Global Information Assurance Certification Paper

Auditing a Corporate E-mail Gateway Running Postfix on Linux: an Administrator's Perspective

GSNA Practical Version 2.1 – Option 1

Author: William Karwisch

Date: 8 November 2003

Abstract

This is a report of the audit of a corporate e-mail relay from an administrator's viewpoint. The audit process optimized the scope of the audit using a pre-audit risk assessment. The audit objectively showed the reduction of risk from the un-audited state of the system through the audit and the post-audit remediation of findings. The subject of the audit, a Postfix e-mail relay running on a Linux server, was installed and configured approximately three months prior to the audit. The Linux operating system and Postfix e-mail software were installed on the same computer that previously had been running earlier versions of the same software. The goals of upgrading the system included improving the overall security and reliability of the server.

The audit was conducted to determine if the new configuration can adequately protect the e-mail that it transports, defend against external and internal vulnerabilities, and provide reliable service. This report divides the audit process into four sections. The first section describes the system, analyzes its risks, develops the high-level objectives of the audit, and researches current practice. The second section is the audit checklist. The third section documents the actual audit and analyzes the results. The fourth section is a summary of audit findings and the risks they pose, a description of system changes, results of retesting the system, and a justification of the final state of the system.

Table of Contents

Table of Figures

Table of Tables

Section 1 – Research in Audit, Measurement Practice, and Control

Identify the System to be Audited

The subject of the audit is a corporate e-mail relay, or gateway. The subject is a production server for a service organization. It is the single point of contact for e-mail between the company's internal network and the Internet. This server handles all e-mail messages that are exchanged between the Internet and the internal network.

The purpose of e-mail relay is to provide controlled access for inbound e-mail, to isolate the internal e-mail server from the Internet, to filter e-mail for potentially harmful attachments, and to filter out a large percentage of unsolicited commercial e-mail (UCE), usually referred to as spam. Filtering messages at this point has the additional benefit of reducing traffic on the internal e-mail server. The server also acts as a buffer, storing inbound messages temporarily in the event of an outage of the internal e-mail server.

The goal of the audit is to evaluate the security of the mail-gateway function. To view the relay as separate from its environment for audit purposes introduces the risk that the overall audit objective would not be accomplished. Therefore the scope of the audit will include the network, the firewall and the computers that interact with the e-mail relay in as much as they participate in the relay's function. To keep the scope of the audit manageable, however, the scope is limited to the aspects of the network and systems relevant to the mail gateway function and excludes issues related to internal e-mail and other services.

Computer Model, Operating System and Software Version

This system uses Postfix 1.1.12 as the e-mail software, which runs on top of the Red Hat Linux 9.0 operating system on a Compaq DL320 rack-mounted server. This server is now in its third incarnation since it was implemented two years ago. The original system used Postfix running on FreeBSD. The second used Postfix on Linux 7.2. For each incarnation, the system was completely reformatted and fresh installs were performed.

Postfix was chosen as the e-mail software because it was written with security in mind. It has a simpler design than sendmail, which is usually included in Linux distributions by default. Arguably, the current version of sendmail does not have the security deficiencies that plagued older versions, but Postfix has a good reputation for reliability, security, and stability.

FreeBSD was replaced with Linux 7.2 in the second incarnation of the relay to provide better access to resources for support. Although FreeBSD is an excellent system, much more information is available for Red Hat Linux and many more people have experience with it. The decision was made to use Red Hat Linux 9.0

in the latest incarnation because it is likely to be supported longer than the older version. Even though it was released relatively recently, it uses the Linux kernel version 2.4, which was already in use prior to the release; stability of the system was not perceived to be a risk.

Because of the server's role as an e-mail relay, it does not have any graphical user interface (GUI), web server, SNMP, or DNS software. Sendmail was removed from the server before installing Postfix. Software development packages (compilers and other tools) are not installed.

The System's Role in the Organization

The organization depends on this production server to conduct its business effectively. It is used to communicate with clients and to exchange information with off-site employees. Reliable and timely e-mail communication is critical for this company to maintain an efficient operation and build client confidence.

The server acts as the company's e-mail gateway. It is registered in the Domain Name System (DNS) as the company's primary mail exchanger (MX). It is isolated from the Internet by a firewall, which uses a static route for the relay and which only allows external connections to the relay on port 25, which is used for Simple Mail Transport Protocol (SMTP). The server only accepts e-mail destined for the company's domain. It will not relay e-mail destined for other domains.

The server blocks a significant number of undesirable messages, including unsolicited commercial e-mail (UCE or spam). Postfix uses several types of filters to accomplish this, including real-time black lists (RBL) and operator-defined lists such as domain and address lists for offending addresses, keyword lists, and lists of banned mail-from addresses.

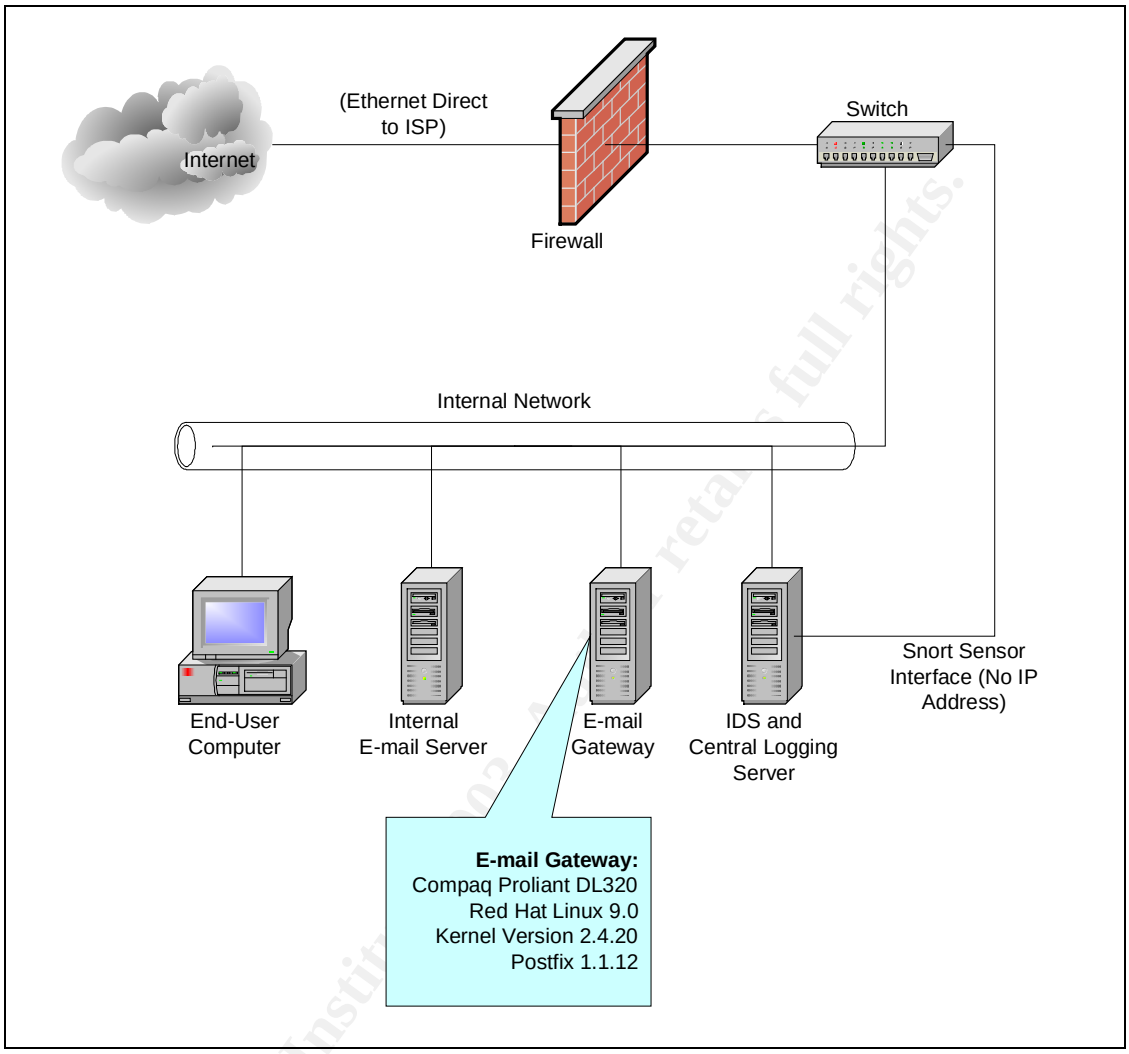
The server has no end-user accounts. It forwards all e-mail to the company's internal e-mail server, which hosts the users' e-mail accounts. The server also accepts outbound messages from internal users and forwards them to their destination.

An intrusion detection system (IDS) monitors inbound and outbound traffic at the inside interface of the firewall. It is connected to the network switch using a spanned port that monitors the internal interface of the firewall. The IDS monitoring interface does not have an IP address. A second interface is used to communicate with the IDS for administration and maintenance. The IDS also serves as the organization's remote logging server. The e-mail relay maintains its own logs and forwards copies of log messages to the IDS.

Finally, the relay functions as a network time protocol (NTP) server for the internal network. It is configured to synchronize with several external sources and to provide time synchronization for other hosts on the network.

Network Diagram (Relevant Portion)

Figure 1 – Network diagram (relevant portion)



Analysis of Network Input Controls

Normal network traffic to the e-mail relay includes port 25 (SMTP), port 22 (SSH), port 53 (DNS from internal servers) and port 123 (NTP). By design, the firewall only allows inbound traffic necessary to the proper function of the server. The relay has additional firewall functionality of its own, using iptables, as an added layer of defense from external traffic and to restrict internal traffic. The IDS reports instances of malicious traffic that it recognizes.

The services that the e-mail relay makes available to the network use versions of software that properly handle known exploits. Postfix handles unexpected traffic reliably. Discoveries of buffer overflows and other exploits are rare. The server logs show numerous instances of malformed packets being handled safely.

Postfix was designed to provide defense in depth. It can be configured to run in a chroot jail, where the execution environment sees its directory as the system root directory. Even if the Postfix environment were compromised, the attacker would not have access to the rest of the system.

Vulnerabilities are occasionally found in OpenSSH. However, if the firewall works correctly, SSH is usable only from the internal network.

Vulnerabilities are occasionally found in NTP, but the network firewall does not allow unsolicited UDP packets to the port 123 on this server. To further reduce the likelihood of attempted exploits of NTP, the startup script for NTP opens the NTP port on the firewall only for the time servers that the e-mail relay uses for synchronization.

The following table summarizes the designed response of the system to various normal and unexpected network inputs:

Table 1 – Network input controls

Port	Source	Type	Response
UDP 123 (NTP)	Internet	Normal – Solicited Response	Allowed
UDP 123 (NTP)	Internet	Normal – Unsolicited Packet	Rejected
UDP 123 (NTP)	Internal Network	Normal	Allowed
UDP 53 (DNS)	Internal DNS Servers	Normal	Allowed
TCP 22 (SSH)	Internet	Normal	Rejected
TCP 22 (SSH)	Internal Network	Normal	Allowed
TCP 25 (SMTP)	All	Normal	Allowed
All other ports	All	Normal	Rejected
UDP 123 (NTP)	All	Malformed	Handled by NTP software on server
TCP 22 (SSH)	Internal Network	Malformed	Handled by OpenSSH software on server
TCP 25 (SMTP)	All	Malformed	Handled by Postfix software on the server and logged
All	All	Packets with known intrusion signatures	Recorded and logged by IDS
All	Internet	SYN Flood	Regulated by network firewall
All	All	Other Denial of Service Attacks	Depends on mode of attack.

Postfix is not typical of the applications that come to mind when discussing application controls. Such applications typically use screens, keyboards and printers. Appropriate controls for these applications include validating keyboard

input, performing integrity checks, application-level permissions and database-level permissions.

Although Postfix does not fit this profile, important controls are in place for input validation and processing. These controls are regulated by settings in the Postfix configuration file. The controls that are most relevant to this implementation of Postfix are summarized in the following table:

Table 2 – Postfix application controls

Control Type	Action
Input	Log and reject messages greater than a specified size
Input	Log and reject messages to specified users
Input	Log and reject messages from specified sources
Input	Log and reject messages according to real-time blacklists (used for open-relays and UCE)
Input	Log and reject messages based on content, including executable extensions
Input	Log and reject relaying to non-local domains from external hosts (no open relaying)
Processing	Relaying is allowed from the Internet to the internal network
Processing	Relaying is allowed from the internal network to anywhere.
Processing	Malformed requests are logged and rejected safely

Evaluate the Risk to the System

Justification for the Audit

This organization makes very few IP services visible to the Internet. The e-mail relay is one of the few direct points of contact from the Internet to the organization's internal network. Because the relay is not in a DMZ, any deficiencies in the security of this system could jeopardize the entire network. Other systems on the network serve a more critical function to the organization's operation, but do not have the direct exposure to attacks that the e-mail relay has. This system was selected for the audit to measure the security of the newly installed system and to improve security by correcting any deficiencies that were found.

Methodology

The organization's existing security policy is extremely high-level and generic. It does not address any issues that are relevant to auditing a system and does not provide any information that could be used as guidance in evaluating risk to the system or developing a checklist. In addition, there was no previous audit of the system that could be used as an input into developing this audit. Therefore, research into best practices and personal experience were used to evaluate the risks and develop the checklist.

One goal for the risk evaluation was to provide an objective result. Typically, objective determinations of risk rely on numerical valuations of vulnerabilities, threats and impacts. Obtaining sufficient data for reliable numeric inputs was not feasible in this case, so a risk model with a subjective starting point was necessary to evaluate the risk.

The methodology used to evaluate the risk was adapted from a presentation by Dr. Donald R. Peeples at the 1997 National Information Systems Security Conference.[1] It is based on the usual definition of risk:

RISK = VULNERABILITY x THREAT x IMPACT

His presentation shows a method for numerical evaluation of risk based on subjective estimates of threats, vulnerabilities and impacts. The method reduces the subjectivity of risk evaluation without depending on strictly objective inputs, which are difficult or impossible to determine. The method substitutes predetermined numeric values in place of the subjective values of Low, Medium, High and Critical to give a mathematical value of the risk.

The values for Threats and Vulnerabilities represent probabilities. For Threats, the measure is the probability that the threat will be present. For Vulnerabilities, the measure is the probability that the threat will be realized if present – in other words, a measure of weakness against attack. The values for Risk and Impact are relative to a scale of 100 and usually refer to economic loss (although other measures can be used); they are unusual in that the difference from one level to the next is exponential instead of linear. The suggested numeric values and ranges in the table below are quoted from Peeples's presentation. The organization has not previously tested this model. The audit results may show that the model could benefit from some adjustments and refinements.

Table 3 – Numeric values for risk assessment

	LOW	MEDIUM	HIGH	CRITIAL
Threat	.12	.37	.62	.87
Vulnerability	.12	.37	.62	.87
Impact	.1	1	10	100
Risk	0-.3	.3-3	3-30	30-100

Applying these values of the vulnerabilities, threats, and impacts to the formula given above will yield a numeric result from subjective inputs. The results will be compared relative to each other and to where they fall in the overall range of risk, which is from 0 to 100. The audit control objectives will be developed from this analysis, using the items that result in critical and high risk.

[1] Peeples, Donald. "The Foundations of Risk Management." 6 May 1997. URL: http://csrc.nist.gov/nissc/1997/proceedings/577slides.pdf (Oct 11, 2003).

The basis for the risk evaluation is that the system has not been audited and therefore no assumptions can be made about its security. The risk assessment does not predict how well the e-mail relay and its surrounding systems mitigate the risks. That determination will be made during the actual audit. Nevertheless, time and resource constraints require that unnecessary and unproductive work be eliminated. For the purpose of efficiently developing the risk evaluation and the rest of this audit, therefore, the basic configuration of the e-mail server will be assumed to be as described above. For example, the audit will not specifically address web-server-related risks because there is no web-server software on the system. The assertions made about the system were verified prior to developing the risk analysis and audit checklist. Because the integrity of the audit depends on these assertions, they will be verified again in the first steps of the checklist to make sure the system has not changed materially.

The criteria for the risk evaluation are the system's reliability, availability, and the ability to perform the function for which it was designed – in spite of the threats and vulnerabilities that it encounters. This scope is much broader than defending against the black-hats.

> "So much time, effort, publicity and just plain 'hype' is devoted to protecting corporate information assets against outside threats that outages due to human frailty are often neglected altogether. System failures due to poor planning, lack of knowledge or faulty design are just not sexy. It should be obvious that it is far easier for one disgruntled, vengeful or just plain klutzy employee with a system user ID to wreak havoc than it is for the most skillful attacker to intrude from outside the organization."[2]

The audit scope will consider environmental, operational, network, operating system, and any other areas where threats and vulnerabilities could result in a system that is unavailable or compromised in some way.

The following procedure will be used to develop the risk model for the e-mail relay:

1. Identify the vulnerabilities and assign values of Low, Medium, High or Critical.
2. Identify the threats and assign values of Low, Medium, High or Critical.
3. Determine which threats can be realized through which vulnerabilities.
4. Determine the impact of each realizable threat and assign a value of Low, Medium, High or Critical.
5. Substitute the numeric values in the table above.
6. Calculate the numeric value of the risk and translate the number to a risk rating of Low, Medium, High or Critical.

[2] Mina, Ted. "Application Security, Information Assurance's Neglected Stepchild – A Blueprint for Risk Assessment." 18-20 May 2001. URL: http://www.sans.org/rr/paper.php?id=56 (4 Oct. 2003).

Identify Vulnerabilities and Assign Values

The values specified in this section are an estimate of the likelihood that if the vulnerability coincides with an appropriate threat, something bad would happen. They are not a judgment of how bad the event would be or an indication of the urgency of correcting the vulnerabilities.

Table 4 – Vulnerabilities identified

Environmental Vulnerabilities	Value
Dependence on environment to be able to operate	Critical
Physical access to server	High
Operational Vulnerabilities	**Value**
Hardware subject to failure	Critical
Backup media may be corrupted or unavailable when needed	Low
System malfunctions may not be detected timely	High
System changes may not be detected timely	High
System has finite processing and storage capacity	Low
Network Vulnerabilities	**Value**
System requires proper communication with DNS server	Critical
System requires proper communication with default gateway	Critical
System requires proper communication with switch	Critical
System requires proper NAT function on firewall	Critical
Linux Vulnerabilities	**Value**
(The following six vulnerabilities are from the UNIX and Linux vulnerabilities of the SANS Top 20 Vulnerabilities List.[3] They are considered critical, and therefore will be assigned a critical value in the risk calculation.)	
Remote Procedure Calls (RPC)	Critical
General UNIX Authentication Accounts with No Passwords or Weak Passwords	Critical
Clear Text Services	Critical
Secure Shell (SSH)	Critical
Misconfiguration of Enterprise Services NIS/NFS	Critical
Open Secure Sockets Layer (SSL)	Critical
Other operating system patches may not be current	High
Other unnecessary services may be enabled	High
SMTP-specific Vulnerabilities	**Value**
Unwanted or harmful messages – e-mail encapsulates almost anything and bypasses most network controls	Critical
SMTP does not check source addresses	Critical
E-mail software can operate as open relay	Critical

[3] "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0. 8 Oct. 2003. URL: http://isc.sans.org/top20.html#u1 (11 Oct. 2003).

Postfix-specific Vulnerabilities	Value
Postfix denial of service attack possible for version 1.1.12 and earlier.[4]	Medium
Postfix environment may not be secured optimally	Medium
Postfix may not be configured correctly to implement its normal function of relaying inbound and outbound messages	Critical

Identify Threats and Assign Values

The values assigned in this section are an estimate of the likelihood that a specific threat will occur; they are not judgments of how likely something bad could result.

Table 5 – Threats identified

Environmental Threats	Value
Physical Destruction	Low
Environment becomes unsuitable for operation (e.g. no power or no cooling)	Medium
Operational Threats	**Value**
Hardware Failure	Low
Unauthorized access	Critical
Operator or Administrator error	High
System overload	Low
Malicious users	Med
Careless and untrained users	High
Network Threats	**Value**
Denial of service attacks	Low
Linux Threats	**Value**
Denial of service attacks	Low
Attacker compromises	Critical
Worms	Critical
E-mail-specific Threats	**Value**
(The items in this section are quoted from Custódio[5], who identifies several threats that are common to all e-mail systems. Threat values are specific to the organization.)	
UCE or spam	Critical
Mail Forgery	High
Availability Attack	Low
Mail Virus	Critical
Confidentiality or Privacy Violation	High
Information Destruction	Low

[4] Davis, Noel. "Postfix Attack." 11 Aug. 2003. URL: http://linux.oreillynet.com/pub/a/linux/2003/08/11/insecurities.html (18 Oct, 2003).
[5] Custódio, Filipe. "Auditing Microsoft Corporate e-mail Solutions (Exchange 5.5 and Outlook 2000)." Sep. 2001. URL: http://www.giac.org/practical/Filipe_Custodio_GSNA.zip (4. Oct. 2003).

Information Hijack	Low
Information Gathering	Medium
Authentication Attack	Low
Identity Theft	Low
Disposing of Evidence	Low

Determination of Impacts and Risks as a Result of Realized Threats

One could develop an impact matrix by examining all possible combinations of threats and vulnerabilities. In practice, this is not feasible because the combinations quickly become too many and most of them do not make sense. For instance, it is unlikely that the Blaster worm could exploit the fact that you do not have a fire extinguisher in your computer room. The vulnerability is not exploitable by the threat.

The following impact and risk matrix was developed by considering which threats could be realized though each vulnerability. Values for impacts indicate the overall severity of the outcome. With the values for the vulnerability, threat, and impact established, determining the risk is simply a matter of multiplying the three values. The result of the risk calculation is shown in the last column.

Each vulnerability may have more than one realizable threat. In some cases, different threats cause different impacts for the same vulnerability; the matrix shows separate values for impact in such cases. In some cases, multiple vulnerabilities share the same threats and impacts; they are combined in the table for simplicity.

Table 6 – Impacts and risks

Vulnerability	Realizable Threats	Impact	Example Outcomes	Vulnerability Value	Threat Value	Impact Value	Risk
Dependence on environment to be able to operate	Physical destruction	Prolonged denial of service, loss of server, and potential loss of queued e-mail. Business and IT (Information Technology) staff productivity impact and cost to replace.	The server could burn in a building fire or be completely destroyed by a terrorist attack.	Critical – .87	Low – .12	Critical – 100	10- High
	Environment becomes unsuitable for operation (e.g. no power or cooling)	Denial of service, potential loss of queued e-mail – business productivity impact – potential cost of relocation.	The server would not perform its function in a prolonged power outage. Or, if the cooling failed in the computer room, the server would have to be shut down until power were restored.		Medium – .37	High – 10	3.2 – High
Physical Access	Unauthorized access	Potential disclosure of confidential information, potential loss of confidence in organization by clients, potential damage to organization's credibility, potential for opening additional vulnerabilities, business and IT staff productivity loss,	An attacker who had physical access to the server could easily gain access with superuser privileges. Once that was done, he could use the server to attack the rest of the internal network, store warez (illegal, cracked versions of software), illegally download and share music files, or	High – .62	Medium – .37	Critical – 100	23 – High

Vulnerability	Realizable Threats	Impact	Example Outcomes	Vulnerability Value	Threat Value	Impact Value	Risk
		potential re-allocation of system resources by attacker for other illegal purposes.	sniff e-mail traffic for confidential information.				
Hardware sometime fails	Hardware failure	Denial of service, potential loss of queued e-mail – Cost to repair or replace hardware – Business and IT staff productivity impact.	A hardware failure would result in the loss of service until the hardware was repaired or replaced. Replacing the hardware would require re-installing the operating system and recovering the application from backup.	Critical – .87	Low – .12	Medium – 1	0.10 – Low
Backup media may be corrupted or unavailable when needed	Physical destruction	Denial of service, but no loss of business-related data (none stored on server). Reload software and manually configure. Business and IT staff productivity impact.	Restoring the system without backup media would require rebuilding the system from scratch. This would require loading Linux and Postfix from distribution media, and configuring the system.	Low – .12	Low – .12	Medium – 1	0.014 – Low
	Operator or administrator error				High – .62		0.074 – Low
	System overload (server upgrade)				Low – .12		0.014 – Low
	Attacker compromises				Critical .87		0.10 – Low
	Worms				Critical .87		0.10 – Low
System malfunctions may not be detected timely	Hardware failure	Denial of service– potential for loss of messages in transit, potential loss of confidence in organization by clients, potential for opening additional vulnerabilities, business and IT staff productivity loss.	Service would be unavailable until the malfunction is detected. The organization's clients may not receive e-mails that they expect, possibly concluding that the organization is neglecting their needs. In the worst cases, confidential information could be disclosed	High – .62	Low – .12	High – 10	0.74 – Medium
	System overload				Low – .12		0.74 – Medium

Vulnerability	Realizable Threats	Impact	Example Outcomes	Vulnerability Value	Threat Value	Impact Value	Risk
	Denial of service attack				Low – .12		0.74 – Medium
	Operator or Administrator Error	Potential disclosure of confidential information, denial of service – potential loss of confidence in organization by clients, potential damage to organization's credibility, potential for opening additional vulnerabilities, business and IT staff productivity loss.			High – .62	Critical – 100	38 – Critical
	Attacker compromise				Critical – .87		54 – Critical
	Worms				Critical – .87		54 – Critical
System changes may not be detected timely	Operator or Administrator Error	Potential disclosure of confidential information, potential loss of confidence in organization by clients, potential damage to organization's credibility, potential for opening additional vulnerabilities, business and IT staff productivity loss, potential re-allocation of system resources by attacker for other illegal purposes.	The organization's clients may not receive e-mails that they expect, possibly concluding that the organization is neglecting their needs. In the worst cases, confidential information could be disclosed, possibly by sending messages to the wrong destination. The result could be a total loss of confidence the organization by its clients. In other cases, vulnerabilities may be exposed that would allow system access to an attacker compromises with outcomes the same as discussed above.	High – .62	High – .62	Critical – 100	38 – Critical
	Attacker compromise				Critical – .87		54 – Critical

Vulnerability	Realizable Threats	Impact	Example Outcomes	Vulnerability Value	Threat Value	Impact Value	Risk
	Worms				Critical – .87		54 – Critical
System has finite processing and storage capacity	Operator or Administrator Error	Denial of service. Possibly upgrade hardware – business and IT staff productivity loss.	The most likely result would be a loss of service while the condition was corrected. The extreme case would require system upgrades.	Low – .12	High – .62	Medium – 1	.074 – Low
	System overload				Low – .12		.014 – Low
	Denial of service attack				Low – .12		.014 – Low
System requires proper communication with DNS server System requires proper communication with default gateway System requires proper communication with switch System requires proper NAT function on firewall	Operator or Administrator Error	Denial of service. Business productivity loss.	If supporting systems do not provide their services correctly, the e-mail relay will not operate, resulting in the loss of service. The condition will continue until the services are restored. In addition, the server could be inadvertently connected to the wrong switch, such as a test network switch, with the result that important network controls are bypassed.	Critical – .87	High – .62	Low – 0.1	.054 – Low
	Denial of service attack				Low – .12		.010 – Low
	Attacker compromises (partial loss of defense in depth)				Critical – .87		5.4 – High

Vulnerability	Realizable Threats	Impact	Example Outcomes	Vulnerability Value	Threat Value	Impact Value	Risk
Remote Procedure Calls (RPC)	Attacker compromises	Potential disclosure of confidential information, potential loss of confidence in organization by clients, potential damage to organization's credibility, potential for opening additional vulnerabilities, business and IT staff productivity loss, potential re-allocation of system resources by attacker for other illegal purposes.	An attacker could gain access, possibly with superuser privileges. Once that was done, he could use the server to attack the rest of the internal network, store warez, illegally download music, or sniff e-mail traffic for confidential information.	Critical – .87	Critical – .87	Critical – 100	76 – Critical
	Worms				Critical – .87		76 – Critical
General UNIX Authentication Accounts with No Passwords or Weak Passwords	Attacker compromises	Potential disclosure of confidential information, potential loss of confidence in organization by clients, potential damage to organization's credibility, potential for opening additional vulnerabilities, business and IT staff productivity loss, potential re-allocation of system resources by attacker for other illegal purposes.	An attacker could gain access, possibly with superuser privileges. Once that was done, he could use the server to attack the rest of the internal network, store warez, illegally download music, or sniff e-mail traffic for confidential information.	Critical – .87	Critical – .87	Critical – 100	76 – Critical

Vulnerability	Realizable Threats	Impact	Example Outcomes	Vulnerability Value	Threat Value	Impact Value	Risk
Clear Text Services	Attacker compromises	Potential disclosure of confidential information, potential loss of confidence in organization by clients, potential damage to organization's credibility, potential for opening additional vulnerabilities, business and IT staff productivity loss, potential re-allocation of system resources by attacker for other illegal purposes.	The most likely outcome would be an attacker using a packet sniffer to capture clear text traffic. Captured transmissions could contain confidential information that is directly useful or usernames and passwords that can be used to gain access to the system.	Critical – .87	Critical – .87	Critical – 100	76 – Critical
Secure Shell (SSH)	Attacker Compromise	Potential disclosure of confidential information, potential loss of confidence in organization by clients, potential damage to organization's credibility, potential for opening additional vulnerabilities, business and IT staff productivity loss, potential re-allocation of system resources by attacker for other illegal purposes.	An attacker could gain access, possibly with superuser privileges. Once that was done, he could use the server to attack the rest of the internal network, store warez, illegally download music, or sniff e-mail traffic for confidential information.	Critical – .87	Critical – .87	Critical – 100	76 – Critical

Vulnerability	Realizable Threats	Impact	Example Outcomes	Vulnerability Value	Threat Value	Impact Value	Risk
Misconfiguration of Enterprise Services NIS/NFS	Attacker Compromise	Potential disclosure of confidential information, potential loss of confidence in organization by clients, potential damage to organization's credibility, potential for opening additional vulnerabilities, business and IT staff productivity loss, potential re-allocation of system resources by attacker for other illegal purposes.	An attacker could mount and explore the file system remotely and explore it. He could download the password file and attempt to crack the passwords with the intent of gaining access, with the results mentioned above.	Critical – .87	Critical – .87	Critical – 100	76 – Critical
Open Secure Sockets Layer (SSL)	Attacker Compromise	Potential disclosure of confidential information, potential loss of confidence in organization by clients, potential damage to organization's credibility, potential for opening additional vulnerabilities, business and IT staff productivity loss, potential re-allocation of system resources by attacker for other illegal purposes.	An attacker could gain access, possibly with superuser privileges. Once that was done, he could use the server to attack the rest of the internal network, store warez, illegally download music, or sniff e-mail traffic for confidential information.	Critical – .87	Critical – .87	Critical – 100	76 – Critical

Vulnerability	Realizable Threats	Impact	Example Outcomes	Vulnerability Value	Threat Value	Impact Value	Risk
Other operating system patches may not be current	Attacker Compromise	Potential disclosure of confidential information, potential loss of confidence in organization by clients, potential damage to organization's credibility, potential for opening additional vulnerabilities, business and IT staff productivity loss, potential re-allocation of system resources by attacker for other illegal purposes.	An attacker could gain access, possibly with superuser privileges. Once that was done, he could use the server to attack the rest of the internal network, store warez, illegally download music, or sniff e-mail traffic for confidential information.	High – .62	Critical – .87	Critical – 100	54 – Critical
Other unnecessary services may be enabled	Attacker Compromise	Potential disclosure of confidential information, potential loss of confidence in organization by clients, potential damage to organization's credibility, potential for opening additional vulnerabilities, business and IT staff productivity loss, potential re-allocation of system resources by attacker for other illegal purposes.	Unnecessary services could be used as a starting point for gaining information about a system. In addition, errors in configuring these services may result in vulnerabilities that could be directly exploited to obtain information or access.	High – .62	Critical – .87	Critical – 100	54 – Critical

Vulnerability	Realizable Threats	Impact	Example Outcomes	Vulnerability Value	Threat Value	Impact Value	Risk
E-mail encapsulates almost anything and bypasses most network controls	Malicious Users	Potential disclosure of confidential information, potential loss of confidence in organization by clients, potential damage to organization's credibility, potential for opening additional vulnerabilities, business and IT staff productivity loss.	SMTP sends messages in clear text. Messages can be sniffed and intercepted. Users can experience problems caused by e-mail including spam, social engineering attacks, worms, viruses, malicious attachments, and spyware. Malicious and careless users can send confidential information outside the organization inappropriately.	Critical – .87	Med – .37	Critical – 100	32– Critical
	Careless or untrained users				High – .62		54 – Critical
	UCE or spam				Critical – .87		76 – Critical
	Mail Virus				Critical – .87		76 – Critical
	Confidentiality or Privacy Violation				Critical – .87		76 – Critical
	Information Gathering				Medium – .37		32 – Critical
	Identity Theft				Low – .12		10 – High
SMTP does not check source addresses	Mail Forgery	Potential loss of confidence in organization by clients, potential damage to organization's credibility.	E-mail can be spoofed by using fictitious source host names and e-mail addresses. Users can be tricked into reading unwanted e-mail or opening malicious attachments, assuming that messages are from known or trusted sources.	Critical – .87	High – .62	Critical – 100	54 – Critical
E-mail software can operate as open relay	Attacker compromise.	Potential loss of confidence in organization by clients. Potential network degradation	A spammer could locate the e-mail relay and use it as a spam amplifier by forwarding e-mail addressed to	Critical – .87	Critical .87	Critical – 100	76 – Critical

Vulnerability	Realizable Threats	Impact	Example Outcomes	Vulnerability Value	Threat Value	Impact Value	Risk
		from high-volume UCE traffic. E-mail server could be blacklisted, with the result that some remote e-mail systems will not accept e-mail from the relay.	multiple users. Multiple RBL operators would likely blacklist the server. The server may experience poor performance due to the spam load. Some spam recipients may determine that the organization is the source of the spam and attempt to take action against the organization.				
Postfix denial of service attack possible for version 1.1.12 and earlier.	Denial of service attack	Denial of service. Cause degradation of performance or potentially completely disable SMTP service. Loss of business productivity. Loss of IT productivity	Loss of service until condition is corrected.	Medium – 0.37	Low – 0.12	Medium – 1	.044 – Low
Postfix environment security may not be secured optimally	Attacker compromise	Potential for an attacker who has already compromised Postfix to gain elevated privileges on the server. Potential disclosure of confidential information, potential loss of confidence in organization by clients, potential	In the unlikely event that an attacker were to break out of the Postfix system using a buffer overrun or other attack, he could launch an attack against the rest of the e-mail relay, resulting in the outcomes discussed above.	Medium – .37	Critical – .87	Critical – 100	32 – Critical

Vulnerability	Realizable Threats	Impact	Example Outcomes	Vulnerability Value	Threat Value	Impact Value	Risk
		damage to organization's credibility, potential for opening additional vulnerabilities, business and IT staff productivity loss, potential re-allocation of system resources by attacker for other illegal purposes					
Postfix may not be configured correctly to implement its normal function of providing inbound and outbound mail relaying.	Operator or Administrator Error	The organization depends on e-mail for its operation. Regardless of how well secured the server may be, if it does not perform its function correctly, the organization has experienced a denial of service.	Misconfiguration may cause the e-mail relay to fail to deliver e-mail messages normally. The organization would experience loss of service and possibly loss of confidence by its clients.	Critical – .87	High – .62	High – 10	5.4 – High

Discussion and Summary of Identified Risks

The realization of a threat causes an impact, but threats generally cannot be mitigated directly – they are a constant presence. To mitigate risk, the vulnerabilities must be eliminated or mitigated by compensating controls. The audit will focus on vulnerabilities that translate into high and critical risks.

The following table summarizes the vulnerabilities and the resulting level of risk according to the analysis presented above. In cases where the same vulnerability results in different levels of risk through more than one threat, the highest risk is used. The table also includes a reference column. These references will be used in the audit checklist steps, in Section 2, to refer to the analysis in this section.

Table 7 – Pre-audit risk by vulnerability

Reference	Vulnerability	Pre-audit Risk
V1	Dependence on physical environment to be able to operate	10 - High
V2	Physical access	23 - High
V3	Backup media may be corrupted or unavailable when needed (included as a best practice)	0.10 - Low
V4	System malfunctions may not be detected timely	54 - Critical
V5	System changes may not be detected timely	54 - Critical
V6	System requires proper communication with DNS server, default gateway and network switch, system requires proper function of NAT on firewall	5.4 - High
V7	SANS Top 20 – RPC vulnerability	76 - Critical
V8	SANS Top 20 – General UNIX/Linux authentication – Accounts with no passwords or weak passwords	76 - Critical
V9	SANS Top 20 – Clear text services	76 - Critical
V10	SANS Top 20 – Secure Shell	76 - Critical
V11	SANS Top 20 – Misconfiguration of enterprise services NIS/NFS	76 - Critical
V12	SANS Top 20 – Open Secure Sockets Layer SSL	76 - Critical
V13	Other operating system patches may not be current	54 - Critical
V14	Other unnecessary services may be enabled	54 - Critical
V15	E-mail encapsulates almost anything and bypasses most network controls	76 - Critical
V16	SMTP does not check source addresses	54 - Critical
V17	E-mail relay could operate as an open relay	76 - Critical
V18	Postfix environment may not be secured optimally	32 - Critical

V19	E-mail relay may not correctly perform its normal function	5.4 - High

Nearly all vulnerabilities identified for this system resulted in a critical risk. (Again, this evaluation does not consider how well the system will actually mitigate these risks.) A large number of the impacts were determined to be critical because the e-mail relay is responsible for a business function that is critical to timely information flow. In addition, it has the potential for disclosing confidential information or otherwise damaging the credibility and integrity of the business.

The risk assessment shows the highest risk occurs in the following categories:

- Physical environment
- Unauthorized access by physical access, weak passwords, or a compromise by an attacker resulting in elevated privileges
- Failure to detect security problems in time to prevent damage
- Problems inherent with e-mail, including viruses, disclosure of confidential information, UCE (spam), and social-engineering attacks

Control Objectives

Controls are the mechanism used to mitigate risks by reducing or eliminating vulnerabilities. Each control in the checklist developed in Section 2 has a specific objective to accomplish and considers well-established security principles, including defense in depth, least privilege, and separation of function.

Defense in depth is one of the key principles that are used to establish best practices in security.

> "Defense in depth follows the premise that there is no single solution to network security that makes a network completely secure. Instead, there is the more practical and effective practice of establishing several layers of security so that an intruder would have to navigate and compromise several layers of devices and policies in order to actually and fully compromise a network without being noticed. [6]

For example, if an attacker were able to disable the firewall, a properly secured e-mail relay would offer substantial resistance of its own, making the attacker's job much more difficult.

Least privilege is another key principle. Each user and system should have only the privileges necessary to do the required work. This minimizes the damage that

[6] Rassmussen, Scott. "Centralized Network Security Management: Combining Defense In Depth with Manageable Security." 29 Jan. 2002. URL: http://www.sans.org/rr/practice/central_netsec.php (18 Oct 2003).

can occur either intentionally, if an account or computer is compromised, or accidentally, if a legitimate user or system does something unexpected. One person should not be able to access and modify enough things to circumvent controls and procedures. Other systems should not have privileges on the e-mail relay and vice versa.

Compartmentalization, or the separation of function, is yet another important security principle. If a system is compromised, less damage will be done if it has limited functionality. For example, less damage would be done with a compromised server that only handles e-mail as opposed to a server that handles e-mail, stores all of a company's files, and hosts the company's web site. The e-mail relay is a good example of compartmentalization because it has only one business function.

The areas to be considered for developing controls are the same as the areas identified for risk. In addition, controls are added for the audit process to help ensure the integrity of the audit. In each of the areas the audit checklist will consider the specific ways that the general objectives listed below can be accomplished by testing the specific vulnerabilities identified above.

Table 8 – Summary of control objectives

Control Category	General Objective
Audit Process Controls	Ensure the success of the audit. Obtain permission for the audit. Establish management expectations about what the audit will deliver. Validate the scope of the audit, the risk evaluation, and development of audit controls by verifying that the assumptions used were correct.
Environmental Controls	Ensure that the environment of the server will support uninterrupted operation and prevent unauthorized physical access.
Network Controls	Protect the server from unwanted and unnecessary network traffic, ensure that the surrounding environment cooperates with the server to provide the e-mail relay function securely, and ensure that the network and surrounding systems provide the operational information necessary to operate effectively.
Linux Operating System Controls	Ensure that the operating system protects the server from unwanted and unnecessary network traffic, ensure that the server can defend itself against attack if surrounding defenses fail, and ensure that the server provides the information necessary to operate effectively.
Postfix Application	Ensure that the Postfix application protects the internal e-mail system from unwanted e-mail, ensure that it protects itself

Controls	against attacks that network defenses and operating system defenses cannot limit, and ensure that it provides the operational information necessary to operate effectively.
Operational Controls	Ensure that operational policies and procedures facilitate the reliable and secure operation of the e-mail relay (or its replacement) so that it can continue to provide the function for which it was designed. Ensure that problems are detected and resolved effectively and timely.

The Current State of Practice

In evaluating the current state of practice, the first step was to research standards for information security auditing. The following standards are widely used and contain a great deal of information. Unfortunately, they proved to be much too broad in scope and high level to be of use in developing the specifics of this audit.

- COBIT (URL: http://www.isaca.org/cobit.htm) (ISACA requires registration for access. Increasing levels of membership provide increased access.)
- FISCAM (URL: http://www.gao.gov/special.pubs/ai12.19.6.pdf)
- ISO 17999 and BS 7799 (URL: https://www.bspsl.com/secure/iso17799software/cvm.cfm) (available for purchase, not freely accessible)

The next step was to search for audits of systems that were similar, with the assumption that the underlying technologies, such as the network and the Linux operating system, would present similar requirements for auditing irrespective of the application they host. Similarly, a search was conducted for audits of e-mail systems. The SANS Reading Room (URL: http://www.sans.org/rr) and GIAC posted practicals (URL http://www.giac.org/cert.php) are known to be rich sources of such information.

Darrin Wassom wrote an excellent paper on auditing a distributed IDS[7] that was used for items related to the audit process and Linux security. Filipe Custódio wrote a paper on auditing Microsoft Exchange[8], which was used to research the state of practice for auditing e-mail systems.

[7] Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003)
[8] Custódio, Filipe. "Auditing Microsoft Corporate e-mail Solutions (Exchange 5.5 and Outlook 2000)." Sep. 2001. URL: http://www.giac.org/practical/Filipe_Custodio_GSNA.zip (4. Oct. 2003).

The SANS top twenty list[9] is always relevant to security. Specific checklist items were developed to address the items from the list that could affect the e-mail relay.

Google was used to search for additional checklists by using many combinations of terms such as audit, information, security, checklist, SMTP, Postfix, e-mail, and Linux. Other terms were used to find information related to specific risks. The following checklist was used in part for this audit.

- "Physical Security Audit Checklist." URL: http://www.knowledgeleader.com/iafreewebsite.nsf/content/TechnologyAuditPhysicalSecurityAuditChecklist?OpenDocument (19 Oct. 2003).

As the focus moved from the more general issues of auditing to the details of this specific system, the amount of available information decreased. General information about information systems security auditing is abundant and easy to locate. Information about auditing Linux systems is available, but requires more research to uncover. Research about auditing Postfix-based relays has not produced any useful results. Nevertheless, specific information about Postfix security was available and checklist items were developed from them.

The Postfix documentation page (URL: http://www.postfix.org/docs.html) has links to extensive information about all aspects of Postfix. The Postfix configuration files that are installed on the system in the /etc/postfix directory are heavily commented and are a significant source of information about how various settings affect the operation and security of the system. Richard Blum wrote an excellent book on Postfix,[10] which was used as reference for many of the fine points of Postfix security.

Details needed for developing specific checklist items required further research. Google and Ask Jeeves searches turned up several useful items:

- "LINUX+ ~ Chapter 7 ~ Linux Installation." URL: http://www.mullensystems.com/~john/ebook/chapter_07.htm (25 Oct. 2003).
- "Listing 2. Generating Messages for All Facilities at Each Priority." URL: http://www.linuxjournal.com/modules.php?op=modload&name=NS-lj-issues/issue92&file=5476l2 (19 Oct 2003).
- "Nmap Network Security Scanner Man Page." URL: http://www.insecure.org/nmap/data/nmap_manpage.html (5 Nov. 2003).
- Bauer, Mick. "Issue 92: Paranoid Penguin: syslog Configuration." 1 Dec. 2001. URL: http://www.linuxjournal.com/article.php?sid=5476 (19 Oct. 2003).

[9] "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0. 8 Oct. 2003. URL: http://isc.sans.org/top20.html#u1 (11 Oct. 2003).
[10] Blum, Richard. Postfix. Indianapolis: Sams Publishing, 2001.

- Bauer, Mick and de Winter, Brenno. “Using Postfix for Secure SMTP Gateways.” 13 Sep. 2000. URL: http://www.postfix.org/linuxjournal.200010/4241.html (26 Oct. 2003)
- Eychenne, Herve. “Iptables(8).” man page. Redhat 9.0. 9 Mar. 2002.
- Kurz, Christian. “LINUX2 – shell script to set up a Postfix chroot jail for Linux.” 1 Feb. 2002. URL: http://orange.kame.net/dev/cvsweb.cgi/postfix/examples/chroot-setup/LINUX2?rev=1.1.1.5&cvsroot=apps (26 Oct. 2003).
- Russell, Rusty. “Linux iptables HOWTO.” 29 Sep. 1999. URL: http://www.linuxguruz.com/iptables/howto/iptables-HOWTO.html (20 Oct 2003).

Section 2 – Audit Checklist

Conventions

The risk evaluation that was given in Section 1 determined how likely risks are to actually occur and described the consequences that could result. The measurement of the risk directly translates to the importance of eliminating or compensating for the underlying vulnerability. The risk evaluation includes details about the consequences associated with the various risks. The analysis is included in this section by reference.

The description of the risk in each checklist step (except for Audit Process Controls) provides a reference to Table 7 – Pre-audit risk by vulnerability. It also includes the level of risk that the step addresses, which was determined by the risk evaluation in Section 1. Items with high and critical risks were chosen for testing. Each step in the checklist addresses one or more of these vulnerabilities and has references to the corresponding items in that table.

Each step has a section for compliance. The compliance section contains a statement indicating whether compliance is binary (strictly pass or fail) or other criteria are to be used for evaluating compliance. If compliance is binary, the remainder of the compliance section contains one or more assertions; if the test shows all the assertions are true, the audit step passes.

Each audit step is either objective or subjective. Objective tests do not require judgment on the part of the auditor. In addition, a test of either type may also be a stimulus-response test, where some action is performed on the system and the response of the system is observed. Issuing commands that only reveal the state of the system are not actions in this context.

System commands are in bold courier new font, for example:

```
rpm –q redhat_release
```

System responses are in normal courier new font, for example:

```
redhat-release-9-3
```

Sanitized information will have actual data replaced by the character “x”. Character replacement is not necessarily on a character-by-character basis. For example:

> “www.nist.gov” may become “xxxx.xxxx.gov.”

All tests are run directly on the e-mail relay unless otherwise noted or obvious from the context.

Checklist

Audit Process Controls	Ensure the success of the audit. Obtain permission for the audit. Establish management expectations about what the audit will deliver. Validate the scope of the audit, the risk evaluation, and development of audit controls by verifying that the assumptions used were correct. (Because this audit is a self-audit and the organization is small, the administrative and organizational controls are greatly abbreviated. Larger organizations probably would need to expand this section and use a more formal approach.)

AUDIT STEP - 1. Discuss need for, scope of, and resources required for audit with management and obtain authorization to conduct audit.
Reference: Personal experience.
Control Objective: Ensure that success of the audit is not jeopardized by lack of communication.
Risk: If management does not understand and agree with the need for the audit and the resources required to conduct it, the administrator may not be able to complete the audit because of subsequent management decisions. Obtaining permission to conduct the audit is critical to prevent negative consequences directed toward the administrator.
Compliance: Compliance is binary. Management understands the need for the audit, commits resources, and gives permission to proceed. (If any item in this step does not comply, the audit may not proceed.)
Testing: • Management agrees that the audit is necessary. • Management commits resources to complete the audit. • Management gives permission to proceed with the audit.
Test Type: Objective

AUDIT STEP - 2. Discuss findings and recommendations with the organization's management during the audit and after completion of the audit.
Reference: Checklist. Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003). 13.
Control Objective: If conditions are uncovered by the audit that result in immediate changes, the findings must be reported irrespective of the changes.
Risk: The integrity of the audit is compromised if any findings are not reported.
Compliance: Compliance is binary. All audit findings are reported.

Testing: • Report all audit findings, irrespective of corrective changes made during the audit.
Test Type: Objective

AUDIT STEP - 3. Determine what documentation exists for the e-mail relay. Locate and organize all system documentation and network diagrams. If documentation does not exist, then it will need to be developed prior to the audit.
Reference: Checklist. Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003).
Control Objective: Documentation is available to support the audit.
Risk: System documentation is critical to understanding the system and how it interacts with the other systems in the network to provide its function. Without proper documentation, it is unlikely that a sufficient understanding of the system can be achieved. This understanding is essential to a successful audit.
Compliance: Compliance depends on the availability and quality of documentation. Documentation is available and adequate for auditing the system.
Testing: Obtain the following items or create them if necessary: • Network diagram • Description of system and function • System configuration details • System documentation
Test Type: Subjective

AUDIT STEP - 4. Reboot server prior to testing it.
Reference: Personal experience.
Control Objective: Make sure the server is operating normally.
Risk: Some services may have been started manually, stopped manually, or stopped because of some malfunction. Some running configurations may have been changed but not saved. Some startup configurations may have been changed since the last startup. If the audit is performed against the server without rebooting, the findings of the audit may not be valid following subsequent reboots.
Compliance: Compliance is objective. The server has been rebooted prior to testing the server. Results of the uptime command verify that reboot has occurred.
Testing: • Determine current uptime for server prior to reboot:

○ **uptime** • Reboot the server. Issue the following commands: ○ **shutdown –r now** • Determine uptime for server after reboot: ○ **Uptime**
Test Type: Objective – Stimulus Response

AUDIT STEP - 5. Test the pre-audit assertions given in Section 1.
Reference: Personal experience.
Control Objective: Ensure that the scope of the audit, the risk evaluation, and the development of audit controls are valid. This step is intended to make sure that the items tested were not installed as packages during the original install or installed as packages later.
Risk: Specific versions of software were given as inputs to the audit process. In addition, specific software packages were stated to be not present. The risks and audit controls were developed based on these assumptions. If the assumptions turn out to be false, then the evaluation of risk is not valid and therefore the audit is not valid.
Compliance: Compliance is binary. (Absolutely proving that no executable on the system could compile code would be difficult. The absence of the gcc compiler will be taken as evidence that the development package was not installed.) All of the following conditions are true: • **rpm -q redhat-release** indicates Red Hat 9.0 • **postconf mail_version** indicates version 1.1.12 • **rpm -q sendmail** indicates the package is not installed • **rpm -q httpd** and **rpm -q apache** indicate the packages are not installed • **rpm -q bind** indicates the package is not installed • **rpm -q net-snmp** indicates the package is not installed. • **rpm -q gcc** indicates the package is not installed. • **rpm -q Xfree86** indicates the package is not installed. • **netstat -l** shows nothing is listening on ports 53, 80, 161 and 6000-6063.
Testing: Run the following commands and observe the results. • **rpm -q redhat-release** • **postconf mail_version** • **rpm -q sendmail** • **rpm -q httpd** (-and-) **rpm -q apache** • **rpm -q bind** • **rpm -q net-snmp** • **rpm -q gcc**

• `rpm -q Xfree86` • `netstat –l`
Test Type: Objective

Environmental Controls	Ensure that the environment of the server will support uninterrupted operation and prevent unauthorized physical access.

AUDIT STEP - 6. Determine if physical access is adequately controlled.
Reference: • Checklist. “Physical Security Audit Checklist.” URL: http://www.knowledgeleader.com/iafreewebsite.nsf/content/TechnologyAuditPhysicalSecurityAuditChecklist?OpenDocument (19 Oct. 2003). • Personal experience.
Control Objective: Prevent unauthorized physical access to the e-mail relay and its supporting systems.
Risk: (Reference: V2 – High) Physical access to computers and network equipment allows an attacker to disrupt service or gain access to the system with elevated privileges.
Compliance: Compliance is evaluated subjectively and includes the following items: • Doors are locked when the computer room is not occupied. • There is a process for issuing keys to the computer room. • Door hinges are not removable from outside the computer room. • Computer room is not marked. • Guest access to the computer room is supervised.
Testing: Answer the following questions. • Are doors locked? • Are keys changed on a regular basis? • Is the process for issuing keys documented? • Who has keys? • Are door hinges removable from outside the computer room? • Are openings other than doors accessible? • Do walls adequately protect the facility? • Does the computer room have any markings or signs indicating its purpose? The auditor should look for any additional ways that unauthorized physical access could be obtained.
Test Type: Subjective

AUDIT STEP - 7. Determine if the physical environment is adequately protected.
Reference: • Research. "Physical Security Audit Checklist." URL: http://www.knowledgeleader.com/iafreewebsite.nsf/content/TechnologyAuditPhysicalSecurityAuditChecklist?OpenDocument (19 Oct. 2003). • Personal experience.
Control Objective: Maintain the environment within acceptable parameters for proper operation of the system. Monitor the system and take corrective action if the environment is threatened.
Risk: (Reference: V1 – High) "If any of the potential threats become a reality without the proper detection, prevention, and monitoring systems in place, significant damage to hardware could occur resulting in loss of operational capability."[11]
Compliance: Compliance is evaluated subjectively over the range of issues listed below. • Fire protection is in place and adequate. • A properly functioning UPS powers the system. • The system is cooled by a properly maintained HVAC system. • Thermostat is set properly. • Automatic and manual fire alarms are present.
Testing: • Document fire protection types and location. • Verify system is plugged into UPS. • Run UPS test cycle and observe results. • Verify that HVAC is working. • Observe thermostat setting. • Observe location of automatic and manual fire alarms.
Test Type: Subjective

Network Controls	Protect the server from unwanted and unnecessary network traffic, ensure that the surrounding environment cooperates with the server to provide the e-mail relay function securely, and ensure that the network and surrounding systems provide the operational information necessary to operate effectively.

[11] "Physical Security Audit Checklist." URL: http://www.knowledgeleader.com/iafreewebsite.nsf/content/TechnologyAuditPhysicalSecurityAuditChecklist?OpenDocument (19 Oct. 2003).

AUDIT STEP - 8. Test network input controls listed in Section 1 regarding unsolicited Internet traffic.
Reference: • Research: "Nmap Network Security Scanner Man Page." URL: http://www.insecure.org/nmap/data/nmap_manpage.html (5 Nov. 2003). • Personal experience.
Control Objective: Ensure that the e-mail relay only accepts unsolicited Internet communications as planned.
Risk: (References: V7, V8, V9, V10, V11, V12, V13, V14 – All critical) If communication is successful on ports and protocols that are not planned, defense in depth is compromised. There would be one less barrier to prevent an attacker from compromising the e-mail relay.
Compliance: Compliance is binary. Nmap shows that traffic to the Internet address associated with the e-mail server will only respond to TCP port 25. All other TCP traffic and all UPD traffic are ignored.

Testing: Use nmap from a different computer at a location outside the firewall to determine which ports and protocols respond. Use the published DNS name for the server. Log the results to files.
• Test all ports for TCP connect:
`nmap –v –sS –r –P0 –p 1-65535 –oN ext_nmap_TCP.txt relay.xxxx.com`
• Test all ports for UDP:
`nmap –v –sU –r –P0 –p 1-65535 –oN ext_nmap_UDP.txt relay.xxxx.com`

Test Type: Objective – Stimulus Response

AUDIT STEP - 9. Test network input controls listed in Section 1 regarding unsolicited internal network traffic.
Reference: • Research: "Nmap Network Security Scanner Man Page." URL: http://www.insecure.org/nmap/data/nmap_manpage.html (5 Nov. 2003). • Personal experience.
Control Objective: Ensure that the e-mail relay only accepts unsolicited internal network communications as planned.
Risk: (References: V7, V8, V9, V10, V11, V12, V13, V14 – All critical) If communication is successful on ports and protocols that are not planned, defense in depth is compromised. There would be one less barrier to prevent an attacker from compromising the e-mail relay.
Compliance: Compliance is binary. Nmap shows that traffic to the Internet address associated with the e-mail server will only respond to TCP port 22, TCP

port 25, and UDP port 123. All other TCP and UDP traffic is ignored. (The relay will respond to UDP port 53, but only from DNS servers).

Testing: Use nmap from a computer (other than a DNS server) on the internal network to determine which ports and protocols respond. Use the internal IP address for the server. Log the results to files.

- Test all ports for TCP connect:

  ```
  nmap –v –sS –r –P0 –p 1-65535 –oN int_nmap_TCP.txt 192.168.10.2
  ```

- Test all ports for UDP:

  ```
  nmap –v –sU –r –P0 –p 1-65535 –oN int_nmap_UDP.txt 192.168.10.2
  ```

Test Type: Objective – Stimulus Response

AUDIT STEP - 10. Test network controls with regard to unexpected communication.

Reference: Personal experience.

Control Objective: Determine if the e-mail relay is susceptible to denial of service or compromised by unexpected traffic.

Risk: (References: V10, V13, V14 – All Critical) The e-mail relay could be compromised, possibly with elevated privileges, or become unresponsive due to unexpected traffic on ports that allow communication.

Compliance: Compliance is subjective. The server cannot be tested against an infinite number of possibilities. However, Nessus should not find any significant vulnerabilities. The e-mail relay's logs should show extensive entries in response to an SMTP attack by Nessus. The IDS logs may record some aspects of the Nessus activity.

Testing: Run Nessus from another host on the internal network to attack the e-mail relay. (Details of running Nessus are outside the scope of this audit.)

- Update the Nessus plug-ins:
  - `nessus-update-plugins`
- Start Nessus and configure the options as follows (other options are defaults):
  - On the Plugins tab:
    - Enable all but dangerous plugins
  - On the Scan Options tab:
    - Remove Ping options
    - Set to scan specified ports
    - Set to include UDP
  - On the Scan Options tab:
    - Set to scan ports 22, 25 and 123 only
  - On the Target tab

▪ Enter the address of the e-mail relay • Run the scan. • Observe the results to see if Nessus found any vulnerabilities. • Inspect the e-mail relay's logs for activity caused by Nessus. • Inspect the IDS's logs for activity caused by Nessus. • Analyze the test and the results.
Test Type: Subjective – Stimulus Response

AUDIT STEP - 11. Verify proper communication with DNS servers, default gateway and network switch.
Reference: Personal experience.
Control Objective: Determine if the e-mail relay has access to vital network services and is communicating with the correct devices.
Risk: (Reference V6 – High) The server requires these services. The server could be obtaining them from a test environment or otherwise incorrect sources. The server could be inadvertently attached to a test or temporary switch.
Compliance: Compliance is binary. The server is configured to use DNS servers at 192.168.xxx.xxx and 192.168.xxx.xxx for name resolution. The server is configured to use 192.168.xxx.xxx for the default gateway. The server is connected to the correct switch.
Testing: • Inspect the DNS configuration file /etc/resolv.conf. • Inspect the network configuration file /etc/sysconfig/network. • Trace the Ethernet connection from the server to the switch. Alternatively, during a non-critical business period, temporarily disconnect the server from the network switch and observe that it is no longer able to communicate.
Test Type: Objective

AUDIT STEP - 12. Verify proper NAT translation by firewall for e-mail relay.
Reference: Personal experience.
Control Objective: Determine if firewall is correctly performing NAT for the internal and external addresses of the e-mail server.
Risk: (Reference V6 – High) The server requires NAT to perform its function. The firewall could be configured incorrectly, routing inbound SMTP traffic to a test server or another device. (NOTE: this is not likely in a production environment where the server has been performing correctly.)
Compliance: Compliance is binary. The firewall is configured to perform NAT from the e-mail relay's external IP address to its internal IP address.
Testing: • Inspect relevant entries in firewall configuration. • Observe normal SMTP traffic inbound from and outbound to external

hosts.
Test Type: Objective

AUDIT STEP - 13. Determine if logging is configured properly on the e-mail relay and on the remote logging server.
Reference: • Research: Bauer, Mick. "Issue 92: Paranoid Penguin: syslog Configuration." 1 Dec. 2001.URL: http://www.linuxjournal.com/article.php?sid=5476 (19 Oct. 2003). • Research: "Listing 2. Generating Messages for All Facilities at Each Priority." URL: http://www.linuxjournal.com/modules.php?op=modload&name=NS-lj-issues/issue92&file=5476l2 (19 Oct 2003).
Control Objective: Make sure that messages are properly logged on the e-mail relay and on the IDS (remote log server).
Risk: (References: V4, V5 – Both Critical) Correct logs are essential to identify system malfunctions and changes. An attacker may alter logs after compromising a system; the remote log is more reliable in such cases, unless the remote logging machine also has been compromised.
Compliance: Compliance is binary. Each test message is logged in the correct facility according to the logging configuration in /etc/syslog.conf on each computer.
Testing: • Inspect the configuration file /etc/syslog.conf on the relay and the IDS. • Use the following script:[12] • Observe results in e-mail relay's logs and in remote logs.

```
#!/bin/bash
#
# Script to generate one log message per
# priority level per facility
#
for i in {auth,authpriv,cron,daemon,kern,lpr,mail,
mark,news,syslog,user,uucp,local0,local1,local2,
local3,local4,local5,local6,local7}

do
  for k in {debug,info,notice,warning,err,crit,
            alert,emerg}
  do
    logger -p $i.$k "Test message, facility $i
                     priority $k"
  done
done
```

[12] "Listing 2. Generating Messages for All Facilities at Each Priority." URL: http://www.linuxjournal.com/modules.php?op=modload&name=NS-lj-issues/issue92&file=5476l2 (19 Oct 2003).

Test Type: Objective – Stimulus Response

Linux Operating System Controls	Ensure that the operating system protects the server from unwanted and unnecessary network traffic, ensure that the server can defend itself against attack if surrounding defenses fail, and ensure that the server provides the information necessary to operate effectively.

AUDIT STEP - 14. Verify that logs are rotated correctly on the e-mail relay.
Reference: Checklist. Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003).
Control Objective: Logs are preserved for an appropriate length of time and deleted before they consume too much disk space.
Risk: (References: V4, V5 – Both Critical) "Log files that get too big are difficult to analyze and review. Log files should be kept for a minimum of 4 weeks in case further review is needed or even correlation of similar events needs to be conducted."[13]
Compliance: Compliance is binary. Wassom gives the following criteria:[14] The following items must be configured in /etc/syslog.conf: • Rotate log files weekly. • Logs are kept 4 weeks. • Create new log after rotating old logs. • wtmp files are rotated monthly and kept for 2 months.

Testing: Wassom gives the following test procedure:[15]
 	
• Examine /etc/syslog.conf to determine log rotation schedule.
  ○ **cat /etc/logrotate.conf** (-or-)
  ○ **more /etc/logrotate.conf**
• Verify that logrotate is included in /etc/cron.daily directory.
  ○ **ls –l /etc/cron.daily**

Test Type: Objective

[13] Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003).
[14] Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003).
[15] Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003).

AUDIT STEP - 15. Verify that the operating system patches are current.
Reference: • Checklist. Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003). • Personal experience.
Control Objective: Protect the system against newly discovered vulnerabilities.
Risk: (Reference: V13 – Critical) New vulnerabilities are continually discovered. Failing to install updates as soon as they are available leaves systems open to exploits.
Compliance: Compliance is variable. Some exceptions are expected, but a large number of available patches that have not been installed could indicate problems with policy or discipline. A few recently released patches that have not been installed are acceptable unless they involve critical services or correct critical vulnerabilities.

Testing: Wassom gives the following test procedure:[16]
• Compare output with the latest packages available from the Red Hat errata pages.
  ○ `rpm –qa > package.txt`
• If the machine has been registered with the Red Hat Network, run the command:
  ○ `up2date –l`

Test Type: Subjective

AUDIT STEP - 16. Verify xinetd services are disabled.
Reference: • Checklist. Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003). • Personal experience.
Control Objective: Make sure xinetd is not used to start any services.
Risk: (Reference: V9, V14 – Critical) Xinetd is used to start services on demand that do not run as daemons. Xinetd services are not needed on this system. Their presence would increase the risk that an attacker could gain additional useful information from the system and would add the risk that the services could be exploited directly.
Compliance: Compliance is binary. The /etc/xinetd.conf does not exist. The chkconfig command reveals the daemon is not running.

[16] Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003).

Testing:

- The following command should show that the xinetd.conf file is not present.
  - **ls /etc/xinetd.d**
- Ensure that xinetd is totally disabled:
  - **chkconfig --list xinetd**

Test Type: Objective

AUDIT STEP - 17. Determine if the firewall on the e-mail relay is properly configured and enabled.

Reference:

- Research: Russell, Rusty. "Linux iptables HOWTO." 29 Sep. 1999. URL: http://www.linuxguruz.com/iptables/howto/iptables-HOWTO.html (20 Oct 2003).
- Research: Eychenne, Herve. "Iptables(8)." man page. Redhat 9.0. 9 Mar. 2002.
- Personal experience.

Control Objective: Ensure that the e-mail relay only accepts unsolicited internal network communications as planned. Previous testing has demonstrated the ability of the server to respond properly to network inputs. One purpose of this test is to differentiate between enforcement of controls by the firewall and the enforcement of controls by restricting the services that are running. Using both types of controls adds to defense in depth.

Risk: (References: V7, V8, V9, V10, V11, V12, V13, V14 – All critical) If communication is successful on ports and protocols that are not planned, defense in depth is compromised. There would be one less barrier to prevent an attacker from compromising the e-mail relay.

Compliance: Compliance is binary. The local firewall enforces the internal network controls discussed in Section 1 with respect to unsolicited internal network traffic. The firewall permits the following:

- TCP port 25 (SMTP) from anywhere
- TCP port 22 (SSH) from the internal network
- UDP packets port 123 (NTP) from the internal network and specific external hosts used for time synchronization
- UDP packets port 53 (DNS) from the internal DNS servers

The firewall denies everything else except localhost traffic.

Testing:

- Inspect the firewall configuration. Use the command to capture the configuration (this is the running configuration – if iptables is stopped the output will not show any firewall rules):

○ **`iptables -L -v >fwconfig.txt`**
Test Type: Objective

AUDIT STEP - 18. Verify that only necessary daemons are running on the system.
Reference: • Checklist. Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003). • Research: "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0. 8 Oct. 2003. URL: http://isc.sans.org/top20.html#u1 (11 Oct. 2003).
Control Objective: Only necessary daemons are to be running on the system. To address a specific SANS Top 20 issue, RPC services are not required on this computer.
Risk: (References: V7, V9, V14 – all critical) The presence of unnecessary services increases the risk that an attacker could gain additional useful information from the system and introduces the risk that the services could be exploited directly.
Compliance: Compliance is binary. The only daemons that are running are smtpd, sshd, ntpd and syslogd.
Testing: • Use the netstat command to see which daemons are running on which ports: ○ **`netstat -atu`** • Use the lsof command to see the network sockets that are open and the associated processes: ○ **`lsof -i +M`**
Test Type: Objective

AUDIT STEP - 19. Verify that OpenSSH is being used and is the latest version.
Reference: • Checklist. Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003). • Research: "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0. 8 Oct. 2003. URL: http://isc.sans.org/top20.html#u1 (11 Oct. 2003). • Personal experience.
Control Objective: OpenSSH is being used and is the latest version.

Risk: (References: V9, V10 – both critical) Besides the risks discussed in Audit Step – 15 regarding keeping patches current, OpenSSH is on the SANS Top Twenty list, which recommends the following:

> Upgrade to the most recent version of either OpenSSH or SSH. Or if SSH or OpenSSH came installed with your operating system, retrieve the latest patches from your operating system vendor. If you use OpenSSL, be sure to use the latest version of those libraries.[17]

Compliance: Compliance is binary. Connecting remotely for this test shows the service is working. The netstat commands indicate that SSH is running and listening on default port 22. The command also reveals an established SSH connection between the relay and the host used to perform the test. The version of OpenSSH being used is the same as the latest RPM provided by Red Hat.

Testing:

- Connect to the e-mail relay using SSH from a remote host.
- Check to see if SSH is running:
  - `netstat -at | grep ssh`
- Determine the version of OpenSSH:
  - `ssh -V`
- Compare with the version of OpenSSH currently offered by Red Hat.

Test Type: Objective

AUDIT STEP - 20. Determine if OpenSSH is properly configured.

Reference:

- Checklist. Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003).
- Research: "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0. 8 Oct. 2003. URL: http://isc.sans.org/top20.html#u1 (11 Oct. 2003).

Control Objective: The configuration of OpenSSH complies with best practices.

Risk: (Reference: V10 – critical) According to SANS:

> While SSH is presented here as one of the Top 20 vulnerabilities, it is more the case that the mismanagement of SSH, specifically misconfiguration and the failure to apply updates and patches in a timely manner, account for its inclusion in this list.[18]

Compliance: Compliance is binary. The /etc/ssh/ssh_config file contains the

[17] "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0. 8 Oct. 2003. URL: http://isc.sans.org/top20.html#u1 (11 Oct. 2003).
[18] "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0. 8 Oct. 2003. URL: http://isc.sans.org/top20.html#u1 (11 Oct. 2003).

following (or provides the equivalent by default):

```
Host *
     ForwardAgent no
     ForwardX11 no
     RhostsAuthentication no
     RhostsRSAAuthentication no
     RSAAuthentication yes
     BatchMode no
     CheckHostIP yes
     StrictHostKeyChecking yes
     IdentityFile ~/.ssh/identity
     IdentityFile ~/.ssh/id_dsa
     IdentityFile ~/.ssh/id_rsa
     Port 22
     Protocol 2
     Cipher blowfish
     EscapeChar ~
```

The /etc/ssh/sshd_config file contains the following (or provides the equivalent by default):

```
Port 22
Protocol 2
ListenAddress 0.0.0.0
HostKey /etc/ssh/ssh_host_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_rsa_key
ServerKeyBits 768
LoginGraceTime 60
KeyRegenerationInterval 3600
PermitRootLogin no
IgnoreRhosts yes
IgnoreUserKnownHosts yes
StrictModes yes
X11Forwarding no
PrintMotd yes
KeepAlive yes
SyslogFacility AUTH
LogLevel INFO
RhostsAuthentication no
RhostsRSAAuthentication no
PasswordAuthentication yes
PermitEmptyPasswords no
Subsystem     sftp    /usr/libexec/openssh/sftp-server
```

Testing:

- Examine the /etc/ssh/ssh_config file:
  - **`cat /etc/ssh/ssh_config`**
- Examine the /etc/ssh/sshd_config file:

- **`cat /etc/ssh/sshd_config`**

Test Type: Objective

AUDIT STEP - 21. Determine if PAM password authentication is being used is being used for OpenSSH.

Reference: Checklist. Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003).

Control Objective: Verify that SSH is using PAM for authentication.

Risk: (Reference: V10 – critical) PAM (Pluggable Authentication Module) makes the authentication function available to applications in a consistent manner. It relieves the responsibility for writing high-quality secure authentication into each application. Applications using their own authentication schemes risk problems that may not be readily identified or fixed.

Compliance: Compliance is binary. The /etc/pam.d/sshd file contains the following:

```
auth     required     /lib/security/pam_stack.so service=system-auth
auth     required     /lib/security/pam_nologin.so
account  required     /lib/security/pam_stack.so service=system-auth
account  required     /lib/security/pam_access.so
account  required     /lib/security/pam_time.so
password required     /lib/security/pam_stack.so service=system-auth
session  required     /lib/security/pam_stack.so service=system-auth
session  required     /lib/security/pam_limits.so
session  optional     /lib/security/pam_console.so
```

Testing:

- Examine the /etc/pam.d/sshd file:
  - **`cat /etc/pam.d/sshd`**

Test Type: Objective

AUDIT STEP - 22. Determine if shadow passwords are enabled and the shadow file is protected.

Reference:

- Research: "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0. 8 Oct. 2003. URL: http://isc.sans.org/top20.html#u1 (11 Oct. 2003).
- Research: "LINUX+ ~ Chapter 7 ~ Linux Installation." URL: http://www.mullensystems.com/~john/ebook/chapter_07.htm (25 Oct. 2003).

Control Objective: Verify that shadow passwords are enabled and the shadow file is protected.

Risk: (Reference: V8 – critical) Users need access to the password file. Even

though the passwords are encrypted, if they are available in the password file, any user can attempt to determine the passwords using cracking tools. Shadow passwords move the encrypted passwords to a separate file to which users do not have access.

Compliance: Compliance is binary. Shadow passwords are used. Users other than root cannot access the file /etc/shadow.

Testing: The following procedure is from Linux+, Chapter 7:[19]

- Log on to the system as a regular non-root user.
- At the command line, type the following command:
  - **`$cat /etc/shadow`**
- If shadow passwords are enabled, you should receive the following message:
  - `$cat: /etc/shadow: permission denied`
- Issue the command:
  - **`$cat /etc/passwd`**
- The password field (the second field in each entry) should be set to x. This indicates that shadow passwords are being used.

Test Type: Objective – Stimulus Response

AUDIT STEP - 23. Determine if user accounts exist with empty password fields.

Reference: Checklist. Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003).

Control Objective: Ensure that no user accounts have empty password fields.

Risk: (Reference: V8 – critical) "A user account with an empty password is basically a wide open door. Many attackers look for default user accounts with no password."[20]

Compliance: Compliance is binary. The command used for listing the accounts produces no results.

Testing:

- Use the awk command to list any accounts that have empty password fields:
  - **`awk –F: '($2==""){print $1}' /etc/shadow`**

Test Type: Objective

AUDIT STEP - 24. Determine if UID 0 accounts exist other than root.

Reference: Checklist. Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003).

[19] Research: "LINUX+ ~ Chapter 7 ~ Linux Installation." URL: http://www.mullensystems.com/~john/ebook/chapter_07.htm (25 Oct. 2003).
[20] Checklist. Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003).

Control Objective: Verify that no UID 0 accounts exist other than root.
Risk: (Reference: V8 – critical) "Any account listed as UID 0 is considered a 'Super User' account. There is no need to have more than one account of this nature on a system. Accounts with UID 0 should be limited to only 'root' and only used when absolutely necessary."[21]
Compliance: Compliance is binary. The only account listed in the test below is root.
Testing: • Use the awk command to list accounts with UID 0: ○ **`awk -F: '($3==0){print $1}' /etc/passwd`**
Test Type: Objective

AUDIT STEP - 25. Determine if minimum password length and maximum password age are enforced.
Reference: • Checklist. Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003). • Personal experience.
Control Objective: Ensure that password policy enforced by the computer is consistent with best practices.
Risk: (Reference: V8 – critical) Passwords are easily cracked or guessed. Therefore, a good security policy should require passwords be a minimum of 8 characters and changed every 90 days. Passwords are often deployed as the first and last defense so it is critical to the security of a system to have a strong password policy.[22]
Compliance: Compliance is binary. The following parameters are defined: • `PASS_MAX_DAYS 90` • `PASS_MIN_LEN 8` The test shows that a new password with length of less than eight characters cannot be created. In addition, the test shows that dictionary words are not allowed and passwords are required to have a degree of complexity.
Testing: • Determine the minimum password length and maximum password length: ○ **`cat /etc/login.defs`** • Create a new user:

[21] Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003).
[22] Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003).

○ **`adduser foo`** • Using the **`passwd`** command, attempt to create a new password with length shorter than the minimum length allowed by the security policy. Attempt to create a new password with dictionary words and minimal complexity. • Remove the new account: ○ **`userdel foo`**
Test Type: Objective – Stimulus Response

AUDIT STEP - 26. Determine if unneeded user accounts are present.
Reference: Checklist. Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003).
Control Objective: Make sure unnecessary accounts are not on the system.
Risk: (Reference: V8 – critical) The goal here is to minimize exposure by reducing the number of user accounts that can be used for a particular system. There are many default user accounts that have easy to guess passwords. Removing any user account that is not needed for proper performance is necessary to reduce the risk of compromise.[23]
Compliance: Compliance is binary. The only user account on the system is "noc".
Testing: • Examine the /etc/passwd file for any unnecessary user accounts: ○ **`cat /etc/passwd`**
Test Type: Objective

AUDIT STEP - 27. Determine if NFS and NIS are installed.
Reference: Research: "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0. 8 Oct. 2003. URL: http://isc.sans.org/top20.html#u1 (11 Oct. 2003).
Control Objective: Ensure that NFS and NIS are not present on the system.
Risk: (Reference: V11 – critical) According to the SANS Top Twenty document: The security problems with both services, represented by the continuous issues discovered over the years (buffer overflows, DoS and weak authentication), made them a frequent target of attack. Besides the unpatched services that are still widely deployed, the higher

[23] Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003).

risks may be represented by the misconfiguration of NFS and NIS that will easily allow security holes to be exploited and accessed by users locally or remotely. [24]
Compliance: Compliance is binary. NFS and NIS (ypbind) are not present on the system.
Testing: • Run rpm to verify that NFS and NIS are not installed: ○ **`rpm -q nfs-utils`** (-and-) ○ **`rpm -q ypbind`**
Test Type: Objective

AUDIT STEP - 28. Determine if OpenSSL is a vulnerable version.
Reference: • Research: "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0. 8 Oct. 2003. URL: http://isc.sans.org/top20.html#u1 (11 Oct. 2003). • Personal experience
Control Objective: Make sure OpenSSL is not vulnerable to known attacks.
Risk: (Reference: V12 – critical) This issue is on the SANS Top Twenty list. According to SANS: Multiple vulnerabilities have been found in OpenSSL, of which the most serious are the set of 4 vulnerabilities listed in CAN-2002-0655, CAN-2002-0656, CAN-2002-0557, and CAN-2002-0659. These allow the remote execution of arbitrary code as the user of the OpenSSL libraries (which in some cases, such as 'sendmail', is the 'root' user).[25] Because of the severity of this vulnerability, a separate check is warranted in addition to the checklist step above that determines if the latest RPMs are installed. Releases of Red Hat RPMs sometimes lag behind releases from the corresponding packages' official support sites.
Compliance: Compliance is binary. The rpm command below shows the version of OpenSSL to be 0.9.7a or later.
Testing: • Run the rpm command to determine the latest version of OpenSSL: ○ **`rpm -q openssl`**
Test Type: Objective

[24] "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0. 8 Oct. 2003. URL: http://isc.sans.org/top20.html#u1 (11 Oct. 2003).
[25] "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0. 8 Oct. 2003. URL: http://isc.sans.org/top20.html#u1 (11 Oct. 2003).

Postfix Application Controls	Ensure that the Postfix application protects the internal e-mail system from unwanted e-mail, ensure that it protects itself against attacks that network defenses and operating system defenses cannot limit, and ensure that it provides the operational information necessary to operate effectively.

Some of the filenames in this section are specific to the configuration on this server and are not expected to be identical in other Postfix implementations. These files are specified in /etc/postfix/main.cf and in the output of the postconf command.

AUDIT STEP - 29. Determine if message size limits are functioning correctly.
Reference: Personal experience.
Control Objective: Ensure that messages greater than a specified size are logged and rejected (application control from Section 1).
Risk: (Reference: V15, V18 – both critical) Large e-mails can take a long time to transmit on slow connections. The primary purpose of message size limits is to prevent overwhelming hosts with slow connections. In addition, incoming messages that are too large could cause resource problems.
Compliance: Compliance is binary. Oversized messages are rejected and logged to /var/log/maillog.
Testing: • Send a message from a remote host with a 20MB attachment to postmaster@xxxxxxx.com. • Check the log /var/log/maillog on the server for indication of rejection.
Test Type: Objective – Stimulus Response

AUDIT STEP - 30. Determine if recipient-based message blocking works correctly.
Reference: • Research: "Postfix Configuration – UCE Controls." URL: http://www.postfix.org/uce.html (26 Oct 3003). • Personal experience.
Control Objective: Ensure that messages to specified users are logged and rejected. (Application control from Section 1).
Risk: (Reference: V15 – Critical) UCE is often sent to certain e-mail addresses frequently enough to establish a recognizable pattern. In addition, e-mail frequently is sent to former employees. Rejecting these at the gateway reduces traffic on the internal network and eliminates clutter in the logs, making them more readable.
Compliance: Compliance is binary. Messages to specified users are rejected

and logged to /var/log/maillog.

Testing:
• Go to the Postfix directory:
  ○ **`cd /etc/postfix`**
• Add the e-mail address test-reject@xxxxx.com to the file /etc/postfix/unkn_users.map.
• Create the database from the source file and reload Postfix:
  ○ **`postmap unkn_users.map`**
  ○ **`postfix reload`**
• Send a test message from a remote host to test-reject@xxxxxx.com. The remote location is required because the configuration allows relaying from internal sources irrespective of this control.
• Check the log /var/log/maillog on the server for indication of rejection.

Test Type: Objective – Stimulus Response

AUDIT STEP - 31. Determine if source-based message blocking works correctly.
Reference: • Research: Research: "Postfix Configuration – UCE Controls." URL: http://www.postfix.org/uce.html (26 Oct 3003). • Personal experience.
Control Objective: Ensure that messages from specified sources are logged and rejected (application control from Section 1).
Risk: (Reference: V15 – Critical) UCE is often sent from certain sources frequently enough to establish a recognizable pattern. Rejecting these at the gateway reduces traffic on the internal network from unwanted messages and eliminates clutter from the logs, making them more readable.
Compliance: Compliance is binary. Messages from specified sources are rejected and logged to /var/log/maillog.

Testing:
• Select a remote address from which to test.
• Go to the Postfix directory:
  ○ **`cd /etc/postfix`**
• Add the address to the file /etc/postfix/myspamlist.map
• Create the database from the source file and reload Postfix:
  ○ **`postmap myspamlist.map`**
  ○ **`postfix reload`**
• Send a test message from the host at the specified address to root@xxxxxxx.com. (The e-mail account must be temporarily configured to use the e-mail relay as the outgoing mail server. If the account uses an ISP's relay, this test will not work.)
• Check the log /var/log/maillog on the server for indication of rejection.

- Remove the blocked address from /etc/postfix/myspamlist.map.
- Create the database from the source file and reload Postfix:
  - **`postmap myspamlist.map`**
  - **`postfix reload`**

Test Type: Objective – Stimulus Response

AUDIT STEP - 32. Determine if RBL-based message blocking works correctly.

Reference:

- Research: "Postfix Configuration – UCE Controls." URL: http://www.postfix.org/uce.html (26 Oct 3003).
- Research: Blum, Richard. Postfix. Indianapolis: Sams Publishing, 2001. 311-312.
- Personal experience.

Control Objective: Ensure that messages are logged and rejected according to real-time blacklists (application control from Section 1).

Risk: (Reference: V15 – Critical) UCE is often sent from certain sources frequently enough to establish a recognizable pattern. RBLs attempt to identify these sources as quickly as possible and add them to a database. The e-mail relay uses three RBLs to drastically limit UCE from entering the internal network based on the determination of spam sources made by the list operators. If this control does not work (e.g. an RBL changed its URL or ceased operations), a lot of UCE would be allowed.

Compliance: Compliance is binary. Messages from sources identified in RBL databases are rejected and logged to /var/log/maillog.

Testing:

- Check the log /var/log/maillog on the server for messages being rejected by the RBLs that are specified in the configuration file /etc/postfix/main.cf.

Test Type: Objective

AUDIT STEP - 33. Determine if message blocking based on header checks works correctly.

Reference:

- Research: "Postfix Configuration – UCE Controls." URL: http://www.postfix.org/uce.html (26 Oct 3003).
- Research: Blum, Richard. Postfix. Indianapolis: Sams Publishing, 2001. 312-314.
- Personal experience.

Control Objective: Ensure that messages are blocked based on header content (application control from Section 1).

Risk: (Reference: V15 – Critical) Virtually identical UCE is often sent from multiple sources. They often have spoofed e-mail addresses or identical subject lines. RBLs may not identify these sources quickly enough. If this control does

not work, a lot of UCE would be allowed. Another use of this type of filtering is to block messages that use subject lines that are used by viruses such as Sobig.F. Prohibiting subject lines that are used by e-mails that are known to be dangerous increases defense in depth and could prevent some e-mail viruses from entering the network.
Compliance: Compliance is binary. Messages are blocked based on header checks and logged to /var/log/maillog.

Testing:
• Go to the Postfix directory:
  ○ **`cd /etc/postfix`**
• Add the following line to the file /etc/postfix/header_checks.regexp:
  `/^Subject:.*Test subject line reject.*/ REJECT`
• Send a test message from the host at the specified address to root@xxxxxxx.com.
• Check the log /var/log/maillog on the server for indication of rejection.

Test Type: Objective – Stimulus Response

AUDIT STEP - 34. Determine if executable extensions are blocked.
• **Reference:** Research: "Postfix Configuration – UCE Controls." URL: http://www.postfix.org/uce.html (26 Oct 3003). • Personal experience.
Control Objective: Ensure that messages with executable extensions are blocked (application control from Section 1).
Risk: (Reference: V15 – Critical) Many e-mail viruses and worms contain attachments with executable extensions. If executable attachments are allowed, the risk of being infected by a virus or worm increases. Even if virus detection software is used, there is always a chance that a virus or worm is newer than the signature files.
Compliance: Compliance is binary. Messages are blocked based on header checks and logged to /var/log/maillog. (This control is implemented using the file body_checks.regexp, in which are listed several extensions that are to be blocked. Extensions exe, com, and vbs are to be used for testing with the assumption that not all extensions need to be tested to verify the function.)
Testing: • Examine the file /etc/postfix/body_checks.regexp and observe the section that rejects messages containing executable extensions. • Send separate e-mails containing attachments with exe, com, and vbs extensions. • Observe the messages on the e-mail relay in /var/log/maillog for evidence that the messages were rejected.
Test Type: Objective – Stimulus Response

AUDIT STEP - 35. Determine if the e-mail relay is an open relay.
Reference: • Research: Blum, Richard. Postfix. Indianapolis: Sams Publishing, 2001. 204-205. • Personal experience.
Control Objective: Ensure that the e-mail relay is not an open relay (application control from Section 1).
Risk: (Reference: V17 – Critical) An open relay accepts mail from any source and forwards it to its destination. Spammers use open relays as spam amplifiers by sending messages to multiple recipients through open relays. The spammer can take advantage of someone else's bandwidth and make tracing the source of the spam very difficult. There are at least three risks related to open relaying: 1. The relay may be seen as a source of spam, which could damage credibility of the organization. 2. Spamming activity could greatly reduce resources available for other needs. 3. The organization's e-mail relay may become blacklisted, resulting in e-mail from the organization not being accepted on some systems.
Compliance: Compliance is binary. The test below shows that relaying is not permitted. (The test is valid only from a remote location, because all relaying is allowed from the internal network.)
Testing: • Use telnet from a remote location to connect with the SMTP service on port 25 and conduct a manual session to test for open relaying: ○ **`telnet relay.xxxx.com`** • Wait for responses and enter the following smtp commands: ○ **`HELO mail.spamtest.net`** ○ **`MAIL FROM: <spammer@spamtest.net>`** ○ **`RCPT TO: <victim@hotmail.com>`** (The e-mail relay should deny relaying at this point) ○ **`QUIT`** • Exit the telnet session. • Examine the logs for evidence that relaying was refused.
Test Type: Objective – Stimulus Response

AUDIT STEP - 36. Determine if server correctly relays external messages for internal users.
Reference: Personal experience.
Control Objective: Verify normal function of the e-mail relay.
Risk: (Reference: V19 – High) The organization depends on e-mail for its operation. Regardless of how well secured the server may be, if it does not

perform its function correctly, the organization would experience a denial of service.
Compliance: Compliance is binary. External messages are correctly relayed to internal users.
Testing: • From a remote host, send an e-mail message to postmaster@xxxxxx.com. • Determine from logs that message was relayed. • Verify that message was received by internal user.
Test Type: Objective – Stimulus response

AUDIT STEP - 37. Determine if server correctly relays internal messages to anywhere.
Reference: Personal experience.
Control Objective: Verify normal function of the e-mail relay.
Risk: (Reference: V19 – High) The organization depends on e-mail for its operation. Regardless of how well secured the server may be, if it does not perform its function correctly, the organization has experienced a denial of service.
Compliance: Compliance is binary. Internal messages are correctly relayed to external users. Internal messages are correctly relayed to internal users.
Testing: • From an internal host, send an e-mail message to postmaster@xxxxxx.com. • Determine from logs that the message was relayed. • Verify that the internal user received the message. • From an internal host, send an e-mail to an external e-mail address. • Determine from the logs that the message was relayed. • Verify that the external host received the message.
Test Type: Objective – Stimulus response

AUDIT STEP - 38. Determine how well Postfix rejects messages with invalid source addresses.
Reference: • Research: Blum, Richard. Postfix. Indianapolis: Sams Publishing, 2001. 204-205. • Personal experience.
Control Objective: Reduce the number of spoofed e-mail messages.
Risk: (Reference: V15, V16 – Both Critical) SMTP does not have built-in controls to verify the source of messages. E-mail can easily be spoofed by pretending to come from a source different from the actual source. Users can be fooled into opening malicious attachments that appear to be from trusted sources. In addition, spammers use e-mail spoofing to prevent detection and avoid

accountability. Strict checking of source addresses can reduce, but not eliminate, spoofed messages by requiring that the sending host has consistent forward and reverse DNS records and that the mail-from e-mail address is properly formed and the domain portion of the address has a valid DNS record. Note that these restrictions cannot guarantee that a message has been sent from the mail-from e-mail address, but only that the sending server and e-mail addresses are properly registered in DNS.

Compliance: Compliance is binary. Postfix does not accept spoofed messages. The test uses spam-test.net, which currently is a non-existent domain. If source checking were enabled, the test would show that messages from spam-test.net were rejected. *(Note: Based on the current configuration, this step is expected to fail).*

Testing:

- Use telnet from a remote location to connect with the SMTP service on port 25 and conduct a manual session to test for susceptibility to spoofing:
  - **`telnet relay.xxxx.com`**
- Wait for responses and enter the following SMTP commands:
  - **`HELO mail.spam-test.net`**
  - **`MAIL FROM: <spammer@spam-test.net>`**
  - **`RCPT TO: <postmaster@xxxxxx.com>`**
  - **`DATA`**
  - **`This is a test`**
  - **`.`**

  (If the relay accepts the spoofed e-mail at this point, the test fails)
  - **`QUIT`**
- Exit the telnet session.
- Examine the logs for evidence that message was rejected.

Test Type: Objective – Stimulus Response

AUDIT STEP - 39. Determine if Postfix is running in chroot jail.

Reference:

- Research: Blum, Richard. Postfix. Indianapolis: Sams Publishing, 2001. 134-135.
- Research: Bauer, Mick and de Winter, Brenno. "Using Postfix for Secure SMTP Gateways." 13 Sep. 2000. URL: http://www.postfix.org/linuxjournal.200010/4241.html (26 Oct. 2003)
- Research: Kurz, Christian. "LINUX2 – shell script to set up a Postfix chroot jail for Linux." 1 Feb. 2002. URL: http://orange.kame.net/dev/cvsweb.cgi/postfix/examples/chroot-setup/LINUX2?rev=1.1.1.5&cvsroot=apps (26 Oct. 2003).

Control Objective: Verify that Postfix runs in chroot jail for enhanced security.

Risk: (Reference: V18 – Critical) Postfix is designed as a secure replacement for sendmail. However, it allows for an additional level of security by running most of the application in a chroot jail. If an intruder breaks out of the program, he would

not have access to the entire system, but only the Postfix execution environment. This greatly reduces the impact of an intrusion from within the Postfix program.

Compliance: Compliance is binary. Postfix is running correctly in a chroot environment. The Postfix execution environment is in /var/spool/postfix, the directory indicated by the chroot setup script referenced above. The Postfix check command verifies the environment is correct. The Postfix configuration file master.cf is configured to run all Postfix executables under chroot except "local" and "pipe".

Testing:

- Determine queue_directory variable from Postfix:
  - **`postconf | grep queue_directory`**
- Verify execution environment is correct:
  - **`postfix check`**
- Inspect the configuration file /etc/postfix/master.cf to verify that all executables except "local" and "pipe" are flagged to run chroot.

Test Type: Objective

AUDIT STEP - 40. Determine how well Postfix responds to unexpected input.

Reference: Personal experience.

Control Objective: Verify that Postfix correctly handles unexpected input.

Risk: (References V17, V18 – Both Critical) An attacker may try many different techniques to exploit the SMTP service. If successful, he may compromise the server completely or make it inoperable.

Compliance: Compliance is subjective. Postfix cannot be tested against an infinite number of possibilities. Nessus should not find any significant vulnerabilities. The e-mail relay's logs should show extensive entries in response to an SMTP attack by Nessus. The IDS logs may record some aspects of the Nessus activity.

Testing: Run Nessus from a remote location to attack the e-mail relay. (Details about running Nessus are outside the scope of this audit.)

- Update the Nessus plug-ins:
  - **`nessus-update-plugins`**
- Start Nessus and configure the options as follows (other options are defaults):
  - On the Plugins tab:
    - Enable all but dangerous plugins
  - On the Scan Options tab:
    - Remove Ping options
    - Set to scan specified ports
  - On the Scan Options tab:
    - Set to scan port 25 only
  - On the Target tab:
    - Enter the address of the e-mail relay
- Run the scan.

• Observe the results to see if Nessus determined any vulnerabilities. • Inspect the e-mail relay's logs for activity caused by Nessus. • Inspect the IDS's logs for activity caused by Nessus. • Analyze the test and the results.
Test Type: Subjective – Stimulus Response

Operational Controls	Ensure that operational policies and procedures facilitate the reliable and secure operation of the e-mail relay (or its replacement) so that it can continue to provide the function for which it was designed. Ensure that problems are detected and resolved effectively and timely.

AUDIT STEP - 41. Determine if host and remote logs are adequately reviewed.
Reference: Checklist. Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditors Perspective." 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003).
Control Objective: Ensure that the IDS (remote log server) and e-mail relay logs are adequately reviewed.
Risk: (References: V4, V5 – Both Critical) If log files are not reviewed frequently enough and in enough detail, problems may not be found. Any problems that were not found would not be corrected. Malfunctions and attacks may be allowed to continue too long resulting in denial of service or a compromised system.
Compliance: Compliance is variable. Logs are reviewed frequently enough and in sufficient detail to make a timely determination of whether or not the systems are malfunctioning or are under attack.
Testing: Determine if log files are being reviewed. Determine how often they are reviewed. Determine by whom they are reviewed. Determine if the review is sufficient to spot problems timely.
Test Type: Subjective

AUDIT STEP - 42. Determine if backup media are available for restore.
Reference: Personal experience.
Control Objective: Ensure system can be recovered in the case of loss or failure.
Risk: (Reference: V3 – Low) If the server fails or is lost and media is not available for restoring the server, excessive downtime would result. In addition, if the current Postfix configuration files were not available, the process of fine-tuning the e-mail filters would have to start over. This risk is low because no critical data is stored on the server. If the server failed without backup media available, Linux and Postfix would be installed fresh and manually configured. (This item is included as a best practice.)
Compliance: The evaluation is subjective. Backups should be made frequently

enough to be able to restore the server to its current state. Backups should be stored offsite.
Testing: Determine how backups are made. Determine where backups are stored.
Test Type: Subjective

Section 3 – Audit Evidence

Results of the Audit

The audit was conducted from 27 Oct. 2003 – 30 Oct. 2003.

Tests were performed from the local network and from an external location. Results of the tests were captured several different ways. Command lines shown for the tests are accurate as far as the syntax required for executing the tests, but, to improve readability, some have been edited to remove the syntax for capturing their output to files.

Steps judged most important to the audit are presented in this section, as well as all steps that failed.

AUDIT STEP – 8 PASS

Test network input controls listed in Section 1 regarding unsolicited Internet traffic.

The following figure contains results from nmap TCP and UDP scans for all ports on the e-mail relay. The scans were performed externally. The syntax for the nmap scans is included in the output. UDP scans were broken into several separate runs because of the extremely long time they took to run.

Figure 2 – External nmap scans

```
# nmap (V. 2.54BETA31) scan initiated Wed Oct 29 17:53:34 2003 as: nmap
-r -P0 -sS -v -p 1-65535 -oN nmap.TCP.ports.1-65535.txt relay.xxxx.com
Interesting ports on relay.xxxx.com (xxx.xxx.xxx.xxx):
(The 65534 ports scanned but not shown below are in state: filtered)
Port       State       Service
25/tcp     open        smtp


# Nmap run completed at Wed Oct 29 19:08:06 2003 -- 1 IP address (1
host up) scanned in 4472 seconds

# nmap (V. 2.54BETA31) scan initiated Tue Oct 28 10:18:16 2003 as: nmap
-r -P0 -sU -v -p 1-1024 -oN nmap.UDP.ports.1-1024.txt relay.xxxx.com
All 1024 scanned ports on relay.xxxx.com (xxx.xxx.xxx.xxx) are:
filtered

# Nmap run completed at Tue Oct 28 10:38:54 2003 -- 1 IP address (1
host up) scanned in 1238 seconds

# nmap (V. 2.54BETA31) scan initiated Tue Oct 28 10:47:18 2003 as: nmap
-r -P0 -sU -v -p 1025-10000 -oN nmap.UDP.ports.1025-10000.txt
relay.xxxx.com
All 8976 scanned ports on relay.xxxx.com (xxx.xxx.xxx.xxx) are:
filtered
```

```
# Nmap run completed at Tue Oct 28 13:47:11 2003 -- 1 IP address (1
host up) scanned in 10793 seconds

# nmap (V. 2.54BETA31) scan initiated Tue Oct 28 13:54:12 2003 as: nmap
-r -P0 -sU -v -p 10001-30000 -oN nmap.UDP.ports.10001-30000.txt
relay.xxxx.com
All 20000 scanned ports on relay.xxxx.com (xxx.xxx.xxx.xxx) are:
filtered

# Nmap run completed at Tue Oct 28 20:34:49 2003 -- 1 IP address (1
host up) scanned in 24037 seconds

# nmap (V. 2.54BETA31) scan initiated Wed Oct 29 03:06:56 2003 as: nmap
-r -P0 -sU -v -p 30001-65535 -oN nmap.UDP.ports.30001-65535.txt
relay.xxxx.com
All 35535 scanned ports on relay.xxxx.com (xxx.xxx.xxx.xxx) are:
filtered

# Nmap run completed at Wed Oct 29 14:58:51 2003 -- 1 IP address (1
host up) scanned in 42715 seconds
```

The results show that only TCP port 25 is allowed from the Internet. This audit step passes.

AUDIT STEP – 9 FAIL (Reference: Finding 2)

Test network input controls listed in Section 1 regarding unsolicited internal network traffic.

The following figure contains results from nmap TCP and UDP scans for all ports on the e-mail relay. The scans were performed from the internal network. The syntax for the nmap scans is included in the output. UDP scans were broken into several separate runs because of the extremely long time that they took to run.

Figure 3 – Internal nmap scans

```
# nmap (V. 3.00) scan initiated Tue Oct 28 07:58:37 2003 as: nmap -v -
sS -r -P0 -p 1-65535 -oN int_map_TCP.txt 192.168.10.2
Interesting ports on relay.xxxx.com (192.168.10.2):
(The 65533 ports scanned but not shown below are in state: filtered)
Port       State       Service
22/tcp     open        ssh
25/tcp     open        smtp

# Nmap run completed at Tue Oct 28 08:43:45 2003 -- 1 IP address (1
host up) scanned in 2708 seconds
# nmap (V. 3.00) scan initiated Wed Oct 29 11:02:55 2003 as: nmap -v -
sU -r -P0 -p 1-1024 -o nmap.U.1-1024.txt 192.168.10.2
All 1024 scanned ports on relay.xxxx.com (192.168.10.2) are: closed
```

```
# Nmap run completed at Wed Oct 29 11:19:54 2003 -- 1 IP address (1
host up) scanned in 1019 seconds

# nmap (V. 3.00) scan initiated Wed Oct 29 11:47:56 2003 as: nmap -v -
sU -r -P0 -p 1025-10000 -o nmap.U.1025-10000.txt 192.168.10.2
All 8976 scanned ports on relay.xxxx.com (192.168.10.2) are: closed

# Nmap run completed at Wed Oct 29 14:16:48 2003 -- 1 IP address (1
host up) scanned in 8932 seconds

# nmap (V. 3.00) scan initiated Wed Oct 29 17:51:07 2003 as: nmap -v -
sU -r -P0 -p 10001-65535 -o nmap.U.10001-65535.txt 192.168.10.2
All 55535 scanned ports on relay.xxxx.com (192.168.10.2) are: closed

# Nmap run completed at Thu Oct 30 09:12:13 2003 -- 1 IP address (1
host up) scanned in 55266 seconds
```

The results show that TCP ports 22 and 25 are allowed as required. However, the network input controls defined in Section 1 specify that UDP port 123 be allowed from the internal network. This is not the case. This audit step fails.

AUDIT STEP – 13 PASS

Determine if logging is configured properly on the e-mail relay and on the remote logging server.

Using a root login, the following script was created as “log.script”.

Figure 4 – Script for automated syslog testing

```
#!/bin/bash
#
# Script to generate one log message per
# priority level per facility
#
for i in {auth,authpriv,cron,daemon,kern,lpr,mail,
mark,news,syslog,user,uucp,local0,local1,local2,
local3,local4,local5,local6,local7}

do
  for k in {debug,info,notice,warning,err,crit,
         alert,emerg}
  do
    logger -p $i.$k "Test message, facility $i
                     priority $k"
  done
done
```

Permissions were changed to 700 to allow execution. The script was executed.

```
# chmod 700 log.script
# ./log.script
```

The relevant log files were examined. Relevant sections of the log files on both the e-mail relay and the remote log server were extracted using the grep command and saved to files for later analysis. One example follows:

```
# grep "Test message, facility" /var/log/messages
```

The output of this test is too long to include in full. The results for a few of the log files are as follows (lengthy results are shown in part):

Figure 5 – E-mail relay – syslog test results

/var/log/messages (e-mail relay):

```
Oct 27 18:56:33 relay noc: Test message, facility auth priority info
Oct 27 18:56:33 relay noc: Test message, facility auth priority notice
Oct 27 18:56:33 relay noc: Test message, facility auth priority warning
Oct 27 18:56:33 relay noc: Test message, facility auth priority err
Oct 27 18:56:33 relay noc: Test message, facility auth priority crit
Oct 27 18:56:33 relay noc: Test message, facility auth priority alert
Oct 27 18:56:34 relay noc: Test message, facility auth priority emerg
Oct 27 18:56:34 relay noc: Test message, facility daemon priority info
Oct 27 18:56:34 relay noc: Test message, facility daemon priority
notice
.
.
.
Oct 27 18:56:34 relay noc: Test message, facility local6 priority alert
Oct 27 18:56:34 relay noc: Test message, facility local6 priority emerg
Oct 27 18:56:34 relay noc: Test message, facility local7 priority info
Oct 27 18:56:34 relay noc: Test message, facility local7 priority
notice
Oct 27 18:56:34 relay noc: Test message, facility local7 priority
warning
Oct 27 18:56:34 relay noc: Test message, facility local7 priority err
Oct 27 18:56:34 relay noc: Test message, facility local7 priority crit
Oct 27 18:56:34 relay noc: Test message, facility local7 priority alert
Oct 27 18:56:34 relay noc: Test message, facility local7 priority emerg
```

/var/log/boot.log (e-mail relay)

```
Oct 27 18:55:45 relay noc: Test message, facility local7 priority debug
Oct 27 18:55:45 relay noc: Test message, facility local7 priority info
Oct 27 18:55:45 relay noc: Test message, facility local7 priority
notice
Oct 27 18:55:45 relay noc: Test message, facility local7 priority err
Oct 27 18:55:45 relay noc: Test message, facility local7 priority crit
Oct 27 18:55:45 relay noc: Test message, facility local7 priority emerg
Oct 27 18:56:34 relay noc: Test message, facility local7 priority debug
Oct 27 18:56:34 relay noc: Test message, facility local7 priority info
Oct 27 18:56:34 relay noc: Test message, facility local7 priority
notice
Oct 27 18:56:34 relay noc: Test message, facility local7 priority
warning
```

```
Oct 27 18:56:34 relay noc: Test message, facility local7 priority err
Oct 27 18:56:34 relay noc: Test message, facility local7 priority crit
Oct 27 18:56:34 relay noc: Test message, facility local7 priority alert
Oct 27 18:56:34 relay noc: Test message, facility local7 priority emerg
```

Figure 6 – Remote log server – syslog test results

/var/log/messages (remote log server)

```
Oct 27 18:56:34 relay.xxxx.com noc: Test message, facility auth
priority info
Oct 27 18:56:34 relay.xxxx.com noc: Test message, facility auth
priority notice
Oct 27 18:56:34 relay.xxxx.com noc: Test message, facility auth
priority warning
Oct 27 18:56:34 relay.xxxx.com noc: Test message, facility auth
priority err
Oct 27 18:56:34 relay.xxxx.com noc: Test message, facility auth
priority crit
Oct 27 18:56:34 relay.xxxx.com noc: Test message, facility auth
priority alert
Oct 27 18:56:34 relay.xxxx.com noc: Test message, facility auth
priority emerg
Oct 27 18:56:34 relay.xxxx.com noc: Test message, facility daemon
priority info
Oct 27 18:56:34 relay.xxxx.com noc: Test message, facility daemon
priority notice
.
.
.
Oct 27 18:56:38 relay.xxxx.com noc: Test message, facility local7
priority alert
Oct 27 18:56:38 relay.xxxx.com noc: Test message, facility local7
priority emerg
```

/var/log/secure (remote log server)

```
Oct 27 18:55:45 relay.xxxx.com noc: Test message, facility authpriv
priority info
Oct 27 18:55:45 relay.xxxx.com noc: Test message, facility authpriv
priority notice
Oct 27 18:55:45 relay.xxxx.com noc: Test message, facility authpriv
priority err
Oct 27 18:55:45 relay.xxxx.com noc: Test message, facility authpriv
priority crit
Oct 27 18:55:45 relay.xxxx.com noc: Test message, facility authpriv
priority emerg
Oct 27 18:56:34 relay.xxxx.com noc: Test message, facility authpriv
priority info
Oct 27 18:56:34 relay.xxxx.com noc: Test message, facility authpriv
priority notice
Oct 27 18:56:34 relay.xxxx.com noc: Test message, facility authpriv
priority warning
Oct 27 18:56:34 relay.xxxx.com noc: Test message, facility authpriv
priority err
Oct 27 18:56:34 relay.xxxx.com noc: Test message, facility authpriv
priority crit
```

```
Oct 27 18:56:34 relay.xxxx.com noc: Test message, facility authpriv
priority alert
Oct 27 18:56:34 relay.xxxx.com noc: Test message, facility authpriv
priority emerg
```

The configuration file /etc/syslog.conf for the e-mail relay follows:

Figure 7 – E-mail relay – Contents of /etc/syslog.conf

```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                         /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none        /var/log/messages
*.info                                          @192.168.10.9

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

# Log all the mail messages in one place.
mail.*                                          /var/log/maillog


# Log cron stuff
cron.*                                          /var/log/cron

# Everybody gets emergency messages
*.emerg                                         *

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

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

The configuration file syslog.conf for the remote log server follows:

Figure 8 – Remote log server – Contents of /etc/syslogd.conf

```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                         /dev/console

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

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

```
# Log all the mail messages in one place.
mail.*                                          /var/log/maillog


# Log cron stuff
cron.*                                          /var/log/cron

# Everybody gets emergency messages
*.emerg                                         *

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

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

The configuration files are identical except for the remote logging server specified in the e-mail relay's configuration.

The log file entries created by the script were checked against the configuration files. All entries were logged in the correct locations on both servers. No entries were logged in inappropriate locations. This audit step passes.

AUDIT STEP – 15 FAIL (Reference: Finding 1)

Verify that the operating system patches are current.

The up2date command was used to determine if any system patches needed to be installed. The output was sent to a file for later analysis:

```
up2date –l
```

The contents of the file:

Figure 9 – System patches that need to be installed

```
Fetching package list for channel: redhat-linux-i386-9...

Fetching Obsoletes list for channel: redhat-linux-i386-9...

Fetching rpm headers...

Name                                    Version        Rel
-----------------------------------------------------------
openssh                                 3.5p1          11
openssh-clients                         3.5p1          11
openssh-server                          3.5p1          11
openssl                                 0.9.7a         20
perl                                    5.8.0          88.3
```

The Red Hat web site (http://www.redhat.com/apps/download/) was used to determine the dates of the new patches:

- openssh: 9 Sep. 2003
- openssh-clients: 9 Sep. 2003
- openssh-server: 9 Sep. 2003
- openssl: 25 Sep. 2003
- perl: 13 Aug. 2003

The evaluation of this step is subjective. Although there are only a few patches missing, most of them are very important to maintaining a high level of security. Since there is no evidence of updating system patches for over two months, compliance is judged inadequate. This audit step fails.

AUDIT STEP – 17 FAIL (Reference: Finding 2)

Determine if the firewall on the e-mail relay (iptables) is properly configured and enabled.

The firewall configuration was captured as follows:

```
iptables –L –v
```

The contents of the file:

Figure 10 – E-mail relay firewall rules (iptables)

```
Chain INPUT (policy ACCEPT 86764 packets, 69M bytes)
 pkts bytes target     prot opt in     out     source
destination
 710K  105M RH-Lokkit-0-50-INPUT  all  --  any    any     anywhere
anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
    0     0 RH-Lokkit-0-50-INPUT  all  --  any    any     anywhere
anywhere

Chain OUTPUT (policy ACCEPT 131K packets, 32M bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain RH-Lokkit-0-50-INPUT (2 references)
 pkts bytes target     prot opt in     out     source
destination
   96  7296 ACCEPT     udp  --  any    any     ns3.oit.unc.edu
anywhere           udp spt:ntp dpt:ntp
   97  7372 ACCEPT     udp  --  any    any     ntp1.jrc.us
anywhere           udp spt:ntp dpt:ntp
```

```
  106  8056 ACCEPT     udp  --  any    any     ns1.usg.edu
anywhere           udp spt:ntp dpt:ntp
   97  7372 ACCEPT     udp  --  any    any     mcs.anl.gov
anywhere           udp spt:ntp dpt:ntp
  114  8664 ACCEPT     udp  --  any    any     proxy.cc.vt.edu
anywhere           udp spt:ntp dpt:ntp
    0     0 ACCEPT     udp  --  any    any     proxy.cc.vt.edu
anywhere           udp spt:ntp dpt:ntp
    8   608 ACCEPT     udp  --  any    any     tock.usno.navy.mil
anywhere           udp spt:ntp dpt:ntp
    0     0 ACCEPT     udp  --  any    any     ns1.usg.edu
anywhere           udp spt:ntp dpt:ntp
    0     0 ACCEPT     udp  --  any    any     proxy.cc.vt.edu
anywhere           udp spt:ntp dpt:ntp
 4614  536K ACCEPT     udp  --  any    any     xxxxxxx.xxxx.com
anywhere           udp spt:domain dpts:1025:65535
  557 29308 ACCEPT     tcp  --  any    any     anywhere
anywhere           tcp dpt:smtp flags:SYN,RST,ACK/SYN
    5   260 ACCEPT     tcp  --  any    any     192.168.10.0/24
anywhere           tcp dpt:ssh flags:SYN,RST,ACK/SYN
   57  8086 ACCEPT     all  --  lo     any     anywhere
anywhere
  199 19889 ACCEPT     udp  --  any    any     xxxxxxxxx.xxxx.com
anywhere           udp spt:domain
 494K   30M REJECT     tcp  --  any    any     anywhere
anywhere           tcp flags:SYN,RST,ACK/SYN reject-with icmp-port-
unreachable
 122K 5768K REJECT     udp  --  any    any     anywhere
anywhere           udp reject-with icmp-port-unreachable
```

The relevant rules are in the section RH-Lokkit-0-50-INPUT. (The first several rules are entered automatically by the ntpd startup script.) The rules show the following:

- UDP is allowed for synchronization with external NTP servers.
- UDP is allowed from the internal DNS servers.
- SMTP is allowed from anywhere.
- SSH is allowed from any host on the internal network.
- All other TCP and UDP packets are rejected.

The internal network controls in Section 1 specify that hosts on the internal network should be able to synchronize time with the e-mail relay. The firewall configuration does not allow this and therefore does not comply with the requirements of this audit step. This audit step fails.

AUDIT STEP – 18 FAIL (Reference: Finding 3)

Verify that only necessary daemons are running on the system.

The netstat command was used to capture information about running processes to a file:

`netstat –atu`

The results:

Figure 11 – Results of "netstat -atu"

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address
State
tcp        0      0 *:1024                  *:*
LISTEN
tcp        0      0 *:sunrpc                *:*
LISTEN
tcp        0      0 *:ssh                   *:*
LISTEN
tcp        0      0 *:smtp                  *:*
LISTEN
tcp        0      0 relay.xxxx.com:ssh    xxxx.xxxxxx.com:2110
ESTABLISHED
tcp        0      0 relay.xxxx.com:smtp   xxxxxx.xxxxxxxxx:25416
TIME_WAIT
tcp        0      0 relay.xxxx.com:smtp   xxx.xxx.xx.xx:61469
ESTABLISHED
udp        0      0 *:1024                  *:*
udp        0      0 *:syslog                *:*
udp        0      0 *:713                   *:*
udp        0      0 *:sunrpc                *:*
udp        0      0 relay.xxxx.com:ntp      *:*
udp        0      0 relay.xxxx.com:ntp      *:*
udp        0      0 *:ntp                   *:*
```

The lsof command was used to determine the active network sockets.

lsof –i +M >lsof.i.+M.txt

The results:

Figure 12 – Results of "lsof -i +M"

```
COMMAND   PID    USER   FD   TYPE DEVICE SIZE NODE NAME
syslogd   496    root    7u  IPv4    911       UDP *:syslog
portmap   518     rpc    3u  IPv4    946       UDP
*:sunrpc[portmapper]
portmap   518     rpc    4u  IPv4    954       TCP
*:sunrpc[portmapper] (LISTEN)
rpc.statd 537 rpcuser    4u  IPv4   1023       UDP *:1024[status]
rpc.statd 537 rpcuser    5u  IPv4    974       UDP *:713
rpc.statd 537 rpcuser    6u  IPv4   1026       TCP *:1024[status]
(LISTEN)
sshd      634    root    3u  IPv4   1156       TCP *:ssh (LISTEN)
ntpd      671     ntp    4u  IPv4   1261       UDP *:ntp
```

```
ntpd       671     ntp    5u  IPv4   1262       UDP relay.xxxx.com:ntp
ntpd       671     ntp    6u  IPv4   1263       UDP relay.xxxx.com:ntp
master     753    root   11u  IPv4   1364       TCP *:smtp (LISTEN)
sshd      1848    root    4u  IPv4  15656       TCP relay.xxxx.com:ssh-
>xxxx.xxxx.com:2110 (ESTABLISHED)
sshd      1851     noc    4u  IPv4  15656       TCP relay.xxxx.com:ssh-
>xxxx.xxxx.com:2110 (ESTABLISHED)
smtpd     2549 postfix    6u  IPv4   1364       TCP *:smtp (LISTEN)
```

In addition to SSH, SMTP, NTP and syslog (which are required), the system is running RPC services, which are not required. Therefore, this is not in compliance. This audit step fails.

AUDIT STEP – 19 FAIL (Reference: Finding 1)

Verify that OpenSSH is being used and is the latest version.

OpenSSH has already been determined not to be the latest version by step 15. No further testing was performed. This audit step fails.

AUDIT STEP – 20 FAIL (Reference: Finding 3)

Determine if OpenSSH is properly configured.

The following is the contents of the configuration file /etc/ssh/ssh_config:

Figure 13 – Contents of /etc/ssh/ssh_config

```
#     $OpenBSD: ssh_config,v 1.16 2002/07/03 14:21:05 markus Exp $

# This is the ssh client system-wide configuration file.  See
# ssh_config(5) for more information.  This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.

# Configuration data is parsed as follows:
#  1. command line options
#  2. user-specific file
#  3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for various options

# Host *
#   ForwardAgent no
#   ForwardX11 no
#   RhostsAuthentication no
#   RhostsRSAAuthentication no
#   RSAAuthentication yes
```

```
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   BatchMode no
#   CheckHostIP yes
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/identity
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   Port 22
#   Protocol 2,1
#   Cipher 3des
#   Ciphers aes128-cbc,3des-cbc,blowfish-cbc,cast128-
cbc,arcfour,aes192-cbc,aes256-cbc
#   EscapeChar ~
Host *
      ForwardX11 yes
```

The configuration file /etc/ssh/sshd_config:

Figure 14 – Contents of /etc/ssh/sshd_config

```
#     $OpenBSD: sshd_config,v 1.59 2002/09/25 11:17:16 markus Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

#Port 22
#Protocol 2,1
#ListenAddress 0.0.0.0
#ListenAddress ::

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 3600
#ServerKeyBits 768

# Logging
#obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO
```

```
# Authentication:

#LoginGraceTime 120
PermitRootLogin no
#StrictModes yes

#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile     .ssh/authorized_keys

# rhosts authentication should not be used
#RhostsAuthentication no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes
# For this to work you will also need host keys in
/etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

#AFSTokenPassing no

# Kerberos TGT Passing only works with the AFS kaserver
#KerberosTgtPassing no

# Set this to 'yes' to enable PAM keyboard-interactive authentication
# Warning: enabling this may bypass the setting of
'PasswordAuthentication'
#PAMAuthenticationViaKbdInt no

#X11Forwarding no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PrintMotd yes
#PrintLastLog yes
#KeepAlive yes
#UseLogin no
#UsePrivilegeSeparation yes
#PermitUserEnvironment no
#Compression yes
```

```
#MaxStartups 10
# no default banner path
#Banner /some/path
#VerifyReverseMapping no

# override default of no subsystems
Subsystem   sftp  /usr/libexec/openssh/sftp-server
```

The following items in ssh_config do not comply (Note: these are defaults):

```
#   StrictHostKeyChecking ask
#   Protocol 2,1
#   Cipher 3des
```

The following items in sshd_config do not comply (Note: these are defaults):

```
#Protocol 2,1
#LoginGraceTime 120
#IgnoreUserKnownHosts no
```

SSH is not configured correctly according to SANS Top Twenty recommendations and best practices. This audit step fails.

AUDIT STEP – 21 FAIL (Reference: Finding 3)

Determine if PAM password authentication is being used for OpenSSH.

The contents of the /etc/pam.d/sshd file:

Figure 15 – Contents of /etc/pam.d/sshd

```
#%PAM-1.0
auth       required     pam_stack.so service=system-auth
auth       required     pam_nologin.so
account    required     pam_stack.so service=system-auth
password   required     pam_stack.so service=system-auth
session    required     pam_stack.so service=system-auth
session    required     pam_limits.so
session    optional     pam_console.so
```

Comparison to the stated requirements shows that the following entries are missing:

```
account  required       /lib/security/pam_access.so
account  required       /lib/security/pam_time.so
```

This audit step fails.

AUDIT STEP – 25 FAIL (Reference: Finding 3)

Determine if minimum password length and maximum password age are enforced.

The following is the contents of the password aging controls section of the /etc/login.defs file:

Figure 16 – Password aging controls

```
# Password aging controls:
#
#PASS_MAX_DAYS    Maximum number of days a password may be used.
#PASS_MIN_DAYS    Minimum number of days allowed between password
changes.
#PASS_MIN_LEN     Minimum acceptable password length.
#PASS_WARN_AGE    Number of days warning given before a password
expires.
#
PASS_MAX_DAYS     99999
PASS_MIN_DAYS     0
PASS_MIN_LEN      5
PASS_WARN_AGE     7
```

The PASS_MAX_DAYS and PASS_MIN_LENTH do not comply with the stated values of 90-day maximum age and eight characters minimum length. This audit step fails.

AUDIT STEP – 27 FAIL (Reference: Finding 3)

Determine if NFS and NIS are installed.

The command rpm was used to determine if the packages for NFS and NIS are installed.

Search for nfs-utils – the package for NFS:

```
rpm –q –nfs-utils
```

Result:

```
nfs-utils-1.0.1-3.9
```

Search for ypbind – the package for NIS:

```
rpm –q ypbind
```

Result:

```
ypbind-1.11-4
```

Both NFS and NIS are installed. This audit step fails.

AUDIT STEP – 32 PASS

Determine if RBL-based message blocking works correctly.

Messages are blocked using the following RBLs, which are configured in the file /etc/postfix/main.cf for use by the e-mail relay.

- relays.ordb.org
- bl.spamcop.net
- blackholes.easynet.nl

The log file /var/log/maillog contains an entry for each rejected message indicating why the message was rejected.

Figure 17 – Sample message rejection by RBL

```
Oct 29 08:50:28 relay postfix/smtpd[8119]: reject: RCPT from
xxxx.xxxxxxxxxx.com[xx.xx.xxx.xx]: 554 Service unavailable;
[xx.xx.xxx.xx] blocked using bl.spamcop.net, reason: Blocked - see
http://www.spamcop.net/bl.shtml?xx.xx.xxx.xx;
from=<xxxx@xxxxxxxxxxxx.com> to=<xxxx@xxxx.com>
```

The following session shows the number of messages blocked at the time of the audit, which includes approximately three days of activity.

Figure 18 – Count of messages blocked by RBLs

```
[root@relay Postfix]# grep "blocked using blackholes.easynet.nl"
/var/log/maillog | wc -l
    273
 [root@relay postfix]# grep "blocked using bl.spamcop.net"
/var/log/maillog | wc -l
    514
[root@relay postfix]# grep "blocked using relays.ordb.org"
/var/log/maillog | wc -l
     19
[root@relay postfix]#
```

The results show that a substantial number of messages are being blocked using RBLs. This audit step passes.

AUDIT STEP – 34 PASS

Determine if executable extensions are blocked.

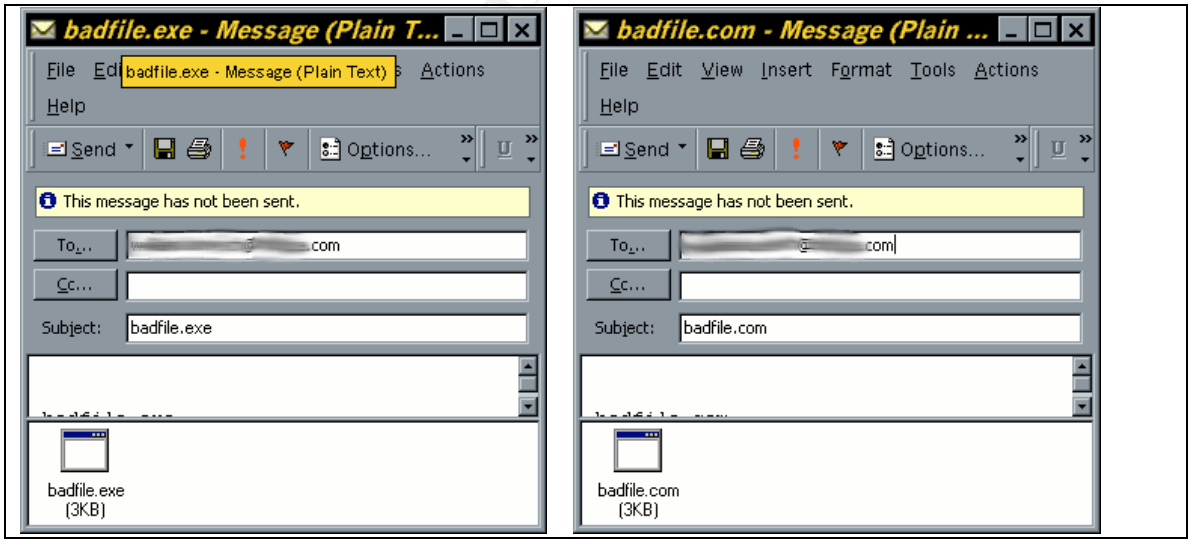
The following is the contents of /etc/postfix/body_checks.regexp showing the section that blocks executable extensions:

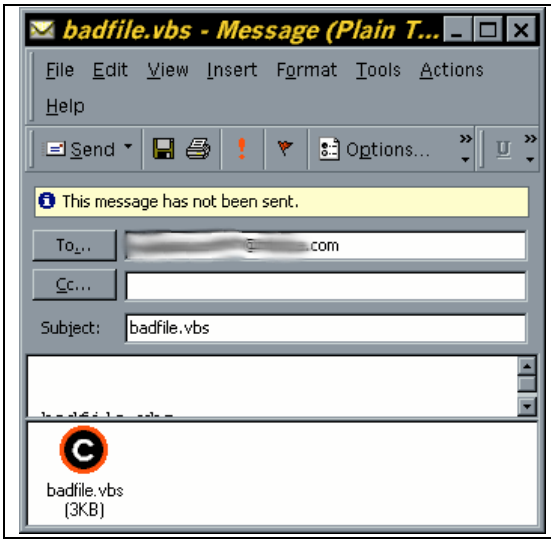
Figure 19 – Contents of /etc/postfix/body_checks.regexp

```
[root@relay postfix]# cat body_checks.regexp
#
/^(.*)filenXame\=\"(.*)\.pdf\"$/                              OK
/^(.*)filenXame\=\"(.*)\.gif\"$/                              OK
/^(.*)filenXame\=\"(.*)\.jpg\"$/                              OK
/^(.*)filenXame\=\"(.*)\.tif\"$/                              OK
/^(.*)filenXame\=\"(.*)\.png\"$/                              OK
#
/^(.*)filenXame\=\"(.*)\.avi\"$/                              OK
/^(.*)filenXame\=\"(.*)\.mov\"$/                              OK
#
/^(.*)filenXame\=\"(.*)\.txt\"$/                              OK
/^(.*)filenXame\=\"(.*)\.rtf\"$/                              OK
/^(.*)filenXame\=\"(.*)\.htm\"$/                              OK
/^(.*)filenXame\=\"(.*)\.html\"$/                             OK
/^(content.*[[:space:]]+|[[:space:]]*)(filename|name)=".*\.(scr|pif|exe
|com|bat|shs|shb|vxd|rm|chm|vbs|ini|cmd|do|hta|xl|reg|lnk|js|jse)"/
REJECT
[root@relay postfix]#
```

Three messages were sent with dummy attachments named badfile.exe, badfile.com, and badfile.vbs.

Figure 20 – E-mails with banned attachments





The following session shows the grep command used to extract the reject notices from /var/log/maillog:

Figure 21 – Blocking executable extensions

```
[root@relay postfix]# grep 'badfile.' /var/log/maillog
Oct 29 09:50:56 relay postfix/cleanup[8304]: 51282518A5: reject: body
?name="badfile.exe"; from=<xxxxxxxx@xxxxxxx.net>
to=<xxxxxxxxxxx@xxxx.com>: Message content rejected
Oct 29 09:53:56 relay postfix/cleanup[8304]: 1E0BD518A5: reject: body
?name="badfile.com"; from=<xxxxxxxx@xxxxxxx.net>
to=<xxxxxxxxxxx@xxxx.com>: Message content rejected
Oct 29 09:55:54 relay postfix/cleanup[8318]: 1F2F0518A5: reject: body
?name="badfile.vbs"; from=<xxxxxxxx@xxxxxxx.net>
to=<xxxxxxxxxxx@xxxx.com>: Message content rejected
```

The messages were properly rejected. This audit step passes.

AUDIT STEP – 35 PASS

Determine if the e-mail relay is an open relay.

The following session is a manual test for open relaying, which was conducted externally relative to the organization's network.

Figure 22 – Open relay test

```
[root@localhost root]# telnet relay.xxxx.com 25
Trying xxx.xxx.xxx.xxx...
Connected to relay.xxxx.com.
Escape character is '^]'.
220 ***************
HELO mail.spamtest.net
```

```
250 relay.xxxx.com
MAIL FROM: <spammer@spamtest.net>
250 Ok
RCPT TO: <victim@hotmail.com>
554 <victim@hotmail.com>: Recipient address rejected: Relay access
denied
QUIT
221 Bye
Connection closed by foreign host.
 [root@localhost root]#
```

The e-mail relay successfully rejected the relay request. This audit step passes.

AUDIT STEP – 38 FAIL (Reference: Finding 4)

Determine how well Postfix rejects messages with invalid source addresses.

The following session is a manual test for spoofed message blocking, which was conducted externally relative to the organization's network.

Figure 23 – Spoofed message blocking test

```
[root@localhost root]# telnet relay.xxxx.com 25
Trying xxx.xxx.xxx.xxx...
Connected to relay.xxxx.com.
Escape character is '^]'.
220 ***************
HELO mail.spamtest.net
250 relay.xxxx.com
MAIL FROM: <spammer@spamtest.net>
250 Ok
RCPT TO: <postmaster@xxxx.com>
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
This is a test
.
250 Ok: queued as 18534518A5
QUIT
221 Bye
Connection closed by foreign host.
[root@localhost root]#
```

The e-mail relay did not reject the spoofed message. This audit step fails.

AUDIT STEP – 39 FAIL (Reference: Finding 5)

Determine if Postfix is running in chroot jail.

The following session shows the location of the Postfix execution environment and checks for any inconsistencies in the files located there:

```
[root@relay postfix]# postconf | grep queue_directory
queue_directory = /var/spool/postfix
[root@relay postfix]# postfix check
[root@relay postfix]#
```

The execution environment is in place correctly and is consistent.

The following is the contents of the /etc/postfix/master.cf file, with the documentation sections deleted:

Figure 24 – Postfix master.cf file

```
==========================================================================
# service type private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (50)
# ==========================================================================
smtp      inet  n       -       n       -       -       smtpd
#628      inet  n       -       n       -       -       qmqpd
pickup    fifo  n       -       n       60      1       pickup
cleanup   unix  n       -       n       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
#qmgr     fifo  n       -       n       300     1       nqmgr
rewrite   unix  -       -       n       -       -       trivial-rewrite
bounce    unix  -       -       n       -       0       bounce
defer     unix  -       -       n       -       0       bounce
flush     unix  n       -       n       1000?   0       flush
smtp      unix  -       -       n       -       -       smtp
showq     unix  n       -       n       -       -       showq
error     unix  -       -       n       -       -       error
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       n       -       -       lmtp
#
# Interfaces to non-Postfix software. Be sure to examine the manual
# pages of the non-Postfix software to find out what options it wants.
# The Cyrus deliver program has changed incompatibly.
#
cyrus     unix  -       n       n       -       -       pipe
  flags=R user=cyrus argv=/cyrus/bin/deliver -e -m ${extension} ${user}
uucp      unix  -       n       n       -       -       pipe
  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)
ifmail    unix  -       n       n       -       -       pipe
  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
bsmtp     unix  -       n       n       -       -       pipe
  flags=Fq. user=foo argv=/usr/local/sbin/bsmtp -f $sender $nexthop $recipient
```

The configuration file shows that no Postfix processes are running under chroot. This audit step fails.

AUDIT STEP – 40 PASS

Determine how well Postfix responds to unexpected input.

Nessus was configured for testing as indicated by Audit Step – 40 in Section 2. The target was specified to be the external DNS name of the e-mail relay. The scan was run from an external location relative to the organization's network. The following is the report generated by Nessus.

Figure 25 – Nessus Scan Report

Nessus Scan Report

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

Scan Details

Hosts which where alive and responding during test
1

Number of security holes found
0

Number of security warnings found
1

Host List

Host(s)
Possible Issue

relay.xxxx.com
Security warning(s) found

[return to top]

Analysis of Host

Address of Host
Port/Service
Issue regarding Port

relay.xxxx.com
smtp (25/tcp)
Security notes found

relay.xxxx.com
general/udp
Security notes found

relay.xxxx.com
general/tcp
Security notes found

relay.xxxx.com
general/icmp
Security warning(s) found

Security Issues and Fixes: relay.xxxx.com

Type
Port
Issue and Fix

Informational
smtp (25/tcp)
An SMTP server is running on this port
Here is its banner :
220 **********
Nessus ID : 10330

Informational
smtp (25/tcp)
Remote SMTP server banner :
220 **********

Nessus ID : 10263

Informational
smtp (25/tcp)
smtpscan was not able to reliably identify this server. It might be:
Postfix
The fingerprint differs from these known signatures on 2 point(s)

If you known precisely what it is, please send this fingerprint
to the Nessus team :
:503:502:501:250:501:250:501:502:502:502:502:502:502:250:502
Nessus ID : 11421

Informational
smtp (25/tcp)
For some reason, we could not send the EICAR test string to this MTA
Nessus ID : 11034

Informational
general/udp
For your information, here is the traceroute to xxx.xxx.xxx.xxx:

[EDITED OUT]

Nessus ID : 10287

Informational
general/tcp
Remote OS guess : AIX 4.02.0001.0000

CVE : CAN-1999-0454
Nessus ID : 11268

Warning
general/icmp

The remote host accepts loose source routed IP packets.
The feature was designed for testing purpose.
An attacker may use it to circumvent poorly designed IP filtering
and exploit another flaw. However, it is not dangerous by itself.

Solution : drop source routed packets on this host or on other ingress
routers or firewalls.

Risk factor : Low
Nessus ID : 11834

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

The e-mail relay logged extensive entries in the log file /var/log/maillog because of the scan. Listing the entries would take approximately 20 pages, so only a few selected entries are shown here.

Figure 26 – Entries in /var/log/maillog from Nessus scan

```
Oct 28 17:27:01 relay postfix/smtpd[6600]: reject: RCPT from
xxxx.xxxx.net[xxx.xx.xx.xxx]: 504 <nessus>: Sender address rejected:
need fully-qualified address; from=<nessus> to=<nobody@nessus.org>
Oct 28 17:27:04 relay postfix/smtpd[6601]: connect from
xxxx.xxxx.net[xxx.xx.xx.xxx]
Oct 28 17:27:04 relay postfix/smtpd[6601]: warning: Illegal address
syntax from xxxx.xxxx.net[xxx.xx.xx.xxx] in MAIL command:
root@relay.xxxx.com
Oct 28 17:27:04 relay postfix/smtpd[6595]: lost connection after HELO
from xxxx.xxxx.net[xxx.xx.xx.xxx]
Oct 28 17:27:04 relay postfix/cleanup[6596]: 509BD518C6: message-
id=<20031028222704.509BD518C6@relay.xxxx.com>
Oct 28 17:27:07 relay postfix/smtpd[6600]: 10FE3518A5:
client=xxxx.xxxx.net[xxx.xx.xx.xxx]
Oct 28 17:27:07 relay postfix/smtpd[6600]: reject: RCPT from
xxxx.xxxx.net[xxx.xx.xx.xxx]: 554 <nobody@nessus.org>: Recipient
address rejected: Relay access denied; from=<> to=<nobody@nessus.org>
=0, status=sent (mailbox)
Oct 28 17:27:51 relay postfix/smtpd[6601]: connect from
xxxx.xxxx.net[xxx.xx.xx.xxx]
Oct 28 17:27:51 relay postfix/smtpd[6601]: warning: Illegal address
syntax from xxxx.xxxx.net[xxx.xx.xx.xxx] in MAIL command:
```

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXX
xxxx.xxxx.net[xxx.xx.xx.xxx]: 550
<nessus1562876827@invalid1082757395.net>: Recipient address rejected:
Domain not found; from=<bounce957953058@[127.0.0.1]>
to=<nessus1562876827@invalid1082757395.net>
```

The scan also resulted in a large number of bounce messages (which the e-mail relay sends to its root account).

The snort-based IDS did not detect this activity.

The e-mail server showed no signs of any problem during or after the attack. This audit step passes.

AUDIT STEP – 41 FAIL (Reference: Finding 6)

Determine if host and remote logs are adequately reviewed.

This is a subjective test. The logs are reviewed daily, with exceptions in cases where priorities dictate otherwise and when the administrator is not in the office. Even though the logs are reviewed, the number of entries in the logs is large enough that detailed review is not possible. Both the e-mail relay and the remote log server run LogWatch, which does not monitor nearly enough items and only creates reports once per day. Not reviewing logs at all clearly would be much worse, but the likelihood that something will not be noticed or not noticed in time seems too great. This audit step fails.

AUDIT STEP – 42 FAIL (Reference: Finding 7)

Determine if backup media are available for restore.

This is a subjective test. Backups are made very infrequently and are not stored offsite. Postfix configuration files are backed up occasionally, but not according to a formal or disciplined method. Postfix package updates, Linux package updates, and Linux configuration changes are frequently made without backing up the system. This audit step fails.

Measurement of Residual Risk

Before the audit was conducted, a pre-audit risk evaluation was performed. Before the audit, no assumptions were made about how well the system was protected with regard to the vulnerabilities that were considered. The risk evaluation was scored with a worst-case bias because the system had not been previously audited.

After auditing the system, the risk of many of the items was reduced by the controls that were found to be operating satisfactorily. The post-audit state of the system is a snapshot. It considers only the state of the system at the time of the audit and does not consider the likelihood of a vulnerability presenting a higher risk later because of operational changes or new threats.

The following table shows the vulnerabilities, the steps that tested controls that eliminate or compensate for each vulnerability, and the rating of the exposure related to each vulnerability. The likelihood remains constant that the associated threats will occur. The method of calculating the risk values is the same as presented in Section 1 and is not presented here.

Just as in the initial risk evaluation, the determination of the post-audit value for the vulnerability was subjective (Low, Medium, High, or Critical). Considerations included whether or not a step that passed completely mitigated the associated vulnerability. Considerations also included whether or not the reason a step failed was relevant to the associated vulnerability. The subjective value was converted to a number to perform the calculations. The results are the evaluation of the residual risk and are shown in the following table:

Table 9 – Residual risk by vulnerability

Ref.	Vulnerability	Audit Step and Result	Comments	Post-audit Vulnerability Exposure	Pre-audit Risk	Post-audit Risk
V1	Dependence on physical environment to be able to operate	Step – 7: PASS	Risk is not eliminated.	Low – 0.12	10 - High	0.44 - Medium
V2	Physical access	Step – 6: PASS	Risk is not eliminated. Calculation for risk changed from 23 to 4.4. Although both are categorized as high, this represents a significant decrease.	Low – 0.12	23 - High	4.4 - High
V3	Backup media may be corrupted or unavailable when needed (included as a best practice)	Step – 42: FAIL		Low – 0.12	0.10 - Low	0.10 - Low
V4	System malfunctions may not be detected timely	Step – 13: PASS Step – 14: PASS Step – 41: FAIL	The post-audit value for the vulnerability was reduced to medium because the logs are usually reviewed daily.	Medium – 0.37	54 - Critical	32 - Critical
V5	System changes may not be detected timely	Step – 13: PASS Step – 14: PASS Step – 41: FAIL	The post-audit value for the vulnerability was reduced to medium because the logs are usually reviewed daily.	Medium – 0.37	54 - Critical	32 - Critical
V6	System requires proper communication with DNS server, default gateway and network switch, system requires proper function of NAT on firewall	Step – 11: PASS Step – 12: PASS		NONE	5.4 - High	NONE
V7	SANS Top 20 – RPC vulnerability	Step – 8: PASS Step – 9: FAIL Step – 17: FAIL Step – 18: FAIL	Step 17 Failure (NTP related) does not affect this item. iptables prevents access to service.	Low – 0.12	76 - Critical	10 - High
V8	SANS Top 20 – General UNIX/Linux authentication – Accounts with no passwords or weak passwords	Step – 8: PASS Step – 9: FAIL Step – 17: FAIL Step – 22: PASS	Step 17 Failure (NTP related) does not affect this item.	Medium -.37	76 - Critical	32 - Critical

Ref.	Vulnerability	Audit Step and Result	Comments	Post-audit Vulnerability Exposure	Pre-audit Risk	Post-audit Risk
		Step – 23: PASS Step – 24: PASS Step – 25: FAIL Step – 26: PASS				
V9	SANS Top 20 – Clear text services	Step – 8: PASS Step – 9: FAIL Step – 16:PASS Step – 17: FAIL Step – 18: FAIL Step – 19: FAIL	Step 17 Failure (NTP related) does not affect this item. iptables does not allow access.	Medium – .37	76 - Critical	32 - Critical
V10	SANS Top 20 – Secure Shell	Step – 8: PASS Step – 9: FAIL Step – 10:PASS Step – 17: FAIL Step – 19: FAIL Step – 20: FAIL Step – 21: FAIL	Step 17 Failure (NTP related) does not affect this item.	Critical – .87	76 - Critical	76 - Critical
V11	SANS Top 20 – Misconfiguration of enterprise services NIS/NFS	Step – 8: PASS Step – 9: FAIL Step – 17: FAIL Step – 27: FAIL	Step 17 Failure (NTP related) does not affect this item. iptables does not allow access. Packages are installed but services are not running	Low – .12	76 - Critical	10 - High
V12	SANS Top 20 – Open Secure Sockets Layer SSL	Step – 8: PASS Step – 9: FAIL Step – 17: FAIL Step – 28: PASS	Step 17 Failure (NTP related) does not affect this item.	NONE	76 - Critical	NONE
V13	Other operating system patches may not be current	Step – 8: PASS Step – 9: FAIL Step – 10:PASS Step – 15: FAIL	Step 17 Failure (NTP related) does not affect this item.	Critical – .87	54 - Critical	54 - Critical

Ref.	Vulnerability	Audit Step and Result	Comments	Post-audit Vulnerability Exposure	Pre-audit Risk	Post-audit Risk
		Step – 17: FAIL				
V14	Other unnecessary services may be enabled	Step – 8: PASS Step – 9: FAIL Step – 10:PASS Step – 16:PASS Step – 17: FAIL Step – 18: FAIL	Step 17 Failure (NTP related) does not affect this item. iptables configuration does not allow access.	Low – .12	54 - Critical	10 - High
V15	E-mail encapsulates almost anything and bypasses most network controls	Step – 29: PASS Step – 30: PASS Step – 31: PASS Step – 32: PASS Step – 33: PASS Step – 34: PASS Step – 38: FAIL	Most UCE is filtered. However, spoofed mail is still a problem, especially when combined with attachments with .zip extensions, which are allowed.	High – .62	76 - Critical	54 - Critical
V16	SMTP does not check source addresses	Step – 38: FAIL	Most UCE is filtered. However, spoofed mail is still a problem, especially when combined with attachments with .zip extensions, which are allowed.	High – .62	54 - Critical	38 - Critical
V17	E-mail relay could operate as an open relay	Step – 35: PASS Step – 40: PASS		None	76 - Critical	NONE
V18	Postfix environment may not be secured optimally	Step – 29: PASS Step – 39: FAIL Step – 40: PASS		Medium – .32	32 - Critical	32 – Critical
V19	E-mail relay may not correctly perform its normal function	Step – 36 PASS Step – 37 PASS		NONE	5.4 - High	NONE

The organization has determined that, generally, each item with critical or high risk should be corrected unless there is an overriding business reason not to. Other risks should be corrected if not too difficult or expensive – otherwise, resources are better spent on other problems.

The risk model presented in Section 1 – and revisited in the table above – has not been previously used by the organization. The parameters and ranges used in the model were taken from the presentation referenced in Section 1. It was anticipated that the model might need to be adjusted to provide the most accurate results. The results, with two exceptions, agree with the administrator's subjective sense of the state of the system.

The risk associated with physical access was determined to be high. Subjectively, the controls in place are judged adequate for the current business environment; therefore, there is no recommendation regarding physical security.

The risk associated with the timely detection of system malfunctions and changes is still critical according to the model, even though the logs generally are reviewed daily. This vulnerability can never be eliminated. Unless zero detect time is achieved, the model will always show high or critical risk. This is another indication that the model needs to be adjusted. One possible adjustment would be to add a value of "very low" to the model. Another would be to modify the numeric values used by the model.

Despite the apparent limitations of the risk model, the time to detect problems is still judged unsatisfactory. The only way to improve is to decrease the time to detect. The only feasible way to decrease detection time is to implement automated monitoring and alerting. There are open-source tools available for performing this task, but implementing and testing would require significant effort – on the order of 50 hours of the administrator's time to research, test, and implement. The recommendation therefore is that management should consider automated monitoring and alerting.

Given current operating constraints, the e-mail relay will not be configured to check source addresses. This decision will allow unrestricted delivery of spoofed messages to continue. Strict source checking can stop many, but not all, spoofed messages; however, earlier testing showed that it blocked too many messages that the organization's employees were expecting. An attempt to create exceptions to allow messages from known senders quickly became too burdensome. The decision was made to allow messages without checking source addresses until the majority of the Internet community adopts the practice of providing correct information in e-mail headers.

Some e-mail related vulnerabilities cannot be fixed. E-mail spoofing by others using the organization's e-mail addresses is one possibility that is entirely outside the control of the organization. The Sobig.F worm is an example. It was the fastest spreading worm in history when released. Although the organization was

not infected with the worm, clients received infected e-mails from other sources that were spoofed with the organization's addresses. The organization experienced loss of customer confidence and possible loss of credibility as a result.

Another example of a vulnerability that cannot be fixed is that SMTP sends content in clear text. The demands of the business environment dictate that the organization cannot require its clients to use encrypted e-mail.

Besides the issues discussed above, there are a number of critical and high risks remaining. Fortunately, they are simple configuration and maintenance issues. The only cost for fixing them is the administrator's time, which is estimated to be less than ten hours for system changes and retesting. The recommendation is to immediately correct these problems.

Is the System Auditable?

Although the time and effort that went into the research and development of the risk model and the checklist steps was far from trivial, the actual audit was uncomplicated. The system has a single job to do – transfer e-mail messages safely, securely, and reliably. The audit was straightforward because very few services are needed on an e-mail relay. All the tests had clear results. Interpretation was required for some test results, but was straightforward and uncomplicated. The system is clearly auditable.

Even thought the audit was thorough, it could not completely cover every possibility. Some of the general control objectives cover areas with an infinite variety of possibilities. Some cover areas that the e-mail relay cannot address.

With regard to unexpected input, the audit can only demonstrate that many known types of unexpected input are properly handled. It is impossible to audit an infinite number of ways to do something strange.

An enormous number of Linux and Postfix settings affect security. Although it would be theoretically possible to check all of them, it is not practical or affordable. In addition, achieving an adequate understanding of all the ways that all the settings interact is beyond the capabilities of most administrators. This audit is designed only to examine the settings that are known to result in high risks for this type of application.

Even a properly operating and properly secured e-mail system can be a gaping hole in an organization's security. Users can experience problems caused by e-mail including spam, social engineering attacks, worms, viruses, malicious attachments, and spyware. Blocking, filtering, and anti-virus software go a long way to alleviate these problems, but many unwanted and unsafe messages still get through. Even worse, malicious and careless users can send confidential information outside the organization inappropriately. The e-mail relay can reduce,

but not eliminate, exposure to e-mail-related problems. This audit is an effective tool for managing some problems, but is not a substitute for effective policies, procedures, and training.

Section 4 – Risk Assessment

Summary

The audit checklist was developed to determine how well the system controlled certain risks. The items to be tested were selected after evaluating the risks to the e-mail relay. The vulnerabilities that resulted in the highest risks (critical and high) were targeted for the audit. In addition, one low-risk item – backup management – was included to be consistent with best practices. The audit tested 36 specific items related to the security of the e-mail relay. (The first five items on the checklist are related to the audit process). Of the 36 items, 23 passed and 13 failed. The steps that failed and their control objectives are listed in the following table.

Table 10 – Audit steps that failed

Audit Step	Control Objective
9	Ensure that the e-mail relay only accepts unsolicited internal network communications as planned.
15	Protect the system against newly discovered vulnerabilities.
17	Ensure that the e-mail relay only accepts unsolicited internal network communications as planned.
18	Only necessary daemons are to be running on the system.
19	OpenSSH is being used and is the latest version.
20	The configuration of OpenSSH complies with best practices.
21	Verify that SSH is using PAM for authentication.
25	Ensure that password policy enforced by the computer is consistent with best practices.
27	Ensure that NFS and NIS are not present on the system.
38	Reduce the number of spoofed e-mail messages.
39	Verify that Postfix runs in chroot jail for enhanced security.
41	Ensure that the IDS (remote log server) logs and e-mail relay logs are adequately reviewed.
42	Ensure system can be recovered in the case of loss or failure.

To summarize, most of the deficiencies noted are a result of the following:

- System updating is inadequate.
- Several Linux configuration items and one Postfix configuration item are not consistent with best practices.
- Two current operating procedures are not adequate: log reviews and backup management.
- Spoofed e-mail is not controlled by the e-mail relay.

Configuration issues are easily correctable and will be addressed later in this section. Of the two operational items, backup management is easily addressed by implementing and adhering to an appropriate backup policy.

Two items are not easily addressed: adequate review of system logs and spoofed e-mail. These are discussed in detail below.

Background/risk

The audit produced several findings. Each of these refers to one or more audit steps and identifies risks that have not been adequately controlled.

Finding 1: (Reference: Audit Steps 15 and 19) Patching should be done more frequently, especially where packages critical to the system's security are concerned. New vulnerabilities are continually discovered. Keeping patches current minimizes the opportunity to exploit new vulnerabilities. A new vulnerability may allow an attacker to gain complete control over the e-mail relay. Once that was done, he could use the server in limitless ways, including attacking the rest of the internal network, attacking other networks, storing and trading illegally copied files, and sniffing e-mail traffic for confidential information. The results could include disclosure of confidential information, loss of client confidence, loss of credibility, and denial of service.

Finding 2: (Reference: Audit Step 9 and 17) The firewall on the e-mail relay (iptables) does not allow UDP port 123 from the internal network, which is needed to allow internal hosts to synchronize time. This is specified as a requirement in the network controls in Section 1. Although this finding does not compromise the security of the e-mail relay, it does compromise the security of the rest of the network, including the remote logging server (IDS), by increasing the risk that the clocks on the internal network cannot be synchronized (time synchronization uses more than one host – the email relay is redundant). Time synchronization is important for proper log management because log events from different computers may need to be analyzed together.

Finding 3: (Reference: Audit Steps 18, 20, 21,25 and 27) Several Linux configuration items are not consistent with best practices.

- RPC services are running and are not necessary.
- OpenSSH is not configured correctly.
- Appropriate password policy is not enforced.
- NFS and NIS are present on the system.

The risk associated with these items is the same as discussed above in Finding 1.

Finding 4: (Reference: Audit Step 38) Postfix does not verify source addresses. Without source address verification, e-mail can be spoofed easily by pretending

to come from a source different from the actual source. Users can be fooled into opening malicious attachments that appear to be from trusted sources. In addition, some types of social-engineering attacks are based on spoofed e-mails. In addition, spammers use e-mail spoofing to prevent detection and avoid accountability. In the worst case, a malicious attachment could be a Trojan that could compromise an internal host, with most of the consequences discussed in Finding 1. A more likely scenario is that a worm or virus could be contained in a zip file or other type of attachment that is not blocked.

Finding 5: (Reference: Audit Step 39) Postfix is not running in chroot jail. In the unlikely event that an attacker were successful in executing a buffer overrun or other type of attack against Postfix that allowed a command shell, the attacker would have access to the entire server (but restricted to the Postfix user's privileges). The attacker would then have the ability to attempt to exploit the server. Running Postfix processes under chroot would restrict the attacker to the Postfix execution environment, limiting the opportunity to damage or exploit the rest of the system.

Finding 6: (Reference: Audit Step 41) Log review is inadequate to ensure timely detection of problems. Although logs are normally reviewed daily, sometimes several days may pass between reviews. In addition, the logs are too large to review adequately. LogWatch reports significant entries once per day, but does not capture all relevant information. There is still a significant chance that a malfunction or a change to the system – either of which could be caused by an attacker – could occur, but not be detected soon enough. The result of an attack would be the same as discussed in Finding 1, but if the attack were noticed quickly enough, there would be a chance to prevent some or all of the damage.

Finding 7: (Reference: Audit Step 42) Backups are inadequate to ensure ability to recover from failure or loss efficiently. In the event of a failure or loss of the e-mail relay, the system would have to be rebuilt by re-loading Linux and Postfix and manually configuring. Although this process would be time-consuming, there are no business related files stored on the relay, so the damage would be restricted to the loss of service during the recovery. In addition, if the Postfix configuration were not available, there would be the additional risk of the Postfix application controls not working as they did before the loss.

System Changes and Further Testing

Many of the findings were directly attributable to Linux and Postfix configuration details. Specifically, the following items summarize these findings:

- The system did not have current patches.
- The Linux firewall did not have a rule to allow internal hosts to synchronize with its NTP server.
- RPC, NFS and NIS packages were present on the system
- OpenSSH was not configured according to best practices.

- Password policy was not consistent with best practices.
- Postfix processes were not running under chroot.

The items that resulted in Findings 1, 2, 3, and 5 were determined to be easily correctable by performing the following steps:

1. Use the up2date command to update all patches to current levels.
2. Add a rule to the firewall on the e-mail relay to allow UDP port 123 from the internal network.
3. Remove RPC, NFS and NIS (all are RPM packages).
4. Make the following changes to configuration files (NOTE: added lines override defaults):
    a. /etc/ssh/ssh_config
        1. Add: StrictHostKeyChecking yes
        2. Add: Protocol 2
        3. Add: Cipher blowfish
    b. /etc/ssh/sshd_config
        1. Add: Protocol 2
        2. Add: LoginGraceTime 60
        3. Add: IgnoreUserKnownHosts yes
    c. /etc/pam.d/sshd
        1. Add: account required pam_access.so
        2. Add: account required pam_time.so
    d. /etc/logins.def
        1. PASS_MAX_DAYS 9999 → PASS_MAX_DAYS 90
        2. PASS_MIN_LEN 5 → PASS_MIN_LEN 8
5. In the Postfix configuration file /etc/postfix/master.cf change all “n” entries to “y” entries in the chroot column for all services except pipe and local.

It was decided to make immediate changes to the system to address these findings. These changes were performed on 31 Oct. 2003 and the system was rebooted. The following are the results of the retest of the associated checklist steps.

AUDIT STEP – 9 PASS

Test network input controls listed in Section 1 regarding unsolicited internal network traffic.

Because the retest is only confirming that the server is now accepting UDP port 123 and because the initial scanning took an extremely long time, only the nmap default ports were scanned and only for UDP. The following figure contains results from the UDP scans. The scan was performed from the organization’s network. The syntax for the nmap scan is included in the output.

Figure 27 – Retest: internal nmap scan

```
# nmap (V. 3.00) scan initiated Thu Oct 30 14:03:41 2003 as: nmap -v -
sU -r -P0 -oN int_nmap_UDP.retest.txt 192.168.10.2
Interesting ports on relay.xxxx.com (192.168.10.2):
(The 1467 ports scanned but not shown below are in state: closed)
Port       State       Service
123/udp    open        ntp

# Nmap run completed at Thu Oct 30 14:28:01 2003 -- 1 IP address (1
host up) scanned in 1460 seconds
```

The network input controls defined in Section 1 specify that UDP port 123 be allowed from the internal network. The scan reports the port is open. This audit step passes.

AUDIT STEP – 15 PASS

Verify that the operating system patches are current.

The up2date command was used to determine if any system patches needed to be installed after the system changes were made.

Figure 28 – Retest: system patches that need to be installed

```
[root@relay root]# up2date -l

Fetching package list for channel: redhat-linux-i386-9...
########################################

Fetching Obsoletes list for channel: redhat-linux-i386-9...
########################################

Fetching rpm headers...

Name                                    Version        Rel
----------------------------------------------------------
```

The results show no packages are out of date. This audit step passes.

AUDIT STEP – 17 PASS

Determine if the firewall on the e-mail relay (iptables) is properly configured and enabled.

The firewall configuration below shows the rules in use after the system changes were made:

Figure 29 – Retest: e-mail relay firewall rules (iptables)

```
root@relay root]# iptables -L -v
Chain INPUT (policy ACCEPT 344K packets, 213M bytes)
 pkts bytes target     prot opt in     out     source
destination
2319K  301M RH-Lokkit-0-50-INPUT  all  --  any    any     anywhere
anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination
    0     0 RH-Lokkit-0-50-INPUT  all  --  any    any     anywhere
anywhere

Chain OUTPUT (policy ACCEPT 567K packets, 129M bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain RH-Lokkit-0-50-INPUT (2 references)
 pkts bytes target     prot opt in     out     source
destination
    1    76 ACCEPT     udp  --  any    any     ns3.oit.unc.edu
anywhere           udp spt:ntp dpt:ntp
    1    76 ACCEPT     udp  --  any    any     ntp1.jrc.us
anywhere           udp spt:ntp dpt:ntp
    9   684 ACCEPT     udp  --  any    any     ns1.usg.edu
anywhere           udp spt:ntp dpt:ntp
    1    76 ACCEPT     udp  --  any    any     mcs.anl.gov
anywhere           udp spt:ntp dpt:ntp
   17  1292 ACCEPT     udp  --  any    any     proxy.cc.vt.edu
anywhere           udp spt:ntp dpt:ntp
    0     0 ACCEPT     udp  --  any    any     proxy.cc.vt.edu
anywhere           udp spt:ntp dpt:ntp
    5   380 ACCEPT     udp  --  any    any     ntp1.usno.navy.mil
anywhere           udp spt:ntp dpt:ntp
    0     0 ACCEPT     udp  --  any    any     ns1.usg.edu
anywhere           udp spt:ntp dpt:ntp
    0     0 ACCEPT     udp  --  any    any     proxy.cc.vt.edu
anywhere           udp spt:ntp dpt:ntp
  151 11092 ACCEPT     udp  --  any    any     192.168.10.0/24
anywhere           udp dpt:ntp
22049 2533K ACCEPT     udp  --  any    any     xxxxxxx.xxxx.com
anywhere           udp spt:domain dpts:1025:65535
 2834  151K ACCEPT     tcp  --  any    any     anywhere
anywhere           tcp dpt:smtp flags:SYN,RST,ACK/SYN
   23  1108 ACCEPT     tcp  --  any    any     192.168.10.0/24
anywhere           tcp dpt:ssh flags:SYN,RST,ACK/SYN
  155 19322 ACCEPT     all  --  lo     any     anywhere
anywhere
  529 53743 ACCEPT     udp  --  any    any     xxxxxxxxxx.xxxx.com
anywhere           udp spt:domain
 825K   44M REJECT     tcp  --  any    any     anywhere
anywhere           tcp flags:SYN,RST,ACK/SYN reject-with icmp-port-
unreachable
```

```
1123K   40M REJECT     udp  --  any    any     anywhere
anywhere           udp reject-with icmp-port-unreachable
```

The relevant rules are in the section RH-Lokkit-0-50-INPUT. (The first several rules are entered automatically by the ntpd startup script.) The rules show the following:

- UDP is allowed from any host on the internal network to allow synchronization with the e-mail relay's NTP server. (This rule was added during the system changes.)
- UDP is allowed for synchronization with external NTP servers.
- UDP is allowed from the internal DNS servers.
- SMTP is allowed from anywhere.
- SSH is allowed from any host on the internal network.
- All other TCP and UDP packets are rejected.

The firewall is consistent with all network input controls specified in Section 1. This audit step passes.

AUDIT STEP – 18 PASS

Verify that only necessary daemons are running on the system.

The netstat command was used to capture information about running processes to a file:

Figure 30 – Retest: results of "netstat -atu"

```
[root@relay root]# netstat -atu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address
State
tcp        0      0 *:ssh                   *:*
LISTEN
tcp        0      0 *:smtp                  *:*
LISTEN
tcp        0      0 relay.xxxx.com:smtp   xxx.xxxxxxxxx.c:35677
ESTABLISHED
tcp        0      0 relay.xxxx.com:ssh    xxxx.xxxx.com:3329
ESTABLISHED
udp        0      0 *:syslog                *:*
udp        0      0 relay.xxxx.com:ntp    *:*
udp        0      0 relay.xxxx.com:ntp    *:*
udp        0      0 *:ntp                   *:*
```

The lsof command was used to determine the active network sockets:

Figure 31 – Retest: results of "lsof -i +M"

```
[root@relay root]# lsof -i +M
COMMAND  PID    USER   FD   TYPE DEVICE SIZE NODE NAME
syslogd  494    root    7u  IPv4    911       UDP *:syslog
sshd     594    root    3u  IPv4   1087       TCP *:ssh (LISTEN)
master   714    root   11u  IPv4   1298       TCP *:smtp (LISTEN)
sshd     801    root    4u  IPv4   1827       TCP relay.xxxx.com:ssh-
>xxxx.xxxx.com:3329 (ESTABLISHED)
sshd     803     noc    4u  IPv4   1827       TCP relay.xxxx.com:ssh-
>xxxx.xxxx.com:3329 (ESTABLISHED)
ntpd    1018     ntp    4u  IPv4   3135       UDP *:ntp
ntpd    1018     ntp    5u  IPv4   3136       UDP relay.xxxx.com:ntp
ntpd    1018     ntp    6u  IPv4   3137       UDP relay.xxxx.com:ntp
smtpd   1024 Postfix    6u  IPv4   1298       TCP *:smtp (LISTEN)
smtpd   1024 Postfix    9u  IPv4   3218       TCP relay.xxxx.com:smtp-
>xxx.xxxxxxxxxx.com:35677 (ESTABLISHED)
```

This system is running SSH, SMTP, NTP, and syslog (all of which are required). It is not running any other services. This audit step passes.

AUDIT STEP – 19 PASS

Verify that OpenSSH is being used and is the latest version.

Use the netstat command to see if ssh is running. Use the ssh command to determine the version of ssh:

Figure 32 – Retest: OpenSSH use and version

```
[root@relay root]# netstat -at | grep ssh
tcp        0      0 *:ssh                   *:*
LISTEN
tcp        0      0 relay.xxxx.com:ssh    xxxxxxxxxx.xxxx.:2350
ESTABLISHED
[root@relay root]# ssh -V
OpenSSH_3.5p1, SSH protocols 1.5/2.0, OpenSSL 0x0090701f
[root@relay root]#
```

The results show OpenSSH is running and is version 3.5p1. The current version offered by Red Hat is 3.5p1 – 11. This step passes.

AUDIT STEP – 20 PASS

Determine if OpenSSH is properly configured.

The following is the contents of the configuration file /etc/ssh/ssh_config:

Figure 33 – Retest: contents of /etc/ssh/ssh_config

```
[root@relay init.d]# cat /etc/ssh/ssh_config
#     $OpenBSD: ssh_config,v 1.16 2002/07/03 14:21:05 markus Exp $

# This is the ssh client system-wide configuration file.  See
# ssh_config(5) for more information.  This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.

# Configuration data is parsed as follows:
#  1. command line options
#  2. user-specific file
#  3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for various options

# Host *
#   ForwardAgent no
#   ForwardX11 no
#   RhostsAuthentication no
#   RhostsRSAAuthentication no
#   RSAAuthentication yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   BatchMode no
#   CheckHostIP yes
StrictHostKeyChecking yes
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/identity
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   Port 22
Protocol 2
#   Protocol 2,1
Cipher blowfish
#   Cipher 3des
#   Ciphers aes128-cbc,3des-cbc,blowfish-cbc,cast128-
cbc,arcfour,aes192-cbc,aes256-cbc
#   EscapeChar ~
Host *
      ForwardX11 yes
```


The following is the contents of the configuration file /etc/ssh/sshd_config:

Figure 34 – Retest: contents of /etc/ssh/sshd_config

```
#     $OpenBSD: sshd_config,v 1.59 2002/09/25 11:17:16 markus Exp $
```

```
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

#Port 22
Protocol 2
#Protocol 2,1
#ListenAddress 0.0.0.0
#ListenAddress ::

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 3600
#ServerKeyBits 768

# Logging
#obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

LoginGraceTime 60
#LoginGraceTime 120
PermitRootLogin no
#StrictModes yes

#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile     .ssh/authorized_keys

# rhosts authentication should not be used
#RhostsAuthentication no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes
# For this to work you will also need host keys in
/etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
IgnoreUserKnownHosts yes
#IgnoreUserKnownHosts no
```

```
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

#AFSTokenPassing no

# Kerberos TGT Passing only works with the AFS kaserver
#KerberosTgtPassing no

# Set this to 'yes' to enable PAM keyboard-interactive authentication
# Warning: enabling this may bypass the setting of
'PasswordAuthentication'
#PAMAuthenticationViaKbdInt no

#X11Forwarding no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PrintMotd yes
#PrintLastLog yes
#KeepAlive yes
#UseLogin no
#UsePrivilegeSeparation yes
#PermitUserEnvironment no
#Compression yes

#MaxStartups 10
# no default banner path
#Banner /some/path
#VerifyReverseMapping no

# override default of no subsystems
Subsystem   sftp  /usr/libexec/openssh/sftp-server
```

All items required by the audit step are in ssh_config and sshd_config. This audit step passes.

AUDIT STEP – 21 PASS

Determine if PAM password authentication is being used for OpenSSH.

The contents of the /etc/pam.d/sshd file:

Figure 35 – Retest: contents of /etc/pam.d/sshd

```
#%PAM-1.0
auth       required     pam_stack.so service=system-auth
auth       required     pam_nologin.so
account    required     pam_access.so
account    required     pam_time.so
account    required     pam_stack.so service=system-auth
password   required     pam_stack.so service=system-auth
session    required     pam_stack.so service=system-auth
session    required     pam_limits.so
session    optional     pam_console.so
```

All entries required by the audit step are present. The audit step passes.

AUDIT STEP – 25 PASS

Determine if minimum password length and maximum password age are enforced.

The following is the contents of the password aging controls section of the /etc/login.defs file:

Figure 36 – Retest: password-aging controls

```
# Password aging controls:
#
#     PASS_MAX_DAYS     Maximum number of days a password may be used.
#     PASS_MIN_DAYS     Minimum number of days allowed between password
changes.
#     PASS_MIN_LEN      Minimum acceptable password length.
#     PASS_WARN_AGE     Number of days warning given before a password
expires.
#
PASS_MAX_DAYS    90
PASS_MIN_DAYS    0
PASS_MIN_LEN     8
PASS_WARN_AGE    14
```

The PASS_MAX_DAYS and PASS_MIN_LENTH comply with the stated values of 90-day maximum age and eight characters minimum length. This audit step passes.

The following session shows the creation of a test account “foo” and several attempts to change the password using a variety of unacceptable choices:

Figure 37 – Retest: password change

```
[root@relay root]# adduser foo
[root@relay root]# echo alpha | passwd foo
Changing password for user foo.
New password: BAD PASSWORD: it is too short
Retype new password:
New password:
New password:
passwd: Conversation error
[root@relay root]# echo alphabet | passwd foo
Changing password for user foo.
New password: BAD PASSWORD: it is based on a dictionary word
Retype new password:
New password:
New password:
passwd: Conversation error
[root@relay root]# echo abababab | passwd foo
Changing password for user foo.
New password: BAD PASSWORD: it does not contain enough DIFFERENT
characters
Retype new password:
New password:
New password:
passwd: Conversation error
[root@relay root]# echo 12345678 | passwd foo
Changing password for user foo.
New password: BAD PASSWORD: it is too simplistic/systematic
Retype new password:
New password:
New password:
passwd: Conversation error
[root@relay root]# echo swo983ab | passwd foo
Changing password for user foo.
New password: Retype new password:
New password:
New password:
passwd: Conversation error
[root@relay root]# echo 'swo983ab' | passwd foo --stdin
Changing password for user foo.
passwd: all authentication tokens updated successfully.
[root@relay root]# userdel foo
[root@relay root]#
```

Passwords that were too short or lacked enough complexity were rejected. (Note that the last password was not rejected, but the conversation error would not allow the command to complete. The --stdin option allowed the command to execute correctly, but was not used in the previous cases because the errors would not have been displayed.) The audit step passes.

AUDIT STEP – 27 PASS

Determine if NFS and NIS are installed.

The rpm command was used to determine if the packages for NFS and NIS were installed.

Figure 38 – Retest: NFS and NIS packages removed

```
[root@relay log]# rpm -q nfs-utils
package nfs-utils is not installed
[root@relay log]# rpm -q ypbind
package ypbind is not installed
root@relay log]#
```

The results show that both packages have been removed. This audit step passes.

AUDIT STEP – 39 PASS

Determine if Postfix is running in chroot jail.

Only the changes in the configuration file /etc/postfix/master.cf were retested. The following is the configuration file with the documentation section removed.

Figure 39 – Retest: Postfix master.cf file

```
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (50)
# ==========================================================================
smtp      inet  n       -       y       -       -       smtpd
#628      inet  n       -       n       -       -       qmqpd
pickup    fifo  n       -       y       60      1       pickup
cleanup   unix  n       -       y       -       0       cleanup
qmgr      fifo  n       -       y       300     1       qmgr
#qmgr     fifo  n       -       n       300     1       nqmgr
rewrite   unix  -       -       y       -       -       trivial-rewrite
bounce    unix  -       -       y       -       0       bounce
defer     unix  -       -       y       -       0       bounce
flush     unix  n       -       y       1000?   0       flush
smtp      unix  -       -       y       -       -       smtp
showq     unix  n       -       y       -       -       showq
error     unix  -       -       y       -       -       error
local     unix  -       n       n       -       -       local
virtual   unix  -       n       y       -       -       virtual
lmtp      unix  -       -       y       -       -       lmtp
#
# Interfaces to non-Postfix software. Be sure to examine the manual
# pages of the non-Postfix software to find out what options it wants.
```

```
# The Cyrus deliver program has changed incompatibly.
#
cyrus     unix  -       n       n       -       -       pipe
  flags=R user=cyrus argv=/cyrus/bin/deliver -e -m ${extension} ${user}
uucp      unix  -       n       n       -       -       pipe
  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)
ifmail    unix  -       n       n       -       -       pipe
  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
bsmtp     unix  -       n       n       -       -       pipe
  flags=Fq. user=foo argv=/usr/local/sbin/bsmtp -f $sender $nexthop $recipient
```

The configuration file shows that all Postfix processes are running under chroot except local and pipe. This audit step passes.

System Justification

Testing subsequent to the system changes shows that all audit steps that pertained to the changes now pass.

The post-remediation state of the risk model is shown in the following table. It includes the pre-audit state for comparison. It shows a significant reduction of overall risk compared to the pre-audit state, when the system was pessimistically assumed wide open to attack.

Table 11 – Post-remediation risk by vulnerability

Ref.	Vulnerability	Audit Step and Result	Comments	Post-audit Vulnerability Rating	Pre-audit Risk	Post-remediation Risk
V1	Dependence on physical environment to be able to operate	Step – 7: PASS	Risk is not eliminated	Low – 0.12	**10 - High**	**1.4 - Medium**
V2	Physical access	Step – 6: PASS	Risk is not eliminated. Calculation for risk changed from 23 to 4.4. Although both are categorized as high, this represents a significant decrease.	Low – 0.12	**23 - High**	**4.4 - High**
V3	Backup media may be corrupted or unavailable when needed (included as a best practice)	Step – 42: FAIL		Low – 0.12	**0.10 - Low**	**0.10 - Low**
V4	System malfunctions may not be detected timely	Step – 13: PASS Step – 14: PASS Step – 41: FAIL	The post-audit value for the vulnerability was reduced to medium because the logs are usually reviewed daily.	Medium – 0.37	**54 - Critical**	**32 - Critical**
V5	System changes may not be detected timely	Step – 13: PASS Step – 14: PASS Step – 41: FAIL	The post-audit value for the vulnerability was reduced to medium because the logs are usually reviewed daily.	Medium – 0.37	**54 - Critical**	**32 - Critical**
V6	System requires proper communication with DNS server, default gateway and network switch, system requires proper function of NAT on firewall	Step – 11: PASS Step – 12: PASS		NONE	**54. - High**	**NONE**
V7	SANS Top 20 – RPC vulnerability	Step – 8: PASS Step – 9: PASS Step – 17: PASS Step – 18: PASS		NONE	**76 - Critical**	**NONE**
V8	SANS Top 20 – General UNIX/Linux authentication – Accounts with no passwords or	Step – 8: PASS Step – 9: PASS		NONE	**76 - Critical**	**NONE**

Ref.	Vulnerability	Audit Step and Result	Comments	Post-audit Vulnerability Rating	Pre-audit Risk	Post-remediation Risk
	weak passwords	Step – 17: PASS Step – 22: PASS Step – 23: PASS Step – 24: PASS Step – 25: PASS Step – 26: PASS				
V9	SANS Top 20 – Clear text services	Step – 8: PASS Step – 9: PASS Step – 16:PASS Step – 17: PASS Step – 18: PASS Step – 19: PASS		NONE	**76 - Critical**	**NONE**
V10	SANS Top 20 – Secure Shell	Step – 8: PASS Step – 9: PASS Step – 10:PASS Step – 17: PASS Step – 19: PASS Step – 20: PASS Step – 21: PASS	Because OpenSSH is used and is on the Top 20 list, it is judged to still be a low-level vulnerability.	Low - .12	**76 - Critical**	**10 - High**
V11	SANS Top 20 – Misconfiguration of enterprise services NIS/NFS	Step – 8: PASS Step – 9: PASS Step – 17: PASS Step – 27: PASS		NONE	**76 - Critical**	**NONE**
V12	SANS Top 20 – Open Secure Sockets Layer SSL	Step – 8: PASS Step – 9: PASS Step – 17: PASS Step – 28: PASS		NONE	**76 - Critical**	**NONE**
V13	Other operating system patches may not be current	Step – 8: PASS Step – 9: PASS Step – 10:PASS Step – 15: PASS Step – 17: PASS		NONE	**54 - Critical**	**NONE**
V14	Other unnecessary services may be enabled	Step – 8: PASS Step – 9: PASS		NONE	**54 - Critical**	**NONE**

Ref.	Vulnerability	Audit Step and Result	Comments	Post-audit Vulnerability Rating	Pre-audit Risk	Post-remediation Risk
		Step – 10:PASS Step – 16:PASS Step – 17: PASS Step – 18: PASS				
V15	E-mail encapsulates almost anything and bypasses most network controls	Step – 29: PASS Step – 30: PASS Step – 31: PASS Step – 32: PASS Step – 33: PASS Step – 34: PASS Step – 38: FAIL	Most UCE is filtered. However, spoofed e-mail is still a problem, especially when combined with attachments with .zip extensions, which are allowed.	High - .62	**76 - Critical**	**54 – Critical**
V16	SMTP does not check source addresses	Step – 38: FAIL	See comment in previous step.	Critical - .87	**54 - Critical**	**54 - Critical**
V17	E-mail relay could operate as an open relay	Step – 35: PASS Step – 40: PASS		NONE	**76 - Critical**	**NONE**
V18	Postfix environment may not be secured optimally	Step – 29: PASS Step – 39: PASS Step – 40: PASS		NONE	**32 - Critical**	**NONE**
V19	E-mail relay may not correctly perform its normal function	Step – 36 PASS Step – 37 PASS		NONE	**5.4 - High**	**NONE**

With regard to the risk model after the system changes were retested, two items, physical access and OpenSSH, still showed a higher level of risk than expected. After careful consideration, the conclusion was reached that this is a result of the design of the model, which does not allow a risk to be significantly mitigated in cases where a critical threat and a critical impact is associated with any remaining vulnerability. Using more appropriate values for very low levels of vulnerability would probably improve the model greatly. For purposes of this risk assessment, judgment and experience overrules the determination of the model for risk associated with physical access and OpenSSH. These are assumed to be medium risks at most and, from a business standpoint, do not warrant any effort to attempt to improve security in these areas.

Three findings were not addressed by system changes:

Finding 4: (Reference: Audit Step – 38) Postfix does not verify source addresses. Approximately a year ago, the organization attempted to reduce the amount of undesirable e-mail by implementing blocking based on checking source addresses. Strict source checking can stop many, but not all, spoofed messages; however, experience indicated that many other messages were blocked that the organization's employees expected and needed. The decision was made to continue to allow messages without checking source addresses until the Internet community as a whole consistently provides correct and verifiable information in their SMTP communications.

Finding 6: (Reference: Audit Step – 41) Log reviews are not adequate to catch problems quickly enough. The administrator reviews logs on the e-mail relay and the IDS (remote log server) daily. Exceptions occur during business trips, vacations, and occasional periods of heavy workloads where other matters take higher priority. Other employees who assume the administrator's role during his absence do not review logs. Besides the occasional gap in the daily review discipline, the logs have too much information to review thoroughly each day. LogWatch runs on both systems and reports some items each day. The likelihood is too high that a problem may go undetected in time to minimize the impact. This situation is not desirable because it exposes an otherwise well-secured system to unnecessary risk. A proposal will be made to management to invest the time and resources to implement better automated analysis and alerting.

Finding 7: (Reference: Audit Step – 42) Backup management is not adequate. Backups are not routinely made for the e-mail relay. Linux and Postfix patches are installed without making backups. Linux configuration changes are not usually backed up. Postfix configuration changes are backed up sporadically. Although rebuilding the system from scratch would not be difficult, recreating the exact details of the Postfix blocking and filtering files would not be possible, and several weeks would elapse before the filters would be tuned adequately. Because of the ease of correcting this deficiency, a new procedure will be implemented to require backups of all changes on all the organization's servers.

In addition to the findings addressed by the audit, significant risks remain that are inherent to a normally operating e-mail system. SMTP sends messages in clear text. Messages can be sniffed and intercepted. Users can experience problems caused by e-mail including spam, social engineering attacks, worms, viruses, malicious attachments, and spyware. Blocking, filtering, and anti-virus software go a long way to alleviate these problems, but many unwanted and unsafe messages still get through. Even worse, malicious and careless users can send confidential information outside the organization inappropriately. The e-mail relay can reduce, but not eliminate, exposure to e-mail-related problems. These issues are not and cannot be addressed by the e-mail relay, but must be addressed through a comprehensive, organization-wide program of security tools, processes, procedures, training and audits.

References

- "LINUX+ ~ Chapter 7 ~ Linux Installation." URL: http://www.mullensystems.com/~john/ebook/chapter_07.htm (25 Oct. 2003).
- "Listing 2. Generating Messages for All Facilities at Each Priority." URL: http://www.linuxjournal.com/modules.php?op=modload&name=NS-lj-issues/issue92&file=5476l2 (19 Oct 2003).
- "Nmap Network Security Scanner Man Page." URL: http://www.insecure.org/nmap/data/nmap_manpage.html (5 Nov. 2003).
- "Physical Security Audit Checklist." URL: http://www.knowledgeleader.com/iafreewebsite.nsf/content/TechnologyAuditPhysicalSecurityAuditChecklist?OpenDocument (19 Oct. 2003).
- "Postfix Configuration – UCE Controls." URL: http://www.postfix.org/uce.html (26 Oct 3003).
- "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus." Version 4.0. 8 Oct. 2003. URL: http://isc.sans.org/top20.html#u1 (11 Oct. 2003).
- Bauer, Mick. "Issue 92: Paranoid Penguin: syslog Configuration." 1 Dec. 2001. URL: http://www.linuxjournal.com/article.php?sid=5476 (19 Oct. 2003).
- Bauer, Mick and de Winter, Brenno. "Using Postfix for Secure SMTP Gateways." 13 Sep. 2000. URL: http://www.postfix.org/linuxjournal.200010/4241.html (26 Oct. 2003).
- Blum, Richard. Postfix. Indianapolis: Sams Publishing, 2001.
- Custódio, Filipe. "Auditing Microsoft Corporate e-mail Solutions (Exchange 5.5 and Outlook 2000)." Sep. 2001. URL: http://www.giac.org/practical/Filipe_Custodio_GSNA.zip (4. Oct. 2003).
- Davis, Noel. "Postfix Attack." 11 Aug. 2003. URL: http://linux.oreillynet.com/pub/a/linux/2003/08/11/insecurities.html (18 Oct. 2003).
- Eychenne, Herve. "Iptables(8)." man pages. Redhat 9.0. 9 Mar. 2002.
- Kurz, Christian. "LINUX2 – shell script to set up a Postfix chroot jail for Linux." 1 Feb. 2002. URL: http://orange.kame.net/dev/cvsweb.cgi/postfix/examples/chroot-setup/LINUX2?rev=1.1.1.5&cvsroot=apps (26 Oct. 2003).

- Mina, Ted. “Application Security, Information Assurance’s Neglected Stepchild – A Blueprint for Risk Assessment.” 18-20 May 2001. URL: http://www.sans.org/rr/paper.php?id=56 (4 Oct. 2003).

- Peeples, Donald. “The Foundations of Risk Management.” 6 May 1997. URL: http://csrc.nist.gov/nissc/1997/proceedings/577slides.pdf (11 Oct. 2003).

- Rassmussen, Scott. “Centralized Network Security Management: Combining Defense In Depth with Manageable Security.” 29 Jan. 2002. URL: http://www.sans.org/rr/practice/central_netsec.php (18 Oct 2003).

- Russell, Rusty. “Linux iptables HOWTO.” 29 Sep. 1999. URL: http://www.linuxguruz.com/iptables/howto/iptables-HOWTO.html (20 Oct 2003).

- Wassom, Darrin. “Auditing a Distributed Intrusion Detection System: An Auditors Perspective.” 1Jul. 2002. URL: http://www.sans.org/rr/paper.php?id=824 (18 Oct. 2003).