconf-0.25-2
gnome-objc-1.0.2-6
gnome-objc-devel-1.0.2-6
gnome-pim-1.0.55-1
gnome-pim-devel-1.0.55-1
gnome-users-guide-1.0.72-1
gnome-utils-1.0.50-4
gnorpm-0.9-15
gnotepad+-1.1.4-3
gnumeric-0.48-3
gpgp-0.4-2
gpm-1.18.1-7
gpm-devel-1.18.1-7
gqview-0.7.0-4
gtk-engines-0.10-3

gtk+-1.2.6-7
gtk+-devel-1.2.6-7
gtk+10-1.0.6-6
gtop-1.0.5-1
guile-1.3-10
gv-3.5.8-9
helptool-2.4-9
ical-2.2-11
lmageMagick-4.2.9-3
imlib-1.9.7-3
imlib-cfgeditor-1.9.7-3
imlib-devel-1.9.7-3
indent-2.2.5-2
inews-2.2.2-3
irda-utils-0.9.10-1
ispell-3.1.20-25
jade-1.2.1-9
kernelcfg-0.5-5
krb5-configs-1.1.1-9
krb5-devel-1.1.1-9
krb5-libs-1.1.1-9
kudzu-devel-0.36-2
libghttp-1.0.4-1
libghttp-devel-1.0.4-1
libglade-0.11-1
libglade-devel-0.11-1
libgr-2.0.13-23
libgr-devel-2.0.13-23
libgr-progs-2.0.13-23
libgtop-1.0.6-1
libgtop-devel-1.0.6-1
libjpeg-6b-10
libjpeg-devel-6b-10
libpng-devel-1.0.5-3
librep-0.10-2
libtermcap-devel-2.0.8-20
libtiff-3.5.4-5
libtiff-devel-3.5.4-5
libtool-1.3.4-3
libungif-4.1.0-4
libungif-devel-4.1.0-4
libxml-1.8.6-2
libxml-devel-1.8.6-2
libxml10-1.0.0-2
linuxconf-devel-1.17r2-6
ltrace-0.3.10-2
lynx-2.8.3-2
m4-1.4-12
magicdev-0.2.7-1
man-pages-1.28-6
mc-4.5.42-10
memprof-0.3.0-4
Mesa-3.2-2
Mesa-devel-3.2-2
metamail-2.7-23
modemtool-1.21-6
mutt-1.0.1i-6
ncurses-devel-5.0-11
netcfg-2.25-1
netscape-common-4.72-6
netscape-communicator-4.72-6
newt-devel-0.50.8-2
nmh-1.0.3-6x
ORBit-0.5.0-3
ORBit-devel-0.5.0-3
patch-2.5-10
pciutils-devel-2.1.5-2
pine-4.21-8
pmake-2.1.34-3
printtool-3.44-1
pygnome-1.0.51-1
pygnome-libglade-0.6.4-1
pygtk-0.6.4-1
pygtk-libglade-0.6.4-1
python-1.5.2-13
pythonlib-1.23-1
rcs-5.7-11
rdist-6.1.5-12
readline-devel-2.2.1-6
rep-gtk-0.8-1
rep-gtk-libglade-0.8-1
rpm-devel-3.0.4-0.48
rpm-python-3.0.4-0.48
rxvt-2.6.1-8
sawmill-0.24-3
sawmill-gnome-0.24-3
screen-3.9.5-4
sgml-common-0.1-7
sgml-tools-1.0.9-5
shapecfg-2.2.12-2

sharutils-4.2.1-2
slang-devel-1.2.2-5
slrn-0.9.6.2-4
strace-4.2-1
svgalib-1.4.1-2
svgalib-devel-1.4.1-2
switchdesk-2.1-1
switchdesk-gnome-2.1-1
tcl-8.0.5-35
tclx-8.0.5-35
tetex-fonts-1.0.6-11
tetex-xdvi-1.0.6-11
texinfo-4.0-5
timetool-2.7.3-1
tin-1.4.2-3
tix-4.1.0.6-35
tk-8.0.5-35
tkinter-1.5.2-13
tksysv-1.1-3
trn-3.6-21
ucd-snmp-4.1.1-2
ucd-snmp-utils-4.1.1-2
umb-scheme-3.2-11
up2date-1.13-1
urlview-0.7-5
usermode-1.20-1
words-2-12
X11R6-contrib-3.3.2-11
Xaw3d-1.3-21
Xaw3d-devel-1.3-21
xchat-1.4.0-1
Xconfigurator-4.3.5-1
XFree86-3.3.6-20
XFree86-75dpi-fonts-3.3.6-20
XFree86-devel-3.3.6-20
xinitrc-2.9-1
xloadimage-4.1-13
xmailbox-2.5-9
xpdf-0.90-4
xpm-3.4k-2
xpm-devel-3.4k-2
xrn-9.02-3
xscreensaver-3.23-2
xsri-1.0-4
xxgdb-1.12-13
zlib-devel-1.1.3-6

10.2. World Writeable Files

/var/lib/svgalib/

The whole /usr/local/apache is world-writeable.

11. Appendix B – Resources and References

This appendix lists the key resources and references used to compile this report. All URLs were valid at the time of this writing.

11.1. Tools

The following tools were used to provide audit information for this report. The output of these tools is available upon request.

Tiger – Host scanner that checks the local system used to identify security related problems as defined in its configuration file.
ftp://net.tamu.edu/pub/security/TAMU/

Nmap – A full-featured port scanning utility that supports a number of different methods of scanning.
http://www.insecure.org/nmap/index.html

Nessus – Intrusion scanning tool that attempts to identify security holes based on known vulnerability. Utilizes **Nmap** and has library of more than 200 attacks. Plug-in language allows new attacks to be added.
http://www.nessus.org

Lsof – Utility that lists open files, network connections, pipes, streams, etc…
ftp://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/lsof/

John the Ripper – Utility to crack passwords
http://www.openwall.com/john/

11.2. Web Sites

RedHat Linux Web site
http://www.redhat.com

Security Focus Web site
http://www.securityfocus.com

CERT Web site
http://www.cert.org

CIAC Web site
http://ciac.llnl.gov

Security Portal
http://www.securityportal.com

Apache HTTP Server Web Site
http://www.apache.org

Apache SSL Web Site
http://www.apache-ssl.org/

11.3. Books

RedHat Linux Administrator's Handbook
– Mohammed J. Kabir

Securing Linux – Step-by-Step
– The SANS Institute

Practical UNIX and Internet Security
– Simson Garfinkel and Gene Spafford