Global Information Assurance Certification Paper

Linux E-Commerce Server Security Audit

For
GIAC Enterprises

GCUX Practical Assignment version 1.9

Option 2 – Consultant's Report From Auditing Unix

Prepared by: Seng Guan Lee

July 2002

Table of Contents

Executive Summary

Introduction

GIAC Enterprises (GIAC) has introduced its e-commerce effort to streamline the operation of selling fortune cookie from order taking to order fulfillment. The store-front for its e-commerce system is a web-based server that takes order from customers and feeds the order to the back-end database system that is connected to other GIAC enterprise systems. This audit gives GIAC a detailed analysis of the store-front server, which runs on Linux operating system with Apache web server application.

Currently, GIAC is using this e-commerce system to consolidate different sale channels' orders at the web-based store-front server. As a key component of its e-commerce infrastructure and facing more external threats from direct Internet connection, keeping the store-front Linux server running is of highest concern for GIAC.

Scope

This document looks specifically into Linux system within GIAC e-commerce information infrastructure. The primary objectives are assessing the platform security, which includes

(i) Hardware configuration
(ii) Operating System
(iii) System utilities

Secondary objectives are to review or assess

(i) Security policies, standards and procedures
(ii) Access controls
(iii) Backup and disaster recovery readiness
(iv) Application security

GIAC intends to carry out security audit on all enterprise system pending the result of this audit.

Major Recommendations

Recommendations are classified either as Quick Fixes or Strategic Initiatives.

Quick Fixes: Easily executed actions such as configuration changes or file deletions/updates that resolve security vulnerabilities. Additionally, actions that should be taken immediately to resolve critical vulnerabilities, even if they require more upfront evaluation are included as well.

Strategy Initiatives: Actions that should be taken to secure the computing environment but include significant change to system/network architecture or operation processes and therefore require proper planning and careful execution. Actions that should be taken to improve the impact of corporate policies and procedures on security are also included in this category.

Quick fixes

- Update server with latest, relevant Red Hat errata packages.
- Remove unnecessary services and rpm packages.
- Password-protect LILO (Linux Loader) prompt.
- Password-protect single user mode.
- Apply stricter host-based packet filtering to control access from internal network.
- Remove compilation tools from core Operating System.
- Apply stricter control on excessively liberal file systems.
- Build new version of Apache with latest third party modules and programs.
- Implement user password management controls.
- Apply “least privilege” principle to system administrator accounts.

Strategic Initiatives

- Create a kickstart script to build a hardened Linux kernel image specific to the hardware use.
- Use security applications to protect Linux system.
  - files fingerprinting, e.g. tripwire
  - mandatory access control, e.g. LIDS (Linux Intrusion Detection System)
  - log files auditing, e.g. logcheck
- Incorporate procedure to perform application assessment to identify and mitigate in-house application security issues.
- Establish procedure to enforce change control.
- Separation of duty for system administrator and database administrator.
- Build a dedicated information security organization, including roles such as Security Manager and Security Administrator, this organization should report directly to GIAC CEO or CTO.
- Establish enterprise wide security program.

1 System Description

1.1 Hardware platform and specifications

GIAC uses IBM Nefinity 5600 to run the store-front web application. Reliability of the server is improved through the ServeRAID adapter card that enables the server system disk to be mirrored. Availability of the store-front Linux server (also known as "audited server" in this document) is increased by having a hot standby server with identical hardware and software configuration as the production server.

Model	: IBM Nefinity 5600
CPU	: 2x Intel Pentium III 733 MHz
Memory	: ECC SDRAM 1 GB
Graphics	: (Onboard) Chipset S3 Trio 3D SDC388/86C365
SCSI	: (Onboard) Adaptec 7897 (Chipset 2x AIC-7896)
RAID	: ServeRAID 3H Ultra2 SCSI Adapter
Network	: PC 10/100 Ethernet Integrated
Hard disk	: 2x (SCSI Ultra2) 9.1 GB
Floppy	: 1x 3.5"
CD-ROM	: 1x ATAPI CDROM drive 40X

1.2 Operating System and version

The audited server uses Linux Operating System (OS) to run its web application. This Red Hat Linux version is relatively stable and has been used in production server since about a year ago and has not been upgraded.

Operating System: Red Hat Linux v7.1

1.3 Role of system

GIAC e-commerce and enterprise network is a separate network segment with its own dedicated Internet connection. This network segment uses a two-tier architecture, which includes front-end web server providing GIAC customers with a web-based interface to manage their own accounts and order fortune cookie. The back-end line of servers and databases hold transaction data and customer information. These back-end database servers are protected by another firewall that separates it from the front-end servers.

The primary role of the store-front Linux server is to present web pages for customers to manage their own account information and more importantly to accept purchase request from them. There are currently two store-front servers with one in live mode and the other in hot standby mode. As a front-end server, the audited system faces more threats from the Internet than other back-end servers.

The simplified network architecture surrounding the store-front Linux server is depicted in Figure 1.1

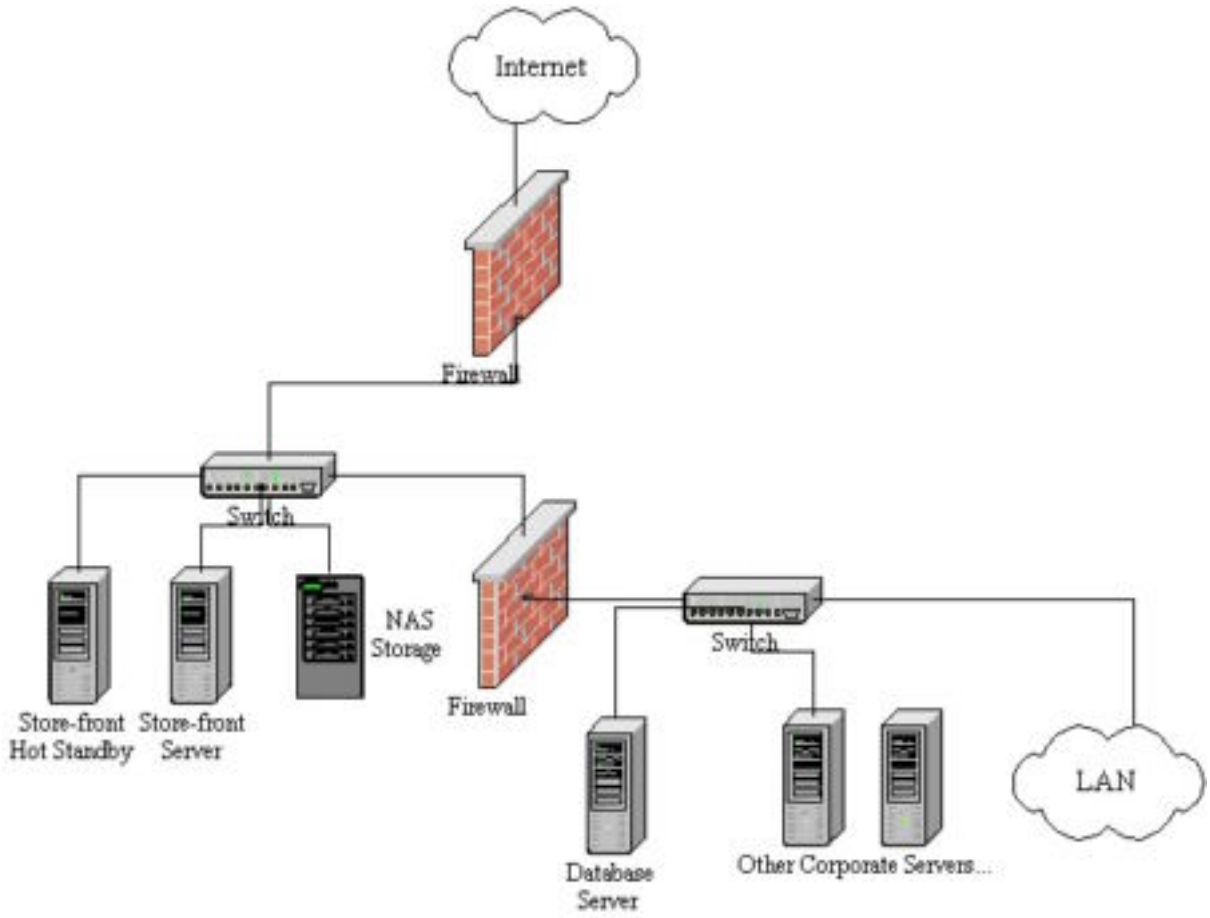

Figure 1.1 Simplified GIAC network diagram

1.4 Applications and Tools

GIAC store-front Linux server runs *Apache* web server to provide HTTP service. It also runs *monit* to monitor and restart running daemons and alert failures through email. *Openssh* is installed for system administrator to remotely log into the server to perform administrative tasks securely. GIAC in-house software adds order handling and account management capabilities to this server. Overall, these key applications provide the functionality the store-front Linux server needs and the tools to administer it. Versions of these key applications and tools are listed below:

- Apache version 1.3.20 built with
  -mod_ssl version 2.8.4
  -mod_perl version 1.25 (openssl 0.9.6)
  -php version 4.0.5
- Monit version 2.2.1
- Openssh version 2.5.2p2

Although these applications were primarily design to operate in Internet environment and secure configuration for them are readily available on the Internet, they nonetheless

introduce their application specific threat into the audited system. Moreover, poorly managed or badly configured application can put the overall system at an even higher risk. These applications also increase the complexity of monitoring vulnerability warning especially those that are less commonly use, for example vulnerability in *monit* may not be featured in major vulnerability advisory system such as *Bugtraq.*

2 Audit Methodology

IT security audit is a policy-based assessment of a particular system and/or network and the procedures and practices of that location. It assesses the level of risk created by these actions and gives a snapshot of the security readiness of a system and/or network.

This particular audit looks beyond the audited system and consider also the human interface to the IT system, i.e. whether security best practices are being use to keep their IT system operating effectively. Basically, the audit was carried out in the following sequence:

2.1 Preparation

After evaluating GIAC objectives and boundary for this audit, it was understood that GIAC specifically required to evaluate the security readiness of its store-front Linux server. Preparation for the audit focused on this single component of GIAC e-commerce network. This single server will be scrutinized to a high level to determine the security issues that may be present.

2.2 Reviewing Policy and Documentation

Security Policy is used as a basis for the work of auditing GIAC storefront Linux server. Policy governing the use, upgrade, and administration of this server was checked for its completeness. Policy governing the configuration of the server was evaluated for its comprehensiveness. The dissemination procedure for the security policy was evaluated for its effectiveness.

Documentation stating the procedure for administrating the server was also checked. Logs for application of patches, system configuration change etc. were also reviewed.

2.3 Interviewing/Talking

Interviews with GIAC technical staff, ordinary application user and manager were carried out to determined whether they have seen and read the security policy and to find out from them personally what can and cannot be done on the audited server.

Actual procedures for changing, recovering, adding user etc. were determined through talking with system administrator and other technical staff. These interviews and casual talks also reveal exactly what the system is used for.

2.4 Technical Investigation

Technical investigation for the audited system began with determination of the system ownership and custodian. It also determined the security classification of the server, data on the server and the network segment that the audited server resides in. The investigation then looked into the audited server from three different angles.

2.4.1 Server build and maintenance processes assessment

First, an assessment of the server build process was performed. However, as the audited server has been installed for more than a year, system administrator cannot recall some details of the build process. No documentation was kept by GIAC for this server build. The purpose of this assessment is to ensure that

- software was obtained from secure and trusted site
- only packages that are required are installed
- security tools are deployed

After that, server maintenance processes was evaluated. In particular, how system custodian monitor new security patch release by vendor and whether latest patches have been tested in test environment before they are applied to the live server. Usually, most vulnerability found in the servers can be attributed to poor system maintenance behavior that includes poor patch management. Change control procedures and practices were looked into.

Then, GIAC in-house software development life cycle was briefly looked into. It was understood that GIAC has different technical person to test in-house program codes. However, no full code review was carried out during the software development life cycle.

2.4.2 Security scan by audit tools

Both network and host based audit tools were used in this security audit to reveal potential vulnerabilities. *Nmap* and *Nessus* were used to scan for open ports and known vulnerabilities from beyond the firewall. Location where the network audit tools were placed is indicated in the Figure 1.2.

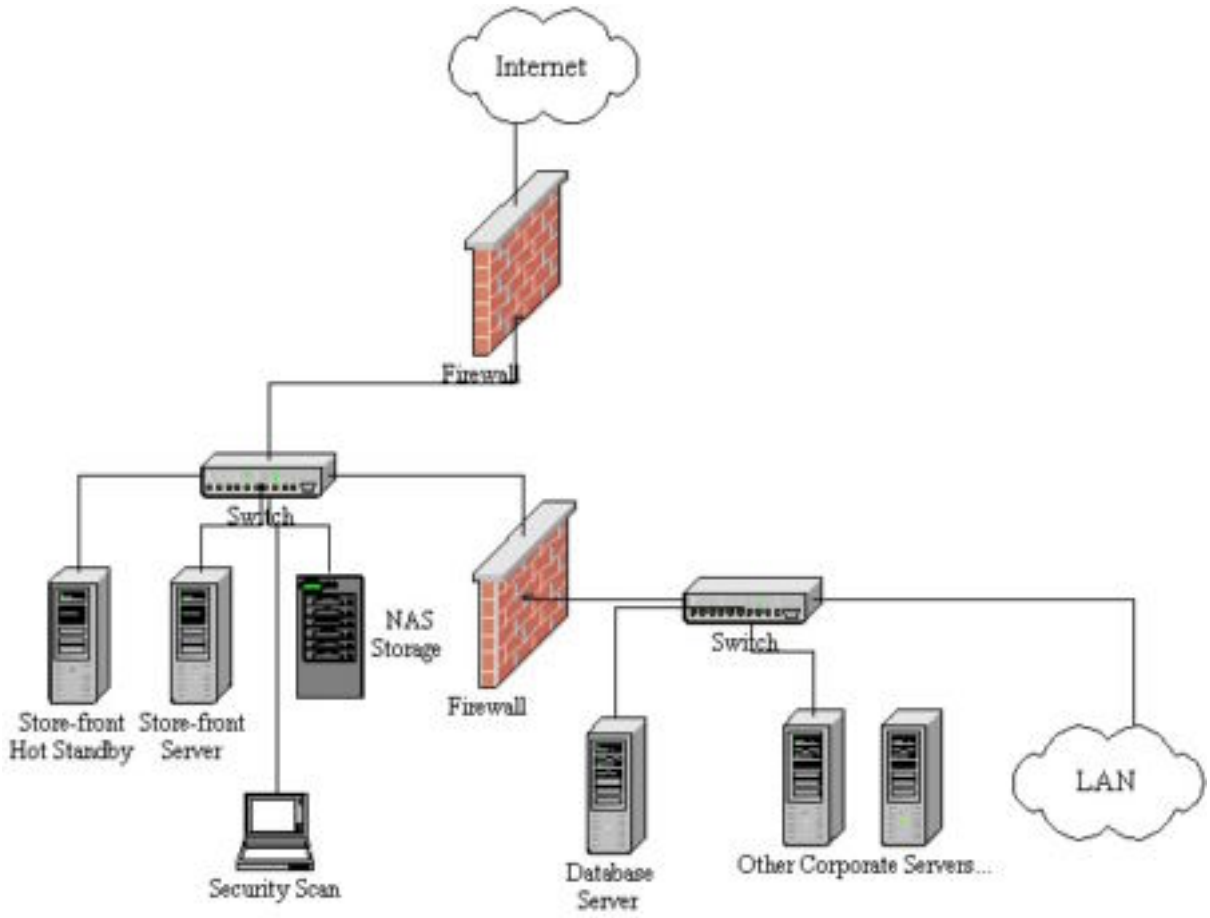

Figure 1.2: Position where the scanning tools were placed for scanning

CISscan was used to check for OS configuration problem. As some negatives report by *CISscan* might not be applicable to the audited system, only warnings are relevant were highlighted in this report. *John the ripper (Jtr)* was used to crack password file obtained from the audited system. As there are several Chinese and Indian among the system administrators and users, Chinese and Indian dictionary were used in this password cracking exercise. No password was cracked after running *Jtr* for two days. Complex combination (brute force method) was not performed due to time constraint.

Results of scan by the audit tools can be found in Appendix A.

2.4.3 Running through security checklists

Security checklists for securing Linux and Apache were ran through manually to determine the soundness of the audited system. These two checklists were consolidated from

- Linux Security Quick Reference Guide by Dave Wreski of Guardian Digital Inc.
- Auditing Linux By Krishni Naidu
- Securing and Optimizing Linux: RedHat Edition by Gerhard Mourani

This exercise also served to verify system configuration weaknesses reported by *CISscan*. Unix commands such as *lsof*, *netstat*, *find*, *chkconfig* etc. were used to either confirm or reject potential vulnerabilities found by audit tools *nmap*, *nessus* and *CISscan*. Actual command issued and their output can be found in the appendix A.

2.5 Reviewing Data and Report Write-up

Data collected by various tools were studied for applicability and accuracy. Only issues that can be positively identified were raised. Appropriate vulnerability warnings issued by Red Hat and other vulnerability advisory systems were searched to support claim of vulnerabilities existence. System configurations weakness were also identified and included in the report. Finally, this write up was prepared and presented to GIAC management.

3 Detail Analysis

3.1 Operating system vulnerabilities

Currently, GIAC store-front server is built with Red Hat Linux Operating System (OS) version 7.1. The latest Linux distribution as of this writing is version 7.3. Although the current live server OS is two versions behind the latest, it is a relatively stable version and the vendor, Red Hat, is still supporting this version in term of releasing software patches. Though it is not an issue to use an older Linux distribution, keeping up with vendor patches is critical for the security and reliability of the server. GIAC store-front Linux server has failed to keep up with vendor software patches.

These operating systems vulnerabilities were found on the GIAC audited system. However, note that some of them can be eliminated by remove the rpm packages from the system rather that applying patch as the programs are not required by this server.

sudo-1.6.5p2-1.7x.1
wu-ftpd-2.6.1-16.7x.1
sendmail-8.11.6-2.7.1
openldap-2.0.21-0.7.1
cyrus-sasl-1.5.24-22.7
xinetd-2.3.3-1
diffutils-2.7-23
openssh-server-3.1p1-5
openssh-clients-3.1p1-5
at-3.1.8-23
glibc-devel-2.2.4-24
man-1.5i2-0.7x.5
openldap-devel-2.0.21-0.7.1
zlib-1.1.3-25.7
kernel-headers-2.4.9-34
glibc-common-2.2.4-24

openssh-3.1p1-5
cyrus-sasl-devel-1.5.24-22.7
zlib-devel-1.1.3-25.7
groff-1.17.2-7.0.2
kernel-2.4.9-34
docbook-utils-0.6-13.2
docbook-style-dsssl-1.64-2

Other rpm packages that have bug fixed or enhancement upgrades are listed below. They should be updated as well.

modutils-2.4.13-0.7.1
popt-1.6.4-7x
e2fsprogs-1.26-1.71
e2fsprogs-devel-1.26-1.71
pam-0.75-18.7
pam-devel-0.75-18.7
quota-3.01pre9-0.7.1
rpm-4.0.4-7x
rpm-build-4.0.4-7x
rpm-devel-4.0.4-7x

For detail description of each security problem or bug fixed, please refer to:

http://rhn.redhat.com/errata/rh71-errata.html

3.2 Security patch installation and management

In operation security, the continual effort of making sure that right policies, standards and procedures are in place (due care) and being followed (due diligence) is critical. The principle of due care and due diligence is applicable to security patch management. Currently, GIAC lacks policy and procedure to guide proper implementation of security patch management. Security patch installation requirement is evaluated on ad-hoc basis. Administrators or managers sound alarm only when vulnerability report is stumbled upon. Then this particular vulnerability will be evaluated on the server. Other vulnerabilities might be discovered during the investigation.

Software patches are applied directly onto live server with hot-standby server retaining the old system software configuration for a week (to provide fallback if patch creates unforeseen problem). No effort was put into looking for specific OS (Red Hat Linux v7.1) and applications (e.g. Apache) vulnerability alerts or advisories relevant to the store-front Linux server. OS patches were installed during initial installation but further upgrade was badly managed and resulted in several vulnerabilities not being patched.

Several OS patches release by the software vendor were not applied as a result. This includes kernel patches. Application like Apache was not updated since the first day

they were built and installed. *Autorpm* was run and Red hat specific upgrades available but not installed are listed in Appendix A-7.

3.3 Configuration vulnerabilities

Configuration weaknesses were discovered from going through Linux security checklist and reports generated by *CISscan* security benchmarks and scoring tool. It is worth noting that Internet service daemons *inetd* was not started on this server. However, this service was installed for system administrator to start network service such as FTP or Telnet when required.

3.3.1 Unnecessary services

Running unnecessary programs increase the security exposures of the system. Disabling unused programs and unnecessary services from Internet facing server is an effective way to reduce risks originating from a remote host. Removing them from the file systems will further reduce risks from host-based vulnerabilities.

Open ports on the store-front server detected by *nmap* and confirm by "netstat –aut" command are listed in Appendix A-1 and A-2. Some of these ports are opened by services that need not be run on this audited server. For a recommended list of services that can be disabled, refer to section 4.2.1.

3.3.2 Unnecessary binaries and source files

Instead of applying the conventional best security practice of installing individual required rpm packages, GIAC custom installation selected a few Red Hat Linux component groups of rpm packages for installation. As a result, an excessive number of unnecessary packages are installed on the production server. For example packages such as *gcc* (the GNU C compiler), *gdb* (the GNU debugger) and *make* introduce risk to production hosts because they provide a malicious attacker with the functionality to compile and debug local exploits. GIAC built Apache application with custom modules and configuration during server build process. Development tools and programs were used for compilation of the application, however they should be removed from the production server after the installation.

Other packages such as *raidtools*, *pump* and *ntsysv* from the "Base" component group, which are installed by default but not use, should not be left on the audited server. Each of these unnecessary programs represents potentially added risk to the production system.

Source files for Apache and its custom modules are also left on the production server after the compilation. Some of the source files are unowned (wrong userid and groupid) and some of them are world-writable. Local user may escalate their access right to that of the root user by exploiting vulnerabilities in other programs through these unowned or world-writable files. Lists of such files are in Appendix A-5.

3.3.3 System boot process

The audited system does not protect the server from anyone who has physical access to the server. Linux bootloader, LILO, offers a lot of ways to get root privilege by people who have physical access to the machine. For example, booting to single-user mode, using an alternate init program and specifying an alternate root partition by passing LILO command-line kernel parameters at boot time. These are features of LILO for system administrator to recover the system from errors, but it also makes it easy for someone to get in inconspicuously. Single user mode can be entered when the server boot encounter errors. For example when *fsck* failed at boot, system will escape into single-user mode.

The following LILO and system boot up process configuration weaknesses enable attacker to take control from system console easily.

- Ctrl-Alt-Del shutdown is not disabled in /etc/inittab system initialization file.
- Single-user mode is not password protected.
- LILO is not password protected.

3.3.4 Loosely configured host-base firewall

Host base firewall, using *iptables*, was used in the audited server to provide depth of defense for itself. Existing *iptables*'s Access Control Lists on the store-front server only restrict traffic from the network interface that has public IP address. Thus, the protection that it gives is only for the threats from Internet and not from internal network users. In fact internal users account for majority of the security breaches, it is therefore recommended that GIAC reconfigure its host base firewall to protect the audited server from internal users as well.

3.3.5 Liberal file, directory and file system protection

Permissions on system files are crucial to maintain host integrity. Unauthorized and unnecessary use of setuid, setgid permissions enable anyone to run "set-user-identifier root" programs as root user. Some programs are setuid or setgid to enable user to perform operations that would otherwise require root privilege. These programs setuid or setgid can be removed if no user requires them. Programs or files with setuid or setgid, unowned or world writable are listed in Appendix A-4 and A-5.

The audited server was also found with very liberal file system, default setting from installation remains for all partitions. Read-write is permitted, allow set-user-identifier or set-group-identifier bits to take effect and allow execution of any binaries on all mounted file systems listed below.

- /
- /boot
- /usr
- /var

Recommended settings for these file system can be found in section 4.7.

Removable media is a common way for malicious program to be introduced to the system. Removable file system /mnt/floppy and /mnt/cdrom for the audited server are not mounted nosuid. Option nosuid should be added to the /etc/fstab lines for these device. Furthermore /etc/security/console.perms lines which contain either "floppy" or "cdrom" should be removed so that normal user is not allowed to use these devices.

3.3.6 Poor Password management

It is noted that shadow password with MD5 hashing and Pluggable Authentication Modules (PAM) are enabled on the audited server. However, no password expiration is enforce for both store-front and database servers. The only time when privilege account password was changed was when one of the system administrator left GIAC. There is no relevant policy to guide the configuration of password management control. It is recommended that appropriate restrictions is put in place over password syntax as required by relevant corporate policy and standard:

- Minimum password length
- Restrictions on password syntax (e.g. limits repeating characters, requires alphanumeric and special character etc.)
- Password lifetime
- Restriction on ability to re-use passwords
- Message presented to user to indicate date and time of last log on

3.3.7 Application that run in a privilege states

No non-system application or program was found to be running in privilege state in the audited server. Program that run in privilege mode poses higher risk to the system. If vulnerability in it is exploited, attacker would have gained root privilege and be able to do anything to the system he wants. Therefore, it is recommended that GIAC continue to monitor the audited server for unauthorized programs that run in privilege mode regularly.

3.3.8 Banner

Default Red Hat 7.1 banner is still being used on the audited server. This banner will reveal OS version information. It is recommended that GIAC use the banner to give warning for inappropriate use of the system instead of revealing its own identity. This warning might help to prosecute unauthorized users of the computing system as well. The warning should states:

- Who owns the computing system.
- Fact that unauthorized usage is illegal and violation of laws.
- Users activities may be monitored.

Below is a sample banner message that could be included in file */etc/issue*, */etc/issue.net* and */etc/motd*.

```
Warning!!!
Computing activities other than those authorized by GIAC
Enterprise is strictly prohibited on this computer. Unauthorized
use or access is regarded as a criminal act in the nature of
theft and violator is subjected to civil and criminal
prosecution. User's activities may be monitored on this computer
without prior notice.
```

3.3.9 Run-time kernel configuration options

Run-time kernel configuration options in the audited system were not tuned to improve security through the /proc pseudo file system. For example enabling IP source routing, where routing path for an IP packet is in the packet itself, is risky because receiving host need to respond in the same routing path. If an attacker is able to send source routed packet into the network where the host reside, he would be able to intercept the respond and fool the host into thinking that it is communicating with a trusted host. Source routing can be disabled by

```
# echo 0 > /proc/sys/net/ipv4/conf/all/accept_source_route
```

Alternatively, the file /etc/sysctl.conf contains /proc/sys/ setting that is processed at system startup. The following network parameters setting for /etc/sysctl.conf is recommended to improve security for the audited server.

```
net.ipv4.ip_forward = 0
net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects= 0
net.ipv4.conf.all.log_martians = 1
```

For explanation of each of these parameters, refer to:

http://www.linuxhq.com/kernel/v2.4/doc/networking/ip-sysctl.txt.html

3.4 Risks from installed third-party software

3.4.1 Apache

Apache is the most widely used HTTP-server in the world. GIAC Apache web server was built from source with custom third party modules and programs like mod_ssl, mod_perl, and PHP4. Care has already been taken to properly set the permissions for files and directories for web server and its configuration files has been immunized. Run time configuration file, /usr/local/Apache/conf/httpd.conf, has also been configured with sercurity in mind. For example automatic indexing has been disabled.

Although the audited server's Apache configuration has already implemented security related configuration and other best practices in running a secure web server are also followed, the version of Apache used is outdated and contains vulnerabilities that were discovered recently. A recent vulnerability noted in CAN-2002-0392 (mitre.org) and [CERT VU#944335] deal with the issue of handling of chunked transfer encoding in Apache web server. This remote vulnerability can be used to launch a denial of service attack and in some cases allow arbitrary code to be run on the server.

Modules built into Apache also have their own vulnerability. For example

- mod_ssl: buffer overflow (CAN-2002-0082)
- PHP: flaw in multipart/form data POST request handling (CVE-2002-0081)

It is recommended that GIAC rebuild the Apache application from the latest source files.

3.4.2 Openssh

The version of openssh used on the audited server flaws such as:

- one that can be exploited remotely and give an attacker a shell on the host.
- another that allow a local user to execute command with root privilege through environment variable vulnerability as noted in CVE-2001-0872.

New updates for openssh from Red Hat should be applied immediately.

3.5 Administrative practices

In general, the roles and responsibilities of systems custodian are well understood by individual system administrator. These roles and responsibilities are in line with the employee's employment contracts. However, there are no formal definition or documentation for security administration. Basically, insufficient standards and guidelines were laid down with regard to general administrative practices in GIAC.

3.5.1 Logging, reporting and auditing

The audited system uses Linux *syslog* facility to log activities on the servers. These logs are not monitored and reviewed regularly by the system administrator. Review of logged information at GIAC is event-oriented, it is recommended that these logs are reviewed periodically according to the need for GIAC.

Nevertheless, default Linux *syslog* facilities is insufficient to ensure that appropriate security events are logged to provide the abilities to monitor system security properly. GIAC should consider using *LIDS* for mandatory access control, *tripwire* for binaries and files finger printing and *logcheck* to automate and provide real-time audit analysis of system logs and logs produce by the other tools. With this security tools in place, GIAC will be able to reduce damage to the whole system by early detection of intrusion and restrict modification or deletion by using stricter file system access control.

3.5.2 Separation of duties

The objective of separation of duties is to ensure that one person acting alone cannot compromise the security of GIAC e-commerce system in any way. Activity such as system administration for order taking and processing server and data capturing and storing server should be assigned to different individuals. This arrangement ensures that GIAC does not put a dangerously high level of trust on one person. Other high-risk activities should have similar arrangement.

Currently in GIAC, same group of system administrator is administering the store-front and back-end database server. They have the privilege account passwords for both servers and database. This enables a single person in GIAC to carry out dangerous fraudulent act to compromise the integrity of the e-commerce system. It is recommended that GIAC practice separation of duties for this system administrator group and at the same time practice job rotation so that GIAC will always have more than one person who understands tasks and responsibilities of these two specific roles.

3.6 Identification and protection of sensitive data on the host

GIAC does not a formal data classification scheme. Though it is understood by the system administrator, users and manager that customer information and customer orders are sensitive data. This data is processed on the audited server but does not reside on it. However, data such as application logs that support non-repudiation objective (to provide prove for important customer click on the web application) were created and reside on the server for up to four weeks, although it was backup on a daily basis. It is recommended that GIAC backup application logs in a real time manner.

3.7 Protection of sensitive data in transit over the network and Internet

Data in transit over the network can be easily sniffed. The risk of confidential data traversing public network being picked up by unauthorized party is high. Confidentiality and integrity of the data can easily be compromised. It is always recommended that sensitive data in transit over the network have to be encrypted.

3.7.1 Public Network

Transaction data flowing through the public Internet is all in the encrypted SSL tunnel. Store-front web pages are served through secure https protocol. Remote administration access to this store-front server is all done through secure-shell (ssh) protocol regardless whether it is done from the private or public network.

This arrangement is sufficient for the operation and administration of store-front server.

3.7.2 Private network

Information traversing between the two-tier network architecture is all in the clear. Transaction data flowing from store-front Linux server to backend database server is in the clear. This private network is assumed to be secure by GIAC. Data on the database server are not encrypted as well.

This arrangement is fine as long as the entire private network segment is classified to the same security level as the most sensitive data that traverse this network (probably highest level in GIAC security classification) and proper control for the operations of all devices and systems in this segment is in place.

3.8 Access controls

3.8.1 Account management

It is noted that unused generic and share account has already been removed from the audited server. GIAC system administrators use their own user account to log in to the audited server and use *sudo* to gain privilege to perform administration tasks. All system administrator accounts are placed in a privilege group, only accounts in this privilege group are able to gain root privilege. There is no restriction on any Unix commands this group of privilege users cannot use once they *sudo* to root privilege. All *sudo* actions are logged.

In-house application administrator has an account on the server. This account only allows log viewing etc. but do not have privilege to manage changes to the live system. System administrator grant this account "*sudo*" when privilege task need to be performed by application administrator.

The principle of least privilege was applied to the user and application administrator of the audited system. However, system administrator has full root privilege after "sudoing". It is recommended that GIAC use features of *sudo* utilities to enforce least privilege principle even on system administrator by restricting the privilege commands that can be executed.

3.8.2 Password management

People tend to be the weakest link in the entire security architecture. Poorly selected password or poor password handling can easily result in password being stolen. The degree of damage is only restricted by the privilege the compromise password has. Modern OS has the ability to enforce various restrictions on the selection of password to ensure that easily "guessable" password cannot be used. GIAC does not have policy or standard to guide the configuration of password management controls or awareness program to educate users on the importance of good password management. Refer to section 3.3.6 for more detail discussion.

3.8.3 User and Group profile configurations

Default system users (e.g. bin, daemon, ftp, mail, and nobody) in /etc/passwd has a valid /bin/sh shell since their account's shell field is empty. All these users do not need a valid shell and should be given /bin/false in the shell field.

Permission of files created by user is determined by the default umask setting of his profile or system wide profile configuration. User with improper umask setting might

create group or world-writable files that may be used to compromise their account. System wide profile setting should be configured to help prevent user from using more liberal umask. GIAC audited server system wide profile files /etc/profile, /etc/csh.login, /etc/csh.cshrc and /etc/bashrc do not have default umask setting of 022.

3.8.4 Remote access

No modem access is available for this server. Remote access is only available through *ssh*. Direct remote root log in is not permitted on the audited server.

3.8.5 System boot process

There are two major flaws in the system boot process. Firstly, boot loader command prompt is not secure with password. Secondly, insufficient control is in place, resulting in unnecessary system services being initiated during system boot. Please refer to "configuration vulnerabilities" section 3.3.1 and 3.3.3 for more detail.

3.9 Backup and disaster preparedness

Disaster readiness has the goal of minimizing the effect of a disaster and ensuring that resources, personnel, and business processes are able to resume operation in a timely manner. Disaster planning needs to be part of the security policy and program. GIAC does not have policy, standard and procedures to guide disaster and backup planning.

As a first line server in a two-tier architecture, this store-front server presents web pages to customers and accepts order requests. Sensitive data do not reside on this server. Backup for this servers only include in-house web application (pretty static) and system and application logs. Apache web server access log was identified as part of the data to fulfill the non-repudiation security objective for this e-commerce transaction. Web application was only backup once a week or whenever changes are made. System and application logs are backup to another server daily. Archive data in the backup server is backup on tape and store onsite and offsite daily together with more important database backup. The current arrangement is sufficient as far as software backup for the store-front Linux server is concern.

No proper documentation for disaster recovery is available in GIAC, however, system administrators and their superior has a common understanding (found out verbally from them individually) for common failures such as device breakdown or server failures. Hardware and facility redundancy is insufficient in the case of catastrophe disruption that might destroy the entire facility that the audited system is being housed. Catastrophe event can be building fire, flood, tornados, hurricanes and earthquake. However, alternate site solution to this problem is expensive. GIAC need to perform risk analysis to determine if this risk is acceptable.

As continual data backup is being performed religiously at GIAC, even no further planning is done for disaster recovery, minimum requirement for backup is met. However, it is recommended that disaster recovery and business continuity should be looked at as part of the GIAC security program.

3.9.1 Hardware and software inventory tracking

Comprehensive and up-to-date equipment inventory list (hardware and software) is kept by GIAC's IT operation department. This list is very useful in day-to-day system maintenance operation and will be useful in disastrous situation as well.

3.10 Other issues

3.10.1 Server build process

More and more organizations like GIAC are utilizing Linux server in their production environment, however when Linux is installed straight out of the box, it is relatively insecure. A proper installation of Linux server is the first step to a stable and secured system. GIAC store-front Linux server was installed from authentic Red Hat Linux 7.1 CDROM. Third party software was downloaded from their official website or trusted source such as www.Apache.org and www.cpan.com. However, MD5 sum for the downloaded tarballs were not checked.

Instead of selecting individual packages for installation, GIAC selected the following component groups for its audited Linux server during installation. As there are many rpm packages that are in these component groups, unnecessary programs were installed. Detail listing of rpm packages in the components group can be found in Red Hat Linux CD /*RedHat/base/comps* file. (Base component group is installed by default.)

- Development
- Utilities

Partition sizes of the system disk for the audited server are correctly based on the function of a server. GIAC uses the following broad steps in building their server build

1) Install a standard Linux server with the above components and system disk partition for server operations.
2) Add security patches.
3) Add applications to provide the functionality the server needs.
4) Test functionality and deploy system.

Recommendation:

1) Install a standard, **hardened** system image of Linux server with only required programs.
2) Add security patches.
3) Add applications to provide the functionality the server needs.
4) Add security application such as binary checksum (fingerprinting) and intrusion detection system.
5) Perform a vulnerability analysis on system
6) Deploy the system into production environment

GIAC can follow Linux security checklist listed in References section to build a hardened system image. It is recommended that GIAC develop server build scripts and configuration file using *kickstart* feature in Red Hat Linux. These installation scripts should follow the steps above to build a Linux server. *Kickstart* installation ensures consistency in server build and provides basic documentation for the entire build process.

3.10.2 Security policies, standards and procedures

Sound security policies, standards and guidelines are fundamental to an effective information protection strategy. An organization's information security policies and standard should communicate management's philosophy regarding the value of corporate information. These policies and standards will set expectations and provide the necessary guidance to protect information throughout the enterprise.

In general, the security policies, standards and procedures governing the deployment, administration, modification and use of audited system are lacking in GIAC. Without strong security policies, GIAC security practices are less effective and do not align with management objectives and desires.

As a strategy initiative, effective information security policies, standards and guidelines has to be developed at GIAC. This initiatives need to come from the management with a clear objective to build a solid foundation to protect GIAC organization's information assets.

4 Critical Issues and Recommendations

4.1 Red Hat errata updates and patch management

Red Hat security related errata updates need to be tested and applied to the audited server as soon as possible. The list of rpms can be found in section 3.1.

An important practice to keep a system continuously free from known OS vulnerabilities is to have proper patch management. *Autorpm* was used in this audit to identify installed rpm packages that were not updated. Though *autorpm* do not differentiate between enhancements and security or bugs updates, it is still an excellent tool to automate the process of monitoring updates from Red Hat errata site.

It is recommended that *autorpm* be installed and configured on the store-front Linux server to alert system administrator for new updates. *Autorpm* should be configured to download updated rpm packages and perform checksum verification but NOT to install them automatically. It should instead send an alert to the designated system custodian. After receiving the alert, proper change control procedure should be followed to update the server in a timely manner.

4.2 Remove unnecessary services, binaries and source files

4.2.1 Remove unnecessary services

Open ports on the audited server, detected by *nmap* and confirm by "netstat –aut" command are listed in Appendix A-1 and A-2. However, GIAC store-front Linux server only requires the following services to perform the functionality that its role required.

```
crond, keytable, netfs, network, random, syslog, httpd, iptables
```

It is recommended that GIAC evaluate the requirement to run other services and disable those that are not required. For example, the following three services needs not be started.

- NFS client with server service running

  The store-front Linux server uses NFS protocol to use Network Attached Storage (NAS). It only required `netfs` service but not `portmap` and `nfs`. Both `portmap` and `nfs` can be disabled.
- NTP client with `ntpd` daemon running.

  NTP client can synchronize time with NTP servers via cron service instead of running in daemon mode. NTP service need not be started during system start up as daemon.

Similarly, other services below are not used and should not be required.

```
atd, apmd, gpm, ipchains, kudzu, rawdevices, sendmail, anacron,
nfslock
```

Use "**chkconfig –-level 345 service off**" command to turn off service so that it will not be started during system boot.

Use "**/bin/netstat –a –p –inet**" to confirm that the services has been disabled.

4.2.2 Remove unnecessary binaries and source files

Rpm packages below from "Base" component group are not used and can be safely removed without affecting the functionality of the server. GIAC should evaluate whether more packages can be removed.

```
# rpm –e lokkit openldap
# rpm –e anacron apmd ash cyrus-sasl devfsd dhcpcd dosfstools \
eject gettext hotplug ipchains kbdconfig krb5-libs kudzu \
mouseconfig ntsysv procmail pump quota raidtools readline \
redhat-logos redhat-release slocate syslinux utempter
```

It is also recommended that every rpm from component groups selected during installation is evaluated and removed if it is not being used. Application source files in /usr/local/src/ directory should be removed as well.

```
# \rm -r /usr/local/src/*
```

4.3 Password-protect LILO prompt

One of the Operating System configuration issue brought up in section 3.3.3 can be resolved by password-protect LILO so that password is required in order to specify additional parameter to the boot loader. Add the **password** and **restricted** arguments to /etc/lilo.conf and then re-run /sbin/lilo to password-protect LILO prompt.

```
image=/boot/vmlinuz-2.2.16
        label=linux
        read-only
        root=/dev/sda5
        restricted
        password=your-password
```

4.4 Password-protect single-user mode and disable Ctrl-Alt-Del shutdown

Single-user mode must be password protect by adding following highlighted login option line to /etc/inittab.

```
# System initialization
si::sysinit:/etc/rc.d/rc.sysinit
~~:S:wait:/sbin/sulogin
```

Ctrl-Alt-Del shutdown must be disabled by commenting out the statement in /etc/inittab to trap Ctrl-Alt-Del.

```
# Trap CTRL-ALT-DELETE
#ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

With measures in section 4.3 and 4.4 implemented, it is more difficult for anyone who has physical access to the audited server to get into the system inconspicuously.

4.5 Stricter host based packet filtering to control access from internal network

Iptables was used on the audited system with the sole purpose of creating a multiple layers packet filtering system for Internet traffic. Currently, *iptables* is only configured to restrict traffic from Internet, there is no filtering of traffic coming from the office internal network. To reduce the risk from internal network, it is recommended that GIAC implement stricter packet filtering rules to restrict access to this production server to just several system administrator's workstations or just a dedicated administration workstation that allow only technical person to log in remotely.

Recommended changes to the firewall script in /etc/rc.d/init.d is highlighted as follow.

```
INTERNAL_INTERFACE="eth0"
INTERNAL_IP_ADDR="192.168.10.1"
INTERNAL_IP_RANGE="192.168.0.0/255.255.0.0"
```

```
ADMIN_WS1="192.168.10.50"

/sbin/iptables -P INPUT DROP
/sbin/iptables -A INPUT -p ALL –i $INTERNAL_INTERFACE –s\
$INTERNAL_IP_RANGE  -d $INTERNAL_IP_ADDR -j ACCEPT
```

(bold, italic line above is to be replaced by the line below in the firewall startup script)

```
/sbin/iptables –A INPUT -p TCP –i $INTERNAL_INTERFACE –s \
$ADMIN_WS1 -d $INTERNAL_IP_ADDR --dport 22 -j ACCEPT
```

Furthermore, *iptables* can further restrict incoming Internet traffic to ports that will be disabled by recommendations made in section 4.2.1.

4.6 Remove compilation tools

In order to have compilation functionality to build Apache from source code, the audited server was installed with Red Hat Linux "Development" component group. However, leaving behind these tools on the server increases the risk for the store-front web server.

Many hackers download the necessary source code to "rootkit" the hacked system. This source codes are downloaded and then compiled on the compromise systems. By removing the compilation tools. Hacker needs to have binary "rootkit" or download compilation tools he requires to the compromise system. This makes the trojan process noisier (more actions need to be taken) and increases the chance for GIAC to detect the intrusion early. Therefore all compilation tools and the dependant rpm that accompany the tools should be removed from the audited system.

Rpm can be removed from the system using "rpm –e" command. Those packages that others have dependency on should be removed first. Complete list of rpm that should be removed under "Development" component group can be found in Red Hat CD /RedHat/base/comps file.

4.7 Apply stricter control on system file system

The following file system layout is recommended for GIAC store-front Linux server. As the server is already properly partition as this recommendation, the necessary change is only the default mounting read-write access control. For example the boot partition should be mounted read-only and nosuid.

This changes should be make in /etc/fstab as follow

System file system		
Partition	**Description**	**Recommendations**
/	root partition contains system configurations	Root partition need to be mounted read-write. Therefore, important configurations files should be immunized to protect them from unauthorized change.
/boot	The /boot partition contains	The /boot should be mounted *read-only*

	binary kernel image	and *nosuid*
/usr	Binary systems programs and utilities resides in /usr.	System binaries need not be updated very frequently. The /usr partition should be mounted *read-only*.
/var	The /var partition is used for storing systems log files	The /var directory should be mounted *nodev*, *nosuid*, *noexec*

Important files should be immunize and/or protected with the following permissions.

```
/bin/chmod 400 /etc/sysctl.conf
/bin/chmod 600 /etc/crontab /etc/shadow /etc/pam.d/* \
/etc/lilo.conf /etc/securetty /etc/security/* /etc/sysconfig \
/bin/chmod 640 /etc/syslog.conf /var/log/wtmp /var/log/lastlog \
/etc/logrotate.conf
/bin/chmod 644 /var/log/messages /etc/passwd
/bin/chmod 700 /etc/rc.d/init.d/* /bin/rpm
/bin/chmod 751 /var/log

/bin/chmod 600 /etc/ftpusers /etc/hosts.allow /etc/hosts.deny \
/etc/shutdown.allow /etc/xinetd.conf /etc/cron.allow \
/etc/cron.deny

# Immunize files
chattr +i /etc/passwd
chattr +i /etc/shadow
chattr +i /etc/group
chattr +i /etc/gshadow
chattr +i /etc/services
chattr +i /etc/lilo.conf
chattr +i /bin/login
```

4.8 Build new version of Apache

The existing version of Apache and custom modules included are outdated and no longer security safe to run on a mission critical system. It is recommended that latest sources for these programs be downloaded from their respective website listed below.

- Apache 1.3.26 from www.Apache.org
- Mod_ssl 2.8.10 from www.modssl.org

Alternatively, use Apache 2.0.39 (with mod_ssl included) if all custom modules used to build the Apache have a version that support Apache 2.0.XX.

- Openssl 0.9.6d from www.openssl.org
- mod_perl version 1.27 from www.Apache.org
- php version 4.2.1 from www.php.net

The process to build a new version of Apache application should be incorporated into the Linux server build process that should be developed after Quick Fixes are completed.

4.9 Password Management Controls

Recommended password management control setting for GIAC store-front server is as follows. For password management discussion, refer to section 3.3.6.

Password Management Control Settings		
File	**Recommendation**	**Command or Entry**
/etc/login.defs	Set the maximum number of days a password may be use to 60 days and minimum acceptable password length to 8.	PASS_MAX_DAYS 60 PASS_MIN_LEN 8 `# chage -M 60 username`
/etc/profile	To make bash shell automatically logout after 15 minutes.	TMOUT=900
/etc/pam.d/system-auth	To keep password history so that it cannot be reused soon.	`# touch /etc/security/opasswd` See note 1 below for configuration
/etc/pam.d/system-auth	To encourage use of uppercase, digit and special character in password.	See note 2 below

In /etc/pam.d/system-auth, modify the following two lines.

Note 2

password required /lib/security/pam_cracklib.so retry=3 **minlen=10 dcredit=2 ucredit=2 ocredit=2 difok=6**

Note 1

password sufficient /lib/security/pam_unix.so nullok use_authtok md5 shadow **remember=5**

4.10 Least Privilege for System Administrator

All GIAC system administrators have full system privilege once they "*sudo*" from their individual account to gain root privilege. This means that system administrators have the entire store-front server at their mercy. They can make changes to the system configurations, modify in-house application codes, and even modify customer transaction data. In other word, system administrator can easily sabotage GIAC using the privilege he has on the store-front server.

It is recommended that GIAC make use of the "Cmnd_Alias" feature of *sudo* to restrict the privilege commands that the administrator group can access. This group of commands should enable him to perform his daily tasks but does not allow him to make critical changes to the system. Only root user can perform other privilege tasks. Root password for the server should be known only to two or three persons out of the administrator group so that when other more critical and less frequently executed tasks

need to be performed, system administrator need the root password holder to enter password before the task can be performed.

5 Securing GIAC store-front server and enterprise network roadmap

GIAC is advised to follow the following steps to secure its store-front Linux server after reviewing this audit report and its recommendations carefully.

- Focus on those immediate security problems that are classified as Quick Fixes and can be resolved quickly. For examples, update server with latest errata packages and password-protect LILO prompt and single user mode. These quick fixes will remove most critical deficiency on the audited Linux server.
- Methodically fix all other Quick Fixes problems that might require more evaluation and planning. For example remove unnecessary rpm packages and to apply "least privilege" principle to system administrator accounts.
- Evaluate and use all the host-base security utilities and applications that are recommended to provide better auditing functionality and intrusion detection capability.
- Create a kickstart script to build a hardened Linux system image with necessary security utilities specific to the hardware used.

After the critical store-front server is secured, GIAC should replace the current security practices with a formal security program. This program should be initiated and supported by the top management. Security policy, standard and guideline should be used as a foundation for this program. This security program will be able to ensure that documentations are updated, servers are secure when they are introduced to GIAC network and put in place procedures and processes to prevent all of the careless or sloppy system administration work that leave behind security holes. Note that during this process, the security measures in the audited server might need to be tuned to meet the newly establish security requirement.

When formal security program has been put in place and computing environment and system secured according to the established policies, it is also recommended that GIAC carry out a security formal audit for it entire enterprise network. The audit should be performed by external security consultants to give an unbiased opinion on the overall IT security in GIAC.

References

1. Dave Wreski, Linux Security Quick Refernece Guide, Guardian Digital Inc., 2000

2. Gerhard Mourani, Securing and Optimizing Linux: RedHat Edition, OpenDocs, June 2000

3. Anonymous, Maximum Linux Security: A Hacker's Guide to Protecting Your Linux Server and Workstation, Sams Publishing, September 1999

4. Christopher M. King, Curtis E. Dalton, T. Ertem Osmanoglu, Security Architecture: Design, Deployment and Operations, RSA Press, 2001

5. Krishni Naidu, Auditing Linux, SANS Institute S.C.O.R.E.,2002

6. Justin Kapp, How To Conduct A Security Audit, PC Network Advisor, July 2000

7. Phillip Robinson, Unix Server Security Audit, GCUX Paper, SANS Institute, 2002

8. Lenny Zeltser, Consultant's Report from Auditing Unix, GCUX Paper, SANA Institute, 2001

9. Jennifer Vesperman, PAM modules, The O'Reilly Network, Sept 2001

10. Jay Beale, Linux Benchmark v1.0.0, The Centre for Internet Security, Apr 2002

Appendix A Results of commands and tools execution

A-1 Results of Nmap port scan

```
# nmap -sS -p 1-65535 xxx.xxx.xxx.xxx

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on  (xxx.xxx.xxx.xxx):
(The 65528 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
80/tcp     open        http
111/tcp    open        sunrpc
443/tcp    open        https
8880/tcp   open        unknown
32768/tcp  open        unknown
32769/tcp  open        unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 4 seconds

# nmap -sU -p 1-1024 xxx.xxx.xxx.xxx

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on  (xxx.xxx.xxx.xxx):
(The 1020 ports scanned but not shown below are in state: closed)
Port       State       Service
111/udp    open        sunrpc
123/udp    open        ntp
661/udp    open        unknown
719/udp    open        unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 1056 seconds
```

A-2 Results of executing "netstat –aut" and "lsof –i"

```
# netstat -aut
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:32768                 *:*                     LISTEN
tcp        0      0 *:32769                 *:*                     LISTEN
tcp        0      0 *:sunrpc                *:*                     LISTEN
tcp        0      0 *:http                  *:*                     LISTEN
tcp        0      0 *:8880                  *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 localhost:smtp          *:*                     LISTEN
tcp        0      0 *:https                 *:*                     LISTEN
udp        0      0 *:32768                 *:*
udp        0      0 *:nfs                   *:*
udp        0      0 *:32769                 *:*
udp        0      0 *:32770                 *:*
udp        0      0 *:661                   *:*
udp        0      0 *:719                   *:*
udp        0      0 *:sunrpc                *:*
udp        0      0 storefront.giac.net:ntp *:*
udp        0      0 localhost:ntp           *:*
```

```
udp        0      0 *:ntp                   *:*

# lsof -i tcp:32768
COMMAND   PID USER   FD   TYPE DEVICE SIZE NODE NAME
rpc.statd 543 root    6u  IPv4    747       TCP *:32768 (LISTEN)

# lsof -i tcp:32769
COMMAND   PID USER   FD   TYPE DEVICE SIZE NODE NAME
rpc.mount 913 root    4u  IPv4   1777       TCP *:32769 (LISTEN)

# lsof -i tcp:8880
COMMAND   PID USER   FD   TYPE DEVICE SIZE NODE NAME
httpd   21443 root   19u  IPv4  62845       TCP *:8880 (LISTEN)
httpd   21444 root   19u  IPv4  62845       TCP *:8880 (LISTEN)
httpd   21445 root   19u  IPv4  62845       TCP *:8880 (LISTEN)
httpd   21446 root   19u  IPv4  62845       TCP *:8880 (LISTEN)
httpd   21447 root   19u  IPv4  62845       TCP *:8880 (LISTEN)
httpd   21448 root   19u  IPv4  62845       TCP *:8880 (LISTEN)

# lsof -i udp:661
COMMAND   PID USER   FD   TYPE DEVICE SIZE NODE NAME
rpc.rquot 908 root    3u  IPv4   1761       UDP *:661

# lsof -i udp:719
COMMAND   PID USER   FD   TYPE DEVICE SIZE NODE NAME
rpc.statd 543 root    4u  IPv4    738       UDP *:719
```

A-3 Result of executing chkconfig --list

```
# chkconfig --list
atd             0:off   1:off   2:off   3:on    4:on    5:on    6:off
gpm             0:off   1:off   2:on    3:on    4:on    5:on    6:off
nfs             0:off   1:off   2:off   3:on    4:on    5:on    6:off
apmd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
ntpd            0:off   1:off   2:off   3:on    4:on    5:on    6:off
sshd            0:off   1:off   2:on    3:on    4:on    5:on    6:off
ipchains        0:off   1:off   2:on    3:on    4:on    5:on    6:off
crond           0:off   1:off   2:on    3:on    4:on    5:on    6:off
httpd           0:off   1:off   2:off   3:on    4:on    5:on    6:off
kudzu           0:off   1:off   2:off   3:on    4:on    5:on    6:off
netfs           0:off   1:off   2:off   3:on    4:on    5:on    6:off
iptables        0:off   1:off   2:on    3:on    4:on    5:on    6:off
rawdevices      0:off   1:off   2:off   3:on    4:on    5:on    6:off
network         0:off   1:off   2:on    3:on    4:on    5:on    6:off
nfslock         0:off   1:off   2:off   3:on    4:on    5:on    6:off
random          0:off   1:off   2:on    3:on    4:on    5:on    6:off
sendmail        0:off   1:off   2:on    3:on    4:on    5:on    6:off
syslog          0:off   1:off   2:on    3:on    4:on    5:on    6:off
anacron         0:off   1:off   2:on    3:on    4:on    5:on    6:off
xinetd          0:off   1:off   2:off   3:off   4:off   5:off   6:off
kdcrotate       0:off   1:off   2:off   3:off   4:off   5:off   6:off
portmap         0:off   1:off   2:off   3:on    4:on    5:on    6:off
keytable        0:off   1:on    2:on    3:on    4:on    5:on    6:off
xinetd based services:
        echo:   off
```

```
time:   off
daytime:        off
chargen-udp:    off
telnet: off
daytime-udp:    off
time-udp:       off
echo-udp:       off
chargen:        off
wu-ftpd:        off
```

A-4 Results of finding SetUID and SetGID files

```
# Find setuid
# find / -type f -perm +4000 -print
/bin/su
/bin/ping
/bin/mount
/bin/umount
/usr/bin/at
/usr/bin/ssh
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/crontab
/usr/bin/chage
/usr/bin/sperl5.6.0
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/suidperl
/usr/sbin/traceroute
/usr/sbin/sendmail
/usr/sbin/usernetctl
find: /proc/921/fd: No such file or directory
find: /proc/21410/fd/4: No such file or directory
/sbin/unix_chkpwd
/sbin/pwdb_chkpwd

# Find setgid
# find / -type f -perm +2000 -print
/usr/bin/man
/usr/bin/wall
/usr/bin/write
/usr/bin/slocate
/usr/bin/minicom
/usr/bin/lockfile
/usr/sbin/utempter
find: /proc/921/fd: No such file or directory
find: /proc/21413/fd/4: No such file or directory
/sbin/netreport
```

A-5 Results of finding unowned and world-writable files

```
# Find world-writable
```

```
# find / -perm -2 ! -type l ! -type c -print
/dev/log
/tmp
/var/tmp
/usr/local/src/mod_perl-1.25/t/docs/hooks.txt
/usr/local/src/mod_perl-1.25/t/docs/.htaccess
/usr/local/src/mod_perl-1.25/t/logs
/usr/local/src/mod_ssl-2.8.4-1.3.20/pkg.eapi/eapi.patch

# Find unowned
# find / -nouser -o -nogroup ! -type c -print
/usr/local/src/Carp-Assert-0.13/blib
/usr/local/src/Carp-Assert-0.13/blib/lib
/usr/local/src/Carp-Assert-0.13/blib/lib/Carp
/usr/local/src/Carp-Assert-0.13/blib/lib/Carp/.exists
/usr/local/src/Carp-Assert-0.13/blib/lib/auto
/usr/local/src/Carp-Assert-0.13/blib/lib/auto/Carp
/usr/local/src/Carp-Assert-0.13/blib/lib/auto/Carp/Assert
/usr/local/src/Carp-Assert-0.13/blib/lib/auto/Carp/Assert/.exists
/usr/local/src/Carp-Assert-0.13/blib/arch
/usr/local/src/Carp-Assert-0.13/blib/arch/auto
/usr/local/src/Carp-Assert-0.13/blib/arch/auto/Carp
/usr/local/src/Carp-Assert-0.13/blib/arch/auto/Carp/Assert
/usr/local/src/Carp-Assert-0.13/blib/arch/auto/Carp/Assert/.exists
/usr/local/src/Carp-Assert-0.13/blib/man3
/usr/local/src/Carp-Assert-0.13/blib/man3/.exists
/usr/local/src/Carp-Assert-0.13/Makefile
/usr/local/src/Carp-Assert-0.13/pm_to_blib
/usr/local/src/IO-Stty-.02/blib
/usr/local/src/IO-Stty-.02/blib/lib
/usr/local/src/IO-Stty-.02/blib/lib/IO
/usr/local/src/IO-Stty-.02/blib/lib/IO/.exists
/usr/local/src/IO-Stty-.02/blib/lib/auto
/usr/local/src/IO-Stty-.02/blib/lib/auto/IO
/usr/local/src/IO-Stty-.02/blib/lib/auto/IO/Stty
/usr/local/src/IO-Stty-.02/blib/lib/auto/IO/Stty/.exists
/usr/local/src/IO-Stty-.02/blib/arch
/usr/local/src/IO-Stty-.02/blib/arch/auto
/usr/local/src/IO-Stty-.02/blib/arch/auto/IO
/usr/local/src/IO-Stty-.02/blib/arch/auto/IO/Stty
/usr/local/src/IO-Stty-.02/blib/arch/auto/IO/Stty/.exists
/usr/local/src/IO-Stty-.02/Makefile
/usr/local/src/IO-Stty-.02/pm_to_blib
```

A-6 Results of CISscan

```
*** CIS Ruler Run ***
Starting at time 20020710-12:21:43

Positive: 1.1 System appears to have been patched within the last month.
Negative: 2.2 No Authorized Only banner for telnet in file
/etc/xinetd.d/telnet.
Negative: 2.2 No Authorized Only banner for ftp in file
/etc/xinetd.d/wu-ftpd.
Positive: 2.3 telnet is deactivated.
```

```
Positive: 2.4 ftp is deactivated.
Positive: 2.5 rsh, rcp and rlogin are deactivated.
Positive: 2.6 tftp is deactivated.
Negative: 2.7 xinetd either requires global 'only-from' statement or
one for each service.
Negative: 3.1 apmd not deactivated.
Negative: 3.1 gpm not deactivated.
Negative: 3.2 NFS Server script nfs not deactivated.
Negative: 3.3 NFS script nfslock not deactivated.
Positive: 3.4 NIS Client processes are deactivated.
Positive: 3.5 NIS Server processes are deactivated.
Negative: 3.6 portmapper not deactivated.
Positive: 3.7 samba windows filesharing daemons are deactivated.
Negative: 3.8 netfs rc script not deactivated.
Positive: 3.9 printing daemon is deactivated.
Positive: 3.10 Graphical login is deactivated.
Negative: 3.11 Mail daemon is on and collecting mail from the network.
Negative: 3.12 httpd web server rc-script not deactivated.
Positive: 3.13 snmp daemon is deactivated.
Positive: 3.14 DNS server is deactivated.
Positive: 3.15 postgresql (SQL) database server is deactivated.
Positive: 3.16 routing daemons are deactivated.
Positive: 3.17 Webmin GUI-based system administration daemon
deactivated.
Positive: 3.18 Squid web cache daemon deactivated.
Positive: 3.19 inetd/xinetd not activated.
Positive: 3.20 Found a good daemon umask.
Negative: 4.1 Coredumps aren't deactivated.
Negative: 4.2 An entry in /etc/exports doesn't have (secure) on it.
Negative: 4.3 /proc/sys/net/ipv4/tcp_max_syn_backlog should be at least
4096 to handle SYN floods.
Negative: 4.4 /proc/sys/net/ipv4/conf/eth1/send_redirects should be 0
to disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/eth0/send_redirects should be 0
to disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/lo/send_redirects should be 0 to
disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/default/send_redirects should be
0 to disable outgoing redirect messages.
Positive: 5.1 syslog captures auth and authpriv messages.
Negative: 6.1 Removable filesystem /mnt/floppy is not mounted nosuid.
Negative: 6.2 PAM allows users to mount CD-ROMS.
(/etc/security/console.perms)
Negative: 6.2 PAM allows users to mount floppies.
(/etc/security/console.perms)
Positive: 6.3 password and group files have right permissions and
owners.
Positive: 6.4 all temporary directories have sticky bits set.
Positive: 7.1 rhosts authentication totally deactivated in PAM.
Positive: 7.2 /etc/hosts.equiv file not present or has size zero.
Negative: 7.3 User rpc is not present in /etc/ftpusers
Negative: 7.3 User rpcuser is not present in /etc/ftpusers
Negative: 7.3 User mailnull is not present in /etc/ftpusers
Negative: 7.4 Couldn't open cron.allow
Negative: 7.4 Couldn't open at.allow
Negative: 7.5 The permissions on /etc/crontab are not sufficiently
restrictive.
```

```
Negative: 7.6 No Authorized Only message in /etc/motd.
Negative: 7.6 No Authorized Only message in /etc/issue.
Negative: 7.7 /etc/securetty has a non tty1-12 line: tty10.
Negative: 7.8 lilo isn't password-protected.
Negative: 8.1 bin has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 daemon has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 ftp has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 mail has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 nobody has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Positive: 8.2 There were no +: entries in passwd, shadow or group maps.
Positive: 8.3 All users have passwords
Positive: 8.4 Only one UID 0 account AND it is named root.
Positive: 8.5 root's PATH is clean of group/world writable directories
or the current-directory link.
Positive: 8.6 root account has no dangerous rhosts, shosts, or netrc
files.
Negative: 8.7 User mail 's homedir is group writable!
Positive: 8.8 No group or world-writable dotfiles!
Positive: 8.9 No user has a .netrc or .rhosts file.
Negative: 8.10 Default umask may not block group-writable.  Check
/etc/csh.login.
Negative: 8.10 Default umask may not block world-writable.  Check
/etc/bashrc.
Negative: 8.10 Default umask may not block group-writable.  Check
/etc/bashrc.
Negative: 8.10 Default umask may not block world-writable.  Check
/etc/csh.cshrc.
Negative: 8.10 Default umask may not block group-writable.  Check
/etc/csh.cshrc.
Positive: 9.1 System is running sshd.
Positive: 9.2 This machine is synced with ntp.
Preliminary rating given at time: Wed Jul 10 12:21:44 2002

        Preliminary rating = 5.71 / 10.00

Positive: 6.5 No non-standard SUID/SGID programs found.
Ending run at time: Wed Jul 10 12:21:44 2002

        Final rating = 5.89 / 10.00
```

A-7 Result of executing "autorpm auto"

```
# autorpm auto
Processing config file: /etc/autorpm.d/autorpm.conf
Processing config file:
/etc/autorpm.d/sample_configs/get-updates.sample

*********************************************
AutoRPM 2.9.1 on storefront.giac.net started Wed Jul 10 12:59:18 GMT 2002
```

```
Comparing to locally installed RPMs
Loading installed RPM list... Done.
Processing and sorting... Done.
RPM Source (FTP Pool): redhat-updates

Connecting to updates.redhat.com...
Logging in as anonymous
Listing Directory: /7.1/en/os/

Comparing to locally installed RPMs
Listing Directory: /7.1/en/os/i386/

Processing and sorting... Done.
-> modutils-2.4.13-0.7.1 is an updated RPM and could be upgraded.
-> sudo-1.6.5p2-1.7x.1 is an updated RPM and could be upgraded.
-> popt-1.6.4-7x is an updated RPM and could be upgraded.
-> e2fsprogs-1.26-1.71 is an updated RPM and could be upgraded.
-> wu-ftpd-2.6.1-16.7x.1 is an updated RPM and could be upgraded.
-> sendmail-8.11.6-2.7.1 is an updated RPM and could be upgraded.
-> openldap-2.0.21-0.7.1 is an updated RPM and could be upgraded.
-> cyrus-sasl-1.5.24-22.7 is an updated RPM and could be upgraded.
-> xinetd-2.3.3-1 is an updated RPM and could be upgraded.
-> diffutils-2.7-23 is an updated RPM and could be upgraded.
-> openssh-server-3.1p1-5 is an updated RPM and could be upgraded.
-> openssh-clients-3.1p1-5 is an updated RPM and could be upgraded.
-> at-3.1.8-23 is an updated RPM and could be upgraded.
-> glibc-devel-2.2.4-24 is an updated RPM and could be upgraded.
-> rpm-4.0.4-7x is an updated RPM and could be upgraded.
-> rpm-build-4.0.4-7x is an updated RPM and could be upgraded.
-> man-1.5i2-0.7x.5 is an updated RPM and could be upgraded.
-> openldap-devel-2.0.21-0.7.1 is an updated RPM and could be upgraded.
-> zlib-1.1.3-25.7 is an updated RPM and could be upgraded.
-> kernel-headers-2.4.9-34 is an updated RPM and could be upgraded.
-> glibc-common-2.2.4-24 is an updated RPM and could be upgraded.
-> pam-0.75-18.7 is an updated RPM and could be upgraded.
-> openssh-3.1p1-5 is an updated RPM and could be upgraded.
-> cyrus-sasl-devel-1.5.24-22.7 is an updated RPM and could be upgraded.
-> quota-3.01pre9-0.7.1 is an updated RPM and could be upgraded.
-> zlib-devel-1.1.3-25.7 is an updated RPM and could be upgraded.
-> pam-devel-0.75-18.7 is an updated RPM and could be upgraded.
-> e2fsprogs-devel-1.26-1.71 is an updated RPM and could be upgraded.
-> rpm-devel-4.0.4-7x is an updated RPM and could be upgraded.
-> groff-1.17.2-7.0.2 is an updated RPM and could be upgraded.

Comparing to locally installed RPMs
Remaining Connected to updates.redhat.com as anonymous...
Listing Directory: /7.1/en/os/i586/

Processing and sorting... Done.

Comparing to locally installed RPMs
Remaining Connected to updates.redhat.com as anonymous...
Listing Directory: /7.1/en/os/i686/

Processing and sorting... Done.
-> kernel-2.4.9-34 is an updated RPM and could be upgraded.
-> glibc-2.2.4-24 is an updated RPM and could be upgraded.
```

```
Comparing to locally installed RPMs
Remaining Connected to updates.redhat.com as anonymous...
Listing Directory: /7.1/en/os/noarch/

Processing and sorting... Done.
-> docbook-utils-0.6-13.2 is an updated RPM and could be upgraded.
-> docbook-style-dsssl-1.64-2 is an updated RPM and could be upgraded.



************************************
Finished Wed Jul 10 13:00:03 GMT 2002


********************************************
AutoRPM 2.9.1 on storefront.giac.net started Wed Jul 10 13:00:03 GMT 2002


Processing Auto-Install Queue:

************************************
Finished Wed Jul 10 13:00:03 GMT 2002
```

A-8 Result of Nessus vulnerabilities scan

```
Nessus Scan Report
------------------



SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 14
 - Number of security warnings found : 10
 - Number of security notes found : 15



TESTED HOSTS

 xxx.xxx.xxx.xxx (Security holes found)



DETAILS

+ xxx.xxx.xxx.xxx :
 . List of open ports :
   o ssh (22/tcp) (Security hole found)
   o http (80/tcp) (Security hole found)
   o sunrpc (111/tcp)
   o https (443/tcp) (Security hole found)
   o unknown (8880/tcp) (Security hole found)
```

```
  o general/tcp (Security notes found)
  o general/icmp (Security warnings found)
  o nfs (2049/udp) (Security warnings found)
  o unknown (32770/udp) (Security warnings found)
  o unknown (661/udp) (Security warnings found)
  o unknown (32768/udp) (Security hole found)
  o nfs (2049/tcp) (Security warnings found)
  o general/udp (Security notes found)

. Vulnerability found on port ssh (22/tcp) :



   You are running a version of OpenSSH which is older than 3.0.1.

   Versions older than 3.0.1 are vulnerable to a flaw in which
   an attacker may authenticate, provided that Kerberos V support
   has been enabled (which is not the case by default).
   It is also vulnerable as an excessive memory clearing bug,
   believed to be unexploitable.

   *** You may ignore this warning if this host is not using
   *** Kerberos V

   Solution : Upgrade to OpenSSH 3.0.1
   Risk factor : Low (if you are not using Kerberos) or High (if kerberos is
    enabled)


. Vulnerability found on port ssh (22/tcp) :



   You are running a version of OpenSSH which is older than 3.4

   There is a flaw in this version that can be exploited remotely to
   give an attacker a shell on this host.


   Solution : Upgrade to OpenSSH 3.4
   Risk factor : High

. Vulnerability found on port ssh (22/tcp) :



   You are running a version of OpenSSH which is older than 3.0.2.

   Versions prior than 3.0.2 are vulnerable to an environment
   variables export that can allow a local user to execute
   command with root privileges.
   This problem affect only versions prior than 3.0.2, and when
   the UseLogin feature is enabled (usually disabled by default)

   Solution : Upgrade to OpenSSH 3.0.2 or apply the patch for prior
   versions. (Available at: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH)
```

```
   Risk factor : High (If UseLogin is enabled, and locally)
   CVE : CVE-2001-0872

. Warning found on port ssh (22/tcp)



   You are running a version of OpenSSH between 2.5.x and
   2.9.x

   Depending on the order of the user keys in
   ~/.ssh/authorized_keys2, sshd might fail to
   apply the source IP based access control
   restriction to the correct key.

   This problem allows users to circumvent
   the system policy and login from disallowed
   source IP address.

   Solution :
   Upgrade to OpenSSH 2.9.9

   Risk factor :
    Medium


. Warning found on port ssh (22/tcp)



   You are running a version of OpenSSH older than OpenSSH 3.2.1

   A buffer overflow exists in the daemon if AFS is enabled on
   your system, or if the options KerberosTgtPassing or
   AFSTokenPassing are enabled.  Even in this scenario, the
   vulnerability may be avoided by enabling UsePrivilegeSeparation.

   Versions prior to 2.9.9 are vulnerable to a remote root
   exploit. Versions prior to 3.2.1 are vulnerable to a local
   root exploit.

   Solution :
   Upgrade to the latest version of OpenSSH

   Risk factor :
    High

. Warning found on port ssh (22/tcp)



   The remote SSH daemon supports connections made
   using the version 1.33 and/or 1.5 of the SSH protocol.

   These protocols are not completely cryptographically
   safe so they should not be used.
```

```
   Solution :
    If you use OpenSSH, set the option 'Protocol' to '2'
    If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'

   Risk factor :
    Low


. Information found on port ssh (22/tcp)


   a ssh server is running on this
    port


. Information found on port ssh (22/tcp)


   Remote SSH version :
    SSH-1.99-OpenSSH_2.5.2p2


. Information found on port ssh (22/tcp)


   The remote SSH daemon supports the following versions of the
   SSH protocol :

     . 1.33
     . 1.5
     . 1.99
     . 2.0

. Vulnerability found on port http (80/tcp) :



   The remote host is using a version of mod_ssl which is
   older than 2.8.7.

   This version is vulnerable to a buffer overflow which,
   albeit difficult to exploit, may allow an attacker
   to obtain a shell on this host.

   *** Some vendors patched older versions of mod_ssl, so this
   *** might be a false positive. Check with your vendor to determine
   *** if you have a version of mod_ssl that is patched for this
   *** vulnerability


   Solution : Upgrade to version 2.8.7 or newer
   Risk factor : High
   CVE : CAN-2002-0082

. Vulnerability found on port http (80/tcp) :
```

```
    The remote host is using a version of mod_ssl which is
    older than 2.8.10.

    This version is vulnerable to an off by one buffer overflow
    which may allow a user with write access to .htaccess files
    to execute abritrary code on the system with permissions
    of the web server.

    Solution : Upgrade to version 2.8.10 or newer
    Risk factor : High

  . Vulnerability found on port http (80/tcp) :



    The remote host appears to be vulnerable to the Apache
    Web Server Chunk Handling Vulnerability.

    If Safe Checks are enabled, this may be a false positive
    since it is based on the version of Apache.  Although
    unpatched Apache versions 1.2.2 and above, 1.3 through
    1.3.24 and 2.0 through 2.0.36, the remote server may
    be running a patched version of Apache

    *** Note : as safe checks are enabled, Nessus solely relied on the banner
to issue this  alert


    Solution : Upgrade to version 1.3.26 or 2.0.39 or newer
    See also : http://httpd.apache.org/info/security_bulletin_20020617.txt
        http://httpd.apache.org/info/security_bulletin_20020620.txt
    Risk factor : High
    CVE : CAN-2002-0392

  . Vulnerability found on port http (80/tcp) :



    The remote host is running a version of PHP earlier
    than 4.1.2.

    There are several flaws in how PHP handles
    multipart/form-data POST requests, any one of which can
    allow an attacker to gain remote access to the system.

    Solution : Upgrade to PHP 4.1.2
    Risk factor : High
    CVE : CVE-2002-0081

  . Warning found on port http (80/tcp)



    The remote host is running php 4.0.5.

    There is a flaw in this version of PHP that allows
```

```
   local users to circumvent the safe mode and to gain
   the uid of the http process.


   Solution : Upgrade to PHP 4.0.6
   Risk factor : High
   CVE : CVE-2001-1246

. Information found on port http (80/tcp)


   a web server is running on this
    port


. Information found on port http (80/tcp)


   The remote web server type is :

   Apache/1.3.20 (Unix) mod_perl/1.25 PHP/4.0.5 mod_ssl/2.8.4 OpenSSL/0.9.6

   We recommend that you configure your web server to return
   bogus versions in order to not leak information

. Information found on port http (80/tcp)


   The following directories were discovered:
   /cgi-bin
   /icons
   /manual


. Vulnerability found on port https (443/tcp) :



   The remote host is using a version of mod_ssl which is
   older than 2.8.7.

   This version is vulnerable to a buffer overflow which,
   albeit difficult to exploit, may allow an attacker
   to obtain a shell on this host.

   *** Some vendors patched older versions of mod_ssl, so this
   *** might be a false positive. Check with your vendor to determine
   *** if you have a version of mod_ssl that is patched for this
   *** vulnerability


   Solution : Upgrade to version 2.8.7 or newer
   Risk factor : High
   CVE : CAN-2002-0082

. Vulnerability found on port https (443/tcp) :
```

```
   The remote host is using a version of mod_ssl which is
   older than 2.8.10.

   This version is vulnerable to an off by one buffer overflow
   which may allow a user with write access to .htaccess files
   to execute abritrary code on the system with permissions
   of the web server.

   Solution : Upgrade to version 2.8.10 or newer
   Risk factor : High

. Vulnerability found on port https (443/tcp) :



   The remote host is running a version of PHP earlier
   than 4.1.2.

   There are several flaws in how PHP handles
   multipart/form-data POST requests, any one of which can
   allow an attacker to gain remote access to the system.

   Solution : Upgrade to PHP 4.1.2
   Risk factor : High
   CVE : CVE-2002-0081

. Information found on port https (443/tcp)


   a web server is running on this
    port


. Information found on port https (443/tcp)


   The remote web server type is :

   Apache/1.3.20 (Unix) mod_perl/1.25 PHP/4.0.5 mod_ssl/2.8.4 OpenSSL/0.9.6

   We recommend that you configure your web server to return
   bogus versions in order to not leak information

. Information found on port https (443/tcp)


   The following directories were discovered:
   /cgi-bin
   /icons
   /manual


. Vulnerability found on port unknown (8880/tcp) :
```

```
   The remote host is using a version of mod_ssl which is
   older than 2.8.7.

   This version is vulnerable to a buffer overflow which,
   albeit difficult to exploit, may allow an attacker
   to obtain a shell on this host.

   *** Some vendors patched older versions of mod_ssl, so this
   *** might be a false positive. Check with your vendor to determine
   *** if you have a version of mod_ssl that is patched for this
   *** vulnerability


   Solution : Upgrade to version 2.8.7 or newer
   Risk factor : High
   CVE : CAN-2002-0082

. Vulnerability found on port unknown (8880/tcp) :



   The remote host is using a version of mod_ssl which is
   older than 2.8.10.

   This version is vulnerable to an off by one buffer overflow
   which may allow a user with write access to .htaccess files
   to execute abritrary code on the system with permissions
   of the web server.

   Solution : Upgrade to version 2.8.10 or newer
   Risk factor : High

. Vulnerability found on port unknown (8880/tcp) :



   The remote host is running a version of PHP earlier
   than 4.1.2.

   There are several flaws in how PHP handles
   multipart/form-data POST requests, any one of which can
   allow an attacker to gain remote access to the system.

   Solution : Upgrade to PHP 4.1.2
   Risk factor : High
   CVE : CVE-2002-0081

. Information found on port unknown (8880/tcp)


   a web server is running on this port

. Information found on port unknown (8880/tcp)


   The following directories were discovered:
```

```
   /cgi-bin
   /icons
   /manual

. Information found on port general/tcp


   Nmap found that this host is running Linux Kernel 2.4.0 - 2.4.17 (X86)

. Information found on port general/tcp


   Nmap only scanned 15000 TCP ports out of 65535.
   Nmap did not do a UDP scan, I
    guess.


. Information found on port general/tcp


   QueSO has found out that the remote host OS is
   * Standard: Solaris 2.x, Linux 2.1.???, Linux 2.2, MacOS


   CVE : CAN-1999-0454

. Warning found on port general/icmp



   The remote host answers to an ICMP timestamp
   request. This allows an attacker to know the
   date which is set on your machine.

   This may help him to defeat all your
   time based authentication protocols.

   Solution : filter out the ICMP timestamp
   requests (13), and the outgoing ICMP
   timestamp replies (14).

   Risk factor : Low
   CVE : CAN-1999-0524

. Warning found on port nfs (2049/udp)



   The nfsd RPC service is running.
   There is a bug in older versions of
   this service that allow an intruder to
   execute arbitrary commands on your system.

   Make sure that you have the latest version
   of nfsd

   Risk factor : High
```

```
   CVE : CVE-1999-0832

. Warning found on port unknown (32770/udp)


   The nlockmgr RPC service is running.
   If you do not use this service, then
   disable it as it may become a security
   threat in the future, if a vulnerability
   is discovered.

   Risk factor : Low
   CVE : CVE-2000-0508

. Warning found on port unknown (661/udp)


   The rquotad RPC service is running.
   If you do not use this service, then
   disable it as it may become a security
   threat in the future, if a vulnerability
   is discovered.

   Risk factor : Low
   CVE : CAN-1999-0625

. Vulnerability found on port unknown (32768/udp) :


   The remote statd service may be vulnerable
   to a format string attack.

   This means that an attacker may execute arbitrary
   code thanks to a bug in this daemon.

   *** Nessus reports this vulnerability using only
   *** information that was gathered. Use caution
   *** when testing without safe checks enabled.

   Solution : upgrade to the latest version of rpc.statd
   Risk factor : High
   CVE : CVE-2000-0666

. Warning found on port unknown (32768/udp)


   The statd RPC service is running.
   This service has a long history of
   security holes, so you should really
   know what you are doing if you decide
   to let it run.

   * NO SECURITY HOLE REGARDING THIS
```

```
      PROGRAM HAVE BEEN TESTED, SO
      THIS MIGHT BE A FALSE POSITIVE *

    We suggest you to disable this
    service.


    Risk factor : High
    CVE : CVE-1999-0018

 . Warning found on port nfs (2049/tcp)


    Here is the export list of xxx.xxx.xxx.xxx :
    /xxx/xxx xxx.xxx.xxx.xxx/255.255.0.0,

    CVE : CAN-1999-0554

 . Information found on port general/udp


    For your information, here is the traceroute to xxx.xxx.xxx.xxx :
    xxx.xxx.xxx.xxx



------------------------------------------------------
This file was generated by the Nessus Security Scanner
```