



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

# Linux Red Hat 7.1 Security Assessment

## GIAC Enterprises

SANS Practicum, DC May 2001 Conference

By: Bente Petersen

Version #: 1.6d

Date: July 25, 2001

## Table of Contents

1	Executive Summary .....	4
1.1	Background.....	5
1.2	Scope.....	5
1.3	Test Environment.....	5
1.4	Involved personnel.....	6
2	Network Environment.....	7
2.1	Hardware/Software Specifications.....	7
3	Analysis of the Computer System.....	8
3.1	Boot Analysis .....	8
3.1.1	BIOS Password .....	8
3.1.2	Reboot Protection .....	8
3.1.3	LILO password .....	9
3.2	Network Cards.....	9
3.3	Configuration.....	10
3.3.1	Service .....	10
3.3.2	Modified Binary Files.....	13
3.3.3	File Setup.....	14
3.3.4	Default File Permissions .....	15
3.3.5	Validation of SUID files .....	15
3.3.6	Trusted hosts .....	16
3.3.7	System Accounts.....	17
3.3.8	General Security Issues .....	17
4	Operating System and Software Maintenance.....	18
4.1	Security Patches .....	18
4.2	Installed Third-Party Software.....	19
4.3	Anti-Virus Software.....	19
5	Data Protection .....	20
5.1	Password Protection.....	20
5.2	Protection of Remote Logon Sessions.....	20
5.3	Tools to Ensure Data Integrity .....	21
6	Logging.....	23
6.1	Central syslog Server .....	23
6.2	Synchronized Clocks .....	24
7	Administrative Practices .....	25
7.1	Security Awareness.....	25
7.2	Upgrades and Security Patches .....	26
7.3	Inventory Lists.....	26
7.4	Log Files .....	26
7.5	Access to root Account.....	27
7.6	Test Environment.....	27
8	Physical Security .....	29
9	Corporate Security Policies .....	30
9.1	Password Policies.....	30
9.1.1	Root Password Maintenance.....	31

9.2	Backup Policies .....	32
9.2.1	Recommendations.....	32
9.3	Disaster Recovery/Business Continuity .....	32
9.4	Incident Response Plan.....	33
9.4.1	Evidence Collection.....	34
9.5	Termination of Employees .....	34
9.5.1	Current Environment.....	34
9.5.2	Testing .....	34
9.5.3	Recommendations.....	35
10	Prioritized List of Issues .....	36
11	A Prioritized List of Recommended Fixes .....	38
12	List of References.....	42
	Appendix A.....	43
	Appendix B .....	81

© SANS Institute 2000 - 2002, Author retains full rights

# 1 Executive Summary

GIAC Enterprises is currently expanding its IT environment. The company is growing fast and the need for a larger IT infrastructure is significant. The management recently decided to lease a DSL connection to connect the company to the Internet, and wanted to ensure that this connection will be as secure as possible. The host Idunn will be functioning as a router/firewall, and the IT management engaged the Internal Audit department to perform an analysis of the host before it will be configured. In addition, management wanted an analysis of the overall security awareness in the organization.

Several tests were done on Idunn to reveal any security flaws and the following high risk issues were detected:

The physical security of the server and its location is of great concern. A new secure computer room is being constructed, but the server needs to be secured in the mean time physically and via software/operating system configurations. Furthermore, the operating system on the server has not been upgraded to ensure that the latest security holes have been closed, and unnecessary services are running leaving potential access paths for intruders.

On Idunn several users with privileged access rights have enabled user accounts even though they have either left the company or moved to other positions within the company. Lack of control and routines for disabling user accounts can cause serious security breaches. Resent studies has shown that a high number of attacks come from within the organization.

The procedures for connecting to servers remotely should be changed immediately since the current methods allow for transferring logon information such as username and password across the network in clear-text. A malicious user may obtain this information by installing a sniffer tool on one of the systems in the network. SSH or another secure method should be implemented and used for all remote connections to the servers from within the internal network or from outside the network via dial-up or DLS connections.

In general the awareness of security in the IT department needs to be enhanced. The System Administrators should be educated in security related issues, and be given time to keep track of the latest security incidents.

Furthermore, there are no policies and procedures for security related issues in the organization and it is important that these will be developed as soon as possible. The policies and procedures should include topics such as backup, incident response, business continuity, passwords, user management etc. Lack of formal policies and procedures at the corporate level can result in security issues not being addressed properly or not at all. Furthermore, policies and procedures can function as a learning tool for new employees and should be made available for all employees at all times.

## 1.1 Background

GIAC Enterprises is a fast growing company which is expanding its current network environment. The company recently obtained a DSL connection which will allow the company's hosts to access the Internet as well as allow for the implementation of a web server which can be accessed by the company's customers. The company would like to expand its network gradually and at minimal cost in the first phase. All servers will therefore be running Linux and use open source software solutions.

## 1.2 Scope

The scope of this project was to ensure that the operating system on the host Idunn is set up as secure as possible. The host will function as a router connecting the internal network to the Internet. The scope of this audit includes a security assessment of the operating system, hardware and physical security as well as security policies and procedures in general. GIAC Enterprises want to ensure that the network is as secure as possible before connecting to the Internet. The security assessment of the host will therefore be performed before it is connected to the Internet. A firewall software is planned to be installed on the server. An audit of firewall rules is beyond the scope of this audit. This will be covered in another audit project.

The report is divided in two main parts. Part one will give a detailed analysis of the security assessment performed on Idunn and what actions need to be taken in order to apply the proper security without hindering the functionality of the host in its future environment. Part two will describe the current procedures and policies implemented in the organization related to the IT environment, and suggested enhancements.

## 1.3 Test Environment

The testing was performed by the Internal Audit IT team. Several tools and commands were run on the server and several files were extracted for analysis. Vulnerability scanning tools were run from an audit laptop connected to the server over the internal network. Since the files extracted, output of commands and reports from the tools as well as this report contain highly sensitive information it was stored on the laptop computer and encrypted with PGP. The deliverable is a PGP encrypted CD containing this report and complete reports of test results and output of commands. The pass-phrase can be obtained from the Internal Audit team.

The following tools<sup>1</sup> were used to perform the audit:

---

<sup>1</sup> Links to all software are listed in [Appendix B](#).

- Tiger** - The system security scanner was run on the server and used to detect insecurities allowing users on the local host to gain unauthorized privileges. Tiger is a freeware developed by Texas A&M. The scanner is not kept up to date with the latest Linux versions so additional security checks will need to be done in order to obtain a complete security assessment. However, the scanner will detect a fair amount of vulnerabilities.
- Nmap**- The port scanner was run from a laptop connected to the internal network and it detected the ports currently set to open on Idunn.
- Crack**- The password file was checked by the Crack application to detect any easily guessable passwords. Crack was developed by Alec D. E. Muffet.

In addition several files were downloaded and analyzed and several commands were run. These will be described in detail where the vulnerabilities are discussed.

## 1.4 Involved personnel

The audit was conducted by Bente Petersen, Internal Audit, IT group, and supervised by John Nilsen, Manager of the Internal Audit group. The audit was conducted July 16<sup>th</sup> - July 20<sup>th</sup>, 2001.

The audit team met with the following personnel:

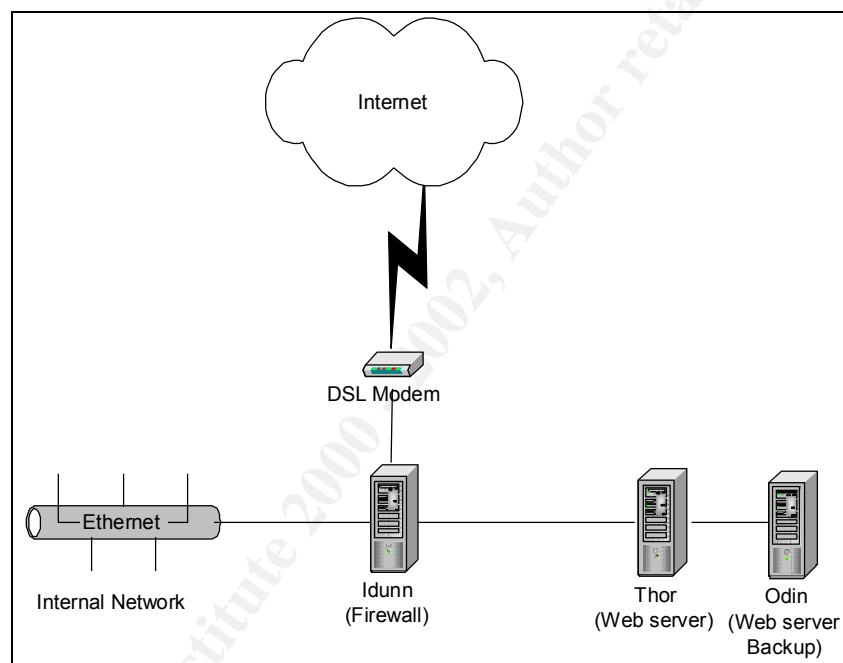
- Ellen Olsen, HR Representative
- Lisa Hansen, IT Director
- Ron Porter, System Administrator
- Matthew Pinetree, Junior System Administrator

© SANS Institute 2000 - 2002, Author retains full rights.

## 2 Network Environment

The host named Idunn was previously used as a test server for the web developers who were primarily outside consultants. For various business reasons the System Administrators were unable to perform the recommended approach which was to rebuild the system from scratch before implementing it as a router.

Idunn will function as the internal network's interface to the Internet and will have firewall software installed. The host has 3 interfaces; 1 for connection to the Internet via DSL, one for connecting to the DMZ environment where the web servers reside and the third connecting to the internal network. The diagram below describes the environment where Idunn will function.



### 2.1 Hardware/Software Specifications

The server has the following hardware specifications:

- Athlon K7V Motherboard
- AMD Athlon K7 – 750 MHz
- 256 Mb Memory
- 1 10GB Western Digital HD
- 2 LinkSys Etherfast Network cards
- 1 3com EtherLink Network Card

The server has the following operating system specifications:

- Red Hat 7.1



## 3 Analysis of the Computer System

### 3.1 Boot Analysis

#### 3.1.1 BIOS Password

The BIOS password was not set on the server. A BIOS password can prevent unauthorized users from changing the CMOS settings on the system. This password should follow general password setting rules, see chapter 9.1, and should by no means be the same as the root password on the system since there are several programs available for cracking BIOS passwords. The BIOS password can be set by entering the system's BIOS settings when booting the system.

#### 3.1.2 Reboot Protection

The `init` process is the first process started on Linux systems. Red Hat and many other distributions of Linux use a System V based `init` process which is based on different runlevels. A runlevel are different modes of running the system such as single user mode, multiuser mode etc. The file called `/etc/inittab` controls the settings for the `init` process. One of the default setting for this process controls whether rebooting from the console using the "Control + Alt + Del" keys is allowed. A review of the `/etc/inittab` file on Idunn showed that this feature is allowed on the server.

The audit team recommends disabling this setting since users with access to reboot a system to single user mode may change security settings and configuration of the system. To disable this setting edit the `/etc/inittab` file and replace the line:

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

with the line:

```
#ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

Also, by default users do not have to enter the root password to enter single user mode when rebooting. Users with access to reboot a system to single user mode may change security settings and configuration on the system.

To disable this feature replace the following line in the `/etc/inittab` file after the `si::sysinit...` entry:

```
~:S:wait:/sbin/sulogin
```

These settings are displayed in more detail in Appendix A, on [page 49](#).

### 3.1.3 LILO password

Analyzing the `/etc/lilo.conf` file revealed that the LILO password is not set on the server.

Since the server is located in a non-secure environment, see chapter 8, the Audit team recommends that the LILO password be set to protect the server in addition to the root password when booting in single user mode. The password is stored in the `/etc/lilo.conf` file in clear text so the permissions of the file should be set to 600. The password should not be the same as the BIOS or root passwords, and should follow general password setting policies, see chapter 9.1.

To set the LILO password edit the following parameters in the `/etc/lilo.conf` file:

```
password = newpassword
restricted
```

The `/etc/lilo.conf` file should only be accessible by root, and to ensure this the following command should be run:

```
chmod 600 /etc/lilo.conf
```

To make the changes to the `/etc/lilo.conf` file take effect, run the following command:

```
/sbin/lilo
```

## 3.2 Network Cards

The server will function as the gateway for traffic coming in and going out of the internal network and will therefore be a prime target for the installation of network sniffers. Since the server was previously used as a test box with no real control of the various types of software installed, a test was conducted to ensure that the network cards were not set in promiscuous mode and allowing for sniffing all traffic passing on the network.

The command `ifconfig` was run on the server and revealed that none of the network cards were in promiscuous mode. The output of this command can be seen in Appendix A, [page 48](#).

The Audit team recommends that this command is run on a regular basis to detect if a sniffer is installed.

## 3.3 Configuration

### 3.3.1 Service

To discover which services were running on Idunn the port scanning tool Nmap was used to see which ports were open and listening. Most services run on predefined ports and this makes it easier for an intruder to know what services are running on the system. Nmap was run using the command line option (the Audit team decided not to use the GUI version called Nmapfe).

Nmap was run with several options to get the most complete scan. The output of the various scans are in Appendix A, [page 65](#).

- Nmap TCP SYNscan:  
This option sends the first SYN packet in the three-way handshake. If the service is listening on this port a SYN/ACK packet will be returned. Nmap will not finish the three-way handshake.
- Nmap TCP connect scan:  
Performs a full TCP connect() port scan. This is the only option available for users running the tool without root privileges.
- Nmap UDP scan:  
A 0-byte UDP packet is sent to each port on the target machine. If the target returns an ICMP port unreachable the port is closed.

The services listed in the table below were detected with the Nmap tool. The table also shows the services started in the `xinetd.conf` file. The `xinetd.conf` file can be seen in Appendix A, [page 50](#).

© SANS Institute 2000 - 2002. Author retains full rights.

Services	Port	xinetd.conf	Description
ftp	TCP 21	X	The File Transfer Protocol (FTP) is used to transfer complete files between systems and was the de-facto file transfer method until HTTP was developed. FTP will authenticate users logging in to the service, but the username and password is sent in clear text. There are several vulnerabilities reported on FTP servers and many of these have lead to compromise of the root account.
ssh	TCP 22	X	SSH was created to be a secure replacement for the r-commands running on UNIX systems such as rlogin. SSH will protect data through various encryption algorithms and also includes several authentication methods.
telnet	TCP 23	X	Telnet allows for logging on to a remote computer on the Internet and provides a “virtual terminal” on the remote computer. Telnet displays all information in clear-text and is therefore a risk for malicious users running sniffer programs on the network. Telnet is also susceptible to hijacking attacks where an attacker will take control of the session during the logon procedure. Telnet requires that the user enters the username and password upon connection, but this information is also transmitted in clear-text.
smtp	TCP 25		The Simple Mail Transfer Protocol (SMTP) allows for transfer of electronic mail between systems. The mail program used most on UNIX system is sendmail <sup>2</sup> . There are several known security vulnerabilities in sendmail. “One of the main reasons for sendmail’s problems is its all-in-one design. The programs is extremely complicated, runs as superuser, freely accepts connections from any computer on the Internet, and has a rich command language.” <sup>3</sup>
finger	TCP 79		Finger is a program which allows for displaying personal information on the server and over the network. It will also display a list of all users on the system, and this information can be exploited by an intruder.
http	TCP 80	X	The Hypertext Transfer Protocol (HTTP) is used to request and receive documents from servers on WWW.
sunrpc	TCP 111, UDP 111		The Sun RPC portmapper programs is used to dynamically assign the TCP and UDP ports used for RPC (Remote Procedure Calls) programs. The portmapper allows any

<sup>2</sup> Developed at the University of California at Berkeley.

<sup>3</sup> Garfinkel & Spafford, Practical UNIX & Internet Security

Services	Port	xinetd.conf	Description
			network client to communicate with any RPC server and assumes that security will be handled by the server itself.
https	TCP 443		HTTPS is the secure version of the HTTP protocol and should be used on sensitive web pages such as pages handling payment etc.
login	TCP 513	X	The rlogin command provides a services similar to Telnet, but rlogin automatically transfers the username at the start of the connection, and allows for login without the use of passwords if the connection is coming from a trusted host <sup>4</sup> . The rlogin service is only for UNIX to UNIX connections. To connect to hosts running other OS the user must run Telnet.
shell	TCP 514	X	The rsh shell is similar to the rlogin service described above. However, rsh only allow the user to run a single command on the remote system, and does not provide the login functionality. The rsh service is only for UNIX to UNIX connections. To connect to hosts running other OS the user must run Telnet.
X11	TCP 6000		X Windows is a network-based window system which allows users to “share” their display to other machines. The security model is fairly simple allowing either all or nothing. So when the remote user connects he/she will have complete control over the display, and can also take over the mouse or the keyboard. The remote user will have the capability to read all commands entered by the local user.
unknown	UDP 907		

<sup>4</sup> Trusted hosts [see chapter 3.3.6](#)

Idunn should only be running the firewall services and all unnecessary services should be removed. The audit team recommends removing the FTP service. The service will not be used on this server and leaving it on the server may cause security risks. Since the service will not be used it will most likely not be maintained and upgraded when new security patches become available for the FTP service.

The finger service should be disabled. The information displayed by this service can be used in a social engineering attack by an intruder.

Idunn will not run as a mail server so the smtp service should be disabled.

The telnet, login and shell services should be disabled. According to the System Administrators Telnet is currently used by the Administrators for connecting to the server remotely. SSH is installed on the server, but not configured and not used by the System Administrators. SSH will allow for the same service as Telnet, but will encrypt the communication session.

HTTPS should be disabled on Idunn since this server will not run as a web server. Even though this is a secure service any unnecessary services should be disabled.

X Windows should also be disabled on Idunn. All remote connections should be done via SSH. If X Windows is needed for administrative purposes it should be forwarded by SSH.

The UDP service on port 907 was listed as unknown by nmap. To further investigate this service the netstat command was run on the Idunn server. This did not reveal the type of service, and the report can be viewed on [page 46](#). The Audit team then used the tool `lsOf`<sup>5</sup> and the tool revealed that the service is an rcp service which should be disabled. The complete output of the `lsOf` command is on [page 47](#).

### **3.3.2 Modified Binary Files**

The server was left unattended in an unsafe area from July 2<sup>nd</sup> until July 15<sup>th</sup> so checks were performed to ensure that no binaries had been edited in this time period. The `touch` command was run to create a file with the time stamp of July 1<sup>st</sup>, then the `find` command was run to detect files that were newer than this file. The complete command sequence and output can be seen on [page 43](#).

---

<sup>5</sup> `lsOf` is included in the Red Hat 7.1 package.

The following files had been edited:

Filename	Edit Date
/usr/programs/security/tiger/tiger-2.2.4p1/bin/getpermit	Thu 12 Jul 2001 11:28:29 PM
/usr/programs/security/tiger/tiger-2.2.4p1/bin/snefru	Thu 12 Jul 2001 11:28:29 PM
/usr/programs/security/tiger/tiger-2.2.4p1/bin/realpath	Thu 12 Jul 2001 11:28:28 PM
/usr/programs/security/tiger/tiger-2.2.4p1/bin/md5	Thu 12 Jul 2001 11:28:28 PM
/usr/programs/security/tiger/tiger-2.2.4p1/bin/testsuid	Thu 12 Jul 2001 11:28:28 PM
/root/simplefw	Thu 12 Jul 2001 11:28:28 PM

The result was discussed with the System Administrators and they could verify that the Tiger application had been installed and run in this time period. The simplefw file is a text file created by one of the System Administrators and will be removed shortly. No issues were detected during the review of the binary files.

### 3.3.3 File Setup

Tiger was used to perform an assessment of potential local security problems. Selections of the report from this scan can be found in Appendix A, [page 70](#). The entries given a warning or fail by Tiger were run through the `tigexp` utility which is part of the Tiger package, to obtain more information about the issues.

The issues noted in the Tiger report are listed in the table below. Only warnings, fails and scan errors are listed:

Selecting the links will take you to the specific entries in the Tiger report on page 70.

Checks Performed by Tiger	Test Result	Description
<a href="#">Password/group files</a>	Warning	Several system and application accounts have been disabled, however they still have valid shells.
<a href="#">PATH (root)</a>	Warning	Several commands set up in root's PATH were not owned by root.
<a href="#">anonymous FTP</a>	Error	Scan failed.
<a href="#">cron entries and inetd</a>	Fail	Several of the services installed are not assigned to the correct port.
<a href="#">Check of file system permissions and owners</a>	Warning/Fail	Several directories are world writeable and several user created files were unowned.
<a href="#">System specific checks</a>	Warning	Several of the executables have relative pathnames.
<a href="#">Embedded pathnames</a>	Warning	Several embedded pathnames were not owned by root.

Even though the login IDs listed in the Tiger report are disabled in the `/etc/passwd` file the login shell for the login IDs are still valid shells (see `/etc/shells` page 55). It is possible to

enable the login ID with a valid shell. To avoid this problem the login shell should be disabled on the listed accounts. This can be done in the `/etc/passwd` file by changing the `/bin/bash` entries to `/bin/false`. For examples see the entries for the user ID Apache, named and portmapper in the `/etc/passwd` file.

It is recommended to use full pathnames in shell scripts or at least ensure that the scripts' default path does not include any world-writeable or otherwise unsafe directories. Relative pathnames always start interpretation from the current directory of the process referencing the item, while full pathnames always start from the root directory.

### **3.3.4 Default File Permissions**

Currently the sticky bit is not set on any directories on Idunn. If the sticky bit is set users with write permissions to a directory can delete or edit files owned by other users within this directory. The Audit team recommends setting the sticky bit on the `/tmp` and `/usr/tmp` directories since all users can add and edit files and directories within these directories. The following command will set the sticky bit:

```
chmod +t /tmp /usr/tmp
```

The default permissions for files and directories should be set to 077 to prevent anyone but the owner to have access to the files and directories. To enable this setting, add the following entries to the users' `.profile` files.

```
umask 077
```

### **3.3.5 Validation of SUID files**

A complete listing of SUID and SGID files were obtained from the Idunn system by running the `find` command. SUID is used when it is desirable to execute a single command with the rights and privileges of another user. The UID of a process executing a SUID program will be changed to the UID of the owner of the program. The GID of a process executing a SGID program will have its GID set to the program's GID. SUID and SGID programs are often not coded correctly and errors in the programs may cause a change in user identification and privileges. Therefore unnecessary SUID and SGID programs should be avoided. On Linux systems SUID or SGID scripts are not supported unless they are a compiled binary <sup>6</sup>.

On Idunn several such programs were found, and they are listed in Appendix A, on [page 44](#). There may be business reasons for keeping some of these files. The Audit team recommends removing the files listed below.

---

<sup>6</sup> Hatch, Lee, Kurtz, Hacking Linux Exposed: Linux Security Secrets & Solutions



File Name	Access Rights	Owner
/usr/bin/rcp	-rwsr-xr-x	root
/usr/bin/rlogin	-rwsr-xr-x	root
/usr/bin/rsh	-rwsr-xr-x	root
/usr/bin/uucp	-r-sr-xr-x	uucp
/usr/bin/uuname	-r-sr-sr-x	uucp
/usr/bin/uustat	-r-sr-xr-x	uucp
/usr/bin/uux	-r-sr-xr-x	uucp
/usr/sbin/sendmail	-r-sr-xr-x	root

All RCP services can be the target of intrusion attacks and should be disabled. This included the rcp, rlogin and rsh services.

UUCP is the UNIX-to-UNIX Copy system and is a collection of programs providing simple networking services for UNIX systems. The service allows files and electronic mail to be transferred and execution of remote commands. UUCP also allows for connection to Usenet. UUCP comes with several security features, but can compromise system security if not configured correctly. The service is not running on Idunn (see nmap scan Appendix A, page 65), so the UUCP SUID programs be removed. This includes the copy command `uucp`, the remote execution command `uux` as well as other UUCP commands such as `uustat` and `uuname`.

The sendmail service is not needed on this server, so the file listed in the table should be removed.

### 3.3.6 Trusted hosts

Hosts running in small environment can be set up in the `/etc/hosts.equiv` file to establish a trusted relationship. If one host trusts another host, then any user who has the same username on both hosts can logon from the trusted host to the other computer without a password. Trusted relationships are implemented on servers on the internal network at GIAC Enterprises, and the System Administrators are considering the same setup for Idunn. The Audit team strongly recommends not to employ trusted relationships on Idunn, since this is a very critical server. Trusted relationships can cause a security vulnerability because you can not always trust the remote hosts and the users on the hosts. Also, a malicious user can unplug a system from the network and set up his/her own system with the same host name, IP address and user names and will then have automatic access to all trusting hosts.

The Audit team recommends implementing SSH on all servers and use it as the standard for remote connections, see chapter 5.2 for a more detailed discussion on SSH.

### 3.3.7 System Accounts

The following system accounts were listed in the `/etc/passwd` file, which can be viewed in Appendix A on page 54. These services should not be running on Idunn and the accounts should be disabled by entering NP in the password field. Several of these services are subject to attacks from malicious users, and since these accounts will not be used they will most likely not be maintained by the System Administrators.

User account	Service using account
mail	Sendmail service
news	NNTP service
uucp	UUCP service
games	Various games
gopher	Gopher service
ftp	FTP server
rpc	RPC Portmapper
apache	WWW server
named	DNS service
mysql	Database server

To enhance security logging, the Logcheck tool, see chapter 7.3, page 25, should be configured to alarm the System Administrators if someone tries to logon using the disabled system accounts.

### 3.3.8 General Security Issues

All shells used by the users should be listed in the `/etc/shells` file. The program `chsh` which allows users to change their shell checks the `/etc/shells` file to determine which files are valid. If the `/etc/shells` file does not exist, a user can select any shell. The review of the `/etc/shells` file did not reveal invalid shells which could have been a potential threat to the system. The content of the file can be seen in Appendix A, [page 54](#).

Currently there are no limit for core dumps on the system. Since the server was previously used for testing purposes the developers found the use of core files valuable for debugging reasons. The server will have a different functionality now, and the Audit team recommends changing the settings so daemons do not dump core. If a daemon crashes the core files may contain information which can be misused by a malicious user. The following command should be included in the boot script to prevent core dumps:

```
ulimit -c 0
```

## 4 Operating System and Software Maintenance

### 4.1 Security Patches

The operating system on the server is Red Hat 7.1. No patches has been installed since the initial installation and this was confirmed during interviews with the System Administrators. Several vulnerabilities have been discovered on this distribution of Red Hat, and it is recommended that GIAC Enterprises install security patches as soon as they are released. Resent patches can be found at Red Hat's Errata page: <http://www.redhat.com/support/errata/rh71-errata.html>.

The following patches were released as of July 17<sup>th</sup>, 2001, and were selected in accordance with the recommended setup of the server Idunn. These patches should be installed as soon as possible:

Date	Name	Synopsis
2001-04-18	up2date (RHBA-2001-048)	New Update Agent with many fixes and enhanced functionality available.
2001-04-30	kdelibs (RHSA-2001-059)	Update of the kdelibs packages, correction of security problem and memory leaks.
2001-05-02	losetup (RHSA-2001-058)	Updated mount package.
2001-05-09	minicom (RHSA-2001-067)	Updated minicom packages.
2001-05-16	krb5 (RHSA-2001-060)	Updated Kerberos 5 packages.
2001-06-06	ypbind (RHBA-2001-076)	New ypbind packages.
2001-06-07	gnupg (RHSA-2001-073)	Updated GnuPG packages.
2001-06-21	kernel (RHSA-2001-084)	Correction of FTP iptables vulnerability in 2.4 kernel and general bug fixes.
2001-06-22	SysVinit (RHBA-2001-085)	New SysVinit package to fix hangs on serial console.
2001-06-22	Xfree86 (RHSA-2001-071)	New updated Xfree86 packages.
2001-07-06	xinetd (RHSA-2001-092)	Updated xinetd package.
2001-07-16	(RHSA-2001-095)	New util-linux packages which corrects vipw permission problems.

A policy for periodically checking for applicable new releases of OS patches should be implemented. This is addressed in further detail in chapter 7.2.

## 4.2 Installed Third-Party Software

Third-party software is software packages which are not included in the native operating system even though they may have been included on the installation media. Most of the third-party software installed on Idunn is not needed for the system to function as a router. The services installed is listed in the `/etc/services` file in Appendix A, [page 56](#).

The following unnecessary software packages were installed on Idunn:

Software	Description	Recommended Action
Apache	This is one of the most popular web servers on the Internet today. Apache is included with most Linux distributions.	Remove the application immediately.
Sendmail	A mail transfer agent which is a program responsible for routing e-mail between machines.	Remove the application immediately.
Bind	The standard Unix implementation of DNS <sup>7</sup> . DNS is a distributed networked-based naming service.	Remove the application immediately.

None of the software packages listed above is needed on Idunn and should therefore be removed immediately. Several of them have known security flaws that can be exploited by a potential attacker. Since none of these applications will be maintained by the System Administrator group the latest security patches will most likely not be installed, thus leaving potential open holes in the system and making the system vulnerable to compromise or denial of service attacks.

## 4.3 Anti-Virus Software

Linux and UNIX systems are not very susceptible to viruses since an essential component of the architecture of these systems are a clear definition of users, groups and file ownership and permissions. This is not the fact for Windows and Macintosh platforms where every program running has full control of the operating system. The software packages on Windows and Macintosh systems can manipulate data in other software packages and thus facilitate spreading of viruses. On Linux and UNIX systems a virus can only affect the user running the particular program and therefore no spreading is possible except when running as root, but spreading to other systems are not possible.

Idunn will not pass any data to Windows and Macintosh platforms and therefore a virus scanning tool running on Linux systems and checking for Windows/Macintosh viruses is not necessary. However, several worms which attack network services have been spread from Linux/UNIX systems, and the System Administrators should implement a routine for keeping up-to-date with the latest security breaches. See chapter 7.1.<sup>8</sup>

<sup>7</sup> Bind was originally developed by Eric Allman at the University of California at Berkeley.

<sup>8</sup>This information was found in Hatch, Lee, Kurtz: Hacing Linux Exposed: Linux Security Secrets & Solutions

## 5 Data Protection

### 5.1 Password Protection

On Idunn user passwords are stored in the `/etc/shadow` file which is encrypted with a `crypt()` function using the MD5 algorithm. MD5 allows for passwords of any length so the users can type passphrases instead of a short password and also accepts special characters such as `./$` etc.

The password cracking tool `crack` was run on the test box to check for password integrity. Certain modifications were needed to make `crack` check for MD5 hashed passwords since `crack` is configured for DES encrypted passwords by default. The `/etc/passwd` and the `/etc/shadow` files were copied from Idunn to the test box and merged into a password-like file which was taken as input to `crack`. `crack` ran for 3 days and 60 % of the passwords were guessed successfully.

The Audit team recommends that password policies and procedures be implemented, see chapter 9.1. Furthermore, a proactive password checker should be implemented to ensure that good passwords are selected by the users. One recommended tool is `passwd+`<sup>9</sup> written by Matthew Bishop, which will ensure that the passwords have a specific length, are mixed case, are not found in a dictionary, are based on user or site information etc.

### 5.2 Protection of Remote Logon Sessions

SSH is installed on the server but currently not used. System Administrators are logging on to the servers remotely using `telnet` which displays all traffic in clear-text. If a sniffer should be installed on the network, the malicious user will be able to see all traffic going to and from the server.

The Audit team recommends that SSH be configured properly and be used as the standard by the System Administrators when connecting to this server and other servers on the network from within the internal network or remotely from home etc. SSH provides full end-to-end encryption which will block sniffing attacks and prevent session hijacking attacks.

SSH should replace any `rlogin`, `rcp` and `rsh` services. It provides encryption for the whole communication session and supports several methods for authentication of users.<sup>10</sup>

SSH supports the user of banners, and since SSH will be the single point of remote communication it is recommended that a banner be configured using the banner feature in SSH.

---

<sup>9</sup> The tool can be downloaded from <ftp://nob.cs.ucdavis.edu/pub/sec-tools/passwd+beta.tar>

<sup>10</sup> Steve Acheson, SANS Unix Security 6.3 Topics in UNIX Security, SSH.

It is important that the banner includes information such as a warning that access to the system is for authorized personnel only, and everyone violating this may be prosecuted. If a proper warning is not implemented in a banner the organization may have problems prosecuting an intruder if a case should go to court.

### 5.3 Tools to Ensure Data Integrity

“Computer forensics boils down to a “game” of what changed and when. File Integrity Assessment tools can be priceless.”<sup>11</sup> (Hal Pomeranz). An attacker who has broken into a system will most likely change a number of files on the system. The time of modification can easily be changed by the attacker so comparing file stamps on files is not a sufficient method.

The Red Hat Package Manager (rpm) utility was used to check for changes of the system files since installation of Red Hat on Idunn, see report in Appendix A, [page 74](#). rpm created a database on the system when the Red Hat packages were installed. The database includes information such as MD5 checksums, UID, GID, mode, size etc. of the installed files. The report shows that the size, MD5 checksum, mode, time stamp and group information have been changed for several files. Most of these files were configuration files such as `/etc/ppp/pppoe.conf`, `/etc/xinetd.conf` and `/etc/syslog.conf`. No unusual file changes was detected.

For continued and more granular checks of file integrity on Idunn, the Audit team recommends running a tool using MD5 checksums which are the strongest and therefore most secure checksums currently available. A recommended tool is Tripwire which allows the System Administrator to specify what files and directories to be monitored. File contents of these files are checksummed and the checksum and other characteristics such as inode information will generate a signature for the individual file. All signatures are stored in a database. The database and the config files should be stored on read-only media to avoid anyone tampering with files, and the temp files generated by the tool should be stored in a protected area. It is recommended that Tripwire is run on a weekly basis to ensure that the files on the system have not been changed and corresponds with the signatures stored in the database. The tool should not be run over the network. Tripwire should be run on Idunn the first time before it is connected to the Internet to ensure that no-one is tampering with the files before the database is created.

At a minimum the following files should be checked by Tripwire since they are the ones most often compromised by attackers<sup>12</sup>:

---

<sup>11</sup> Hal Pomeranz, Track 6 – LevelTwo Securing UNIX, 6.3 Topics in UNIX Security p. 131.

<sup>12</sup> Brian Hatch, James Lee, George Kurtz; Hacking Exposed: Linux Security Secrets & Solutions, page 46.

- /etc/xinetd.conf
- /etc/ftpaccess
- /etc/host.conf
- /etc/sysconfig/network
- /etc/ld.so.conf/
- /etc/nsswitch.conf
- /etc/cron.daily/\*
- /var/spool/cron/root
- /bin/su
- /bin/ping
- /usr/bin/chfn
- /sbin/dump
- /sbin/netreport
- /usr/bin/lpr
- /usr/bin/write
- /usr/bin/man

© SANS Institute 2000 - 2002, Author retains full rights

## 6 Logging

Idunn is set to run the default logging settings in Red Hat 7.1, the syslogd package which uses the `syslogd` daemon for system messages and `klogd` daemon for kernel messages. The log-files are currently kept locally on the host. The `/etc/syslog.conf` file is displayed in Appendix A, [page 53](#). The default log settings are not sufficient for a critical server such as Idunn, and the Audit team recommends to optimize the syslog settings by adding the following lines to the `/etc/syslog.conf` file:

```
*.warn;*.err      /var/log/syslog  
kern.*            /var/log/kernel
```

The new log files need to be created for the logging to take effect. The following commands will create the log files with the appropriate permission settings:

```
touch /var/log/syslog /var/log/kernel  
chmod 700 /var/log/syslog /var/log/kernel
```

For routines of checking log files see chapter 7.4.

### 6.1 Central syslog Server

Currently all logs are written to a directory locally on the server. The audit team recommends implementing a syslog server which will receive and store all logs from all servers. If the local server is hacked by an intruder, he/she will not have immediate access to modify the logs and must break into another server to delete potential traces.

The syslog server should be as secure as possible and only running the syslog service and SSH for remote administration purposes. All syslog daemons on the servers should send the syslog server periodic messages to indicate that they are alive and have not been accidentally or intentionally killed. The syslog server should be configured in such a way that System Administrators are notified via pager and/or e-mail if a syslog daemon goes down on any of the servers. Furthermore, to prevent denial of services attacks from an outside network ipchains on the syslog server must be configured to only allow packets from the local network through the syslog port (UDP 514). Denial of service attacks coming from a local server can not be prevented however since the service must be open to the local hosts.



## 6.2 Synchronized Clocks

There are no utilities implemented for ensuring that the clocks on all the servers at GIAC Enterprises are synchronized. If the clocks are not synchronized, investigating a break-in can be very difficult.

The Audit team recommends that the Network Time Protocol (NTP) be implemented and configured. This protocol was designed for use in large and smaller networks to ensure accurate synchronization of system clocks. It provides accuracies typically within a millisecond on LANs. Available over the Internet are several primary (Stratum 1), secondary (Stratum 2) and third-level (Stratum 3) NTP servers. GIAC Enterprises' NTP server should synchronize to a Stratum 2 or 3 server. Furthermore, they should set up 2 NTP servers for redundancy to synchronize with a Stratum 2 server, and have all network servers synchronizing with these NTP servers.

© SANS Institute 2000 - 2002, Author retains full rights.

## 7 Administrative Practices

### 7.1 Security Awareness

The overall awareness of security needs to be enhanced in the System Administration group. They have a very good understanding of UNIX administration, but do not have the in-depth understanding of the level of security needed to secure the IT environment.

Learning security on the fly will not ensure that the System Administrators understand the whole picture regarding the implementation and configurations they perform, and may cause other security breaches while trying to fix some. The following types of training is recommended for selected personnel of the System Administrator group. The System Administrators receiving training should then in turn train the other System Administrators in security related issues. The training should include the following topics:

- UNIX security
- Firewall design
- Network security
- Attack and penetration
- Encryption and secure communication
- Web server/FTP/database server administration
- Security policies and procedures
- Disaster recovery / business continuity
- Computer forensics

Time should be set aside for selected System Administrators to do research on security related issues. Suggested web sites that should be checked periodically are:

- <http://www.securityfocus.com/>
- <http://www.cert.org/>
- <http://www.packetstorm.securify.com/>
- <http://www.ciac.org/ciac/>
- <http://www.ieee-security.org/index.html>
- <http://www.sans.org/newlook/home.htm>
- <http://www.isc2.org>

The System Administrators responsible for security should also subscribe to mailing lists to keep up to date with the latest security breaches. Following is a list of suggested mailing lists:

- [http://www.cert.org/contact\\_cert/certmaillist.html](http://www.cert.org/contact_cert/certmaillist.html)
- <http://www.sans.org/sansnews>
- <http://www.securityfocus.com> - select Bugtraq from left-hand menu.

## 7.2 Upgrades and Security Patches

Currently there are no routines for notification and installation of the latest security patches, see Security Patches chapter 4.1. The Audit team recommends implementing a routine for checking the Red Hat Errata page on a weekly basis, <http://www.redhat.com/support/rh71-errata.html>. All security patches and upgrades to the operating system and software packages should be installed and tested in the test environment previous to installation on the production host, see chapter 7.6.

Strict routines for communications with outside vendors should also be implemented to prevent intruders from contacting the System Administrators and offering patches including malicious software.

## 7.3 Inventory Lists

Interviews with the System Administrators revealed that there are no inventory lists of computer equipment and software installed due to the small environment.

The Audit team recommends that an inventory list be created for both hardware and software. When new equipment is purchased or older equipment is retired a routine for ensuring updates to the list should be implemented. Also, checks that the list is up to date should take place every 6 month. All equipment should have an asset tag indicating the name of the company and an asset tag number. The inventory list should include the asset tag number as well as information about the equipment such as serial numbers on memory, disk drivers etc., manufacturer, owner, location etc.

The inventory list for software should include version number and number of licenses purchased. Checks to ensure that the license number is maintained should be done on periodically.

## 7.4 Log Files

Currently there are no routines for the System Administrators to review the log files. The System Administrators informed that due to the heavy work-load they are not able to establish a routine for periodic checking of the log files.

The Audit team recommends installing the Logcheck application which was developed by Craig Rowland. This tool is part of the Abacus suite by Psionic Software. Logcheck will analyze the log files and only notify specified personnel upon unusual incidents. It is essentially looking for attempts of hack attacks and security violations. The tool comes with default patterns from logs from known attacks, security tools such as TCP wrappers and messages specific to Linux systems, so minimal configuration is required. Specific entries to be ignored by Logcheck can also be specified in the configuration files.

Logcheck can be downloaded from: <http://www.psionic.com/abacus/logcheck>.

## 7.5 Access to root Account

Currently all the System Administrators have access to the root password regardless of their job function. The wheel functionality which allows only users that are members of the wheel group access to su to root, is not enabled. Even if the current support group only consists of 3 people, the System Administrators admits that they have had problems with changes being done at random to the systems and no control of changes being performed or by whom. Since all System Administrators logon as root there are no audit trail and therefore not possible to monitoring actions done by the individual System Administrator. An intern is currently creating user accounts and resetting passwords on all the systems, and has been given root access in order to do these tasks.

The Audit team recommends that the su functionality which allows the System Administrators to log on using their own accounts and change user (su) to the root account to perform the necessary administrative tasks. Only tasks requiring root access should be done while logged in as root. All other tasks should be done while logged on to the personal accounts.

SUDO is already installed on the server, but not used. The Audit team recommends that the tool be configured and used for users who need to perform administrative tasks, but do not need full root access. This tool allows for granting users granular access to do administrative tasks without root access, and the privileged access can be configured to reflect their job function within the organization. A thorough analysis of the System Administrator positions to identify the tasks done by each and what privileged access is needed should be done to ensure that the minimum privileged access needed to perform the job function is granted. For example, the intern can be given access only to use the User Administration tool and update the `/etc/passwd` file. Also, an audit trail can be created using the SUDO tool. When configuring the SUDO utility care should be taken to ensure that the commands allowed to be run by the user can not spawn a sub-shell or execute external commands.

Root login should be restricted to only be done at the console. Remote use of the root account should require login to the personal user account followed by an su to root. This will limit intruders who can login directly as root to only users who obtain physical access to the server. For an overview of the physical security see chapter 8.

## 7.6 Test Environment

Currently there is a small test environment for the WWW servers at GIAC Enterprises. A test server should also be implemented for the router server. The test server should mirror the production server when it comes to operating system configuration and software installed. However, due to cost issues the test server does not have to have a similar hardware setup.

All software, patches and configuration updates should be tested on the test server before being installed on the production server to ensure that it works correctly and also works correctly with the configuration setup of the production server.

© SANS Institute 2000 - 2002, Author retains full rights.

## 8 Physical Security

GIAC Enterprises are currently in the process of building a computer room, and the audit team looked at the construction plans to ensure the proper security equipment will be in place. The room will have raised floors, the walls will go through the drop ceilings and raised floors to prevent access via false ceiling/floor, and humidity and temperature is controlled and automatically adjusted upon change. There will also be a fire suppression system which will have a dead-man switch and an analog phone line next to it. There will only be one door which will be protected by a finger print reader and a PIN entering device. All devices will be placed on racks and network cables will run in conduits along the walls.

The Audit team recommends having lockable racks to ensure no access from unauthorized personnel to CD-ROM and floppy drives or to reboot the system. Unauthorized users with access to boot a system from OS media on either CD or floppy can get user access to change the root password or create a set-UID shell. Also, repeatedly turning the system off and on or disconnect and reconnect the keyboard may corrupt a system in such a way that manual intervention is needed and allowing the unauthorized user access to change the root password, create a set-UID shell etc. Smoke and heat detectors should also be placed under the floors and in ceilings to enhance the ability to detect a fire as early as possible.

Currently the servers are residing in a closet with none of the above mention protection features. Since this is an intermediate solutions GIAC Enterprises decided not put any security features in this room. The Audit team recommends that at a minimum a lock should be installed on the door and only authorized personnel should be given access. Furthermore, an air-conditioner needs to be installed since overheating can cause the systems to fail, fire-extinguishers need to be in place and the sprinkler system needs to be disconnected in this room.

© SANS Institute

## 9 Corporate Security Policies

There are currently no formal corporate security policies at GIAC Enterprises. Lack of security policies at the corporate level can result in security issues not being addressed properly or not at all. The policies should be applied to both internal and external users. Formally documented and implemented security policies will allow GIAC Enterprises to have binding legal documents to pursue the people responsible should a security breach or misuse of any systems take place.

The Audit team recommends developing security policies including specific policies for the Linux environment which includes, but are not limited to, guidelines describing the particular environments such as DMZ, web servers, routers etc. A security policy will ensure that security features are applied to systems in a consistent manner throughout the organization, and will also ensure consistent ways of communicating security features to new employees. GIAC Enterprises should also consider establishing a position within the MIS environment for someone responsible for security. All users should be required to have training in the organization's IT policies and procedures upon starting with the company and periodically attend follow-up training. The policies and procedures should be made available on the Intranet for all internal users.

### 9.1 Password Policies

There are no policies for password requirements at GIAC Enterprises and no review or enforced changes of passwords. Currently there are no helpdesk function to assist users in changing passwords and other account administrative tasks. This is done by the System Administrator group. The passwords are distributed via the phone and no identification needs to be provided by the users upon resetting of the password.

The Audit team recommends that formal password policies be developed and implemented for the whole organization. The following table lists the recommended password settings:

Password Parameters	Recommended Settings	
	User Accounts	root Account
Password Length	6 character	8 characters
Password Characters	2 upper, 2 number, 1 special	2 upper, 3 number, 3 special
Password Change Frequency	90 days	30 days
Password History	4	8

Special characters includes the following characters: `~!@#\$%^&\*()-\_+=[]{}|'";<.>/?<sup>13</sup>  
The passwords should not contain names or something that can be referred back to the particular user, i.e. name of dog, SSN# etc. It should not contain a name or word where certain letters are substituted by a number or special character, i.e. p@ssword , since the password cracking tools will take this into consideration when guessing passwords. The password should not contain a

<sup>13</sup> Lee, Ranch: Securing Linux Step by Step, page 10

word from another language since there are word lists available for most languages. Users should be forced to change their password on first login.

Password and account names should never be embedded in files, applications, login scripts etc, since everyone with read access to these files will have access to see the password/account information. To search for this information in the files use the `grep password / *` command for files and the `strings -a` command for executables. These commands should be run on a weekly basis to detect the use of such information in files at an early stage.

On Idunn and other servers running the MD5 version of `crypt()` the users should be encouraged to use passphrases instead of regular passwords. MD5 supports very long passwords and a passphrase will make it more difficult to crack the passwords.

Furthermore, a position should be created for help desk functionality which will include resetting of user passwords. All users should be required to identify themselves by informing of either their Social Security Number or Employee ID number in order to obtain any assistance from the help desk.

### **9.1.1 Root Password Maintenance**

The root passwords should apply to the recommended policies described above. Also, each critical server should have a separate root password. The passwords for each server can have the same change cycle for administrative purposes, but should never have any similarities or be of the same genre, such as rock-groups, seasons, etc.

A password distribution sheet should be developed for informing System Administrators of new passwords. This piece of information should be created on a secure machine and printed at a secure printer. The file should be deleted upon completion or kept in encrypted format. The recommended format of the sheet is the smallest readable font, all uppercase characters are displayed in lower case but underlined, and all instances of the letter e is replaced by the number 3. The sheet should be the size of a driver's license to fit into a wallet. The order of server password should be memorized by the System Administrators so no server information need to be written on the password sheet.

An example of a root account password sheet:

6.rtg\+1 pd+-l/9u ui2.=3tp
----------------------------------



## **9.2 Backup Policies**

GIAC Enterprises does full backups every other Monday and incremental backups nightly Monday-Friday on all the critical servers. Backup is done to tape. Currently the full backup tapes are taken off site and kept at one of the System Administrator's house. The incremental backup tapes are rotated on a 20 day cycle and kept on a shelf in the computer room. There are no formal procedures for testing of the backup tapes, but the System Administrator verified that restoration has been done successfully when needed. There are no formal policies and procedures for the backup routines.

### **9.2.1 Recommendations**

The audit team recommends storing the full backup tapes off site in a secure facility such as companies specializing in protection of backup material etc. The incremental backup tapes can be stored on-site but in another part of the building. Furthermore, they need to be locked up in a fire-proof cabinet in an area with restricted access and with the proper environment such as not excessively high temperature or humidity.

The ability to restore data from backup tapes need to be tested on a periodic basis. A few files from the full backup media should be restored after each full backup in order to ensure the ability to read from the backup media. Should the hard-drive on a critical server fail it will be disastrous if the backup media is also malfunctioning. Twice a year the entire system should be completely restored from backup tapes to ensure that the entire backup system is working properly. It is also recommended that the tapes are write protected when stored, this will eliminate the potential for accidentally erasing data on the tape.

Formal policies and procedures for performing backups should be developed. The policies should include personnel responsible for performing backups, how the tapes should be handled and stored, frequency of testing etc. Checklists should be created to ensure that the backups are performed timely and stored properly.

## **9.3 Disaster Recovery/Business Continuity**

There are no formal Disaster Recovery Plan (DRP) or Business Continuity Plan (BCP) at GIAC Enterprises. In the event of a disaster such as fire, earthquake, flooding, technology failure etc. it is critical for GIAC Enterprises to be up and running as soon as possible.

A contingency plan is: "A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation..." (National Computer Security Center 1988).

The goal of a DRP/BCP plan is to assist the business to continue to function in the event that normal operations are disrupted. The plan will help the personnel to know what actions to take ahead of the disaster which in most situations work better than planning after the disaster has occurred.

The key word in a speedy recovery of a disaster is redundancy; redundancy of data, equipment, facilities, communications methods, personnel, procedures etc. For a small business such as GIAC Enterprises this can be very expensive, and a risk analysis should be performed to identify the most critical elements and find the best recovery solutions within GIAC Enterprises budget capabilities.

A recovery environment should be established at a remote site to ensure that the business's IT environment can be recovered in the less amount of time as possible. Since establishing a recovery site is costly, the Audit team recommends contracting with a recovery site, a so called "cold site". A "cold site" will provide the same equipment and recreate the environment from backup tapes in a specified time-frame, as opposed to a "hot site" where the equipment is up and running with mirrored data from the main site.

GIAC Enterprises does not have a UPS system to ensure a safe shut down of the systems in case of a power failure. The Audit team recommends purchasing a UPS system which will be powerful enough to safely allow all critical servers to shut down properly. Since the company is growing they should consider future expansions to the server and networking environment when considering a UPS system.

The UPS system should be tested every 3-6 months to ensure that it is in good condition and properly configured before a power outage occurs.

## **9.4 Incident Response Plan**

GIAC Enterprises does not have a formal Incident Response plan. If a security incident should happen either from an external source or from within the organization there are no procedures or plans of action to take.

The Audit team recommends developing a formal plan of how and to whom the incident should be reported if one should occur and what actions to take.

The plan should include contact information of someone high up in the organization who will take charge of the internal investigation. If the incident came from within the organization caution need to be taken so the suspect is not alarmed. Furthermore, the plan should include contact information to local law enforcements who can assist with the investigation, and outside firms who can assist with the computer forensics exercise.

### **9.4.1 Evidence Collection**

In case the incident will be investigated internally the Incident Response plan needs detailed instructions on how to collect evidence without destroying it. A secure toolkit need to be created since the tools on the “corrupted” system may have been compromised by the attacker. A toolkit should be created and kept on CD-ROM, and it should be updated every 6 month. Special care of collecting evidence need to be taken if the case is going to be prosecuted by a court. The computer forensics investigator should not be left alone with the evidence at any point in time, and the evidence must be securely captured, labeled and stored. Filming the evidence collection process may help to ensure that the investigators did not tamper with the evidence.

## **9.5 Termination of Employees**

### **9.5.1 Current Environment**

Users resigning from the company or users who are terminated should have their access to hosts and network terminated.

Currently there are no existing formal procedures for handling resignation or termination of employees. An interview with an HR representative (Ellen Olsen) was conducted and the following informal routines were described:

- Upon resignation or termination of an employee the user’s access to hosts and network would usually be terminated upon the user’s last day of employment.
- The HR representative will contact the System Administrators via phone or e-mail to inform of the employee’s departure from the company.
- There are no verification procedures going back to HR that the user was actually terminated.

### **9.5.2 Testing**

- A list of employees and outside contractors who have left the company within the last year was obtained from HR. The list included the date the person was leaving as well as their position in the company.
- In addition the test team went through the list with the System Administrator to ensure that all users having an account on the system still need access to Idunn in order to perform their job functions.
- Also, a list of users with access to the root account was obtained and walked through with the System Administrator.
- The current list of users with access to Idunn was obtained by looking at the
  - `/etc/passwd`<sup>14</sup> and

---

<sup>14</sup> See Appendix A, page 54, for a complete listing the `/etc/passwd` file.

- /etc/shadow files
- The following information was revealed:

Employee/Contractor leaving after 7/8/2000	Termination/Resignation Date	Title	Account on Idunn	Group Membership	Account Name
Gary Eriksen	7/30/2000	Technical Writer			
Abraham Hansen	9/15/2000	Junior System Administrator	Inactive	users	ahansen
Mona Nilsen	12/8/2000	Administrative Assistant			
Paul Rosen	2/16/2001	Contractor	Inactive	users	prosen
Nina Olsen	2/23/2001	Contractor	Active	users	nolsen
Sean McCarthy	3/6/2001	System Administrator	Active	users	smccarthy
Alan Sullivan	4/20/2001	Contractor		users	asullivan

### 9.5.3 Recommendations

Two accounts of terminated employees were still active (these accounts are highlighted). One of the accounts belonged to a former System Administrator. It was also noted that two users, Rita Gilbert (rgilbert) and Simon Martin (smartin) have access to the system. They do not need access to Idunn anymore since they have moved to other positions within the company. It is recommended that these accounts be disabled immediately.

A formal documentation for Termination Procedures should be developed and implemented. This document should include the process from HR is informed of the employee leaving until the user's access to the hosts and network is terminated. Furthermore, the document should include different procedures for users resigning and users being terminated from the company;

- Users resigning from the company should have the access to the network and/or hosts disabled upon their last day of employment.
- Upon termination of an employee the employee's manager or someone equivalent should be notified and access to hosts and network terminated immediately.
- Also, when the employee's access to hosts and network is disabled a verification should be sent to the HR representative who initiated the process, i.e. a confirmation e-mail.

Periodic testing of current user accounts against lists of users who have left the company or moved to other positions should be conducted. Frequency of the test is suggested to every 3-6 month. As GIAC Enterprises grow and a larger number of users will get access to the system, the need for clearly established routines becomes more important.

Access to the root account should only be given to users who need this in order to perform their job function. It is recommended that the System Administrator goes through the list of users with privileged access on a periodic basis to ensure root access is only given to required personnel.

When users are away from work for a longer period of time due to vacation, disability, extended leave such as sabbaticals, maternity etc, their user account should be disabled until they return.

## 10 Prioritized List of Issues

Priority	Risk Level	Vulnerability	Referenced	Comments
1	High	Temporarily improve physical security for Idunn.	Chapter 9	Must be done immediately.
2	High	Configure a test server for Idunn.	Chapter 8.5	This must be done before any patches or upgrades can be installed.
3	High	Install security patches.	Chapter 5.1	The server should not be connected to the Internet until the patches are installed. The patches must be tested on the test server before installed in production.
4	High	Disable unused user accounts.	Chapter 10.5	
5	High	Disable unnecessary services.	Chapter 3.3.1	
6	High	Install and configure SSH.	Chapter 6.2	
7	High	Boot and reboot protection.	Chapter 3.1	Was set to risk level high due to insufficient physical security.
8	High	Removal of unnecessary services from xinetd.conf file	Chapter 3.3.1	
9	High	Install and configure Tripwire.	Chapter 6.3	
10	High	Remove SUID and SGID programs.	Chapter 3.3.5	
11	High	Disable unused system accounts.	Chapter 3.3.7	
12	High	Remove unnecessary third-party software.	Chapter 5.2	
13	High	Create and implement various corporate security policies	Chapter 10	
14	High	Create and implement password policies	Chapter 10.1	
15	Medium	Enhance security knowledge of System Administrators		
16	Medium	Set login shells of disabled user accounts to /bin/false.	Chapter 3.3.3	

17	Medium	Set sticky bit on temporary files.	Chapter 3.3.4	
18	Medium	Install and configure passwd+.	Chapter 6.1	
19	Medium	Install and configure Logcheck.	Chapter 8.3	
20	Medium	Install and configure SUDO	Chapter 8.4	
21	Medium	Update /etc/syslog.conf and set log file permissions.	Chapter 7	
22	Medium	Configure a syslog server.	Chapter 7.1	
23	Medium	Install and configure NTP.	Chapter 7.2	
24	Medium	Create inventory list.	Chapter 8.2	

## Risk Levels

The risk levels were chosen according to the likelihood of the exploitation of a system or organization vulnerability. The issues were viewed in light of the functionality of the server when ranked.

Risk Level	Description
Low risk	the vulnerability will not cause a major threat to the IT environment, and the likelihood of a malicious user exploiting this vulnerability is minimal.
Medium risk	the vulnerability could cause a significant threat to the IT environment, and the likelihood of a malicious user exploiting this vulnerability is significant.
High risk	the vulnerability could not cause a real danger to the IT environment, and the likelihood of a malicious user exploiting this vulnerability is considered very high.

## 11 A Prioritized List of Recommended Fixes

Priority	Vulnerability	Recommended Action	Time to Correct Hrs	Cost
1	Temporarily improve physical security for Idunn.	Install lock	2	\$160.00
		Install air-conditioner	5	\$400.00
		Purchase fire-extinguishers	2	\$160.00
		Disconnect sprinkler system.	3	\$240.00
2	Configure a test server for Idunn.	Purchase of Hardware		\$3000.00
		Implementation and configuration	12	\$960.00
3	Install security patches.		8	\$640.00
4	Disable unused user accounts		2	\$160.00
5	Disable unnecessary services.		4	\$320.00
6	Install and configure SSH.		16	\$1,280.00
7	Boot and reboot protection.	Disable reboot using Control+Alt+Del keys	1	\$80.00
		Enable root password when reboot to single user mode	1	\$80.00
		Enable LILO password	1	\$80.00
		Enable BIOS password	1	\$80.00
8	Removal of unnecessary services from xinetd.conf file		1	\$80.00
9	Install and configure Tripwire.	Analysis of which files to protect.	6	\$480.00
10		Configuration of Tripwire	6	\$480.00
11	Remove SUID and SGID programs.		4	\$320.00

12	Disable unused system accounts.		3	\$240.00
13	Remove unnecessary third-party software.		8	\$640.00
14	Create and implement password policies		40	\$3,200.00
15	Enhance security knowledge of System Administrators.	2 System Administrators should take 1 week class.	80	
		Course expenses x2		\$3,000.00
		Travel expenses (airfare, hotel, meals etc.) x2		\$5,500.00
16	Create and implement various corporate security policies	Backup policy	20	\$1,600.00
		DisasterRecovery/Business Continuity plan	80	\$6,400.00
		Incident response plan	80	\$6,400.00
		Termination policy	40	\$3,200.00
		Implementation of policies (user training, changing of routines etc.)	120	\$9,600.00
17	Set login shells of disabled user accounts to /bin/false.		1	\$80.00
18	Set sticky bit on temporary files.		1	\$80.00
19	Install and configure passwd+.		8	\$640.00
20	Install and configure Logcheck.		8	\$640.00
21	Identify tasks for each System Administrator position.		12	\$960.00
22	Configure SUDO according to analysis done in previous step.		5	\$400.00
23	Update /etc/syslog.conf and set log file permissions.		2	\$160.00
24	Configure a syslog server.	Purchase of Hardware		\$5000.00



		Implementation and configuration	12	\$960.00
25	Install and configure NTP.		6	\$480.00
26	Create inventory list.		8	\$640.00

The cost was estimated based on an hourly rate of \$80.00.

Total cost for implementing all recommendations: \$58,820.00

Total cost for implementing recommendations for Idunn only: \$12,360.00

Total cost for implementing high risk issues: \$13,080.00

## TO-DO's

On a weekly basis the following commands and tools should be run either manually or in cron jobs:

- Check for sniffers installed: `ifconfig | grep PROMISC`
- Run Tripwire to ensure that no files have been changed
- Identify network connections: `lsof -i`
- Check file integrity: `rpm -Va`
- Check for password information in files:  
`grep password / *`  
`grep passwd / *`
- Check for SUID/SGID files:  
`find /\ (-perm -4000 -o -perm -2000 \) -type -f -fls output.txt`
- Check for recently modified binaries (especially for files not protected by Tripwire):  
`touch -m 070f date /tmp/tstamp`  
`find /n -newer /tmp/tstamp -type f -user root -perm +111 -printf "%Tc %k %h/%fn" |`  
`sort -r -k3,5`  
(set the *date* variable to be the benchmark, and you want to check for files with a time-stamp newer than this date. The date should be of format ddmmyyyy)

On a weekly basis the following tasks should be done:

- Check for new security patches at the Red Hat errata page  
<http://www.redhat.com/support/errata/rh71-errata.html>.
- Check for new security incidents on various security web sites, see chapter 7.1

Every 6 months the following tasks should be done:

- Run crack to ensure proper password settings are used (or review passwd+ settings).
- Ensure that all policies and procedures are up-to-date.
- Review Tripwire settings.
- Review user accounts for terminated users.
- Review user accounts with root access to verify that elevated access is needed.
- Ensure that the inventory list for HW/SW is up-to-date.
- Testing of UPS.
- Update computer forensics toolkit.

## 12 List of References

### Literature:

1. Hal Pomeranz , Steve Acheson, Matt Bishop, Lee Brotzman (2001), 6 books from Track 6 – Level Two Securing Unix, SANS Institute.
2. Simson Garfinkel and Gene Spafford (1996), Practical Unix & Internet Security, O'Reilly & Associates.
3. Brian Hatch, James Lee, George Kurtz (1996), Hacking Exposed: Linux Security Secrets & Solutions, Osborne/McGraw-Hill.
4. The SANS Institute, edited by Lee Brotzman and David A. Ranch (2000), Securing Linux Step-by-Step v.1.0, The SANS Institute.
5. Tim Parker (1998)Linux Third Edition Unleashed, Sams Publishing.
6. William Stallings (1995), Network and Internetwork Security, Prentice Hall, IEEE Press

### WWW Links:

1. NTP: <http://www.eecis.udel.edu/~ntp>
2. Linux: <http://www.redhat.com>  
<http://www.redhat.com/mirrors/LDP/HOWTO/HOWTO-INDEX/howtos.html>

© SANS Institute 2000 - 2002, Author retains full rights.

## Appendix A

### Changed Binary Files

Script started on Wed Jul 18 23:54:01 2001

[Back to chapter 3.3.2](#)

```
[root@idunn list1]# touch -m 070f 102001 /tmp/tstamp
[root@idunn list1]# find /n -newer /tmp/tstamp -type f -user root -perm +111 -printf "%Tc %k %h/%f\n" |
sort -r - k3,5
```

```
Thu 12 Jul 2001 11:28:29 PM EDT 20 /usr/programs/security/tiger/tiger-2.2.4p1/bin/getpermit
Thu 12 Jul 2001 11:28:28 PM EDT 36 /usr/programs/security/tiger/tiger-2.2.4p1/bin/snefru
Thu 12 Jul 2001 11:28:28 PM EDT 20 /usr/programs/security/tiger/tiger-2.2.4p1/bin/realpath
Thu 12 Jul 2001 11:28:28 PM EDT 20 /usr/programs/security/tiger/tiger-2.2.4p1/bin/md5
Thu 12 Jul 2001 11:28:28 PM EDT 16 /usr/programs/security/tiger/tiger-2.2.4p1/bin/testsuid
Thu 12 Jul 2001 10:25:47 PM EDT 1 /root/simplefw
```

```
[root@idunn list1]# exit
```

Script done on Wed Jul 18 23:56:38 2001

## SUID/SGID Programs

Command: `find /\ ( -perm -4000 -o -perm -2000 \) -type f -fls suidfiles.dat`

[Back to chapter 3.3.5](#)

Output:

163312	40	-rwsr-xr-x	1	root	root	37764	Apr	4	17:00	/usr/bin/at
163346	36	-rwxr-sr-x	1	root	man	35676	Feb	4	13:40	/usr/bin/man
163351	168	-rwxr-sr-x	1	root	uucp	167324	Feb	23	07:31	/usr/bin/minicom
163426	784	-rws--x--x	2	root	root	795092	Mar	23	12:55	/usr/bin/suidperl
163426	784	-rws--x--x	2	root	root	795092	Mar	23	12:55	/usr/bin/sperl5.6.0
163437	12	-rwxr-sr-x	1	root	mail	11124	Jan	6	2001	/usr/bin/lockfile
163482	16	-rwsr-xr-x	1	root	root	14332	Feb	5	17:43	/usr/bin/rcp
163484	12	-rwsr-xr-x	1	root	root	10844	Feb	5	17:43	/usr/bin/rlogin
163485	8	-rwsr-xr-x	1	root	root	7796	Feb	5	17:43	/usr/bin/rsh
163523	36	-rwsr-xr-x	1	root	root	34588	Mar	9	14:31	/usr/bin/chage
163525	36	-rwsr-xr-x	1	root	root	36228	Mar	9	14:31	/usr/bin/gpasswd
163537	24	-rwxr-sr-x	1	root	slocate	24508	Feb	26	12:42	/usr/bin/slocate
163622	16	-r-s--x--x	1	root	root	13536	Jul	12	2000	/usr/bin/passwd
163690	8	-r-xr-sr-x	1	root	tty	6492	Apr	4	09:06	/usr/bin/wall
164013	16	-rws--x--x	1	root	root	13048	Apr	8	10:11	/usr/bin/chfn
164014	16	-rws--x--x	1	root	root	12600	Apr	8	10:11	/usr/bin/chsh
164032	8	-rws--x--x	1	root	root	5460	Apr	8	10:11	/usr/bin/newgrp
164043	12	-rwxr-sr-x	1	root	tty	8692	Apr	8	10:11	/usr/bin/write
164068	196	-rwsr-xr-x	1	root	root	195472	Apr	8	19:10	/usr/bin/ssh
164084	24	-rwsr-xr-x	1	root	root	21312	Mar	8	15:56	/usr/bin/crontab
164211	8	-rwsr-xr-x	1	root	root	7300	Apr	3	15:32	/usr/bin/kcheckpass
164220	60	-rwxr-sr-x	1	root	root	55400	Apr	3	15:32	/usr/bin/kdesud
164392	32	-r-sr-x---	1	root	news	29212	Feb	14	10:12	/usr/bin/inndstart
164418	60	-r-sr-x---	1	uucp	news	53942	Feb	14	10:10	/usr/bin/rnews
164431	28	-r-sr-x---	1	root	news	25564	Feb	14	10:12	/usr/bin/startinnfeed
164657	84	---s--x--x	1	root	root	81020	Feb	23	16:45	/usr/bin/sudo
164748	132	-r-sr-sr-x	1	uucp	uucp	129188	Jan	6	2001	/usr/bin/cu
164749	96	-r-sr-xr-x	1	uucp	uucp	91688	Jan	6	2001	/usr/bin/uucp
164751	40	-r-sr-sr-x	1	uucp	uucp	38756	Jan	6	2001	/usr/bin/uuname
164753	104	-r-sr-xr-x	1	uucp	uucp	101656	Jan	6	2001	/usr/bin/uustat
164755	96	-r-sr-xr-x	1	uucp	uucp	93540	Jan	6	2001	/usr/bin/uux
423918	20	-rwsr-xr-x	1	root	root	18256	Dec	1	2000	/usr/sbin/traceroute
423919	8	-rwxr-sr-x	1	root	utmp	6584	Jul	13	2000	/usr/sbin/utempter

423942	416	-r-sr-xr-x	1	root	root	417828	Mar	3	01:43	/usr/sbin/sendmail
423947	12	-rwxr-sr-x	1	root	utmp	9180	Mar	16	15:05	/usr/sbin/gnome-pty-helper
424110	8	-rwsr-xr-x	1	root	root	6392	Apr	7	11:12	/usr/sbin/usernetctl
424176	24	-rws--x--x	1	root	root	20696	Feb	14	15:18	/usr/sbin/userhelper
426147	12	-r-s--x---	1	root	apache	10976	Mar	29	12:52	/usr/sbin/suexec
426198	228	-r-sr-sr-x	1	uucp	uucp	228096	Jan	6	2001	/usr/sbin/uucico
426201	108	-r-sr-sr-x	1	uucp	uucp	103600	Jan	6	2001	/usr/sbin/uuxqt
33143	8	-rws--x--x	1	root	root	6040	Mar	30	21:51	/usr/X11R6/bin/Xwrapper
36146	24	-rwsr-xr-x	1	root	root	22620	Jan	16	2001	/bin/ping
36199	57	-rwsr-xr-x	1	root	root	56444	Mar	22	11:13	/bin/mount
36200	26	-rwsr-xr-x	1	root	root	24796	Mar	22	11:13	/bin/umount
36215	15	-rwsr-xr-x	1	root	root	14112	Jan	16	2001	/bin/su
62314	16	-r-sr-xr-x	1	root	root	14960	Apr	7	13:47	/sbin/pwdb_chkpwd
62315	17	-r-sr-xr-x	1	root	root	15448	Apr	7	13:47	/sbin/unix_chkpwd
62347	5	-rwxr-sr-x	1	root	root	4160	Apr	7	11:12	/sbin/netreport

## Network Connections (netstat)

Command: netstat -a --inet

Output:

```
Script started on Wed Jul 18 23:42:45 2001
root@idunn list1]# netstat -a --inet
```

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	*:32768	*:*	LISTEN
tcp	0	0	*:sunrpc	*:*	LISTEN
tcp	0	0	*:http	*:*	LISTEN
tcp	0	0	*:x11	*:*	LISTEN
tcp	0	0	*:ftp	*:*	LISTEN
tcp	0	0	*:ssh	*:*	LISTEN
tcp	0	0	*:telnet	*:*	LISTEN
tcp	0	0	localhost.localdom:smtp	*:*	LISTEN
tcp	0	0	*:https	*:*	LISTEN
udp	0	0	*:32768	*:*	
udp	0	0	*:907	*:*	
udp	0	0	*:sunrpc	*:*	

```
[root@idunn list1]# exit
```

```
Script done on Wed Jul 18 23:42:53 2001
```

[Back to chapter 3.3.1](#)

## Network Connections (lsof)

Command: `lsof -i`

[Back to chapter 3.3.1](#)

Output:

Script started on Wed Jul 18 23:43:04 2001

[root@idunn list1]# `lsof -i`

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE	NODE	NAME
portmap	716	root	3u	IPv4	954		UDP	*:sunrpc
portmap	716	root	4u	IPv4	955		TCP	*:sunrpc (LISTEN)
rpc.statd	731	root	4u	IPv4	982		UDP	*:907
rpc.statd	731	root	5u	IPv4	999		UDP	*:32768
rpc.statd	731	root	6u	IPv4	1002		TCP	*:32768 (LISTEN)
sshd	891	root	3u	IPv4	1153		TCP	*:ssh (LISTEN)
xinetd	911	root	3u	IPv4	1183		TCP	*:ftp (LISTEN)
xinetd	911	root	4u	IPv4	1184		TCP	*:telnet (LISTEN)
sendmail	943	root	4u	IPv4	1225		TCP	localhost.localdomain:smtp (LISTEN)
X	1069	root	1u	IPv4	1354		TCP	*:x11 (LISTEN)
httpd	1270	root	16u	IPv4	3299		TCP	*:https (LISTEN)
httpd	1270	root	17u	IPv4	3300		TCP	*:http (LISTEN)
httpd	1273	root	16u	IPv4	3299		TCP	*:https (LISTEN)
httpd	1273	root	17u	IPv4	3300		TCP	*:http (LISTEN)
httpd	1274	root	16u	IPv4	3299		TCP	*:https (LISTEN)
httpd	1274	root	17u	IPv4	3300		TCP	*:http (LISTEN)
httpd	1275	root	16u	IPv4	3299		TCP	*:https (LISTEN)
httpd	1275	root	17u	IPv4	3300		TCP	*:http (LISTEN)
httpd	1276	root	16u	IPv4	3299		TCP	*:https (LISTEN)
httpd	1276	root	17u	IPv4	3300		TCP	*:http (LISTEN)
httpd	1277	root	16u	IPv4	3299		TCP	*:https (LISTEN)
httpd	1277	root	17u	IPv4	3300		TCP	*:http (LISTEN)
httpd	1278	root	16u	IPv4	3299		TCP	*:https (LISTEN)
httpd	1278	root	17u	IPv4	3300		TCP	*:http (LISTEN)
httpd	1279	root	16u	IPv4	3299		TCP	*:https (LISTEN)
httpd	1279	root	17u	IPv4	3300		TCP	*:http (LISTEN)
httpd	1280	root	16u	IPv4	3299		TCP	*:https (LISTEN)
httpd	1280	root	17u	IPv4	3300		TCP	*:http (LISTEN)

[root@idunn list1]# `exit`



Script done on Wed Jul 18 23:43:10 2001

© SANS Institute 2000 - 2002, Author retains full rights.

## Ifconfig

[Back to chapter 3.2](#)

Script started on Wed Jul 18 23:43:27 2001

[root@idunn]# ifconfig

```
eth0      Link encap:Ethernet  HWaddr 00:50:BA:47:2C:76
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:954 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1018 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:10 Base address:0xa000

eth1      Link encap:Ethernet  HWaddr 00:01:02:A1:F7:CF
          inet addr:192.168.1.1  Bcast:255.255.255.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5605 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4593 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:9 Base address:0x9000

eth2      Link encap:Ethernet  HWaddr 00:01:02:A1:F5:CF
          inet addr:192.168.2.1  Bcast:255.255.255.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5605 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4593 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:9 Base address:0x8000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0

ppp0      Link encap:Point-to-Point Protocol
          inet addr:141.155.184.239  P-t-P:10.3.36.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1492  Metric:1
          RX packets:710 errors:0 dropped:0 overruns:0 frame:0
          TX packets:774 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
```

[root@idunn list1]# exit

Script done on Wed Jul 18 23:43:39 2001

## Inittab

[Back to chapter 3.1.2](#)

```
#
# inittab          This file describes how the INIT process should set up
#                  the system in a certain run-level.
#
# Author:          Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>
#                  Modified for RHS Linux by Marc Ewing and Donnie Barnes
#

# Default runlevel. The runlevels used by RHS are:
#  0 - halt (Do NOT set initdefault to this)
#  1 - Single user mode
#  2 - Multiuser, without NFS (The same as 3, if you do not have networking)
#  3 - Full multiuser mode
#  4 - unused
#  5 - X11
#  6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit

10:0:wait:/etc/rc.d/rc 0
11:1:wait:/etc/rc.d/rc 1
12:2:wait:/etc/rc.d/rc 2
13:3:wait:/etc/rc.d/rc 3
14:4:wait:/etc/rc.d/rc 4
15:5:wait:/etc/rc.d/rc 5
16:6:wait:/etc/rc.d/rc 6

# Things to run in every runlevel.
ud::once:/sbin/update

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

# When our UPS tells us power has failed, assume we have a few minutes
# of power left.  Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have powerd installed and your
# UPS connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"

# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"

# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6
```

Add this line here:

~~:S:wait:/sbin/sulogin

Comment out this line:

#ca::ctrlaltdel:/sbin/shutdown -t3 -r now

```
# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

© SANS Institute 2000 - 2002, Author retains full rights.

## xinetd.conf

Script started on Wed Jul 18 23:04:08 2001

[Back to chapter 3.3](#)

```
[root@idunn list2]# cat /etc/xinetd.conf
#
# Simple configuration file for xinetd
#
# Some defaults, and include /etc/xinetd.d/

defaults
{
    instances                = 60
    log_type                  = SYSLOG authpriv
    log_on_success            = HOST PID
    log_on_failure            = HOST
}

includedir /etc/xinetd.d

#
# Sample configuration file for xinetd
#
# defaults
#{
#     log_type                = FILE /var/log/servicelog
#     log_on_success          = PID
#     log_on_failure          = HOST RECORD
#     only_from               = 128.138.193.0 128.138.204.0 128.138.209.0
#     only_from               = 128.138.252.1
#     instances               = 10
#     disabled                = rstatd
#}

#
# Note 1: the protocol attribute is not required
# Note 2: the instances attribute overrides the default
#
service login
{
    socket_type               = stream
#     protocol                 = tcp
    wait                      = no
    user                      = root
    server                    = /usr/etc/in.rlogind
    instances                 = UNLIMITED
}

#
# Note 1: the instances attribute overrides the default
# Note 2: the log_on_success flags are augmented
#
service shell
{
    socket_type               = stream
    wait                      = no
    user                      = root
```

```

        instances          = UNLIMITED
        server              = /usr/etc/in.rshd
        log_on_success      += HOST RECORD
    }

service ftp
{
    socket_type            = stream
    wait                   = no
#    nice                   = 10
    user                   = root
    server                  = /usr/sbin/in.ftpd
    server_args             = -l
    instances               = 4
#    log_on_success         += DURATION HOST USERID
#    access_times           = 2:00-9:00 12:00-24:00
}

# Limit telnet sessions to 8 Mbytes of memory and a total
# 20 CPU seconds for child processes.
service telnet
{
    socket_type            = stream
    wait                   = no
#    nice                   = 10
    user                   = root
    server                  = /usr/sbin/in.telnetd
#    rlimit_as              = 8M
#    rlimit_cpu             = 20
}

#
# This entry and the next one specify internal services. Since
# this is the same service using a different socket type, the
# id attribute is used to uniquely identify each entry
#

service echo
{
    id                     = echo-stream
    type                   = INTERNAL
    socket_type            = stream
#    user                   = root
    wait                   = no
}
#
# Sample RPC service
#

service rstatd
{
    type                   = RPC
    socket_type            = dgram
    protocol               = udp
    server                  = /usr/etc/rpc.rstatd
    wait                   = yes
    user                   = root

```

```
        rpc_version      = 2-4
        env               = LD_LIBRARY_PATH=/etc/securelib
    }

service http
{
    socket_type           = stream
    protocol              = tcp
    wait                  = no
    user                  = root
    server                = /usr/sbin/httpd httpd
}

[root@idunn list2]# exit
Script done on Wed Jul 18 23:04:19 2001
```

© SANS Institute 2000 - 2002, Author retains full rights.

```

# /etc/profile

# System wide environment and startup programs
# Functions and aliases go in /etc/bashrc
PROFILE_LOADED=1

PATH="$PATH:/usr/X11R6/bin"

if [ `id -gn` = `id -un` -a `id -u` -gt 14 ]; then
    umask 002
else
    umask 022
fi

USER=`id -un`
LOGNAME=$USER
MAIL="/var/spool/mail/$USER"

HOSTNAME=`/bin/hostname`
HISTSIZE=1000

if [ -z "$INPUTRC" -a ! -f "$HOME/.inputrc" ]; then
    export INPUTRC=/etc/inputrc
fi


export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE

if i in /etc/profile.d/*.sh ; do
    if [ -x $i ]; then
        . $i
    fi
done

unset i

```

Change to:  
umask 027



© SANS Institute 2000 - 2002 Author retains full rights.



## etc/syslog.conf

[Back to chapter 6](#)

```
# Various entry
auth,authpriv.*                /var/log/auth.log
*.*;auth,authpriv.none         /var/log/syslog
user.*                          /var/log/user.log

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none /var/log/messages

# The authpriv file has restricted access.
authpriv.*                     /var/log/secure

# Mail logging
mail.=debug;mail.=info;mail.=notice /var/log/mail/info
mail.=warn                     /var/log/mail/warnings
mail.err                       /var/log/mail/errors

# Cron logging
cron.=debug;cron.=info;cron.=notice /var/log/cron/info
cron.=warn                     /var/log/cron/warnings
cron.err                       /var/log/cron/errors

# Kernel logging
kern.=debug;kern.=info;kern.=notice /var/log/kernel/info
kern.=warn                     /var/log/kernel/warnings
kern.err                       /var/log/kernel/errors

# Lpr logging
lpr.=debug;lpr.=info;lpr.=notice    /var/log/lpr/info
lpr.=warn                       /var/log/lpr/warnings
lpr.err                          /var/log/lpr/errors

# News logging
news.=debug;news.=info;news.=notice /var/log/news/info
news.=warn                       /var/log/news/warnings
news.err                         /var/log/news/errors

# Daemons logging
daemon.=debug;daemon.=info;daemon.=notice /var/log/daemons/info
daemon.=warn                       /var/log/daemons/warnings
daemon.err                           /var/log/daemons/errors

# Everybody gets emergency messages
*.emerg                            *

# Save mail and news errors of level err and higher in a
# special file.
uucp,news.crit                    /var/log/spooler

# Save boot messages also to boot.log
local7.*                          /var/log/boot.log
*.* /dev/tty12
```

© SANS Institute 2000 - 2002, Author retains full rights.

## /etc/passwd

[Back to chapter 3.17](#)

```
Script started on Wed Jul 18 22:51:16 2001
[root@idunn list2]# cat /etc/passwd
```

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:
operator:x:11:0:operator:/root:
games:x:12:100:games:/usr/games:
gopher:x:13:30:gopher:/usr/lib/gopher-data:
ftp:x:14:50:FTP User:/var/ftp:
nobody:x:99:99:Nobody:/:
nscd:x:28:28:NSCD Daemon:/:bin/false
mailnull:x:47:47::/var/spool/mqueue:/dev/null
ident:x:98:98:pident user:/:bin/false
rpc:x:32:32:Portmapper RPC user:/:bin/false
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/bin/false
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
apache:x:48:48:Apache:/var/www:/bin/false
named:x:25:25:Named:/var/named:/bin/false
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
ahansen:NP:1001:1001:Abraham Hansen:/home/ahansen:/bin/bash
prosen:NP:1002:1001:Paul Rosen:/home/prosen:/bin/bash
nolsen:x:1003:1001:Nina Olsen:/home/nolsen:/bin/bash
smccarthy:x:1004:1001:Sean McCarthy:/home/smccarthy:/bin/bash
asullivan:x:1005:1001:Alan Sullivan:/home/asullivan:/bin/bash
rporter:x:1006:1001:Ron Porter:/home/rporter:/bin/bash
mpinetree:x:1007:1001:Matthew Pinetree:/home/mpinetree:/bin/bash
rgilbert:x:1008:1001:Rita Gilbert:/home/rgilbert:/bin/bash
smartin:x:1009:1001:Simon Martin:/home/smartin:/bin/bash
```

```
[root@idunn list2]# exit
Script done on Wed Jul 18 22:51:32 2001
```

© SANS Institute 2000 - 2002. Author retains full rights.

## Shells

[Back to chapter 3.3.8](#)

```
Script started on Wed Jul 18 23:03:07 2001  
[root@idunn list2]# cat /etc/shells
```

```
/bin/bash2  
/bin/bash  
/bin/sh  
/bin/ash  
/bin/bsh  
/bin/tcsh  
/bin/csh
```

```
[root@idunn list2]# exit
```

```
Script done on Wed Jul 18 23:03:19 2001
```

© SANS Institute 2000 - 2002, Author retains full rights.

## Services

[Back to chapter 4.2](#)

Script started on Wed Jul 18 23:04:57 2001

[root@idunn list2]# cat /etc/services

```
# /etc/services:
# $Id: services,v 1.17 2001/02/28 20:11:31 notting Exp $
#
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, most entries here have two entries
# even if the protocol doesn't support UDP operations.
# Updated from RFC 1700, ``Assigned Numbers'' (October 1994). Not all ports
# are included, only the more common ones.
#
# The latest IANA port assignments can be gotten from
#   http://www.isi.edu/in-notes/iana/assignments/port-numbers
# The Well Known Ports are those from 0 through 1023.
# The Registered Ports are those from 1024 through 49151
# The Dynamic and/or Private Ports are those from 49152 through 65535
#
# Each line describes one service, and is of the form:
#
# service-name port/protocol [aliases ...] [# comment]

tcpmux          1/tcp          # TCP port service
multiplexer
tcpmux          1/udp          # TCP port service
multiplexer
rje             5/tcp          # Remote Job Entry
rje             5/udp          # Remote Job Entry
echo            7/tcp
echo            7/udp
discard         9/tcp          sink null
discard         9/udp          sink null
systat          11/tcp         users
systat          11/udp         users
daytime         13/tcp
daytime         13/udp
qotd            17/tcp          quote
qotd            17/udp          quote
msp             18/tcp          # message send protocol
msp             18/udp          # message send protocol
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp-data        20/udp
ftp             21/tcp
ftp             21/udp
ssh             22/tcp          # SSH Remote Login Protocol
ssh             22/udp          # SSH Remote Login Protocol
telnet          23/tcp
telnet          23/udp
smtp            25/tcp          mail
```

smtp	25/udp	mail	
time	37/tcp	timserver	
time	37/udp	timserver	
rlp	39/tcp	resource	# resource location
rlp	39/udp	resource	# resource location
nameserver	42/tcp	name	# IEN 116
nameserver	42/udp	name	# IEN 116
nicname	43/tcp	whois	
nicname	43/udp	whois	
tacacs	49/tcp		# Login Host Protocol
(TACACS)			
tacacs	49/udp		# Login Host Protocol
(TACACS)			
re-mail-ck	50/tcp		# Remote Mail Checking
Protocol			
re-mail-ck	50/udp		# Remote Mail Checking
Protocol			
domain	53/tcp	nameserver	# name-domain server
domain	53/udp	nameserver	
whois++	63/tcp		
whois++	63/udp		
bootps	67/tcp		# BOOTP server
bootps	67/udp		
bootpc	68/tcp		# BOOTP client
bootpc	68/udp		
tftp	69/tcp		
tftp	69/udp		
gopher	70/tcp		# Internet Gopher
gopher	70/udp		
netrjs-1	71/tcp		# Remote Job Service
netrjs-1	72/tcp		# Remote Job Service
netrjs-2	72/udp		# Remote Job Service
netrjs-3	73/tcp		# Remote Job Service
netrjs-3	73/udp		# Remote Job Service
netrjs-4	74/tcp		# Remote Job Service
netrjs-4	74/udp		# Remote Job Service
finger	79/tcp		
finger	79/udp		
http	80/tcp	www www-http	# WorldWideWeb HTTP
http	80/udp	www www-http	# HyperText Transfer Protocol
kerberos	88/tcp	kerberos5 krb5	# Kerberos v5
kerberos	88/udp	kerberos5 krb5	# Kerberos v5
supdup	95/tcp		
supdup	95/udp		
hostname	101/tcp	hostnames	# usually from sri-nic
hostname	101/udp	hostnames	# usually from sri-nic
iso-tsap	102/tcp	tsap	# part of ISODE.
csnet-ns	105/tcp	cso	# also used by CSO name
server			
csnet-ns	105/udp	cso	# unfortunately the poppassd (Eudora)
uses a port which has already			
			# been assigned to a different
			service. We list the poppassd as an
			# alias here. This should work for
			programs asking for this service.
			# (due to a bug in inetd the 3com-
			tsmux line is disabled)

#3com-tsmux	106/tcp	poppassd	
#3com-tsmux	106/udp	poppassd	
rtelnet	107/tcp		# Remote Telnet
rtelnet	107/udp		
pop2	109/tcp	pop-2 postoffice	# POP version 2
pop2	109/udp	pop-2	
pop3	110/tcp	pop-3	# POP version 3
pop3	110/udp	pop-3	
sunrpc	111/tcp	portmapper	# RPC 4.0 portmapper TCP
sunrpc	111/udp	portmapper	# RPC 4.0 portmapper UDP
auth	113/tcp	authentication tap ident	
auth	113/udp	authentication tap ident	
sftp	115/tcp		
sftp	115/udp		
uucp-path	117/tcp		
uucp-path	117/udp		
nnntp	119/tcp	readnews untp	# USENET News Transfer
Protocol			
nnntp	119/udp	readnews untp	# USENET News Transfer
Protocol			
ntp	123/tcp		
ntp	123/udp		# Network Time Protocol
netbios-ns	137/tcp		# NETBIOS Name Service
netbios-ns	137/udp		
netbios-dgm	138/tcp		# NETBIOS Datagram Service
netbios-dgm	138/udp		
netbios-ssn	139/tcp		# NETBIOS session service
netbios-ssn	139/udp		
imap	143/tcp	imap2	# Interim Mail Access Proto
v2			
imap	143/udp	imap2	
snmp	161/tcp		# Simple Net Mgmt Proto
snmp	161/udp		# Simple Net Mgmt Proto
snmptrap	162/udp	snmp-trap	# Traps for SNMP
cmip-man	163/tcp		# ISO mgmt over IP (CMOT)
cmip-man	163/udp		
cmip-agent	164/tcp		
smip-agent	164/udp		
mailq	174/tcp		# MAILQ
mailq	174/udp		# MAILQ
xdmcp	177/tcp		# X Display Mgr. Control
Proto			
xdmcp	177/udp		
nextstep	178/tcp	NeXTStep NextStep	# NeXTStep window
nextstep	178/udp	NeXTStep NextStep	# server
bgp	179/tcp		# Border Gateway Proto.
bgp	179/udp		
prospero	191/tcp		# Cliff Neuman's Prospero
prospero	191/udp		
irc	194/tcp		# Internet Relay Chat
irc	194/udp		
smux	199/tcp		# SNMP Unix Multiplexer
smux	199/udp		
at-rtmp	201/tcp		# AppleTalk routing
at-rtmp	201/udp		
at-nbp	202/tcp		# AppleTalk name binding
at-nbp	202/udp		

at-echo	204/tcp		# AppleTalk echo
at-echo	204/udp		
at-zis	206/tcp		# AppleTalk zone information
at-zis	206/udp		
qmt	209/tcp		# Quick Mail Transfer
Protocol			
qmt	209/udp		# Quick Mail Transfer
Protocol			
z39.50	210/tcp	z3950 wais	# NISO Z39.50 database
z39.50	210/udp	z3950 wais	
ipx	213/tcp		# IPX
ipx	213/udp		
imap3	220/tcp		# Interactive Mail Access
imap3	220/udp		# Protocol v3
link	245/tcp	ttylink	
link	245/udp	ttylink	
rsvp_tunnel	363/tcp		
rsvp_tunnel	363/udp		
rpc2portmap	369/tcp		
rpc2portmap	369/udp		# Coda portmapper
codauth2	370/tcp		
codauth2	370/udp		# Coda authentication server
ulistserv	372/tcp	ulistserv	# UNIX Listserv
ulistserv	372/udp	ulistserv	
ldap	389/tcp		
ldap	389/udp		
svrloc	427/tcp		# Server Location Protocol
svrloc	427/udp		# Server Location Protocol
mobileip-agent	434/tcp		
mobileip-agent	434/udp		
mobileip-mn	435/tcp		
mobileip-mn	435/udp		
https	443/tcp		# MCom
https	443/udp		# MCom
snpp	444/tcp		# Simple Network Paging
Protocol			
snpp	444/udp		# Simple Network Paging
Protocol			
microsoft-ds	445/tcp		
microsoft-ds	445/udp		
kpasswd	464/tcp	kpwd	# Kerberos "passwd"
kpasswd	464/udp	kpwd	# Kerberos "passwd"
photuris	468/tcp		
photuris	468/udp		
saft	487/tcp		# Simple Asynchronous File
Transfer			
saft	487/udp		# Simple Asynchronous File
Transfer			
gss-http	488/tcp		
gss-http	488/udp		
pim-rp-disc	496/tcp		
pim-rp-disc	496/udp		
isakmp	500/tcp		
isakmp	500/udp		
gdomap	538/tcp		# GNUstep distributed objects
gdomap	538/udp		# GNUstep distributed objects
iiop	535/tcp		



iiop	535/udp		
dhcpv6-client	546/tcp		
dhcpv6-client	546/udp		
dhcpv6-server	547/tcp		
dhcpv6-server	547/udp		
rtsp	554/tcp		# Real Time Stream Control
Protocol			
rtsp	554/udp		# Real Time Stream Control
Protocol			
nntps	563/tcp		# NNTP over SSL
nntps	563/udp		# NNTP over SSL
whoami	565/tcp		
whoami	565/udp		
submission	587/tcp	msa	# mail message submission
submission	587/udp	msa	# mail message submission
npmp-local	610/tcp	dqs313_qmaster	# npmp-local / DQS
npmp-local	610/udp	dqs313_qmaster	# npmp-local / DQS
npmp-gui	611/tcp	dqs313_execd	# npmp-gui / DQS
npmp-gui	611/udp	dqs313_execd	# npmp-gui / DQS
hmmp-ind	612/tcp	dqs313_intercell	# HMMP Indication / DQS
hmmp-ind	612/udp	dqs313_intercell	# HMMP Indication / DQS
ldaps	636/tcp		# LDAP over SSL
ldaps	636/udp		# LDAP over SSL
acap	674/tcp		
acap	674/udp		
ha-cluster	694/tcp		# Heartbeat HA-cluster
ha-cluster	694/udp		# Heartbeat HA-cluster
kerberos-adm	749/tcp		# Kerberos `kadmin' (v5)
kerberos-iv	750/udp	kerberos4 kerberos-sec kdc	
kerberos-iv	750/tcp	kerberos4 kerberos-sec kdc	
webster	765/tcp		# Network dictionary
webster	765/udp		
phonebook	767/tcp		# Network phonebook
phonebook	767/udp		
rsync	873/tcp		# rsync
rsync	873/udp		# rsync
telnets	992/tcp		
telnets	992/udp		
imaps	993/tcp		# IMAP over SSL
imaps	993/udp		# IMAP over SSL
ircs	994/tcp		
ircs	994/udp		
pop3s	995/tcp		# POP-3 over SSL
pop3s	995/udp		# POP-3 over SSL
#			
# UNIX specific services			
#			
exec	512/tcp		
biff	512/udp	comsat	
login	513/tcp		
who	513/udp	whod	
shell	514/tcp	cmd	# no passwords used
syslog	514/udp		
printer	515/tcp	spooler	# line printer spooler
printer	515/udp	spooler	# line printer spooler
talk	517/udp		

ntalk	518/udp		
utime	519/tcp	unixtime	
utime	519/udp	unixtime	
efs	520/tcp		
router	520/udp	route routed	# RIP
ripng	521/tcp		
ripng	521/udp		
timed	525/tcp	timeserver	
timed	525/udp	timeserver	
tempo	526/tcp	newdate	
courier	530/tcp	rpc	
conference	531/tcp	chat	
netnews	532/tcp	readnews	
netwall	533/udp		# -for emergency broadcasts
uucp	540/tcp	uucpd	# uucp daemon
klogin	543/tcp		# Kerberized `rlogin' (v5)
kshell	544/tcp	krcmd	# Kerberized `rsh' (v5)
afpovertcp	548/tcp		# AFP over TCP
afpovertcp	548/udp		# AFP over TCP
remotefs	556/tcp	rfs_server rfs	# Brunhoff remote filesystem

```
#
# From ``PORT NUMBERS'':
#
#>REGISTERED PORT NUMBERS
#>
#>The Registered Ports are listed by the IANA and on most systems can be
#>used by ordinary user processes or programs executed by ordinary
#>users.
#>
#>Ports are used in the TCP [RFC793] to name the ends of logical
#>connections which carry long term conversations. For the purpose of
#>providing services to unknown callers, a service contact port is
#>defined. This list specifies the port used by the server process as
#>its contact port.
#>
#>The IANA registers uses of these ports as a convenience to the
#>community.
```

socks	1080/tcp	# socks proxy server
socks	1080/udp	# socks proxy server
skkserv	1178/tcp	# SKK Japanese input method
h323hostcallsc	1300/tcp	# H323 Host Call Secure
h323hostcallsc	1300/udp	# H323 Host Call Secure
ms-sql-s	1433/tcp	# Microsoft-SQL-Server
ms-sql-s	1433/udp	# Microsoft-SQL-Server
ms-sql-m	1434/tcp	# Microsoft-SQL-Monitor
ms-sql-m	1434/udp	# Microsoft-SQL-Monitor
ica	1494/tcp	# Citrix ICA Client
ica	1494/udp	# Citrix ICA Client
wins	1512/tcp	# Microsoft's Windows
Internet Name Service		
wins	1512/udp	# Microsoft's Windows
Internet Name Service		
ingreslock	1524/tcp	
ingreslock	1524/udp	
prospero-np	1525/tcp	# Prospero non-privileged

prospero-np	1525/udp		
support	1529/tcp	prmsd gnatsd	# cygnus bug tracker
datametrics	1645/tcp	old-radius	# datametrics / old radius
entry			
datametrics	1645/udp	old-radius	# datametrics / old radius
entry			
sa-msg-port	1646/tcp	old-radacct	# sa-msg-port / old radacct
entry			
sa-msg-port	1646/udp	old-radacct	# sa-msg-port / old radacct
entry			
kermit	1649/tcp		
kermit	1649/udp		
l2tp	1701/tcp		
l2tp	1701/udp		
h323gatedisc	1718/tcp		
h323gatedisc	1718/udp		
h323gatestat	1719/tcp		
h323gatestat	1719/udp		
h323hostcall	1720/tcp		
h323hostcall	1720/udp		
tftp-mcast	1758/tcp		
tftp-mcast	1758/udp		
hello	1788/tcp		
hello	1788/udp		
radius	1812/tcp		# Radius
radius	1812/udp		# Radius
radius-acct	1813/tcp	radacct	# Radius Accounting
radius-acct	1813/udp	radacct	# Radius Accounting
mtp	1911/tcp		#
mtp	1911/udp		#
hsrp	1985/tcp		# Cisco Hot Standby Router
Protocol			
hsrp	1985/udp		# Cisco Hot Standby Router
Protocol			
licensedaemon	1986/tcp		
licensedaemon	1986/udp		
gdp-port	1997/tcp		# Cisco Gateway Discovery
Protocol			
gdp-port	1997/udp		# Cisco Gateway Discovery
Protocol			
nfs	2049/tcp	nfsd	
nfs	2049/udp	nfsd	
zephyr-srv	2102/tcp		# Zephyr server
zephyr-srv	2102/udp		# Zephyr server
zephyr-clt	2103/tcp		# Zephyr serv-hm connection
zephyr-clt	2103/udp		# Zephyr serv-hm connection
zephyr-hm	2104/tcp		# Zephyr hostmanager
zephyr-hm	2104/udp		# Zephyr hostmanager
cvspserver	2401/tcp		# CVS client/server
operations			
cvspserver	2401/udp		# CVS client/server
operations			
venus	2430/tcp		# codacon port
venus	2430/udp		# Venus callback/wbc
interface			
venus-se	2431/tcp		# tcp side effects
venus-se	2431/udp		# udp sftp side effect

codasrv	2432/tcp		# not used
codasrv	2432/udp		# server port
codasrv-se	2433/tcp		# tcp side effects
codasrv-se	2433/udp		# udp sftp side effectQ
corbaloc	2809/tcp		# CORBA naming service
locator			
icpv2	3130/tcp		# Internet Cache Protocol V2
(Squid)			
icpv2	3130/udp		# Internet Cache Protocol V2
(Squid)			
mysql	3306/tcp		# MySQL
mysql	3306/udp		# MySQL
trnsprntproxy	3346/tcp		# Trnsprnt Proxy
trnsprntproxy	3346/udp		# Trnsprnt Proxy
prsvp	3455/tcp		# RSVP Port
prsvp	3455/udp		# RSVP Port
rwhois	4321/tcp		# Remote Who Is
rwhois	4321/udp		# Remote Who Is
krb524	4444/tcp		# Kerberos 5 to 4 ticket
xlator			
krb524	4444/udp		# Kerberos 5 to 4 ticket
xlator			
rfe	5002/tcp		# Radio Free Ethernet
rfe	5002/udp		# Actually uses UDP only
cfengine	5308/tcp		# CFengine
cfengine	5308/udp		# CFengine
cvsup	5999/tcp	CVSup	# CVSup file transfer/John
Polstra/FreeBSD			
cvsup	5999/udp	CVSup	# CVSup file transfer/John
Polstra/FreeBSD			
x11	6000/tcp	X	# the X Window System
afs3-fileserver	7000/tcp		# file server itself
afs3-fileserver	7000/udp		# file server itself
afs3-callback	7001/tcp		# callbacks to cache managers
afs3-callback	7001/udp		# callbacks to cache managers
afs3-prserver	7002/tcp		# users & groups database
afs3-prserver	7002/udp		# users & groups database
afs3-vlserver	7003/tcp		# volume location database
afs3-vlserver	7003/udp		# volume location database
afs3-kaserver	7004/tcp		# AFS/Kerberos authentication
service			
afs3-kaserver	7004/udp		# AFS/Kerberos authentication
service			
afs3-volser	7005/tcp		# volume managment server
afs3-volser	7005/udp		# volume managment server
afs3-errors	7006/tcp		# error interpretation
service			
afs3-errors	7006/udp		# error interpretation
service			
afs3-bos	7007/tcp		# basic overseer process
afs3-bos	7007/udp		# basic overseer process
afs3-update	7008/tcp		# server-to-server updater
afs3-update	7008/udp		# server-to-server updater
afs3-rmtsys	7009/tcp		# remote cache manager
service			
afs3-rmtsys	7009/udp		# remote cache manager
service			

```

sd                9876/tcp                # Session Director
sd                9876/udp                # Session Director
amanda            10080/tcp               # amanda backup services
amanda            10080/udp               # amanda backup services
h323callsigalt    11720/tcp               # H323 Call Signal Alternate
h323callsigalt    11720/udp               # H323 Call Signal Alternate
quake            26000/tcp                #
quake            26000/udp                #
wnn6-ds           26208/tcp                #
wnn6-ds           26208/udp                #
traceroute        33434/tcp                #
traceroute        33434/udp                #

#
# Datagram Delivery Protocol services
#
rtmp              1/ddp                   # Routing Table Maintenance
Protocol
nbp              2/ddp                   # Name Binding Protocol
echo             4/ddp                   # AppleTalk Echo Protocol
zip              6/ddp                   # Zone Information Protocol
#
# Kerberos (Project Athena/MIT) services
# Note that these are for Kerberos v4, and are unofficial.  Sites running
# v4 should uncomment these and comment out the v5 entries above.
#
kerberos_master   751/udp                 # Kerberos authentication
kerberos_master   751/tcp                 # Kerberos authentication
passwd_server     752/udp                 # Kerberos passwd server
krbupdate         760/tcp                 kreg  # Kerberos registration
kpop              1109/tcp                 # Pop with Kerberos
knetd             2053/tcp                 # Kerberos de-multiplexor
#
# Kerberos 5 services, also not registered with IANA
#
krb5_prop         754/tcp                 # Kerberos slave propagation
eklogin           2105/tcp                 # Kerberos encrypted rlogin
#
# Unofficial but necessary (for NetBSD) services
#
supfilesrv        871/tcp                 # SUP server
supfiledbg        1127/tcp                 # SUP debugging
#
# Unofficial but useful/necessary other services
#
netstat           15/tcp                   # (was once assigned, no
more)
fsp              21/udp                    fspd  #
linuxconf         98/tcp                   # Linuxconf HTML access
poppassd          106/tcp                   # Eudora
poppassd          106/udp                   # Eudora
smtps             465/tcp                   # SMTP over SSL (TLS)
gii              616/tcp                   # gated interactive interface
omirr            808/tcp                    omirrd # online mirror
omirr            808/udp                    omirrd # online mirror
swat              901/tcp                   # Samba Web Administration
Tool

```

rmtcfg	1236/tcp	# Gracilis Packeten remote
config server		
xtel	1313/tcp	# french minitel
support	1529/tcp	# GNATS
cfinger	2003/tcp	# GNU Finger
ninstall	2150/tcp	# ninstall service
ninstall	2150/udp	# ninstall service
afbackup	2988/tcp	# Afbbackup system
afbackup	2988/udp	# Afbbackup system
squid	3128/tcp	# squid web proxy
postgres	5432/tcp	# POSTGRES
postgres	5432/udp	# POSTGRES
fax	4557/tcp	# FAX transmission service
(old)		
hylafax	4559/tcp	# HylaFAX client-server
protocol (new)		
sgi-dgl	5232/tcp	# SGI Distributed Graphics
sgi-dgl	5232/udp	
noclog	5354/tcp	# noclogd with TCP (nocol)
noclog	5354/udp	# noclogd with UDP (nocol)
hostmon	5355/tcp	# hostmon uses TCP (nocol)
hostmon	5355/udp	# hostmon uses TCP (nocol)
ircd	6667/tcp	# Internet Relay Chat
ircd	6667/udp	# Internet Relay Chat
xfs	7100/tcp	# X font server
tircproxy	7666/tcp	# Tircproxy
http-alt	8008/tcp	
http-alt	8008/udp	
webcache	8080/tcp	# WWW caching service
webcache	8080/udp	# WWW caching service
tpoxy	8081/tcp	# Transparent Proxy
tpoxy	8081/udp	# Transparent Proxy
jetdirect	9100/tcp	# laserjet hplj
mandelspawn	9359/udp	# mandelbrot
kamanda	10081/tcp	# amanda backup services
(Kerberos)		
kamanda	10081/udp	# amanda backup services
(Kerberos)		
amandaidx	10082/tcp	# amanda backup services
amidxtape	10083/tcp	# amanda backup services
isdnlog	20011/tcp	# isdn logging system
isdnlog	20011/udp	# isdn logging system
vboxd	20012/tcp	# voice box system
vboxd	20012/udp	# voice box system
binkp	24554/tcp	# Binkley
binkp	24554/udp	# Binkley
asp	27374/tcp	# Address Search Protocol
asp	27374/udp	# Address Search Protocol
tfido	60177/tcp	# Ifmail
tfido	60177/udp	# Ifmail
fido	60179/tcp	# Ifmail
fido	60179/udp	# Ifmail

# Local services

[root@idunn list2]# exit

Script done on Wed Jul 18 23:05:10 2001

## Nmap TCP SYN (half-open) scans

Command: `nmap -sS 192.168.1.1`

[Back to chapter 3.3](#)

### Output:

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host (192.168.1.1) appears to be up ... good.
Initiating SYN half-open stealth scan against (192.168.1.1)
Adding TCP port 111 (state open).
Adding TCP port 514 (state open).
Adding TCP port 25 (state open).
Adding TCP port 23 (state open).
Adding TCP port 22 (state open).
Adding TCP port 513 (state open).
Adding TCP port 79 (state open).
Adding TCP port 80 (state open).
Adding TCP port 6000 (state open).
Adding TCP port 443 (state open).
Adding TCP port 21 (state open).
The SYN scan took 1 second to scan 1523 ports.
For OSScan assuming that port 21 is open and port 1 is closed and neither are firewalled
For OSScan assuming that port 21 is open and port 1 is closed and neither are firewalled
For OSScan assuming that port 21 is open and port 1 is closed and neither are firewalled
Interesting ports on (192.168.1.1):
(The 1516 ports scanned but not shown below are in state: closed)
Port      State      Service
21/tcp    open       ftp
22/tcp    open       ssh
23/tcp    open       telnet
25/tcp    open       smtp
79/tcp    open       finger
80/tcp    open       http
111/tcp   open       sunrpc
443/tcp   open       https
513/tcp   open       login
514/tcp   open       shell
6000/tcp  open       X11

TCP Sequence Prediction: Class=random positive increments
```

Difficulty=4845611 (Good luck!)

Sequence numbers: 438AA931 444823F0 445214E8 4436AA6B 439D2979 43BD2C5E

No OS matches for host (If you know what OS is running on it, see <http://www.insecure.org/cgi-bin/nmap-submit.cgi>).

TCP/IP fingerprint:

TSeq (Class=RI%gcd=1%SI=49F6E5)

TSeq (Class=RI%gcd=1%SI=49EFEE)

TSeq (Class=RI%gcd=1%SI=49F02B)

T1 (Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)

T2 (Resp=N)

T3 (Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)

T4 (Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)

T5 (Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)

T6 (Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)

T7 (Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)

PU (Resp=Y%DF=Y%TOS=C0%IPLEN=164%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Nmap run completed -- 1 IP address (1 host up) scanned in 90 seconds



## Nmap TCP Connect

Command: `nmap -sT 192.168.1.1`

[Back to chapter 3.4](#)

### Output

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host (192.168.1.1) appears to be up ... good.
Initiating TCP connect() scan against (192.168.1.1)
Adding TCP port 22 (state open).
Adding TCP port 79 (state open).
Adding TCP port 443 (state open).
Adding TCP port 111 (state open).
Adding TCP port 514 (state open).
Adding TCP port 25 (state open).
Adding TCP port 513 (state open).
Adding TCP port 23 (state open).
Adding TCP port 80 (state open).
Adding TCP port 6000 (state open).
Adding TCP port 21 (state open).
The TCP connect scan took 2 seconds to scan 1523 ports.
For OSScan assuming that port 21 is open and port 1 is closed and neither are firewalled
For OSScan assuming that port 21 is open and port 1 is closed and neither are firewalled
For OSScan assuming that port 21 is open and port 1 is closed and neither are firewalled
Interesting ports on (192.168.1.1):
(The 1516 ports scanned but not shown below are in state: closed)
Port      State      Service
21/tcp    open       ftp
22/tcp    open       ssh
23/tcp    open       telnet
25/tcp    open       smtp
79/tcp    open       finger
80/tcp    open       http
111/tcp   open       sunrpc
443/tcp   open       https
513/tcp   open       login
514/tcp   open       shell
6000/tcp  open       X11

TCP Sequence Prediction: Class=random positive increments
```

Difficulty=1064038 (Good luck!)

Sequence numbers: 33DF27C4 34093318 33D67114 33C926B5 34078F8C 3430D125

No OS matches for host (If you know what OS is running on it, see <http://www.insecure.org/cgi-bin/nmap-submit.cgi>).

TCP/IP fingerprint:

TSeq(Class=RI%gcd=1%SI=103CAD)

TSeq(Class=RI%gcd=1%SI=103C55)

TSeq(Class=RI%gcd=1%SI=103C66)

T1 (Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)

T2 (Resp=N)

T3 (Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)

T4 (Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)

T5 (Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)

T6 (Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)

T7 (Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)

PU (Resp=Y%DF=Y%TOS=C0%IPLEN=164%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Nmap run completed -- 1 IP address (1 host up) scanned in 124 seconds

## Nmap UDP

Command: `nmap -sU 192.168.1.1`

[Back to chapter 3.4](#)

### Output:

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host (192.168.1.1) appears to be up ... good.
Initiating FIN, NULL, UDP, or Xmas stealth scan against (192.168.1.1)
Too many drops ... increasing senddelay to 50000
Too many drops ... increasing senddelay to 100000
Too many drops ... increasing senddelay to 200000
Too many drops ... increasing senddelay to 400000
Too many drops ... increasing senddelay to 800000
The UDP or stealth FIN/NULL/XMAS scan took 1472 seconds to scan 1448 ports.
Warning: No TCP ports found open on this machine, OS detection will be MUCH less reliable
Interesting ports on (192.168.1.1):
(The 1446 ports scanned but not shown below are in state: closed)
Port      State      Service
111/udp    open       sunrpc
907/udp    open       unknown

Remote OS guesses: Linux 2.3.49 x86, Linux 2.3.99-pre2 x86

Nmap run completed -- 1 IP address (1 host up) scanned in 1483 seconds
```

## Tiger

Security scripts \*\*\* 2.2.3, 1994.0309.2038 \*\*\*

Mon Jul 16 22:38:49 EDT 2001

22:38> Beginning security report for idunn (i686 Linux 2.4.2-2).

# Performing check of passwd files...

# Performing check of group files...

[Back to chapter 3.3.3](#)

# 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 daemon is disabled, but still has a valid shell (/bin/sh).

--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 gopher is disabled, but still has a valid shell (/bin/sh).

--WARN-- [acc001w] Login ID lp is disabled, but still has a valid shell (/bin/sh).

--WARN-- [acc001w] Login ID mysql is disabled, but still has a valid shell (/bin/bash).

--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 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).

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

# Checking accounts from /etc/passwd...

# Performing check of .netrc files...

# Checking accounts from /etc/passwd...

[Back to chapter 3.6.4](#)

# Performing check of PATH components...

# Only checking user 'root'

--WARN-- [path002w] /usr/bin/cancel in root's PATH from default is not owned by root (owned by lp).

--WARN-- [path002w] /usr/bin/lp in root's PATH from default is not owned by root (owned by lp).

--WARN-- [path002w] /usr/bin/lpq in root's PATH from default is not owned by

```

    root (owned by lp).
--WARN-- [path002w] /usr/bin/lpr in root's PATH from default is not owned by
    root (owned by lp).
--WARN-- [path002w] /usr/bin/lprm in root's PATH from default is not owned by
    root (owned by lp).
--WARN-- [path002w] /usr/bin/lpstat in root's PATH from default is not owned
    by root (owned by lp).

# Performing check of anonymous FTP...
--ERROR-- [init004e] `0' is not executable (command GROUPS).

# 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-- [inet002f] Service link is assigned to port 245/tcp which should be
    87/tcp.
--FAIL-- [inet002f] Service link is assigned to port 245/ucp which should be
    87/tcp.
--FAIL-- [inet002f] Service mtp is assigned to port 1911/tcp which should be
    57/tcp.
--FAIL-- [inet002f] Service mtp is assigned to port 1911/udp which should be
    57/tcp.
--FAIL-- [inet002f] Service rje is assigned to port 5/tcp which should be
    77/tcp.
--FAIL-- [inet002f] Service rje is assigned to port 5/udp which should be
    77/tcp.
--FAIL-- [inet003f] The port for service dos is assigned to service
    afs3-fileserver.
--FAIL-- [inet003f] The port for service hostnames is assigned to service
    hostname.
--FAIL-- [inet003f] The port for service irc is assigned to service ircd.
--FAIL-- [inet003f] The port for service name is assigned to service
    nameserver.
--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 route is assigned to service router.
--FAIL-- [inet003f] The port for service snmp-trap is assigned to service
    snmptrap.
--FAIL-- [inet003f] The port for service whois is assigned to service
    nicname.
# Checking inetd entries from /etc/inetd.conf

# Performing NFS exports check...

```

[Back to chapter 3.6.4](#)

[Back to chapter 3.6.4](#)

```
# Performing check of system file permissions...
```

[Back to chapter 3.6.4](#)

```
--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.
--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.
```

```
>>>>> Linux 2.0.35
```

```
# Checking for known intrusion signs...
```

```
--WARN-- [kis004w] /lost+found is not empty:
Files:
```

```
# 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...
```

[Back to chapter 3.6.4](#)

```
--WARN-- [fsys002w] setuid program /usr/bin/rnews has relative pathnames.
--WARN-- [fsys002w] setuid program /usr/bin/sperl5.6.0 has relative
pathnames.
--WARN-- [fsys002w] setuid program /usr/bin/suidperl 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/sbin/suexec has relative pathnames.
--WARN-- [fsys002w] setuid program /usr/sbin/uucico has relative pathnames.
--WARN-- [fsys002w] setuid program /usr/sbin/uuxqt has relative pathnames.
```

```
-r-sr-x--- root      news      /usr/bin/inndstart
-r-sr-x--- root      news      /usr/bin/startinnfeed
-r-sr-xr-x root      root      /sbin/unix_chkpwd
-r-sr-x--- uucp      news      /usr/bin/rnews
-r-s--x--- root      apache    /usr/sbin/suexec
-rwsr-xr-x root      root      /usr/bin/kcheckpass
-rwsr-xr-x root      root      /usr/bin/ssh
```

```

-rws--x--x root      root      /usr/bin/sperl5.6.0
---s--x--x root      root      /usr/bin/sudo

# 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:
/usr/programs/bridge/BRCFG/
/var/lock/xemacs/
/var/spool/samba/
/var/spool/vbox/
--WARN-- [xxxxx] The following files are unowned:
/usr/programs/bridge/*
/usr/programs/firewall/*
/usr/programs/security/*

# Performing check of embedded pathnames... Back to chapter 3.6.4
--WARN-- [embed002w] Path `/etc/rc.news' is not owned by root (owned by
news).
Embedded references in: /etc/rc.d/init.d/innd
--WARN-- [embed001w] Path `/proc/self/exe' contains
`/usr/programs/security/tiger/tiger-2.2.4p1' which is not owned by
root (owned by 2566).
Embedded references in: /bin/ash.static->/default (PATH)
                        /bin/rpm->/default (PATH)
                        /usr/bin/db_dump185->/default (PATH)
                        /usr/bin/statserial->/default (PATH)
--WARN-- [embed001w] Path `/proc/self/exe' contains
`/usr/programs/security/tiger/tiger-2.2.4p1/bin' which is not owned
by root (owned by 2566).
Embedded references in: /bin/ash.static->/default (PATH)
                        /bin/rpm->/default (PATH)
                        /usr/bin/db_dump185->/default (PATH)
                        /usr/bin/statserial->/default (PATH)
--WARN-- [embed002w] Path `/usr/sbin/lpc' is not owned by root (owned by lp).
Embedded references in: /usr/bin/klpq->/default (PATH)

```

## RPM Report

Command: rpm -Va

[Back to chapter 5.3](#)

Output:

```
Script started on Wed Jul 18 23:44:07 2001
[root@idunn list1]# rpm -Va
```

```
.M..... /var/spool/at/.SEQ
S.5....T c /usr/share/a2ps/afm/fonts.map
S.5....T /usr/lib/mozilla/component.reg
S.5....T /usr/lib/mozilla/components/xpti.dat
S.5....T /usr/lib/mozilla/components/xptitemp.dat
missing /etc/rpm/macros.db1
..5....T c /etc/inittab
S.5....T c /etc/sysconfig/network-scripts/ifcfg-lo
..5....T c /etc/sysctl.conf
SM5....T /usr/X11R6/lib/X11/fonts/Speedo/encodings.dir
.M.....T /usr/X11R6/lib/X11/fonts/Speedo/fonts.dir
SM5....T /usr/X11R6/lib/X11/fonts/Type1/encodings.dir
.M.....T /usr/X11R6/lib/X11/fonts/Type1/fonts.dir
S.5....T /usr/X11R6/lib/X11/fonts/misc/fonts.dir
.....T /usr/share/apps/kfind/icons/locolor/22x22/actions/archive.png
.....T /usr/share/apps/kfind/icons/locolor/22x22/actions/delete.png
.....T /usr/share/apps/kfind/icons/locolor/22x22/actions/idea.png
.....T /usr/share/apps/kfind/icons/locolor/22x22/actions/info.png
.....T /usr/share/apps/kfind/icons/locolor/22x22/actions/openfile.png
.....T /usr/share/apps/kfind/icons/locolor/22x22/actions/save.png
.....T /usr/share/apps/kfind/icons/locolor/22x22/actions/search.png
S.5....T c /etc/httpd/conf/httpd.conf
S.5....T c /etc/named.conf
S.5....T c /etc/printcap
.M..... /dev/console
.M....G. /dev/jsfd
.....G. /dev/tty0
.M....G. /dev/tty1
.M....G. /dev/tty2
.M....G. /dev/tty3
.M....G. /dev/tty4
.M....G. /dev/tty5
.M....G. /dev/tty6
.....G. /dev/tty7
S.5....T c /etc/syslog.conf
.....T c /etc/pam.d/system-auth
S.5....T c /etc/openldap/ldap.conf
S.5....T c /etc/ldap.conf
S.5....T /boot/kernel.h-2.4.2
.....T /lib/modules/2.4.2-2/modules.dep
.....T /lib/modules/2.4.2-2/modules.generic_string
.....T /lib/modules/2.4.2-2/modules.isapnpmap
.....T /lib/modules/2.4.2-2/modules.parportmap
.....T /lib/modules/2.4.2-2/modules.pcimap
.....T /lib/modules/2.4.2-2/modules.usbmap
S.5....T c /etc/ppp/pppoe.conf
```



```

.M..... /usr/bin/filter
.M..... c /etc/logrotate.d/ftpd
S.5....T c /etc/alchemy/namespace/apache/local.adl
SM5....T c /etc/conf.linuxconf
missing   /etc/ntp/drift
missing   /etc/ntp/step-tickers
missing   /usr/share/ssl/certs/stunnel.pem
missing   /var/cache/ssl_gcache_data.dir
missing   /var/cache/ssl_gcache_data.pag
missing   /var/cache/ssl_gcache_data.sem
..5....T c /etc/mime.types
S.5....T c /etc/ppp/chap-secrets
S.5....T c /etc/ppp/pap-secrets
.....T c /etc/krb5.conf
..5....T /usr/lib/rhs/python/Conf.pyc
..5....T /usr/lib/rhs/python/PasswordCrypt.pyc
..5....T /usr/lib/rhs/python/buttonbar.pyc
..5....T /usr/lib/rhs/python/foldertabs.pyc
..5....T /usr/lib/rhs/python/listbox.pyc
..5....T /usr/lib/rhs/python/rhdialog.pyc
..5....T /usr/lib/rhs/python/rhentry.pyc
..5....T /usr/lib/rhs/python/rhtkinter.pyc
..5....T /usr/lib/rhs/python/rhutil.pyc
..5....T /usr/lib/rhs/python/textbox.pyc
missing   /etc/identd.key
S.5....T c /etc/X11/fs/config
.....T c /etc/yp.conf
S.5....T c /etc/xinetd.conf
S.5....T c /etc/php.ini
SM5..UGT c /etc/rndc.conf
missing   /var/log/mysqld.log

```

```
[root@idunn list2]# exit
```

```
Script done on Wed Jul 18 23:09:10 2001
```

© SANS Institute 2000 - 2002, Author retains full rights.

## Appendix B

Links to tools used or recommended in the audit:

Tiger: <ftp://net.tamu.edu/pub/security/TAMU/tiger-2.2.4p1.tar.gz>

Nmap: <http://www.insecure.org/nmap/dis/nmap-2.53.tgz>

Crack: <ftp://coast.cs.purdue.edu/pub/tools/unix/pwdutils/crack/crack5.0.tar.gz>

Tripwire: <ftp://coast.cs.purdue.edu/pub/tools/unix/ids/Tripwire/tripwrie-1.2.tar.Z>

Logcheck: <http://www.psionic.com/abacus/logcheck/>

SUDO: <http://www.courtesan.com/sudo>

Passwd+: <ftp://nob.cs.ucdavis.edu/pub/sec-tools/passwd+beta.tar>

© SANS Institute 2000 - 2002, Author retains full rights.