GIAC GSNA Certification
Auditing Networks, Perimeters, and Systems

GSNA Practical Assignment
Version 3.2
Option 1

Auditing the Astaro Secure Linux Firewall: An Evaluation for Commercial Use

Jeff Groman

January 9, 2005

Table of Contents

Introduction

Abstract

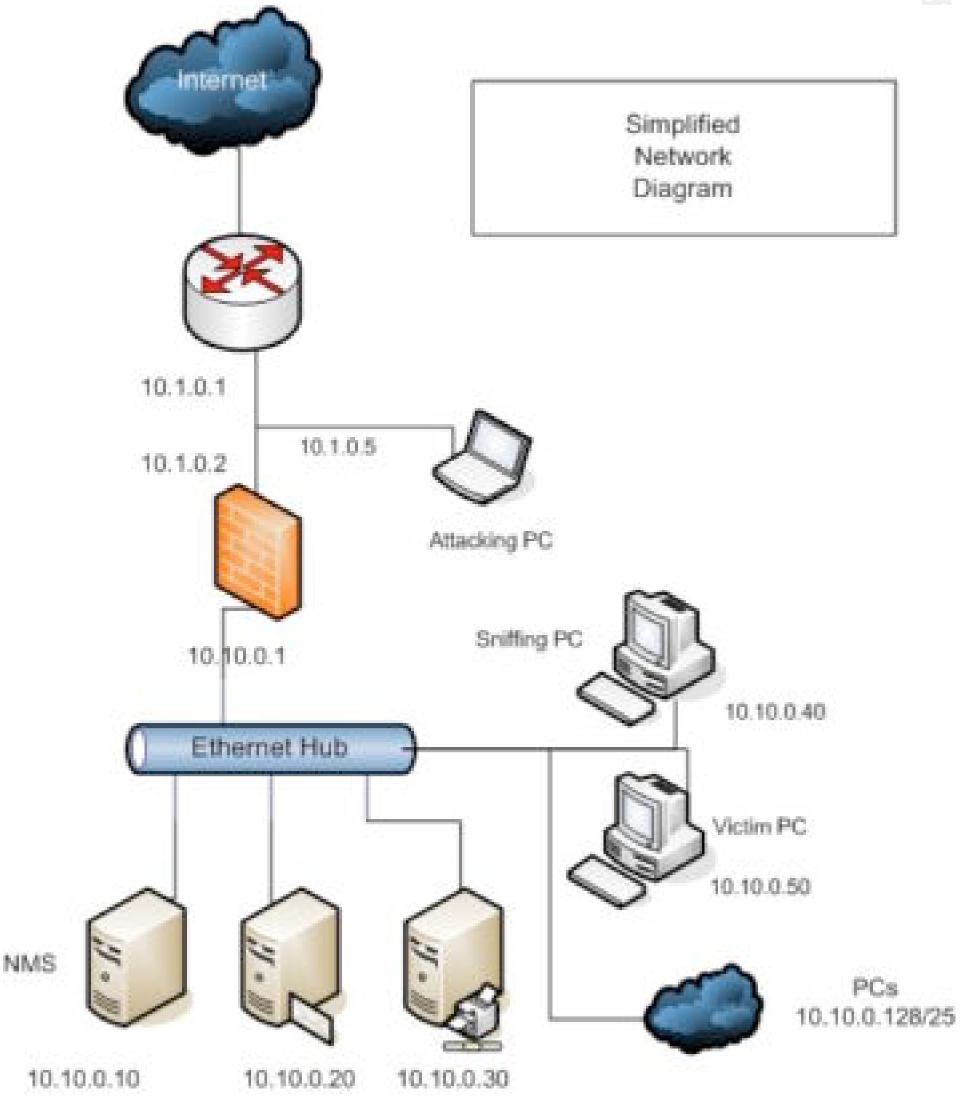
Historically, it has not been cost effective for the small office to employ a stateful firewall, the only options being high-end firewall packages or appliances. Lately, however, products have been introduced that are priced not only for the small business, but are even aimed at the consumer market. Moreover, with the advent of the Linux 2.4 kernel and IPTables (which replaced the venerable ipchains), this functionality comes bundled with any Linux distribution.

With that backdrop, this audit addresses a firewall replacement project in a smaller environment where the current firewall consists of packet filtering on a Cisco 2621 router.

The organization has determined that the Astaro firewall package is a good fit since it runs on inexpensive Intel-based hardware and comes with many add-ons such as virus protection, spam filtering, and VPN termination, as well as commercial support. However, before purchasing this product, they want a comprehensive audit done of both the firewall features, and the underlying OS.

Description of the Environment

The firewall to be audited is slated to replace an existing packet screen firewall router, and will become the primary perimeter defense for the corporate network. It should be noted, however, that the packet screening router should remain in place in order to maintain “defense in depth”. The figure below depicts the new environment, while also displaying the devices to be used in the audit:



The audit will be performed on a test segment, using test hardware. The following table lists the devices used in this audit.

	Make/Model	Processor	RAM	Drive	OS
Firewall	Dell GX1	Pentium III	128 MB	6 GB	Astaro Linux 5.0.14
Sniffer	Dell GX50	Celeron	128 MB	15 GB	Fedora Core 2
Victim	Dell GX1	Pentium II	128 MB	6 GB	Fedora Core 2
Attacker	Mac PowerBook	G4	1 GB	60 GB	Mac OS X 10.3.4

The firewall should be placed behind the packet screening router, but would still be the primary perimeter defense. Because of its role, it is critical that the firewall performs as expected, i.e. that it is configured to match the firewall policy.

Purpose of the Audit

Generally, a firewall should control the only entry point (or choke point) into a private network. Its role must be not only to control what traffic enters the internal network, but also what traffic leaves the network. That being said, the focus of this audit is to verify that this implementation will do just that.

A firewall's ability to control the choke point is based on how it is configured. Therefore, the main area that this audit focuses on is verifying that the firewall configuration is correct. Additionally, it is critical that the firewall OS is secure, and that will be verified as well. Though it is reasonable to expect the firewall to perform as advertised, its performance will also be verified in this audit.

Scope of the Audit

This audit addresses only the firewall configuration (not the antivirus, antispam, vpn, or other features of the Astaro firewall), and the underlying OS of the platform. Process, policy, and procedure will be mentioned, but these can be separate audit projects in themselves. Specifically, the audit will examine the firewall configuration to assess whether it matches the firewall policy, and determine if the firewall performs as expected.

The Astaro firewall offers a robust set of features, but these same features can potentially introduce new vulnerabilities. Therefore, the audit must examine the individual processes running, and determine if these processes introduce any additional exposures.

Vulnerabilities, Threats, Impacts, and Risks

The following table lists the significant vulnerabilities along with a value that describes the relative likelihood of a threat combining with the vulnerability to cause damage.

Vulnerabilities	Value
Environmental	
Environmental control failure	High
Physical security	High
Operational	
Network administrator does not properly understand how to configure firewall	High
Firewall configuration does not match corporate firewall policy.	High
ACL failure on edge router (defense in depth)	Med
Firewall policy is not in place	High
Incident Handling procedure is not in place	Med
Logging is not being monitored	High
Updates to firewall platform do not occur (patching)	High
Lack of Incident Handling procedure	High
Lack of Change Management procedure.	High
Hardware chosen is not sufficient for the traffic and processing load	High
Hardware fails	High
Lack of Business Continuity Plan	High
Backups not being made	Low
Firewall	
Firewall does not behave as expected	High
Firewall management interface (web) passwords weak, can be brute forced	High
Underlying Linux OS	
The following is from SANS Top 10 (Unix):	
Bind (named)	High
RPC	High
Apache (httpd)	High
Unnecessary user accounts, weak, or no password	High
Clear Text Services	High
Sendmail	High
SNMP	High
SSH	High
Misconfiguration of NIS/NFS	High
OpenSSL	High
The following is from the Cert Bulletin (June 9-June 22):	
Squid Cache Buffer Overflow	High
Linux Kernel Vulnerability	High
Syslog-ng not configured for log rotations, etc.	High
Exim buffer overflow	High
NTP not being used for logging synchronization	Med

The following list shows the possible threats and the likelihood of them occurring. However, the values do not indicate any possible impacts, just the likelihood of the threats occurring.

Threats	Value
Environmental	
Fire, flood, or other disaster	Low
Unauthorized access	High
Firewall hardware failure	Low
Operational	
Firewall can be breached (allows traffic through that it should not)	High
Firewall overtaxed (relative to hardware and traffic loads)	Low
DoS attack directed at firewall	Low
Administrator error	High
Unscheduled downtime	High
Attacks being ignored (no one is monitoring the logs).	High
Logs can not be synchronized, so forensic data will be lost.	High
Underlying Linux OS	
Attacker compromises OS	Low
DoS attack directed at OS	Low

In order to calculate the risk associated with each vulnerability/threat pair, the NIST Risk Management Guide[1] was referenced. Each risk value was obtained by multiplying the values for vulnerability, threat, and impact together. The following table shows the values used in the calculation.

	Low	Medium	High
Vulnerability	0.1	0.5	1
Threat	0.1	0.5	1
Impact	10	50	100

The table below displays a matrix of vulnerability, threat, impact, and associated risk. Not every combination of vulnerabilities and threats is valid, so this matrix only shows those pairs that can lead to pernicious outcomes. The assigned values were derived based on the subject environment, and the auditor's experience.

[1] United States. Dept. of Commerce. National Institute of Standards and Technology. Risk Management Guide for Information Technology Systems. Washington: NIST, July 2002. URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Vulnerability	Realizable Threat	Impact	Vulnerability Value	Threat Value	Impact Value	Risk Value	Risk
Lack of Business Continuity plan	Fire, flood, or other disaster	All business functions would be down for a prolonged time.	1.0	0.1	100.0	10.0	Low
Backups not being made			0.1	0.1	100.0	1.0	Low
Physical Access	Unauthorized access	Firewall could be compromised, affecting the confidentiality, integrity, and availability of business critical systems and data.	1.0	1.0	100.0	100.0	High
User accounts with weak passwords			1.0	1.0	100.0	100.0	High
Environmental Controls	Firewall hardware failure	Business applications requiring internet access would be down.	1.0	0.1	50.0	5.0	Low
Hardware fails		The availability of business critical systems and data could be compromised.	1.0	0.1	50.0	5.0	Low
Backups not being made			0.1	0.1	50.0	0.5	Low
Administrator Error	Firewall can be breached (allows traffic through that it should not)	Internal systems could be compromised. This could include both servers and workstations, leading to corruption or loss of data.	1.0	1.0	100.0	100.0	High
Firewall does not behave as expected.			1.0	1.0	100.0	100.0	High
Firewall does not match policy.			1.0	1.0	100.0	100.0	High
Firewall web interface can be brute force attacked.			1.0	1.0	100.0	100.0	High

Vulnerability	Realizable Threat	Impact	Vulnerability Value	Threat Value	Impact Value	Risk Value	Risk
Chosen hardware is underpowered.	Firewall overtaxed (relative to hardware and traffic loads)	Firewall could crash periodically affecting availability of services.	1.0	0.1	50.0	5.0	Low
ACL failure at edge	DoS attack directed at firewall		0.5	0.1	50.0	2.5	Low
Logging not being kept or monitored	Administrator error	Attacks could take place undetected, affecting confidentiality, integrity, and availability of internal systems and data.	1.0	1.0	100.0	100.0	High
Firewall updates not occurring			1.0	1.0	100.0	100.0	High
Backups not being made			0.1	1.0	100.0	10.0	Low
Logging not monitored	Attacks are being ignored (no one is monitoring the logs).		1.0	1.0	100.0	100.0	High
Logs not rotated			1.0	1.0	100.0	100.0	High
Syslog-ng not configured properly			1.0	1.0	100.0	100.0	High
NTP not running	Logs not synchronized, so forensic data will be lost	Getting to root cause of compromises or attacks may be impossible leading to further incidents.	0.5	1.0	50.0	25.0	Med
ACL failure at edge	Attacker compromises OS	Firewall is compromised, leading to attacks and compromising of internal systems affecting confidentiality, integrity, and availability of systems and data.	0.5	0.5	100.0	25.0	Low
Bind			1.0	0.5	100.0	50.0	Med
RPC			1.0	0.5	100.0	50.0	Med
Apache			1.0	0.5	100.0	50.0	Med
User accounts			1.0	0.5	100.0	50.0	Med
Clear text services			1.0	0.5	100.0	50.0	Med
Sendmail			1.0	0.5	100.0	50.0	Med
SNMP			1.0	0.5	100.0	50.0	Med
SSH			1.0	0.5	100.0	50.0	Med
NIS/NFS			1.0	0.5	100.0	50.0	Med
OpenSSL			1.0	0.5	100.0	50.0	Med
Squid			1.0	0.5	100.0	50.0	Med
Linux kernel			1.0	0.5	100.0	50.0	Med

Vulnerability	Realizable Threat	Impact	Vulnerability Value	Threat Value	Impact Value	Risk Value	Risk
Exim	Attacker compromises OS	Firewall is compromised, leading to attacks and compromising of internal systems affecting confidentiality, integrity, and availability of systems and data.	1.0	0.5	100.0	50.0	Med
ACL failure at edge	DoS attack directed at OS	Firewall could crash periodically affecting availability of services.	0.5	0.5	50.0	12.5	Low
Bind			1.0	0.5	50.0	25.0	Low
RPC			1.0	0.5	50.0	25.0	Low
Apache			1.0	0.5	50.0	25.0	Low
User accounts			1.0	0.5	50.0	25.0	Low
Clear text services			1.0	0.5	50.0	25.0	Low
Sendmail			1.0	0.5	50.0	25.0	Low
SNMP			1.0	0.5	50.0	25.0	Low
NIS/NFS			1.0	0.5	50.0	25.0	Low
OpenSSL			1.0	0.5	50.0	25.0	Low
Lack of Change Management procedures	Unscheduled Downtime	Firewall, or a subset of its rules, could impede services that should be allowed to function. This would affect the availability of some or all services through the firewall.	1.0	1.0	50.0	50.0	Med

Current State of Practice

There are many resources available on the Internet that can help in a firewall implementation and audit. Below are listed several of these that were used in preparing and performing this audit.

These are some general sites for systems security:

- NIST – The National Institute for Standards and Technology has a vast collection of "Special Publications" that can be found at http://csrc.nist.gov/publications/nistpubs/index.html. These include several on securing IT systems, in addition to those dealing with security policy and procedure.
- NSA – The National Security Agency has published several guides on securing systems. These can be found at http://www.nsa.gov/snac/.
- CIAC – The Department of Energy maintains an excellent site for its Computer Incident Advisory Capability. Information can be found regarding new vulnerabilities, bulletins, and the like. Their home page is found at http ://ciac.org/ciac/index.html.
- The German Federal Office for Information Security has published a "Baseline Protection Manual" which contains a lot of information about securing common IT platforms. It can be found at http://www.bsi.de/gshb/english/etc/index.htm.

These are some specific sites for auditing:

- OSSTMM – The Institute for Security and Open Methodologies hosts the Open Source Security Testing Methodology Manual written by Pete Herzog. This can be found at http://www.isecom.org/osstmm/.

- ISACA – The Information Systems Audit and Control Association published the IS Auditing Procedure, Firewalls, Document #6, which is a comprehensive checklist for auditing a firewall, and can be found at http://www.isaca.org/standard/procedure7.pdf.

- For this audit, the Astaro Security Linux WebAdmin User Manual was invaluable. The documentation can be found at http://docs.astaro.org/ACM_manuals/.

- Avishai Wool, an assistant professor at Tel Aviv University published an interesting paper describing the ways that firewalls are typically misconfigured. This paper can be found at http://www.eng.tau.ac.il/~yash/computer2004.pdf.

- There are many examples of firewall audits as well. Some are listed below:
  - Auditing Firewalls – Todd Bennett http://www.itsecurity.com/papers/p5.htm
  - Auditing Your Firewall Setup – Lance Spitzner http://www.spitzner.net/audit.html
  - Auditing a Checkpoint Firewall - http://www.giac.org/practical/GSNA/Kevin_Liston_GSNA.pdf
  - Auditing an Internet Firewall from an ISO17799 perspective - http://www.giac.org/practical/GSNA/Richard_Seiersen_GSNA.pdf

More references are mentioned below at each audit step. These include web sites that pertain to specific vulnerabilities, and technical books that address the topics.

Audit Checklist

The following is a subset of the vulnerabilities listed above. They were chosen based on the scope of the audit, and the level of risk and significance.

Vulnerabilities	Reference No:
Physical access	V1
Administrator knowledge and training	V2
Firewall configuration does not match corporate firewall policy.	V3
Firewall management interface (web) passwords weak, can be brute forced	V4
Bind (named)	V5
RPC	V6
Apache (httpd)	V7
Unnecessary user accounts, weak, or no password	V8
Clear Text Services	V9
Sendmail	V10
SNMP	V11
SSH	V12
Misconfiguration of NIS/NFS	V13
OpenSSL	V14
Squid Cache buffer overflow	V15
Linux kernel vulnerability	V16
Syslog-ng not configured for log rotations, etc.	V17
Exim buffer overflow	V18
NTP not being used for logging synchronization	V19

Audit Steps

Hands-Off Phase

While all steps in the audit are technical in nature, these first two steps are administrative and operational. These steps are not actually part of the scope of the audit, but are mentioned here for completeness.

STEP 1:

V1: Verify physical access is controlled

Reference:

- Hansche, Susan, Berti, John, and Hare, Chris. Official (ISC)2 Guide to the CISSP Exam. Boca Raton: Auerbach, 2004. Chapter 7 gives a great overview of what items should exist on a checklist.
- Personal Experience

Risk:

In a computing environment, physical access is tantamount to ownership. Operating systems allow a user with physical access to shutdown and reset the system, gain access to the operating system, and sometimes even reset passwords. Thus, it is imperative to maintain strict procedures for who can access these devices. Moreover, the physical environment must be secured.

Testing and Compliance:

Compliance is based on a checklist including the following:

- Fire suppression
- Surveillance
- Door locks with procedures for handing out and collecting keys
- Door codes with procedures for handing out and changing of codes
- Badge access with procedures for obtaining, activating, and deactivating badges

From physical inspection and interviews, the auditor may find other unique critical items needing attention.

Test Nature:

Subjective

Evidence:

Findings:

STEP 2:

V2: Evaluate administrator knowledge and training level

Reference:

Personal Experience

Risk:

Since many service outages are the result of different types of administrator error, it is critical to ascertain the level of experience and knowledge of the firewall administrator. This shouldn't be taken as a personal affront; it is commonplace for a person to be responsible for many distinct platforms while not being properly trained on all of them. Indeed, it is this auditor's experience, for example, that a truly proficient network engineer might not understand how to manage a Linux firewall.

Compliance/Testing:

This can only be accomplished by interviewing the individual(s) responsible for maintaining the firewall platform. The following is a short list of questions that need to be asked:

- Have you received any training on the firewall platform?
- What is your background in firewall and ACL configuration?
- Who has access to read or modify the firewall configuration?
- What is your current procedure for making changes to the firewall rule set?

    - Is there a procedure for changing the firewall policy before making changes to the firewall?
    - What are the criteria for deciding if the change should be made?
- How often are changes made to the firewall?

Test Nature:

Subjective

Evidence:

Findings:

Hands-On Phase

STEP 3:

Preliminary Work:

The audit steps enumerated below will help ensure the viability of the firewall server platform. However, before going through those steps, it is important to “get a feel” for the server and its related processes, and derive a baseline of information, all of which can be referred back to later.

In order to do this, the following operations will be conducted, and the results will be recorded in the next section.

1. Reboot the server to verify which processes actually start up and run without intervention.
2. ps ax
    - Get a feel for what is running. The results are ephemeral, but it can still give some interesting information.
3. uname -a
    - Which Linux kernel is running?
4. top
    - Which processes seem to be utilizing the most resources? These results are also ephemeral, but again they can yield interesting results.
5. cat /etc/passwd
    - What types of accounts are present?
6. cat /etc/hosts.equiv
    - Are tcp wrappers being used?
7. cat /etc/hosts.allow
    - Are rlogin, rsh, etc. configured?
8. rpm -qa > installed-packages.out
    - Which packages are installed via rpm?

All of this information should give a sense of what the server does.

Next, a baseline scan of the firewall will be obtained from both the outside and the inside that can be referred back to during the audit steps. Tools like nmap and nessus will be used to accomplish this from both the outside and inside interfaces.

From the outside:

```
nmap -sT -O 10.1.0.2
```

This will map the ports in use by the firewall, and try to fingerprint the OS from the outside. An attacker would likely probe similarly. It is important to see what an attacker would see.

From the inside:

```
nmap 10.10.0.1
```

It is necessary to know which ports are open or in use on the inside of the firewall. Nessus will be run, using all applicable plugins. **(Note:** The nessus plugins change frequently, and those applicable to a Linux firewall can be found in several of the plugin categories. Therefore, it is recommended to manually go through all applicable categories and check the individual plugins before starting a scan.)

Evidence:

Findings:

STEP 4:

V3: Firewall configuration doesn't match corporate firewall policy

Reference:

- Netfilter Organization. Documentation found at http://www.netfilter.org/documentation/index.html.
- Jones, Alan. "Netfilter and IPTables – A Structural Examination." GSEC Practical, Feb 2004.
- Nemeth, Snyder, Hein. "Linux Administration Handbook." Prentice Hall PTR, 2002. Pages 679-683
- Zwicky, Simon, and Chapman. "Building Internet Firewalls." 2nd Edition. O'reilly and Associates, June 2000. Page 746

Risk:

After the initial firewall configuration is completed, it is imperative that the rule set be compared with the corporate policy to verify that they match. Furthermore, before any future changes are made to the firewall, the policy needs to be updated. If the firewall rule set does not match the policy, then one of two outcomes will result: either the firewall will be blocking that which it should not, resulting in lack of availability; or, the firewall will not be blocking what it should, risking one or more compromised systems on the inside, which could result in a lack of confidentiality, integrity, and/or availability.

Testing and Compliance:

By issuing the following command, a dump of the firewall configuration is redirected into a text file. The –L (or –list) parameter lists all chains regardless of interface.

```
iptables -L > fwconfig.txt
```

This file can then be compared with the firewall policy line by line to verify that implementation matches policy.

Compliance is based on the output actually matching both what the policy allows and what the policy denies. However, the auditor cannot merely trust the output of the firewall application. He needs to test the firewall policy as well. This can be accomplished by placing an “attacking” PC on the outside, and “victim” and “sniffing” PCs on the inside. The auditor can then test by scanning across the firewall, and then trying to connect to the victim PC on different ports.

The first step will be to probe across the firewall. This will be used as a baseline.

```
nmap -sP 10.10.0.*
```

The auditor will also use hping to craft packets to simulate the following attacks:

- Incoming web traffic (made to look like a response)
- FTP data channel being initiated from the internet
- SMTP traffic sent to mail server
- NTP attacks directed at servers

```
hping 10.10.0.50 -c 1 –SL -s 80 -p 17865 -d 500

hping 10.10.0.50 -c 1 -udp -s 22 -p 17865 -d 500

hping 10.10.0.20 -c 1 -s 25 -p 25 -d 100

hping 10.10.0.20 -c 1 -s 123 -p 123 -d 50
```

Compliance is based on the firewall behaving as the firewall policy dictates.

Test Nature:

Objective

Evidence:

Findings:

STEP 5:

V4 Firewall management interface (web) passwords weak, can be broken

Reference:

- SANS Track 7 Section 7.3 Auditing Web Applications
- Belani, Rohyt. “Basic Web Session Impersonation.” <u>Security Focus</u> 14 April 2004. URL: http://www.securityfocus.com/infocus/1774
- Nikto Web CGI Scanning Tool. URL: http://www.cirt.net/code/nikto.shtml
- Personal experience

Risk:

The web interface is the one portal for configuring all aspects of the firewall. If a brute-force attack were successful, the firewall would then be compromised, which would lead to servers and workstations being compromised. The auditor will focus on the web application here, and delve into the web server application in V7 below.

Testing and Compliance:

Two separate categories of tests need to be performed here. The first is scanning of the web server for cgi vulnerabilities. The second test is to try and brute force attack the login page to verify that strong passwords are being used for the admin account(s). The cgi scanners used for this test are nessus and nikto. These were chosen because of their reputations, ease of use, and functionality. Nessus will be used to check the general configuration of the web server, while nikto will be utilized with its SSL capabilities to delve further. For brute-force attacking the passwords themselves, the auditor can use something like Brutus with stunnel, L0phtcrack, or authforce.

The auditor will concentrate his efforts on the inside interface. He will refer back to the nmap output obtained in step V3 to determine whether an attack from the outside interface is warranted. The auditor will also refer back to the nessus scan made earlier.

Compliance is based on nessus not finding any known vulnerabilities that can be exploited. Only notices, and possibly warnings should result. All of these will be listed with the findings.

Nikto will be used as follows:

```
nikto -h 10.10.0.1 -port 443 -ssl 443 -verbose
```

Compliance is based on nikto not finding any critical vulnerabilities. Anything found will be listed in the findings.

The auditor will forgo the brute force attack on the passwords. This is due to the use of weak passwords in the test environment. However, these passwords need to be changed before moving the firewall into production, and this test should be performed at that time.

Test Nature:

Objective

Evidence:

Findings:

STEP 6:

V5 BIND vulnerabilities

Reference:

- Carnegie Mellon Software Engineering Institute. URL: http://www.cert.org/nav/index_red.html (Advisories and Incidents)
- Internet Software Consortium (writers of BIND). URL: http://www.isc.org/products/BIND/bind-security.html (additional security issues with BIND)
- Nemeth, Snyder, Hein. “Linux Administration Handbook.” Prentice Hall PTR, 2002. Chapter 16.
- SANS Top 10 Unix vulnerabilities. URL: http://www.sans.org/top20/#u1
- Personal experience

Risk:

If the BIND version running contains one of the buffer overflow vulnerabilities, and BIND is being run as root, this can lead to the compromising of the firewall. Thus, the BIND version needs to be ascertained, and whether it is being run as a different user in a chroot()ed jail.

Testing and Compliance:

Determine the version of BIND running:

```
named -v
```

Determine where named runs from, who it runs as, and if it is running from a chroot() directory.

```
ps ax | grep named
grep bin /etc/init.d/named
```

The auditor should also test if other devices can resolve using this server. He can use the attacker laptop with nslookup or dig. Ideally, the server will not respond to these types of requests. This will be done from the inside interface.

The nessus scan will be referred to in order to determine if there were any bind vulnerabilities.

Compliance is based on running version 8.3.7 or later or 8.4.3 or later, and that internal devices cannot connect to our firewall for the purpose of name resolution. Compliance is not necessarily based on chroot() being used, but this is still recommended.

Test Nature:

Objective

Evidence:

Findings:

STEP 7:

V6 RPC vulnerabilities

Reference:

- SANS Top 10 Unix vulnerabilities. URL: http://www.sans.org/top20/#u2
- Garfinkel, Spafford, and Schwartz. "Practical Unix and Internet Security." O'reilly and Associates, February, 2003. Chapters 13 and 15.

Risk:

Many vulnerabilities exist both in the RPC functions themselves, and in those applications that use RPC. If one of these vulnerabilities were combined with a threat, the firewall would be compromised. Moreover, there is no reason for a firewall to run RPC. Its services are not required for the basic functionality. Therefore, it should be verified that RPC is not running.

Testing and Compliance:

To verify that no RPC services are running, the first step is to check the processes that are running using *ps* and *netstat*:

```
ps ax | grep rpc
ps ax | grep portmap
netstat -a | grep portmap
ps ax | grep nfs
```

Next, check that inetd or xinetd don't start RPC services.

```
cat /etc/inetd.conf
ls /etc/xinetd.d/
```

Compliance is based on no rpc services being used or turned on.

Test Nature:

Objective

Evidence:

Findings:

STEP 8:

V7 Apache httpd vulnerabilities

Reference:

- Apache Security (version 1.3). URL: http://www.apacheweek.com/features/security-13
- Apache Security (version 2.0). URL: http://www.apacheweek.com/features/security-20
- SANS Top 10 Unix vulnerabilities. URL: http://www.sans.org/top20/#u3

Risk:

The Astaro firewall uses the Apache web server to run its web interface. If Apache were compromised with a buffer overflow that would drop the attacker into a shell as root, this would lead to the firewall also being compromised. The web application has already been explored for vulnerabilities in V4. Therefore, the auditor will focus on Apache here.

Testing and Compliance:

The first step is to check which version of Apache the Astaro firewall uses:

```
httpd -v
```

The most current version as of this writing is 2.0.50, however, new patch versions come out frequently.

It is also important to know whether httpd is running as root, or as another user.

```
ps axu | grep httpd
```

The next step is to test Apache using the nessus vulnerability scanner. The auditor will enable all Apache plugins.

Compliance is based on running 2.0.50 or later, and/or finding no vulnerabilities. (The reason for this ambiguity is that it is nearly impossible for a vendor to be at the latest version of Apache since new versions come out frequently.) While there is no strict requirement for running httpd as a non-root user, if it is running as root, this will be noted.

Test Nature:

Objective

Evidence:

Findings:

STEP 9:

V8 Unnecessary user accounts, weak, or no password

Reference:

- SANS Top 10 Unix vulnerabilities. URL: http://www.sans.org/top20/#u4
- Garfinkel, Spafford, and Schwartz. "Practical Unix and Internet Security." O'reilly and Associates, February, 2003. Chapter 19.
- Personal experience

Risk:

User accounts that have either default or no passwords are potentially a direct attack vector. Thus, all of the accounts that are not being used should be either disabled or deleted, or if they are required, they should be given strong passwords, and no login access.

Testing and Compliance:

The first step is to verify which accounts are required, and to identify those that need to be locked down.

```
cat /etc/passwd
```

This will also indicate if shadow passwords are being used. If so, the second field in each entry should only have an asterisk (*) or some other character rather than a hash value.

Those accounts that are required but should never be logged in to should be "login disabled" by setting their login shells to /bin/false.

All login accounts should have strong passwords.

The difficult part is determining which accounts are required and which are not. Certain accounts, including uucp and nuucp are almost never used anymore. (UUCP is the Unix to Unix Copy Protocol, and was originally used in dial-up networks to retrieve mail and news.) Furthermore, many accounts that are required for services to run do not require a login. These include bin, sys, daemon, and nobody.

Compliance is based on disabling unnecessary accounts, and verifying passwords comply with rules of strong passwords.

Test Nature:

Objective

Evidence:

Findings:

STEP 10:

V9 Clear text services

Reference:

- SANS Top 10 Unix vulnerabilities. URL: http://www.sans.org/top20/#u5
- Personal Experience

Risk:

Clear text services are a high risk because they send login credentials unencrypted. Thus if someone were sniffing the network using a tool like dsniff, they could obtain the credentials to compromise the firewall and access the internal network. Since this is a firewall, there is no need to run services such as ftp and telnet. All of these types of services can be shut off without affecting the service of the firewall itself.

Testing and Compliance:

Since the auditor has already verified that RPC services are shut off (see V9), the focus will shift to ftp, telnet, http, and smtp. The only service that the firewall may run is the latter, and that only to send notification alerts to the firewall administrators. It just needs to be verified that this is the case.

First, inetd and xinetd must be checked to see if they are running telnet or ftp.

```
grep telnet /etc/inetd.conf
grep disable /etc/xinetd.d/telnet

grep ftp /etc/inetd.conf
grep disable /etc/xinetd.d/ftp
```

Second, it must be verified that these daemons are not running independently of the inet services.

```
ps ax | grep ftp
ps ax | grep telnet
ps ax | grep rexecd
ps ax | grep rlogind
ps ax | grep rshd
```

If any of these tests yielded positive results, the appropriate lines in the inet configuration file(s) need to be commented out, or the daemons disabled directly in the rc.d directory.

As an example, here are two lines from a sample inetd.conf file:

```
ftp stream tcp nowait root /usr/sbin/ftpd ftpd
ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd
```

The first line is without tcp wrapper support, and the second is with tcp wrapper support. In order to disable ftp in this example, just insert a "#" at the beginning of the line to form a comment.

Below is an example from an xinetd implementation.

```
service ftp
{
    disable         = yes
    socket_type     = stream
    wait            = no
    user            = root
    server          = /usr/libexec/ftpd
    server_args     = -l
    groups          = yes
    flags           = REUSE IPv6
}
```

In this example, ftp is disabled from the "disable" line.

In order to test for http, the host will be scanned to verify it is not listening on those ports (80, 8000, 8080, etc.), and the Apache configuration file will be checked directly. The nmap scan performed earlier can be referenced.

```
grep -i listen /etc/httpd.conf
```

If httpd is listening for http in addition to https, this needs to be turned off in the httpd.conf file. (Note that httpd.conf may be located in another location, e.g. /usr/local/httpd/etc.)

Exim needs to be verified that it is configured to only send mail, and not to receive it (see V18 below).

Compliance is based on ftp, telnet, and http not running on this system.

Test Nature:

Objective

Evidence:

Findings:

STEP 11:

V10 Sendmail vulnerabilities

Reference:

- SANS Top 10 Unix vulnerabilities. URL: http://www.sans.org/top20/#u6
- Costales, Bryan and Allman, Eric. "sendmail." O'reilly and Associates, November 1997.

Risk:

The Astaro firewall should not be running sendmail (since it uses exim), but this needs to be verified. If it is running, it can be a source of additional exposures.

Testing and Compliance:

First, it needs to be determined if sendmail is running:

```
ps ax | grep sendmail
```

If sendmail is not running, it needs to be determined whether sendmail is even installed on the firewall.

```
rpm -qa | grep sendmail
find / -name sendmail
```

If it is in fact installed on the server, which version is it?

```
sendmail -d0.1 < /dev/null | grep -i version
```

Compliance is based on sendmail running 8.12.10 or later. Preferably, sendmail would not be installed on the firewall.

Test Nature:

Objective

Evidence:

Findings:

STEP 12

V11 SNMP vulnerabilities

Reference:

- SANS Top 10 Unix vulnerabilities. URL: http://www.sans.org/top20/#u7
- CERT SNMP Advisory. URL: http://www.cert.org/advisories/CA-2002-03.html

Risk:

SNMP agents have become notorious over the last couple of years for being vulnerable to several types of attacks. Many devices use these agents for network management purposes, especially for alerting administrators when certain events occur. The concern here is that these vulnerabilities could be used as an attack vector in order to compromise the firewall.

Testing and Compliance:

Since the Astaro firewall uses SNMP for administrative alerts, it needs to be verified that the firewall isn't listening for SNMP messages, but rather only sending traps periodically. The auditor needs to scan from both interfaces to verify this condition. The nmap scan performed above can be referenced. The nessus scan will also be referenced to determine if default or easily guessed community strings are being used.

It must also be determined if snmp traps are being sent using a default community string. The only way to determine this is to capture the snmp trap packets. A network sniffer such as dsniff can be used for this task.

```
dsniff -n -m -w dsniff.out
```

Compliance is based on the firewall not responding to SNMP queries, and the community strings being something other than the defaults.

Test Nature:

Objective

Evidence:

Findings:

STEP 13:

V12 SSH vulnerabilities

Reference:

- SANS Top 10 Unix vulnerabilities. URL: http://www.sans.org/top20/#u8
- CERT OpenSSH Challenge Response Handling Vulnerability. URL: http://www.cert.org/advisories/CA-2002-18.html
- CERT OpenSSH Buffer Management Vulnerability. URL: http://www.cert.org/advisories/CA-2003-24.html
- OpenSSH Security Page. URL: www.openssh.org/security.html

Risk:

The Astaro firewall uses ssh for administrators to access to the server. Since sshd is running, if it were vulnerable to attack, it would be an easy attack vector to compromise the server. Thus, the risk is high, and it must be ensured that the version running does not have known vulnerabilities.

Testing and Compliance:

The first test is to verify that sshd is running.

```
ps ax | grep sshd
```

Next, the version of ssh needs to verified.

```
ssh -V
```

Affected versions include 2.3.1p1 through 3.3, with newer vulnerabilities in later versions. As of this writing, the current version is 3.7.1p2.

Compliance is based on running sshd version 3.7.1p2 or later. If the firewall is running a vulnerable version, it must be upgraded to a version that includes a fix. In order to ascertain whether the version is free of vulnerabilities, the references above should be checked. Generally, the latest version of OpenSSH is preferred.

Test Nature:

Objective

Evidence:

Findings:

STEP 14:

V13 Misconfiguration of NIS/NFS

Reference:

- SANS Top 10 Unix vulnerabilities. URL: http://www.sans.org/top20/#u9
- Nemeth, Snyder, Hein. "Linux Administration Handbook." Prentice Hall PTR, 2002. Chapters 17 and 18.

Risk:

Many vulnerabilities in these services have come out over the years including buffer overflows, DoS, and weak authentication. Any of these could be targeted and exploited by an internal host. In fact, it could even happen by a misconfigured Unix-like server. Since the firewall has no need to run either of these services, it needs to be verified that they are turned off, and if possible, not even installed on the device.

Testing and Compliance:

Verify that NIS is off:

```
ps ax | grep ypbind
ps ax | grep ypserv
ps ax | grep nscd
```

Verify that NFS is off:

```
ps ax | grep nfsd
```

Compliance is based on neither NFS nor NIS running.

Test Nature:

Objective

Evidence:

Findings:

STEP 15:

V14 OpenSSL vulnerabilities

Reference:

- CERT OpenSSL Multiple Vulnerabilities. URL: http://www.cert.org/advisories/CA-2002-23.html
- OpenSSL Security Advisory. URL: http://www.openssl.org/news/secadv_20040317.txt

Risk:

OpenSSL is a critical component of both the Apache web interface and the ssh interface on the firewall. Therefore, this is yet another vulnerability that could be exploited to compromise the firewall, and it is a risk that must be mitigated.

Testing and Compliance:

Test which version is running:

```
openssl version
```

The current version as of this writing is 0.9.7d.

Compliance is based on running openssl 0.9.7d or later. If the firewall is running a vulnerable version, it must be upgraded to a version that includes a fix. In order to ascertain whether the version is free of vulnerabilities, the references above should be checked. Generally, the latest version of OpenSSL is preferred.

Test Nature:

Objective

Evidence:

Findings:

STEP 16:

V15 Squid cache buffer overflow

Reference:

- CIAC Squid NTLM Buffer Overflow. URL: http://www.ciac.org/ciac/bulletins/o-168.shtml
- Squid Security Advisory. URL: http://www.squid-cache.org/Advisories/SQUID-2004_2.txt

Risk:

The Astaro firewall uses squid for content filtering, and offers the Windows domain authentication function as well. Since this vulnerability exists in the NTLM authentication piece, it becomes imperative to test on the firewall platform. If this feature were enabled on the firewall, it could potentially result in the firewall being compromised.

Testing and Compliance:

The first step is to verify the version of squid running:

```
squid -v
```

If this is a vulnerable version, the next step is to determine if the vulnerable ntlm binary is being used. This can be determined by checking the squid.conf file.

```
find / -name squid.conf
grep ntlm squid.conf
```

Squid version 2.5.STABLE5 and earlier are vulnerable. The squid.conf file needs to be checked for the string 'ntlm_auth'. If it is not being referenced in squid.conf, then the installation is not vulnerable.

Compliance is based on the firewall running neither a vulnerable version of squid nor the ntlm.auth binary.

Test Nature:

Objective

Evidence:

Findings:

STEP 17:

V16 Linux kernel vulnerabilities

Reference:

- Security Focus: Multiple Linux Kernel Vulnerabilities. URL: http://www.securityfocus.com/bid/9985
- CERT Linux Kernel Vulnerability. URL: http://www.kb.cert.org/vuls/id/301156/

Risk:

It goes without saying that if the kernel is vulnerable, at the very least, the firewall could suffer a DoS attack, or it could be compromised altogether. Thus, this becomes a critical issue.

Testing and Compliance:

The only action is to determine which kernel is running:

```
uname -a
```

This issue has been resolved as of the 2.4.23 kernel.

Compliance is based on running a kernel version of 2.4.23 or later.

Test Nature:

Objective

Evidence:

Findings:

STEP 18:

V17 Syslog-ng not configured for log rotations, etc.

Reference:

- Syslog-ng Home Page. URL: http://www.balabit.com/products/syslog_ng/
- Syslog-ng FAQ. URL: http://www.campin.net/syslog-ng/faq.html#compression
- Configuring syslog-ng. URL: http://sial.org/howto/logging/syslog-ng/
- Astaro User manual. URL: http://docs.astaro.org/ACM_manuals/
- Personal experience

Risk:

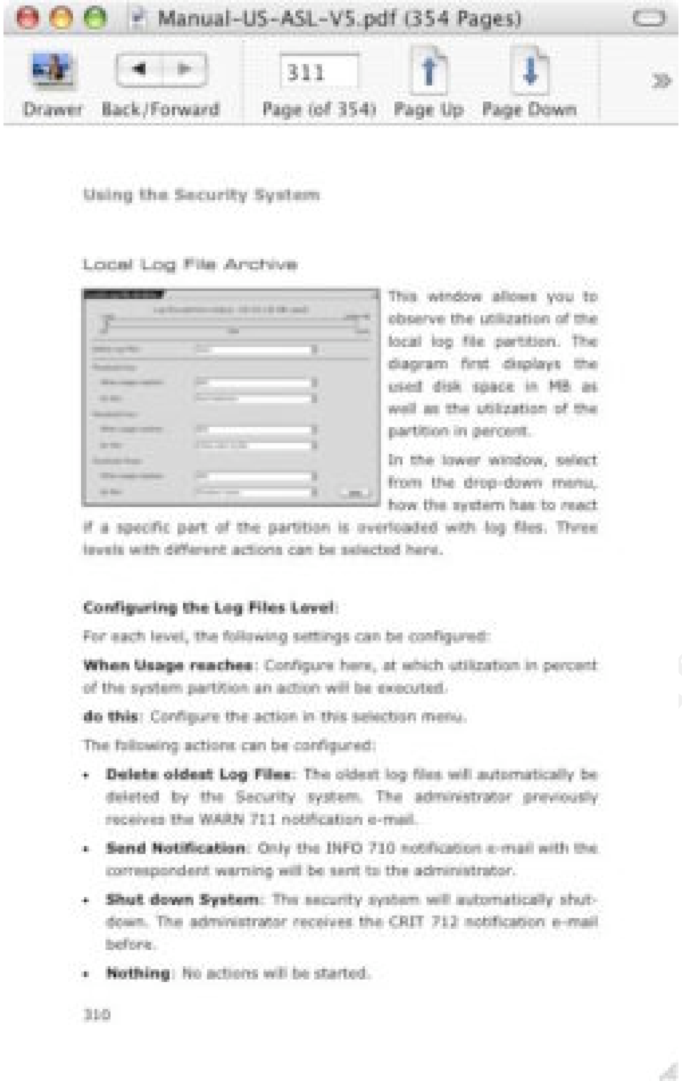
Log rotation is a double-edged sword. On the one hand, as log files get large, they are difficult to manage, extract data from, and can even fill up the file system. On the other hand, if the log rotation overwrites files after a certain period, older logs can get lost.

A good policy is one that keeps the files to 10MB or so, and deposits older log files into a separate file system without overwriting older log files. Since this is a firewall, those old logs are needed; it may be necessary to refer back to them sometime in the future. (Note that 10MB is a general rule of thumb derived from personal experience. Perl and other script languages can take a long time to chug through files much larger than 10MB.)

Testing and Compliance:

Since there are several ways to configure syslog-ng and log rotation in general, it will be necessary to check the GUI to see how logs are configured, and look at the configuration files on the server. This can be documented after the fact.

Check the syslog-ng.conf file. It should have a directive that rotates logs periodically. Also, check the user interface, and see how it is configured.



Using the Security System

Local Log File Archive

This window allows you to observe the utilization of the local log file partition. The diagram first displays the used disk space in MB as well as the utilization of the partition in percent.

In the lower window, select from the drop-down menu, how the system has to react if a specific part of the partition is overloaded with log files. Three levels with different actions can be selected here.

Configuring the Log Files Level:

For each level, the following settings can be configured:

When Usage reaches: Configure here, at which utilization in percent of the system partition an action will be executed.

do this: Configure the action in this selection menu.

The following actions can be configured:

- **Delete oldest Log Files**: The oldest log files will automatically be deleted by the Security system. The administrator previously receives the WARN 711 notification e-mail.
- **Send Notification**: Only the INFO 710 notification e-mail with the correspondent warning will be sent to the administrator.
- **Shut down System**: The security system will automatically shut-down. The administrator receives the CRIT 712 notification e-mail before.
- **Nothing**: No actions will be started.

310

Figure 1 Log rotation section of Astaro manual

Compliance is based on utilizing any means of achieving log rotations and log retention.

Test Nature:

Objective

Evidence:

Findings:

STEP 19:

V18 Exim buffer overflow

Reference:

- Neohapsis Exim Buffer Overflow. URL: http://archives.neohapsis.com/archives/secunia/2004-q2/0284.html

Risk:

The firewall should not be accepting smtp connections from the outside; rather it should only use the mail server to send messages to the administrators. This fact alone limits the exposure of any vulnerabilities in the mail transport agent (mta). However, since this is a firewall server, it is better not to rely solely on the configuration; the firewall should be secure even if the mail application is misconfigured.

Testing and Compliance:

As of version 4.32, the vulnerability has been fixed. Therefore, the first step is to ascertain which version our firewall is running.

```
exim -bV
```

Furthermore, header syntax checking should also be disabled. First, locate the configuration file:

```
find / -name exim.conf
```

Once found, check two lines to see if they have been changed from default values. There are actually two vulnerabilities that have been found in versions prior to 4.32.

```
grep -i sender_verify exim.conf
```

The value should be *false*.

```
grep -i headers_check_syntax exim.conf
```

If the value is *header_syntax,* then this is exploitable.

It also needs to be determined that exim is only configured to send mail, and not to listen for incoming mail. Generally, if it is configured to receive mail, it will with the -*bd* option.

Compliance is based on running exim version 4.32 or later, and that header syntax checking is disabled.

Test Nature:

Objective

Evidence:

Findings:

STEP 20:

V19 NTP not being used for logging synchronization

Reference:

- NTP Man Page
- Astaro User Manual. URL: http://docs.astaro.org/ACM_manuals/

Risk:

Without the use of a time protocol such as ntp, the various log files that are kept on disparate systems that make up the modern data center would not be synchronized. Consequently, it would be very difficult to correlate logs when an incident occurs, or when trying to be proactive.

Testing and Compliance:

The auditor will start by checking to see whether ntp is running on the system:

```
ps ax | grep ntp
```

Next, he will check to see how ntp is configured:

```
cat /etc/ntp.conf
```

At a minimum, the configuration file should include *server* directive(s) to point to upstream time server(s).

If ntp is not running, then cron should be checked to see if ntpdate is being run manually. This can be done by checking the crontab as root:

```
crontab -l
```

Compliance will be based on ntp running (either as a daemon, or out of cron), and configured to synchronize with an outside ntp server.

Test Nature:

Objective

Evidence:

Findings:

Conducting the Audit

STEP 3:

Preliminary Work:

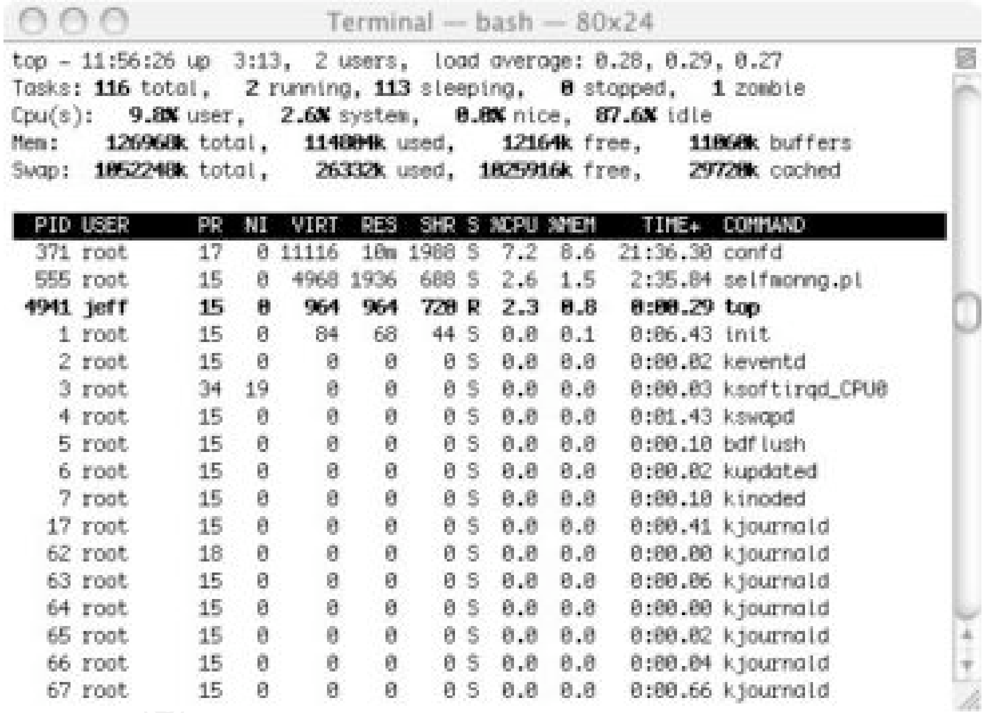
Evidence:

```
jeff@astaro:/home/jeff > ps ax
  PID TTY      STAT   TIME COMMAND
    1 ?        S      0:06 init
    2 ?        SW     0:00 [keventd]
    3 ?        SWN    0:00 [ksoftirqd_CPU0]
    4 ?        SW     0:01 [kswapd]
    5 ?        SW     0:00 [bdflush]
    6 ?        SW     0:00 [kupdated]
    7 ?        SW     0:00 [kinoded]
   17 ?        SW     0:00 [kjournald]
   62 ?        SW     0:00 [kjournald]
   63 ?        SW     0:00 [kjournald]
   64 ?        SW     0:00 [kjournald]
   65 ?        SW     0:00 [kjournald]
   66 ?        SW     0:00 [kjournald]
   67 ?        SW     0:00 [kjournald]
  196 ?        S      0:11 /sbin/syslog-ng -f /etc/syslog-ng.conf
  263 ?        S      0:00 /usr/sbin/cron
  362 ?        S      0:02 /usr/bin/dns_resolver 127.0.0.1:16498 /etc/confd/disp
  363 ?        S      0:01 /usr/local/bin/alicd -L syslog --daemon --loglevel 2
  367 ?        S      0:32 /usr/bin/v4watcher 127.0.0.1:16498 /etc/confd/dispatc
  371 ?        S     21:25 /usr/bin/confd 127.0.0.1:16498 /etc/confd/dispatcher.
  408 ?        S      0:01 /usr/sbin/httpd -f /etc/httpd/httpd.conf
  524 ?        S      1:13 /var/mdw/mdw_daemon.pl
  555 ?        S      2:34 /usr/local/bin/selfmonng.pl
  556 ?        S      0:00 /usr/local/bin/daemon-watcher selfmonng.pl /usr/local
  557 tty1     S      0:00 login -- root
  558 tty2     S      0:00 /sbin/mingetty --no-hostname tty2
  559 tty3     S      0:00 /sbin/mingetty --no-hostname tty3
  560 tty4     S      0:00 /sbin/mingetty --no-hostname tty4
  561 ?        S      0:00 /var/aua/aua.bin /etc/wfe/conf/aua_main_config.ini
  595 tty1     S      0:00 -bash
  604 ?        S      0:00 /usr/sbin/sshd -4 -f /etc/ssh/sshd_config
  756 ?        S      0:00 /bin/logger -t httpd -p local6.notice
  766 ?        S      0:00 /usr/sbin/fcgi- -f /etc/httpd/httpd.conf
  883 ?        S      0:00 /usr/bin/hyperdyper
  .
  .
  .
  944 ?        S      0:00 /usr/bin/hyperdyper
  955 ?        S      0:00 /sbin/squidf -sYD
  962 ?        S      0:01 (squid) -sYD
  968 ?        S      0:00 (unlinkd)
  969 ?        S      0:00 syslogger squid_access
  970 ?        S      0:00 /usr/sbin/localhttpd -f /etc/httpd/httpd-loopback.con
  982 ?        S      0:00 /usr/sbin/localhttpd -f /etc/httpd/httpd-loopback.con
  983 ?        S      0:00 /usr/sbin/localhttpd -f /etc/httpd/httpd-loopback.con
  985 ?        S      0:00 /usr/sbin/localhttpd -f /etc/httpd/httpd-loopback.con
  998 ?        S      0:00 /usr/bin/weed 127.0.0.1:16464 /etc/weed/weed.xml
  999 ?        S      0:00 /usr/bin/weed 127.0.0.1:16464 /etc/weed/weed.xml
 1005 ?        S      0:00 /usr/bin/weed 127.0.0.1:16464 /etc/weed/weed.xml
 2288 ?        S      0:00 /usr/bin/perl /usr/local/bin/sarg-logger.pl -f blocke
 2289 ?        S      0:00 /usr/bin/perl /usr/local/bin/sarg-logger.pl -f access
 2290 ?        S      0:00 /usr/bin/perl /usr/local/bin/reporter/vpn-reporter.pl
 2291 ?        S      0:01 /usr/bin/perl /usr/local/bin/reporter/ips-reporter.pl
 2295 ?        S      0:01 /usr/bin/perl /usr/local/bin/reporter/cfilter-reporte
 2296 ?        S      0:15 /usr/bin/perl /usr/local/bin/reporter/pfilter-reporte
 2297 ?        S      0:00 /usr/bin/perl /usr/local/bin/reporter/socks-reporter.
 2298 ?        S      0:00 /usr/bin/perl /usr/local/bin/reporter/smtp-reporter.p
 2299 ?        S      0:01 /usr/bin/perl /usr/local/bin/reporter/admin-reporter.
 2300 ?        S      0:01 /usr/bin/perl /usr/local/bin/notifier.pl
 2321 ?        S      0:00 /bin/exim -bd -q20m
 4140 ?        Z      0:00 [aua.bin] <defunct>
 4241 ?        S      0:06 /var/wfe/index.fpl
 4511 ?        S      0:33 /usr/sbin/httpd -f /etc/httpd/httpd.conf
 4514 ?        S      0:23 /usr/sbin/httpd -f /etc/httpd/httpd.conf
 4732 ?        S      0:00 /usr/sbin/sshd -4 -f /etc/ssh/sshd_config
 4734 ?        S      0:00 /usr/sbin/sshd -4 -f /etc/ssh/sshd_config
 4735 pts/0    S      0:00 -bash
 4864 pts/0    R      0:00 ps ax
jeff@astaro:/home/jeff >
```

Figure 2 Output from "ps ax"

```
jeff@astaro:/home/jeff > uname -a
Linux astaro.mycompany.com 2.4.21-21503-default #1 Wed May 5 15:40:13 UTC 2004 i686
unknown
```

Figure 3 Output from "uname –a"



```
top - 11:56:26 up  3:13,  2 users,  load average: 0.28, 0.29, 0.27
Tasks: 116 total,   2 running, 113 sleeping,   0 stopped,   1 zombie
Cpu(s):   9.8% user,   2.6% system,   0.0% nice,  87.6% idle
Mem:    126960k total,   114004k used,    12164k free,    11060k buffers
Swap:  1052240k total,    26332k used,  1025916k free,    29720k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
  371 root      17   0 11116  10m 1988 S  7.2  8.6  21:36.30 confd
  555 root      15   0  4968 1936  688 S  2.6  1.5   2:35.04 selfmonng.pl
 4941 jeff      15   0   964  964  720 R  2.3  0.8   0:00.29 top
    1 root      15   0    84   68   44 S  0.0  0.1   0:06.43 init
    2 root      15   0     0    0    0 S  0.0  0.0   0:00.02 keventd
    3 root      34  19     0    0    0 S  0.0  0.0   0:00.03 ksoftirqd_CPU0
    4 root      15   0     0    0    0 S  0.0  0.0   0:01.43 kswapd
    5 root      15   0     0    0    0 S  0.0  0.0   0:00.10 bdflush
    6 root      15   0     0    0    0 S  0.0  0.0   0:00.02 kupdated
    7 root      15   0     0    0    0 S  0.0  0.0   0:00.10 kinoded
   17 root      15   0     0    0    0 S  0.0  0.0   0:00.41 kjournald
   62 root      18   0     0    0    0 S  0.0  0.0   0:00.00 kjournald
   63 root      15   0     0    0    0 S  0.0  0.0   0:00.06 kjournald
   64 root      15   0     0    0    0 S  0.0  0.0   0:00.00 kjournald
   65 root      15   0     0    0    0 S  0.0  0.0   0:00.02 kjournald
   66 root      15   0     0    0    0 S  0.0  0.0   0:00.04 kjournald
   67 root      15   0     0    0    0 S  0.0  0.0   0:00.66 kjournald
```

Figure 4 Output from "top"

```
jeff@astaro:/home/jeff > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
wwwrun:x:30:65534:WWW daemon apache:/var/lib/wwwrun:/bin/bash
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
sshd:x:71:65:SSH daemon:/var/lib/sshd:/bin/false
ntp:x:74:65534:NTP daemon:/var/lib/ntp:/bin/false
loginuser:x:100:100:remote login user:/home/login:/bin/bash
chroot:x:666:666:chroot user:/var:/bin/false
jeff:x:667:100::/home/jeff:/bin/bash
jeff@astaro:/home/jeff >
```

Figure 5 Contents of “/etc/passwd”

```
Output from “cat /etc/hosts.equiv”:

jeff@astaro:/home/jeff > cat /etc/hosts.equiv
#
# hosts.equiv   This file describes the names of the hosts which are
#               to be considered "equivalent", i.e. which are to be
#               trusted enough for allowing rsh(1) commands.
#
# hostname
```

Figure 6 Contents of “/etc/hosts.equiv”

```
jeff@astaro:/home/jeff > cat /etc/hosts.deny
# /etc/hosts.deny
# See `man tcpd? and `man 5 hosts_access? as well as /etc/hosts.allow
# for a detailed description.

http-rman : ALL EXCEPT LOCAL
```

Figure 7 Contents of "/etc/hosts.deny"

```
jeff@astaro:/home/jeff > cat /etc/hosts.allow
# /etc/hosts.allow
# See `man tcpd? and `man 5 hosts_access? for a detailed description
# of /etc/hosts.allow and /etc/hosts.deny.
#
# short overview about daemons and servers that are built with
# tcp_wrappers support:
#
# package name  |       daemon path     |       token
# ----------------------------------------------------------------------------
# ssh, openssh  |  /usr/sbin/sshd       |  sshd, sshd-fwd-x11, sshd-fwd-<port>
# quota         | /usr/sbin/rpc.rquotad |  rquotad
# tftpd         | /usr/sbin/in.tftpd    |  in.tftpd
# portmap       |  /sbin/portmap        |  portmap
#                       The portmapper does not verify against hostnames
#                       to prevent hangs. It only checks non-local addresses.
#
# (kernel nfs server)
# nfs-utils     |  /usr/sbin/rpc.mountd |  mountd
# nfs-utils     |  /sbin/rpc.statd      |  statd
#
# (unfsd, userspace nfs server)
# nfs-server    |  /usr/sbin/rpc.mountd |  rpc.mountd
# nfs-server    |  /usr/sbin/rpc.ugidd  |  rpc.ugidd
#
# (printing services)
# lprng         |  /usr/sbin/lpd        |  lpd
# cups          |  /usr/sbin/cupsd      |  cupsd
#                       The cupsd server daemon reports to the cups
#                        error logs, not to the syslog(3) facility.
#
# All of the other network servers such as samba, apache or X, have their own
# access control scheme that should be used instead.
#
# In addition to the services above, the services that are started on request
# by inetd or xinetd use tcpd to "wrap" the network connection. tcpd uses
# the last component of the server pathname as a token to match a service in
# /etc/hosts.{allow,deny}. See the file /etc/inetd.conf for the token names.
# The following examples work when uncommented:
#
#
# Example 1: Fire up a mail to the admin if a connection to the printer daemon
# has been made from host foo.bar.com, but simply deny all others:
# lpd : foo.bar.com : spawn /bin/echo "%h printer access" | \
#                                mail -s "tcp_wrappers on %H" root
#
#
# Example 2: grant access from local net, reject with message from elsewhere.
# in.telnetd : ALL EXCEPT LOCAL : ALLOW
# in.telnetd : ALL : \
#    twist /bin/echo -e "\n\raccess from %h declined.\n\rGo away.";sleep 2
#
#
# Example 3: run a different instance of rsyncd if the connection comes
#            from network 172.20.0.0/24, but regular for others:
# rsyncd : 172.20.0.0/255.255.255.0 : twist /usr/local/sbin/my_rsyncd-script
# rsyncd : ALL : ALLOW
#


jeff@astaro:/home/jeff >
```

Figure 8 Contents of "/etc/hosts.allow"

```
jeff@astaro:/home/jeff > rpm -qa
filesystem-2002.9.2-5608
glibc-2.2.5-21301
attr-2.4.2-5501
acl-2.0.19-7601
fileutils-4.1.11-10701
ncurses-5.2-40202
readline-4.3-5301
bash-2.05b-5301
fillup-1.10-3201
gdbm-1.8.0-68901
binutils-2.12.90.0.15-5001
bzip2-1.0.2-5101
popt-1.6-35601
zlib-1.1.4-5101
diffutils-2.8.1-4901
e2fsprogs-1.34-38
file-3.37-20601
findutils-4.1.7-43501
gawk-3.1.1-32701
grep-2.5.1-8401
iputils-ss020124-45701
iptables-1.2.9-7
joe-2.9.8-13001
less-376-3101
modutils-2.4.25-5301
net-tools-1.60-45501
nacctd-0.71-4
netcat-1.10-61201
netdiag-20010114-13901
recode-3.6-24001
sash-3.4-50401
sed-3.02.80-5301
devs-2002.10.4-901
sysvinit-2.82-36401
tar-1.13.25-4601
textutils-2.1-3901
```

```
zip-2.3-49001
timezone-2.2.5-21301
terminfo-5.2-40202
gzip-1.3-32601
libgcc-3.2.2-3801
libstdc++-3.2.2-3801
db-4.0.14-19401
iproute2-2.4.7-49501
g3utils-1.1.28-25402
mgetty-1.1.28-25402
cracklib-2.7-71601
pam-0.76-10901
libxcrypt-1.1-5401
sh-utils-2.0-37702
sudo-1.6.6-5101
vlan-1.6-7401
libcap-1.92-22601
perl-5.8.0-11501
perl-XML-Parser-2.31-4001
perl-XML-Simple-1.08-4301
perl-Unix-Syslog-0.98-2601
perl-MIME-Lite-2.117-2601
perl-MIME-Types-0.16-6801
perl-HTML-Tagset-3.03-30001
perl-HTML-Parser-3.26-3901
lilo-22.3.2-5701
gpg-1.0.7-9401
openssl-0.9.6g-11401
heimdal-lib-0.4e-20701
cyrus-sasl-1.5.27-28001
openldap2-client-2.1.4-7001
shadow-4.0.2-36502
vim-6.1-19401
aaa_base-2003.3.27-5504
ash-0.2-64101
util-linux-2.11u-9502
mktemp-1.5-48201
k_deflt-2.4.21-21503
kbd-1.06-16901
openssh-3.4p1-26301
ps-2003.10.7-101
pam-modules-2002.8.29-1201
xntp-4.1.1-28902
rpm-3.0.6-55401
expat-1.95.4-4101
pcre-3.9-13101
libpcap-0.7.1-17601
tcpdump-3.7.1-35101
netcfg-2002.9.4-1301
logrotate-3.5.9-19801
ncftp-3.1.3-5601
cron-3.0.1-83901
hwinfo-5.62-101
gmp-4.0-14901
rrdtool-1.0.39-5701
des-4.04b-51801
rsync-2.5.5-13701
hdparm-5.2-3301
freetype2-2.0.9-8701
libxml2-2.5.11-121
xmlwrapp-0.4.1-13
libxslt-1.0.26-12
apache2-2.0.49-31
syslog-ng-1.6.0rc4-21
ez-ipupdate-3.0-5
perl-Mail-SpamAssassin-2.63-6
spamassassin-2.63-6
smbclient-3.0.1-4
sarg-1.4.1-2
pcmcia-cs-3.2.7-4
wireless_tools-26-1
hostap-0.1.2-2
tools-5.0-8
```

```
chroot-bind-5.0-20
chroot-dhcpc-5.0-20
dhcpcd-1.3.22pl1-12901
chroot-dhcps-5.0-19
dhcp-chroot-server-3.0.1rc9-4301
chroot-http-5.0-21
chroot-ident-5.0-16
chroot-ipsec-5.0-33
chroot-kav-5.0-13
kaspersky-5.0.1.0-19
chroot-pop3-5.0-24
chroot-ppp-5.0-23
chroot-pppoe-5.0-26
chroot-pptp-5.0-20
chroot-pptpc-5.0-18
chroot-smtp-5.0-32
chroot-snmp-5.0-19
net-snmp-5.1-101
chroot-snort-5.0-23
chroot-socks-5.0-16
chroot-squid-2.5-23
chroot-weed-5.0-26
ep-docs-5.0-16
ep-licd-5.0-19
ep-init-texts-5.0-3
ep-libs-5.0-25
ep-wool-1.0-313
ep-confd-1.0-414
ep-confd-helpers-5.0-274
ep-chroot-squid-5.0-25
ep-webadmin-external-helpers-5.0-93
ep-webadmin-helpers-5.0-95
ep-notifier-db-5.0-12
ep-backupconverter-5.0-23
ep-webadmin-pics-5.0-86
ep-webadmin-5.0-113
ep-license-tools-5.0-12
ep-tools-5.0-48
ep-up2date-pattern-5.0-3
ep-hyperdyper-0.1-304
ep-up2date-system-5.0-3
ep-syslog-ng-5.0-38
ep-logging-5.0-45
ep-notifier-5.0-43
ep-reporting-5.0-50
ep-pcmcia-5.0-17
ep-ha-5.0-43
ep-sarg-5.0-4
ep-lcd-5.0-7
ep-webadmin-log-helpers-5.0-7
ep-localpics-5.0-3
ep-chroot-bind-5.0-21
ep-chroot-dhcpc-5.0-17
ep-chroot-dhcps-5.0-17
ep-chroot-ident-5.0-18
ep-chroot-ipsec-5.0-28
ep-chroot-ppp-5.0-20
ep-chroot-pppoe-5.0-24
ep-chroot-pptp-5.0-22
ep-chroot-pptpc-5.0-19
ep-chroot-smtp-5.0-21
ep-chroot-snort-5.0-28
ep-chroot-socks-5.0-17
ep-weed-http-0.3-347
ep-weed-pop3-0.3-347
ep-weed-smtp-0.3-347
ep-up2date-5.0-60
ep-wool-pop3-1.0-324
ep-wool-smtp-1.0-324
ep-wool-weed-1.0-324
ep-mrpopper-1.1-112
ep-capwrapper-1-4
ep-contentfilter-templates-5.0-5
```

```
ep-defaults-5.0-48
ep-defaults-kaspersky-5.0-10
ep-confd-default-config-5.0-3
ep-bootsplash-5.0-6
ep-aua-5.0-36
ep-init-5.0-63
ep-mdw-5.0-103
ep-selfmon-5.0-42
ep-webadmin-lang-us-5.0-88
ep-weed-0.3-347
ep-wool-http-1.0-324
ep-wool-squid-1.0-324
jeff@astaro:/home/jeff >
```

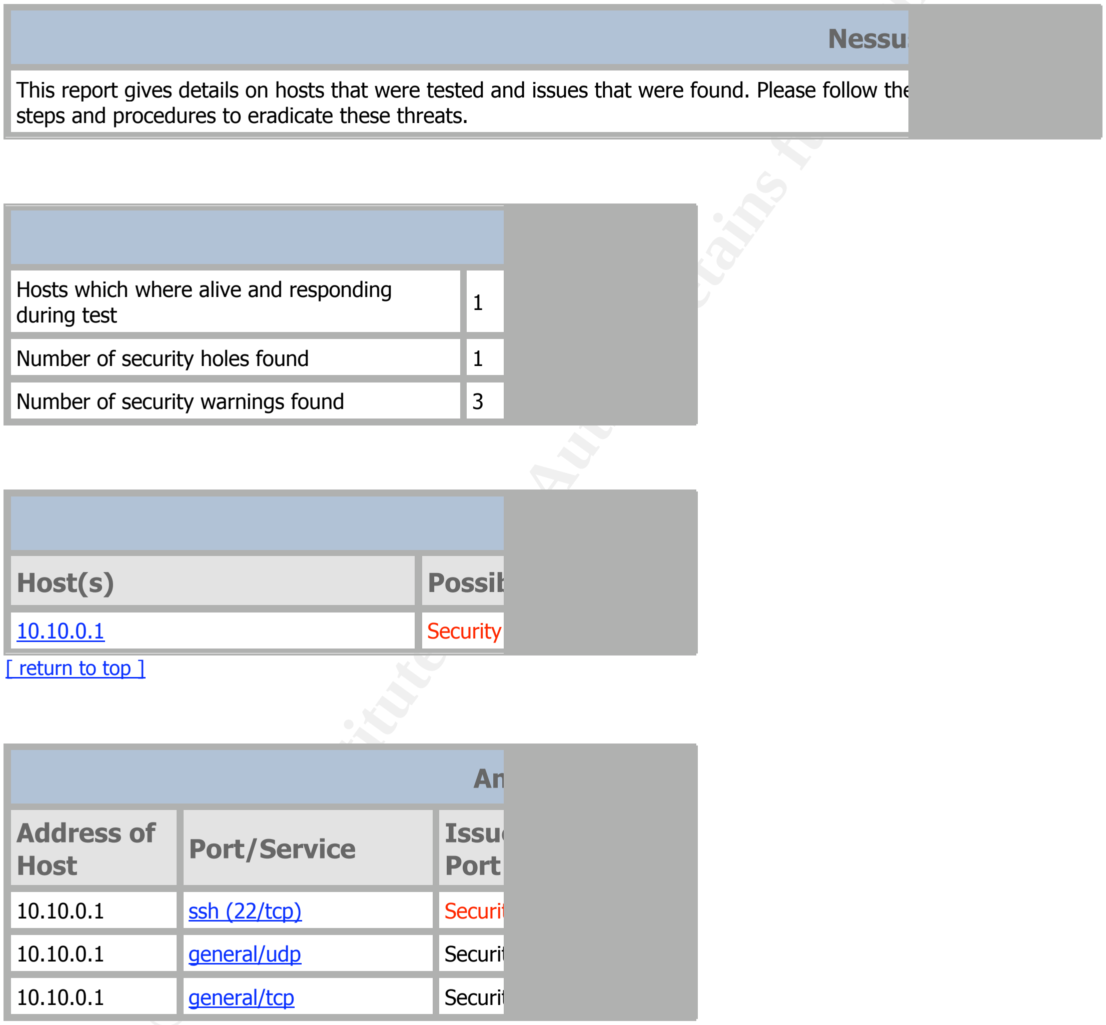
Figure 9 Output from “rpm –qa”

```
$ sudo nmap -sT -O 10.1.0.2

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-09-19 11:57 EDT
Warning:  OS detection will be MUCH less reliable because we did not find at lea
st 1 open and 1 closed TCP port
Interesting ports on 10.1.0.2:
(The 1658 ports scanned but not shown below are in state: filtered)
PORT    STATE SERVICE
443/tcp open  https
Device type: general purpose
Running: Linux 2.4.X
OS details: Linux Kernel 2.4.19 - 2.4.20
Uptime 0.055 days (since Sun Sep 19 10:39:44 2004)

Nmap run completed -- 1 IP address (1 host up) scanned in 76.507 seconds
```

Figure 10 Running “nmap” from the outside

```
$ sudo nmap 10.10.0.1

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-09-19 14:06 EDT
Interesting ports on 10.10.0.1:
(The 1656 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE
22/tcp  open   ssh
53/tcp  closed domain
443/tcp open   https

Nmap run completed -- 1 IP address (1 host up) scanned in 68.881 seconds
```

Figure 11 Running “nmap” from the inside



Nessu

This report gives details on hosts that were tested and issues that were found. Please follow the steps and procedures to eradicate these threats.

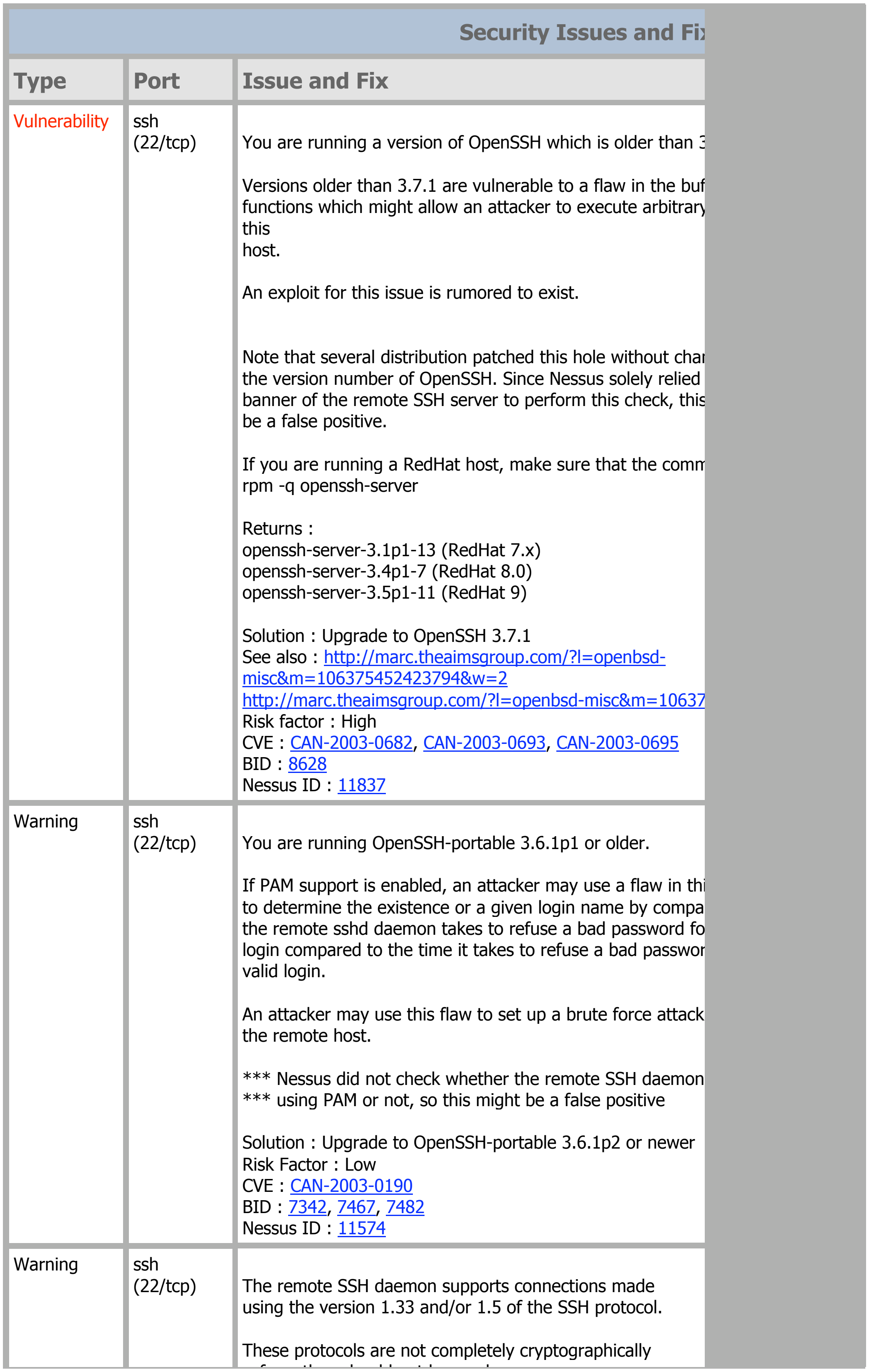
Hosts which where alive and responding during test	1
Number of security holes found	1
Number of security warnings found	3

Host(s)	Possib
10.10.0.1	Security

[return to top]

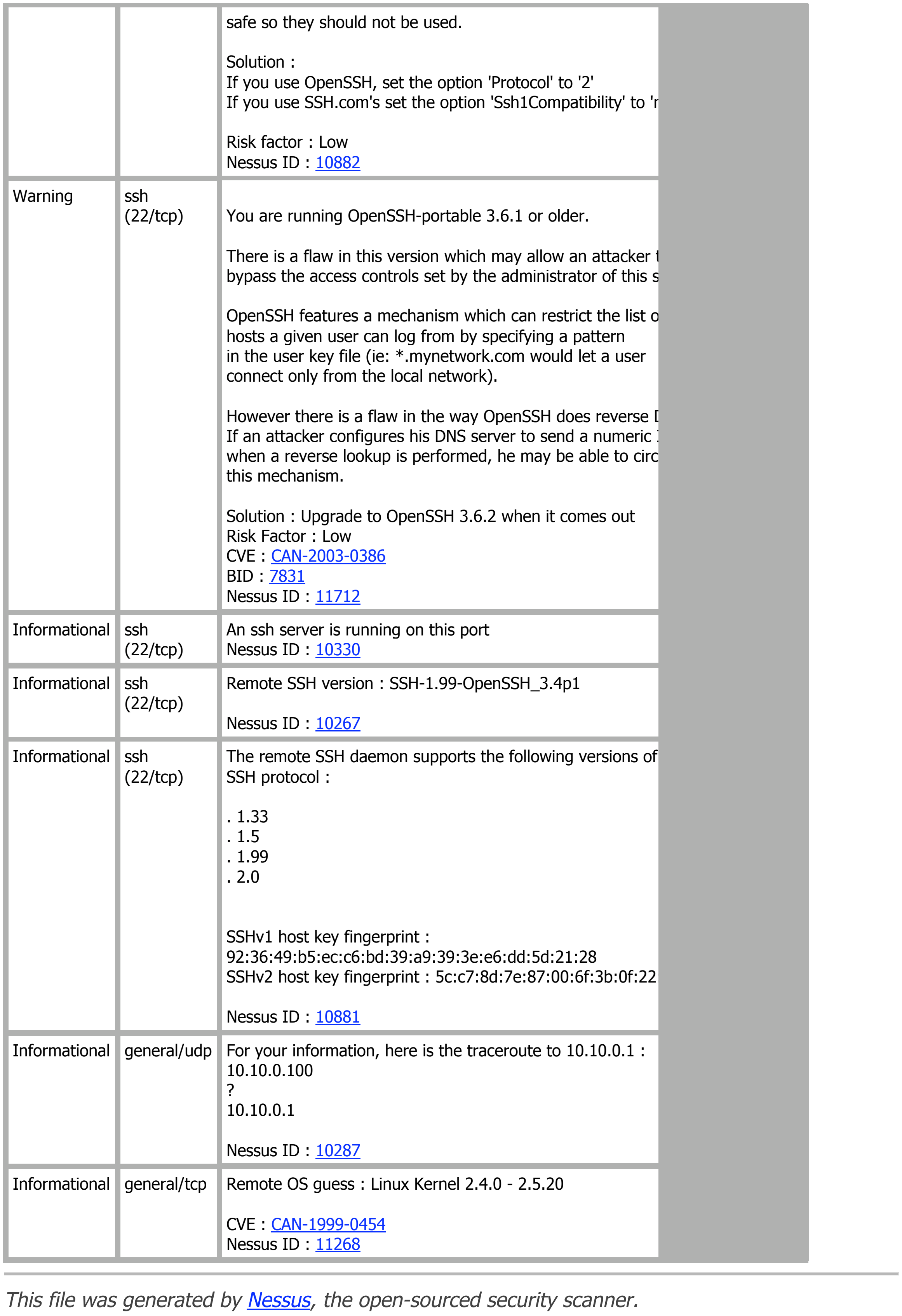
An

Address of Host	Port/Service	Issu Port
10.10.0.1	ssh (22/tcp)	Securi
10.10.0.1	general/udp	Securi
10.10.0.1	general/tcp	Securi



Security Issues and Fi

Type	Port	Issue and Fix
Vulnerability	ssh (22/tcp)	You are running a version of OpenSSH which is older than 3 Versions older than 3.7.1 are vulnerable to a flaw in the buf functions which might allow an attacker to execute arbitrary this host. An exploit for this issue is rumored to exist. Note that several distribution patched this hole without chan the version number of OpenSSH. Since Nessus solely relied banner of the remote SSH server to perform this check, this be a false positive. If you are running a RedHat host, make sure that the comm rpm -q openssh-server Returns : openssh-server-3.1p1-13 (RedHat 7.x) openssh-server-3.4p1-7 (RedHat 8.0) openssh-server-3.5p1-11 (RedHat 9) Solution : Upgrade to OpenSSH 3.7.1 See also : http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375452423794&w=2 http://marc.theaimsgroup.com/?l=openbsd-misc&m=10637 Risk factor : High CVE : CAN-2003-0682, CAN-2003-0693, CAN-2003-0695 BID : 8628 Nessus ID : 11837
Warning	ssh (22/tcp)	You are running OpenSSH-portable 3.6.1p1 or older. If PAM support is enabled, an attacker may use a flaw in thi to determine the existence or a given login name by compa the remote sshd daemon takes to refuse a bad password fo login compared to the time it takes to refuse a bad passwor valid login. An attacker may use this flaw to set up a brute force attack the remote host. *** Nessus did not check whether the remote SSH daemon *** using PAM or not, so this might be a false positive Solution : Upgrade to OpenSSH-portable 3.6.1p2 or newer Risk Factor : Low CVE : CAN-2003-0190 BID : 7342, 7467, 7482 Nessus ID : 11574
Warning	ssh (22/tcp)	The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol. These protocols are not completely cryptographically



		safe so they should not be used. Solution : If you use OpenSSH, set the option 'Protocol' to '2' If you use SSH.com's set the option 'Ssh1Compatibility' to 'r Risk factor : Low Nessus ID : 10882
Warning	ssh (22/tcp)	You are running OpenSSH-portable 3.6.1 or older. There is a flaw in this version which may allow an attacker t bypass the access controls set by the administrator of this s OpenSSH features a mechanism which can restrict the list o hosts a given user can log from by specifying a pattern in the user key file (ie: *.mynetwork.com would let a user connect only from the local network). However there is a flaw in the way OpenSSH does reverse D If an attacker configures his DNS server to send a numeric I when a reverse lookup is performed, he may be able to circ this mechanism. Solution : Upgrade to OpenSSH 3.6.2 when it comes out Risk Factor : Low CVE : CAN-2003-0386 BID : 7831 Nessus ID : 11712
Informational	ssh (22/tcp)	An ssh server is running on this port Nessus ID : 10330
Informational	ssh (22/tcp)	Remote SSH version : SSH-1.99-OpenSSH_3.4p1 Nessus ID : 10267
Informational	ssh (22/tcp)	The remote SSH daemon supports the following versions of SSH protocol : . 1.33 . 1.5 . 1.99 . 2.0 SSHv1 host key fingerprint : 92:36:49:b5:ec:c6:bd:39:a9:39:3e:e6:dd:5d:21:28 SSHv2 host key fingerprint : 5c:c7:8d:7e:87:00:6f:3b:0f:22 Nessus ID : 10881
Informational	general/udp	For your information, here is the traceroute to 10.10.0.1 : 10.10.0.100 ? 10.10.0.1 Nessus ID : 10287
Informational	general/tcp	Remote OS guess : Linux Kernel 2.4.0 - 2.5.20 CVE : CAN-1999-0454 Nessus ID : 11268

This file was generated by Nessus, the open-sourced security scanner.

Figure 12 Results of nessus scan

Findings:
Many packages have been installed in a chroot() environment, and tcp wrappers is installed as well. But the most significant find is an ssh vulnerability found by nessus. This will be expanded upon below.

STEP 4:

V3 Firewall configuration does not match corporate firewall policy

While working with the client, it was learned that no firewall policy exists. The auditor came up with a "boiler-plate" policy that the client could take and customize later. The following list shows the generic firewall policy.

- Ports allowed:
  - Inside network, Outbound: WWW, ICMP echo request, FTP, DNS, NTP (for 2 servers), SMTP (from the mail server)
  - Inside network, Inbound: SMTP (to the mail server)
  - Packet filtering done at edge router:
    - Block Inbound: RFC 1918, Multicast, Bogon, NetBios, SNMP, spoofed private addresses, destination of firewall DMZ interface IP
    - Block Outbound: RFC 1918, NetBios, SNMP, source of firewall DMZ interface IP
- Firewall not accessible to internet (only DMZ interface may have public address)
- Procedures for updating the firewall rules, and moving them into production
- Procedures for updating firewall software

Firewall rules translated to the client's network:

Source	Destination	Ports	Action
10.10.0.128/25	Any	80, 8000, 8080, 443	Allow
10.10.0.128/25	Any	22	Allow
10.10.0.128/25	Any	ICMP Echo request	Allow
10.10.0.128/25	Any	DNS lookup	Allow
10.10.0.128/25	Any	Any	Deny
10.10.0.0/25	Any	123	Allow
10.10.0.20/32	Any	25	Allow
Any	10.10.0.20/32	25	Allow
Any	Any	Any	Deny

Evidence:

```
astaro:/home/jeff # iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
SPOOFING_PROTECTION  all  --  anywhere             anywhere
HA         all  --  anywhere             anywhere
SANITY_CHECKS  all  --  anywhere             anywhere
AUTO_INPUT  all  --  anywhere             anywhere
USR_INPUT  all  --  anywhere             anywhere
LOGDROP    all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
SPOOFING_PROTECTION  all  --  anywhere             anywhere
SANITY_CHECKS  all  --  anywhere             anywhere
AUTO_FORWARD  all  --  anywhere             anywhere
USR_FORWARD  all  --  anywhere             anywhere
LOGDROP    all  --  anywhere             anywhere

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
HA         all  --  anywhere             anywhere
SANITY_CHECKS  all  --  anywhere             anywhere
AUTO_OUTPUT  all  --  anywhere             anywhere
USR_OUTPUT  all  --  anywhere             anywhere
LOGDROP    all  --  anywhere             anywhere

Chain AUTO_FORWARD (1 references)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere

Chain AUTO_INPUT (1 references)
target     prot opt source               destination
ACCEPT     tcp  --  10.10.0.0/24         anywhere            tcp spts:tcpmux:65535
dpt:ssh
LOGDROP    tcp  --  anywhere             anywhere            tcp spts:tcpmux:65535
dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere            tcp spts:1024:65535
dpt:https
LOGDROP    tcp  --  anywhere             anywhere            tcp spts:1024:65535
dpt:https
ACCEPT     tcp  --  10.10.0.0/24         anywhere            tcp spts:domain:65535
dpt:domain
ACCEPT     udp  --  10.10.0.0/24         anywhere            udp spts:domain:65535
dpt:domain
ACCEPT     tcp  --  astaro.mycompany.com  anywhere            tcp spts:tcpmux:65535
dpt:http-alt
ACCEPT     icmp --  anywhere             anywhere
```

```
LOGDROP    tcp  --  anywhere             anywhere            tcp spts:tcpmux:65535
dpt:smtp
ACCEPT     udp  --  10.10.0.10           anywhere            udp spts:1024:65535 dpt:snmp

Chain AUTO_OUTPUT (1 references)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             10.1.0.10           tcp spts:domain:65535
dpt:domain OWNER CMD match named
ACCEPT     udp  --  anywhere             10.1.0.10           OWNER CMD match named udp
spts:domain:65535 dpt:domain
ACCEPT     tcp  --  anywhere             anywhere            tcp spts:1024:65535 dpt:http
OWNER CMD match squidf
ACCEPT     tcp  --  anywhere             anywhere            tcp spts:1024:65535 dpt:http
OWNER CMD match hyperdyper
ACCEPT     tcp  --  anywhere             anywhere            tcp spts:1024:65535
dpt:https OWNER CMD match squidf
ACCEPT     tcp  --  anywhere             anywhere            tcp spts:1024:65535
dpt:https OWNER CMD match hyperdyper
ACCEPT     tcp  --  anywhere             anywhere            tcp spts:1024:65535 dpt:ftp
OWNER CMD match squidf
ACCEPT     tcp  --  anywhere             anywhere            tcp spts:1024:65535 dpt:ftp
OWNER CMD match hyperdyper
ACCEPT     tcp  --  anywhere             anywhere            tcp spts:1024:65535
dpt:http-alt OWNER CMD match squidf
ACCEPT     tcp  --  anywhere             anywhere            tcp spts:1024:65535
dpt:http-alt OWNER CMD match hyperdyper
ACCEPT     tcp  --  anywhere             anywhere            tcp spts:1024:65535 dpt:ldap
OWNER CMD match squidf
ACCEPT     tcp  --  anywhere             anywhere            tcp spts:1024:65535 dpt:ldap
OWNER CMD match hyperdyper
ACCEPT     tcp  --  anywhere             anywhere            tcp spts:1024:65535 dpt:x11
OWNER CMD match weed
ACCEPT     udp  --  anywhere             anywhere            OWNER CMD match net
select udp spts:1024:65535 dpts:33000:34000
ACCEPT     icmp --  anywhere             anywhere            icmp type 8 code 0
ACCEPT     tcp  --  anywhere             anywhere            tcp spts:tcpmux:65535
dpt:smtp OWNER CMD match exim
ACCEPT     udp  --  anywhere             astaro.mycompany.com OWNER CMD match syslog-ng
udp spts:1024:65535 dpt:syslog
ACCEPT     tcp  --  anywhere             anywhere            tcp spts:tcpmux:65535
dpt:https OWNER CMD match aus
ACCEPT     tcp  --  anywhere             anywhere            tcp spts:tcpmux:65535
dpt:http OWNER CMD match aus
ACCEPT     tcp  --  anywhere             anywhere            tcp spts:tcpmux:65535
dpt:https OWNER CMD match pattern_aus
ACCEPT     tcp  --  anywhere             anywhere            tcp spts:tcpmux:65535
dpt:http OWNER CMD match pattern_aus
ACCEPT     udp  --  anywhere             anywhere            OWNER CMD match net
select udp spts:1024:65535 dpts:33000:34000
ACCEPT     udp  --  anywhere             10.1.0.10           udp spts:1024:65535 dpt:ntp

Chain HA (2 references)
target     prot opt source               destination

Chain INVALID_PKT (0 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere            LOG level info prefix
`INVALID_PKT: '
DROP       all  --  anywhere             anywhere

Chain LOGACCEPT (0 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere            LOG level info prefix
`ACCEPT: '
ACCEPT     all  --  anywhere             anywhere

Chain LOGDROP (6 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere            LOG level info prefix `DROP:
'
DROP       all  --  anywhere             anywhere

Chain LOGREJECT (1 references)
```

```
target     prot opt source               destination
LOG        all  --  anywhere             anywhere            LOG level info prefix
`REJECT: '
REJECT     all  --  anywhere             anywhere            reject-with icmp-port-
unreachable

Chain SANITY_CHECKS (3 references)
target     prot opt source               destination
SYNRATE_LIMIT  tcp  --  anywhere             anywhere            tcp
flags:SYN,RST,ACK/SYN
SYNRATE_LIMIT  udp  --  anywhere             anywhere

Chain SPOOFING_PROTECTION (2 references)
target     prot opt source               destination
SPOOF_DROP  all  --  astaro.mycompany.com  anywhere
SPOOF_DROP  all  --  10.1.0.0/24          anywhere
SPOOF_DROP  all  --  astaro.mycompany.com  anywhere
SPOOF_DROP  all  --  10.10.0.0/24         anywhere

Chain SPOOF_DROP (4 references)
target     prot opt source               destination
LOG        all  --  anywhere             anywhere            LOG level info prefix `IP-
SPOOFING DROP: '
DROP       all  --  anywhere             anywhere

Chain STRICT_TCP_STATE (0 references)
target     prot opt source               destination

Chain SYNRATE_LIMIT (2 references)
target     prot opt source               destination
RETURN     tcp  --  anywhere             anywhere            limit: avg 100/sec burst 30
mode srcip-dstip htable-size 0 htable-max 0 htable-gcinterval 1000 htable-expire 10000
RETURN     udp  --  anywhere             anywhere            limit: avg 100/sec burst 30
mode srcip-dstip htable-size 0 htable-max 0 htable-gcinterval 1000 htable-expire 10000
LOG        tcp  --  anywhere             anywhere            LOG level info prefix
`SYNRATE_LIMIT: '
LOG        udp  --  anywhere             anywhere            LOG level info prefix
`SYNRATE_LIMIT: '
DROP       tcp  --  anywhere             anywhere
DROP       udp  --  anywhere             anywhere

Chain USR_FORWARD (1 references)
target     prot opt source               destination
ACCEPT     tcp  --  10.10.0.128/25       anywhere            tcp spts:1024:65535 dpt:http
ACCEPT     tcp  --  10.10.0.128/25       anywhere            tcp spts:1024:65535
dpt:irdmi
ACCEPT     tcp  --  10.10.0.128/25       anywhere            tcp spts:1024:65535
dpt:http-alt
ACCEPT     tcp  --  10.10.0.128/25       anywhere            tcp spts:1024:65535
dpt:https
ACCEPT     tcp  --  10.10.0.128/25       anywhere            tcp spts:1024:65535
dpts:ftp-data:ftp
ACCEPT     tcp  --  10.10.0.128/25       anywhere            tcp spts:tcpmux:65535
dpt:domain
ACCEPT     udp  --  10.10.0.128/25       anywhere            udp spts:tcpmux:65535
dpt:domain
ACCEPT     icmp --  10.10.0.128/25       anywhere            icmp type 8 code 0
REJECT     all  --  10.10.0.128/25       anywhere            reject-with icmp-port-
unreachable
ACCEPT     udp  --  10.10.0.10           anywhere            udp spt:ntp dpt:ntp
ACCEPT     udp  --  10.10.0.20           anywhere            udp spt:ntp dpt:ntp
ACCEPT     tcp  --  anywhere             10.10.0.20          tcp spts:tcpmux:65535
dpt:smtp
ACCEPT     icmp --  anywhere             anywhere            icmp type 0 code 0
LOGREJECT  icmp --  anywhere             anywhere            icmp type 0 code 0

Chain USR_INPUT (1 references)
target     prot opt source               destination

Chain USR_OUTPUT (1 references)
target     prot opt source               destination
astaro:/home/jeff #
```

Figure 13 Output from IPTables

The firewall rules that were entered appear under the USR_FORWARD chain. These do match the basic policy outlined in the table above. The rules for managing the firewall via ssh, https, and snmp can be found under the AUTO_INPUT rule. It is also apparent that in addition to the firewall rules that were entered, the firewall has its own default settings, like controlling tcp syn rates, not allowing spoofed addresses, and settings for logging.

```
$ sudo nmap -sP 10.10.0.*

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-09-19 12:08 EDT
Host 10.10.0.1 appears to be up.
Nmap run completed -- 256 IP addresses (1 host up) scanned in 6.662 seconds
```

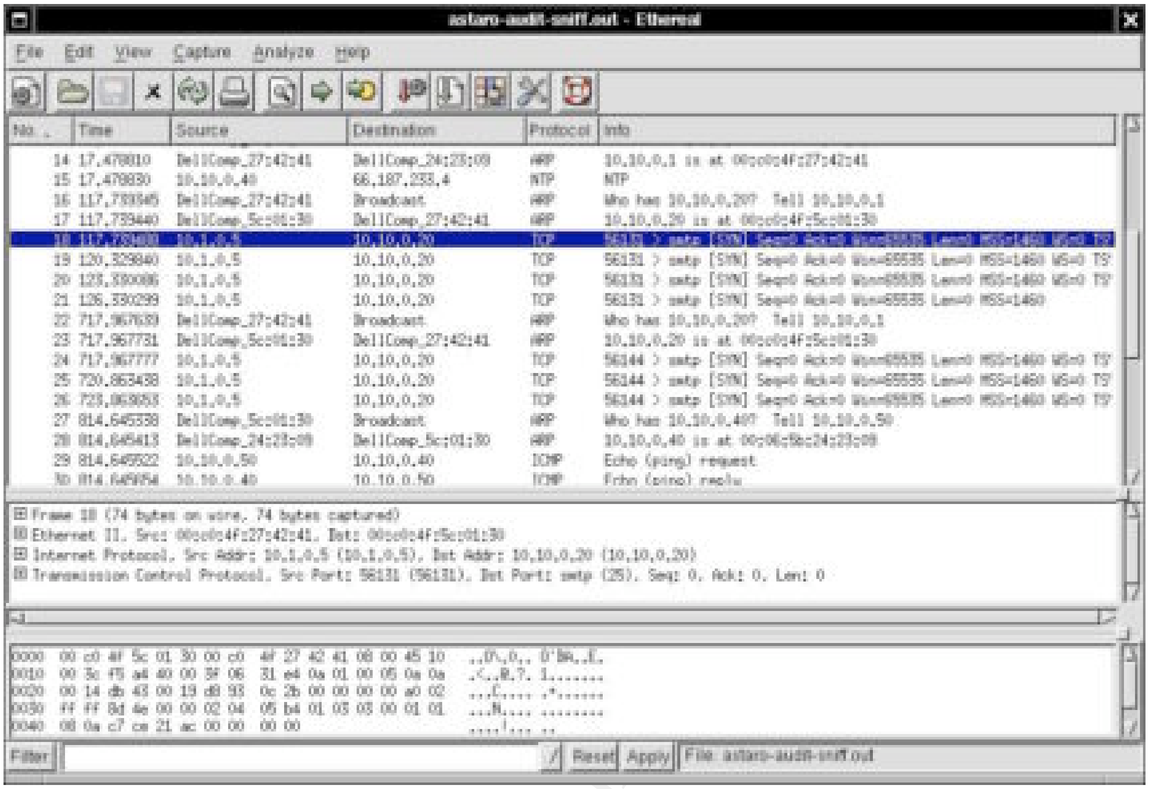
Figure 14 Output from nmap probe of the inside network from the outside

This scan reveals little information, which indicates that the firewall is doing its job.

```
$ sudo hping 10.10.0.50 -c 1 -j -V -s 80 -p 17865 -d
 500
using en0, addr: 10.1.0.5, MTU: 1500
HPING 10.10.0.50 (en0 10.10.0.50): NO FLAGS are set, 40 headers + 500 data bytes

--- 10.10.0.50 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms


$ sudo hping 10.10.0.20 -c 1 -j -V -s 25 -p 25 -d 50
0
using en0, addr: 10.1.0.5, MTU: 1500
HPING 10.10.0.20 (en0 10.10.0.20): NO FLAGS are set, 40 headers + 500 data bytes

--- 10.10.0.20 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Figure 15 Output from hping

It is not clear whether these packets actually got through or not. True, there was no response, but that does not tell the entire story. Below is a portion of the packet capture which shows that the smtp packets did go through. However, the other hping attempts do not show up on the sniff. Therefore, the firewall seems to be acting as it is expected to.


astaro-audit-sniff.out - Ethereal
File
Edit
View
Capture
Analyze
Help
Filter
Reset
Apply
File: astaro-audit-sniff.out

```
No. .  Time        Source              Destination         Protocol  Info
    14 17.478810   DellComp_27:42:41   DellComp_24:23:09   ARP       10.10.0.1 is at 00:c0:4f:27:42:41
    15 17.478830   10.10.0.40          66.187.233.4        NTP       NTP
    16 117.739345  DellComp_27:42:41   Broadcast           ARP       Who has 10.10.0.20?  Tell 10.10.0.1
    17 117.739440  DellComp_5c:01:30   DellComp_27:42:41   ARP       10.10.0.20 is at 00:c0:4f:5c:01:30
    18 117.739488  10.1.0.5            10.10.0.20          TCP       56131 > smtp [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460 WS=0 TS
    19 120.329840  10.1.0.5            10.10.0.20          TCP       56131 > smtp [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460 WS=0 TS
    20 123.330086  10.1.0.5            10.10.0.20          TCP       56131 > smtp [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460 WS=0 TS
    21 126.330299  10.1.0.5            10.10.0.20          TCP       56131 > smtp [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
    22 717.967639  DellComp_27:42:41   Broadcast           ARP       Who has 10.10.0.20?  Tell 10.10.0.1
    23 717.967731  DellComp_5c:01:30   DellComp_27:42:41   ARP       10.10.0.20 is at 00:c0:4f:5c:01:30
    24 717.967777  10.1.0.5            10.10.0.20          TCP       56144 > smtp [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460 WS=0 TS
    25 720.863438  10.1.0.5            10.10.0.20          TCP       56144 > smtp [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460 WS=0 TS
    26 723.863853  10.1.0.5            10.10.0.20          TCP       56144 > smtp [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460 WS=0 TS
    27 814.645338  DellComp_5c:01:30   Broadcast           ARP       Who has 10.10.0.40?  Tell 10.10.0.50
    28 814.645413  DellComp_24:23:09   DellComp_5c:01:30   ARP       10.10.0.40 is at 00:06:5b:24:23:09
    29 814.645522  10.10.0.50          10.10.0.40          ICMP      Echo (ping) request
    30 814.645854  10.10.0.40          10.10.0.50          ICMP      Echo (ping) reply

⊞ Frame 18 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: 00:c0:4f:27:42:41, Dst: 00:c0:4f:5c:01:30
⊞ Internet Protocol, Src Addr: 10.1.0.5 (10.1.0.5), Dst Addr: 10.10.0.20 (10.10.0.20)
⊞ Transmission Control Protocol, Src Port: 56131 (56131), Dst Port: smtp (25), Seq: 0, Ack: 0, Len: 0

0000  00 c0 4f 5c 01 30 00 c0  4f 27 42 41 08 00 45 10   ..O\.0.. O'BA..E.
0010  00 3c f5 a4 40 00 3f 06  31 e4 0a 01 00 05 0a 0a   .<..@.?. 1.......
0020  00 14 db 43 00 19 d8 93  0c 2b 00 00 00 00 a0 02   ...C.... .+......
0030  ff ff 8d 4e 00 00 02 04  05 b4 01 03 03 00 01 01   ...N.... ........
0040  08 0a c7 ce 21 ac 00 00  00 00                     ....!... ..
```

Figure 16 Ethereal packet capture

Findings:
The output from iptables indicates that the firewall is configured correctly. However, this had to be tested empirically as well. The output from nmap and hping, correlated with our sniffing box running ethereal proves that at least for the tests that were run, the firewall is behaving as expected.

Referring back to the nmap scan ran above, the web interface is listening on both Ethernet interfaces. This should be shut off on the external interface. The Astaro firewall web interface provides a method for doing just that. It also provides a feature to block an IP that tries to brute force attack the password to login.

PASS

STEP 5:

V4 Firewall management interface

Evidence:

```
---------------------------------------------------------------------------
- Nikto 1.32/1.27     -     www.cirt.net
V: - Testing open ports for web servers
V: - Checking for HTTP on port 10.10.0.1:443
V: - Checking for HTTPS on port 10.10.0.1:443
+ Target IP:       10.10.0.1
+ Target Hostname: 10.10.0.1
+ Target Port:     443
---------------------------------------------------------------------------
+ SSL Info:        Ciphers: EDH-RSA-DES-CBC3-SHA
                   Info:    /C=DE/ST=BW/L=Karlsruhe/O=Astaro AG/CN=firewall.doma
```

```
in.example/emailAddress=firewall@domain.example
                   Subject: /C=DE/ST=BW/L=Karlsruhe/O=Astaro AG/CN=firewall.doma
in.example/emailAddress=firewall@domain.example
+ Start Time:      Sun Sep 19 13:15:55 2004
---------------------------------------------------------------------------
- Scan is dependent on "Server" string which can be faked, use -g to override
+ Server: Apache
+ No CGI Directories found (use '-C all' to force check all possible dirs)
V: - Checking for CGI in:
V: - Server category identified as 'apache', if this is not correct please use -
g to force a generic scan.
V: - 1832 server checks loaded
V: - 200 for GET:       /
.
.
.
V: - 404 for GET:       /zentrack/index.php
+ 1832 items checked - 1 item(s) found on remote host(s)
+ End Time:        Sun Sep 19 13:22:04 2004 (369 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure 17 Output from nikto

Findings:
As mentioned above, the brute force attack against the administrator's password was not attempted. This step is critical, and needs to be performed later. That being said, the output from nikto showed no vulnerabilities or issues with the web application.

As mentioned above, the firewall web interface is accessible via the outside interface (refer to figure 10 above). This needs to be turned off in the firewall configuration.

PASS

STEP 6:

V5 Bind

Evidence:

The bind binary, named, was not found in a usual location (/sbin, or /usr/sbin). It appears that it has been placed in a chroot()ed jail.

```
jeff@astaro:/home/jeff > /var/chroot-bind/usr/sbin/named -v
named 8.4.4 Wed Mar 31 18:47:49 CEST 2004
```

Figure 18 Output from named –V

The firewall is running bind 8.4.4.

```
jeff@astaro:/home/jeff > ps ax | grep named
 4763 pts/0    R      0:00 grep named
jeff@astaro:/home/jeff >
```

Figure 19 Is bind running?

Named is not running, but found in /var/chroot-bind/usr/bin/named

Furthermore, when nslookup was pointed to use the firewall as its server, it just times out. This is confirmed by the nmap output above, which shows that the port was closed (see figure 11).
In addition, nessus found no vulnerabilities (see figure 12 above.)

Findings:
The firewall is running BIND version 8.4.4, which is a compliant version in the version 8 code train.

PASS

Step 8:

V7 Apache

Evidence:

```
jeff@astaro:/home/jeff > /usr/sbin/httpd -v
Server version: Apache/2.0.49
```

Figure 20 Apache version

```
jeff@astaro:/home/jeff > ps -axu | grep http
root       408  0.0  0.1  5300  240 ?        S    08:43   0:01 /usr/sbin/httpd -f
/etc/httpd/httpd.conf
wwwrun     766  0.0  0.3  5300  436 ?        S    08:44   0:00 /usr/sbin/fcgi- -f
/etc/httpd/httpd.conf
root       970  0.0  0.0  5184   92 ?        S    08:44   0:00 /usr/sbin/localhttpd -f
/etc/httpd/httpd-loopback.conf
wwwrun     982  0.0  0.0  5196    4 ?        S    08:44   0:00 /usr/sbin/localhttpd -f
/etc/httpd/httpd-loopback.conf
wwwrun     983  0.0  0.0  5196    4 ?        S    08:44   0:00 /usr/sbin/localhttpd -f
/etc/httpd/httpd-loopback.conf
wwwrun     985  0.0  0.0  5196    4 ?        S    08:44   0:00 /usr/sbin/localhttpd -f
/etc/httpd/httpd-loopback.conf
wwwrun    4511  0.8  1.9  5544 2428 ?        S    11:22   0:34 /usr/sbin/httpd -f
/etc/httpd/httpd.conf
wwwrun    4514  0.5  1.8  5544 2400 ?        S    11:23   0:24 /usr/sbin/httpd -f
/etc/httpd/httpd.conf
jeff      5365  0.0  0.3  1364  484 pts/0    S    12:31   0:00 grep http
--
jeff@astaro:/home/jeff >
```

Figure 21 httpd processes

The web server seems to be running as the user “wwwrun” (the important thing is that this is **not** root). Note that the “httpd” binary and “localhttpd” file are the same; the latter is merely a soft link to the former.

Findings
The firewall is not running the latest version of Apache, but no vulnerabilities were found. Still, the firewall should be brought up to the latest patch level.

PASS

Step 13:

V12 SSH

Evidence:

```
604 ?        S      0:00 /usr/sbin/sshd -4 -f /etc/ssh/sshd_config
4732 ?        S      0:00 /usr/sbin/sshd -4 -f /etc/ssh/sshd_config
4734 ?        S      0:00 /usr/sbin/sshd -4 -f /etc/ssh/sshd_config
```

Figure 22 sshd is running

```
jeff@astaro:/home/jeff > /usr/sbin/sshd -V
sshd: option requires an argument -- V
sshd version OpenSSH_3.4p1
Usage: sshd [options]
Options:
  -f file    Configuration file (default /etc/ssh/sshd_config)
  -d         Debugging mode (multiple -d means more debugging)
```

Figure 23 Version of sshd

Findings:
As shown above, nessus found that our version of ssh has a known vulnerability, and a possible exploit. This needs to be updated before the firewall can be ready for production.

FAIL

STEP 15:

V14 OpenSSL

Evidence:

```
openssl-0.9.6g-11401
```

Figure 24 openssl version taken from the rpm package

```
jeff@astaro:/home/jeff > /usr/bin/openssl version
OpenSSL 0.9.6g [engine] 9 Aug 2002
```

Figure 25 openssl version found directly

The same results were obtained by looking at the rpm packages (figure 9 above), and from running openssl directly.

Findings:
The version running is not the current version of 0.9.7d. This should be upgraded, and the latest firewall patch may accomplish this.

FAIL

STEP 16:

V15 Squid cache

Evidence:

```
chroot-squid-2.5-23
```

Figure 26 Version of squid found from rpm package

```
jeff@astaro:/home/jeff > /var/storage/chroot-squid/sbin/squidf -v
Squid Cache: Version 2.5.STABLE4
configure options:  --prefix=/
jeff@astaro:/home/jeff >
```

Figure 27 Version of squid found by asking

```
$ grep ntlm squid.conf
#       Specify the command for the external ntlm authenticator.
#       and replies with the ntlm CHALLENGE, then waits for the
#       If you use an ntlm authenticator, make sure you have 1 acl
#       of type proxy_auth.  By default, the ntlm authenticator_program
#       auth_param ntlm program //bin/ntlm_auth
#       auth_param ntlm children 5
#       The maximum number of times a challenge given by a ntlm
#       caching) See max_ntlm_challenge_lifetime for more information.
#       auth_param ntlm max_challenge_reuses 0
#       The maximum time period that a ntlm challenge is reused
#       auth_param ntlm max_challenge_lifetime 2 minutes
#auth_param ntlm program <uncomment and complete this line to activate>
#auth_param ntlm children 5
#auth_param ntlm max_challenge_reuses 0
#auth_param ntlm max_challenge_lifetime 2 minutes
```

Figure 28 Checking for ntlm support in squid.conf

Findings:
The firewall is running a vulnerable version of squid, but ntlm support is not activated. The firewall should be updated to the latest patch level. If NT authentication is enabled in the content filter feature, this will need to be revisited.

PASS

STEP 17:

V16 Linux kernel

Evidence:

The firewall is running the 2.4.21 kernel. This is taken from figure 3 above.

Findings:
This is an older version of the kernel, and needs to be upgraded to the 2.4.23 kernel. Again, by updating the firewall to the latest patch level, the kernel may be updated as well.

FAIL

STEP 18:

V17 Log rotation

Evidence:

```
jeff@astaro:/home/jeff > cat /etc/syslog-ng.conf
###############################################################
# syslog-ng config file - asl customized                      #
#                                                             #
# This file is auto-generated. Edit the configuration file or #
# the template and re-run the template parsing engine.        #
#                                                             #
# Generated on: Wed Sep 29 13:54:40 2004                      #
###############################################################



########################################
# global section
########################################
options {
        group("log");
        log_fifo_size(1000);
        long_hostnames(off);
        owner("root");
        perm(0640);
        stats(43200);
        sync(0);
};

########################################
# section 1: astaro.mycompany.com
########################################
source s_local_asl { unix-dgram("/dev/log"); internal(); pipe("/proc/kmsg" log_p
refix("kernel: "));
         unix-stream("/var/chroot-dhcps/dev/log"); unix-stream("/var/chroot-dhcp
c/dev/log");
         unix-stream("/var/chroot-ipsec/dev/log"); unix-stream("/var/chroot-pop3
/dev/log");
         unix-stream("/var/chroot-pppoe/dev/log"); unix-stream("/var/chroot-snor
t/dev/log");
         unix-stream("/var/chroot-pptpc/dev/log"); unix-stream("/var/chroot-weed
/dev/log");
         unix-stream("/var/chroot-snmp/dev/log"); unix-stream("/var/chroot-socks
/dev/log");
         unix-stream("/var/chroot-squid/dev/log"); unix-stream("/var/chroot-iden
t/dev/log");
         unix-stream("/var/chroot-pptp/dev/log"); unix-stream("/var/chroot-ppp/d
ev/log");
         unix-stream("/var/chroot-bind/dev/log"); unix-stream("/var/chroot-smtp/
dev/log");
         unix-stream("/var/chroot-http/dev/log");
 };
# destination and log statemens for astaro.mycompany.com
filter f_astaro         { match('\[(INFO|WARN|CRIT|DEBUG)-[0-9]+\]'); };
filter f_ainfo          { level(info); };
filter f_ainfo_notif    { level(notice); };
filter f_awarn          { level(warning); };
filter f_awarn_notif    { level(err); };
filter f_acrit          { level(crit) or level(alert); };
filter f_acrit_notif    { level(emerg); };
destination d_notif     { program("/usr/local/bin/notifier.pl"  template("$YEAR:
$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no) ); };
destination d_adminrr   { program("/usr/local/bin/reporter/admin-reporter.pl" te
mplate("$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no) );
};
destination d_smtprr    { program("/usr/local/bin/reporter/smtp-reporter.pl" tem
plate("$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no) ); }
;
```

```
destination d_socksrr   { program("/usr/local/bin/reporter/socks-reporter.pl" te
mplate("$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no) );
};
destination d_pcktrr    { program("/usr/local/bin/reporter/pfilter-reporter.pl"
template("$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no) )
; };
destination d_cfrr      { program("/usr/local/bin/reporter/cfilter-reporter.pl"
template("$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no) )
; };
destination d_ipsrr     { program("/usr/local/bin/reporter/ips-reporter.pl" temp
late("$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no) ); };

destination d_vpnrr     { program("/usr/local/bin/reporter/vpn-reporter.pl" temp
late("$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no) ); };

destination d_sarg_a    { program("/usr/local/bin/sarg-logger.pl -f access" temp
late("$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no) ); };

destination d_sarg_b    { program("/usr/local/bin/sarg-logger.pl -f blocked" tem
plate("$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no) ); }
;
destination d_astaro.mycompany.com_logging0 { file("/var/log/logging.log" templa
te("$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no)); };
log {  source(s_local_asl); filter(f_astaro); filter(f_ainfo);  destination(d_as
taro.mycompany.com_logging0); flags(final); };

log {  source(s_local_asl); filter(f_astaro); filter(f_ainfo_notif);  destinatio
n(d_astaro.mycompany.com_logging0); destination(d_notif); flags(final); };

log {  source(s_local_asl); filter(f_astaro); filter(f_awarn);  destination(d_as
taro.mycompany.com_logging0); flags(final); };

log {  source(s_local_asl); filter(f_astaro); filter(f_awarn_notif);  destinatio
n(d_astaro.mycompany.com_logging0); destination(d_notif);  flags(final); };

log {  source(s_local_asl); filter(f_astaro); filter(f_acrit);  destination(d_as
taro.mycompany.com_logging0); flags(final); };

log {  source(s_local_asl); filter(f_astaro); filter(f_acrit_notif);  destinatio
n(d_astaro.mycompany.com_logging0); destination(d_notif); flags(final); };

filter          f_syslog { facility(syslog) or program("syslog-ng"); };
destination d_astaro.mycompany.com_system0 { file("/var/log/system.log" template
("$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no)); };
log {  source(s_local_asl); filter(f_syslog);  destination(d_astaro.mycompany.co
m_system0); };

filter          f_crond { facility(cron) or program("cron"); };
log {  source(s_local_asl); filter(f_crond);  destination(d_astaro.mycompany.com
_system0); };

filter          f_kernel { facility(kern); };
filter          f_iptbl { match('(DROP:|ACCEPT:|REJECT:|ICMP REDIRECT:|INVALID_T
CP_PACKET:)'); };
destination d_astaro.mycompany.com_packetfilter0 { file("/var/log/packetfilter.l
og" template("$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(n
o)); };
destination d_astaro.mycompany.com_packetfilter1 { udp(10.10.0.1 port(514) templ
ate("$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC  $MSG\n") template_escape(no));  };
log {  source(s_local_asl); filter(f_kernel); filter(f_iptbl); destination(d_pck
trr);  destination(d_astaro.mycompany.com_packetfilter0); destination(d_astaro.m
ycompany.com_packetfilter1); flags(final); };

filter          f_synlim { match('(SYNRATE_LIMIT:)'); };
log {  source(s_local_asl); filter(f_kernel); filter(f_synlim);  destination(d_a
staro.mycompany.com_packetfilter0); destination(d_astaro.mycompany.com_packetfil
ter1); flags(final); };

filter          f_portscan { match(' Portscan detected:'); };
destination d_astaro.mycompany.com_portscan0 { file("/var/log/portscan.log" temp
late("$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no)); };
log {  source(s_local_asl); filter(f_kernel); filter(f_portscan); destination(d_
ipsrr);  destination(d_astaro.mycompany.com_portscan0); flags(final); };
```

```
destination d_astaro.mycompany.com_kernel0 { file("/var/log/kernel.log" template
("$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no)); };
log {  source(s_local_asl); filter(f_kernel);  destination(d_astaro.mycompany.co
m_kernel0); };

filter          f_auth  { facility(auth); };
filter          f_sshd  { program('sshd'); };
destination d_astaro.mycompany.com_sshd0 { file("/var/log/sshd.log" template("$Y
EAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no)); };
log {  source(s_local_asl); filter(f_auth); filter(f_sshd); destination(d_adminr
r);  destination(d_astaro.mycompany.com_sshd0); flags(final); };

filter          f_sulogin { program('su');  };
destination d_astaro.mycompany.com_login0 { file("/var/log/login.log" template("
$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no)); };
log {  source(s_local_asl); filter(f_auth); filter(f_sulogin); destination(d_adm
inrr);  destination(d_astaro.mycompany.com_login0); flags(final); };

filter          f_mingetty { program('mingetty');  };
log {  source(s_local_asl); filter(f_auth); filter(f_mingetty);  destination(d_a
staro.mycompany.com_login0); flags(final); };

filter          f_authpriv { facility(authpriv); };
filter          f_pluto { program('pluto'); };
destination d_astaro.mycompany.com_ipsec0 { file("/var/log/ipsec.log" template("
$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no)); };
log {  source(s_local_asl); filter(f_authpriv); filter(f_pluto); destination(d_v
pnrr);  destination(d_astaro.mycompany.com_ipsec0); flags(final); };

log {  source(s_local_asl); filter(f_authpriv); filter(f_login);  destination(d_
astaro.mycompany.com_login0); flags(final); };

filter          f_mail { facility(mail); };
filter          f_spamd { program('spamd'); };
destination d_astaro.mycompany.com_contentfilter0 { file("/var/log/contentfilter
.log" template("$YEAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape
(no)); };
log {  source(s_local_asl); filter(f_mail); filter(f_spamd);  destination(d_asta
ro.mycompany.com_contentfilter0); flags(final); };

filter          f_smtp { program('exim'); };
destination d_astaro.mycompany.com_smtp0 { file("/var/log/smtp.log" template("$Y
EAR:$MONTH:$DAY-$HOUR:$MIN:$SEC $HOST $MSG\n") template_escape(no)); };
log {  source(s_local_asl); filter(f_mail); filter(f_smtp); destination(d_smtprr
);  destination(d_astaro.mycompany.com_smtp0); flags(final); };
.
.
.
```

Figure 29 Output from syslog-ng.conf

Nothing in the configuration file indicates that the logs are being rotated.

```
$ more packetfilter-2004-09-19.10h46m.log
2004:09:19-08:26:32 (none) kernel: DROP: IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:0
a:95:b3:bc:68:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x00 PREC=0x00 T
TL=255 ID=14124 PROTO=UDP SPT=68 DPT=67 LEN=308
2004:09:19-08:26:34 (none) kernel: DROP: IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:0
a:95:b3:bc:68:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x00 PREC=0x00 T
TL=255 ID=14125 PROTO=UDP SPT=68 DPT=67 LEN=308
2004:09:19-08:26:36 (none) kernel: DROP: IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:0
a:95:b3:bc:68:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x00 PREC=0x00 T
TL=255 ID=14126 PROTO=UDP SPT=68 DPT=67 LEN=308
2004:09:19-08:26:40 (none) kernel: DROP: IN=eth1 OUT= MAC=ff:ff:ff:ff:ff:ff:00:0
a:95:b3:bc:68:08:00 SRC=0.0.0.0 DST=255.255.255.255 LEN=328 TOS=0x00 PREC=0x00 T
TL=255 ID=14127 PROTO=UDP SPT=68 DPT=67 LEN=308
```

Figure 30 Sample logs to verify that logging is taking place

Findings:
Logging is currently set for log files to be retained forever (and this was confirmed through the web gui). The firewall seems to have a separate disk partition just for the logs. Depending on the size of the drives on the production firewall platform, this may not be practical. Therefore, this should be revisited once the production hardware is acquired. The firewall also supports remote log archival, which would be a good practice regardless of disk sizes.

PASS

STEP 20:

V19 NTP

Evidence:

```
astaro:/var/storage/chroot-smtp/bin # ps ax | grep ntp
 5709 pts/0    R      0:00 grep ntp
astaro:/var/storage/chroot-smtp/bin #
```

Figure 31 NTP is not running

```
astaro:/var/storage/chroot-smtp/bin # cat /etc/ntp.conf
################################################################################
## /etc/ntp.conf
##
## Sample NTP configuration file.
## See package 'xntp-doc' for documentation, Mini-HOWTO and FAQ.
## Copyright (c) 1998 S.u.S.E. GmbH Fuerth, Germany.
--

driftfile /var/lib/ntp/ntp.drift # path for drift file

logfile   /var/log/ntp          # alternate log file
# logconfig =syncstatus + sysevents
--
#
# keys /etc/ntp.keys            # path for keys file
# trustedkey 1 2 3 4 5 6 14 15  # define trusted keys
--
```

Figure 32 NTP is not configured

Findings:
It is clear that ntp is not running, nor is it configured either as a daemon, or through cron.

FAIL

Audit Report

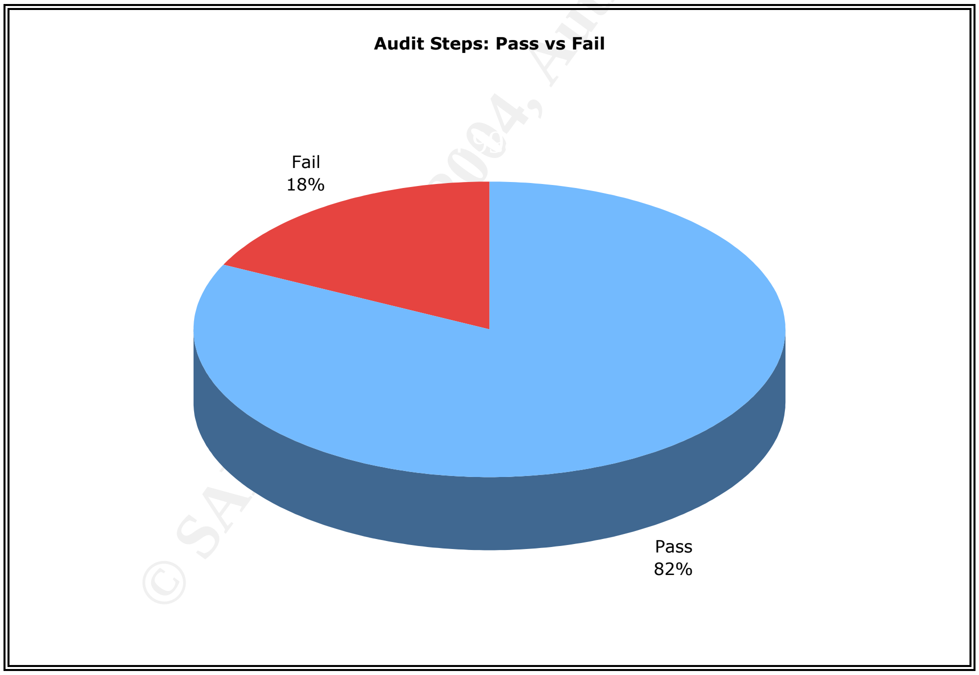
Executive Summary

The most significant risks in a firewall installation do not lie in the firewall device itself. Rather, they tend to be manifest in the implementation. In this audit, vulnerabilities were found to exist in the firewall, but they can be mitigated by installing the latest patches, and denying access to the firewall appliance. This will be described in more detail below. However, the most significant risks were found in the configuration of the firewall, and in the procedures surrounding the management of the firewall.

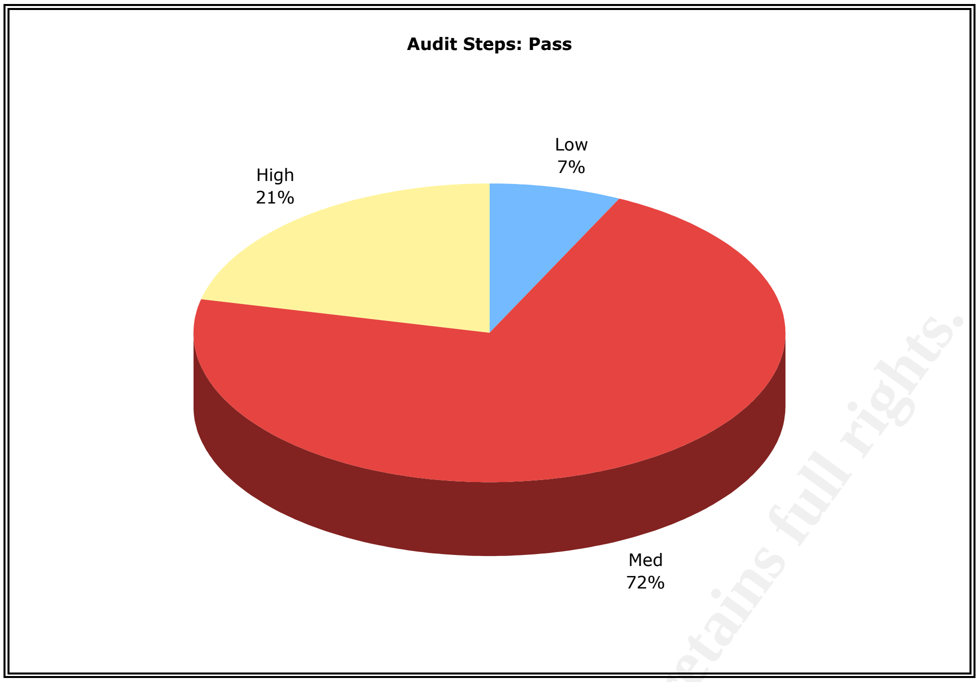
The audit covered all of these issues, and the results should be very helpful in the implementation phase of this project.

Audit Findings

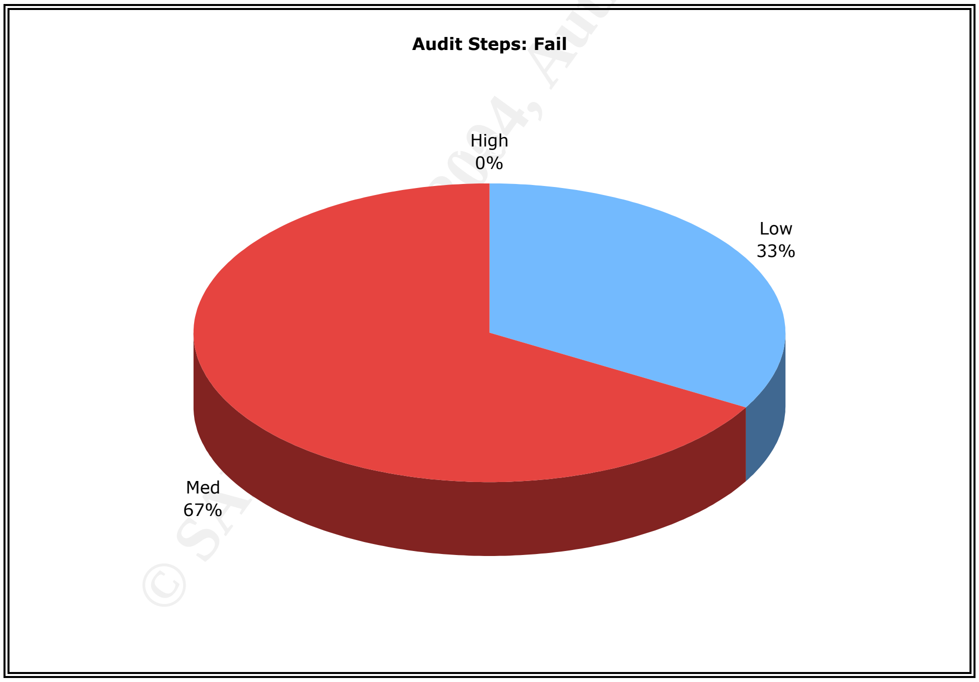
The audit consisted of 19 separate steps examining 19 potential vulnerabilities. The following chart shows how the firewall performed throughout all steps of the audit. Note that not all of the 19 steps were covered in detail in the preceding section.



This chart shows that the firewall passed the vast majority of tests performed. However, the chart does not give weight to the criticality of each step. The following two charts show this detail.



This chart shows the audit steps that the firewall passed, and how the percentages broke down between low, medium and high.



The important fact to note is that the firewall did not fail any high vulnerability tests. Most of the tests that the firewall failed were based on the use of older versions of software packages. This issue will be elaborated upon in the next section.

Audit Recommendations

Since several software packages, which make up the firewall, are out of date, the first step in mitigation must be to update the firewall to its latest version. (Ideally, those audit steps that failed should be retried at that point.) Moreover, a plan or routine should be put into place whereby new patches are periodically installed on the firewall. The Astaro firewall also features an auto-update function. Either method is reasonable (manual or automatic), as long as it is agreed upon and documented.

In addition to these steps, the packet filtering router can be used to protect the firewall against would-be outside attackers. Since the routing hardware exists, and the router sits between the Internet and the firewall, this would be a zero-cost option, which could tremendously increase network security from outside attacks. To protect against inside attacks, ACLs should be configured (either on the firewall, or on an internal router) to allow only distinct hosts access to ssh and to the browser-based interface.

Another area of concern involves the current configuration of the firewall. Some less critical features have not been configured properly, and should be addressed. These include the use of the network time protocol (ntp), which is used to synchronize log entries, and the lack of log file rotation.

Aside from the technical aspects of the audit, other procedural issues also came up. These include the lack of a comprehensive firewall policy. A firewall policy is used to outline, in plain language, the firewall rules. Furthermore, a firewall policy should outline the procedure for updating the policy, and consequently for making changes to the firewall itself. It is also crucial that the firewall administrators get the required training in order to be proficient at configuring the firewall. As cited above, studies have shown that a large portion of outages result from misconfiguration. This last point cannot be emphasized strongly enough.

Overall, a few issues came to light from this audit. However, none of them should be construed as reasons to change the project plan for the implementation of the firewall. Certain steps that have been outlined in this section need to be taken, but aside from these, the implementation plan is sound.

References

1. United States. Dept. of Commerce. National Institute of Standards and Technology. Risk Management Guide for Information Technology Systems. Washington: NIST, July 2002. URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
2. Hansche, Susan, Berti, John, and Hare, Chris. Official (ISC)2 Guide to the CISSP Exam. Boca Raton: Auerbach, 2004.
3. Netfilter Organization. Documentation found at http://www.netfilter.org/documentation/index.html
4. Jones, Alan. "Netfilter and IPTables – A Structural Examination." GSEC Practical, Feb 2004.
5. Nemeth, Snyder, Hein. "Linux Administration Handbook." Prentice Hall PTR, 2002.
6. Zwicky, Cooper, and Chapman. "Building Internet Firewalls." 2nd Edition. O'reilly and Associates, June 2000. Page 746
7. SANS Track 7 Section 7.3 Auditing Web Applications
8. Belani, Rohyt. "Basic Web Session Impersonation." Security Focus 14 April 2004. URL: http://www.securityfocus.com/infocus/1774
9. http://www.cirt.net/code/nikto.shtml (CGI scanning tool)
10. Brutus brute force cracking tool. URL: http://www.hoobie.net/brutus/index.html
11. Carnegie Mellon Software Engineering Institute. URL: http://www.cert.org/nav/index_red.html (Advisories and Incidents)
12. Internet Software Consortium (writers of BIND). URL: http://www.isc.org/products/BIND/bind-security.html (additional security issues with BIND)
13. SANS Top 10 Unix vulnerabilities. URL: http://www.sans.org/top20/#u1
14. Garfinkel, Spafford, and Schwartz. "Practical Unix and Internet Security." O'reilly and Associates, February, 2003. Chapters 13 and 15.
15. Apache Security (version 1.3). URL: http://www.apacheweek.com/features/security-13
16. Apache Security (version 2.0). URL: http://www.apacheweek.com/features/security-20
17. Costales, Bryan and Allman, Eric. "sendmail." O'reilly and Associates, November 1997.
18. CERT SNMP Adivisory. URL: http://www.cert.org/advisories/CA-2002-03.html
19. CERT OpenSSH Challenge Response Handling Vulnerability. URL: http://www.cert.org/advisories/CA-2002-18.html
20. CERT OpenSSH Buffer Management Vulnerability. URL: http://www.cert.org/advisories/CA-2003-24.html
21. OpenSSH Security Page. URL: www.openssh.org/security.html
22. CERT OpenSSL Multiple Vulnerabilities. URL: http://www.cert.org/advisories/CA-2002-23.html
23. OpenSSL Security Advisory. URL: http://www.openssl.org/news/secadv_20040317.txt
24. CIAC Squid NTLM Buffer Overflow. URL: http://www.ciac.org/ciac/bulletins/o-168.shtml
25. Squid Security Advisory. URL: http://www.squid-cache.org/Advisories/SQUID-2004_2.txt
26. Security Focus: Multiple Linux Kernel Vulnerabilities. URL: http://www.securityfocus.com/bid/9985
27. CERT Linux Kernel Vulnerability. URL: http://www.kb.cert.org/vuls/id/301156/
28. Syslog-ng Home Page. URL: http://www.balabit.com/products/syslog_ng/
29. Syslog-ng FAQ. URL: http://www.campin.net/syslog-ng/faq.html#compression
30. Configuring syslog-ng. URL: http://sial.org/howto/logging/syslog-ng/

31. Astaro User manual. URL: http://docs.astaro.org/ACM_manuals/
32. Neohapsis Exim Buffer Overflow. URL: http://archives.neohapsis.com/archives/secunia/2004-q2/0284.html