Global Information Assurance Certification Paper

SANS Unix Security Audit

Client XYZ

Conducted by: Jennifer Redding

January 12, 2001

Table of Contents

Executive Summary

We audited a backup server running RedHat Linux 6.2 for a small IT consulting firm. We ran the audit using a Unix Security Checklist to analyze the server in the areas of Operating System security, risks from third-party software, administrative practices, protecting sensitive data with encryption, protection against programmed threats, account security, file systems security, network security, backup/restore strategy, disaster recovery strategy, and physical security.

To conduct the analysis we used various security auditing tools and Unix scripts. We used Tiger and Nessus to inspect the system for basic security vulnerabilities. We conducted a port scan using nmap. We used PortSentry to detect port scans. Then we attempted to crack passwords using Crack. We used Tripwire to capture the initial system configuration and detect unauthorized changes.

We found several vulnerabilities in the server. Several known vulnerabilities exist in the operating system which can be fixed with the latest patches. We found vulnerabilities in Client XYZ's administrative practices, password policy, and security auditing practices. We discovered a list of Setuid programs with a known security vulnerability that could allow an attacker to gain root access. Client XYZ has never conducted a backup on this box and has no disaster recovery site to use in the event of data loss. In addition, there is very little protection from fire.

We made a number of recommendations to improve the security of the Linux box. We provide a reference for a list of patches Client XYZ should install to fix known vulnerabilities. We installed and ran tools that should be used as part of a regular security audit. Client XYZ should document and enforce a password policy and set up a welcome message to warn intruders. We recommend Client XYZ develops and implements the appropriate backup strategy and disaster recovery plan to protect data in the event of a loss. Client XYZ should purchase a fire extinguisher and train their personnel to use the extinguisher in the event of a fire. To ensure Client XYZ's environment is physically secure, a burglar alarm should be installed to discourage intruders.

Introduction

Client XYZ and Environment

Client XYZ is a small IT consulting firm in Bethesda, Maryland, made up of 5 software developers. Client XYZ asked us to audit their backup file server that is used by two Client XYZ partners. The critical data on the box is the company's financial data. The box sits behind a Cisco CSU/DSU router with packet filtering.

The operating system is Red Had Linux 6.2 on a Pentium (i386 architecture) 233 with 32mb of RAM, 60GB IDE drive, 1 Linksys 10/100 ethernet card, Diamond Stealth 64 4MB VRAM, CDROM, floppy.

Methodology

We created a Unix Security Checklist to audit the following areas:

- System Configuration
- Risks From Third-party software
- Administrative Practices
- Protecting Sensitive Data and Encryption
- Protecting Against Programmed Threats
- Account Security
- Files System Security
- Network Security
- Backup/Recovery
- Disaster Recovery
- Physical Security

This checklist was created from recommendations in the Accenture Unix Security Checklist and Practical Unix and Internet Security.

Tools

Tiger was used to locate potential problems in the system configuration. We used tiger-2.2.4p1.tar.gz. from http://net.tamu.edu/network/tools/tiger.html .

Nessus was used to locate vulnerabilities. We downloaded version 1.0.6 from http://www.nessus.org/download.html.

We ran a network scan using **nmap**. Nmap scans hosts looking for open ports. We used version 2.53 from http://www.insecure.org/nmap/dist/nmap-2.53.tgz.

We used **PortSentry** to detect port scans. PortSentry is a program designed to detect and respond to port scans against a target host in real-time. The software is available at http://www.psionic.com/abacus/portsentry/.

Tripwire was used to detect unauthorized and unexpected changes to files. We used version 1.2 from ftp://coast.cs.purdue.edu/pub/tools/unix/Tripwire/tripwire-1.2.tar.Z.

Crack was used to detect weak passwords. Crack is a password guessing program that is designed to quickly locate insecurities in password files by scanning the contents of a password file, looking for users who have chosen a weak login password. Crack can be downloaded from http://www.securityfocus.com/data/tools/crackers/crack5.0.tar.gz.

Analysis

Operating system

The Operating System is RedHat Linux 6.2. No patches have been installed since the initial installation.

System Configuration

- PATH environment variable includes only trusted, secure paths
- No welcome message in /etc/motd
- UMASK set to 002.

Administrative practices

- No system auditing tools running
- Syslogs, wtmp, and security tool logs are checked once a month
- Logs from other machines are transferred to this machine. Since this box is not a critical server, logs are not transferred to another box
- Logs are rotated daily and weekly. Syslogs are rotated daily and purged after 7 days.
- Does not periodically run security auditing tools to check for security violations
- Does not automate log scanning with Swatch
- Does not automatically alarm the system administrator for CRIT, ALERT or EMERG level log messages
- No hardcoding of passwords in any files including scripts
- Reports all security violations to the network administrator

- Conducts a complete security review of the system every 3 months by running port scanning tools and examining logs.
- Does not install vendor supplied patches
- Gets proper approval before changing "required" security provisions
- Does not log all new system files and changes to configurations or file permissions
- Tests the effect of all changes on system performance and security. No performance monitoring, but if the system is running slow, knows there is a problem. Scans box after installing software.

Third Party Software

The following software is installed on the server:

- ISC DHCPD
- SMBD
- Open SSH 2.1.1
- X11 R6 Version 4
- Netscape Navigator 4.75
- Lynx

Sensitive Data and Encryption

- Does not use ROT13 as an encryption method to protect data. In the ROT13 cipher, each letter of the alphabet is replaced with a letter that is 13 letters ahead. For example, A would be replaced with N, B with O, etc… There is no key and anyone can decrypt the cipher text.
- Uses MD5 based crypt in shadow password file
- Does not use the compress command (or similar compression system) on files before encrypting them
- Never uses a login password as an encryption password
- Protects encryption key - does not write it down, put it in a shell file or store online
- Not running FIPS 140-1 on this box. Uses SSL on this box.
- Avoids proprietary encryption methods whose strengths are not known
- Does not use PGP software, but uses secure email. Use PKCS7 encoded messages that use 168 bit triple DES, SSH1 message authentication and 1024 bit RSA signatures and public key exchange.

Protecting Against Programmed Threats

- No anti-virus software is installed. Anti-virus software is installed on the client machine. All data on this server is transferred from client to server, so viruses will be detected on the client side.
- Integrity checks are run at bootup automatically using fsck

- Does not include nonstandard directories in execution path
- Does not leave any bin or library directories writable by untrustworthy accounts
- Permissions set on commands to prevent unauthorized alteration
- Home directories and dot files are not world writable or group writable. The ./cvs/cvsroot/CVSROOT/history is group writable because it is a source code repository that is shared among programmers
- No SUID or SGID shell scripts
- The xargs and find commands are not susceptible to a filename attack. We ran a script to check the behavior of xargs and the find command.
- Devices used for backup are not world readable
- Shared libraries are properly protected and protections can not be overridden.

Account Security

- No password security policy. Recommendations is distributed to all users, but not enforced. There are 3 users on the box, including 'redding' for auditing purposes. Password policy is distributed via word of mouth.
- We installed and ran Crack to check for weak passwords. Crack found one weak password.
- Does not automatically logoff users after a certain period of inactivity. We found a root account that had been logged on and idle for 7 days.
- No unauthorized user Ids of 0 or accounts without passwords
- Confirmed no unauthorized users have been added
- Confirmed no vendor-supplied default passwords exist.
- No unauthorized entries are in /etc/hosts.equiv file (hosts.equiv does not exist)
- Does not display last login date, time and unsuccessful attempts to user when user logs in
- Login failures and successes are logged in /var/log/messages
- Standard login naming scheme across all systems on the network
- All users have separate accounts to do day-to-day activities. Users su to root when they need to be superuser
- No guest login ids
- Uses shadow password file to hide encrypted passwords for local logins
- Does not include "." in PATH variable used by all users
- No "group" logins (i.e., logins shared by a group of users for performing a common function)
- Groups segregate users on the system
- Every group ID (GID) is unique throughout the network.

- Established and maintain security group which includes the superuser who maintains user accounts. There are users outside the security group that have access to the su command.
- Permissions on su are set to 755

File System Security

- No unauthorized processes are being executed via cron or at
- No entries in /etc/inetd.conf
- Uucp is disabled
- Setuid and setgid files exist with xterm logging vulnerability (CERT® Advisory CA-1993-17)
- No unauthorized versions of critical systems files
- No unowned files
- All users must have on individual home directory
- Directories containing system configuration files are not owned by ordinary users.
- System directories do not have "sticky bit" set to prevent files in the directory from being renamed or deleted
- System directories are not owned by ordinary users, and do not have write access.
- Permissions on application specific directories should be set to 700. They are set to 755
- User home directories are set to 750 and sticky bit is not set
- There is no subdirectory created (such as "local") in user's login directory for personal files, owned by the user with permissions 750
- Permissions on "." files are not set to 740
- No .rhosts files and .netrc reside in user directories
- All directories common to groups of users are owned by root and have group ownership set to the appropriate group
- Permissions set to 755 on common directories, but sticky bit not set
- Permissions on root directory are set to 755
- All subdirectories of the root directory are write protected except /tmp
- The terminal line configuration file has permissions set to 700
- The following files were run by inittab

```
redding@fs /sbin]$ ls -al /etc/rc.sysinit
rwxr-xr-x    1 root  root  13679 Feb 23  2000 rc.sysinit

redding@fs /sbin]$ ls -al /etc/rc
-rwxr-xr-x    1 root     root         2889 Nov  8  1999 rc

redding@fs /sbin]$ ls -al update
```

```
-rwxr-xr-x    1 root     root         7412 Feb  3  2000 update

[redding@fs /sbin]$ ls -al shutdown
-rwxr-xr-x    1 root     root        14128 Mar  7  2000
shutdown

[redding@fs /sbin]$ ls -al /sbin/mingetty
-rwxr-xr-x    1 root     root         8112 Feb  3  2000
/sbin/mingetty
```

- Maintains a listing of all "non-standard" setuid and setgid programs
- All device files are set to 600 except the following:
  ida = 775? (Script to create device nodes for SMART array controllers)
  Log=666 (valid dev file)
  null=666 (this is okay)
  ptmx=666 (used for telnet connections)
  pty=666 (this is okay)
  rd=755 (valid dev file)
  raw=775 (valid dev file)
  tty*=666 (this is okay)
  zero=666 (valid dev file)
- No unauthorized device files

Network Security

- inetd is not running
- Sendmail installed but not running.
- etc/ttys does not exist
- not using NFS
- /etc/exports file is empty
- not using ftpd
- no terminal and no modem
- not running nameserver software
- Blocks NTP connections from outside organization
- Blocks SNMP connections from outside organization
- /etc/hosts.equiv file and /etc/rhosts files empty
- Block incoming RIP packets; use static routes where possible and practical
- Disable UUCP over IP unless needed
- uses SSH

Backup/ Recovery

Does not perform backups. Server has never been backed up.

Disaster Recovery

No formal disaster recovery plan. Has insurance to cover damage. All mission critical data is the work Client XYZ does for clients and this is stored off site. Financial data is stored on alternate server.

Physical Security

- Servers reside locked room in the basement of a house. All servers are 6 inches off the floor. No protection from fire. Servers are not racked. Climate control - AC and heater.
- Room is locked and accessed from public access. Only the 2 users know combination to lock.
- Smoke alarm. No heat alarm.
- No fire extinguisher
- Smoking prohibited. Eating and drinking prohibited.
- Air filters cleaned once a year.
- Temperature controlled. No humidity controls. Does not get humid.
- No steel structural members.
- All windows are covered.
- No burglar alarm

Key Security Vulnerabilities

The following is a list of security issues uncovered during the audit.

- **Vulnerabilities exist in Operating System**

A number of vulnerabilities have been discovered in RedHat Linux 6.2. For a complete list, see RedHat Linux 6.2 Vulnerabilities

- **No welcome message to warn intruders**

According to officials of the US Department of Justice legal actions against intruders have failed because the owner of the computer failed to put up the equivalent of a "No Trespassing" sign. In addition, some users complain about being monitored without having given permission to be monitored. The logon message provides an opportunity to tell users who don't want to be monitored to stop using the system.

- **Poor security auditing practices**

Client XYZ does not run security auditing tools periodically to check for security violations or unauthorized system configuration changes. There is no security monitoring in place so an intrusion could be easily missed.

- **Password policy not enforced**

Crack was able to crack one of the user's passwords in minutes. An attacker could easily do the same.

- **Setuid and setgid files exist with vulnerability**

According to CERT, a vulnerability in the logging function of xterm exists in many versions of xterm that operate as a setuid or setgid process. The vulnerability allows local users to create files or modify any existing files. This vulnerability allows anyone with access to a user account to gain root access.

- **Does not conduct backups**

Without a restorable backup copy, data can not be recovered in the event of a loss.

- **No Disaster Recovery plan**

Client XYZ maintains all their hardware in one location. If this site is down for an extended period of time due to power failure, network failure, natural disaster etc, Client XYZ will be down for an extended period of time.

- **No Protection from Fire**

Computers are easily damaged by fire. Client XYZ has no fire extinguishers to put out fires. If the fire doesn't destroy the computer, the water used to put out the fire may.

Recommended Fixes

The following is a list of recommended fixes:

1. Get the Latest Version of Software

Download and install the patches to fix the vulnerabilities listed in the RedHat Linux 6.2 Vulnerabilities from http://www.redhat.com/support/errata/rh62-errata-security.html

2. Create a Logon Message to Warn Intruders

To create a welcome message, edit the /etc/motd file with the message you wish to display. A sample banner from the Department of Justice may provide a starting point for your message:

"WARNING! By accessing and using this system you are consenting to system monitoring for law enforcement and other purposes. Unauthorized use of this computer system may subject you to criminal prosecution and penalties."

3. Conduct Periodic Security Audits

- Automate log scanning with Swatch

Client XYZ examines log files periodically for abnormal behavior. This can be automated with Swatch. Swatch can be obtained at ftp://ftp.stanford.edu/general/security-tools/swatch/swatch.tar.

In addition to log monitoring, it is recommended that Client XYZ run security auditing tools to check for security violations.

- Run Tripwire to examine file changes

Tripwire is a file integrity checking mechanism that detects unauthorized and/or unexpected changes to files. During the audit, we ran Tripwire to capture an initial snapshot of the system. Tripwire should be run periodically in the capture changes to the system. All valid system configuration changes should be recorded.

- Run PortSentry to detect port scans

PortSentry should be run to detect and respond to port scans against a target host in real-time.

4. Enforce Account Security

- Enforce a Password Policy

Password normally UNIX's first line of defense against outsiders who want to break into the system. Many break-ins result because of poorly chosen or poorly protected passwords. Crack revealed that some users at Client XYZ choose poor passwords. It is highly recommended that Client XYZ enforce their password policy. Tools such as passwd, yppasswd and authbkr automatically enforce security policy for passwords. In addition, it is recommended that Client XYZ run Crack periodically to check for weak passwords.

- Tighten File permissions by setting the UMASK = 027

- Automatically logoff users after a certain period of inactivity

- Display last login date, time and unsuccessful attempts to user when user logs in

This will alert the user to unusual activity.

5. Remove Setuid and Setgid files

All of the following solutions require that a new version of xterm be installed. When installing the new xterm, it is important either to remove the old version of xterm or to clear the setuid and setgid bits from the old xterm.

CERT suggests one of the following solutions:

A. Install vendor supplied patch if available. CERT is hopeful that patches will be forthcoming. CERT will be maintaining a status file, xterm-patch-status, and will add patch availability information to this file as it becomes known. The file is available from:
http://www.cert.org/advisories/CA-1993-17/patch-status.txt
For more up-to-date information, contact the vendor.

B. If your site is using the X Consortium's X11R5, install the public patch #26. This patch is available via anonymous FTP from ftp.x.org as the file /pub/R5/fixes/fix-26. Install all patch files up to and including fix-26.
By default, the patch disables logging. If you choose to enable logging, a variation of the vulnerability still exists.
Checksum information:

```
BSD Unix Sum:  19609 47

System V Sum:  51212 94

MD5 Checksum:  e270560b6e497a0a71881d4ff4db8c05
```

C. If your site is using an earlier version of the X Consortium's X11, upgrade to X11R5. Install all patches up to and including fix-26.

D. If you are unable to upgrade to the X Consortium's X11R5, modify the xterm source code to remove the logging feature. Familiarity with X11 and its installation and configuration is recommended before implementing these modifications.

6. Develop and Implement a Backup/Restore Strategy

It is essential to conduct regular backups to protect your system from data loss due to natural disaster, human mistakes, a system attack, software failure, hardware failure, etc... Develop a backup strategy that is suitable for your company's needs. Conduct a full backup periodically and conduct a restore to test the backup. Encrypt the data, write-protect the backup tape and store the tapes in a secure offsite location.

7. Develop and Implement a Disaster Recovery Strategy

Create a formal Disaster Recovery and Business Continuity plan in place, including plans for rapidly acquiring new equipment and software. Document contingencies for loss of phone or network, vendor bankruptcy, death or incapacitation of key personnel.

8. Protect Systems from Fire

Obtain and install a fire extinguisher and train users of the system how to use the fire extinguisher. Rack the servers. Install a burglar alarm.

9. Install a Burglar Alarm

From the Chubb Electronic Security website, "Burglar alarm systems can warn you and your security service that urgent response is needed. Early warning reduces the time available to burglars, limiting their pickings and the damage they can do. Burglar alarm systems must be configured to warn you that a break-in or attempted break-in is taking place when you are in the house and, additionally, when you return to your home that a break-in or attempted break-in has occurred. It must be noted that a burglar alarm system is only as good as the response it generates from the monitoring company."

References

1. Accenture (September 6, 1996). *UNIX Security Checklist*

2. Simson Garfinkel and Gene Spafford (1996), *Practical Unix and Internet Security* (2nd ed), O'Reilly & Associates

3. W. Richard Stevens(1993), *Advanced Programming in the UNIX Environment* (1st ed), Addison Wesley Longman, Inc.

4. Muffet, Alec (2001, January 12). *Crack.* URL: http://www.securityfocus.com/tools/7

5. Psionic Software, Inc (May 10 2000). *Psionic Port Sentry 1.0: Port Scan Detection and Active Defense System*, URL: http://www.psionic.com/abacus/portsentry/

6. Red Hat Inc (January 12, 2001), *RedHat Linux 6.2 Security Advisories*, URL: http://www.redhat.com/support/errata/rh62-errata-security.html

7. Seifried, Kurt (December 2, 2000). ISC DHCPD, *SecurityPortal*, URL: http://securityportal.com/closet/closet20001129.html

8. OpenBSD.org(December 26,2000). *OpenBSD Security*, URL: http://www.openbsd.org/security.html#28

9. Carnegie Mellon University (November 11, 1993). *CERT® Advisory CA-1993-17 xterm Logging Vulnerability*, URL: http://www.cert.org/advisories/CA-1993-17.html

10. Chubb Electronic Security (November 2000). *Burglar Alarms and Armed Response*, URL: http://www.chubb.co.za/security/balarms.html

Appendix I: Unix Security Checklist

TOPIC NUMBER	CONTROL CONCERN	ISSUE DESCRIPTION	IMPLEMENTED? (Y or N)
1.00	**Operating System**		
		Update latest patches	No
2.00	**System Configuration**		
2.01		Install Tiger to locate potential problems in system configuration.	Yes
2.02		Install PortSentry to check for security violations.	Yes
2.03		Install Tripwire to check for security violations.	Yes
2.04		Replace any welcome message from your *login* program and */etc/motd* file with warnings to unauthorized users stating that they are not welcome.	No
2.05		Set the PATH environment variable to include only trusted, secure paths.	Yes
2.06		Set the UMASK environment variable to 027 (check the rc structure).	No, UMASK set to 002
3.00	**Risks from installed third-party software**		
3.01		ISC DHCPD	
3.02		SMBD	
3.03		Open SSH	
3.04		X11 R6 Version 4	

3.05		Netscape Navigator 4.75	
3.06		Lynx	
3.07		Services: Port State Service 22/tcp open ssh 25/tcp open smtp 111/tcp open sunrpc 113/tcp open auth 139/tcp open netbios-ssn 515/tcp open printer 934/tcp open unknown 1024/tcp open kdm 6000/tcp open X11 7101/tcp open unknown	
4.00	**Administrative practices**		
4.01		Turn on all system auditing tools	No system auditing tools running. Would slow system down.
4.02		Review the syslog, wtmp and security tool logs regularly for unauthorized activity.	Yes, check these logs once a month
4.03		Securely transfer the logs of critical machines to other network systems	Not a critical machine. Logs from other machines are transferred to this machine.
4.04		Rotate and archive system log files weekly	Logs are rotated daily and weekly. Syslogs are rotated daily and purged after 7 days.
4.05		Periodically run Tripwire, COPS and Tiger and act on	No

		any security violations.	
4.06		Automate log scanning with Swatch	No
4.07		Automatically alarm the system administrator for CRIT, ALERT or EMERG level log messages	No
4.08		No hardcoding of passwords in any files including scripts	Yes
4.09		Report all security violations to the network administrator	Yes (user is the network administrator!)
4.10		Conduct a complete security review of the system on a periodic basis	Every 3 months run port scanning tools and examines logs
4.11		Install vendor supplied patches	No
4.12		Get proper approval before changing "required" security provisions	Yes (gets approval from self!)
4.13		Log all new system files and changes to configurations or file permissions	No
4.14		Test the effects of all changes on system performance and security	Yes. No performance monitoring, but if the system is running slow, knows there is a problem. Scans box after installing software.
5.00	**Sensitive Data and Encryption**		
5.01		Never use rot13 as an encryption method to protect data	No
5.02		Don't depend on the crypt command to protect anything particularly sensitive	Uses crypt version that comes with RedHat Linux 6.2, uses MD5 hash
5.03		Use the compress command (or similar compression system) on files before encrypting them	No

5.04	Learn how to use message digests. Obtain and install a message digest program (such as MD5)	Yes, uses MD5
5.05	Never use a login password as an encryption key	Yes
5.06	Protect your encryption key as you would your password, don't write it down, put it in a shell file, or store it online	Yes
5.07	Protect your encryption programs against tampering	No, FIPS 140-1 is the standard for cryptographic modules in the Federal Government. Does not runs Netscape in FIPS 140-1 mode, which means the cryptography could be tampered with if someone had root access. Uses SSL on this box.
5.08	Avoid proprietary encryption methods whose strengths are not known	Yes
5.09	Use PGP software and make it available to your users	Does not use PGE software, but uses secure email. Use PKCS7 encoded messages that use 168 bit triple DES, SSH1 message authentication and 1024 bit RSA signatures and public key exchange.
5.10	Data is sent over the Internet encrypted	fetches files using FTP, HTTP over the LAN
6.00	**Protecting Against Programmed Threats**	

6.01	Anti-virus software is updated (if used as a server for Windows systems)	No, no anti-virus software is installed. Anti-virus software is installed on the client machine. All data on this server is transferred from client to server, so viruses will be detected on the client side.
6.02	Run integrity checks on your system on a regular basis	Yes, Integrity checks are run at bootup automatically using fsck
6.03	Don't include nonstandard directories in your execution path	Yes
6.04	Don't leave any bin or library directories writable by untrustworthy accounts.	Yes
6.05	Set permissions on commands to prevent unauthorized alteration	Yes
6.06	Scan your system for any user home directories or dot files that are world writable or group writable	Yes, ./cvs/cvsroot/CVSROOT/history is group writable because it is a source code repository that is shared among programmers
6.07	Never write or use SUID or SGID shell scripts	Yes
6.08	Disable terminal answer-back	Yes (no terminal)
6.09	Check the behavior of your xargs and find commands. Review the use of these commands (and the shell) in all scripts executed by cron	No, we ran a script to test the xargs, find and shell commands. The shell command failed.
6.10	Make sure the devices used for backups are not world readable	Yes

6.11		Make sure that any shared libraries are properly protected and that protections cannot be overridden.	Yes
7.00	**Account Security**		
7.01		Define password security policy, distribute to all users and enforce. Policy should include: length, strength and aging	Recommendations is distributed to all users, but not enforced. 3 users on the box (including me for auditing purposes). Password policy is distributed via word of mouth.
7.02		Make passwd, yppasswd and authbkr automatically enforce security policy for passwords	No (no security policy)
7.03		Install Crack to check for weak passwords	Yes, but not run periodically
7.04		Automatically logoff users after a certain period of inactivity.	No, we found a root account that had been logged on and idle for 7 days
7.05		Confirm no unauthorized user IDs of 0, accounts without passwords (this will be caught by COPS and Tiger)	Yes
7.06		Confirm no unauthorized users have been added	Yes
7.07		Confirm no vendor-supplied default passwords exist.	Yes
7.08		Limit access to trusted systems; no unauthorized entries are in /etc/hosts.equiv file	Yes, /etc/hosts.equiv does not exist
7.09		Display last login date, time and unsuccessful attempts to user when user logs in	No
		Record successful and unsuccessful attempts to log in	Yes, login failures and successes are

		logged in /var/log/messages
7.10	Create standard login naming scheme across all systems on the network	Yes
7.11	Superusers should have separate accounts to conduct day-to-day activities (UID <> 0) and to perform sys admin (UID = 0). Also ALL administrators - those w/ UID = 0 - should be kept in local password files, NOT in master NIS map.	Yes, all users su to root when they need to be superuser
7.12	Delete all guest login Ids	Yes
7.13	Use shadow password file to hide encrypted passwords for local logins (i.e., those not in NIS)	Yes
7.14	Set the UMASK environment variable to 027 for prod and admin users, 022 for developers (verify in the users profile)	No, Set to 022 for all users
7.15	Never include "." (current directory) in PATH variable used by all users	Yes
7.16	There should be no "group" logins (i.e., logins shared by a group of users for performing a common function)	No
7.17	Establish groups to segregate users on the system	Yes
7.18	Every group ID (GID) should be unique throughout the network. If the same group is on multiple systems the GID should be the same on all systems	Yes
7.19	Establish and maintain a "security" group which includes the superuser who maintains user accounts	Yes, Gene is the security group.

7.20		Only members of the "security" group should have access to the "su" command.	No
7.21		Permissions on su should be 750	No, Permissions are set to 755
8.00	**File System Security**		
8.01		Verify no unauthorized processes are being executed via cron or at	Yes
8.02		Examine /etc/inetd.conf file for unauthorized changes or entries and confirm that all files specified in by inetd.conf are correct (this will be verified with Tiger)	Yes, no entries in /etc/inetd.conf
8.03		Disable uucp	Yes
8.04		Search for and remove hidden files with odd names	Yes. (this was checked by Tiger).
8.05		Search for and remove files with setuid or setgid capabilities	No. Files exist with setuid bits set
8.06		Search for and remove unauthorized versions of critical systems files	Yes
8.07		Search for unowned files and remove or assign an owner to them	Yes
8.08		All users must have on individual home directory	Yes
8.09		All directories containing system configuration files should not be owned by ordinary users.	Yes, found a few device files owned by a user
8.10		System directories should have "sticky bit" set to prevent files in the directory from being renamed or deleted	No

8.11	System directories should not be owned by ordinary users, nor should they have write access.	Yes (checked by Tiger)
8.12	Permissions on application specific directories should be set to 700.	No, Directories set to 755
8.13	All user home directories should be owned by the user with permissions set to 750 and the "sticky bit" set. This will prevent users from renaming or deleting files from this directory and from creating dangerous files here (e.g., .rhosts files).	No, permissions not set to 750 and sticky bit is not set
8.14	Establish subdirectory (such as "local") in user's login directory for personal files, owned by the user with permissions 750	No
8.15	Set permissions on all .filename files to 740	No
8.16	Eliminate any .rhosts files in users' home directories	Yes
8.17	Eliminate any .netrc files in the users' home directories.	Yes
8.18	All directories common to groups of users should be owned by root and should have group ownership set to the appropriate group	Yes
8.19	Set permissions on common directories to 755 with the "sticky bit" set to prevent unauthorized deletions	No, Permissions set to 755, but sticky bit not set
8.20	Establish permissions on the root directory ("/") as 755.	Yes
8.21	All subdirectories of the root directory should be write protected except /tmp.	Yes,

8.22	The terminal line configuration file should have permissions set to 700	Yes
8.23	All files processed by /etc/inittab, both directly and indirectly, should have least privilege possible.	No. The following files were run by inittab redding@fs /sbin]$ ls -al /etc/rc.sysinit rwxr-xr-x 1 root root 13679 Feb 23 2000 rc.sysinit redding@fs /sbin]$ ls -al /etc/rc -rwxr-xr-x 1 root root 2889 Nov 8 1999 rc redding@fs /sbin]$ ls -al update -rwxr-xr-x 1 root root 7412 Feb 3 2000 update [redding@fs /sbin]$ ls -al shutdown -rwxr-xr-x 1 root root 14128 Mar 7 2000 shutdown [redding@fs /sbin]$ ls -al /sbin/mingetty -rwxr-xr-x 1 root root 8112 Feb 3 2000 /sbin/mingetty
8.24	Maintain a listing of all "non-standard" setuid and setgid programs	Yes

8.25		Ensure the proper permissions are set for the devices in /dev	ida = 775? (Script to create device nodes for SMART array controllers) Log=666 (valid dev file) null=666 (this is okay) ptmx=666 (used for telnet connections) pty=666 (this is okay) rd=755 (valid dev file) raw=775 (valid dev file) tty*=666 (this is okay) zero=666 (valid dev file)
9.00	**Network Security**		
9.01		Remove Sendmail if not needed, otherwise install latest version of Sendmail.	No. Sendmail installed but not running
9.02		Turn off rexecd, rshd, rlogind, tftpd and rcpd	Yes
9.03		Turn off .rhosts access	Yes
9.04		Turn off .netrc access	Yes
9.05		Enable X access control by default	Yes
9.06		Turn off NIS	Yes
9.07		Verify no unauthorized mail aliases exist in /usr/lib/aliases file (look at /etc/aliases and .forward files)	Yes
9.08		Verify correct "secure" settings for all terminal types in /etc/ttys or equivalent file	Yes, etc/ttys does not exist
9.09		Use a portmapper that prevents NFS access.	Yes, not using NFS

9.10	Check the configuration of /etc/export files for: self-references, "localhost" entry, global exports, any wildcard characters, lists exceeding 256 characters, read-only access wherever possible.	Yes, /etc/exports file is empty
9.11	Install latest ftpd	N/A, not using ftpd
9.12	No "decode" alias in the aliases file	Yes
9.13	No "wizard" password in sendmail.cf	Yes
9.14	Investigate modem usage on each system and ensure that modems and terminals handle hang-ups properly	Yes, no terminal and no modem
9.15	Permissions on devices connected to incoming modems should be set to 600.	N/A
9.16	Make sure the modem's escape sequence is disabled by the modem control program.	N/A
9.17	Ensure that the versions of "cu" and "tip" on the system do not give the users the program's UID when users attempt a shell escape.	N/A
9.18	Make sure that you are running the latest version of the nameserver software with all patches applied	N/A, not running nameserver software
9.19	Make sure that your finger program is more recent that November 5, 1988	Yes, Finger service not used
9.20	Disable or replace the finger service with something that provides less information	Yes, Finger service not used
9.21	Block NTP connections from outside your organization	Yes
9.22	Block SNMP connections from outside your organization	Yes

9.23		Do not place usernames in your /etc/hosts.equiv file	Yes
9.24		If you have a plus sign (+) in your /etc/hosts.equiv file, remove it.	Yes
9.25		Block incoming RIP packets; use static routes where possible and practical	Yes
9.26		Disable UUCP over IP unless needed	Yes
9.27		Setup your logindevperm or fbtab files to restrict permissions on frame buffers and devices, if this is possible on your system.	N/A
9.28		If your X11 Server blocks on null connections, get an updated version.	N/A
9.29		Enable the best X11 authentication possible in your configuration (e.g., Kerberos, Secure RPC, "magic cookies") instead of using xhost.	Yes, use SSH
9.30		Scan your network with Nessus to determine if you have uncorrected vulnerabilities - before an attacker does the same.	Yes, found 1 security hole. Running RPC. Configured box to not start RPC. Rebooted box and reran Nessus. Nessus did not find any security holes.
9.31		Turn off all unnecessary services in /etc/inetd.conf	Yes, no services running
10.00	**Backup/ Recovery**		
10.01		Perform a level 0 backup monthly and a incremental backup weekly.	No. Does not perform backups. Server has never been backed up.
10.02		Store backups in a secure off-site location	N/A
10.03		Install a UPS system	Yes. APC SmartUPS1000-RM
10.04		Prepare the system for elegant shutdown in the event of	No.

		a system halt	
10.05		Be certain that *everything* on your system is on your backups	No.
10.06		Make copies of critical files for comparison or rebuilding your system (/etc/password, /ect/rc, /etc/fstab)	No.
10.07		Make at least every other backup onto a different tape to guard against media failure	No.
10.08		Do not reuse a backup tape too many times, because the tapes will eventually fail	N/A
10.09		Try to restore a few files from your backup tapes on a regular basis	N/A
10.10		Try to completely rebuild your system from a set of backup tapes to be certain that your backup procedures are complete	N/A
11.00	**Disaster Recovery**		
11.01		A formal Disaster Recovery and Business Continuity plan in place, including plans for rapidly acquiring new equipment and software. Document contingencies for loss of phone or network, vendor bankruptcy, death or incapacitation of key personnel	No formal disaster recovery plan. Have insurance to cover damage. All mission critical data is off site. Mission critical data the work we do for clients. This is stored at client sites. Financial data is stored alternate server on backup server.
11.02		Plan tested by renting or borrowing a computer system and trying to restore the system.	No

12.00	**Physical Security**		
12.01		Protect the system from earthquakes, explosions, fire, heat, moisture, etc.	Servers reside locked room in the basement of a house. All servers are 6 inches off the floor. No protection from fire. Servers are not racked. Climate control - AC and heater.
12.02		Physically lock and isolate the system and console from public access	yes. Dave and Gene know combination to room
12.03		Secure all peripheral devices connected to the system.	Yes
12.04		Have heat and smoke alarms in your computer room.	Smoke alarm. No heat alarm.
12.05		Check the placement and recharge status of fire extinguishers on a regular basis	No fire extinguisher
12.06		Make sure the personnel know how to use all fire protection and suppression equipment	N/A
12.07		Make sure that the placement and nature of fire-suppression systems will not endanger personnel or equipment more than necessary	N/A
12.08		Have water sensors installed above and below raised floors in your computer room	N/A
12.09		Strictly prohibit smoking, eating, and drinking water in your computer room or near computer equipment	Smoking prohibited. Eating and drinking prohibited.
12.10		Install and regularly clean air filters in your computer room	Air filters cleaned once a year.

12.11	Have temperature and humidity controls in your computer room. Have alarms associated with the systems to indicate if values get out of range. Have recorders to monitor these values over time	No. Temperature controlled. No humidity controls. Does not get humid.
12.12	Have antistatic measures in place	No.
12.13	Store computer equipment and magnetic media away from building structural steel members that might conduct electricity after a lightening strike	No steel structural members.
12.14	Avoid having glass walls or large windows in your computer room	No. Windows are covered.
	Burglar alarm installed and working properly.	No.

Appendix II: Tiger Report

```
Security scripts *** 2.2.3, 1994.0309.2038 ***
Thu Jan  4 15:34:33 EST 2001
15:34> Beginning security report for fs (i586 Linux 2.2.14-5.0).

# Performing check of passwd files...

# Performing check of group files...

# Performing check of user accounts...
# Checking accounts from /etc/passwd.
--WARN-- [acc001w] Login ID adm is disabled, but still has a
valid shell
         (/bin/sh).
--WARN-- [acc001w] Login ID bin is disabled, but still has a
valid shell
         (/bin/sh).
--WARN-- [acc001w] Login ID cvs is disabled, but still has a
valid shell
         (/bin/bash).
--WARN-- [acc001w] Login ID daemon is disabled, but still has a
valid shell
         (/bin/sh).
--WARN-- [acc001w] Login ID <USERNAME> is disabled, but still
has a valid shell
         (/bin/bash).
--WARN-- [acc001w] Login ID <USERNAME> is disabled, but still
has a valid shell
         (/bin/bash).
--WARN-- [acc001w] Login ID ftp is disabled, but still has a
valid shell
         (/bin/sh).
--WARN-- [acc001w] Login ID games is disabled, but still has a
valid shell
         (/bin/sh).
--WARN-- [acc001w] Login ID gdm is disabled, but still has a
valid shell
         (/bin/bash).
--WARN-- [acc001w] Login ID gopher is disabled, but still has a
valid shell
         (/bin/sh).
```

```
--WARN-- [acc001w] Login ID gportnoy is disabled, but still has
a valid shell
         (/bin/bash).
--WARN-- [acc001w] Login ID lp is disabled, but still has a
valid shell
         (/bin/sh).
--WARN-- [acc001w] Login ID mail is disabled, but still has a
valid shell
         (/bin/sh).
--WARN-- [acc001w] Login ID news is disabled, but still has a
valid shell
         (/bin/sh).
--WARN-- [acc001w] Login ID nobody is disabled, but still has a
valid shell
         (/bin/sh).
--WARN-- [acc001w] Login ID operator is disabled, but still has
a valid shell
         (/bin/sh).
--WARN-- [acc001w] Login ID pvm is disabled, but still has a
valid shell
         (/bin/bash).
--WARN-- [acc001w] Login ID redding is disabled, but still has a
valid shell
         (/bin/bash).
--WARN-- [acc001w] Login ID root is disabled, but still has a
valid shell
         (/bin/bash).
--WARN-- [acc001w] Login ID uucp is disabled, but still has a
valid shell
         (/bin/sh).
--WARN-- [acc006w] Login ID cvs's home directory (/home/cvs) has
group `cvs'
         write access.
--WARN-- [acc006w] Login ID lp's home directory (/var/spool/lpd)
has group
         `daemon' write access.
--WARN-- [acc006w] Login ID mail's home directory
(/var/spool/mail) has group
         `mail' write access.

# Performing check of /etc/hosts.equiv and .rhosts files...

# Checking accounts from /etc/passwd...
```

```
# Performing check of .netrc files...

# Checking accounts from /etc/passwd...

# Performing check of PATH components...
# Only checking user 'root'

# Performing check of anonymous FTP...

# Performing checks of mail aliases...
# Checking aliases from /etc/aliases.

# Performing check of `cron' entries...

# Performing check of 'services' and 'inetd'...
# Checking services from /etc/services.
--FAIL-- [inet002f] Service echo is assigned to port 4/ddp which
should be
         7/tcp.
--FAIL-- [inet002f] Service echo is assigned to port 4/ddp which
should be
         7/udp.
--FAIL-- [inet002f] Service irc is assigned to port 194/tcp
which should be
         6667/tcp.
--FAIL-- [inet002f] Service irc is assigned to port 194/udp
which should be
         6667/tcp.
--FAIL-- [inet003f] The port for service dos is assigned to
service bbs.
--FAIL-- [inet003f] The port for service irc is assigned to
service ircd.
--FAIL-- [inet003f] The port for service pop-2 is assigned to
service pop2.
--FAIL-- [inet003f] The port for service pop-3 is assigned to
service pop3.
--FAIL-- [inet003f] The port for service http is assigned to
service www.
# Checking inetd entries from /etc/inetd.conf

# Performing NFS exports check...

# Performing check of system file permissions...
--WARN-- [perm006w] /root/.bashrc should not have group read.
```

```
--WARN-- [perm006w] /root/.bashrc should not have world read.
--WARN-- [perm006w] /root/.cshrc should not have group read.
--WARN-- [perm006w] /root/.cshrc should not have world read.
--FAIL-- [perm007f] /etc/aliases should not have group read.
--FAIL-- [perm007f] /etc/aliases should not have world read.
--FAIL-- [perm007f] /etc/aliases.db should not have group read.
--FAIL-- [perm007f] /etc/aliases.db should not have world read.
--WARN-- [perm008w] /etc/exports should not have group read.
--WARN-- [perm008w] /etc/exports should not have world read.
--WARN-- [perm003w] /etc/fstab should not have group read.
--WARN-- [perm003w] /etc/fstab should not have world read.
--WARN-- [perm012w] /etc/inetd.conf should not have group read.
--WARN-- [perm012w] /etc/inetd.conf should not have world read.
--FAIL-- [perm015f] /etc/rc.d should not have group read.
--FAIL-- [perm015f] /etc/rc.d should not have group search.
--FAIL-- [perm015f] /etc/rc.d should not have world read.
--FAIL-- [perm015f] /etc/rc.d should not have world search.
--WARN-- [perm017w] /var/run/utmp should not have group write.
--WARN-- [perm021w] Disk device /dev/hda8 has read/write access
for group
         disk.
--WARN-- [perm021w] Disk device /dev/hda1 has read/write access
for group
         disk.
--WARN-- [perm021w] Disk device /dev/hda5 has read/write access
for group
         disk.
--WARN-- [perm021w] Disk device /dev/hda7 has read/write access
for group
         disk.
--WARN-- [perm021w] Disk device /dev/hda6 has read/write access
for group
         disk.

# Performing signature check of system binaries...
--WARN-- [sig004w] None of the following versions of /bin/bash
(-rwxr-xr-x)
         matched the /bin/bash on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /bin/login
(-rwxr-xr-x)
         matched the /bin/login on this machine.
         >>>>>> Linux 2.0.35
```

```
--WARN-- [sig004w] None of the following versions of /bin/mount
(-rwsr-xr-x)
         matched the /bin/mount on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /bin/ping
(-rwsr-xr-x)
         matched the /bin/ping on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /bin/su (-
rwsr-xr-x)
         matched the /bin/su on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /bin/tcsh
(-rwxr-xr-x)
         matched the /bin/tcsh on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /bin/umount
(-rwsr-xr-x)
         matched the /bin/umount on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/sbin/cardctl
         (-rwxr-xr-x) matched the /sbin/cardctl on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /sbin/dump
(-rwsr-sr-x)
         matched the /sbin/dump on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/sbin/netreport
         (-rwxr-sr-x) matched the /sbin/netreport on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/sbin/pwdb_chkpwd
```

```
         (-r-sr-xr-x) matched the /sbin/pwdb_chkpwd on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/sbin/restore
         (-rwsr-sr-x) matched the /sbin/restore on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/bin/at
(-rwsr-xr-x)
         matched the /usr/bin/at on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/chage
         (-rwsr-xr-x) matched the /usr/bin/chage on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/chfn
         (-rws--x--x) matched the /usr/bin/chfn on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/chsh
         (-rws--x--x) matched the /usr/bin/chsh on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/crontab
         (-rwsr-xr-x) matched the /usr/bin/crontab on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/bin/cu
(-r-sr-sr-x)
         matched the /usr/bin/cu on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/dumpreg
```

```
         (-rwxr-xr-x) matched the /usr/bin/dumpreg on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/gpasswd
         (-rwsr-xr-x) matched the /usr/bin/gpasswd on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/inc (-rwxr-xr-x)
         matched the /usr/bin/inc on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/lockfile
         (-rwxr-sr-x) matched the /usr/bin/lockfile on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/lpq (-r-sr-sr-x)
         matched the /usr/bin/lpq on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/lpr (-r-sr-sr-x)
         matched the /usr/bin/lpr on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/lprm
         (-r-sr-sr-x) matched the /usr/bin/lprm on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/man (-rwxr-sr-x)
         matched the /usr/bin/man on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/minicom
```

```
         (-rwxr-sr-x) matched the /usr/bin/minicom on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/mutt
         (-rwxr-xr-x) matched the /usr/bin/mutt on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/newgrp
         (-rws--x--x) matched the /usr/bin/newgrp on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/passwd
         (-r-s--x--x) matched the /usr/bin/passwd on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/procmail
         (-rwsr-sr-x) matched the /usr/bin/procmail on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/rcp (-rwsr-xr-x)
         matched the /usr/bin/rcp on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/restorefont
         (-rwxr-xr-x) matched the /usr/bin/restorefont on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/restorepalette
         (-rwxr-xr-x) matched the /usr/bin/restorepalette on
this machine.
         >>>>>> Linux 2.0.35
```

```
--WARN-- [sig004w] None of the following versions of
/usr/bin/restoretextmode
         (-rwxr-xr-x) matched the /usr/bin/restoretextmode on
this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/rlogin
         (-rwsr-xr-x) matched the /usr/bin/rlogin on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/rsh (-rwsr-xr-x)
         matched the /usr/bin/rsh on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/screen
         (-rwxr-xr-x) matched the /usr/bin/screen on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/suidperl
         (-rws--x--x) matched the /usr/bin/suidperl on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/telnet
         (-rwxr-xr-x) matched the /usr/bin/telnet on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/uucp
         (-r-sr-xr-x) matched the /usr/bin/uucp on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/uuname
         (-r-sr-sr-x) matched the /usr/bin/uuname on this
machine.
```

```
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/uustat
         (-r-sr-xr-x) matched the /usr/bin/uustat on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/uux (-r-sr-xr-x)
         matched the /usr/bin/uux on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/wall
         (-r-xr-sr-x) matched the /usr/bin/wall on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/bin/write
         (-rwxr-sr-x) matched the /usr/bin/write on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/in.fingerd
         (-rwxr-xr-x) matched the /usr/sbin/in.fingerd on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/in.ftpd
         (-rwxr-xr-x) matched the /usr/sbin/in.ftpd on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/in.rexecd
         (-rwxr-xr-x) matched the /usr/sbin/in.rexecd on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/in.rlogind
```

```
         (-rwxr-xr-x) matched the /usr/sbin/in.rlogind on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/in.rshd
         (-rwxr-xr-x) matched the /usr/sbin/in.rshd on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/in.telnetd
         (-rwxr-xr-x) matched the /usr/sbin/in.telnetd on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/in.tftpd
         (-rwxr-xr-x) matched the /usr/sbin/in.tftpd on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/inetd
         (-rwxr-xr-x) matched the /usr/sbin/inetd on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/lpc
         (-rwxr-sr-x) matched the /usr/sbin/lpc on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/lpd
         (-rwxr--r--) matched the /usr/sbin/lpd on this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/rpc.mountd
         (-rwxr-xr-x) matched the /usr/sbin/rpc.mountd on this
machine.
         >>>>>> Linux 2.0.35
```

```
--WARN-- [sig004w] None of the following versions of
/usr/sbin/rpc.yppasswdd
         (-rwxr-xr-x) matched the /usr/sbin/rpc.yppasswdd on
this machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/Sendmail
         (-rwsr-sr-x) matched the /usr/sbin/Sendmail on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/tcpd
         (-rwxr-xr-x) matched the /usr/sbin/tcpd on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/traceroute
         (-rwsr-xr-x) matched the /usr/sbin/traceroute on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/userhelper
         (-rwsr-xr-x) matched the /usr/sbin/userhelper on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/usernetctl
         (-rwsr-xr-x) matched the /usr/sbin/usernetctl on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/uucico
         (-r-sr-sr-x) matched the /usr/sbin/uucico on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/uuxqt
```

```
         (-r-sr-sr-x) matched the /usr/sbin/uuxqt on this
machine.
         >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of
/usr/sbin/ypserv
         (-rwxr-xr-x) matched the /usr/sbin/ypserv on this
machine.
         >>>>>> Linux 2.0.35


# Checking for known intrusion signs...

# Performing check of files in system mail spool...

# Performing system specific checks...
# Performing checks for Linux/2...
# Running './scripts/check_sendmail'...

# Checking Sendmail...

# Checking setuid executables...
--WARN-- [misc013w]
         /home/<USERNAME>/sterling.<DOMAIN
NAME>/usr/X11R6/bin/nxterm: see CERT
         Advisory CA-93:17 about a security hole in xterm.
--WARN-- [misc013w]
         /home/<USERNAME>/sterling.<DOMAIN
NAME>/usr/X11R6/bin/xterm: see CERT
         Advisory CA-93:17 about a security hole in xterm.
--WARN-- [fsys002w] setuid program
         /home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/uucp
has relative
         pathnames.
--WARN-- [fsys002w] setuid program
         /home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/uustat
has relative
         pathnames.
--WARN-- [fsys002w] setuid program
         /home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/uux has
relative
         pathnames.
--WARN-- [fsys002w] setuid program
```

```
         /home/<USERNAME>/sterling.<DOMAIN NAME>/usr/sbin/uucico
has relative
         pathnames.
--WARN-- [fsys002w] setuid program
         /home/<USERNAME>/sterling.<DOMAIN NAME>/usr/sbin/uuxqt
has relative
         pathnames.
--WARN-- [fsys002w] setuid program /sbin/pwdb_chkpwd has
relative pathnames.
--WARN-- [fsys002w] setuid program /sbin/unix_chkpwd has
relative pathnames.
--WARN-- [fsys002w] setuid program /usr/bin/uucp has relative
pathnames.
--WARN-- [fsys002w] setuid program /usr/bin/uustat has relative
pathnames.
--WARN-- [fsys002w] setuid program /usr/bin/uux has relative
pathnames.
--WARN-- [fsys002w] setuid program /usr/libexec/pt_chown has
relative
         pathnames.
--WARN-- [fsys002w] setuid program /usr/sbin/uucico has relative
pathnames.
--WARN-- [fsys002w] setuid program /usr/sbin/uuxqt has relative
pathnames.

---s--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/X11R6/bin/xlock
-r-s--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/zgv
-r-sr-sr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/cu
-r-sr-sr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/lpq
-r-sr-sr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/lpr
-r-sr-sr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/lprm
-r-sr-sr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/uuname
-r-sr-sr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/sbin/uucico
-r-sr-sr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/sbin/uuxqt
```

```
-r-sr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/sbin/pwdb_chkpwd
-r-sr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/X11R6/bin/XConsole
-r-sr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/passwd
-r-sr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/uucp
-r-sr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/uustat
-r-sr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/uux
-r-sr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/sbin/sendmail
-r-sr-xr-x root     root     /sbin/unix_chkpwd
-rwSr-Sr-- <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN
NAME>/var/lib/games/trojka.scores
-rwSr-Sr-- <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN
NAME>/var/lib/games/xtrojka.score
-rws--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/bin/login
-rws--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/X11R6/bin/kterm
-rws--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/X11R6/bin/nxterm
-rws--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/X11R6/bin/xterm
-rws--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/chfn
-rws--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/chsh
-rws--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/ct
-rws--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/newgrp
-rws--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/sperl5.00401
-rws--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/suidperl
-rws--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/games/vga_connectN
```

```
-rws--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/games/vga_klondike
-rws--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/games/vga_mines
-rws--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/games/vga_ohhell
-rws--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/games/vga_othello
-rws--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/games/vga_solitaire
-rws--x--x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/games/vga_spider
-rws--x--x root     root     /usr/bin/sperl5.00503
-rwsr-sr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/sbin/dump
-rwsr-sr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/sbin/restore
-rwsr-sr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/mh/inc
-rwsr-sr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/procmail
-rwsr-x--- <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/sbin/inndstart
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/bin/mount
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/bin/ping
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/bin/su
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/bin/umount
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/sbin/cardctl
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/X11R6/bin/rxvt
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/X11R6/bin/xhextris
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN
NAME>/usr/X11R6/bin/xscreensaver
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/X11R6/bin/xserver-
wrapper
```

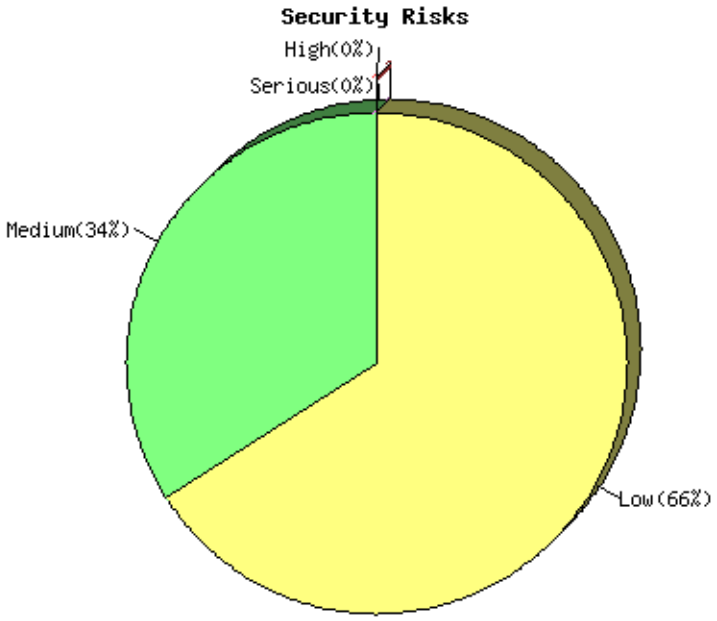
```
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/at
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/chage
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/crontab
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/dos
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/dumpreg
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/gpasswd
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/mh/msgchk
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/nwsfind
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/rcp
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/restorefont
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/restorepalette
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/restoretextmode
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/rlogin
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/rsh
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/bin/screen
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/sbin/traceroute
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/sbin/userhelper
-rwsr-xr-x <USERNAME>  staff
/home/<USERNAME>/sterling.<DOMAIN NAME>/usr/sbin/usernetctl
-rwsr-xr-x root     root     /usr/bin/ssh
-rwsr-xr-x root     root     /usr/libexec/pt_chown


# Checking setgid executables...

# Checking unusual file names...
```

```
# Looking for unusual device files...

# Checking symbolic links...

# Checking for writable directories...
--INFO-- [fsys008i] The following directories are world
writable:
/var/lib/cddb/
/var/lib/svgalib/
/var/spool/samba/

# Performing check of embedded pathnames...
--WARN-- [embed001w] Path `/proc/self/exe' contains
`/home/redding' which is
         not owned by root (owned by redding).
         Embedded references in: /bin/ash.static->/default(PATH)
                                 /bin/rpm->/default(PATH)
                                 /usr/bin/nc->/default(PATH)
                                 /usr/bin/rpm2cpio-
>/default(PATH)
                                 /usr/bin/statserial-
>/default(PATH)
--WARN-- [embed001w] Path `/proc/self/exe' contains
         `/home/redding/tiger-2.2.4p1' which is not owned by
root (owned by
         redding).
         Embedded references in: /bin/ash.static->/default(PATH)
                                 /bin/rpm->/default(PATH)
                                 /usr/bin/nc->/default(PATH)
                                 /usr/bin/rpm2cpio-
>/default(PATH)
                                 /usr/bin/statserial-
>/default(PATH)
--WARN-- [embed001w] Path `/proc/self/exe' contains
         `/home/redding/tiger-2.2.4p1/bin' which is not owned by
root (owned
         by redding).
         Embedded references in: /bin/ash.static->/default(PATH)
                                 /bin/rpm->/default(PATH)
                                 /usr/bin/nc->/default(PATH)
                                 /usr/bin/rpm2cpio-
>/default(PATH)
                                 /usr/bin/statserial-
>/default(PATH)
```

```
# Running Crack on password files...
--ERROR-- [init001e] Don't have required command CRACK.
--ERROR-- [init001e] Don't have required command REPORTER.
```

Appendix III: Nessus Report

Repartition of the level of the security problems :



List of open ports :

- ssh (22/tcp) (Security notes found)
- netbios-ssn (139/tcp)
- general/tcp (Security warnings found)
- netbios-ns (137/udp) (Security warnings found)
- general/udp (Security notes found)
- general/icmp (Security warnings found)

Information found on port ssh (22/tcp)
Remote SSH version : ssh-1.99-openssh_2.1.1

Warning found on port general/tcp
The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.

An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things.

Solution : Contact your vendor for a patch
Risk factor : Low

Information found on port general/tcp
Nmap found that this host is running Linux 2.1.122 - 2.2.14

Warning found on port netbios-ns (137/udp)
The following 5 NetBIOS names have been gathered :
FS = This is the computer name registered for workstation services by a WINS client.
FS = Computer name that is registered for the messenger service on a computer that is a WINS client.
FS
CLIENTXYZ = Workgroup / Domain name
CLIENTXYZ

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

Information found on port general/udp
For your information, here is the traceroute to XX.XX.XXX.XXX : XX.XX.XXX.XXX

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

Appendix IV: Nmap Port Scan

```
(The 65525 ports scanned but not shown below are in state:
closed)
Port       State       Service
22/tcp     open        ssh
25/tcp     open        smtp
111/tcp    open        sunrpc
113/tcp    open        auth
139/tcp    open        netbios-ssn
515/tcp    open        printer
934/tcp    open        unknown
1024/tcp   open        kdm
6000/tcp   open        X11
7101/tcp   open        unknown

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=1017298 (Good luck!)

Sequence numbers: 4A6D64C3 4A0A0913 4A2EFF97 49C9AED8 4A6E9168
4A439622
Remote operating system guess: Linux 2.1.122 - 2.2.14
OS Fingerprint:
TSeq(Class=RI%gcd=3%SI=F85D2)
T1(Resp=Y%DF=Y%W=7F53%ACK=S++%Flags=AS%Ops=MENNTNW)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=7F53%ACK=S++%Flags=AS%Ops=MENNTNW)
T4(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=C0%IPLEN=164%RIPTL=148%RID=E%RIPCK=E%UCK=E%UL
EN=134%DAT=E
)


Nmap run completed -- 1 IP address (1 host up) scanned in 43
seconds
```

Appendix V: Crack Report

```
---- passwords cracked as of Mon Jan  8 17:06:10 EST 2001 ----

Guessed redding [sushi]   [/tmp/es /bin/bash]

---- errors and warnings ----

---- done ----
```

Appendix VI: RedHat Linux 6.2 Vulnerabilities

Date	Name	Synopsis
19-Dec-2000	gnupg (RHSA-2000:131)	gnupg packages which repair security issues
19-Dec-2000	slocate (RHSA-2000:128)	new slocate packages close database parsing vulnerability
06-Dec-2000	ed (RHSA-2000:123)	ed editor /tmp vulnerability fixed
01-Dec-2000	tcsh (RHSA-2000:121-04)	Updated tcsh to fix symbolic link attack vulnerability
01-Dec-2000	PAM packages (RHSA-2000:120-04)	Updated PAM packages are now available for Red Hat Linux 6.x and 7.
27-Nov-2000	bind (RHSA-2000:107-04)	Updated bind packages fixing DoS attack available
27-Nov-2000	nss_ldap (RHSA-2000:024-03)	Updated nss_ldap packages are now available for Red Hat Linux 6.1, 6.2, and 7.
27-Nov-2000	apache, php, mod_perl, auth_ldap (RHSA-2000:088-05)	Updated apache, php, mod_perl, and auth_ldap packages are now available.
27-Nov-2000	usermode (RHSA-2000:075-08)	Updated usermode packages are now available for Red Hat Linux 6.x and 7
27-Nov-2000	gnorpm (RHSA-2000:072-08)	Updated gnorpm packages are available to fix security hole as well as other bugfixes
27-Nov-2000	pine, imap (RHSA-2000:102-05)	Updated pine and imap packages are available for Red Hat Linux 5.2, 6.x and 7
27-Nov-2000	modutils (RHSA-2000:108-05)	A new modutils package has been released to correctly enable safeguard measures.
27-Nov-2000	Netscape (RHSA-2000:109-05)	New Netscape packages are available that fix a buffer overflow
27-Nov-2000	bash (1.x) (RHSA-2000:117-01)	Updated bash (1.x) package to fix security problem.
26-Nov-2000	ncurses (RHSA-2000:115-02)	New ncurses packages fixing buffer overrun available
26-Nov-2000	ghostscript (RHSA-2000:114-04)	ghostscript package to fix usage of mktemp and improper LD_RUN_PATH
20-Nov-2000	joe (RHSA-2000:110-06)	Updated joe packages are available for Red Hat Linux 5.2, 6.x and 7.

02-Nov-2000	dump (RHSA-2000:100-02)	Red Hat 7.0 dump is being released for Red Hat 6.x and Red Hat 5.x
23-Oct-2000	ypbind (RHSA-2000:086-05)	local root exploit for ypbind fixed
20-Oct-2000	gnupg (RHSA-2000:089-04)	Updated gnupg packages are now available
18-Oct-2000	iputils (RHSA-2000:087-02)	Potential security problems in ping fixed
09-Oct-2000	usermode (RHSA-2000:075-05)	Updated usermode packages available
06-Oct-2000	tmpwatch (RHSA-2000:080-01)	local denial of service and root exploit fixed
06-Oct-2000	traceroute (RHSA-2000:078-02)	root exploit and several additional bugs in traceroute have been corrected
06-Oct-2000	esound (RHSA-2000:077-03)	race condition in esound fixed
04-Oct-2000	lpr (RHSA-2000:066-05)	lpr security, compatibility, and race conditions fixed.
18-Sep-2000	sysklogd (RHSA-2000:061-02)	syslog format vulnerability in klogd fixed
14-Sep-2000	xpdf (RHSA-2000:060-03)	security problem in temporary file and malicious URL fixes
11-Sep-2000	mgetty (RHSA-2000:059-02)	Updated mgetty packages are now available.
07-Sep-2000	glibc (RHSA-2000:057-04)	glibc vulnerabilities in ld.so, locale and gettext
30-Aug-2000	mailx and perl (RHSA-2000:048-03)	Updated perl and mailx package are now available.
29-Aug-2000	usermode (RHSA-2000:053-02)	Updated usermode packages are now available.
23-Aug-2000	XChat (RHSA-2000:055-03)	possible security hole with XChat passing URLs from IRC to a shell is fixed
18-Aug-2000	Netscape Packages (RHSA-2000:054-01)	New Netscape packages fix Java security hole
09-Aug-2000	RPM (RHEA-2000:051-01)	New version of rpm is now required to install Red Hat updates
07-Aug-2000	umb-scheme (RHSA-2000:047-03)	New umb-scheme packages are available that fix a problem with file permissions.
28-Jul-2000	Netscape (RHSA-2000:046-02)	New Netscape packages available to fix JPEG problem
26-Jul-2000	gpm (RHSA-2000:045-01)	gpm security flaws have been addressed
21-Jul-2000	PAM packages (RHSA-2000:044-02)	Updated pam packages are available for Red Hat Linux 6.x.
21-Jul-2000	nfs-utils (RHSA-2000:043-03)	Updated package for nfs-utils available
03-Jul-2000	imwheel (RHSA-2000:016-03)	Multiple local imwheel vulnerabilities resolved
03-Jul-2000	man (RHSA-2000:041-02)	man package's 'makewhatis' uses insecure

		handling of files in /tmp
23-Jun-2000	wu-ftpd (RHSA-2000:039-02)	wu-ftpd remote root exploit (SITE EXEC) fixed
21-Jun-2000	kernel-2.2.16-3 (RHSA-2000:037-05)	New Linux kernel fixes security bug
16-Jun-2000	Emacs Packages (RHSA-2000:036-02)	New Emacs packages available
16-Jun-2000	Kerberos 5 Packages (RHSA-2000:025-13)	Updated Kerberos 5 packages are now available.
19-May-2000	Netscape 4.73 (RHSA-2000:028-02)	Netscape 4.73 available.
18-May-2000	Kerberos 5 packages (RHSA-2000:025-07)	Updated Kerberos 5 packages are now available for Red Hat Linux.
26-April-2000	piranha-0.4.14-1 (RHSA-2000:014-16)	Piranha web GUI exposure security fix
21-April-2000	imwheel-0.9.8-1 (RHSA-2000:016-02)	imwheel buffer overflow fix
21-April-2000	openldap-1.2.9-6 (RHSA-2000:012-05)	New openldap package to fix symlink vulnerability
12-April-2000	gpm-1.19.1-1 (RHSA-2000:009-02)	New gpm package to fix gpm-root privilege problem
30-Mar-00	ircii-4.4M-1 (RHSA-2000:008-01)	New ircii packages available

Last Updated: July 25th, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**