Global Information Assurance Certification Paper

Linux Firewall Audit
GIAC Enterprises

Elaine Madison
GCUX Version 1.9, Option 2 - Consultant's Report from Auditing Unix

Table of Contents

Executive Summary	3
Section 1 – System and Audit Methodology	4
Section 2 – Detailed Analysis	7
Section 3 – Critical Issues and Recommendations	22
References	30
Appendix A – Installed RPM's	31
Appendix B – CISscan output	34
Appendix C – Nmap output	39
Appendix D – Suid/Sguid Files	45
Appendix E – Firewall Rules	47

Executive Summary

GIAC Enterprises has contracted with the Security and Auditing Team (SAT) to conduct a security audit of their firewalls. The firewalls audited by SAT have been identified as critical systems on the GIAC Enterprises network. Without these systems, your business loses Internet access, an essential component of your daily email and web communications with GIAC Enterprises customers.

Both of the audited systems have been found to be in critical need of software updates and regular monitoring. Servers connected to the Internet are always targets for attackers; this is one reason why maintenance is so important. With an out-dated server it is more likely a matter of when it will be compromised then if it will be a target. An attack on your systems can mean unplanned and possibly lengthy downtime to recover the systems. However, updating the servers alone will not completely protect your systems. A written plan needs to be established regarding the network security requirements of your business and the network access necessary to carry out your business functions. Once this has been completed, you will be able to assess if the current firewall configuration meets your needs and how to implement new requirements in the future as your business grows.

The purpose of the systems should also be a factor in determining what applications are running on the servers. Telnet (remote server access) and DNS (domain name resolution used for accessing servers by name) are both insecure services. Telnet can be replaced with Secure Shell (ssh) if remote access is required. DNS should be moved to an application server.

Consideration should also be given to the risk of one or both of these servers being down and the cost associated with that downtime. Then comprehensive backup and disaster recovery plans can be developed to ensure that the business risk and costs are at an acceptable level.

Since significant changes need to be made to the operating system software and installed applications, SAT recommends installing and running the scanning tools Nmap and CISscan after the upgrades have been completed to reassess the vulnerabilities of the servers. These scans can also be run on a regular basis (always check for current versions) to make sure no new vulnerabilities have surfaced.

Section 1 – System and Audit Methodology

GIAC Enterprises has two firewalls, firewall-x and firewall-i, that were installed several years ago by a vendor who is no longer available to service the systems. The purpose of this audit is to establish "where do we stand" with these systems. GIAC Enterprises is an e-business, and as such requires a stable and secure Internet connection to maintain communications with their customers and suppliers. The two firewalls create a demilitarized zone (DMZ) for the web/email server used by customers and GIAC employees. GIAC Enterprises local area networks (LAN's) are behind the firewall firewall-i; LAN's are using private network addresses.

Firewall-x Server
IP Address: 10.10.229.113
Operating System: Redhat Linux 7.1
Hardware: Intel Celeron 466 MHz CPU
64Mb RAM
4Gb IDE Hard Disk
Packages and Versions:

OpenSSH	2.1.1, protocol version 1.5/2.0
named	8.2.2-P5
ipchains	1.3.9
kernel	2.2.16-22

Primary Role: Firewall-x is the bastion firewall and primary domain name server (secondary DNS is provided by a 3rd party service) for GIAC Enterprises. The firewall-x server is a packet filtering firewall with interfaces to the Internet and the DMZ. This server is the gateway to the businesses' Internet communication with customers and suppliers.

The risks to this server are attacks from the Internet, the DMZ and the Internal LAN's. A compromise of this server could have several outcomes:

- Loss of Internet access for GIAC Enterprises
- Loss of access for customers to the web server
- Loss of DNS service (which will appear to web/email users as if the network is down)
- There is also the potential for an attacker to subvert the firewall, ssh or DNS configurations and use the server for their own purposes.
- Use of this server as a stepping stone to attack another server on the DMZ

Firewall-I Server
IP Address: 10.10.229.114
Operating System: Redhat Linux 6.1
Hardware: Intel Celeron 466 MHz CPU
64Mb RAM
4Gb IDE Hard Disk

Packages and Versions:

DHCP	2.0-3
OpenSSH	2.1, protocol version 1.5/2.0
ipchains	1.3.9
kernel	2.2.12-20

Primary Role: Firewall-i is the choke firewall for GIAC Enterprises.
The firewall-i server is a packet filtering firewall with interfaces to the internal LAN's and the DMZ. Firewall-i also provides network address translation (NAT), and Dynamic Host Configuration Protocol (DHCP) for the LAN's.

The risks for this server are similar to those for firewall-x from a network standpoint. A compromise of this server could drastic effects on the Internal LAN systems.

- Loss of Internet access for GIAC Enterprises
- Loss of employee email access
- Loss of employee access to the company web server
- Loss of DNS service
- The potential for an attacker to subvert the firewall, and use the server for their own purposes.
- A compromise of this server could give an attacker access to the systems on the Internal LAN's.

It is critical for business continuity that both of these servers to be configured in a very secure manner.

1.1 Network Infrastructure

The company's network is a star topology. The firewall-x acts as a router connected to the Internet provider and the DMZ. Firewall-i acts as a router between the GIAC Enterprises private LAN's and the DMZ. The current topology was selected to allow for growth in the DMZ and the company's LAN's.

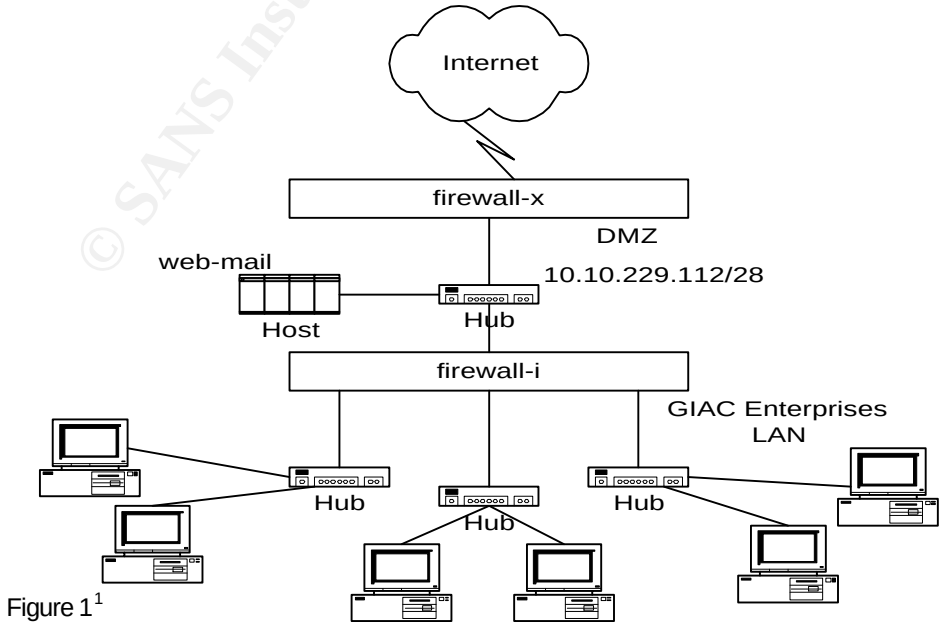

Figure 1[1]

1.2 Audit Methodology

The audit conducted by SAT addressed three areas of security physical, technical and administrative. An onsite review of the physical access to the hosts included interviews to establish what practices were being used to allow users to access to the computer room. A review of the security policies found that no formal documentation of security policies exists. There is an expectation the firewall will provide the necessary network protection and should be as restrictive as possible, without impeding communication with the customer. Employees are expected to be honest and conduct business with the company's best interests and security in mind.

The technical review was accomplished using scanning tools at the host and network levels, and manual host configuration analysis. The scanning tool Nmap version 3.0 was run from a host on the Internet for a view of what the world could see; and from the host "firewall-x" to assess vulnerabilities of the DMZ servers if the firewall-x host were compromised. The CISscan^2 version 1.2 tool was installed on "firewall-x" and "firewall-i" for host based scanning. The configuration analysis was accomplished using a terminal session on the host. The manual analysis included reviewing system configuration files (using cat), reviewing the process list for unnecessary processes (using ps -ef), running netstat to check which ports where listening, and a password and account review. SAT also used the command "find" to scan the file systems for suid files, devices files located outside of the /dev directory, and regular files in the /dev directory.

Host scanning and configuration analysis of the web-email server is not in the scope of this audit. Network scanning output is provided as information for administrators to validate what ports they believe are open.

Section 2 – Detailed Analysis

2.1 Operating System Vulnerabilities

There is no documentation on the installation procedures followed for installing the O/S on the systems audited. The consulting firm hired to do the installation and has since gone out of business. The operating system installed on firewall-i, Redhat Linux version 6.1 no longer has errata support[3]. Firewall-x has Redhat Linux version 7.1, the operating system on this server was updated in April 2001 after it was determined that the host had been compromised. Redhat Linux 7.1 will be supported through December 2003[4]. Once patch support for an operating system has been discontinued there is no fix for known vulnerabilities. This makes the servers a target for attackers.

Currently, there is no procedure in place for monitoring necessary Operating System updates or patch installation and management. A review of the Red Hat Linux 7.1 Security Advisories web page showed there have been 141 security patches released since April 2001. A manual check of security patches by running the command "rpm --query <service name>" for each patch and then comparing then version with the errata information on the web site did not find any that had been applied. Patches fix known vulnerabilities; an unpatched server whether at the O/S level or application level is a target for attackers looking for machines with specific vulnerabilities. Red Hat Network[5] has a service that helps automate the patching process and notify you when your system needs updates based on a system profile. This service could be beneficial to GIAC Enterprises for identifying new patches that need installed.

2.2 Configuration vulnerabilities – Scanner output

The Center for Internet Security (CIS), a group whose mission is to help organizations manage the risks related to information security has developed a benchmark-scanning tool CISscan[2]. CISscan, a host-based scanner checks specific configuration files against best-practice security configurations and provides a score for each system. The specifications for these configurations have been developed by a large group of organizations and security professionals. The CISscan was run on the firewall-x and firewall-i hosts; the score for firewall-x was 5.89, firewall-i received a 6.07 of a possible 10. Appendix B shows the entire output for each host. The negative results are analyzed below.

Negative: 1.1 System appears not to have been patched within the last month.

Patches are how known problems and security holes in the operating system and applications get fixed. Redhat releases patches for bug fixes and

enhancements quarterly and security patches as needed. The patches should be applied on a regularly as they become available.

Negative: 2.2 No Authorized Only banner for telnet in file etc/xinetd.d/telnet.
Negative: 2.2 No Authorized Only banner for login in file etc/xinetd.d/rlogin.

The "Authorized Only" banner for these hosts is in /etc/issue. No action needed.

Negative: 2.3 telnet not deactivated.

Telnet service is being used for remote access the server; telnet does not provide secure access. SAT recommends deactivating telnet. To deactivate telnet on firewall -x, edit the /etc/xinetd.conf file and add the line "disabled = telnet". Additionally, the line "disable = yes" can be added to the /etc/xinetd.d/telnet file.

To deactivate telnet on firewall-i, edit the /etc/inetd.conf file and remove the entry:
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd

Once the changes have been made the xinetd or inetd process needs to reread its configuration file. This can be accomplished by restarting the service or with the command "kill -HUP <pid>".

Ssh should be used if remote access is necessary.

Negative: 2.5 rsh (shell) should be deactivated.
Negative: 2.5 rlogin (rlogin) should be deactivated.
Negative: 2.7 xinetd either requires global 'only-from' statement or one for each service.

The shell and login commands have been disabled in the /etc/xinetd.conf file but, not in the related files in the /etc/xinetd.d directory. SAT recommends adding the line "disabled = yes" to the rsh and rlogin files in the /etc/xinetd.d directory.

The 'only_from' statement allows the administrator to specify which hosts can use a specific service. The statement can be added to the file for each service in the /etc/xinetd.d directory (e.g. telnet) or set globally in the /etc/xinetd.conf file. The entry will look something like "only_from = 10.10.229.114" which would allow access from GIAC's LAN's. Multiple IP addresses can be defined in each entry, use a space to separate the IP addresses.

The changes to xinetd configuration files will become effective when it is either restarted or you send it a signal using the "kill -SIGUSR1 <pid>" command to the service. Pid is the process id found by the command "ps -ef | grep xinetd".

Once telnet has been disabled, there will be no need to run xinetd; xinetd should then be removed from the server.

Negative: 3.1 apmd not deactivated.
Negative: 3.1 gpm not deactivated.
Negative: 3.6 portmapper not deactivated.

The apmd(Advanced Power Management), gpm(mouse server for virtual consoles) and portmapper(RPC program mapper) services are not needed on these servers. SAT recommends the unneeded process be stopped using their respective startup/shutdown scripts in /etc/rc.d/init.d (e.g. /etc/rc.d/init.d/apmd stop) and then disabled from startup using the "chkconfig --level 2345 <service name> off" command.

Negative: 3.14 named DNS server not deactivated.

The name server is providing primary domain name service for two domains. Historically, DNS servers have been vulnerable to attacks, this services is better suited to an application server.

Negative: 3.19 xinetd is still active.

Xinetd should be removed from the host firewall-x once telnet has been disabled. To remove xinetd from the server:

- shutdown xinetd - /etc/rc.d/init.d/xinetd stop
- find the name of the installed package – rpm --query xinetd
- remove the package – rpm -e xinetd-2.1.8.9pre9-6

Negative: 3.20 umask not found in first /etc/rcX.d script /etc/rc3.d/S05kudzu

Kudzu is used to detect new/changed hardware on the system, only and administrator should be using this feature. SAT recommends the umask be set to 077 in the script.

Negative: 4.1 Coredumps aren't deactivated.

Core dump analysis should not be needed on the applications running on these hosts. The core dump size can be identified using the command ulimit -c. Setting the core dump size can be done in the /etc/profile for all users using the command "ulimit -c 0". Be aware, users can reset this setting.

Negative: 4.3 IP forwarding is activated.

These systems need IP forwarding to route between networks. No action is necessary.

Negative: 4.3 /proc/sys/net/ipv4/tcp_max_syn_backlog should be at least 4096 to handle SYN floods.

A SYN flood[6] attack sends TCP connection requests faster than the host can process them. The current value is 128, raising the value to 4096 will help mitigate the affects of these attacks. To raise the value 4096, run the command "echo 4096 > /proc/sys/net/ipv4/tcp_max_syn_backlog"[7].

Negative: 4.4 /proc/sys/net/ipv4/conf/eth1/send_redirects should be 0 to disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/eth0/send_redirects should be 0 to disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/lo/send_redirects should be 0 to disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/default/send_redirects should be 0 to disable outgoing redirect messages.

ICMP redirects are messages that tell a host to use another gateway[6]. Turning off redirects will mean that the server does not send any ICMP redirect packets. To turn off ICMP redirects, change the 1 in each of these files to a 0 (e.g. "echo 0 > /proc/sys/net/ipv4/conf/eth1/send_redirects"[7]).

Negative: 6.1 Removable filesystem /mnt/floppy is not mounted nosuid.
Negative: 6.2 PAM allows users to mount CD-ROMS. (/etc/security/console.perms)
Negative: 6.2 PAM allows users to mount floppies. (/etc/security/console.perms)

Users do not need to mount floppies on these servers, this feature is restricted by removing the following lines in the /etc/security/console.perms file:
<console> 0660 <floppy> 0660 root.floppy
<console> 0600 <cdrom> 0600 root.disk

Negative: 7.1 rhosts authentication not deactivated in /etc/pam.d/rlogin.
Negative: 7.1 rhosts authentication not deactivated in /etc/pam.d/rsh.

Remote rhosts authentication requires "trust" to be established between two hosts and allows users to login to the other host without a password. Establishing this kind of trust means the compromise of one host can lead directly to the compromise of all other trusted hosts, this is very dangerous, especially when the business of your host is security. To deactivate rhosts authentication, edit the file remove the lines that begin with auth in these two files[7].

/etc/pam.d/rlogin – lines to remove

```
auth       required     /lib/security/pam_securetty.so
auth       sufficient   /lib/security/pam_rhosts_auth.so
auth       required     /lib/security/pam_pwdb.so shadow nullok
auth       required     /lib/security/pam_nologin.so
```

/etc/pam.d/rsh – lines to remove

```
auth       required     /lib/security/pam_rhosts_auth.so
auth       required     /lib/security/pam_nologin.so
```

Negative: 7.3 /etc/ftpusers doesn't exist

/etc/ftpusers does not allow the users listed in the file to login via ftp. Ftp is disabled on firewall-x, and ftp access is blocked on the firewall. Adding the users in /etc/passwd to the /etc/ftpusers file is another safeguard to preventing users from logging on through ftp if it was accidentally enabled. The format of the file is a single account name per line.

Negative: 7.4 Couldn't open cron.allow
Negative: 7.4 Couldn't open at.allow

Only the root account should be able to set up “cron” and “at” jobs on these hosts. Create the files /etc/cron.allow and /etc/at.allow each with the entry “root” to restrict access to these jobs.

Negative: 7.5 The permissions on /etc/crontab are not sufficiently restrictive.

The system crontab file is world readable, which allows any user on the system to view the file. The jobs that are referenced in this file are also world readable, which could give valuable information about your system to an attacker. The permissions on these files should be modified so that only root has access. Use the command chmod -R go-rwx /etc/cron* to correct the file permissions.

Negative: 7.6 No Authorized Only message in /etc/motd.

The “Authorized access only” message is displayed by /etc/issue on these hosts.

Negative: 7.7 /etc/securetty has a non tty1-12 line: tty10.

The /etc/securetty file allows you to specify where root is allowed to login; pseudo terminals, virtual consoles or system consoles. SAT recommends root only login at a system console. To limit root’s access to the system console remove all ttyp# and vc# lines from the /etc/securetty file. Users needing root access from a terminal session can “su” to root.

Additionally, the ssh configuration should have the “PermitRootLogin” parameter set to no, then root cannot login via ssh.

Negative: 7.8 lilo isn't password-protected.

Lilo is the Linux boot loader responsible for booting the Linux kernel. If physical security is compromised, an intruder could override the boot process, compromising the system. The lilo password is set by editing the /etc/lilo.conf file and adding the “password=<set password here>” statement. Once this file contains a password, it is important that it is not world readable. Set the permissions of the file using the command “chmod 600 /etc/lilo.conf”. Run the command “/sbin/lilo -v -v” for the changes to take affect[8].

SAT recommends that a lilo password be set to remove this capability from unauthorized users.

Negative: 8.1 uucp has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 operator has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 adm has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 bin has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 daemon has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 ftp has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 games has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 gopher has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 lp has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 mail has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 news has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 nobody has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.

All accounts in the password should have a valid shell, even if it is /dev/null. The accounts that are application accounts (e.g. gopher and news) should be deleted. Valid accounts should have a valid shell added to the /etc/passwd record.

Negative: 8.7 User mail 's homedir is group writable!

This warning was reported in error. No action is necessary.

Negative: 8.10 Default umask may not block group-writable. Check /etc/csh.login
Negative: 8.10 Default umask may not block world-writable. Check /etc/bashrc.
Negative: 8.10 Default umask may not block group-writable. Check /etc/bashrc.
Negative: 8.10 Default umask may not block world-writable. Check /etc/csh.cshrc.

The umask sets the default permissions that will be used when a file or directory gets created. The umask 022 is set in /etc/profile; which is run each time a user logs on the system. The umask may also be set in each of these files by adding the line “umask 022”.

Negative: 9.2 This machine isn't synced with ntp.

Ntp stands for Network time protocol. This service is used to keep the hosts time synchronized with another servers or time sources. Time synchronization is very important when troubleshooting problems on or between hosts or investigating compromises. The time on of these hosts was off by 30 (firewall-i) and 80 (firewall-x) minutes. Trying to compare the logs with such a large variance is extremely difficult.

Additional configuration problems found on firewall-i

Negative: 2.7 TCP Wrappers not configured for default-deny on this inetd-based system.
Negative: 3.19 inetd is still active.
Negative: 2.4 ftp not deactivated.

SAT recommends deactivating telnet and ftp. Since these are the only services running in out of inetd, when you are ready to shut them down proceed with the following steps:

Shutdown inetd -- /etc/rc.d/init.d/inetd stop
Disable it from startup – chkconfig –level 2345 inetd off
Identify the telnet package installed – rpm --query telnet
Identify the ftp package installed – rpm --query ftp
Remove the packages – rpm -e telnet-0.10-31
rpm -e ftp-0.15-1

Negative: 7.3 User gopher is not present in /etc/ftpusers

Negative: 7.3 User xfs is not present in /etc/ftpusers
Negative: 7.3 User postgres is not present in /etc/ftpusers

Ftp should be deactivated. However, these users should be added to the /etc/ftpusers file until that time.

Negative: 8.7 User lp 's homedir is group writable!
Negative: 8.7 User mail 's homedir is group writable!
Negative: 8.7 User news 's homedir is group writable!

Permissions on users home directories should be corrected. Use the command chmod g-w <home directory name> to remove group write from these directories.

Negative: 9.1 System isn't running sshd.

Ssh is a secure protocol for remote access. Ssh is installed on the server and should be used for remote access. Before starting ssh make sure you have the latest patches from Redhat at https://rhn.redhat.com/network/errata/search.pxt. enter "ssh" in the search window for a listing. Ssh should be configured to use protocol ssh2 only. The ssh2 daemon uses the file /etc/ssh2/sshd2_config. Key values to check in the sshd2_config file are:

AllowHosts/DenyHosts – make sure you're only letting those you want to
IgnoreRhosts – do you want to allow users to have .rhosts and .shosts files (not recommended) otherwise it uses /etc/hosts.equiv or /etc/shosts.equiv (which is set up by the administrator)
PermitRootLogin – set to no

2.3 Configuration vulnerabilities – Manual review

The manual review of the following configuration files detected these additional vulnerabilities:

/etc/inittab vulnerabilities – The /etc/inittab files is read using the command "cat /etc/inittab". Currently, someone with physical access to the server could reboot the server using the key sequence "Control + Alt + Del" and boot the server into single user mode and gain root access. The /etc/inittab file defines the boot behavior of the init process and allows system administrators to disable the "Control + Alt + Del" key sequence and require a password for single-user access.

File System mount vulnerabilities – To check how the file systems are mounted, use the "mount" command. The output will display the device, directory the file system is mounted on, file system type and the mount options that are currently set. For example "/dev/hda7 on /usr type ext2 (rw)" shows the /usr file system mounted with read and write options. Other options available are suid/nosuid and dev/nodev. Each file system should be checked to make sure

that it is not being mounted with options that it does not need. In this example, /usr is being mounted with the option write. Since /usr contains only programs it should be mounted read only, except when you are applying patches. This will also keep an attacker from putting files in the /usr directory.

File System scans – File system scans were performed to identify files which had suid/sguid permissions, to find regular files which were in the /dev directory, and to find device files outside of /dev. Suid/sguid permissions allow users to run a command as the owner(suid) or group(sguid) of the file. If that owner is root, the commands are run as root. To identify these programs run the following commands:

Get a list of suid/sguid root programs.
find / \(-perm -4000 -o -perm -2000 \) -user 0 ! -type d ! -type l -exec ls -ldb {} \;

Get a list of suid/sguid programs not owned by root.
find / \(-perm -4000 -o -perm -2000 \) ! -user 0 ! -type d ! -type l -exec ls -ldb {} \;

There are commands for which these permissions are necessary, for example /usr/bin/passwd which allows users to change their passwords. However, if users do not need to run a program these permissions should be removed. A list of the identified files is in Appendix D, programs which should be reviewed by the system administrator for their need to be run suid/sguid are in bold. To remove permissions, use the following commands:

To remove the suid permission:
chmod u-s /path/<suid file>

To remove the sguid permission:
chmod g-s /path/<sguid file>

The review of devices files outside of /dev and regular files inside of /dev, is meant to identify potential problems. For example, an attacker may try to hide their presence by placing files in /dev where you're not likely to run across them. It will also find administrator errors that just need to be cleaned up. There were no device files found outside of /dev and there were no regular files found inside the /dev directory. Use the following commands to scan for these types of files:

Get a list of regular files, sockets, links and named pipes which reside in the /dev directory.
find / \(-type f -o -type f -type p -o -type s \) -name /dev -prune -exec ls -ldb {} \;

Get a list of device files which reside outside of /dev directory.
find / \(-type b -o -type c \) -name /dev -prune -exec ls -ldb {} \;

The find commands in this section can easily be placed in a script to create a report that can be mailed to the system administrators on a regular basis.

2.4 Network Vulnerabilities

SAT chose nmap version 3.0, a "utility for network exploration or security auditing"[9] to scan the ports on each server. Nmap was run from a host on the Internet (1) in the chart and from firewall-x (2) on the chart. Because these servers are firewalls, we also ran the command "netstat -a" on each server to establish open ports that were not visible from the network. Table 1 below shows a summary of the ports found open on each server, the complete nmap and netstat output is listed in Appendix C. The ports discovered by nmap were expected based on the running services that were discovered in the configuration analysis. As discussed in section 2.2 telnet and should not be used for remote access and should be disabled. Three other services sunrpc (or portmapper), auth and login are not being used. Although they are being filtered by the firewall, unused services should not be running on the firewall-x server. They provide a risk that an attacker could use against you if the server is compromised. Additionally, unused services are probably not being monitored and if a change in the firewall configuration accidentally allowed access to these ports the problem may go unnoticed for long time adding to your vulnerabilities.

The firewall-i server is not running sendmail(smtp), or web(http) services. These ports are configured to forward the smtp and http services to a server on the internal LAN. Since these services are available on a DMZ server, they should be moved to the DMZ host. PCAnywhere requires multiple ports to work, this may be an error in the firewall configuration. If PCAnywhere access is required, SAT recommends that GIAC Enterprises consider setting up a Virtual Private Network (VPN). Bootps is only available on the private network and therefore was not detected by the nmap scan.

Port	Service	Server firewall-x	Server firewall-i
21/tcp	ftp		3
22/tcp	ssh		
23/tcp	telnet	1,2,3	1,2,3
25/tcp	smtp		1,2
53/tcp	domain	1,2,3	
67/udp	bootps		3
80/tcp	http		1,2
111/tcp	sunrpc	2,3	
111/udp	sunrpc	3	
113/tcp	auth	1,2,3	
513/tcp	login	2,3	
514/tcp	shell	2,3	
5631/tcp	pcanywheredata		2

Legend

1=nmap on Internet host
2=nmap on firewall-x
3= netstat

Table 1: nmap scan summary of open ports

2.5 Firewall Configuration

The firewall configuration is critical to keeping out the improper attempts to access your systems. These are packet filtering firewalls, lists of acceptance and rejection rules for incoming (input rule chain) and outgoing (output rule chain) packets. Packets are matched against each rule in the appropriate chain until a match is made, if no match is made the packet is rejected.

An error in the firewall configuration[1] can open an unintended access to your network. All changes to the firewall configuration should be well documented and tested. The current firewall configuration listing (/sbin/ipchains --list) contains several rules that should be reviewed to make sure the access is intended, see Appendix E for a full list of firewall rules for each server. (Universe is defined as any address on the Internet.)

Firewall-x
Rule 6: universe ftp to the External IP address of the firewall
Rule 8: universe www to the External IP address of the firewall
Rule 12: universe https to the External IP address
These rules allow access to the external (Internet side) of firewall-x. The ftp and www services are not running on these ports however, if these ports are opened on the server all of the Internet will be able to access them which may not be the intent.

Rule 9: universe www to the DMZ LAN
Rule 13: universe https to the DMZ LAN
Allowing access to the DMZ LAN, allows access to all of the hosts on the DMZ. This includes the DMZ side of the firewall, since the server is not running a web server and these ports are not open, the access should not be configured. The destination in these rules should be changed to the web server.

Rule 19: universe telnet to the External IP address
Rule 20: universe telnet to the DMZ LAN
Telnet should not be used to access the servers. These rules allow telnet access to both the Internet and DMZ ports on the firewall as well as every host on the DMZ.

Rule 38: universe on port 2048 to the DMZ LAN
Rule 39: universe on port 8890 to the DMZ LAN
Rule 40: universe on port 9000 to the DMZ LAN
These ports are not open on the firewall-x server. If the ports are required on another server on the DMZ LAN, the destination should be changed to the address of the specific host that can accept these connections.

Rule 42: universe on port 5632 to firewall-i
This port is not open on firewall-i, the rule should not be needed.

Rule 44 - 47: universe domain to universe
Domain queries should be sent only to the DNS server from the Internal LAN and DMZ servers.

Rule 48: universe smtp to DMZ LAN
Rule 51,53,54,56,: universe mail client protocols to DMZ
Client as server mail should be directed to the mail server specifically.

Firewall-i
Rule 1-6: ftp from the 192.168.1.0 LAN to the DMZ LAN
Rule 8,10: ftp from all Internal LAN's to the universe
Ftp is not a secure protocol and it has been recommended in section 2.2 that it be deactivated. Ftp can be allowed to the Internet without allowing it to the DMZ LAN by adding a reject rule to the DMZ LAN before the accept rule for the universe.

Rule 14: universe www to firewall-i
Rule 51: universe smtp to firewall-i
Rule 62,63: universe on port 5632 tcp/udp to firewall-i
These ports are not open on firewall-i, the rules should be removed.

Rule 21: universe telnet to firewall-i
Section 2.2 recommended deactivating telnet on the server. This rule should be removed to make sure that the port cannot be accessed.

Rule 41: universe on port 2048 to the Internal LAN
Rule 42: universe on port 8890 to the Internal LAN
Rule 43: universe on port 9000 to the Internal LAN
These rules potentially create a hole through the firewall to the Internal LAN. Since the firewall's purpose is to protect the Internal LAN these rules are very dangerous.

Rule 60,61: universe on port 5631 tcp/udp to firewall-i
Port 5631/tcp is open on firewall-i. This rule should be checked to make sure that universe access is appropriate for the service running here.

Rule 64: universe on port 22/udt to firewall-i
This may be a configuration error for port 22/tcp, which is ssh.

When configuring rules on the firewall, it is important to note that allowing (or rejecting) a packet to the DMZ LAN means that the rule applies to the DMZ LAN interfaces of both firewalls, not just the hosts on the DMZ LAN. The DMZ LAN is also part of the "universe". SAT recommends that services that are not used on

a server do not have rules that would allow the packets to be accepted. If a new service is turned on, then a rule should be added to the firewall to allow the specific access that is needed.

2.6 Logging and Monitoring

Each of these systems has syslog enabled and running, the command "ps -ef | grep log" displays the syslogd and klogd (kernel logging) processes. A review of the /etc/syslog.conf file shows the servers are logging info, authpriv, mail, cron, boot and emerg messages to various files. Ipchains, the firewall application manages logging in the /etc/rc.d/firewall.rc configuration, logging of a rule must be specifically configured. Ipchains is logging all rejected packets and some accepted packets to the /var/log/messages file. However, no one is monitoring the logs on a regular basis and logs are rotated and removed on a monthly basis. There are no automated report or alert mechanisms.

Without monitoring, system compromises can go unnoticed for an extended period of time. These servers could be used in attacks against other servers, which could cause GIAC Enterprises to be blocked from Internet sites. An automated log watcher like swatch[10] will assist the system administrator with task of monitoring logs by filtering out interesting items. Basically log entries that do not match a set of defined rules.

It is also essential to monitor the systems to make sure critical files have not been changed. A tool like tripwire[11] will allow you to configure a database of files to monitor along with their attributes. It can be configured to send the system administrator a report when changes to the specified files have been detected.

2.7 Risks from installed third-party software

There is an extensive list of packages installed on each of these hosts (see Appendix A), firewall-x has 99 packages and firewall-i has 330. While there are a few packages that the systems need firewall systems should be as stripped down as possible. Each non-essential package creates a potential weak point for compromising the system or something that could be used by an attacker if they do compromise the system. The more packages that need to be installed, the greater the need for maintenance and monitoring to make sure that everything is running securely.

2.8 Password and Account Security

User account information is stored in the /etc/passwd file, shadow passwords are used. The /etc/shadow file, viewable only as root, holds the user login name and encrypted password. This file can also hold password aging information. Password aging allows the administrator to set up the minimum and maximum time between password changes, minimum password length and the number of

days to start warning users that their password will need changing. SAT recommends adding password aging to ensure that users are changing their passwords on a regular basis.

Only administrators should need access to these servers, in this case that means 2 or 3 users per system. Unnecessary application accounts, inactive accounts, and accounts for non-administrators should be removed. Each administrator should have their own account and use su or sudo to run commands as root. Su allows administrators to become root by issuing the command "/bin/su -" and providing the root password at the password prompt. An alternative to su is sudo. Sudo[12] (superuser do) is a program to allow the system administrator to give a user or group of users permission to run commands as root. The software configuration is very flexible so that users can be given as many or as few commands as they need and it's easy to use. The advantages of sudo are, you won't need to give users the root password and the commands run with sudo will be logged.

2.9 Server Processes

Server processes can be viewed with the command "ps -ef". The firewalls should run a minimal set of daemons. SAT found several processes Advanced power management daemon (apmd), TCP/IP IDENT protocol server (identd), and DARPA port to RPC program number mapper (portmap) running on firewall-x. The apmd daemon is also running on firewall-i. Running processes that you aren't using means you probably aren't monitoring what those processes are doing. Therefore you won't know if they are doing something bad. The best practice is if you don't need it, don't run it.

2.10 Identification and Protection of Sensitive Data

The critical data on firewall-x and firewall-i lies in their firewall configurations. The files themselves are not readable by a normal user. The password files are also sensitive. GIAC is using shadow passwords to protect the password data. Additionally the primary DNS files for giacenterprises.com hold important information for access to the DMZ servers from both internal and external networks.

Data transmitted through the network is more sensitive. Most customers use credit cards to make purchases from GIAC Enterprises. The firewall's purpose is to keep unwanted traffic out of the DMZ, however, the protection of this data must rely on the protocols used on the web-mail host which is servicing the requests. The web-mail host security is out of the scope of this audit.

2.11 Physical Security

GIAC Enterprises houses the firewall hosts and network equipment in a specialized computer room. The room provides a raised floor, climate control, and UPS protection. There is only one access door to this room, which is inside an office that has security alarms. During off-business hours, an alarm code is required to enter and leave the office; during business hours the doors are usually unsecured. The entrance to the computer room is controlled by a combination lock. The combination has been given to only a few people however it is not changed regularly.

Servers can be compromised without the root password if an attacker can get physical access. Access to this area during business hours should be monitored to make sure that no unauthorized personnel are entering the area.

2.12 Policies

GIAC Enterprises is a small but growing company, formal written policies have not been part of the administrative practices. Unfortunately this leads to confusion among the staff as to how specific problems are handled. SAT recommends that written policies be developed for backups, disaster recovery, and security practices. Without these formal policies it will be difficult to measure the effectiveness of or make realistic decisions regarding security at GIAC Enterprises.

2.13 Backups

Backups are not currently being run on either firewall server. Additionally, there is currently no tape device to use for backups. There is an emergency boot disk and CD's available in case the server needed to be rebuilt. While the O/S could certainly be rebuilt, without copies the current configuration files it could be a lengthy process. SAT recommends purchasing tape devices and establishing a regular backup rotation with off-site storage and restore testing.

Section 3 – Critical Issues and Recommendations

3.1 Develop a written Security Policy - In order to determine how the servers should be configured, what services should be installed, and who should have access to the servers; a security policy needs to be drafted outlining the policies GIAC Enterprises intends to enforce. The security policy should address issues like user access, change control, intruder detection, acceptable use of the network and servers, and monitoring. Guides for developing policies are available from the SANS Institute[13].

3.2 Install a backup device – Before installing or upgrading the server, installing a backup device and creating a backup will reduce the risk of extended downtime while trying to remember and recreate a forgotten configuration file. At least two full backups should be completed and tested (restore a few files to a temporary directory) before proceeding with new software installs or reconfiguring the servers.

3.3 Install the latest version of the Operating System[14] – Since the Red Hat Linux 6.1 operating system is no longer being supported with errata, SAT recommends that both servers be installed with the latest version of Redhat Linux, currently 9.0. Maintaining the servers at the same operating system level will make management of the servers easier. This will also provide a solid basis for the rest of the configuration changes.

The new operating system should be a custom installation with only the minimum required packages installed. If possible this should be a new installation, with the disks wiped clean rather than an upgrade. This will remove problems related to the current systems. For example: If there were any undetected compromises on the server, an upgrade would not eliminate any files that had been placed on server by an intruder.

Before starting the install process, download the latest security patches at https://rhn.redhat.com/errata/rh9-errata-security.html to a separate server or PC.

Information you'll need on hand to complete this process:
IP Address
Subnet mask
Gateway IP address
DNS server IP addresses
/etc/password file
/etc/shadow file
/etc/rc.d/rc.firewall file
blank diskette (to create a boot disk)
Full backup
For firewall-i you'll also want to have a copy of the /etc/dhcp.conf file.

There are many options that may be configured in a Red Hat Linux installation, the instructions below are meant to install a minimal system and are not inclusive of all of the options available. Additional packages may be installed as needed after the initial installation.

When you are ready to start the install process, make sure the server is disconnected from the network until the operating system upgrade is complete and security patches have been installed. To start the install, Insert the CD-ROM into the drive and reboot the server. Follow the prompts to select the appropriate language, keyboard and mouse configuration after making your selections in each screen, click "Next" to continue.

At the "Upgrade Examine" screen select "Perform a new Red Hat Linux Installation". Next you'll be prompted for "Installation type", select "Custom". You'll then be prompted for the Disk Partitioning Setup, select "Automatically partition". To get a clean system you'll need to wipe out any data that you currently have, select "Remove all Linux partitions on this system". The Partitioning screen will display the automatic settings, click "Next" to accept these settings and continue.

The "Boot Load Configuration" window will display, the Default box should be checked next the Red Hat Linux label. Click Next to go to the "Advanced Boot Loader Configuration" window. The "/dev/hda Master Boot Record" radio button should be selected in this window, then click "Next" to continue.

At the "Network Configuration" window, you'll need to configure each device with your IP information. To configure a device, select the device and click on "Edit". Deselect the DHCP option and manually enter the IP information in this window, click on OK when you're finished. When you've completed all of the network devices, click on "Next". The "Firewall Configuration" window will display select the "No firewall" option and click on "Next".

At the "Additional Language Support" window, make sure your language is selected and click "Next". Then select your time zone in the "Time Zone Selection" window.

The next window will prompt you to set the root password, enter one you'll remember and click "Next" for the "Authentication Configuration" window. Enable MD5 passwords and shadow passwords and click "Next".

Now it's time to configure the packages. In the "Package Group Selection" window select "Minimal" in the Miscellaneous section, then click on Select Individual packages and click on "Next". The Individual packages will display in Tree view, select "System" packages and then select "ipchains". Click "Next" to continue. If there dependencies listed in the "Check for Dependencies" window, select "Install packages to satisfy dependencies".

Next you'll get the "Preparing to Install" window, click "Next" to start the installation process. Once the installation is complete you'll get a "Boot Diskette Creation" window. Select "Yes, I would like to create a boot diskette", insert your floppy in the drive and click on "Next".

The next window is a "Graphic Interface (X) Configuration window" you didn't install the "X Window System" packages, select on "Skip X configuration" and click on "Next". Your Red Hat installation is now complete.

Since this was a new installation you'll need to restore/recreate your /etc/passwd and /etc/shadow files and the /etc/rc.d/rc.firewall file. Make sure to install the latest security patches before reconnecting the server to the Internet.

3.4 Install the latest patches – Once the operating system is up-to-date it is critical to keep it current to mitigate known threats. Before attaching the server to the network, install the patches you downloaded from https://rhn.redhat.com/errata/rh9-errata-security.html.

1. Create a directory /tmp/updates and copy the patches to the new directory. If you downloaded the patches to another server or PC use a cross-over cable to "network" the two machines together to copy the files safely.
2. Get the Red Hat GPG key[8] so that you can verify the GPG signature of RPM's before installing them.
   Mount the Red Hat Linux distribution CD-Rom and type the command: rpm --import /<cdrom path>/PRM-GPG-KEY
3. Display the list of keys installed with the command: rpm -qa gpg-pubkey* The output should include: gpg-pubkey-db42a60e-37ea5438
4. Verify the signature of the RPM files before installing them. rpm -K /tmp/updates/*.rpm
   For each packages the GPG key verifies successfully you'll see "gpg OK" Remove any files that do not verify
5. For the files which verify ok, install the patches with the following command: rpm -Uvh /tmp/updates/*.rpm

If the security errata included any kernel patches, you'll need to reboot the server for the patches to take effect. Once the patches have been installed the server can be connected to the network.

Applications should be updated as well using steps 4 and 5; patches can be downloaded from https://rhn.rehat.com/errata. Redhat provides quarterly errata updates for bug fixes, and enhancements. Redhat Network[5] provides a signup for notification of errata releases, this is a convenient way for system administrators to keep up-to-date. Once you've installed the new operating system, get your product registered and get on the mailing list for updates.

3.5 Deactivate/remove unnecessary services – Shutdown apmd, gpm and portmapper, xinetd (or inetd) services, and identd. The start/stop scripts are located in /etc/init.d. The syntax is: /etc/init.d/<daemon name> stop

Then run chkconfig for each service to disable the service from being started at bootup. The syntax for chkconfig is: chkconfig --level 2345 <service> off

The packages should also be removed. The syntax for package removal is: rpm -e <package name>

3.6 Log monitoring – Log monitoring is key to knowing what is going on in regard to these systems. Logs can be overwhelming. SAT recommends GIAC Enterprises create a central logging server and install a log monitor like swatch, which will report interesting entries in the log files based on a set of rules. The rules can be customized using regular expressions to filter out log entries you don't want to see.

The logs will still be available on each server for the administrators to view as needed. To send syslog messages to the logging server add the line "*.info;mail.err @<loghostname>" to /etc/syslog.conf file. This will send syslog mail messages at the "err" (and higher) level and other messages and the "info" and higher levels to the central logging server.

Logs can be monitored at regular increments by adding a cron script to email output directly to the system administrator.

3.7 Install/configure tripwire[15] – Tripwire is available at http://www.redhat.com/apps/download/advanced_search.html, make sure to select your architecture, and click on "All Releases" enter "tripwire" in the "By Keyword" window and click on Search. A list of available versions will display. Click on details next to the version and make sure that you meet all the dependencies, click on download and follow the prompts to download the software.

Install tripwire with the command, "rpm -Uvh /<directory path>/tripwire*.rpm". Tripwire comes with a sample configuration file in /etc/tripwire/twcfg.txt, check this file to make sure everything is correct you probably won't need to make any changes.

The tripwire policy file /etc/tripwire/twpol.txt should be edited to add files specific to your system that need to be watched. The file is well commented so you'll find it easy to add or remove files. Make sure that all of your suid/sguid files are listed, the command to find them is in section 2.3. Add in your /etc/rc.d/rc.firewall file in the Configuration file section. For email notification, add the emailto=<email address> in each rule directive section. When you have

completed your modifications, run the /etc/tripwire/twinstall.sh script and follow the prompts for entering passwords.

Next you'll need to initialize the tripwire database, this builds the database that serves as a baseline for the later integrity checks. To initialize the database run the command "/usr/sbin/tripwire --init".

Finally, run an integrity check to make sure you're getting the results you want with the command "/usr/sbin/tripwire --check". The report will be stored in the /var/lib/tripwire/report directory. To view the report, use the command "/usr/sbin/twprint –m r --twrfile /var/lib/tripwire/report/<filename>.twr".

Tripwire creates a daily cron job during the installation process. When tripwire finds violations, you'll need to decide whether or not those are actual security problems or normal file modifications (e.g. from installing updated software). If it is a security problem you'll need to handle the breach based on the requirements documented in the security policies.

3.8 Manage root logins on the server –To prevent root from logging through the network, remove all lines except tty#'s in the /etc/securetty file. This will allow root to only login at the console.

To prevent root from logging on through ssh, modify the sshd_config file set the parameter "PermitRootLogin" to no.

The root password should be closely controlled so that only those who need root access have it, the fewer the better. If it is necessary to have the password written down, make sure it is put in a sealed envelope and stamped across the seal. The envelope should be placed in a lock box with restricted access.

Root's password should be changed on a regular basis (monthly or quarterly) and whenever an employee with access leaves the company. Make sure the password is difficult to guess. Avoid using passwords that are dictionary words or names, or dictionary names prefixed or suffixed by a number or punctuation character. Also avoid words with simple alphabetic to numeric or punctuation substitutions (such as the dollar sign ($) for "s", or one for the letter "l", as in "$pecia1")

Some good ways to create passwords are using parts of a phrase, selecting the first letter of each word in a phrase or combining words adding numbers and punctuation is also good. For example: "bktafas" or "bk2afas" from the phrase "be kind to a friend and smile".

3.9 Secure the named service – Firewall-x is providing primary domain name services for two domains. SAT recommends the DNS server be moved to an application server on the DMZ.

Moving the DNS server to another server will require setting up the named application on the new server, configuring the domains and creating the zone files for each domain. The current named configuration is specified in the /etc/named.conf file; the named zone files located in /var/named.

Once the configuration is in place on the new server, you'll need to change the name server configuration in DHCP to point to the new DNS server, and notify the domain registry and secondary DNS providers of the change. You'll also need to manually configure dns for any machines that have hard coded IP addresses and do not use DHCP.

The changes will take a few hours to propagate throughout the Internet. Then you can shut down the DNS service on firewall-x. First shutdown the service with the command "/etc/rc.d/init.d/named stop". Then remove the service from startup "chkconfig --level 2345 named off". Next, find the name of the installed rpm with the command "rpm -q bind" (Bind is the package for the DNS server). Remove the package with the command "rpm –e <package name>". You may need to manually remove the /etc/named.conf file and /var/named/* files.

3.10 Verify the firewall rules – Review the need for each rule identified in section 2.5 by port, source and destination. To deactivate a rule in the firewall, comment out the rule using a pound (#) sign. When you change or remove a rule, you must stop and start the firewall for the new configuration to take effect. Use the following commands to restart the firewall: "/etc/rc.d/init.d/firewall stop" and "/etc/rc.d/init.d/firewall start".

Carefully test the firewall configuration to make sure the results are what you intended. For example: If you remove the telnet rule #21 on firewall-i, try to telnet from the Internal LAN, the DMZ LAN and the Internet to make sure you can't get a connection to the firewall-i server. Once the configuration is tested you may want to go back and remove the commented out firewall rules. This way you won't accidentally reactivate them.

3.11 Other Recommendations:

- Being able to establish time frames will be key to gathering information if an attacker does compromise these systems. NTP (Network Time Protocol) is available at http://www.redhat.com/apps/download/advanced_search.html, make sure to select your architecture, and click on "All Releases" enter "ntp" in the "By Keyword" window and click on Search. A list of available versions will display. Click on details next to the version and make sure that you meet all the dependencies, click on download and follow the prompts to download the software.

Ntp can be run as a daemon (ntpd) and will synchronize with specified time servers or it can be run via cron (ntpdate) to retrieve the time from a specified time server.

A list of Public time servers for synchronization is available at URL: http://www.eecis.udel.edu/~mills/ntp/servers.html

- Develop and document backup and disaster recovery plans – Backup and Disaster recovery plans minimize downtime when a problem occurs. The plans should include contingencies for a system compromise or a natural disaster disabling the systems.

  Remember to test your procedures, and your backups.

- Use mount options to restrict write, suid and dev files in files systems where these options are not necessary. The following entries can be modified in the /etc/fstab file:

Current:	/dev/hda5	/home	ext2	defaults	1 2
New:	/dev/hda5	/home	ext2	ro,nosuid,nodev	1 2
Current:	LABEL=/usr	/usr	ext2	defaults	1 2
New:	LABEL=/usr	/usr	ext2	ro,nodev	1 2
Current:	LABEL=/usr/local	/usr/local	ext2	defaults	1 2
New:	LABEL=/usr/local	/usr/local	ext2	ro,nosuid,nodev	1 2
Current:	LABEL=/var	/var	ext2	defaults	1 2
New:	LABEL=/var	/var	ext2	nosuid,nodev	1 2
Current:	/dev/fd0	/mnt/floppy	auto	noauto,owner	0 0
New:	/dev/fd0	/mnt/floppy	auto	noauto,owner,nosuid	0 0

- Configure a lilo password[8] – Set a password on the lilo Linux boot loader by adding the following line to the /etc/lilo.conf file after the image statement:

  password=Somthin-Hard2ge

  Check the permissions of the file and make sure that it is not readable by anyone other than root. If necessary run the command "chmod 600 /etc/lilo.conf" to set the correct permissions. Then run the command "/sbin/lilo -v –v" for the changes to take affect.

- SAT recommends deleting the floppy and cdrom lines from the /etc/security/console.perms file.

  /etc/security/console.perms – lines to delete
  <console> 0660 <floppy> 0660 root.floppy
  <console> 0600 <cdrom> 0600 root.disk

- Modify the /etc/inittab to add to password protection for booting into single user mode and disable the “Control + Alt + Del” key sequence.

  The entry for adding a password to single user mode is:
  sum:S:wait:/sbin/sulogin

  Disable the “Control + Alt + Del” key sequence by removing the line:
  ca::ctrlaltdel:/sbin/shutdown -t3 -r

  To make these changes take effect, run the command “init q”.

- Account cleanup – Application accounts that are not used should be removed. SAT has identified application accounts below that are not needed. GIAC Enterprises should review the remaining list of users for employees who are no longer with the company or, have changed job functions and no longer need the account.

  The following accounts should be removed from **firewall-x**: lp, mail, news, uucp, operator, games, gopher, ftp, named, rpcuser, rpc, mailnull, and ncsd

  The following accounts should be removed from **firewall-i**: lp, mail, news, uucp, operator, games, gopher, ftp, xfs, and postgres

- Set up password aging. Password aging defaults are setup in the /etc/login.defs file.

  PASS_MAX_DAYS – Sets the maximum number of days a password may be used. If a user does not change their password before this day, they will be forced to change it at the next login.
  PASS_MIN_DAYS – Sets the minimum number of days allowed between password changes. Setting this number encourages users to get used to their new password and not just change it back to the previous one immediately.
  PASS_MIN_LEN – Specifies the minimum acceptable password length.
  PASS_WARN_AGE – Users will get a warning this number of before their password expires. This gives users a chance to change the password at their convenience before they are forced to change the password.

- SAT recommends changing the combination lock quarterly or when ever an employee with access leaves. Additionally SAT recommends that GIAC Enterprises consider installing an electronic lock system and cameras that will allow for better controls as the company grows.

References

1. Ziegler, Robert L. Linux Firewalls. New Riders Publishing, 2000. 127 - 229.
2. CIS Level-1 Benchmark and Scoring Tool for Linux. URL: http://www.cisecurity.org/ (22 February 2003).
3. Errata: Security Alerts, Bugfixes, and Enhancements. URL: http://www.redhat.com/apps/support/errata (2 April 2003).
4. Red Hat Linux 7.1 Security Advisories. URL: http://rhn.redhat.com/errata/rh71-errata-security.html (2 April 2003).
5. Red Hat Network. URL: http://rhn.redhat.com (3 May 2004).
6. Hunt, Craig. TCP/IP Network Administration, First Edition. O'Reilly and Associates, Inc., September 1993.
7. Red Hat. Official Red Hat Linux Administrator's Guide. Wiley Publishing, Inc., 2003. 116-117, 392-398.
8. Red Hat Linux 9: Red Hat Linux Security Guide. URL: http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/pdf/rhl-sg-en-9.pdf (7 May 2003). 17 – 24.
9. INSECURE.ORG. URL: http://www.insecure.org/ (11 February 2003).
10. SourceForge.net Project: Swatch: Summary. URL: http://sourceforge.net/projects/swatch/ (3 April 2003).
11. Tripwire Open Source, Linux Edition FAQ. URL: http://www.tripwire.org/qanda/faq.php (3 April 2003).
12. Sudo Main Page, 3 May 2003. URL: http://www.courtesan.com/sudo
13. Sans Institute – Security Policy Project. URL: http://www.sans.org/resources/policies/ (3 April 2003).
14. Red Hat. Red Hat Linux Installation Guide. Red Hat, Inc., 2003.
15. Red Hat Linux 9: Red Hat Linux Reference Guide, Chapter 19. URL: http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/ch-tripwire.html (7 May 2003).

Appendix A – Installed RPM's

firewall-x host

filesystem-2.0.7-1
glibc-2.1.92-14
mktemp-1.5-5
libtermcap-2.0.8-25
anacron-2.3-9
ncurses-5.1-2
fileutils-4.0x-3
ash-0.2-26
authconfig-4.0.16-4
bdflush-1.5-14
words-2-16
pwdb-0.61.1-1
gawk-3.0.6-1
e2fsprogs-1.18-15
popt-1.6-4
sysklogd-1.3.33-6
which-2.11-4
modutils-2.3.14-3
initscripts-5.49-1
glib-1.2.8-4
sh-utils-2.0-11
db2-2.4.14-4
perl-5.6.0-9
bind-utils-8.2.2_P5-25
caching-nameserver-7.0-6
cpio-2.4.2-20
cyrus-sasl-1.5.24-6
dev-3.0.6-5
diffutils-2.7-21
eject-2.0.2-6
findutils-4.1.5-4
finger-server-0.17-4
gmp-3.0.1-5
gpm-1.19.3-4
gzip-1.3-6
indexhtml-7.0-2
iptables-1.1.1-2
isapnptools-1.22-2
kernel-2.2.16-22
kernel-utils-2.2.16-22
kudzu-0.72-3
libstdc++-2.96-54
linuxconf-1.19r2-4
mailcap-2.0.9-2
MAKEDEV-3.0.6-5
mkbootdisk-1.2.8-2
mount-2.10m-5
ncftp-3.0.1-7
net-tools-1.56-2
nfs-utils-0.1.9.1-7
openldap-1.2.11-15
openssh-2.1.1p4-1
openssh-server-2.1.1p4-1
pciutils-2.1.8-8
portmap-4.0-29
pump-0.8.3-2
python-xmlrpc-1.0-8
raidtools-0.90-13
readline-4.1-5
redhat-release-7.0-1
rmt-0.4b19-4
rpm-4.0-4
rsh-0.17-2.2
rusers-0.17-6
rwall-server-0.17-5
sash-3.4-8
setserial-2.17-2
slang-1.4.1-5
stat-2.2-1
sysstat-3.2.4-3
yp-tools-2.4-4
ypserv-1.3.11-9
lsof-4.60-2
setup-2.3.4-1
basesystem-7.0-2
chkconfig-1.2.16-1
termcap-11.0.1-3
bash-2.04-11
apmd-3.0final-18
info-4.0-15
grep-2.4.2-4
at-3.1.8-12
bc-1.05a-13
cracklib-2.7-8
cracklib-dicts-2.7-8
mingetty-0.9.4-13
sed-3.02-8
procps-2.0.7-3
logrotate-3.5.2-1
psmisc-19-4
vixie-cron-3.0.1-56
shadow-utils-19990827-18
db3-3.1.14-6
pam-0.72-26
textutils-2.0e-8
gdbm-1.8.0-5
bind-8.2.2_P5-25
bzip2-1.0.1-3
console-tools-19990829-25
crontabs-1.8-1
db1-1.85-4
dhcpcd-1.3.18pl8-6
ed-0.2-17
file-3.30-7

firewall-i host

ElectricFence-2.1-1
setup-2.0.5-1
filesystem-1.3.5-1
basesystem-6.0-4
ldconfig-1.9.5-15
glibc-2.1.2-11
indexhtml-6.1-1
inews-2.2.1-1
pwdb-0.60-1
pam-0.68-7
sh-utils-2.0-1
inn-2.2.1-1
rhl-rg-6.1en-1
rhs-printfilters-1.57-3
rootfiles-5.2-5
routed-0.10-16
rpm-3.0.3-2
rpm-devel-3.0.3-2

shadow-utils-19990827-2
mktemp-1.5-1
termcap-9.12.6-15
libtermcap-2.0.8-18
bash-1.14.7-16
MAKEDEV-2.5-2
SysVinit-2.77-2

mingetty-0.9.4-10
ncurses-4.2-25
info-3.12h-2
gawk-3.0.4-1
sed-3.02-4
e2fsprogs-1.15-3
chkconfig-1.0.7-2
fileutils-4.0-8
console-tools-19990302-17
procps-2.0.4-2
vixie-cron-3.0.1-39
modutils-2.1.121-14
logrotate-3.3-1
sysklogd-1.3.31-12
psmisc-18-3
grep-2.3-2
tcsh-6.08.00-6
initscripts-4.48-1
XFree86-libs-3.3.5-3
XFree86-xfs-3.3.5-3
chkfontpath-1.5-1
XFree86-75dpi-fonts-3.3.5-3
anonftp-2.8-1
mailcap-2.0.3-1

textutils-2.0-2
apache-1.3.9-4
apmd-3.0beta9-3
arpwatch-2.1a4-16
ash-0.2-18
at-3.1.7-11
authconfig-2.0-2
autoconf-2.13-5
automake-1.4-5
bc-1.05a-4
bdflush-1.5-10

ipchains-1.3.9-3
ipxutils-2.2.0.16.a-1
isapnptools-1.18c-1
ispell-3.1.20-22
kbdconfig-1.9.2.1-1
kernel-2.2.12-20
kernel-pcmcia-cs-2.2.12-20

knfsd-1.4.7-7
knfsd-clients-1.4.7-7
kudzu-0.20-1
kudzu-devel-0.20-1
ld.so-1.9.5-11
less-340-1
libc-5.3.12-31
libgr-2.0.13-20
libgr-devel-2.0.13-20

libjpeg-6b-9
libjpeg-devel-6b-9
libpng-1.0.3-4
libpng-devel-1.0.3-4
gdbm-1.8.0-2
gdbm-devel-1.8.0-2
libstdc++-2.9.0-24
libtermcap-devel-2.0.8-18
libtiff-3.4-6
libtiff-devel-3.4-6
libungif-devel-4.1.0-2
lilo-0.21-10
redhat-release-6.1-1

linuxconf-1.16r3.2-2
linuxconf-devel-1.16r3.2-2

losetup-2.9u-4
lpr-0.41-2
lrzsz-0.12.20-2
lsof-4.45-1
lynx-2.8.2-2
m4-1.4-12
mailx-8.1.1-9
make-3.77-6
man-1.5g-6
man-pages-1.26-5
mars-nwe-0.99pl17-4

rsh-0.10-28
rsync-2.3.1-2
rusers-0.15-6
rwho-0.15-2
samba-2.0.5a-12
samba-client-2.0.5a-12
samba-common-2.0.5a-12

sash-3.3-1
screen-3.9.4-2
sendmail-8.9.3-15
setconsole-1.0-8
setserial-2.15-2
setuptool-1.2-3
shapecfg-2.2.12-2
sharutils-4.2-14
slang-1.2.2-4

slang-devel-1.2.2-4
slocate-2.0-3
slrn-0.9.5.7-2
stat-1.5-11
statserial-1.1-13
strace-3.99.1-2
svgalib-1.4.0-2
svgalib-devel-1.4.0-2
talk-0.11-3
tar-1.13.11-1
tcp_wrappers-7.6-9
tcpdump-3.4-16
telnet-0.10-31

texinfo-3.12h-2
tftp-0.15-1

time-1.7-9
timeconfig-3.0-5
timed-0.10-23
tin-1.4_990517-1
tmpwatch-2.0-1
traceroute-1.4a5-16
trn-3.6-18
ucd-snmp-4.0.1-4
ucd-snmp-utils-4.0.1-4
urlview-0.7-4
urw-fonts-1.1-8

bind-utils-8.2.2_P3-1
bootparamd-0.10-24
binutils-2.9.1.0.23-6
bison-1.28-1
byacc-1.9-11
bzip2-0.9.5c-1
caching-nameserver-6.0-2
cdecl-2.5-9
cleanfeed-0.95.7b-4
rmt-0.4b4-11
cpio-2.4.2-13
cpp-1.1.2-24
cproto-4.6-2
cracklib-2.7-5
cracklib-dicts-2.7-5
crontabs-1.7-7
ctags-3.2-1
cvs-1.10.6-2
dev-2.7.10-2
dev86-0.14.9-1
diffutils-2.7-16
dip-3.3.7o-15
dump-0.4b4-11
ed-0.2-12
egcs-1.1.2-24
egcs-c++-1.1.2-24
eject-2.0.2-3
elm-2.5.1-1
emacs-20.4-4
emacs-nox-20.4-4
etcskel-2.0-1
faces-devel-1.6.1-17
fetchmail-5.1.0-1
file-3.27-3
findutils-4.1-32
finger-0.10-25
flex-2.5.4a-7
freetype-1.2-7
ftp-0.15-1
fwhois-1.00-11
gd-1.3-5
gd-devel-1.3-5
gdb-4.18-4
bc-1.05a-4
gdbm-1.8.0-2
gdbm-devel-1.8.0-2
metamail-2.7-22
minicom-1.82.1-1
mkbootdisk-1.2.2-1
mkinitrd-2.3-1
mod_perl-1.21-2
mount-2.9u-4
mouseconfig-4.1-1
mpage-2.4-7
mt-st-0.5b-4
mutt-1.0pre3i-1
ncftp-3.0beta19-2
ncompress-4.2.4-14
ncpfs-2.2.0.16.a-1
ncurses-devel-4.2-25
net-tools-1.53-1
netkit-base-0.10-37
newt-0.50-13
newt-devel-0.50-13
ntsysv-1.0.7-2
passwd-0.63-1
patch-2.5-9
pciutils-2.0-2
pciutils-devel-2.0-2
perl-5.00503-6
php-3.0.12-6
pidentd-3.0.7-5
piranha-0.2.1-1
pmake-2.1.33-5
popt-1.4-1
portmap-4.0-17
postgresql-6.5.2-1
postgresql-devel-6.5.2-1
postgresql-server-6.5.2-1
ppp-2.3.10-1
procinfo-17-1
procmail-3.13.1-4
pump-0.7.2-2
python-1.5.2-7
quota-1.66-8
raidtools-0.90-5
piranha-0.2.1-1
pmake-2.1.33-5
popt-1.4-1
portmap-4.0-17
postgresql-6.5.2-1
postgresql-devel-6.5.2-1
utempter-0.5.1-2
util-linux-2.9w-24
uucp-1.06.1-20
vim-common-5.4-2
vim-minimal-5.4-2
which-2.8-1
words-2-12
wu-ftpd-2.5.0-9
wvdial-1.40-5
yp-tools-2.3-2
ypbind-3.3-24
zlib-1.1.3-5
zlib-devel-1.1.3-5
bind-8.2.2_P3-1
openssh-2.1.0p2-1
gated-3.5.10-10
bash2-2.03-6
bash2-doc-2.03-6
dhcpcd-1.3.17pl5-2
dhcp-2.0-3
openssl-0.9.5a-1
openssh-server-2.1.0p2-1
openssh-clients-2.1.0p2-1
ipmasqadm-0.4.2-4
piranha-0.2.1-1
pmake-2.1.33-5
popt-1.4-1
portmap-4.0-17
postgresql-6.5.2-1
postgresql-devel-6.5.2-1
postgresql-server-6.5.2-1
ppp-2.3.10-1
procinfo-17-1
procmail-3.13.1-4
pump-0.7.2-2
python-1.5.2-7
quota-1.66-8
raidtools-0.90-5
rcs-5.7-10
rdate-0.960923-8
rdist-6.1.5-11
readline-2.2.1-5
readline-devel-2.2.1-5
redhat-logos-1.1.0-1
rhl-gsg-6.1en-2
rhl-ig-6.1en-1

gettext-0.10.35-13
getty_ps-2.0.7j-7
ghostscript-5.10-10
ghostscript-fonts-5.10-3
git-4.3.17-5
glib-1.2.5-1
kernel-headers-2.2.12-20
glibc-devel-2.1.2-11
gmp-2.0.2-10
gnupg-1.0.0-1
gpm-1.17.9-3
gpm-devel-1.17.9-3
gdbm-1.8.0-2
groff-1.11a-9
gzip-1.2.4-14
hdparm-3.5-1
indent-2.2.0-1
postgresql-server-6.5.2-1
ppp-2.3.10-1
procinfo-17-1
procmail-3.13.1-4
pump-0.7.2-2
python-1.5.2-7
quota-1.66-8
raidtools-0.90-5
piranha-0.2.1-1
rcs-5.7-10
rdate-0.960923-8
rdist-6.1.5-11
readline-2.2.1-5
readline-devel-2.2.1-5
redhat-logos-1.1.0-1
rhl-gsg-6.1en-2
rhl-ig-6.1en-1
rhl-rg-6.1en-1
rhs-printfilters-1.57-3
rootfiles-5.2-5
routed-0.10-16
rpm-3.0.3-2
rpm-devel-3.0.3-2
rsh-0.10-28
rsync-2.3.1-2
rusers-0.15-6
rwho-0.15-2
samba-2.0.5a-12
samba-client-2.0.5a-12
samba-common-2.0.5a-12
sash-3.3-1
screen-3.9.4-2

Appendix B – CISscan Output

CISscan for firewall-x server

*** CIS Ruler Run ***
Starting at time 20030222-13:44:33

Positive: 1.1 System appears to have been patched within the last month.
Negative: 2.2 No Authorized Only banner for telnet in file /etc/xinetd.d/telnet.
Negative: 2.2 No Authorized Only banner for login in file /etc/xinetd.d/rlogin.
Negative: 2.3 telnet not deactivated.
Positive: 2.4 ftp is deactivated.
Negative: 2.5 rsh (shell) should be deactivated.
Negative: 2.5 rlogin (rlogin) should be deactivated.
Positive: 2.6 tftp is deactivated.
Negative: 2.7 xinetd either requires global 'only-from' statement or one for each service.
Negative: 3.1 apmd not deactivated.
Negative: 3.1 gpm not deactivated.
Positive: 3.2 NFS Server script nfs is deactivated.
Positive: 3.3 This machine isn't being used as an NFS client.
Positive: 3.4 NIS Client processes are deactivated.
Positive: 3.5 NIS Server processes are deactivated.
Negative: 3.6 portmapper not deactivated.
Positive: 3.7 samba windows filesharing daemons are deactivated.
Positive: 3.8 netfs rc script is deactivated.
Positive: 3.9 printing daemon is deactivated.
Positive: 3.10 Graphical login is deactivated.

Positive: 3.11 Mail daemon is not listening on TCP 25.
Positive: 3.12 Web server is deactivated.
Positive: 3.13 snmp daemon is deactivated.
Negative: 3.14 named DNS server not deactivated.
Positive: 3.15 postgresql (SQL) database server is deactivated.
Positive: 3.16 routing daemons are deactivated.
Positive: 3.17 Webmin GUI-based system administration daemon deactivated.
Positive: 3.18 Squid web cache daemon deactivated.
Negative: 3.19 xinetd is still active.
Note: 3.20 Bad or no umask set in /etc/rc.d/init.d/functions -- checking another file now.
Negative: 3.20 umask not found in first /etc/rcX.d script /etc/rc3.d/S05kudzu.
Negative: 4.1 Coredumps aren't deactivated.
Positive: 4.2 /etc/exports is empty or doesn't exist, so it doesn't need to be tuned for privports.
Negative: 4.3 IP forwarding is activated.
Negative: 4.3 /proc/sys/net/ipv4/tcp_max_syn_backlog should be at least 4096 to handle SYN floods.
Negative: 4.4 /proc/sys/net/ipv4/conf/eth1/send_redirects should be 0 to disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/eth0/send_redirects should be 0 to disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/lo/send_redirects should be 0 to disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/default/send_redirects should be 0 to disable outgoing redirect messages.
Positive: 5.1 syslog captures auth and authpriv messages.
Negative: 6.1 Removable filesystem /mnt/floppy is not mounted nosuid.
Negative: 6.2 PAM allows users to mount CD-ROMS. (/etc/security/console.perms)
Negative: 6.2 PAM allows users to mount floppies. (/etc/security/console.perms)
Positive: 6.3 password and group files have right permissions and owners.
Positive: 6.4 all temporary directories have sticky bits set.
Negative: 7.1 rhosts authentication not deactivated in /etc/pam.d/rlogin.
Negative: 7.1 rhosts authentication not deactivated in /etc/pam.d/rsh.
Positive: 7.2 /etc/hosts.equiv file not present or has size zero.
Negative: 7.3 /etc/ftpusers doesn't exist
Negative: 7.4 Couldn't open cron.allow
Negative: 7.4 Couldn't open at.allow
Negative: 7.5 The permissions on /etc/crontab are not sufficiently restrictive.
Negative: 7.6 No Authorized Only message in /etc/motd.
Positive: 7.6 All authorized-use-only warning banners are in place.
Negative: 7.7 /etc/securetty has a non tty1-12 line: tty10.
Negative: 7.8 lilo isn't password-protected.
Negative: 8.1 uucp has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.

Negative: 8.1 operator has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 adm has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 bin has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 daemon has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 ftp has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 games has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 gopher has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 lp has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 mail has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 news has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 nobody has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Positive: 8.2 There were no +: entries in passwd, shadow or group maps.
Positive: 8.3 All users have passwords
Positive: 8.4 Only one UID 0 account AND it is named root.
Positive: 8.5 root's PATH is clean of group/world writable directories or the current-directory link.
Positive: 8.6 root account has no dangerous rhosts, shosts, or netrc files.
Negative: 8.7 User mail 's homedir is group writable!
Positive: 8.8 No group or world-writable dotfiles!
Positive: 8.9 No user has a .netrc or .rhosts file.
Negative: 8.10 Default umask may not block group-writable. Check /etc/csh.login
Negative: 8.10 Default umask may not block world-writable. Check /etc/bashrc.
Negative: 8.10 Default umask may not block group-writable. Check /etc/bashrc.
Negative: 8.10 Default umask may not block world-writable. Check /etc/csh.cshrc.
Positive: 9.1 System isn't running sshd, but isn't running inetd so you're probably not using any remote access/administration tool.
Negative: 9.2 This machine isn't synced with ntp.
Preliminary rating given at time: Sat Feb 22 13:44:34 2003

Preliminary rating = 5.71 / 10.00

Positive: 6.5 No non-standard SUID/SGID programs found.
Ending run at time: Sat Feb 22 13:44:57 2003

Final rating = 5.89 / 10.00

CISscan for firewall-I server

*** CIS Ruler Run ***
Starting at time 20030301-17:22:04

Negative: 1.1 System appears not to have been patched within the last month.
Negative: 2.2 No Authorized Only banner for in.telnetd.
Negative: 2.2 No Authorized Only banner for in.ftpd.
Negative: 2.2 No Authorized Only banner for in.rlogind.
Negative: 2.3 telnet not deactivated.
Negative: 2.4 ftp not deactivated.
Positive: 2.5 rsh, rcp and rlogin are deactivated.
Positive: 2.6 tftp is deactivated.
Negative: 2.7 TCP Wrappers not configured for default-deny on this inetd-based system.
Positive: 3.1 Miscellaneous scripts are all turned off.
Positive: 3.2 NFS Server script nfs is deactivated.
Positive: 3.3 This machine isn't being used as an NFS client.
Positive: 3.4 NIS Client processes are deactivated.
Positive: 3.5 NIS Server processes are deactivated.
Positive: 3.6 portmapper has been deactivated.
Positive: 3.7 samba windows filesharing daemons are deactivated.
Positive: 3.8 netfs rc script is deactivated.
Positive: 3.9 printing daemon is deactivated.
Positive: 3.10 Graphical login is deactivated.
Positive: 3.11 Mail daemon is not listening on TCP 25.
Positive: 3.12 Web server is deactivated.
Positive: 3.13 snmp daemon is deactivated.
Positive: 3.14 DNS server is deactivated.
Positive: 3.15 postgresql (SQL) database server is deactivated.
Positive: 3.16 routing daemons are deactivated.
Positive: 3.17 Webmin GUI-based system administration daemon deactivated.
Positive: 3.18 Squid web cache daemon deactivated.
Negative: 3.19 inetd is still active.
Note: 3.20 Bad or no umask set in /etc/rc.d/init.d/functions -- checking another file now.
Negative: 3.20 umask not found in first /etc/rcX.d script .
Negative: 4.1 Coredumps aren't deactivated.
Positive: 4.2 /etc/exports is empty or doesn't exist, so it doesn't need to be tuned for privports.
Negative: 4.3 IP forwarding is activated.
Negative: 4.3 /proc/sys/net/ipv4/tcp_max_syn_backlog should be at least 4096 to handle SYN floods.

Negative: 4.4 /proc/sys/net/ipv4/conf/eth4/send_redirects should be 0 to disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/eth3/send_redirects should be 0 to disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/eth2/send_redirects should be 0 to disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/eth1/send_redirects should be 0 to disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/eth0/send_redirects should be 0 to disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/lo/send_redirects should be 0 to disable outgoing redirect messages.
Negative: 4.4 /proc/sys/net/ipv4/conf/default/send_redirects should be 0 to disable outgoing redirect messages.
Positive: 5.1 syslog captures auth and authpriv messages.
Negative: 6.1 Removable filesystem /mnt/floppy is not mounted nosuid.
Negative: 6.2 PAM allows users to mount CD-ROMS. (/etc/security/console.perms)
Negative: 6.2 PAM allows users to mount floppies. (/etc/security/console.perms)
Positive: 6.3 password and group files have right permissions and owners.
Positive: 6.4 all temporary directories have sticky bits set.
Negative: 7.1 rhosts authentication not deactivated in /etc/pam.d/rlogin.
Negative: 7.1 rhosts authentication not deactivated in /etc/pam.d/rsh.
Positive: 7.2 /etc/hosts.equiv file not present or has size zero.
Negative: 7.3 User gopher is not present in /etc/ftpusers
Negative: 7.3 User xfs is not present in /etc/ftpusers
Negative: 7.3 User postgres is not present in /etc/ftpusers
Negative: 7.4 Couldn't open cron.allow
Negative: 7.4 Couldn't open at.allow
Negative: 7.5 The permissions on /etc/crontab are not sufficiently restrictive.
Negative: 7.6 No Authorized Only message in /etc/motd.
Positive: 7.6 All authorized-use-only warning banners are in place.
Positive: 7.7 /etc/securetty doesn't have any lines other than tty1..6.
Negative: 7.8 lilo isn't password-protected.
Negative: 8.1 uucp has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 operator has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 adm has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 bin has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 daemon has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 ftp has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.

Negative: 8.1 games has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 gopher has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 lp has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 mail has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 news has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 nobody has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 postgres has a valid shell of /bin/bash.
Positive: 8.2 There were no +: entries in passwd, shadow or group maps.
Positive: 8.3 All users have passwords
Positive: 8.4 Only one UID 0 account AND it is named root.
Positive: 8.5 root's PATH is clean of group/world writable directories or the current-directory link.
Positive: 8.6 root account has no dangerous rhosts, shosts, or netrc files.
Negative: 8.7 User lp 's homedir is group writable!
Negative: 8.7 User mail 's homedir is group writable!
Negative: 8.7 User news 's homedir is group writable!
Positive: 8.8 No group or world-writable dotfiles!
Positive: 8.9 No user has a .netrc or .rhosts file.
Negative: 8.10 Default umask may not block group-writable. Check /etc/csh.login
Negative: 8.10 Default umask may not block world-writable. Check /etc/bashrc.
Negative: 8.10 Default umask may not block group-writable. Check /etc/bashrc.
Negative: 9.1 System isn't running sshd.
Negative: 9.2 This machine isn't synced with ntp.
Preliminary rating given at time: Sat Mar 1 17:22:06 2003

Preliminary rating = 6.07 / 10.00

Negative: 6.5 Non-standard SUID program /usr/bin/ssh
Ending run at time: Sat Mar 1 17:22:09 2003

Final rating = 6.07 / 10.00

CISscan for firewall-i host

Appendix C – NMAP Output

Nmap output when run from firewall-x server
nmap -sT -sR -O -v -p 1-65535 -T Normal 10.10.229.112/28

Starting nmap V. 3.00 (www.insecure.org/nmap/)

```
Host   (10.10.229.112) seems to be a subnet broadcast address (returned 3 extra
 pings). Skipping host.
Host firewall-x.local.domain (10.10.229.113) appears to be up ... good.
Initiating Connect() Scan against firewall-x.local.domain (10.10.229.113)
Adding open port 53/tcp
Adding open port 111/tcp
Adding open port 113/tcp
Adding open port 23/tcp
Adding open port 513/tcp
Adding open port 514/tcp
The Connect() Scan took 6 seconds to scan 65535 ports.
Initiating RPCGrind Scan against firewall-x.local.domain (10.10.229.113)
The RPCGrind Scan took 2 seconds to scan 0 ports.
For OSScan assuming that port 23 is open and port 1 is closed and neither are
firewalled
Interesting ports on firewall-x.local.domain (10.10.229.113):
(The 65529 ports scanned but not shown below are in state: closed)
Port       State       Service (RPC)
23/tcp     open        telnet
53/tcp     open        domain
111/tcp    open        sunrpc (rpcbind V2)
113/tcp    open        auth
513/tcp    open        login
514/tcp    open        shell
Remote operating system guess: Linux 2.1.19 - 2.2.20
Uptime 5.830 days (since Mon Feb 24 05:48:48 2003)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=6037324 (Good luck!)
IPID Sequence Generation: Incremental

Host firewall-i.local.domain (10.10.229.114) appears to be up ... good.
Initiating Connect() Scan against firewall-i.local.domain (10.10.229.114)
Adding open port 25/tcp
Adding open port 80/tcp
Adding open port 23/tcp
Adding open port 5631/tcp
Bumping up senddelay by 10000 (to 10000), due to excessive drops
Bumping up senddelay by 20000 (to 30000), due to excessive drops
Bumping up senddelay by 30000 (to 60000), due to excessive drops
Bumping up senddelay by 40000 (to 100000), due to excessive drops
Bumping up senddelay by 50000 (to 150000), due to excessive drops
Bumping up senddelay by 60000 (to 210000), due to excessive drops
Bumping up senddelay by 75000 (to 285000), due to excessive drops
Bumping up senddelay by 75000 (to 360000), due to excessive drops
The Connect() Scan took 1596 seconds to scan 1601 ports.
Initiating RPCGrind Scan against hydra.stratcoinc.com (66.228.213.114)
```

```
The RPCGrind Scan took 6 seconds to scan 0 ports.
For OSScan assuming that port 23 is open and port 1 is closed and neither are fi
rewalled
Interesting ports on hydra.stratcoinc.com (10.10.229.114):
(The 1597 ports scanned but not shown below are in state: closed)
Port       State       Service (RPC)
23/tcp     open        telnet
25/tcp     open        smtp
80/tcp     open        http
5631/tcp   open        pcanywheredata
Remote operating system guess: Linux 2.2.14
Uptime 136.377 days (since Wed Dec 18 09:06:42 2002)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=1888418 (Good luck!)
IPID Sequence Generation: Incremental

Host  (10.10.229.115) appears to be down, skipping it.
Host mail.local.domain (10.10.229.116) appears to be up ... good.
Initiating Connect() Scan against mail.local.domain (10.10.229.116)
Adding open port 8890/tcp
Adding open port 143/tcp
Adding open port 21/tcp
Adding open port 9000/tcp
Adding open port 111/tcp
Adding open port 80/tcp
Adding open port 113/tcp
Adding open port 23/tcp
Adding open port 7100/tcp
Adding open port 513/tcp
Adding open port 22/tcp
Adding open port 515/tcp
Adding open port 109/tcp
Adding open port 514/tcp
Adding open port 587/tcp
Adding open port 79/tcp
Adding open port 3306/tcp
Adding open port 25/tcp
Adding open port 110/tcp
Adding open port 1024/tcp
The Connect() Scan took 11 seconds to scan 65535 ports.
Initiating RPCGrind Scan against mail.local.domain (10.10.229.116)
The RPCGrind Scan took 6 seconds to scan 0 ports.
For OSScan assuming that port 21 is open and port 1 is closed and neither are
firewalled
Interesting ports on mail.local.domain (10.10.229.116):
(The 65515 ports scanned but not shown below are in state: closed)
```

```
Port       State       Service (RPC)
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     open        telnet
25/tcp     open        smtp
79/tcp     open        finger
80/tcp     open        http
109/tcp    open        pop-2
110/tcp    open        pop-3
111/tcp    open        sunrpc (rpcbind V2)
113/tcp    open        auth
143/tcp    open        imap2
513/tcp    open        login
514/tcp    open        shell
515/tcp    open        printer
587/tcp    open        submission
1024/tcp   open        kdm (status V1)
3306/tcp   open        mysql
7100/tcp   open        font-service
8890/tcp   open        unknown
9000/tcp   open        unknown
Remote operating system guess: Linux 2.1.19 - 2.2.20
Uptime 5.519 days (since Mon Feb 24 13:22:05 2003)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=5882400 (Good luck!)
IPID Sequence Generation: Incremental

Host  (10.10.229.117) appears to be down, skipping it.
Host  (10.10.229.118) appears to be down, skipping it.
Host  (10.10.229.119) appears to be down, skipping it.
Host  (10.10.229.120) appears to be down, skipping it.
Host  (10.10.229.122) appears to be down, skipping it.
Host  (10.10.229.123) appears to be down, skipping it.
Host  (10.10.229.124) appears to be down, skipping it.
Host  (10.10.229.125) appears to be down, skipping it.
Host  (10.10.229.126) appears to be down, skipping it.
Host   (10.10.229.127) seems to be a subnet broadcast address (returned 4 extra
 pings). Skipping host.
Nmap run completed -- 16 IP addresses (6 hosts up) scanned in 1461 seconds
```

Nmap output when run from host on the Internet

```
nmap -sT -sR -v -O -p 1-65535 64.255.229/28

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host   (10.10.229.112) seems to be a subnet broadcast address (returned 1 extra
pings). Skipping host.
```

```
Host  (10.10.229.113) appears to be up ... good.
Initiating Connect() Scan against  (10.10.229.113)
Adding open port 23/tcp
Adding open port 53/tcp
Adding open port 113/tcp
The Connect() Scan took 17456 seconds to scan 65535 ports.
Initiating RPCGrind Scan against  (10.10.229.113)
The RPCGrind Scan took 0 seconds to scan 0 ports.
For OSScan assuming that port 23 is open and port 11583 is closed and neither
are firewalled
Interesting ports on  (10.10.229.113):
(The 65527 ports scanned but not shown below are in state: filtered)
Port       State       Service (RPC)
23/tcp     open        telnet
53/tcp     open        domain
113/tcp    open        auth
11583/tcp  closed      unknown
11966/tcp  closed      unknown
14176/tcp  closed      unknown
25474/tcp  closed      unknown
32490/tcp  closed      unknown
Remote operating system guess: Linux 2.2.14
Uptime 148.019 days (since Fri Sep 27 17:47:48 2002)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=1763400 (Good luck!)
IPID Sequence Generation: Incremental

Host  (10.10.229.114) appears to be up ... good.
Initiating Connect() Scan against  (10.10.229.114)
Adding open port 80/tcp
Adding open port 23/tcp
Adding open port 5631/tcp
Adding open port 25/tcp
The Connect() Scan took 17287 seconds to scan 65535 ports.
Initiating RPCGrind Scan against  (10.10.229.114)
The RPCGrind Scan took 0 seconds to scan 0 ports.
Warning:  OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
For OSScan assuming that port 23 is open and port 32707 is closed and neither
are firewalled
Interesting ports on  (10.10.229.114):
(The 65531 ports scanned but not shown below are in state: filtered)
Port       State       Service (RPC)
23/tcp     open        telnet
25/tcp     open        smtp
80/tcp     open        http
```

```
5631/tcp   open       pcanywheredata
Remote OS guesses: Linux 2.1.19 - 2.2.20, Linux kernel 2.2.13, Linux 2.2.14
Uptime 66.679 days (since Wed Dec 18 09:10:19 2002)
TCP Sequence Prediction: Class=random positive increments
                  Di  fficulty=3413719 (Good luck!)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 17298 seconds
```

Netstat -a output – firewall –x

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp        0    136 athena.stratcoin:telnet hydra.stratcoinc.c:1040 ESTABLISHED
tcp        0      0 athena.stratcoin:domain *:*                  LISTEN
tcp        0      0 64.255.228.67:domain    *:*                  LISTEN
tcp        0      0 localhost:domain        *:*                  LISTEN
tcp        0      0 *:shell                 *:*                  LISTEN
tcp        0      0 *:telnet                *:*                  LISTEN
tcp        0      0 *:login                 *:*                  LISTEN
tcp        0      0 *:auth                  *:*                  LISTEN
tcp        0      0 *:sunrpc                *:*                  LISTEN
udp        0      0 athena.stratcoin:domain *:*
udp        0      0 64.255.228.67:domain    *:*
udp        0      0 localhost:domain        *:*
udp        0      0 *:sunrpc                *:*
raw        0      0 *:icmp                  *:*                  7
raw        0      0 *:tcp                   *:*                  7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  0      [ ]         STREAM     CONNECTED     235    @00000028
unix  0      [ ACC ]     STREAM     LISTENING     1185   /dev/gpmctl
unix  0      [ ACC ]     STREAM     LISTENING     1131   /var/run/ndc
unix  8      [ ]         DGRAM                    1001   /dev/log
unix  0      [ ]         DGRAM                    44877
unix  0      [ ]         DGRAM                    1225
unix  0      [ ]         DGRAM                    1196
unix  0      [ ]         DGRAM                    1129
unix  0      [ ]         DGRAM                    1111
unix  0      [ ]         DGRAM                    1064
unix  0      [ ]         DGRAM                    1044
unix  0      [ ]         DGRAM                    1016
```

Netstat -a output – firewall –i

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp        0    138 hydra.stratcoinc:telnet evrtwa1-ar10-4-43-:4220 ESTABLISHED
```

```
tcp        0      0 *:telnet                *:*                     LISTEN
tcp        0      0 *:ftp                   *:*                     LISTEN
udp        0      0 *:bootps                *:*
raw        0      0 *:icmp                  *:*                     7
raw        0      0 *:icmp                  *:*                     7
raw        0      0 *:tcp                   *:*                     7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ]         DGRAM                    154528 /dev/log
unix  0      [ ]         STREAM     CONNECTED     112    @00000012
unix  0      [ ]         DGRAM                    158078
unix  0      [ ]         DGRAM                    155287
unix  0      [ ]         DGRAM                    154521
unix  0      [ ]         DGRAM                    136043
```

Appendix D: SUID/SGUID Files

firewall-x

```
find / \(  -perm -4000 -o -perm -2000 \)  -user 0 ! -type d ! -type l -exec ls -ldb {} \;
-rwsr-xr-x    1 root     root        35964 Aug 23  2000 /usr/bin/at
-rwsr-xr-x    1 root     root        21248 Aug 24  2000 /usr/bin/crontab
-rwsr-xr-x    1 root     root        34220 Aug  8  2000 /usr/bin/chage
-rwsr-xr-x    1 root     root        36344 Aug  8  2000 /usr/bin/gpasswd
-rws--x--x    2 root     root       793603 Aug  7  2000 /usr/bin/suidperl
-rws--x--x    2 root     root       793603 Aug  7  2000 /usr/bin/sperl5.6.0
-rwxr-sr-x    1 root     man         35260 Aug 23  2000 /usr/bin/man
-rwsr-xr-x    1 root     root       155436 Jul 17  2000 /usr/bin/ssh
-r-s--x--x    1 root     root       13536 Jul 12  2000 /usr/bin/passwd
-rwxr-sr-x    1 root     mail        10932 Aug 11  2000 /usr/bin/lockfile
-rwsr-sr-x    1 root     mail        63772 Aug 11  2000 /usr/bin/procmail
-rwsr-xr-x    1 root     root        14492 Jul 21  2000 /usr/bin/rcp
-rwsr-xr-x    1 root     root        10876 Jul 21  2000 /usr/bin/rlogin
-rwsr-xr-x    1 root     root         7828 Jul 21  2000 /usr/bin/rsh
-rwxr-sr-x    1 root     slocate     23964 Aug 23  2000 /usr/bin/slocate
-r-xr-sr-x    1 root     tty          6524 Aug  8  2000 /usr/bin/wall
-rws--x--x    1 root     root        13184 Aug 30  2000 /usr/bin/chfn
-rws--x--x    1 root     root        12640 Aug 30  2000 /usr/bin/chsh
-rws--x--x    1 root     root         5464 Aug 30  2000 /usr/bin/newgrp
-rwxr-sr-x    1 root     tty         8500 Aug 30  2000 /usr/bin/write
-rwsr-xr-x    1 root     root         6288 Aug 23  2000 /usr/sbin/usernetctl
-r-sr-xr-x    1 root     root       401748 Aug 22  2000 /usr/sbin/sendmail
-rwsr-xr-x    1 root     root        16992 Jul 19  2000 /usr/sbin/traceroute
-rwxr-sr-x    1 root     utmp         6584 Jul 12  2000 /usr/sbin/utempter
-rwsr-xr-x    1 root     root        14184 Jul 12  2000 /bin/su
```

-rwsr-xr-x 1 root root 20604 Aug 8 2000 **/bin/ping**
-rwsr-xr-x 1 root root 55356 Aug 5 2000 **/bin/mount**
-rwsr-xr-x 1 root root 25404 Aug 5 2000 **/bin/umount**
-rwxr-sr-x 1 root root 4116 Aug 23 2000 **/sbin/netreport**
-r-sr-xr-x 1 root root 14732 Aug 22 2000 **/sbin/pwdb_chkpwd**
-r-sr-xr-x 1 root root 15340 Aug 22 2000 **/sbin/unix_chkpwd**

find / \(-perm -4000 -o -perm -2000 \) ! -user 0 ! -type d ! -type l -exec ls -ldb {} \;
No matching files

firewall-i

find / \(-perm -4000 -o -perm -2000 \) -user 0 ! -type d ! -type l -exec ls -ldb {} \;

-rwxr-sr-x 1 root mail 16104 Sep 25 1999 **/usr/lib/emacs/20.4/i386-redhat-linux-gnu/movemail**
-rwsr-xr-x 1 root root 35168 Sep 22 1999 **/usr/bin/chage**
-rwsr-xr-x 1 root root 36756 Sep 22 1999 **/usr/bin/gpasswd**
-r-xr-sr-x 1 root tty 6788 Sep 6 1999 **/usr/bin/wall**
-rwsr-xr-x 1 root root 21816 Sep 10 1999 **/usr/bin/crontab**
-rwsr-xr-x 1 root root 33152 Aug 16 1999 **/usr/bin/at**
-r-sr-x--- 1 root news 42652 Aug 30 1999 **/usr/bin/inndstart**
-r-sr-x--- 1 root news 40060 Aug 30 1999 **/usr/bin/startinnfeed**
-r-sr-sr-x 1 root lp 15816 Sep 10 1999 **/usr/bin/lpq**
-r-sr-sr-x 1 root lp 15768 Sep 10 1999 **/usr/bin/lpr**
-r-sr-sr-x 1 root lp 16216 Sep 10 1999 **/usr/bin/lprm**
-rwxr-sr-x 1 root man 34656 Sep 13 1999 /usr/bin/man
-rwxr-sr-x 1 root uucp 164696 Jul 30 1999 **/usr/bin/minicom**
-r-s--x--x 1 root root 22312 Sep 25 1999 /usr/bin/passwd
-rws--x--x 2 root root 518140 Aug 30 1999 **/usr/bin/suidperl**
-rws--x--x 2 root root 518140 Aug 30 1999 **/usr/bin/sperl5.00503**
-rwxr-sr-x 1 root mail 12072 Aug 16 1999 /usr/bin/lockfile
-rwsr-sr-x 1 root mail 69556 Aug 16 1999 /usr/bin/procmail
-rwsr-xr-x 1 root root 14868 Jul 30 1999 **/usr/bin/rcp**
-rwsr-xr-x 1 root root 10708 Jul 30 1999 **/usr/bin/rlogin**
-rwsr-xr-x 1 root root 7908 Jul 30 1999 **/usr/bin/rsh**
-rwxr-sr-x 1 root slocate 24744 Sep 20 1999 **/usr/bin/slocate**
-rws--x--x 1 root root 14024 Sep 8 1999 /usr/bin/chfn
-rws--x--x 1 root root 13768 Sep 8 1999 **/usr/bin/chsh**
-rws--x--x 1 root root 5576 Sep 8 1999 /usr/bin/newgrp
-rwxr-sr-x 1 root tty 8328 Sep 8 1999 /usr/bin/write
-rwsr-xr-x 1 root root 147872 May 19 2000 /usr/bin/ssh
-rwsr-xr-x 1 root root 5896 Sep 26 1999 **/usr/sbin/usernetctl**
-rws--x--x 1 root root 9392 Sep 21 1999 **/usr/sbin/suexec**
-rwxr-sr-x 1 root lp 24136 Sep 10 1999 **/usr/sbin/lpc**
-rwsr-sr-x 1 root root 319908 Sep 1 1999 **/usr/sbin/sendmail**

```
-rwsr-xr-x   1 root     bin        16488 Jul  2  1999 /usr/sbin/traceroute
-rwxr-sr-x   1 root     utmp        6096 Sep 13  1999 /usr/sbin/utempter
-rwsr-xr-x   1 root     root       14124 Aug 17  1999 /bin/su
-rwsr-xr-x   1 root     root       53620 Sep 13  1999 /bin/mount
-rwsr-xr-x   1 root     root       26700 Sep 13  1999 /bin/umount
-rwsr-xr-x   1 root     root       18228 Sep 10  1999 /bin/ping
-rwxr-sr-x   1 root     root        3860 Sep 26  1999 /sbin/netreport
-rwsr-sr-x   1 root     tty        39948 Sep 25  1999 /sbin/dump
-rwsr-sr-x   1 root     tty        64652 Sep 25  1999 /sbin/restore
-r-sr-xr-x   1 root     root       26503 Sep 24  1999 /sbin/pwdb_chkpwd
```

find / \(-perm -4000 -o -perm -2000 \) ! -user 0 ! -type d ! -type l -exec ls -ldb {} \;

```
-r-xr-sr-x   1 news     news        72312 Aug 30  1999 /usr/bin/inews
-r-sr-x---   1 uucp     news        88544 Aug 30  1999 /usr/bin/rnews
-r-sr-sr-x   1 uucp     uucp       127924 Aug 23  1999 /usr/bin/cu
-r-sr-xr-x   1 uucp     uucp        92884 Aug 23  1999 /usr/bin/uucp
-r-sr-sr-x   1 uucp     uucp        39364 Aug 23  1999 /usr/bin/uuname
-r-sr-xr-x   1 uucp     uucp       101056 Aug 23  1999 /usr/bin/uustat
-r-sr-xr-x   1 uucp     uucp        93920 Aug 23  1999 /usr/bin/uux
-r-sr-sr-x   1 uucp     uucp       225008 Aug 23  1999 /usr/sbin/uucico
-r-sr-sr-x   1 uucp     uucp       103196 Aug 23  1999 /usr/sbin/uuxqt
```

Appendix E: Firewall Rules (/sbin/ipchains --list)

firewall-x – ipchains output

Chain input (policy REJECT):

	target	prot	opt	source	destination	ports
1.	ACCEPT	tcp	------	Anywhere	10.10.229.112/28	ftp -> any
2.	ACCEPT	tcp	------	Anywhere	10.10.229.112/28	ftp-data -> any
3.	ACCEPT	tcp	------	Anywhere	10.10.229.112/28	any -> ftp
4.	ACCEPT	tcp	------	Anywhere	10.10.229.112/28	any -> ftp-data
5.	ACCEPT	tcp	------	Anywhere	10.10.229.112/28	1024:65535 -> 1024:65535
6.	ACCEPT	tcp	------	Anywhere	10.10.212.67	any -> ftp
7.	ACCEPT	tcp	------	anywhere	10.10.212.67	any -> ftp-data
8.	ACCEPT	tcp	------	anywhere	10.10.212.67	any -> www
9.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	any -> www
10.	ACCEPT	tcp	------	anywhere	10.10.212.67	https -> any
11.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	https -> any
12.	ACCEPT	tcp	------	anywhere	10.10.212.67	any -> https
13.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	any -> https
14.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	www -> any
15.	ACCEPT	icmp	------	anywhere	firewall-x.local.domain	any -> any
16.	ACCEPT	icmp	------	anywhere	10.10.229.112/28	any -> any

17.	ACCEPT	icmp	------	anywhere	10.10.212.67	any -> any
18.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	nntp -> any
19.	ACCEPT	tcp	------	anywhere	10.10.212.67	any -> telnet
20.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	any -> telnet
21.	ACCEPT	tcp	------	anywhere	10.10.212.67	any -> ssh
22.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	any -> ssh
23.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	1723 -> any
24.	REJECT	all	----l-	10.10.229.112/28	anywhere	n/a
25.	REJECT	tcp	------	anywhere	10.10.212.67	any -> 2049
26.	REJECT	tcp	------	anywhere	10.10.212.67	2049 -> any
27.	REJECT	tcp	------	anywhere	10.10.212.67	any -> netbios-ns
28.	REJECT	udp	------	anywhere	10.10.212.127	any -> netbios-ns
29.	REJECT	tcp	------	anywhere	10.10.212.127	any -> netbios-ns
30.	REJECT	tcp	------	anywhere	10.10.212.67	any -> netbios-dgm
31.	REJECT	udp	------	anywhere	10.10.212.127	any -> netbios-dgm
32.	REJECT	tcp	------	anywhere	10.10.212.127	any -> netbios-dgm
33.	REJECT	tcp	------	anywhere	10.10.212.67	any -> netbios-ssn
34.	REJECT	tcp	------	anywhere	10.10.212.67	netbios-ns -> any
35.	REJECT	tcp	------	anywhere	10.10.212.67	netbios-dgm -> any
36.	REJECT	tcp	------	anywhere	10.10.212.67	netbios-ssn -> any
37.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	telnet -> any
38.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	any -> 2048
39.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	any -> 8890
40.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	any -> 9000
41.	ACCEPT	tcp	------	10.10.97	10.10.229.112/28	591 -> any
42.	ACCEPT	udp	------	anywhere	firewall-i.local.domain	5632 -> any
43.	ACCEPT	tcp	------	anywhere	anywhere	any -> auth
44.	ACCEPT	tcp	------	anywhere	anywhere	any -> domain
45.	ACCEPT	tcp	------	anywhere	anywhere	domain -> any
46.	ACCEPT	udp	------	anywhere	anywhere	any -> domain
47.	ACCEPT	udp	------	anywhere	anywhere	domain -> any
48.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	any -> smtp
49.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	smtp -> any
50.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	pop3 -> any
51.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	any -> pop3
52.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	imap2 -> any
53.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	any -> imap2
54.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	any -> ssmtp
55.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	ssmtp -> any
56.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	any -> pop3s
57.	ACCEPT	tcp	------	anywhere	10.10.229.112/28	pop3s -> any
58.	ACCEPT	all	------	10.10.229.112/28	anywhere	n/a
59.	ACCEPT	all	------	anywhere	anywhere	n/a
60.	ACCEPT	tcp	!y----	anywhere	10.10.212.67	any -> 1024:65535
61.	ACCEPT	tcp	------	anywhere	10.10.212.67	ftp-data -> 1024:65535
62.	ACCEPT	udp	------	anywhere	10.10.212.67	any -> 1024:65535

63. REJECT all ----l- anywhere anywhere n/a

Chain forward (policy REJECT):

	target	prot	opt	source	destination	ports
64.	ACCEPT	all	------	anywhere	10.10.229.112/28	n/a
65.	ACCEPT	all	------	10.10.229.112/28	anywhere	n/a
66.	REJECT	all	----l-	anywhere	anywhere	n/a

Chain output (policy REJECT):

	target	prot	opt	source	destination	ports
67.	ACCEPT	all	------	anywhere	10.10.229.112/28	n/a
68.	ACCEPT	all	------	anywhere	anywhere	n/a
69.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	any -> telnet
70.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	ftp -> any
71.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	any -> ftp
72.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	ftp-data -> any
73.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	any -> ftp-data
74.	ACCEPT	tcp	------	10.10.212.67	anywhere	www -> any
75.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	www -> any
76.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	any -> www
77.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	any -> https
78.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	https -> any
79.	ACCEPT	tcp	------	10.10.212.67	anywhere	telnet -> any
80.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	telnet -> any
81.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	1024:65535 -> ftp
82.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	ftp -> 1024:65535
83.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	ftp-data -> 1024:65535
84.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	1024:65535 -> ftp-data
85.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	1024:65535 -> 1024:65535
86.	ACCEPT	tcp	------	10.10.229.112/28	10.10.97	any -> 591
87.	ACCEPT	tcp	------	10.10.212.67	anywhere	ssh -> any
88.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	ssh -> any
89.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	any -> 1723
90.	ACCEPT	tcp	------	anywhere	anywhere	auth -> any
91.	ACCEPT	udp	------	10.10.229.112/28	anywhere	32769:65535->33434:33523
92.	ACCEPT	tcp	------	10.10.212.67	anywhere	domain -> any
93.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	domain -> any
94.	ACCEPT	tcp	------	10.10.229.112/28	anywhere	any -> domain
95.	ACCEPT	udp	------	10.10.212.67	anywhere	domain -> any
96.	ACCEPT	udp	------	10.10.229.112/28	anywhere	domain -> any
97.	ACCEPT	udp	------	10.10.229.112/28	anywhere	any -> domain
98.	ACCEPT	tcp	------	10.10.212.67	209.20.248.5	any -> domain

99. ACCEPT	tcp	------	firewall-x.local.domain	209.20.248.5	any -> domain
100 ACCEPT	udp	------	10.10.212.67	209.20.248.5	any -> domain
101 ACCEPT	udp	------	firewall-x.local.domain	209.20.248.5	any -> domain
102 ACCEPT	icmp	------	anywhere	anywhere	any -> any
103 ACCEPT	tcp	------	10.10.229.112/28	anywhere	any -> nntp
104 ACCEPT	tcp	------	10.10.229.112/28	anywhere	any -> smtp
105 ACCEPT	tcp	------	10.10.229.112/28	anywhere	smtp -> any
106 ACCEPT	tcp	------	10.10.229.112/28	anywhere	any -> pop3
107 ACCEPT	tcp	------	10.10.229.112/28	anywhere	pop3 -> any
108 ACCEPT	tcp	------	10.10.229.112/28	anywhere	any -> imap2
109 ACCEPT	tcp	------	10.10.229.112/28	anywhere	imap2 -> any
110 ACCEPT	tcp	------	10.10.229.112/28	anywhere	any -> ssmtp
111 ACCEPT	tcp	------	10.10.229.112/28	anywhere	ssmtp -> any
112 ACCEPT	tcp	------	10.10.229.112/28	anywhere	any -> pop3s
113 ACCEPT	tcp	------	10.10.229.112/28	anywhere	pop3s -> any
114 ACCEPT	tcp	----l-	10.10.212.67	anywhere	any -> 5631
115 ACCEPT	tcp	----l-	10.10.229.112/28	anywhere	any -> 5631
116 ACCEPT	udp	----l-	10.10.212.67	anywhere	any -> 5631
117 ACCEPT	tcp	----l-	10.10.212.67	anywhere	any -> 5632
118 ACCEPT	udp	----l-	10.10.229.112/28	anywhere	any -> 5632
119 ACCEPT	udp	----l-	10.10.212.67	anywhere	any -> ssh
120 ACCEPT	udp	----l-	10.10.229.112/28	anywhere	any -> ssh
121 REJECT	all	----l-	anywhere	10.10.229.112/28	n/a
122 REJECT	all	----l-	10.10.229.112/28	anywhere	n/a
123 REJECT	udp	----l-	10.10.212.67	anywhere	any -> netbios-ns
124 REJECT	udp	----l-	10.10.212.67	anywhere	any -> netbios-dgm
125 REJECT	udp	----l-	10.10.212.67	anywhere	any -> netbios-ssn
126 REJECT	udp	----l-	10.10.212.67	anywhere	netbios-ns -> netbios-ns
127 REJECT	udp	----l-	10.10.212.67	anywhere	netbios-dgm ->netbios-dgm
128 REJECT	udp	----l-	10.10.212.67	anywhere	netbios-ssn -> netbios-ssn
129 REJECT	udp	----l-	10.10.212.67	anywhere	any -> sunrpc
130 REJECT	udp	----l-	10.10.212.67	anywhere	sunrpc -> any
131 REJECT	udp	----l-	10.10.212.67	anywhere	any -> 635
132 REJECT	udp	----l-	10.10.212.67	anywhere	635 -> any
133 REJECT	tcp	----l-	10.10.212.67	anywhere	any -> 1723
134 REJECT	udp	----l-	10.10.212.67	anywhere	any -> 1723
135 REJECT	tcp	----l-	10.10.212.67	anywhere	any -> 1745
136 REJECT	udp	----l-	10.10.212.67	anywhere	any -> 1745
137 REJECT	tcp	----l-	10.10.212.67	anywhere	any -> 2049
138 REJECT	tcp	----l-	10.10.212.67	anywhere	2049 -> any
139 REJECT	udp	----l-	10.10.212.67	anywhere	any -> nfsd

140	REJECT	udp	----l-	10.10.212.67	anywhere	nfsd -> any
141	REJECT	tcp	----l-	10.10.212.67	anywhere	any -> X:6010
142	REJECT	udp	----l-	10.10.212.67	anywhere	any -> 6000:6010
143	REJECT	tcp	----l-	10.10.212.67	anywhere	any -> 12345
144	REJECT	tcp	----l-	10.10.212.67	anywhere	any -> 12346
145	REJECT	tcp	----l-	10.10.212.67	anywhere	any -> 20034
146	REJECT	udp	----l-	10.10.212.67	anywhere	any -> 31337
147	REJECT	tcp	----l-	10.10.212.67	anywhere	any -> 5742
148	REJECT	tcp	----l-	10.10.212.67	anywhere	any -> 30303
149	REJECT	tcp	----l-	10.10.212.67	anywhere	any -> 40421
150	REJECT	tcp	----l-	10.10.212.67	anywhere	27665 -> any
151	REJECT	udp	----l-	10.10.212.67	anywhere	27444 -> any
152	REJECT	udp	----l-	10.10.212.67	anywhere	31335 -> any
153	REJECT	tcp	----l-	10.10.212.67	anywhere	500 -> any
154	REJECT	tcp	----l-	10.10.212.67	anywhere	any -> 500
155	REJECT	tcp	----l-	10.10.212.67	anywhere	20432 -> any
156	REJECT	udp	----l-	10.10.212.67	anywhere	18753 -> any
157	REJECT	udp	----l-	10.10.212.67	anywhere	20433 -> any
158	ACCEPT	tcp	------	10.10.212.67	anywhere	1024:65535 -> any
159	ACCEPT	udp	------	10.10.212.67	anywhere	1024:65535 -> any
160	REJECT	all	----l-	anywhere	anywhere	n/a

firewall-i – ipchains output

Chain input (policy REJECT):

	target	prot	opt	source	destination	ports
1.	ACCEPT	tcp	------	192.168.1.0/24	10.10.229.112/28	any -> ftp
2.	ACCEPT	tcp	------	192.168.1.0/24	10.10.229.112/28	ftp -> any
3.	ACCEPT	tcp	------	192.168.1.0/24	10.10.229.112/28	any -> ftp-data
4.	ACCEPT	tcp	------	192.168.1.0/24	10.10.229.112/28	ftp-data -> any
5.	ACCEPT	tcp	------	192.168.1.0/24	10.10.229.112/28	any -> ssh
6.	ACCEPT	tcp	------	192.168.1.0/24	10.10.229.112/28	any -> any
7.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	any -> ftp
8.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	ftp -> any
9.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	any -> ftp-data
10.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	ftp-data -> any
11.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	ftp-data -> any
12.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	ftp -> any
13.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	1024:65535 -> 1024:65535
14.	ACCEPT	tcp	----l-	anywhere	firewall-i.local.domain	any -> www
15.	ACCEPT	tcp	----l-	192.168.0.0/16	anywhere	any -> www
16.	ACCEPT	tcp	!y----	anywhere	anywhere	nntp -> any
17.	ACCEPT	tcp	!y----	anywhere	anywhere	any -> nntp
18.	ACCEPT	icmp	------	192.168.0.0/16	anywhere	any -> any

19.	ACCEPT	icmp	------	anywhere	192.168.0.0/16	any -> any
20.	ACCEPT	icmp	------	anywhere	10.10.229.112/28	any -> any
21.	ACCEPT	tcp	------	anywhere	firewall-i.local.domain	any -> telnet
22.	ACCEPT	tcp	------	anywhere	firewall-i.local.domain	any -> ssh
23.	ACCEPT	udp	------	securehost1.domain	192.168.1.0/24	500 -> 500
24.	ACCEPT	50	------	securehost1.domain	192.168.1.0/24	n/a
25.	ACCEPT	tcp	------	securehost1.domain	192.168.1.0/24	any -> 1723
26.	ACCEPT	47	------	securehost1.domain	192.168.1.0/24	n/a
27.	REJECT	all	----l-	192.168.0.0/16	anywhere	n/a
28.	REJECT	tcp	------	anywhere	firewall-i.local.domain	any -> 2049
29.	REJECT	tcp	------	anywhere	firewall-i.local.domain	2049 -> any
30.	REJECT	tcp	------	anywhere	firewall-i.local.domain	any -> netbios-ns
31.	REJECT	udp	------	anywhere	10.10.229.127	any -> netbios-ns
32.	REJECT	tcp	------	anywhere	10.10.229.127	any -> netbios-ns
33.	REJECT	tcp	------	anywhere	firewall-i.local.domain	any -> netbios-dgm
34.	REJECT	udp	------	anywhere	10.10.229.127	any -> netbios-dgm
35.	REJECT	tcp	------	anywhere	10.10.229.127	any -> netbios-dgm
36.	REJECT	tcp	------	anywhere	firewall-i.local.domain	any -> netbios-ssn
37.	REJECT	tcp	------	anywhere	firewall-i.local.domain	netbios-ns -> any
38.	REJECT	tcp	------	anywhere	firewall-i.local.domain	netbios-dgm -> any
39.	REJECT	tcp	------	anywhere	firewall-i.local.domain	netbios-ssn -> any
40.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	any -> telnet
41.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	any -> 2048
42.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	any -> 8890
43.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	any -> 9000
44.	ACCEPT	tcp	----l-	10.10.97	192.168.0.0/16	591 -> any
45.	ACCEPT	tcp	----l-	192.168.0.0/16	10.10.97	any -> 591
46.	ACCEPT	tcp	------	anywhere	anywhere	any -> auth
47.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	any -> domain
48.	ACCEPT	udp	------	192.168.0.0/16	anywhere	any -> domain
49.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	smtp -> any
50.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	pop-3 -> any
51.	ACCEPT	tcp	------	anywhere	firewall-i.local.domain	any -> smtp
52.	ACCEPT	all	------	192.168.1.0/24	anywhere	n/a
53.	ACCEPT	all	------	192.168.2.0/24	anywhere	n/a
54.	ACCEPT	all	------	192.168.3.0/24	anywhere	n/a
55.	ACCEPT	all	------	192.168.4.0/24	anywhere	n/a
56.	ACCEPT	all	------	anywhere	anywhere	n/a
57.	ACCEPT	tcp	!y----	anywhere	firewall-i.local.domain	any -> 1024:65535
58.	ACCEPT	tcp	----l-	anywhere	firewall-i.local.domain	ftp-data -> 1024:65535
59.	ACCEPT	udp	------	anywhere	firewall-i.local.domain	any -> 1024:65535
60.	ACCEPT	tcp	----l-	anywhere	firewall-i.local.domain	any -> 5631
61.	ACCEPT	udp	----l-	anywhere	firewall-i.local.domain	any -> 5631
62.	ACCEPT	tcp	----l-	anywhere	firewall-i.local.domain	any -> 5632
63.	ACCEPT	udp	----l-	anywhere	firewall-i.local.domain	any -> 5632
64.	ACCEPT	udp	----l-	anywhere	firewall-i.local.domain	any -> ssh

Chain forward (policy REJECT):

	target	prot	opt	source	destination	ports
65.	MASQ	udp	------	192.168.0.0/16	anywhere	ssh -> any
66.	MASQ	udp	------	192.168.0.0/16	anywhere	5632 -> any
67.	MASQ	tcp	------	192.168.0.0/16	anywhere	5632 -> any
68.	MASQ	udp	------	192.168.0.0/16	anywhere	5631 -> any
69.	MASQ	tcp	------	192.168.0.0/16	anywhere	5631 -> any
70.	MASQ	tcp	------	192.168.0.0/16	anywhere	smtp -> any
71.	MASQ	tcp	------	192.168.0.0/16	anywhere	www -> any
72.	MASQ	all	------	192.168.0.0/16	anywhere	n/a
73.	ACCEPT	all	------	anywhere	192.168.0.0/16	n/a
74.	ACCEPT	all	------	192.168.0.0/16	anywhere	n/a
75.	REJECT	all	----l-	anywhere	anywhere	n/a

Chain output (policy REJECT):

	target	prot	opt	source	destination	ports
76.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	ftp -> any
77.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	ftp-data -> any
78.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	ftp -> any
79.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	ftp-data -> any
80.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	telnet -> any
81.	ACCEPT	tcp	------	firewall-i.local.domain	anywhere	telnet -> any
82.	ACCEPT	tcp	------	10.10.229.112/28	192.168.0.0/16	telnet -> any
83.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	any -> telnet
84.	ACCEPT	tcp	------	firewall-i.local.domain	anywhere	www -> any
85.	ACCEPT	tcp	------	anywhere	192.168.1.2	any -> any
86.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	www -> any
87.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	https -> any
88.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	any -> https
89.	ACCEPT	tcp	------	anywhere	anywhere	any -> nntp
90.	ACCEPT	tcp	------	anywhere	anywhere	nntp -> any
91.	ACCEPT	tcp	------	192.168.1.0/24	anywhere	telnet -> any
92.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	telnet -> any
93.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	ftp -> any
94.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	ftp-data -> any
95.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	ftp -> any
96.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	ftp-data -> any
97.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	telnet -> any
98.	ACCEPT	tcp	------	firewall-i.local.domain	anywhere	telnet -> any
99.	ACCEPT	tcp	------	10.10.229.112/28	192.168.0.0/16	telnet -> any
100.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	any -> telnet
101.	ACCEPT	tcp	------	firewall-i.local.domain	anywhere	www -> any
102.	ACCEPT	tcp	------	anywhere	192.168.1.2	any -> any

103.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	www -> any
104.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	https -> any
105.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	any -> https
106.	ACCEPT	tcp	------	anywhere	anywhere	any -> nntp
107.	ACCEPT	tcp	------	anywhere	anywhere	nntp -> any
108.	ACCEPT	tcp	------	192.168.1.0/24	anywhere	telnet -> any
109.	ACCEPT	tcp	------	192.168.0.0/16	anywhere	telnet -> any
110.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	1024:65535 -> 1024:65535
111.	ACCEPT	tcp	----l-	192.168.0.0/16	10.10.97	any -> 591
112.	ACCEPT	tcp	----l-	10.10.97	192.168.0.0/16	591 -> any
113.	ACCEPT	tcp	------	firewall-i.local.domain	anywhere	ssh -> any
114.	ACCEPT	tcp	------	192.168.1.0/24	anywhere	ssh -> any
115.	ACCEPT	udp	------	192.168.1.0/24	securehost1.domain	500 -> 500
116.	ACCEPT	50	------	192.168.1.0/24	securehost1.domain	n/a
117.	ACCEPT	tcp	------	192.168.1.0/24	securehost1.domain	any -> 1723
118.	ACCEPT	47	------	192.168.1.0/24	securehost1.domain	n/a
119.	ACCEPT	tcp	------	anywhere	anywhere	auth -> any
120.	ACCEPT	udp	------	192.168.0.0/16	anywhere	32769:65535->33434:33523
121.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	domain -> any
122.	ACCEPT	udp	------	anywhere	192.168.0.0/16	domain -> any
123.	ACCEPT	icmp	------	anywhere	anywhere	any -> any
124.	ACCEPT	tcp	------	firewall-i.local.domain	anywhere	smtp -> any
125.	ACCEPT	tcp	------	anywhere	firewall-i.local.domain	smtp -> any
126.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	smtp -> any
127.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	pop-3 -> any
128.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	imap2 -> any
129.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	ssmtp -> any
130.	ACCEPT	tcp	------	anywhere	192.168.0.0/16	spop3 -> any
131.	ACCEPT	tcp	----l-	firewall-i.local.domain	anywhere	5631 -> any
132.	ACCEPT	udp	----l-	firewall-i.local.domain	anywhere	5631 -> any
133.	ACCEPT	tcp	----l-	firewall-i.local.domain	anywhere	5632 -> any
134.	ACCEPT	udp	----l-	firewall-i.local.domain	anywhere	5632 -> any
135.	ACCEPT	udp	----l-	firewall-i.local.domain	anywhere	ssh -> any
136.	REJECT	all	----l-	anywhere	192.168.0.0/16	n/a
137.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	any -> netbios-ns
138.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	any -> netbios-dgm
139.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	any -> netbios-ssn
140.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	netbios-ns -> netbios-ns
141.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	netbios-dgm -> netbios-dgm
142.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	netbios-ssn -> netbios-ssn
143.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	any -> sunrpc

144.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	sunrpc -> any
145.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	any -> 635
146.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	635 -> any
147.	REJECT	tcp	----l-	firewall-i.local.domain	anywhere	any -> 1723
148.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	any -> 1723
149.	REJECT	tcp	----l-	firewall-i.local.domain	anywhere	any -> 1745
150.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	any -> 1745
151.	REJECT	tcp	----l-	firewall-i.local.domain	anywhere	any -> 2049
152.	REJECT	tcp	----l-	firewall-i.local.domain	anywhere	2049 -> any
153.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	any -> 2049
154.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	2049 -> any
155.	REJECT	tcp	----l-	firewall-i.local.domain	anywhere	any -> 6000:6010
156.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	any -> 6000:6010
157.	REJECT	tcp	----l-	firewall-i.local.domain	anywhere	any -> 12345
158.	REJECT	tcp	----l-	firewall-i.local.domain	anywhere	any -> 12346
159.	REJECT	tcp	----l-	firewall-i.local.domain	anywhere	any -> 20034
160.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	any -> 31337
161.	REJECT	tcp	----l-	firewall-i.local.domain	anywhere	any -> 5742
162.	REJECT	tcp	----l-	firewall-i.local.domain	anywhere	any -> 30303
163.	REJECT	tcp	----l-	firewall-i.local.domain	anywhere	any -> 40421
164.	REJECT	tcp	----l-	firewall-i.local.domain	anywhere	27665 -> any
165.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	27444 -> any
166.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	31335 -> any
167.	REJECT	tcp	----l-	firewall-i.local.domain	anywhere	500 -> any
168.	REJECT	tcp	----l-	firewall-i.local.domain	anywhere	any -> 500
169.	REJECT	tcp	----l-	firewall-i.local.domain	anywhere	20432 -> any
170.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	18753 -> any
171.	REJECT	udp	----l-	firewall-i.local.domain	anywhere	20433 -> any
172.	ACCEPT	all	------	192.168.1.0/24	anywhere	n/a
173.	ACCEPT	all	------	192.168.2.0/24	anywhere	n/a
174.	ACCEPT	all	------	192.168.3.0/24	anywhere	n/a
175.	ACCEPT	all	------	192.168.4.0/24	anywhere	n/a
176.	ACCEPT	tcp	------	firewall-i.local.domain	anywhere	1024:65535 -> any
177.	ACCEPT	udp	------	firewall-i.local.domain	anywhere	1024:65535 -> any
178.	REJECT	all	----l-	anywhere	anywhere	n/a

Chain acctboth (0 references):

	target	prot	opt	source	destination	ports
179.	-	all	------	firewall-i.local.domain	anywhere	n/a
180.	-	all	------	anywhere	firewall-i.local.domain	n/a
181.	-	all	------	lan.local.domain	anywhere	n/a
182.	-	all	------	anywhere	lan.local.domain	n/a
183.	-	all	------	lan.local.domain	anywhere	n/a
184.	-	all	------	anywhere	lan.local.domain	n/a
185.	-	all	------	lan.local.domain	anywhere	n/a

186.-	all	------ anywhere	lan.local.domain	n/a
187.-	all	------ 192.168.4.1	anywhere	n/a
188.-	all	------ anywhere	192.168.4.1	n/a
189.-	all	------ anywhere	anywhere	n/a

Last Updated: January 22nd, 2019

Upcoming Training

SANS 2019	**Orlando, FL**	**Apr 01, 2019 - Apr 08, 2019**	**Live Event**
SANSFIRE 2019	**Washington, DC**	**Jun 15, 2019 - Jun 22, 2019**	**Live Event**
Community SANS New York SEC506	**New York, NY**	**Jul 15, 2019 - Jul 20, 2019**	**Community SANS**
SANS Network Security 2019	**Las Vegas, NV**	**Sep 09, 2019 - Sep 16, 2019**	**Live Event**