Global Information Assurance Certification Paper

AUDIT OF THE GIAC ENTERPRISES PRODUCTION WEB AND DATABASE SERVERS

Allen Stone
GCUX Practical Assignment v1.9
Option 2
February 6, 2004

Abstract

The purpose of this paper is to document the security audit of selected systems owned by GIAC Enterprises for the practical portion of the GCUX certification, v1.9, option #2. GIAC Enterprises is a company of 173 people whose business model is totally based on income from the Internet via the sale of fortune cookie sayings. A group of four RedHat Linux systems, three Web servers and one database server, was chosen to be the subject of the audit. These four systems represent GIAC's online presence. The company has been gaining in notoriety for providing high quality fortunes at a resonable price. To ensure that they do not lose momentum due to bad publicity, GIAC's management decided to bring in the professional security assessment services of the Wonderingmuse Group; a consulting firm that specializes in the auditing of online fortune cookie companies. The audit examined the systems, individually and as a group, using tools that are freely available to potential attackers.

Table of Contents

Executive Summary

Purpose

GIAC Enterprises (www.giacfortunes.com) engaged the Wonderingmuse Group, a security consulting firm, to audit a total of four systems, three production Web servers and one production database server. The project was undertaken and completed during the third week in December of 2003.

Scope

The audit focused not only on each system, but also on the interactions between the four systems. Management felt that testing the company's Web interface for buffer overflows and other vulnerabilities presented too large of a risk and, instead, requested that the source code for the company's in-house-developed CGI programs be examined. Tools that were approved for use in assessing the systems were the Nmap port scanner, the Nessus vulnerability scanner, the CIS host-based scanner, chkrootkit for detecting trojaned files, John the Ripper for weak password detection and RATS for use in analyzing the company's CGI source code.

State of Security

The company is at a high risk of compromise from vulnerabilities discovered during this audit and should waste no time in addressing the issues documented in this assessment.

Recommendations

- [Risk Level: High] Rewriting parts of the CGI programs and installing security modules in the Apache Web Server application are required to make the handling of input from the Web more secure. Several serious vulnerabilities in the Web site were discovered through analysis of the source code of the CGI programs. The issues include the presence of a buffer overflow condition and use of the wrong account combined with the lack of restrictions on the correct account when querying the database; all of which could allow an attacker to access sensitive information.
- [Risk Level: High] Use of a Tripwire-like application is needed to monitor for file change. Without the proper level of vigilance over the data stored on a system, the company exposes itself to the possibility of undetected data manipulation.
- [Risk Level: High] The company needs to develop a patch management process that encompasses all programs installed on the production systems. The current patch management process does not provide coverage for all applications on the production systems. With the daily discovery of new vulnerabilities, daily, the company runs the risk of a possible compromise by not keeping its Internet-facing systems up-to-date.

1.0 Audit Methodology and Description of Systems

1.1 Pre-Audit Planning

A meeting with GIAC's upper management was held, prior to beginning the audit, in which the scope and the schedule for the audit were defined. The scope of the audit included a total of four servers, a single database server (webdb) and three Web servers (web1, web2 and web3), which make up the company's Internet presence. The goal was defined as assessing the security of each system and the security of the systems as a group. Proposed tools for conducting the audit and their uses were outlined. At this point concern was expressed regarding the use of any tools that would attempt to enter data in the forms on the Web site, like wpoison (http://sourceforge.net/projects/wpoison/). Management's primary concern was the impact of such actions on both the servers and the Web site. The GIAC employees attending the meeting were advised that, without testing the Web site for possible vulnerabilities within the CGI applications, the audit would be ignoring the main vector of attack. The company did agree, however, to allow Nessus to run using the available "safe" Web site checks. As well, in lieu of running a Web application-testing tool, management requested that the source code for the CGI programs be analyzed for issues.

Additional precautions were discussed, while creating the audit schedule, to ensure that the audit did not interfere with the company's operations. Evaluation would occur only after 7PM, local time. During the day, the audit would focus on evaluating procedures and policies. While on-site, the auditor would be accompanied by GIAC personnel. A copy of the software, and the commands used to run the software, for the audit was provided to GIAC.

Evaluation of the systems would include the following:

- Network scans conducted from both inside and outside the firewall using Nmap and Nessus.
- Host-based scans conducted on all four systems using CIS Scan.
- Assessment of password strength using John the Ripper on /etc/shadow from all four systems.
- Analysis of the source code for the company's CGI applications using RATS.

Evaluation of policies and procedures would include the following:

- Review of security policies.
- Interviews with staff to learn the specifics of the company's operations.
- Inspection of physical security with concern to the systems being audited.

GIAC provided designated contacts as resources for the audit and guaranteed full the cooperation of its employees. It was agreed that all of GIAC's procedures and pertinent sensitive information would be provided as long as all furnished data, written or electronic, remained on the premises.

1.2 Interviews

During the audit, the company provided representatives from the various departments in the company for interviews. The interviews covered what access that person's group had the production systems and what services they used in their day-to-day business functions. Among other things, representatives from the IT department were interviewed regarding their daily procedures that involved the production systems and their procedures for originally configuring the production systems.

1.3 Approved Tools

For tests that were conducted while not logged into the production systems, a Dell Latitude C640 laptop was used. It was booted from a Knoppix-STD (http://www.knoppix-std.org/) CD-ROM and reports were saved to an external floppy disk. This was done as a safety measure to protect the company's data, which included password files, source code and vulnerability scan data, by ensuring that the data did not remain resident on the laptop. A second CD-ROM was used to run the host-based tests on the production systems.

Table 1.1 Tools Used to Perform Audit

Tool Name	Tool Version	Tool Function	Executed On	URL
Nmap	3.10 ALPHA4	Port Scanner	Laptop	http://www.insecure.org
Nessus	2.0.4	Vulnerability Scanner	Laptop	http://www.nessus.org
CIS Scan	1.4.2-1.0	System Benchmark	Servers	http://www.cisecurity.com/bench_linux.html
John	1.6	Password Auditing	Laptop	http://www.openwall.com/john
Chkrootkit	0.42b	Trojan Detection	Servers	http://www.chkrootkit.org
RATS	2.1	Source Code Analysis	Laptop	http://www.securesw.com/rats

1.4 Description of Systems

1.3.1 Hardware

All systems run on Intel-based IBM servers. The three Web servers run on three individual IBM x235's, while the database server runs on an IBM x255.

Table 1.2 Hardware Configurations

System Type	Web Servers	Database Server

Model	IBM x235	IBM x255
Processor(s)	2x 2.40GHz Xeon	4x 1.60GHz Xeon
RAM	2GB	6GB
Hard Drive Controller	U320 PCI-X	ServeRAID-6M Ultra320 SCSI [RAID5 configured]
Hard Drive(s)	1x 36GB	3x 73GB
Backup Drive	None	IBM 160/320GB SDLT Tape Drive
Removable Media Drive(s)	1x 3.5", 1.44MB Floppy 1x 40X SCSI CDROM	1x 3.5", 1.44MB Floppy 1x 40X SCSI CDROM
Input Device(s)	Keyboard, mouse & monitor shared between all four servers via Belkin KVM switch	
Network Interface	1x 10/100/1000 Mbps Ethernet [Integrated]	1x 10/100/1000 Mbps Ethernet [Integrated]

1.3.2 Operating System

All four servers are running RedHat Linux 7.3 (2.4.18-3smp) and were installed from the same CD-ROM media.

```
# cat /proc/version
Linux version 2.4.18-3smp (bhcompile@daffy.perf.redhat.com) (gcc
version 2.96 20000731 (Red Hat Linux 7.3 2.96-110)) #1 SMP Thu
Apr 18 07:27:31 EDT 2002
```

1.3.3 Third-Party Applications

It was discovered through the interview with members of the IT staff that all four systems were set up using the default "server" install from the RedHat 7.3 cd-roms. Any third-party software that was not included in the default server install was then installed from RPM or source distribution. Applications that are currently installed on the servers and run as services or are used as part of a system's role, are listed below.

Table 1.2 Installed Applications

Application	Systems Installed on
Amanda 2.4.2p2-7	webdb
Apache 1.3.27/mod_ssl 2.8.14/OpenSSL 0.9.6g/mm 1.2.1	web1, web2, web3
AutoRPM 3.3-1	web1, web2, web3, webdb
MySQL 3.23.58-1	webdb
OpenSSH 3.1p1-14	web1, web2, web3, webdb
Xalan-C 1.4.0	web1, web2 & web3
Xerces-C 2.0.0	web1, web2 & web3

The audit will include assessing each application's configurations. Applications not listed in this table are not needed in supporting any of the systems' functions within the production environment.

1.5 System role within network

The Web servers (web1, web2 and web3) run the company's Web site that provides a portal for customers to create, modify, and track orders. The database server (webdb) contains customer and product information. This data is also made available internally to customer service representatives to help assist customers. In addition, the data is also available to various members of the accounting and sales staff.

1.6 Risks Associated with System Roles

1.6.1 Web Servers

The Web servers have only one role, to server content for the company's web site. The major risk associated with any Web server is its exposure to the Internet. The slightest error in configuring a Web server can aid an attacker in compromising the system. The most common of these errors include:

- Failure to disable any default settings that are not required to host the Web site.
- Failure to remove any example programs.
- Relaxing permissions on resources to allow poorly written CGI applications to run.
- Assuming that all data entered through the CGI applications will be legitimate.
- Enabling a setting without understanding its impact on security.

Another common misconception is that having a firewall will protect the Web site and Web server application. While the firewall can help to limit access to just those services a company makes available to the Internet, it does not protect the content of the Web site from malicious input.

1.6.2 Database Server

The database server holds all of the information needed to host a successful e-commerce site. While not directly connected to the Internet, the data this system serves is available to the Internet via the CGI applications on the Web servers. This makes the database server a primary target. The most common security errors made on databases are:

- Failure to disable any default features that are not required for the database to function in a production environment.
- Failure to remove any example databases.
- A lack of restrictive privileges granted to users.
- Use of shared accounts to access data.
- Use of root (or sa) account for daily maintenance and development.
- Weak or blank passwords.
- Developer access to production data and/or database application.

1.6.3 Network Connectivity

All four systems sit on a VLAN (Virtual Local Area Network) by themselves. All other servers, regardless of function, are on the enterprise server VLAN. The company utilizes five VLANs to divide the network by department and restrict access to certain resources.

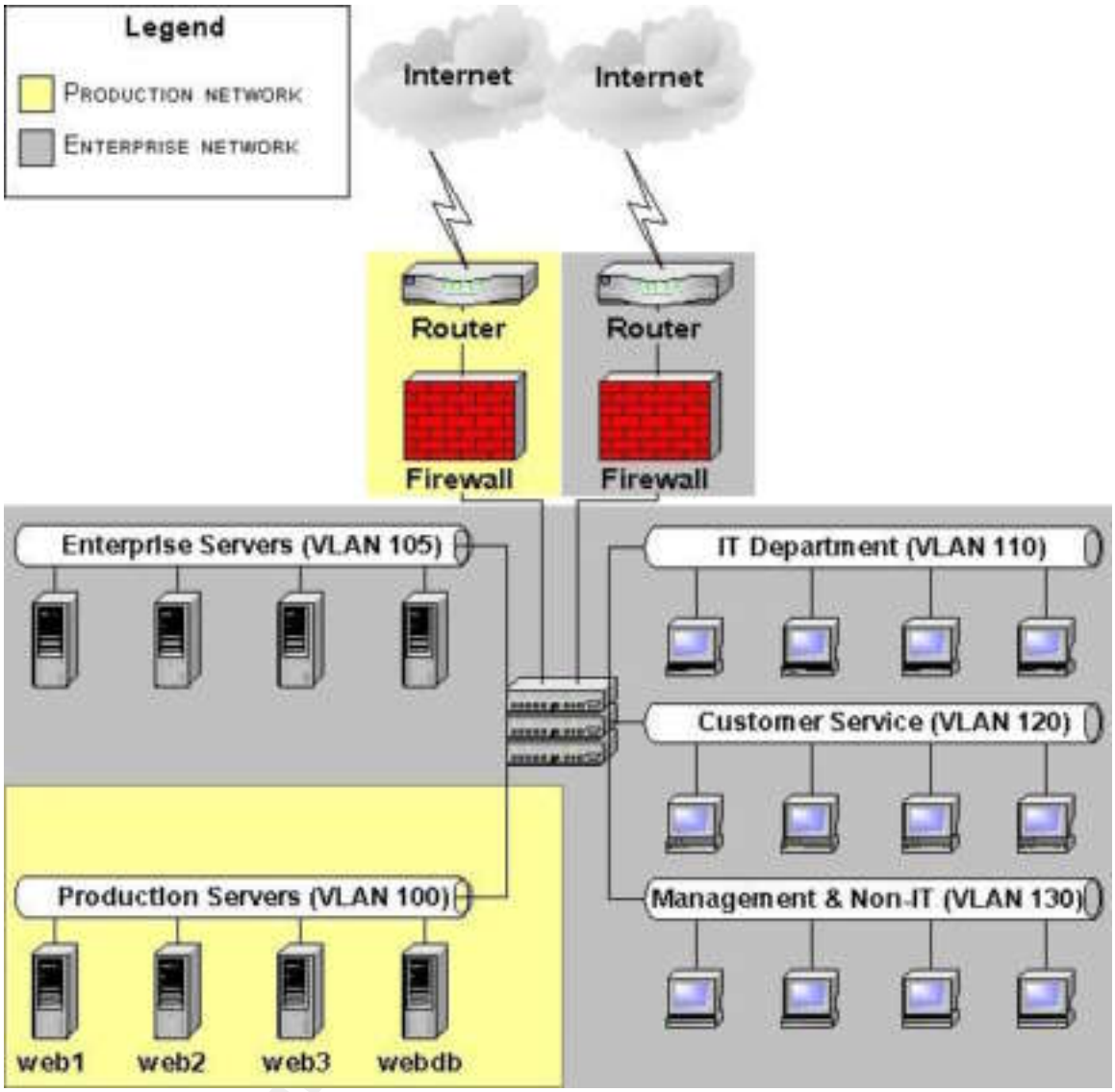
Table1.3 VLANs

VLAN Number	Computers Present	IP Address
100	Production Web & Database Servers	192.168.100.x
105	Email and Enterprise Servers	192.168.105.x
110	IT Staff Workstations	192.168.110.x
120	Customer Service Staff Workstations	192.168.120.x
130	Management & Non-IT Staff Workstations	192.168.130.x

Restricting access to a resource for a given VLAN is achieved by not creating a route to that resource on the switch. Thus, to keep the enterprise servers separate from the production servers no route was created between the two VLANs. However, this is the extent of separating the production and enterprise networks. All other computers on the network can see each other.

GIAC uses a Cisco PIX firewalls to provide protection for the company's network from the Internet. The production environment has it's own firewall and ISP. Likewise, the enterprise environment has its own firewall and ISP. No other firewalls are used on the network.

Graphic 1.1 Network Map



2.0 Detailed Analysis

Since all servers were set up from the same RedHat 7.3 distribution, and all default settings were accepted, it was found that for the most part all of the servers shared the same security issues. The difference in the configurations of the servers was found to be third-party applications that were installed after the systems were initially set up.

The CIS Scanner rated each system on a scale from one to ten, ten being a perfect score. The database server (webdb) scored slightly higher than the web servers, however its score was still only 5.24 out of 10. Below are the scores that the CIS Scanner awarded each system.

Table 2.1 CIS Scanner Ratings

System	Rating (out of 10)
web1	5.08
web2	5.08
web3	5.08
webdb	5.24

2.1 Operating system vulnerabilities

The current version of the Linux kernel has several flaws that have been correlated with several vulnerabilities. The current AutoRPM automated update process ignores kernel updates. AutoRPM should be configured to ignore kernel updates since anything affecting the architecture of the kernel should be tested and then manually installed.

2.1.1 Real-time clock vulnerability (CAN-2003-0984)

Description from mitre.org:
"Real time clock (RTC) routines in Linux kernel 2.4.23 and earlier do not properly initialize their structures, which could leak kernel data to user space" (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0984).
Corresponding RedHat Errata:
https://rhn.redhat.com/errata/RHSA-2003-417.html

2.1.2 mremap system call vulnerability (CAN-2003-0985)

Description from mitre.org:
"The mremap system call (do_mremap) in Linux kernel 2.4 and 2.6 does not properly perform bounds checks, which allows local users to cause a denial of service and possibly gain privileges by causing a remapping of a virtual memory area (VMA) to create a zero length VMA" (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0984).
Corresponding RedHat Errata:

https://rhn.redhat.com/errata/RHSA-2003-417.html

2.1.3 do_brk function vulnerability (CAN-2003-0961)

Description from mitre.org:
"Integer overflow in the do_brk function for Linux kernel 2.4.22 and earlier allows local users to gain root privileges. (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0961)"
Corresponding RedHat Errata:
https://rhn.redhat.com/errata/RHSA-2003-392.html
Numerous other kernel vulnerabilities listed in
https://rhn.redhat.com/errata/RHSA-2003-238.html
The vulnerabilities listed in this alert are addressed in the updates above.

Affected Systems:
web1 (2.4.18-3smp)
web2 (2.4.18-3smp)
web3 (2.4.18-3smp)
webdb(2.4.18-3smp)

2.2 Configuration vulnerabilities

2.2.1 OpenSSH

CIS Scanner reported that the sshd_config file is not configured securely. By default, the sshd configuration file is set for compatibility, allowing users to connect using old ssh clients. Using the default configuration file in a production environment can lead to compromising the level of security.
CIS Scanner results:

```
Negative: 1.2 sshd_config parameter Protocol is not set.
Negative: 1.2 ssh_config must have 'Protocol 2' underneath Host
*.
Negative: 1.2 sshd_config parameter PermitRootLogin is not set.
Negative: 1.2 sshd_config parameter PermitEmptyPasswords is not
set.
```

As well, additional settings were found to pose a security risk to the system in the sshd configuration file. In most cases, the setting correctly exists, it is just commented out. While some commented-out settings are default settings, it is always best to explicitly state the settings than to implicitly trust the default configuration.

StrictModes tells the ssh daemon to check the permissions on the user's home directory and rhosts files before allowing the user to login. (http://www.tldp.org/LDP/solrhe/Securing-Optimizing-Linux-RH-Edition-v1.3/chap15sec122.html) StrictModes should be set to "yes" in the configuration.

RhostsAuthentication allows users to set up .rhosts files which contain trusted users/computers/networks which can login without supplying a password. RhostsAuthentication should be set to “no” in the configuration.

RhostsRSAAuthentication works on the same premise as RhostsAuthentication plus RSA authentication. RhostsRSAAuthentication should be set to “no” in the configuration.

IgnoreRhosts specifies that sshd is not to use the users’ .rhosts/.shosts files. IgnoreRhosts should be set to “yes” in the configuration.

LoginGraceTime specifies the amount of time (in seconds) that are given for a user to login at the login prompt. Setting the time-out low makes it more difficult to brute force attack a user’s account. LoginGraceTime should be set to atleast “300”, if not lower. 300 seconds (5 min.) is a very generous amount of time to complete a login.

PasswordAuthentication requires that password authentication be used (as opposed to public key authentication, etc). PasswordAuthentication should be set to “yes” in the configuration.

Banner is used to display warning messages above the login prompt. Banner should be set to /etc/issue.net. /etc/issue.net should be created if it does not exist.

LogLevel is used to tell sshd what level of logging should be done to syslog. “SyslogFacility AUTHPRIV” is already set. LogLevel should be set to INFO in the configuration.

Affected Systems:
web1
web2
web3
webdb

2.2.2 Enabled Services

CIS Scanner found that several services are enabled to run at start up. The table below shows the services the CIS Scanner found enabled that are not needed on the system.

Table 2.2 Unneeded Active Services

Service	CIS Benchmark	Affected Systems
xinetd	3.2	web1, web2, web3
Smtp	3.3	web1, web2, web3, webdb

xfs	3.5	web1, web2, web3, webdb
apmd	3.6	web1, web2, web3, webdb
samba	3.7	web1, web2, web3
nfslock	3.9	web1, web2, web3, webdb
autofs	3.9	web1, web2, web3, webdb
portmap (rpc)	3.12	web1, web2, web3, webdb
netfs	3.13	web1, web2, web3, webdb
lpd	3.14	web1, web2, web3, webdb
kudzu	3.21	web1, web2, web3, webdb
ntpd	None	web1, web2, web3, webdb

Xinetd is a wrapper for services (like in.telnetd, in.ftpd, rlogind, rshd, fingerd, and other services found in /etc/xinetd.d), and acts as an intermediary between the service and remote requests to these services. All three Web servers are currently running xinetd when there are no services enabled that xinetd controls.

Sendmail (smtp) is enabled on all four servers. Not one is acting as a mail server and Sendmail should either be disabled or un-daemonized so that it does not accept remote connections.

Xfs is enabled on all four servers. Since there is no need for anyone to use X Windows on any of these servers, this service should be disabled.

Apmd is the power management service designed to monitor battery status. This service is not needed.

Samba allows Linux systems to share files with and participate in a Microsoft Windows network. Through interviews with the IT staff, it was discovered that at one time Samba was used for updating the Web site. However, now sftp is used in its place. Through an oversight, Samba was never totally disabled. As well, the Nessus scanner was able to enumerate shared folders on all Web of the servers, but examination of these shares showed that none expose sensitive data. Samba should be uninstalled from all three Web servers as its presence places the servers at risk of SMB-related attacks as well as exposing information about the servers.
From the output of Nessus:

```
The following shares can be accessed using a NULL session :
IPC$
ADMIN$
```

Nfslock starts the NFS file locking daemon. No NFS-shared folders were found using showmount –d <server> on each of the servers. Since NFS is not needed on any of these systems, it should be disabled.

Autofs controls the automount process at start up. It is not needed in a production environment since any "mount" commands should be issued manually by an administrator and should be disabled.

Portmap is a wrapper for RPC services. This service, too, does not provide any function that is needed in the production environment and should be disabled. While Nessus was unable to associate a particular vulnerability with this service, a general warning was issued:

```
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.
```

Netfs controls the mounting of NFS and SMB remote shares. Since it is not needed, it should be disabled.

Lpd is the printer daemon. Since printing is not needed, it should be disabled.

Kudzu detects hardware changes so it should not need to run all the time. If new hardware is added later the daemon can be manually started to detect the hardware and then turned off again.

Ntpd synchronizes the system's clock with Internet time servers. Nmap found the NTP daemon listening on port 123/udp. Since the only reason NTP is installed is so that the system can synchronize its clock with Internet time servers, there is no need for the service to be listening on 123/udp. Rather than running ntpd in daemon mode, it can be invoked through cron (hourly) with the "-q" option which should make the application behave as ntpdate. If this is done then "chkconfig ntpd off" can be run to disable the NTPd daemon start up scripts.

```
Port        State       Service
123/udp     open        ntp
```

2.2.3 IP Parameters

CIS-Scanner reported that the network parameters are not set to properly protect the system from some network attacks.

SYN flood protection. This option will limit the number of connections for which the server has not received an ACK. Increasing the number will allow for more backlogged SYN connections and will allow it to better withstand a SYN flood attack (http://lwn.net/Articles/45386/).

```
Negative: 4.1 /proc/sys/net/ipv4/tcp_max_syn_backlog should
be at least 4096 to handle SYN floods.
```

Source routing control. This option, when set to 0, will deny and packets with the SRR set (http://lwn.net/Articles/45386/). This option should be applied to all interfaces under /proc/sys/net/ipv4/conf.

```
Negative: 4.1
/proc/sys/net/ipv4/conf/eth0/accept_source_route should be
set to 0
Negative: 4.1
/proc/sys/net/ipv4/conf/lo/accept_source_route should be
set to 0.
```

Accept redirects. This option, when set to 0, will deny ICMP redirects. This option should be applied to all interfaces under /proc/sys/net/ipv4/conf.

```
Negative: 4.1 /proc/sys/net/ipv4/conf/eth0/accept_redirects
should be set to 0.
Negative: 4.1 /proc/sys/net/ipv4/conf/lo/accept_redirects
should be set to 0.
```

Secure redirects. This option, when set to 0, will deny ICMP redirects specifically for any gateways listed in the default gateway list (http://lwn.net/Articles/45386/). This option should be applied to all interfaces under /proc/sys/net/ipv4/conf.

```
Negative: 4.1 /proc/sys/net/ipv4/conf/eth0/secure_redirects
should be set to 0.
Negative: 4.1 /proc/sys/net/ipv4/conf/lo/secure_redirects
should be set to 0.
```

Send redirects. This option, when set to 0, will disable the system's ability to send redirects. This option should be applied to all interfaces under /proc/sys/net/ipv4/conf.

```
Negative: 4.2 /proc/sys/net/ipv4/conf/eth0/send_redirects
should be set to 0.
Negative: 4.2 /proc/sys/net/ipv4/conf/lo/send_redirects
should be set to 0.
```

Affected Systems:
web1
web2
web3
webdb

2.2.4 File System Mounts – Nodev

CIS Scanner found that partitions were mounted without the "nodev" option. This option should be used to keep the user from accessing any "character or block special devices on the file system" (mount manpage). This will prevent the user from accessing mounted devices that would normally be mounted in /dev (CIS Benchmark 24). One warning is issued under Section 6.1 in the CIS Linux Benchmark Guide (24) with regard to using this setting on mounts in which chroot has created special devices for the purpose of running a program with limited access to system resources. Thus, if the company is planning on "chroot-ing" any of its applications, this setting could cause issues.

```
Negative: 6.1 /boot is not mounted nodev.
Negative: 6.1 /var is not mounted nodev.
Negative: 6.1 /home is not mounted nodev.
Negative: 6.1 /usr is not mounted nodev.
Negative: 6.2 Removable filesystem /mnt/floppy is not
mounted nodev.
Negative: 6.2 Removable filesystem /mnt/cdrom is not
mounted nodev.
```

Affected Systems:
web1
web2
web3
webdb

2.2.5 File System Mounts – Nosuid

CIS Scanner found that the floppy and cdrom devices are not mounted with the "nosuid" option. The "nosuid" option will prevent existing uid's/gid's from being copied with the files from that mount point to another. By adding nosuid to the options column in /etc/fstab this issue can be fixed. Since the servers are kept in a secure room with limited access, this only poses a small risk.

```
Negative: 6.2 Removable filesystem /mnt/floppy is not
mounted nosuid.
Negative: 6.2 Removable filesystem /mnt/cdrom is not
mounted nosuid.
```

Affected Systems:
web1
web2
web3
webdb

2.2.6 File System Mounts – Removable Media

CIS Scanner found that removable media can be mounted by any user. This means that anyone can potentially copy data on or off the system. Since the servers are kept in a secure room with limited access, this only poses a small risk.

```
Negative: 6.3 PAM allows users to mount removable media:
<floppy>.  (/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media:
<cdrom>.  (/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media:
<pilot>.  (/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media:
<jaz>.  (/etc/security/console.perms)
```

```
Negative: 6.3 PAM allows users to mount removable media:
<zip>.  (/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media:
<ls120>.  (/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media:
<camera>.  (/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media:
<memstick>.  (/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media:
<flash>.  (/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media:
<diskonkey>.  (/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media:
<rem_ide>.  (/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media:
<rio500>.  (/etc/security/console.perms)
```

Affected Systems:
web1
web2
web3
webdb

2.2.7 Cron/At Security – Access Lists

CIS Scanner found that the scheduling services are not secured. The ".allow" files for both the Cron and At services restrict user access by allowing the listed users to schedule commands through either service. Thus, anyone who has an account on the system can create cronjobs. Totally restricting access to At is recommended since Cron is available.

```
Negative: 7.5 Couldn't open cron.allow
Negative: 7.5 Couldn't open at.allow
```

Affected Systems:
web1
web2
web3
webdb

2.2.8 Cron/At Security – Crontab Permissions

CIS Scanner found that permissions are lax on /etc/crontab. The only user who should need access to /etc/crontab is root and permissions on the file should reflect this.

```
Negative: 7.6 The permissions on /etc/crontab are not
sufficiently restrictive.
```

Affected Systems:

web1
web2
web3
webdb

2.2.9 Xinetd Security

CIS Scanner found that Xinetd is missing the “only-from” statement in its configuration.

```
Negative: 7.8 xinetd either requires global 'only-from'
statement or one for each service.
```

However, instead of specifying the “only-from” option in Xinetd, it is recommended that /etc/hosts.allow and /etc/hosts.deny be used since Xinetd services and some non-Xinetd services (like SSH) read their access lists from these files. Use of these two files will be discussed later in this report.

Affected Systems:
web1
web2
web3
webdb

2.2.10 Root Login

CIS Scanner found that the root user has the ability to login remotely. Root should only be allowed to login at the console. All other access by root to the system should be done through "su" and "sudo." Only lines tty1 – tty6 should be in /etc/securetty. All others should be removed. This, however, does not disable root logins through SSH. Disabling root logins through SSH is done through /etc/ssh/sshd_config.

```
Negative: 7.9 /etc/securetty has a non console or tty 1-6
line: vc/7.
Negative: 7.9 /etc/securetty has a non console or tty 1-6
line: vc/8.
Negative: 7.9 /etc/securetty has a non console or tty 1-6
line: vc/9.
Negative: 7.9 /etc/securetty has a non console or tty 1-6
line: vc/10.
Negative: 7.9 /etc/securetty has a non console or tty 1-6
line: vc/11.
Negative: 7.9 /etc/securetty has a non console or tty 1-6
line: tty7.
Negative: 7.9 /etc/securetty has a non console or tty 1-6
line: tty8.
Negative: 7.9 /etc/securetty has a non console or tty 1-6
line: tty9.
```

```
Negative: 7.9 /etc/securetty has a non console or tty 1-6
line: tty10.
Negative: 7.9 /etc/securetty has a non console or tty 1-6
line: tty11.
```

Affected Systems:
web1
web2
web3
webdb

2.2.11 Grub Boot Loader

CIS Scanner found that the Linux boot loader, Grub, should be secured to prevent unauthorized access to the boot menu. If the system is rebooted, the possibility exists for someone to change the settings that control loading the operating system. Using the utility /sbin/grub-md5-crypt will allow the use of an encrypted password in /etc/grub.conf.

```
Negative: 7.10 GRUB isn't password-protected.
```

Affected Systems:
web1
web2
web3
webdb

2.2.12 Single-user Mode

CIS Scanner reported that the potential exists for anyone to boot the system and enter single-user mode without a password. At this point, system files can be edited. Adding a line for single-user mode containing /sbin/sulogin will prevent access without a password.

```
Negative: 7.11 /etc/inittab needs a /sbin/sulogin line for
single user mode.
```

Affected Systems:
web1
web2
web3
webdb

2.2.13 Service Accounts with Valid Shells

CIS Scanner found that two accounts on all of the servers have valid shells. Since service accounts do not need a valid shell these shells should be changed to /sbin/nologin.

```
Negative: 8.1 news has a valid shell of /bin/sh.  Remember,
an empty shell field in /etc/passwd signifies /bin/sh.
```

```
Negative: 8.1 rpm has a valid shell of /bin/bash.
```

Affected Systems:
web1
web2
web3
webdb

2.2.14 Password Policy

CIS Scanner reported that password aging is not implemented for users. While no password policy appears to have been implemented on the production systems, through the interviews with the IT staff, it was learned that the company does have a written password policy and it is applied to their corporate Windows network. If the password policy is not enforced on the production systems, users will be able to choose weak passwords. A weak password is one that is easily guessed, either by being too short or by failing to use numbers and symbols. As well, if the password is not forced to change, the attacker has more time (and chances) to figure out the password.

Maximum Age. The company's password policy states that the maximum password age should be no greater than 45 days.

```
Negative: 8.3 /etc/login.defs value PASS_MAX_DAYS = 99999,
but should not exceed 90.
Negative: 8.3 User bsmith should have a maximum password
life of between 1 and 90 days.
Negative: 8.3 User tjohnson should have a maximum password
life of between 1 and 90 days.
Negative: 8.3 User rsimms should have a maximum password
life of between 1 and 90 days.
Negative: 8.3 User vpendly should have a maximum password
life of between 1 and 90 days.
Negative: 8.3 User twilson should have a maximum password
life of between 1 and 90 days.
Negative: 8.3 User fhill should have a maximum password
life of between 1 and 90 days.
```

Minimum Age. The company's password policy states that the minimum password age should be no less than two days. Note: password age should be manually applied to users using either "chage" or "passwd."

```
Negative: 8.3 /etc/login.defs value PASS_MIN_DAYS = 0, but
should not be less than 7.
Negative: 8.3 User bsmith should have a minimum password
life of at least 7 days.
Negative: 8.3 User tjohnson should have a minimum password
life of at least 7 days.
```

```
Negative: 8.3 User rsimms should have a minimum password
life of at least 7 days.
Negative: 8.3 User vpendly should have a minimum password
life of at least 7 days.
Negative: 8.3 User twilson should have a minimum password
life of at least 7 days.
Negative: 8.3 User fhill should have a minimum password
life of at least 7 days.
```

Password Strength. The company's password policy states that the password should have a minimum length of 10 characters. Note: While CIS Scanner checked /etc/login.defs, the better place to check is the arguments for cracklib.so in /etc/pam.d/system-auth. Cracklib can be used to enforce password policy system-wide. Examination of this file on all four systems confirmed that no password policy was in effect for the production systems.

```
Negative: 8.3 /etc/login.defs value PASS_MIN_LEN = 5, but
should be at least 6.

# cat /etc/pam.d/system-auth | grep ^password
password  required  /lib/security/pam_cracklib.so retry=3
type=
password  sufficient     /lib/security/pam_unix.so nullok
use_authtok md5 shadow
password  required  /lib/security/pam_deny.so
```

The line containing "pam_cracklib.so" does not have the argument "menlen=," which would enforce a minimum password length.

Affected Systems:
web1
web2
web3
webdb

2.2.15 Users with Weak Passwords

Using John the Ripper on the /etc/shadow files from all four systems, two accounts were discovered to have weak passwords. These users should be required to change their passwords. Below are the results for /etc/shadow from webdb. All shadow files were observed to be identical.

```
# ./john -w:password.lst -rules shadow.webdb > /dev/null ; ./john -show
shadow.webdb | awk –F: '{ print $1 }'
fhill
rsimms

2 password cracked, 22 left
```

The wordlist was downloaded from ftp://ftp.openwall.com/pub/wordlists/.

2.2.16 Home Directories

CIS Scanner found that one user's home directory was consistently world-writable across all four systems. As well, at least one .* file in this user's home directory was world-writable or group-writable. Permissions on home directories should not allow for group or world access.

```
Negative: 8.7 User rsimms has a world-writable homedir!
Negative: 8.7 User rsimms has a group-writable homedir!
Negative: 8.7 User rsimms has a world-executable homedir!
Negative: 8.7 User rsimms has a world-readable homedir!
Negative: 8.8 User rsimms has world/group-writable dot-
files (.*) in his/her home directory.
```

Affected Systems:
web1
web2
web3
webdb

2.2.17 Core File Security

CIS Scanner reported that core dumps are enabled. When a program errors-out, it can produce a core file. The core file contains information that was loaded into memory for the program at the time the error occurred. Core files are useful for development, but should not be enabled in a production environment. Thus, if the program was working with any sensitive information (such as passwords, system configuration, or even customer data), that information could potentially be written to the disk in the core file. Use of the program file "strings" would be able to display information stored within the core file. Core dumps can be eliminated system-wide by editing the /etc/security/limits.conf file.

```
Negative: 8.11 Coredumps aren't deactivated.
```

Further investigation of the systems (`find / -name "core*"`) produced a core dump file web3 dating back eight months was found in the script directory of the Web site (/usr/local/apache/secure/cgi-bin). Through the use of a debugger, gdb (http://www.gnu.org/software/gdb/gdb.html), it was discovered that the dump was produced by the cgi application named "`confucius`."

```
(gdb) core-file core.31668
Core was generated by `./confucius'.
```

The risk of exposing customer data through this file is minimal since the file is not executable and Apache only allows execute permissions in this directory. However, the fact that customer can be present in the script directory is cause enough to eliminate the possibility of core files being created.

Affected Systems:
web1
web2
web3
webdb

2.3 Vulnerabilities from Third-party Applications

2.3.1 IPTables

IPTables is a kernel-level packet-filtering program that should be used like a miniature firewall for each system on which it is installed. While the presence of IPTables does not pose a risk to the security of the system in its current configuration, utilization of this program will help greatly increase the system's overall security. With IPTables, it is possible to create access lists for incoming traffic to allowed services on the system. Since the production servers interact with systems inside the network, there is a need for the protection that this package offers.

Manual checking of the systems showed that all had IPTables installed (rpm –q iptables) and enabled in run levels 2345 (chkconfig --list iptables). However, IPTables is not configured to protect the systems.

```
# iptables -L
Chain INPUT (policy ACCEPT)
target    prot   opt    source   destination

Chain FORWARD (policy ACCEPT)
target    prot   opt    source   destination

Chain OUTPUT (policy ACCEPT)
target    prot   opt    source   destination
```

If rules were in place they would show up here. The default (current) configuration allows all traffic to and from these systems. Access to each system should be configured to only allow required connections and to drop everything else.

Affected Systems:
web1
web2
web3
webdb

2.3.2 In-House-Developed Web Applications

The biggest security risks are associated with the applications and services that are exposed to the Internet. GIAC created and maintains the Web interface for its site, which also includes the C++ applications that handle authentication, dynamic content, and order placement. Because the applications

are such a critical part of the company's operations, GIAC management deemed it necessary to include an examination of the web-based applications in the assessment.

The Web site is run by two C++, cgi programs, "confucius" and "login." As expected, login handles the customer login to the site. Upon successful authentication, through querying the MySQL database, it sets up the session and creates the authentication token (in this case a cookie). Once this is complete, the users interact with "confucius" until they log out or the session expires. The "confucius" application handles a myriad of functions including manipulating or displaying customer data, order placement, product offerings, and (of course) displaying fortune cookie sayings. In reviewing the source code of both applications, several major issues were noted.

Buffer Overflow. Of primary concern is the discovery of a buffer overflow condition within the "confucius" application. This is a direct result of using the strcpy() function to copy an environment variable from user input into an unchecked buffer. The unchecked input is received through the "order comments" text box in the order submission form. This programming oversight could allow an attacker to compromise any of the Web servers.

The output from the Rough Auditing Tool for Security (RATS) shows three different lines (numbers 2052, 2053 and 2054), which together produce the condition. The reason for RATS outputting four lines in this example is that one line (2054) contains two potentially insecure functions, "getenv" and "strcpy."

```
1) confucius.cpp:2052: High: fixed size local buffer
                char comment[512];
Extra care should be taken to ensure that character arrays
that are allocated on the stack are used safely.  They are
prime targets for buffer overflow attacks.

2) confucius.cpp:2053: High: getenv
                if (getenv("COMMENT") != NULL)
   confucius.cpp:2054: High: getenv
                    strcpy(comment,getenv("COMMENT"));
Environment variables are highly untrustable input. They
may be of any length, and contain any data. Do not make any
assumption ns regarding content or length. If possible
avoid using them, and if it is necessary, sanitize them and
truncate them to a reasonable length.

3) confucius.cpp:2055: High: strcpy
                strcpy(comment,getenv("COMMENT"));
Check to be sure that argument 2 passed to this function
call will not copy more data than can be handled, resulting
in a buffer overflow.
```

The buffer overflow occurs because a size of 512 is defined for “comment” (line 2052) and strcpy() (line 2054) does not check or limit the size of the data that is being copied from the Web form. Thus, data exceeding the defined size of 512 will overflow the buffer, which presents the opportunity for an attacker to possibly insert pointers to other areas in memory and run code.

The vulnerability is minimized by its location on the Web site. A user must first submit a valid credit card for a valid order before being presented with the opportunity to exploit this issue. At this point, it appears that this vulnerability has not been intentionally exploited. However, the company’s first priority should be to address this issue.

MySQL Root. A second issue was found in “confucius” that also presents a high risk. Analysis of confucius.cpp uncovered use of the MySQL “root” account. Results of search for the string “connect” in confucius.cpp and login.cpp are below.

```
# for file in confucius.cpp login.cpp ; do echo $file: ; \
    cat $file | grep connect ; done
confucius.cpp:
Connection connect("customers","webdb","root","giac");
Connection connect("furtunes","webdb","web","webpass");
Connection connect("orders","webdb","web","webpass");
Connection connect("products","webdb","web","webpass");
login.cpp:
Connection connect("customers","webdb","web","webpass");
```

Note: The format for the connect() function is `connect(“db_name”,”db_server”,”username”,”password”);`, provided by lines 63 & 64 of `connection1.hh` from the MySQL++ package.

The MySQL “root” account should be protected from use by any application that interacts with the Internet. Should an attacker succeed in passing a SQL query command to the Web application, the attacker would have full control over the database and its contents. Coupled with the lack of input validation that was observed when looking over the code, the possibility exists that an attacker could pass SQL queries to the database via forms on the Web site.

Note: Testing of input validation through the Web site was not possible because management requested that no testing be done on the production Web site.

2.3.3 MySQL Security

The MySQL database on webdb houses all of the company’s vital commerce-related data and should be protected at all costs. Several

configuration vulnerabilities were discovered by manually inspecting the MySQL application.

Remote root access. Remote root access should not be allowed. Just as with SSH logins to the systems, no one should be allowed to remotely login as root in MySQL.

```
mysql> select user,host from mysql.user where user="root";
```

User	Host
Root	admin1
Root	admin2
Root	admin3
Root	devstation1
Root	localhost
Root	web1
Root	web2
Root	web3
Root	Webdb

```
9 rows in set (0.00 sec)
```

Restrict permissions. The user account that is set up for the Web applications and the customer service application to access the database has full privileges over all databases.

```
mysql> select user,host from mysql.user where user="web";
```

User	host
Web	%
Web	web1
Web	web2
Web	web3

```
4 rows in set (0.00 sec)

mysql> show grants for web@web1;
```

Grants for web@web1
GRANT ALL PRIVILEGES ON *.* TO 'web'@'web1' IDENTIFIED BY PASSWORD ...
GRANT SELECT, INSERT, UPDATE, DELETE ON `products`.* TO 'web'@'web1'
GRANT SELECT, INSERT, UPDATE, DELETE ON `fortunes`.* TO 'web'@'web1'
GRANT SELECT, INSERT, UPDATE, DELETE ON `orders`.* TO 'web'@'web1'
GRANT SELECT, INSERT, UPDATE, DELETE ON `customers`.* TO 'web'@'web1'

```
5 rows in set (0.00 sec)

mysql> show grants for web@web1;
```

Grants for web@web2
GRANT ALL PRIVILEGES ON *.* TO 'web'@'web1' IDENTIFIED BY PASSWORD ...
GRANT SELECT, INSERT, UPDATE, DELETE ON `products`.* TO 'web'@'web1'
GRANT SELECT, INSERT, UPDATE, DELETE ON `fortunes`.* TO 'web'@'web1'
GRANT SELECT, INSERT, UPDATE, DELETE ON `orders`.* TO 'web'@'web1'
GRANT SELECT, INSERT, UPDATE, DELETE ON `customers`.* TO 'web'@'web1'

```
5 rows in set (0.00 sec)
```

```
mysql> show grants for web@web1;
```

Grants for web@web3
GRANT ALL PRIVILEGES ON *.* TO 'web'@'web1' IDENTIFIED BY PASSWORD ...
GRANT SELECT, INSERT, UPDATE, DELETE ON `products`.* TO 'web'@'web1'
GRANT SELECT, INSERT, UPDATE, DELETE ON `fortunes`.* TO 'web'@'web1'
GRANT SELECT, INSERT, UPDATE, DELETE ON `orders`.* TO 'web'@'web1'
GRANT SELECT, INSERT, UPDATE, DELETE ON `customers`.* TO 'web'@'web1'

```
5 rows in set (0.00 sec)

mysql> show grants for web;
```

Grants for web@%
GRANT USAGE ON *.* TO 'web'@'%' IDENTIFIED BY PASSWORD ...
GRANT SELECT, INSERT, UPDATE, DELETE ON `products`.* TO 'web'@'web1'
GRANT SELECT, INSERT, UPDATE, DELETE ON `fortunes`.* TO 'web'@'web1'
GRANT SELECT, INSERT, UPDATE, DELETE ON `orders`.* TO 'web'@'web1'
GRANT SELECT, INSERT, UPDATE, DELETE ON `customers`.* TO 'web'@'web1'

```
5 rows in set (0.00 sec)
```

The "web" account should be limited to delete, insert, select and update privileges on the customers, fortunes, orders and products databases. Rather than "`ALL PRIVILEGES on *.*`" for "web" on web1, web2 and web3, the privilege of "`USAGE on *.*`" should be granted, as in the case of web@%. Currently, "web" has full control over all customer information.

Restrict remote access. Wildcards should not be used when specifying the host from which a user account can connect. While this is allows for ease of management, it disables part of the access list function within MySQL by allowing a specified user to connect to the database from any system.

```
mysql> select user,host from mysql.user where host="%" ;
```

User	Host
Web	%

```
1 row in set (0.02 sec)
```

Regardless of the privileges (or lack there of) that an account has been granted, allowing "web" from any host could afford direct access to the database from the Internet, should an attacker find a way to bypass the firewall's security. With the exception of computers with DHCP-leased addresses, hosts must be specified to prevent unauthorized access. In the case of DHCP-leased computers, the host can be a range of IP addresses, but should still be as limiting as possible.

Weak passwords. The passwords for the "root" and "web" accounts (discovered in the source code of the Web application) are too simple.

```
Connection connect("customers","webdb","root","giac");
Connection connect("furtunes","webdb","web","webpass");
```

The password should follow the guidelines set forth in the company's password policy. As well, the root account should be renamed. Ideally, this is designed to thwart any attempts to brute-force the MySQL "root" user's account.

2.3.4 Apache Security

Nessus reported that Apache is using a version of OpenSSL that is vulnerable to timing based attacks (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0078 and http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0131). Since Apache was compiled and installed from source distributions rather than from RPM packages, it is not included in the current patch maintenance using AutoRPM.

Output from Nessus:

```
The remote host is using a version of OpenSSL which is
older than 0.9.6j or 0.9.7b.
This version is vulnerable to a timing based attack which
may allow an attacker to guess the content of fixed data
blocks and may eventually be able to guess the value of the
private RSA key of the server.
An attacker may use this implementation flaw to sniff the
data going to this host and decrypt some parts of it, as
well as impersonate your server and perform man in the
middle attacks.
```

As well, Nessus reported that the Apache server version and component versions were identifiable through the banner that was returned. While this is not a vulnerability, the majority of reconnaissance tools rely on banners received from target Web servers to identify their type and version. Turning off the "ServerSignature" returned to a client can help to hide important information that these tools rely upon. If the tool cannot determine the type and version of the target Web server, it cannot determine whether the target is vulnerable to an attack or not.

Output from Nessus:

```
Warning found on port https (443/tcp)
It seems that your web server tries to hide its version or
name, which is a good thing.
However, using a special crafted request, Nessus was able
to discover it.
Risk factor : None
Solution : Fix your configuration.
```

A manual check (using `/usr/local/apache/bin/httpd -l`) showed unneeded modules installed:
mod_autoindex.c provides automated indexing of directories and discloses information that should be kept unavailable.

mod_status.c provides the server's status if set in httpd.conf. Since the module is not used it should be left out of the build.
mod_userdir.c provides users the ability to serve Web pages out of their home directories if set in httpd.conf (Koconis et al. 28). Since the module is not used, it should be left out of the build.

2.4 Identification of Sensitive Data.

2.4.1 Sensitive Data on the Host

Sensitive data on the systems can be broken in to two categories: system files on each of the systems and customer data the webdb database.

System data. All four systems suffer from the lack of a routine file integrity verification process. This means that data can be added, changed or deleted without anyone knowing. Additionally, the lack of a verification process results in an absence of accountability. In the event that malicious manipulation of the data on a system forces the company to attempt to restore the system's data from tape, the company will not know when the data was modified and cannot be sure that the restored data is safe to use.

Customer data. Customer data is located in four separate databases; all run under one instance of MySQL. Directory permissions are correct and only allow access to the raw data to the user "mysql."

```
# ls -al | awk '{ printf "%10s %-6s %-6s %-10s\n",
$1,$3,$4,$9 }'
drwxr-xr-x mysql  mysql  .
drwxr-xr-x root   root   ..
drwx------ mysql  mysql  customers
drwx------ mysql  mysql  fortunes
drwx------ mysql  mysql  mysql
drwx------ mysql  mysql  orders
drwx------ mysql  mysql  products
```

With the exception of user account passwords for the Web site, customer data is not encrypted in the production database.

```
mysql> select username,passwd from customers.account ;
```

username	Passwd
1luckyman	8e<rest of encrypted password>
3dognight	5c<rest of encrypted password>

...

This means that there is no added layer of protection for sensitive customer data outside of access permissions. Thus, once an attacker is able to gain access to the raw data, there is nothing stopping him/her from viewing it. Below is a proof of concept that shows how one can access sensitive customer data outside of MySQL.

```
# strings /var/lib/mysql/customers/payment.MYD
 1luckyman  visa    <clear text sanitized data>
 ...
```

Another reason for encrypting the data is that anyone who has been granted "select" privileges on the customers.payment table can view credit card information. This includes all customer service representatives, dba's and admins. The way to help protect against customer data theft is to use additional encryption functions within the application that interfaces with the database to encrypt the data before it is written in the database. Applications would use a decryption function (if needed) to display the information to the screen. Even though someone may gain access to the data within the database, encrypting sensitive customer data before it is entered in will slow (if not prevent) an attacker's access to customer data.

2.4.2 Sensitive Data on the Network

The transit of sensitive data across the network falls into two categories: transmission of data across the Internet (such as the transmission of data between customer and Web site), and transmission of data across the intranet (such as the transmission of data between Web application and database). *Internet*. Transmission of sensitive data between the customer and the Web site is protected via encryption. However, Nessus reported that the configuration of the Web server allows browsers to negotiate a weak encryption.
Output from Nessus:

```
This TLSv1 server also accepts SSLv2 connections.
This TLSv1 server also accepts SSLv3 connections.

Here is the list of available SSLv2 ciphers:
RC4-MD5
EXP-RC4-MD5
RC2-CBC-MD5
EXP-RC2-CBC-MD5
DES-CBC-MD5
DES-CBC3-MD5
RC4-64-MD5
```

The two export-grade ciphers are the weakest ones enabled. These are `EXP-RC4-MD5` and `EXP-RC2-CBC-MD5`. Before disabling any of the ciphers, the company must first realize that customers using old browsers or export versions of browsers could be alienated if the ciphers are restricted to just the strongest choices. More information on a possible solution can be found in the mod_ssl online documentation: http://www.modssl.org/docs/2.8/ssl_howto.html#cipher-sgc.

Intranet. Through interviews with the developers, it was discovered that the transmission of sensitive customer data across the intranet is not encrypted.

Encrypting the data before it crosses the intranet will help defend against someone capturing the data through sniffing the network traffic. Since the company created and maintains both the Web application and the customer service application, it is possible to encrypt transmissions to and from the database.

2.5 Security Patch Installation and Management

AutoRPM is used to keep all four systems patched. It is configured to automatically apply any new updates except for those classified as kernel updates. No other patch management process is employed on any of the four servers. Several issues were found regarding the company's patch management process.

2.5.1 Non-RPM packages

The first is the lack of a process to keep non-RPM packages updated. This is a side effect of exclusively using AutoRPM. Applications that were built and installed from source code fall into this category. These applications include Apache, Xalan and Xerces. It should be noted that OpenSSL, mod_ssl, and mm were used to compile Apache, but were not installed. Thus, no other package relies upon these out-of-date components.

2.5.2 RPM Packages

The second issue was found with the use of AutoRPM. As of January 1 2004, RedHat discontinued support for RedHat Linux 8.0 and below (https://www.redhat.com/support/errata/archives/). This means that, as future vulnerabilities are uncovered, GIAC will not be able to patch its systems if the current process remains unmodified. The company should evaluate its different options and move forward toward a process whereby all packages are maintained.

2.5.3 Dependency on Upgrade of Kernel

The final issue was found in the output of AutoRPM. Because the kernel has not been updated, any package with a dependency on the updated kernel cannot be updated. This is the case with IPTables.

```
Package iptables-1.2.8-8.72.3 (Upgrade from 1.2.5-3)
FAILED!
Needs Dependency: kernel >= 2.4.20
1 RPM(s) waiting to be installed/updated/removed
Interactively
```

Manual intervention will be required to patch the kernel. After that, AutoRPM will be able to update IPTables.

2.6 Administrative Practices

2.6.1 System Monitoring

No third-party applications or commercial packages have been utilized to monitor the systems. While systems are monitored through in-house created scripts that run periodically through out the day, monitoring is not centralized. Currently, system resources are monitored through a script that runs every ten minutes. It outputs the information from running /bin/cat against different resources under /proc, compares the results with a set threshold and if any exceeds the threshold, an email is send to the administrators alerting them to the problem. As well, system log messages are monitored through another script that looks for pre-defined "bad" messages. The implementation of this script is very similar to Swatch in concept, however there seems to be less of a focus on security than there is on performance.

2.6.2 Network Monitoring

The state of the network directly affects the production servers. Currently, the company does not have a process in place to monitor the firewall logs. Nor does the company have IDS. Thus, if an attack occurs, there will be no indication that the slowness of the systems is due to an attack.

2.6.3 Change Control

The company does not have an official change control process. It is up to the developers to ensure that changes are tested before they are pushed out into production. Since developers are not allowed to have accounts on production systems, the administrators are responsible for making the changes. Without a formal process, this presents the possibility of a miscommunication between the developer and administrator making the change. Additionally, in the event the change fails to work or creates an issue, back-out procedures for changes are not documented to ensure that additional complications are not created. Should the company expand its size or its product offerings, it would greatly benefit from a structured process through which changes (and their back-out procedures) are documented. As well, the company would benefit from the review process of proposed changes by representatives from the different departments that a formalized change control process provides.

2.6.4 Emergency Response

The administrator group maintains an on-call schedule that is followed religiously. At any given time a primary and secondary contact are required to be available should an emergency arise. Since the Web and database servers were deployed, no problems have arisen requiring immediate attention.

2.6.5 Documented Processes

The administrators run a departmental Web server that hosts all of the documentation that they have created. The documentation is not extensive;

however, the IT department has recently begun formalizing its documentation process.

2.7 Backup and Disaster Recovery

Currently, only the database server, webdb, is backed up regularly. During an interview with the administrators, the topic of backing up the Web servers was brought up. The general consensus is that in the event a Web server needs to be restored, the most efficient way to do so is by rebuilding the system. After consulting the documentation on the administrators' departmental Web server, it seems possible that a single server can be rebuilt in less than a day without losing Web site availability. However, should all three Web servers need restoring, the business would be offline until at least one system is available to run the site. In terms of business continuity, this is not acceptable. The Web servers should be backed up regularly. The company should also have the capability to restore any number of Web servers in a short amount of time to reduce down-time in the event of an emergency.

Amanda (http://www.amanda.org) is used to perform backups on webdb on a weekly cycle. Below is an excerpt taken from /etc/amanda/localhost/amanda.conf.

```
dumpcycle 1 week          # the number of days in the normal\
                            dump cycle
runspercycle 7 days       # the number of amdump runs in\
                            dumpcycle days
tapecycle 9 tapes         # the number of tapes in rotation
```

Tapes are stored on site in a room that is accessible only from the server room. With such a close proximity to the production systems, the company would suffer greatly should a building-wide disaster occur. The company keeps the tapes for at least five years. However, there is no separate tape verification process to ensure that the tapes can be successfully restored. This is usually done in the form of performing a restore on a non-production system. Without a verification process, there is no way of telling if a tape, after having been in the tape room for some time, can be relied upon to perform a restore.

The most notable problem discovered regarding the backup process is the lack of data encryption. Should one of the tapes manage to walk out of the building, there is nothing stopping someone from extracting sensitive data off the tape. To prevent data theft, the data should be encrypted before it is written to tape.

2.8 Access Control

2.8.1 Physical Access

Physical access is well thought out. The company is the only occupant in the building and utilizes 100% of the space. Access is controlled via magnetic

card swipe locks. In addition, access to each protected area in the building (including access to the front door) is separately maintained, providing a granular physical access scheme. With the exception of the company's officers, no employee has access to all protected areas. Access to the server room (and the adjacent tape storage room) is restricted to the IT staff and the company's officers.

Production systems have their own enclosure that remains locked. During an interview with the members of the IT department, it was learned that only the administrators have access to the production enclosure. The company should consider limiting access to the server room to those employees who require access in order to perform their jobs.

2.8.2 Network Access

Internally (in relation to the firewall), network access to production systems is not as strict as it could be. The four systems, which are the focus of this audit, are the only systems on VLAN 100. The only restriction that is in place is the lack of a route between the enterprise and production VLANs. Nothing is in place that can restrict access to certain services on the production servers. Moreover, since the entire company needs to access the Web site, all workstations can access any service running on any production system. The company should consider implementing a more granular level of access, which will limit access to only those services on the production systems that are required.

Externally, Internet users are only allowed to get to http and https on the three Web servers. No access to the database server is afforded.

2.8.3 System Access

System access is fairly strict. As a general rule, only administrators are allowed to have accounts on the production systems. Thus, any changes to the Web site require the participation of an administrator. During the assessment of each system, no developer accounts were found.

2.8.4 Root-level Access

Root access is afforded to the administrators using Sudo, which allows the system's root password to be protected. Outside of a select few within the administrators group, no one in the company knows the current root password. Upon reviewing /etc/sudoers, it became apparent why none of the administrators required the root password.
Output from sudoers table on web1; all systems share identical files.

```
# cat /etc/sudoers

# Root global access
root      ALL=(ALL) NOPASSWD: ALL
```

```
# Machine Aliases
Host_Alias     MYSQLHOSTS=webdb1
Host_Alias     WEBHOSTS=web1,web2,web3
Host_Alias     ALLHOSTS=webdb1,web1,web2,web3

# User Aliases
User_Alias     MYSQLROOT=bsmith,tjohnson,rsimms,vpendly
User_Alias     MYSQL     =rsimms
User_Alias     WEBROOT=bsmith,tjohnson,twilson,fhill

# Sudo Rules
MYSQLROOT MYSQLHOSTS=(root) NOPASSWD: ALL
WEBROOT   WEBHOSTS=(root) NOPASSWD: ALL
MYSQL          MYSQLHOSTS=(mysql) NOPASSWD: ALL
```

Granting access to “all” presents the possibility that a user will use "sudo <shell>." Regardless of one’s intentions, using this bypasses all logging mechanisms and removes any accountability on the system. Replacing “all” with a defined list of files or a directory can help to limit access to only those programs that are required for administering the system.

2.9 Additional Issues

The company lacks an ongoing security evaluation program. Since new vulnerabilities are constantly found, applications that are secure today could be exploitable tomorrow. Possessing a security assessment program, the company can maintain its level of security over time and help the company to take a proactive approach to designing and deploying new product offerings.

3.0 Top Ten Recommendations

The following "top ten" list is designed to help the company prioritize its efforts in addressing the issues documented during this assessment.

3.1 Web Application Security

Risk: High

The Web applications require immediate attention and all available resources should be committed to correcting the documented problems.

3.1.1 Buffer Overflow

Issue

Analysis of the "confucius" cgi application found a buffer overflow condition that can be exploited via the order comments area of the order form on the Web site. The presence of this flaw provides a possible entry point into the network for an attacker.

Solution

A fast remedy would be to replace all occurrences of strcpy() with strncpy(). Strncpy() adds an additional element over strcpy() by allowing the programmer to declare the size of the data that is to be copied into the buffer. Below uses strncpy() and strlen() to correct the code from confucius.cpp.

Note: This is a quick fix to address the improper handling of the input length by strcpy(). This does not address other issues that may exist within the source code. The development team must revisit the entire source code of all CGI applications to make permanent, secure adjustments.

```
char comment[512];
if (getenv("COMMENT") != NULL){
     if (strlen(getenv("COMMENT")) < 512){
          strncpy(comment,getenv("COMMENT"),512);
          [...continue with order...]
     }
     else{
          printf( "Please limit your comments to around 500
     characters\n" );
          [...reload page and have customer try again...]
     }
}
```

Long term, the best way to remedy this is using libraries that provide secure replacement functions designed to validate input. Two examples are Libsafe (http://www.research.avayalabs.com/project/libsafe/) and Safestr

(http://www.zork.org/safestr). Libsafe functions more like a wrapper than a library in that no modification is needed to the source code in order for it to intercept "all calls to library functions that are known to be vulnerable" (http://www.research.avayalabs.com/project/libsafe/doc/libsafe.8.html). Safestr provides "a rich string-handling library for C that has safe semantics yet interoperates with legacy library code in a straightforward manner" (http://www.zork.org/safestr/safestr.html). Both can (and should) be used together without interfering with the system's operation or consuming additional resources. More in-depth explanations and examples for secure programming can be found in "Secure Programming Cookbook for C and C++" by John Viega & Matt Messier.

3.1.2 MySQL Root

Issue

The MySQL root account is used to open a connection with the production database in the "confucius" Web application. This exposes the company to potential theft of customer data should an attacker successfully pass SQL commands via the Web interface.

```
Connection connect("customers","webdb","root","confucius");
```

Solution

Replace all occurrences of "root" with "web" in confucius.cpp before recompiling the application. Use of the root account should only be done so with extreme care. In this case, root is used to connect to the "customers" database, which not only stores usernames and passwords, but also personal preferences like payment information and shipping addresses.

3.1.3 Core Dumps

Issue

The Web applications rely on the system's settings to prevent core dumps. In the event those settings are modified, the two applications will be able to generate dumps.

Solution

By using the setrlimit() function, which is provided by /usr/include/sys/resource.h, to set the core dump size to zero, the application will be prevented from generating a core dump even if the system's settings change (Viega & Messier 35).

3.1.4 Customer Data

Issue

Currently, with the exception of the customer's password, no customer data in the database is encrypted.

Solution

The Web and customer service applications should include an encryption function to encrypt the data before it is entered into the database. There are many options available, but the company should consider using strong encryption when dealing with customer data.

3.2 MySQL Security

Risk: High

The company's existence revolves around the information contained within the production database on webdb. This data should be protected at all costs.

3.2.1 MySQL Root Access

Issue

The root account is allowed to access the database remotely. Root should never be allowed to connect remotely. Because sessions to the database are not encrypted, use of the root account remotely presents the possibility of someone discovering the root password by sniffing the network. While it is a "switched environment" someone with access to either endpoint will have no trouble viewing the data that is transmitted across the network. In addition, the more people who use the root account to troubleshoot problems, the more likely the password will be divulged.

Solution

Root should only be allowed to access the database locally on webdb. The following command should be issued after an alternate (and more restrictive) means of access to the database has been created and any code using root changed.

```
mysql> delete from mysql.user where (user="root" and
host!="localhost" and host!="webdb") ;
mysql> flush privileges ;
```

3.2.2 User Privileges

Issue

The "web" user account is granted all privileges on all databases, allowing this user to perform tasks that should be restricted to the root account. This could have been done unintentionally, as the MySQL manual describes, "if you specify 'ON *' and you don't have a current database, you will affect the global privileges" (MySQL Manual, 246).

Solution

"Web" should only be given (at most) delete, insert, select and update permissions on the customers, fortunes, orders and products databases. The following command will correct the privileges for user "web."

```
mysql> revoke all on *.* from
web@web1,web@web2,web@web3,web@'%' ;
mysql> flush privileges ;
mysql> grant select,insert,update,delete on customers.* to
web@web1,web@web2,web@web3,web@'%';
mysql> grant select,insert,update,delete on fortunes.* to
web@web1,web@web2,web@web3,web@'%';
mysql> grant select,insert,update,delete on products.* to
web@web1,web@web2,web@web3,web@'%';
mysql> grant select,insert,update,delete on orders.* to
web@web1,web@web2,web@web3,web@'%';
mysql> flush privileges ;
```

To help further limit access within MySQL, line 37 in /etc/init.d/mysqld can be modified to add three security-related startup options.

```
/usr/bin/safe_mysqld  --defaults-file=/etc/my.cnf \
--safe-show-database \
--safe-user-create \
--local-infile=0 >/dev/null 2>&1 &
```

- *safe-show-database* "returns only those databases for which the user has some kind of privilege" (MySQL Manual, 222)
- *safe-user-create* prevents users from creating "new users with the GRANT command, if the user doesn't have the INSERT privilege for the mysql.user table" (MySQL Manual, 222)
- *local-infile=0* prevents the loading of data locally from a file using `LOAD DATA LOCAL INFILE` (MySQL Manual, 222).

3.2.3 Limiting Access

Issue

The user "web@%" allows a person on any computer to connect to the MySQL database as web.

Solution

Access lists within MySQL should be utilized to only allow access to those systems (or networks) that have a business requirement for accessing the database. Based on the information provided, limiting the hosts to specific IP addresses is not feasible. However, rather than using a wildcard (%) in place of a host, networks (or hosts where possible) should be specified. For example, to change the current wildcard host to specify just the customer service network (VLAN 120 = 192.168.120.0/24), the following commands should be issued.

```
mysql> UPDATE mysql.user SET
host="192.168.120.0/255.255.255.0" where (user="web" and
host="%") ;
```

```
mysql> UPDATE mysql.db SET
host="192.168.120.0/255.255.255.0" where (user="web" and
host="%") ;
mysql> flush privileges ;
```

Additionally, different user roles should be created within MySQL, rather than just relying upon allowing all employees to connect as "web." Depending on what different groups of employees need, accounts can be created and limited to specific areas. This will help to protect customer information.

3.2.4 Encrypting Transmissions

Issue

Encryption is not used for protecting transmissions to or from the database server across the intranet.

Solution

MySQL now supports OpenSSL. The company should seriously consider upgrading to the current release of MySQL 4.x, which is 4.0.17 (http://www.mysql.com/downloads/mysql-4.0.html). While version 3.23 is still being supported, it is missing some of the default functionality of 4.x. It is possible to utilize OpenSSL to encrypt the transmissions on either version, however employing OpenSSL-encrypted transmissions in version 3.23, will require modifications to some of the tables under the mysql database. See the MySQL manual, p. 258, for more information. Use of OpenSSL encryption in MySQL is recommended above all other options because this would offer support for the customer service application. As an alternative, Stunnel (http://www.stunnel.org), which is already installed on all four of the systems, is capable of providing a wrapper for the communications between the production systems.

3.2.5 Weak Passwords

Issue

The passwords observed in the source code of the Web applications are very weak. The company's password policy should be followed when creating passwords in MySQL as well as system passwords.

Solution

To change the passwords for "root" and "web" run the following commands:

```
mysql> update mysql.user set password=password('<new strong
password>') where user="root" ;
mysql> update mysql.user set password=password('<new strong
password>') where user="web" ;
```

As well, the company should consider renaming the root account to thwart possible brute force attacks against the database, should an attacker find a way to pass SQL commands to the database via the Web applications.

3.3 Patch Management

Risk: High

The current patch management process does not provide updates for all applications installed on the production systems.

3.3.1 Source Distributions

Issue

Applications installed from source distributions are not maintained by the current patch management process.

Solution

Patches will have to be manually applied to out-dated applications and a patch management process will have to be created to facilitate future updates. For now, applications should be updated as shown in the tables below.

Table 3.1 Source Code Distributions for Apache

Application	Installed	Available	Location
Apache	1.3.27	1.3.29	http://www.apache.org
Mm	1.2.1	1.3.0	http://www.ossp.org/pkg/lib/mm/
Mod_ssl	2.8.14	2.8.16	http://www.modssl.org/source/
Openssl	0.9.6g	0.9.6l	http://www.openssl.org/source/

Table 3.2 Source Code Distributions for Xerces and Xalan:

Application	Installed	Available	Location
Xalan-c	1.4.0	1.6.0	http://www.apache.org/dyn/closer.cgi/xml/xalan-c
Xerces-c	2.0.0	2.4.0	http://www.apache.org/dyn/closer.cgi/xml/xerces-c

3.3.2 RPM Distributions

Issue

With RedHat discontinuing support for RedHat Linux 7.3, the current pact management process will no longer be sufficient to keep the systems secure.

Solution

The solution for this problem will ultimately be to upgrade to a currently supported version since core operating systems patches may not be available in the future. As well, the company will need to decide whether to begin to manage it's own updates or to seek out a commercially available update solution. Kurt Seifried wrote a good article addressing this issue. It can be found at

http://seifried.org/security/redhat/20031230-redhat-support.html. In it, he details possible solutions for dealing with the lack of RedHat-supplied patches.

3.4 Apache Security

Risk: High

"The most visible features of a Web application that [potential] intruders will note and immediately seek to exploit are vulnerabilities in the Web server software itself" (Scambray & Shema, 42).

3.4.1 Input Validation

Issue

There is no input validation of user-provided information performed by Apache. While programs can be compiled using secure library functions, it is necessary for the Web server application to also validate input from the Web pages it serves.

Solution

There are many Apache modules available that are designed to increase the security of a Web server. One example is mod_security (http://www.modsecurity.org). The primary function of mod_security is to detect and block harmful content. Since it operates as a part of Apache, rather than being compiled into a cgi program, potentially malicious data is blocked before it even reaches the Web application. The configuration for mod_security, like other Apache modules, is handled through httpd.conf.
An example of a filter that would help to prevent a SQL injection attack from listing all of the user information in the mysql.user table is:
SecFilter "select.*mysql.user" "deny, log,status:404"

In this case mod_security would look for any requests containing "select" and "mysql.user" with wildcard data in between. Upon positively matching the expression, the action taken would be to deny the request, log it and send a 404 (not found) message back to the attacker. Filters are infinitely configurable allowing for very a very granular set of rules. Included with the source code distribution are examples that can be built on in customizing the configuration.

3.4.2 Unneeded Modules

Issue

There are unneeded modules that were enabled by default during the build of Apache.

Solution

Rebuild Apache without the following modules using "`--disable-module=<name>`" when running `./configure`.

Table 3.3 Unneeded Apache Modules

Module Name	Purpose	./configure usage
Mod_autoindex	Automatically provides directory listings.	--disable-module=autoindex
Mod_status	Provides server status information.	--disable-module=status
Mod_userdir	Allows access to Web content in a user's $HOME.	--disable-module=userdir

3.4.3 Server Signature

Issue

Scanning tools are able to enumerate server information such as Apache version and some enabled modules.

Solution

Concealing the server version is possible by limiting the amount of information that the server is allowed to return to a client. Ensure that the server's signature is disabled.

```
ServerSignature Off
```

3.4 Ensuring Data Integrity

Risk: High

Protecting data is the driving force behind any security infrastructure, however when it comes to data integrity verification, it is this very data that is most commonly neglected.

3.5.1 File Integrity

Issue

There is no means of checking files on each system for unauthorized modification.

Solution

The company needs to deploy program into production that routinely checks various properties of files to monitor for modification. The most widely known application designed to ensure data integrity is Tripwire (http://sourceforge.net/projects/tripwire/). However, a nice (and preferred) alternative is AIDE (http://sourceforge.net/projects/aide/). Both work along the same premise of using various hashing techniques to detect file changes. Detailed information on setting up Tripwire can be found in "Linux Security Cookbook" by Barrett, Silverman and Byrnes, while information on AIDE can be found at http://www.cs.tut.fi/~rammer/aide/manual.html.

An example of how to use AIDE to monitor /etc/syslog.conf for changes in owner, group, permissions, size, and MD5 checksum would be the following line in aide.conf:

```
/etc/syslog.conf u+g+p+s+md5
```

By default AIDE is configured to monitor all files. The administrators will need to figure out which files change on a regular basis before specifying which files and directories AIDE should not monitor.

3.5.2 Anti-Virus Software

Issue

No anti-virus software was found on any of the four servers.

Solution

In addition to a file integrity verification program, the company should also deploy anti-virus software in production. Several Open Source and commercial products are available. One example of an Open Source product is Clam Anti-Virus (http://sourceforge.net/projects/clamav/). The simplest implementation of clamav is to cronjob the following line. This will scan all directories under "/" and will only show infected files that are found.

```
/<path>/clamscan --recursive --infected --disable-summary /
```

3.5.3 Verifying Tape Backups

Issue

Tape backups are not routinely tested to ensure that the data they possess will be available should a restore be required.

Solution

Using Amanda, previously recorded tapes can be verified. The "amverify" command will test the integrity of the data on the tape. As well, running "amcheckdb" compares known tapes to the entries in the Amanda database and reports inconsistencies to the screen. "Amcheckdb" can be made into a cronjob, but "amverify" will have to be a manual process because different tapes will have to be tested over time.

3.5.4 Web Server Backups

Issue

There is a lack of a backup process for the Web systems. While the company does have a recovery plan, this plan only takes into account the possibility of one (or possibly even two) of the systems being down.

Solution

Regardless of whether or not all three Web servers are to remain identical in setup and configuration in the future, each system should be baked up routinely to prevent as little down-time to the Web site as possible.

3.6 Securing IP Parameters

Risk: Medium

Because the Web servers are Internet-accessible, they could be the target of a denial of service attack. In the event that this does occur, modifying the settings governing IP behavior would help mitigate the impact on the production Web servers.

The changes below (to harden the network parameters) should be applied to all production servers. These changes should be made through /etc/sysctl.conf.

To enable SYN flood protection for all adapters, add:

```
net.ipv4.tcp_max_syn_backlog = 4096
```

To disable IP source routing for all adapters, add:

```
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.eth0.accept_source_route = 0
net.ipv4.conf.lo.accept_source_route = 0
```

To disable the system's ability to accept ICMP redirects, add:

```
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.eth0.accept_redirects = 0
net.ipv4.conf.lo.accept_redirects = 0
```

To disable the system's ability to send ICMP redirects, add:

```
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.eth0.send_redirects = 0
net.ipv4.conf.lo.send_redirects = 0
```

To disable the systems ability to accept ICMP redirect messages for gateways defined in default gateway list:

```
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.conf.eth0.secure_redirects = 0
net.ipv4.conf.lo.secure_redirects = 0
```

To enable TCP SYN flood protection:

```
net.ipv4.tcp_syncookies = 1
```

To enable the system's ability to ignore ICMP broadcasts:

```
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

To log packets with impossible addresses to kernel log (http://lwn.net/Articles/45386):

```
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1
Net.ipv4.conf.eth0.log_martians = 1
net.ipv4.conf.lo.log_martians = 1
```

3.7 Controlling Network Access

Risk: Medium

Additional protection is needed to ensure that traffic allowed by the firewall and/or switch is limited to just those resources that are intended to be available.

3.7.1 Limiting Access with IPTables

Issue

IPTables is installed, but not configured to protect any of the four servers.

Solution

The access list for incoming traffic should be tightened to allow network access to only those services that are required for business operations. All other incoming traffic should be blocked by changing the default setting for incoming traffic from "accept" to "drop." The company should investigate limiting outgoing connections from the production servers since the majority of connections initiated from these systems are to predefined endpoints. Below is an example of an IPTables initialization script. Comments are included to better explain the process that the script goes through. Additionally, each comment line contains the servers to which the commands are relevant, in parenthesis. It is important to note that IPTables commands are case-sensitive.

```
# Flush all rules
# (web1,web2,web3,webdb)
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD

# FORWARDING RULES
# Disable forwarding rules by default
# (web1,web2,web3,webdb)
iptables -P FORWARD DROP

# OUTGOING RULES
# Allow outgoing traffic by default
# (web1,web2,web3,webdb)
iptables -P OUTPUT ACCEPT

# INCOMING RULES
# Allow loopback interface connections
```

```
# (web1,web2,web3,webdb)
iptables -A INPUT -i lo -j ACCEPT

# Allow established connections
# (web1,web2,web3,webdb)
iptables -A INPUT -i eth0 -m state \
 --state ESTABLISHED,RELATED -j ACCEPT

# Allow SSH from the administrators' workstations
# (web1,web2,web3,webdb)
# Example:
iptables -A INPUT -i eth0 -s 192.168.110.25 \
 -p tcp --dport 22 -j ACCEPT

# Allow MySQL (webdb)
iptables -A INPUT -i eth0 -s 192.168.100.0/24 \
 -p tcp --dport 3306 -j ACCEPT
iptables -A INPUT -i eth0 -s 192.168.110.0/24 \
 -p tcp --dport 3306 -j ACCEPT
iptables -A INPUT -i eth0 -s 192.168.120.0/24 \
 -p tcp --dport 3306 -j ACCEPT
iptables -A INPUT -i eth0 -s 192.168.130.0/24 \
 -p tcp --dport 3306 -j ACCEPT

# Allow HTTP  (web1,web2,web3)
iptables -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT

# Allow HTTPS  (web1,web2,web3)
iptables -A INPUT -i eth0 -p tcp --dport 443 -j ACCEPT

# Log and drop everything else (web1,web2,web3,webdb)
iptables -A INPUT -j LOG
iptables -P INPUT DROP
```

3.7.2 Limiting Access with TCPWrappers

Issue

Tcpwrappers is not utilized to limit access to services defined in /etc/hosts.allow and /etc/hosts.deny.

Solution

Implicitly deny incoming traffic, then explicitly allow specific IP addresses access to specific resources.
In /etc/hosts.deny, add the following line to implicitly deny all traffic.
ALL: ALL

/etc/hosts.allow: The following is an example of lines that explicitly allow specific IP addresses to specific resources.
ALL: 127.0.0.1
sshd: 192.168.110.25, 192.168.110.26

This will allow the company to grant SSH access to only the administrators. Granting access to all services for the loopback address will allow any service, which needs to communicate locally via a network port, to function unencumbered.

Note: Only sshd and those services controlled by xinetd can be specified in the hosts.allow or hosts.deny file.

3.7.3 Limiting Access in OpenSSH

Issue

The sshd daemon is not securely configured.

Solution

Make modifications to the configuration files for both the SSH client and server.

Modify /etc/ssh/ssh_config to reflect the following settings:

```
Protocol 2
```

Modify /etc/ssh/sshd_config to reflect the following settings:

```
Protocol 2
PermitEmptyPasswords no
PermitRootLogin no
StrictModes yes
RhostsAuthentication no
RhostsRSAAuthentication no
IgnoreRhosts yes
LoginGraceTime 300
PasswordAuthentication yes
Banner /etc/issue.net
PrintMotd yes
SyslogFacility AUTH
LogLevel INFO
```

3.8 Unneeded Services

Risk: Medium

Services that are not required to perform a specific business function pose a security risk because they can provide additional information about or even a way into the system.

3.8.1 Disabling Services

Issue

Unneeded services not only provide a potential avenue for compromise, but also give out information about a system, which could aid an attacker.

Solution

Because few of the services, which are enabled by default are needed in the production environment, the following services should be disabled and possibly removed.

To disable all unneeded services on web1, web2 and web3, the following can be incorporated in a script or run from the command line:

```
for svc in xinetd xfs apmd samba nfslock autofs portmap \
netfs lpd kudzu ntpd ; do
  chkconfig $svc off
done
```

To disable all unneeded services on webdb:

```
for svc in xfs apmd nfslock autofs portmap netfs lpd \
kudzu ntpd ; do
  chkconfig $svc off
done
```

3.8.2 Un-daemonizing Services

Issue

Some services, such as Sendmail and NTP, are needed, but do not need to be available remotely.

Solution

The best approach to limiting access to these services, without relying on another application to control access, is to remove the service's ability to run in daemon mode.

To un-damonize Sendmail:
1) modify /etc/sysconfig/sendmail to reflect the following settings:

```
DAEMON=no
QUEUE=15m
```

2) Run: `/etc/init.d/sendmail restart`

To confirm that Sendmail is no longer listening for incoming connections use "`ps -ef | grep sendmail`" to ensure that the service is running and use "`netstat -an | awk '{ print $4 }' | grep "[0-9]:25$`" to ensure that Sendmail is no longer listening on 25/TCP.

To un-daemonize NTP:
Create a script in /etc/cron.hourly named ntp.cron which contains the following lines:

```
#!/bin/bash
ntpd -qg -U ntp &
```

3.9 Centralized Logging and Monitoring

Risk: Medium

The lack of a centralized logging and monitoring process reduces the likelihood that anomalies in the log files will be noticed and investigated in a timely manner.

3.9.1 Syslog

Issue

While the company does employ scripts to separately monitor the logs on each system, these scripts are not geared toward searching for possible signs of security-related messages.

Solution

It is recommended that the company deploy a syslog server that is capable of consolidating the log messages from all production systems, including level 6 syslog messages from both the firewall and switch. By consolidating the logs, it will be much easier to correlate events across multiple platforms. Plus, should a security compromise occur on one production system, the attacker will not have access to the all the logs to hide his/her tracks. The option is available to engineer this solution in-house or to purchase a commercial product, like "LogSmart" from Network Intelligence (http://www.network-intelligence.com/LS/). As long as detecting and alerting security events is designed into the solution, either option would be a great improvement over the current logging infrastructure.

3.9.2 IDS

Issue

The company lacks and intrusion detection system.

Solution

An investment in IDS should be made to provide additional monitoring of events on the production network. This will help to identify attacks that are being launched against the company, in real-time. There are plenty of commercial offerings available, however the best choice for an Open Source IDS is Snort (http://www.snort.org). Snort should be deployed on the network where it can monitor the production network. Its configuration should also be customized to remove alerts that are not relevant to the production environment.

3.10 Password Policy

Risk: Medium
While the company does have a password policy, it has not been implemented in the production environment.

3.10.1Password Age

Issue

Nothing is in place to force a user's password to change after a defined amount of time. The company's password policy states that passwords should have a maximum age of forty-five days and minimum age of seven days.

Solution

The following changes should be made to /etc/login.defs to bring the password age on the production systems into compliance with the policy.

```
PASS_MAX_DAYS   45
PASS_MIN_DAYS   7
PASS_WARN_AGE   7
```

As well, to apply password aging to existing users accounts, the following (example) can be incorporated in a script or run from the command line:

```
for user in bsmith tjohnson rsimms vpendly twilson \
fhill ; do
  passwd -n 7 -x 45 -w 7 $user
done
```

3.10.2 Password Strength

Issue

Nothing is in place to enforce the creation of strong passwords. The company's password policy states that new passwords should have:

- Minimum length of ten characters
- Minimum of five different characters from the last password
- Minimum of one character that is a digit
- Minimum of one upper case character
- Minimum of one special character

Solution

Based on the company's password policy, the following changes need to be made to ensure that passwords are strong:

1) Create the file in which the password history can be stored.

```
cp /dev/null /etc/security/opasswd
chmod 600 /etc/security/opasswd
```

2) Modify /etc/pam.d/system-auth.

- Remove `type=` as it is not needed in this case.

- Add `difok=5` to meet the password policy's requirement of new passwords having at least five different characters than the old password.
- Add `menlen=10` to meet the password policy's requirement of new passwords having at least ten characters.
- Add `dcredit=-1` to meet the password policy's requirement of new passwords having at least one digit. To reference the PAM Module Reference Guide (http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam-6.html#ss6.3), the reason for setting the value to -1 on any of the "credit" strings is because using +<number> gives a user +<number> credits toward meeting the password length. Thus, if dcredit=1 the minlen would have to be set to minlen=11 to ensure that the requirement of ten characters.
- Add `ucredit=-1` to meet the password policy's requirement of new passwords having at least one uppercase letter.
- Add `lcredit=0`. Since lowercase passwords are the "norm" the password policy does not specify that a user must have lowercase letters in the password.
- Add `ocredit=-1` to meet the password policy's requirement of new passwords having at least one special character.
- Add debug. This setting causes any log messages generated by Cracklib to be logged to syslog, which will allow for better log consolidation.

The final result line should look like this:

```
password  required  /lib/security/pam_cracklib.so retry=3
 difok=5 minlen=10 dcredit=-1 ucredit=-1 lcredit=0
 ocredit=-1 debug
```

3.10.3 Password History

Issue

Nothing is in place to prevent users from reusing the same password. The company's password policy states that a password history of four passwords should be maintained to keep users from reusing any of the previous four passwords.

Solution

Modify /etc/pam.d/system-auth and add `remember=4` to meet the password policy's requirement of of a new password not matching the previous four passwords (http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam-6.html#ss6.26).

The line should look like this when done:

```
password  sufficient     /lib/security/pam_unix.so nullok
  use_authtok md5 shadow remember=4
```

3.10.4 Users with Weak Passwords

Issue

Two user accounts were found to have weak passwords: fhill and rsimms

Solution

The users should be notified. As well their user accounts on the production systems should be forced to change the password at next login. The following can be run from the command line or in a script to force users with weak passwords to change their passwords.

Note: To err on the side of caution, the shadow file should be backed up before manipulating it.

This will replace will force a password change for fhill and rsimms.

```
cp /etc/shadow /etc/shadow.bak && for user in fhill rsimms ; do \
old_date=$(grep ^$user /etc/shadow | awk -F: '{ print $3 }') ; \
 sed -e "/$user/s/:$old_date:/:0:/" /etc/shadow > /etc/shadow.tmp ; \
 mv /etc/shadow.tmp /etc/shadow; done
```

3.11 Additional Recommendations

3.11.1 Security Policy Review

The company should review its existing policies and create new ones to ensure that guidelines cover all aspects of security. This will benefit the organization, as a whole, by having the necessary framework in place that will guide the development of new projects. As well, it will help to provide a structured process for responding to security issues. Knowing what to do, or who to contact, in the event of a network emergency can save time and money.

3.11.2 Security Assessment Program

The company should invest in an ongoing security assessment program. This can be facilitated by investing in security training for the current administrative staff and/or by creating a computer security position within the company. The use of the same tools that were used during this audit is highly encouraged. As well, the assessment program should work to establish more security policies that provide guidance on engineering, programming and other projects that could benefit from a structured review process.

3.11.3 Security Awareness Program

Additionally, the company should invest in security awareness for all of its employees. Providing a foundation in security for the different roles within the company will help to save the company a lot of money later on.

3.11.4 Staying Informed

The administrators should subscribe to several mailing lists to stay informed of the latest vulnerabilities. Three very helpful, security-related lists are:

- "BugTraq" (bugtraq-subscribe@securityfocus.com); a moderated list devoted to disclosing and discussing vulnerabilities.
- "Linux Focus" (focus-linux-subscribe@securityfocus.com); a moderated list devoted to Linux security discussions.
- "Incidents" (incidents-subscribe@securityfocus.com); a moderated list devoted to the discussion of security events.

References

Tools Referenced

Aide Project Information. SourceForge.net. 16 Jan. 2004 <http://sourceforge.net/projects/aide/>.

Amanda, The Advanced Maryland Automatic Network Disk Archiver. Amanda.org. 16 Jan. 2004 <http://www.amanda.org>.

Apache Software Foundation, The. Apache.org. 5 Jan. 2004 <http://www.apache.org>.

Avaya Labs Research - Projects: Libsafe. Avaya, Inc. 29 Jan. 2004 <http://www.research.avayalabs.com/project/libsafe/>.

chkrootkit -- locally checks for signs of a rootkit. Chkrootkit.org. 14 Dec. 2003 <http://www.chkrootkit.org>.

Clam Anti-Virus Project Information. SourceForge.net. 16 Jan. 2004 <http://sourceforge.net/projects/clamav/>.

GDB: The GNU Project Debugger. Gnu.org. 16 Jan. 2004 <http://www.gnu.org/software/gdb/gdb.html>.

John the Ripper password cracker. Openwall.com. 28 Dec. 2003 <http://www.openwall.com/john>.

Knoppix-STD. Knoppix-STD.org. 28 Dec. 2003 <http://www.knoppix-std.org/>.

Linux Benchmarks. The Center for Internet Security. 14 Dec. 2003. <http://www.cisecurity.com/bench_linux.html>.

LS series logging appliance. Network Intelligence. 20 Jan. 2004. <http://www.network-intelligence.com/LS/>.

mm: Shared Memory Allocation. Open Source Software Project. 5 Jan. 2004 <http://www.ossp.org/pkg/lib/mm/>.

mod_ssl: The Apache Interface to OpenSSL. modssl.org. 5 Jan. 2004 <http://www.modssl.org>.

ModSecurity - Web Intrusion Detection And Prevention. ModSecurity.org. 16 Jan. 2004 <http://www.modsecurity.org>.

Nessus. Nessus.org. 14 Dec. 2003 <http://www.nessus.org>.

Nmap Free Security Scanner, Tools & Hacking resources. Insecure.Org. 28 Dec. 2003 <http://www.insecure.org>.

OpenSSL: The Open Source toolkit for SSL/TLS. OpenSSL.org. 5 Jan. 2004 <http://www.openssl.org>.

Secure Software: RATS. Secure Software. 29 Dec. 2003 <http://www.securesw.com/rats>.

Snort: The Open Source Network Intrusion Detection System. Snort.org. 20 Jan. 2004 <http://www.snort.org>.

Stunnel.org: Universal SSL Wrapper. Stunnel.org. 10 Jan. 2004 <http://www.stunnel.org>.

Tripwire Project Information. SourceForge.net. 16 Jan. 2004 <http://sourceforge.net/projects/tripwire/>.

Wpoison Project Information. SourceForge.net. 10 Jan. 2004 <http://sourceforge.net/projects/wpoison/>.

Xalan-C++. The Apache XML Project. 5 Jan. 2004 <http://xml.apache.org/xalan-c/index.html>.

Xerces-C++. The Apache XML Project. 5 Jan. 2004 <http://xml.apache.org/xerces-c/index.html>.

Works Cited

Barrett, Daniel J., Richard E. Silverman, and Robert G. Byrnes. Linux Security Cookbook. Sebastopol: O'Reilly, 2003.

CAN-2003-0078 (under review): ssl3_get_record in s3_pkt.c for OpenSSL. Mitre.org. 5 Jan. 2004 <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0078>.

CAN-2003-0131 (under review): unauthorized RSA private key operation. Mitre.org. 5 Jan. 2004 <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0131>.

CAN-2003-0961 (under review): Integer overflow in the do_brk function. Mitre.org. 5 Jan. 2004 <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0961>.

CAN-2003-0984 (under review): Real time clock (RTC) routines. Mitre.org. 5 Jan. 2004 <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0984>.

Engelschall, Ralf S. User Manual: mod_ssl version 2.8. modssl.org. 18 Jan. 2004 <http://www.modssl.org/docs/2.8/ssl_howto.html#cipher-sgc>.

Graff, Mark G., and Kenneth R. van Wyk. Secure Coding Principles and Practices. Sebastopol: O'Reilly, 2003.

Koconis, David, et al. Securing Linux: A Survival Guide for Linux Security. USA: SANS Institute, 2003.

Kuznetsov, Alexey. Documentation: ip-sysctl.txt. 2001. LWN.net. 15 Jan. 2004 <http://lwn.net/Articles/45386/>.

Libsafe ManPage. Avaya, Inc. 29 Dec. 2003 <http://www.research.avayalabs.com/project/libsafe/doc/libsafe.8.html>.

Lehti, Rami. Aide Manual version 0.1. Tampere University of Technology, Finland. 16 Jan. 2004 <http://www.cs.tut.fi/~rammer/aide/manual.html>.

Linux Benchmark, v1.1.0. 29 July 2003. The Center for Internet Security. Online. 14 Dec. 2003 <http://www.cisecurity.com/bench_linux.html>.

Linux Programmer's Manual: Mount(8). 14 Sep 1997. ManPage.

Linux-PAM System Administrators' Guide: 6.26 The Unix Password module. Kernel.org. 16 Jan. 2004 <http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam-6.html#ss6.26>.

Linux-PAM System Administrators' Guide: 6.3 Cracklib pluggable password strength-checker. Kernel.org. 16 Jan. 2004 <http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam-6.html#ss6.3>.

Mourani, Gerhard. Securing and Optimizing Linux: RedHat Edition -A Hands on Guide. 2000. The Linux Documentation Project. 15 Jan. 2004 <http://www.tldp.org/LDP/solrhe/Securing-Optimizing-Linux-RH-Edition-v1.3/>.

MySQL Reference Manual. MySQL.com. 16 Dec. 2003 <http://www.mysql.com/get/Downloads/Manual/manual.pdf/from/pick>.

Pomeranz, Hal. Track 6 – Securing Unix. 5 vols. USA: The SANS Institute, 2003.

redhat.com | End of Life Products. RedHat.com. 5 Jan. 2004. <https://www.redhat.com/support/errata/archives/>.

redhat.com | RedHat Support: Updated 2.4 kernel fixes privilege escalation security vulnerability. RedHat.com. 5 Jan. 2004 <https://rhn.redhat.com/errata/RHSA-2003-392.html>.

redhat.com | RedHat Support: Updated 2.4 kernel fixes vulnerabilities. RedHat.com. 5 Jan. 2004 <https://rhn.redhat.com/errata/RHSA-2003-238.html>.

redhat.com | RedHat Support: Updated kernel resolves security vulnerability. RedHat.com. 5 Jan. 2004 <https://rhn.redhat.com/errata/RHSA-2003-417.html>.

Ristic, Ivan. mod_security: Reference Manual, v1.7.4. 6 Dec. 2003. modsecurity.org 16 Jan. 2004 <http://www.modsecurity.org/documentation/modsecurity-manual-1.7.4.pdf>

Russell, Ryan, and Stace Cunningham. Hack Proofing Your Network: Internet Tradecraft. Rockland: Syngress, 2000.

Scambray, Joel, and Mike Shema. Hacking Exposed: Web Applications. New York: McGraw-Hill, 2002.

Seifried, Kurt. Dealing With The End Of Life Of Red Hat Linux 7.x, 8.0 and 9. Jan. 2004. seifried.org. 31 Dec. 2003 <http://seifried.org/security/redhat/20031230-redhat-support.html>.

Viega, John, and Matt Messier. Safestr: Safe C String Library v1.0.2. Nov. 2003. Zork.org. 29 Dec. 2003 <http://www.zork.org/safestr/>.

Viega, John, and Matt Messier. Secure Programming Cookbook for C and C++. Sebastapol: O'Reilly, 2003.

Appendix A Examples of CIS Scanner Results

Note: To keep from presenting too much information, examples of a web server and the database server have been provided.

Results from CIS Scanner run on webdb

```
*** CIS Ruler Run ***
Starting at time 20031216-19:50:43

Positive: 1.1 System appears to have been patched within the last
month.
Negative: 1.2 sshd_config parameter Protocol is not set.
Negative: 1.2 sshd_config parameter PermitRootLogin is not set.
Negative: 1.2 sshd_config parameter PermitEmptyPasswords is not set.
Negative: 1.2 ssh_config must have 'Protocol 2' underneath Host *.
Positive: 2.1 inetd/xinetd is not listening on any of the miscellaneous
ports checked in this item.
Positive: 2.2 telnet is deactivated.
Positive: 2.3 ftp is deactivated.
Positive: 2.4 rsh, rcp and rlogin are deactivated.
Positive: 2.5 tftp is deactivated.
Positive: 2.6 imap is deactivated.
Positive: 2.7 POP server is deactivated.
Positive: 3.1 Found a good daemon umask of 022 in
/etc/rc.d/init.d/functions.
Negative: 3.2 xinetd is still active.
Negative: 3.3 Mail daemon is still listening on TCP 25.
Positive: 3.4 Graphical login is deactivated.
Negative: 3.5 X Font Server (xfs) script has not been deactivated
Negative: 3.6 apmd not deactivated.
Negative: 3.6 gpm not deactivated.
Positive: 3.7 Windows compatibility servers (samba) have been
deactivated.
Positive: 3.8 NFS Server script nfs is deactivated.
Negative: 3.9 NFS script nfslock not deactivated.
Negative: 3.9 NFS script autofs not deactivated.
Positive: 3.10 NIS Client processes are deactivated.
Positive: 3.11 NIS Server processes are deactivated.
Negative: 3.12 RPC rc-script (portmap) has not been deactivated.
Negative: 3.13 netfs rc script not deactivated.
Negative: 3.14 lpd (line printer daemon) not deactivated.
Positive: 3.15 Web server is deactivated.
Positive: 3.16 SNMP daemon is deactivated.
Positive: 3.17 DNS server is deactivated.
Negative: 3.18 mySQL (SQL) database server not deactivated.
Positive: 3.19 Webmin GUI-based system administration daemon
deactivated.
Positive: 3.20 Squid web cache daemon deactivated.
Negative: 3.21 Kudzu hardware detection program has not been
deactivated.
Negative: 4.1 /proc/sys/net/ipv4/conf/eth0/accept_source_route should
be set to 0.
```

```
Negative: 4.1 /proc/sys/net/ipv4/conf/lo/accept_source_route should be
set to 0.
Negative: 4.1 /proc/sys/net/ipv4/conf/eth0/accept_redirects should be
set to 0.
Negative: 4.1 /proc/sys/net/ipv4/conf/lo/accept_redirects should be set
to 0.
Negative: 4.1 /proc/sys/net/ipv4/conf/eth0/secure_redirects should be
set to 0.
Negative: 4.1 /proc/sys/net/ipv4/conf/lo/secure_redirects should be set
to 0.
Negative: 4.1 /proc/sys/net/ipv4/tcp_max_syn_backlog should be at least
4096 to handle SYN floods.
Negative: 4.2 /proc/sys/net/ipv4/conf/eth0/send_redirects should be set
to 0.
Negative: 4.2 /proc/sys/net/ipv4/conf/lo/send_redirects should be set
to 0.
Positive: 5.1 syslog captures authpriv messages.
Positive: 5.2 FTP server is configured to do full logging.
Positive: 5.3 All logfile permissions and owners match benchmark
recommendations.
Negative: 6.1 /boot is not mounted nodev.
Negative: 6.1 /var is not mounted nodev.
Negative: 6.1 /home is not mounted nodev.
Negative: 6.1 /usr is not mounted nodev.
Negative: 6.2 Removable filesystem /mnt/floppy is not mounted nosuid.
Negative: 6.2 Removable filesystem /mnt/floppy is not mounted nodev.
Negative: 6.2 Removable filesystem /mnt/cdrom is not mounted nosuid.
Negative: 6.2 Removable filesystem /mnt/cdrom is not mounted nodev.
Negative: 6.3 PAM allows users to mount removable media: <floppy>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <cdrom>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <pilot>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <jaz>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <zip>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <ls120>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <camera>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <memstick>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <flash>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <diskonkey>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <rem_ide>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <rio500>.
(/etc/security/console.perms)
Positive: 6.4 password and group files have right permissions and
owners.
Positive: 6.5 all temporary directories have sticky bits set.
```

```
Negative: 7.1 rhosts authentication not deactivated in
/etc/pam.d/rlogin.  *NOTE Does not impact system.  rlogin does not
exist in /etc/securetty.
Negative: 7.1 rhosts authentication not deactivated in /etc/pam.d/rsh.
*NOTE Does not impact system.  rlogin does not exist in /etc/securetty.
Positive: 7.2 /etc/hosts.equiv and root's .rhosts/.shosts files either
don't exist, are zero size or are links to /dev/null.
Positive: 7.3 FTP daemons do not permit system users to use FTP.
Positive: 7.4 X11 Server is blocked from listening on TCP port 6000.
Negative: 7.5 Couldn't open cron.allow
Negative: 7.5 Couldn't open at.allow
Negative: 7.6 The permissions on /etc/crontab are not sufficiently
restrictive.
Negative: 7.7 No Authorized Only message in /etc/motd.
Negative: 7.7 No Authorized Only banner for telnet in file
/etc/xinetd.d/telnet.  *NOTE Does not impact system.  Telnet server
disabled.
Negative: 7.7 No Authorized Only banner for rlogin in file
/etc/xinetd.d/rlogin.  *NOTE Does not impact system.  Rlogin server
disabled.
Negative: 7.7 No Authorized Only banner for rsh in file
/etc/xinetd.d/rsh.        *NOTE Does not impact system.  Rsh server
disabled.
Negative: 7.8 xinetd either requires global 'only-from' statement or
one for each service.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: vc/7.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: vc/8.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: vc/9.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: vc/10.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: vc/11.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: tty7.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: tty8.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: tty9.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: tty10.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: tty11.
Negative: 7.10 GRUB isn't password-protected.
Negative: 7.11 /etc/inittab needs a /sbin/sulogin line for single user
mode.
Positive: 7.12 /etc/exports is empty or doesn't exist, so it doesn't
need to be tuned for privports.
Negative: 8.1 news has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 rpm has a valid shell of /bin/bash.
Positive: 8.2 All users have passwords
Negative: 8.3 User bsmith should have a minimum password life of at
least 7 days.
Negative: 8.3 User bsmith should have a maximum password life of
between 1 and 90 days.
Negative: 8.3 User tjohnson should have a minimum password life of at
least 7 days.
Negative: 8.3 User tjohnson should have a maximum password life of
between 1 and 90 days.
Negative: 8.3 User rsimms should have a minimum password life of at
least 7 days.
Negative: 8.3 User rsimms should have a maximum password life of
between 1 and 90 days.
```

```
Negative: 8.3 User vpendly should have a minimum password life of at
least 7 days.
Negative: 8.3 User vpendly should have a maximum password life of
between 1 and 90 days.
Negative: 8.3 User twilson should have a minimum password life of at
least 7 days.
Negative: 8.3 User twilson should have a maximum password life of
between 1 and 90 days.
Negative: 8.3 User fhill should have a minimum password life of at
least 7 days.
Negative: 8.3 User fhill should have a maximum password life of between
1 and 90 days.
Negative: 8.3 /etc/login.defs value PASS_MAX_DAYS = 99999, but should
not exceed 90.
Negative: 8.3 /etc/login.defs value PASS_MIN_DAYS = 0, but should not
be less than 7.
Negative: 8.3 /etc/login.defs value PASS_MIN_LEN = 5, but should be at
least 6.
Positive: 8.4 There were no +: entries in passwd, shadow or group maps.
Positive: 8.5 Only one UID 0 account AND it is named root.
Positive: 8.6 root's PATH is clean of group/world writable directories
or the current-directory link.
Negative: 8.7 User rsimms has a world-writable homedir!
Negative: 8.7 User rsimms has a group-writable homedir!
Negative: 8.7 User rsimms has a world-executable homedir!
Negative: 8.7 User rsimms has a world-readable homedir!
Negative: 8.8 User rsimms has world/group-writable dot-files (.*) in
his/her home directory.
Positive: 8.9 No user has a .netrc file.
Negative: 8.10 Current umask setting in file /etc/profile is 023 -- it
should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/profile is 023 -- it
should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/csh.login is 000 --
it should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/csh.login is 000 --
it should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/bashrc is 022 -- it
should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/bashrc is 022 -- it
should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/csh.cshrc is 002 --
it should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/csh.cshrc is 002 --
it should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.bash_profile is 000
-- it should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.bash_profile is 000
-- it should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.bashrc is 000 -- it
should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.bashrc is 000 -- it
should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.cshrc is 000 -- it
should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.cshrc is 000 -- it
should be stronger to block group-read/write/execute.
```

```
Negative: 8.10 Current umask setting in file /root/.tcshrc is 000 -- it
should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.tcshrc is 000 -- it
should be stronger to block group-read/write/execute.
Negative: 8.11 Coredumps aren't deactivated.
Preliminary rating given at time: Tue Dec 16 19:50:44 2003

      Preliminary rating = 5.08 / 10.00

Positive: 6.7 No non-standard SUID/SGID programs found.
Ending run at time: Tue Dec 16 19:50:47 2003

      Final rating = 5.24 / 10.00
```

Output from CIS Scanner on web1

```
*** CIS Ruler Run ***
Starting at time 20031216-19:41:02

Positive: 1.1 System appears to have been patched within the last
month.
Negative: 1.2 sshd_config parameter Protocol is not set.
Negative: 1.2 sshd_config parameter PermitRootLogin is not set.
Negative: 1.2 sshd_config parameter PermitEmptyPasswords is not set.
Negative: 1.2 ssh_config must have 'Protocol 2' underneath Host *.
Positive: 2.1 inetd/xinetd is not listening on any of the miscellaneous
ports checked in this item.
Positive: 2.2 telnet is deactivated.
Positive: 2.3 ftp is deactivated.
Positive: 2.4 rsh, rcp and rlogin are deactivated.
Positive: 2.5 tftp is deactivated.
Positive: 2.6 imap is deactivated.
Positive: 2.7 POP server is deactivated.
Positive: 3.1 Found a good daemon umask of 022 in
/etc/rc.d/init.d/functions.
Negative: 3.2 xinetd is still active.
Negative: 3.3 Mail daemon is still listening on TCP 25.
Positive: 3.4 Graphical login is deactivated.
Negative: 3.5 X Font Server (xfs) script has not been deactivated
Negative: 3.6 apmd not deactivated.
Negative: 3.6 gpm not deactivated.
Negative: 3.7 samba smb rc script has not been deactivated.
Positive: 3.8 NFS Server script nfs is deactivated.
Negative: 3.9 NFS script nfslock not deactivated.
Negative: 3.9 NFS script autofs not deactivated.
Positive: 3.10 NIS Client processes are deactivated.
Positive: 3.11 NIS Server processes are deactivated.
Negative: 3.12 RPC rc-script (portmap) has not been deactivated.
Negative: 3.13 netfs rc script not deactivated.
Negative: 3.14 lpd (line printer daemon) not deactivated.
Negative: 3.15 Apache web server rc-script not deactivated.
Negative: 3.15 Web server not deactivated.
Positive: 3.16 SNMP daemon is deactivated.
Positive: 3.17 DNS server is deactivated.
```

```
Positive: 3.18 SQL database server is deactivated.
Positive: 3.19 Webmin GUI-based system administration daemon
deactivated.
Positive: 3.20 Squid web cache daemon deactivated.
Negative: 3.21 Kudzu hardware detection program has not been
deactivated.
Negative: 4.1 /proc/sys/net/ipv4/conf/eth0/accept_source_route should
be set to 0.
Negative: 4.1 /proc/sys/net/ipv4/conf/lo/accept_source_route should be
set to 0.
Negative: 4.1 /proc/sys/net/ipv4/conf/eth0/accept_redirects should be
set to 0.
Negative: 4.1 /proc/sys/net/ipv4/conf/lo/accept_redirects should be set
to 0.
Negative: 4.1 /proc/sys/net/ipv4/conf/eth0/secure_redirects should be
set to 0.
Negative: 4.1 /proc/sys/net/ipv4/conf/lo/secure_redirects should be set
to 0.
Negative: 4.1 /proc/sys/net/ipv4/tcp_max_syn_backlog should be at least
4096 to handle SYN floods.
Negative: 4.2 /proc/sys/net/ipv4/conf/eth0/send_redirects should be set
to 0.
Negative: 4.2 /proc/sys/net/ipv4/conf/lo/send_redirects should be set
to 0.
Positive: 5.1 syslog captures authpriv messages.
Positive: 5.2 FTP server is configured to do full logging.
Positive: 5.3 All logfile permissions and owners match benchmark
recommendations.
Negative: 6.1 /boot is not mounted nodev.
Negative: 6.1 /var is not mounted nodev.
Negative: 6.1 /home is not mounted nodev.
Negative: 6.1 /usr is not mounted nodev.
Negative: 6.2 Removable filesystem /mnt/floppy is not mounted nosuid.
Negative: 6.2 Removable filesystem /mnt/floppy is not mounted nodev.
Negative: 6.2 Removable filesystem /mnt/cdrom is not mounted nosuid.
Negative: 6.2 Removable filesystem /mnt/cdrom is not mounted nodev.
Negative: 6.3 PAM allows users to mount removable media: <floppy>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <cdrom>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <pilot>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <jaz>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <zip>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <ls120>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <camera>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <memstick>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <flash>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <diskonkey>.
(/etc/security/console.perms)
```

```
Negative: 6.3 PAM allows users to mount removable media: <rem_ide>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <rio500>.
(/etc/security/console.perms)
Positive: 6.4 password and group files have right permissions and
owners.
Positive: 6.5 all temporary directories have sticky bits set.
Negative: 7.1 rhosts authentication not deactivated in
/etc/pam.d/rlogin.  *NOTE Does not impact system.  rlogin does not
exist in /etc/securetty.
Negative: 7.1 rhosts authentication not deactivated in /etc/pam.d/rsh.
*NOTE Does not impact system.  rlogin does not exist in /etc/securetty.
Positive: 7.2 /etc/hosts.equiv and root's .rhosts/.shosts files either
don't exist, are zero size or are links to /dev/null.
Positive: 7.3 FTP daemons do not permit system users to use FTP.
Positive: 7.4 X11 Server is blocked from listening on TCP port 6000.
Negative: 7.5 Couldn't open cron.allow
Negative: 7.5 Couldn't open at.allow
Negative: 7.6 The permissions on /etc/crontab are not sufficiently
restrictive.
Negative: 7.7 No Authorized Only message in /etc/motd.
Negative: 7.7 No Authorized Only banner for telnet in file
/etc/xinetd.d/telnet.  *NOTE Does not impact system.  Telnet server
disabled.
Negative: 7.7 No Authorized Only banner for rlogin in file
/etc/xinetd.d/rlogin.  *NOTE Does not impact system.  Rlogin server
disabled.
Negative: 7.7 No Authorized Only banner for rsh in file
/etc/xinetd.d/rsh.        *NOTE Does not impact system.  Rsh server
disabled.
Negative: 7.8 xinetd either requires global 'only-from' statement or
one for each service.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: vc/7.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: vc/8.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: vc/9.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: vc/10.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: vc/11.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: tty7.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: tty8.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: tty9.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: tty10.
Negative: 7.9 /etc/securetty has a non console or tty 1-6 line: tty11.
Negative: 7.10 GRUB isn't password-protected.
Negative: 7.11 /etc/inittab needs a /sbin/sulogin line for single user
mode.
Positive: 7.12 NFS server restricts clients to privileged ports.
Negative: 8.1 news has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 rpm has a valid shell of /bin/bash.
Positive: 8.2 All users have passwords
Negative: 8.3 User bsmith should have a minimum password life of at
least 7 days.
Negative: 8.3 User bsmith should have a maximum password life of
between 1 and 90 days.
Negative: 8.3 User tjohnson should have a minimum password life of at
least 7 days.
```

```
Negative: 8.3 User tjohnson should have a maximum password life of
between 1 and 90 days.
Negative: 8.3 User rsimms should have a minimum password life of at
least 7 days.
Negative: 8.3 User rsimms should have a maximum password life of
between 1 and 90 days.
Negative: 8.3 User vpendly should have a minimum password life of at
least 7 days.
Negative: 8.3 User vpendly should have a maximum password life of
between 1 and 90 days.
Negative: 8.3 User twilson should have a minimum password life of at
least 7 days.
Negative: 8.3 User twilson should have a maximum password life of
between 1 and 90 days.
Negative: 8.3 User fhill should have a minimum password life of at
least 7 days.
Negative: 8.3 User fhill should have a maximum password life of between
1 and 90 days.
Negative: 8.3 /etc/login.defs value PASS_MAX_DAYS = 99999, but should
not exceed 90.
Negative: 8.3 /etc/login.defs value PASS_MIN_DAYS = 0, but should not
be less than 7.
Negative: 8.3 /etc/login.defs value PASS_MIN_LEN = 5, but should be at
least 6.
Positive: 8.4 There were no +: entries in passwd, shadow or group maps.
Positive: 8.5 Only one UID 0 account AND it is named root.
Positive: 8.6 root's PATH is clean of group/world writable directories
or the current-directory link.
Negative: 8.7 User rsimms has a world-writable homedir!
Negative: 8.7 User rsimms has a group-writable homedir!
Negative: 8.7 User rsimms has a world-executable homedir!
Negative: 8.7 User rsimms has a world-readable homedir!
Negative: 8.8 User rsimms has world/group-writable dot-files (.*) in
his/her home directory.
Positive: 8.9 No user has a .netrc file.
Negative: 8.10 Current umask setting in file /etc/profile is 023 -- it
should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/profile is 023 -- it
should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/csh.login is 000 --
it should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/csh.login is 000 --
it should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/bashrc is 022 -- it
should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/bashrc is 022 -- it
should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/csh.cshrc is 002 --
it should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/csh.cshrc is 002 --
it should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.bash_profile is 000
-- it should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.bash_profile is 000
-- it should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.bashrc is 000 -- it
should be stronger to block world-read/write/execute.
```

```
Negative: 8.10 Current umask setting in file /root/.bashrc is 000 -- it
should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.cshrc is 000 -- it
should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.cshrc is 000 -- it
should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.tcshrc is 000 -- it
should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.tcshrc is 000 -- it
should be stronger to block group-read/write/execute.
Negative: 8.11 Coredumps aren't deactivated.
Preliminary rating given at time: Tue Dec 16 19:41:06 2003

      Preliminary rating = 4.92 / 10.00

Positive: 6.7 No non-standard SUID/SGID programs found.
Ending run at time: Tue Dec 16 19:41:09 2003

      Final rating = 5.08 / 10.00
```

Appendix B Nessus Scanner Results

Note: Because the results are identical for the web servers, an example report has been provided to keep the Appendix short.

Nessus Report of web2.giacfortunes.com

```
+ web2.giacfortunes.com :
 . List of open ports :
   o ssh (22/tcp) (Security warnings found)
   o www (80/tcp) (Security warnings found)
   o sunrpc (111/tcp) (Security notes found)
   o https (443/tcp) (Security warnings found)
   o netbios-ssn (139/tcp) (Security hole found)
   o unknown (32768/tcp) (Security notes found)
   o general/tcp (Security notes found)
   o general/icmp (Security warnings found)
   o sunrpc (111/udp) (Security notes found)
   o unknown (32768/udp) (Security warnings found)

 . 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)

    An ssh server is running on this port

 . 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

 . Warning found on port www (80/tcp)

    It seems that your web server tries to hide its version or name,
    which is a good thing.
    However, using a special crafted request, Nessus was able to
    discover it.
```

```
   Risk factor : None

   Solution : Fix your configuration.

. Warning found on port www (80/tcp)

   The remote host is using a version of OpenSSL which is older than
   0.9.6j or 0.9.7b

   This version is vulnerable to a timing based attack which may allow
   an attacker to guess the content of fixed data blocks and may
   eventually be able to guess the value of the private RSA key of the
   server.

   An attacker may use this implementation flaw to sniff the data
   going to this host and decrypt some parts of it, as well as
   impersonate your server and perform man in the middle attacks.

   *** Nessus solely relied on the banner of the remote host
   *** to issue this warning

   See also : http://www.openssl.org/news/secadv_20030219.txt
       http://lasecwww.epfl.ch/memo_ssl.shtml
       http://eprint.iacr.org/2003/052/

   Solution : Upgrade to version 0.9.6j (0.9.7b) or newer
   Risk factor : Medium
   CVE : CAN-2003-0078, CAN-2003-0131
   BID : 6884

. Information found on port www (80/tcp)

   A web server is running on this port

. Information found on port sunrpc (111/tcp)

   The RPC portmapper is running on this port.

   An attacker may use it to enumerate your list of RPC services. We
   recommand you filter traffic going to this port.

   Risk factor : Low
   CVE : CAN-1999-0632, CVE-1999-0189
   BID : 205

. Information found on port sunrpc (111/tcp)

   RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind)
   is running on this port

. Warning found on port https (443/tcp)

   The SSLv2 server offers 5 strong ciphers, but also 0 medium
   strength and 2 weak "export class" ciphers.  The weak/medium
   ciphers may be chosen by an export-grade or badly configured client
   software. They only offer a limited protection against a brute
```

```
   force attack.
   Solution: disable those ciphers and upgrade your client software if
   necessary

. Warning found on port https (443/tcp)

   It seems that your web server tries to hide its version or name,
   which is a good thing.  However, using a special crafted request,
   Nessus was able to discover it.

   Risk factor : None

   Solution : Fix your configuration.

. Warning found on port https (443/tcp)

   The remote host is using a version of OpenSSL which is older than
   0.9.6j or 0.9.7b

   This version is vulnerable to a timing based attack which may allow
   an attacker to guess the content of fixed data blocks and may
   eventually be able to guess the value of the private RSA key of the
   server.

   An attacker may use this implementation flaw to sniff the data
   going to this host and decrypt some parts of it, as well as
   impersonate your server and perform man in the middle attacks.

   *** Nessus solely relied on the banner of the remote host
   *** to issue this warning

   See also : http://www.openssl.org/news/secadv_20030219.txt
       http://lasecwww.epfl.ch/memo_ssl.shtml
       http://eprint.iacr.org/2003/052/

   Solution : Upgrade to version 0.9.6j (0.9.7b) or newer
   Risk factor : Medium
   CVE : CAN-2003-0078, CAN-2003-0131
   BID : 6884

. Information found on port https (443/tcp)

   A TLSv1 server answered on this port

. Information found on port https (443/tcp)

   A web server is running on this port through SSL

. Information found on port https (443/tcp)

   Here is the SSLv2 server certificate:
   Certificate:
       Data:
           ...
           Signat ure Algorithm: md5WithRSAEncryption
           ...
```

```
. Information found on port https (443/tcp)

   Here is the list of available SSLv2 ciphers:
   RC4-MD5
   EXP-RC4-MD5
   RC2-CBC-MD5
   EXP-RC2-CBC-MD5
   DES-CBC-MD5
   DES-CBC3-MD5
   RC4-64-MD5


. Information found on port https (443/tcp)

   This TLSv1 server also accepts SSLv2 connections.
   This TLSv1 server also accepts SSLv3 connections.

. Vulnerability found on port netbios-ssn (139/tcp) :

   . It was possible to log into the remote host using a NULL session.
     The concept of a NULL session is to provide a null username and a
     null password, which grants the user the 'guest' access

     To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and
     Q246261 (Windows 2000).
     Note that this won't completely disable null sessions, but will
     prevent them from connecting to IPC$
     Please see
     http://msgs.securepoint.com/cgi-bin/get/nessus-0204/50/1.html

   . All the smb tests will be done as ''/'whatever' in domain MGOP
     CVE : CAN-1999-0504, CAN-1999-0506, CVE-2000-0222
     BID : 990

. Vulnerability found on port netbios-ssn (139/tcp) :

   The following shares can be accessed using a NULL session  :

   - IPC$  - (readable?, writeable?)

   Solution : To restrict their access under WindowsNT, open the
   explorer, do a right click on each, go to the 'sharing' tab, and
   click on 'permissions'
   Risk factor : High
   CVE : CAN-1999-0519, CAN-1999-0520

. Warning found on port netbios-ssn (139/tcp)

   Here is the browse list of the remote host :

   WEB2 -

   This is potentially dangerous as this may help the attack of a
   potential hacker by giving him extra targets to check for

   Solution : filter incoming traffic to this port
   Risk factor : Low
```

```
. Warning found on port netbios-ssn (139/tcp)

   Here is the list of the SMB shares of this host :

   IPC$ -
   ADMIN$ -

   This is potentially dangerous as this may help the attack of a
   potential hacker.

   Solution : filter incoming traffic to this port
   Risk factor : Medium

. Information found on port netbios-ssn (139/tcp)

   The remote native lan manager is : Samba 2.2.7-security-rollup-fix
   The remote Operating System is : Unix
   The remote SMB Domain Name is : WEBSERVERS

. Information found on port unknown (32768/tcp)

   RPC program #100024 version 1 'status' is running on this port


. Information found on port general/tcp

   HTTP NIDS evasion functions are enabled.
   You may get some false negative results

. Information found on port general/tcp

   Remote OS guess : Linux Kernel 2.4.0 - 2.5.20
   CVE : CAN-1999-0454

. Warning found on port netbios-ns (137/udp)

   . The following 7 NetBIOS names have been gathered :
     WEB2         = This is the computer name registered for
                    workstation services by a WINS client.
     WEB2         = Computer name that is registered for the messenger
                    service on a computer that is a WINS client.
     WEB2
     __MSBROWSE__
     WEBSERVERS   = Workgroup / Domain name
     WEBSERVERS
     WEBSERVERS   = Workgroup / Domain name (part of the Browser
                    elections)

   . This SMB server seems to be a SAMBA server (this is not a
     security risk, this is for your information). This can be told
     because this server claims to have a null MAC address

     If you do not want to allow everyone to find the NetBios name of
     your computer, you should filter incoming traffic to this port.

     Risk factor : Medium
```

```
      CVE : CAN-1999-0621

. 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

. Information found on port sunrpc (111/udp)

   RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind)
   is running on this port

. 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 HOLES REGARDING THIS
     PROGRAM HAVE BEEN TESTED, SO
     THIS MIGHT BE A FALSE POSITIVE *

   We suggest that you disable this service.

   Risk factor : High
   CVE : CVE-1999-0018, CVE-1999-0019, CVE-1999-0493
   BID : 127, 450

. Information found on port unknown (32768/udp)

   RPC program #100024 version 1 'status' is running on this port

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

Appendix C Examples of Nmap Scanner Results

Example of TCP connect(), Ident and RPC scan on ports 1-65535.

```
# nmap -sT -sR -p 1-65535 -O -I web2.giacfortunes.com
Interesting ports on web2.giacfortunes.com:
(The 65532 ports scanned but not shown below are in state: closed)
Port       State       Service (RPC)           Owner
22/tcp     open        ssh
80/tcp     open        http
111/tcp    open        sunrpc  (rpcbind V2)
139/tcp    open        netbios-ssn
443/tcp    open        https
32768/tcp  open                (status V1)
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20
Uptime 3.889 days (since Mon Dec 15 14:55:01 2003)
TCP Sequence Prediction: Class=random positive increments
Difficulty=1724346 (Good luck!)
IPID Sequence Generation: All zeros

Nmap run completed -- 1 IP address (1 host up) scanned in 15.442
seconds
```

Example of TCP SYN scan on ports 1-65535.

```
# nmap -sS -p 1-65535 -O web1.giacfortunes.com
Interesting ports on web1.giacfortunes.com:
(The 65532 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
139/tcp    open        netbios-ssn
443/tcp    open        https
32768/tcp  open        unknown
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20
Uptime 19.211 days (since Thu Nov 27 10:54:21 2003)
TCP Sequence Prediction: Class=random positive increments
Difficulty=1724346 (Good luck!)
IPID Sequence Generation: All zeros

Nmap run completed -- 1 IP address (1 host up) scanned in 12.542
seconds
```

Example of UDP scan on ports 1-65535.

```
# nmap -sU –sR -p 1-65535 webdb.giacfortunes.com
Interesting ports on webdb.giacfortunes.com:
(The 65532 ports scanned but not shown below are in state: closed)
Port       State       Service (RPC)
123/udp    open        ntp
10080/udp  open        Amanda
32768/udp  open                (status V1)
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 474.021
seconds
```

Appendix D Example of Chkrootkit Results

```
# uname -n
webdb.giacfortunes.com
# ./chkrootkit
ROOTDIR is `/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not infected
Checking `chsh'... not infected
Checking `cron'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
Checking `fingerd'... not infected
Checking `gpm'... not infected
Checking `grep'... not infected
Checking `hdparm'... not infected
Checking `su'... not infected
Checking `ifconfig'... not infected
Checking `inetd'... not tested
Checking `inetdconf'... not found
Checking `identd'... not infected
Checking `init'... not infected
Checking `killall'... not infected
Checking `ldsopreload'... can't exec ./strings-static, not tested
Checking `login'... not infected
Checking `ls'... not infected
Checking `lsof'... not infected
Checking `mail'... not infected
Checking `mingetty'... not infected
Checking `netstat'... not infected
Checking `named'... not found
Checking `passwd'... not infected
Checking `pidof'... not infected
Checking `pop2'... not found
Checking `pop3'... not found
Checking `ps'... not infected
Checking `pstree'... not infected
Checking `rpcinfo'... not infected
Checking `rlogind'... not infected
Checking `rshd'... not infected
Checking `slogin'... not infected
Checking `sendmail'... not infected
Checking `sshd'... not infected
Checking `syslogd'... not infected
Checking `tar'... not infected
Checking `tcpd'... not infected
Checking `tcpdump'... not infected
```

```
Checking `top'... not infected
Checking `telnetd'... not infected
Checking `timed'... not found
Checking `traceroute'... not infected
Checking `vdir'... not infected
Checking `w'... not infected
Checking `write'... not infected
Checking `aliens'... no suspect files
Searching for sniffer's logs, it may take a while... nothing found
Searching for HiDrootkit's default dir... nothing found
Searching for t0rn's default files and dirs... nothing found
Searching for t0rn's v8 defaults... nothing found
Searching for Lion Worm default files and dirs... nothing found
Searching for RSHA's default files and dir... nothing found
Searching for RH-Sharpe's default files... nothing found
Searching for Ambient's rootkit (ark) default files and dirs... nothing
found
Searching for suspicious files and dirs, it may take a while...
/usr/lib/perl5/5.6.1/i386-linux/.packlist

Searching for LPD Worm files and dirs... nothing found
Searching for Ramen Worm files and dirs... nothing found
Searching for Maniac files and dirs... nothing found
Searching for RK17 files and dirs... nothing found
Searching for Ducoci rootkit... nothing found
Searching for Adore Worm... nothing found
Searching for ShitC Worm... nothing found
Searching for Omega Worm... nothing found
Searching for Sadmind/IIS Worm... nothing found
Searching for MonKit... nothing found
Searching for Showtee... nothing found
Searching for OpticKit... nothing found
Searching for T.R.K... nothing found
Searching for Mithra... nothing found
Searching for OBSD rk v1... nothing found
Searching for LOC rootkit ... nothing found
Searching for Romanian rootkit ... nothing found
Searching for HKRK rootkit ... nothing found
Searching for Suckit rootkit ... nothing found
Searching for Volc rootkit ... nothing found
Searching for Gold2 rootkit ... nothing found
Searching for TC2 Worm default files and dirs... nothing found
Searching for Anonoying rootkit default files and dirs... nothing found
Searching for ZK rootkit default files and dirs... nothing found
Searching for ShKit rootkit default files and dirs... nothing found
Searching for anomalies in shell history files... nothing found
Checking `asp'... not infected
Checking `bindshell'... not infected
Checking `lkm'... Checking `rexedcs'... not found
Checking `sniffer'... Checking `w55808'... not infected
Checking `wted'... not tested: can't exec ./chkwtmp
Checking `scalper'... not infected
Checking `slapper'... not infected
Checking `z2'... not tested: can't exec ./chklastlog
```