Global Information Assurance Certification Paper

Auditing an ISP POP/IMAP Email Server

An Independent Auditor's Perspective

SANS GSNA Practical Assignment
Version 2.1
Option 1
2-23-2004

Mike Maxwell GCIA

Table of Contents

Assignment Abstract 4

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

Primary Goal of this Audit 4
Identify the System to be Audited 4
Hardware Model and Operating System and Software Versions 4
The System's Role in the Organization 5
Simplified Network Diagram 6
Network Level Access and Input Controls 6
Evaluate the Risk to the System 7
Physical Threats 8
Software Vulnerabilities 8
Network Access 9
Administrator Misconfiguration or Error 9
What is the Current State of Practice? 10

Assignment 2 – Create an Audit Checklist

Item 1 –Physical Security 11
Item 2 –Ensure that all patches have been applied 13
Item 3 –Ensure that SSH is in use 13
Item 4 –Ensure remote syslog is in use and working properly 14
Item 5 –Ensure xinetd is only running necessary services 15
Item 6 –Ensure SMTP service only receives traffic from Filtering server 15
Item 7 –Verify that all end user accounts have /bin/false Shell 16
Item 8 –Verify that shadow passwords are in use for all Accounts 17
Item 9 –Verify that only "root" has console login permissions 17
Item 10 –Verify that the host based IDS Portsentry is in use 18
Item 11 –Verify that original sendmail package has been Removed 19
Item 12 –Verify than change documentation is maintained For the server 19
Item 13 –Test network level controls from outside the Server segment 20
Item 14 –Verify all listening services on the system 20
Item 15 –Verify system backups are performed regularly And valid 21
Item 16 –Ensure logs are monitored and notification procedure Is in place 22

Item 17 –Verify that regular vulnerability scans are performed 23
Item 18 –Are the Qmail packages installed the latest 23
Available versions
Item 19 –Does the server comply with written security policies 24
For the system
Item 20 –Is NTP in use for time synchronization 24

Assignment 3 –Audit Evidence

Conduct the Audit
Checklist Item 3 –Ensure that SSH is in use 25
Checklist Item 4 –Ensure remote syslog is in use and working 27
Properly
Checklist Item 5 –Ensure xinetd is only running necessary services 30
Checklist Item 6 –Ensure SMTP service only receives traffic from 30
Filtering server
Checklist Item 9 –Verify that only "root" has console login 31
Permissions
Checklist Item 10 –Verify that the host based IDS Portsentry 33
Is in use
Checklist Item 11 –Verify that original sendmail package has 35
Been removed
Checklist Item 13 –Test network level controls from outside the 36
Server segment
Checklist Item 14 –Verify all listening services on the system 37
Checklist Item 19 –Does the server comply with written security 38
Policies for the system?

Measure Residual Risk
Summary of Audit Results 39
Evaluate the Audit 42

Assignment 4 –Audit Report

Executive Summary

Assignment Abstract

The following paper consists of four closely related sections. Section one defines best practices for auditing the system in question and defines control objectives and methods for completion using technology. Section two establishes an audit checklist for meeting the control objectives. Section three provides examples of ten of the objectives from the audit checklist in section two being performed. Section four provides an audit report summarizing all of the audit's findings and recommendations for actions to resolve issues discovered during the audit.

Assignment One – Research in Audit, Measurement Practices, and Control

Primary Goal of this Audit

The primary reason the ISP has requested the audit of all of their systems is to provide them with a framework for building a security strategy for the entire company. When the business was started, their main focus was on establishing a customer base and building a quality reputation. Over the past few years, they have fallen victim to occasional security breaches that have resulted in damage to this reputation and unplanned system downtime. They have decided that it is imperative for the future success of their business to define a security strategy to prevent any further damage to the business.

Identify the system to be audited

The system to be audited for this assignment is an Internet Service Provider's POP/IMAP email server. This system is responsible for all email services provided by the ISP that have to do with delivery to the customers. Outbound SMTP and inbound virus and SPAM filtering are provided by separate standalone systems. The box is located on a “server only” subnet with all of the other ISP's servers. While the primary scope of this audit is the email server itself, the ISP has requested that we investigate the network level access controls in place for this system as well. All network level controls are performed using Cisco ACLs on a Cisco 3640 running IOS version 12.1(5)T15. We will not concern ourselves with the security of the router itself, but only whether or not appropriate network access controls are in place.

Hardware Model and Operating System and Software Versions

The server is a Dell Poweredge 6650 running RedHat Linux Enterprise Edition v3.0. It is equipped with redundant network cards and power supplies and utilizes a RAID controller to provide a RAID level 5 disk array for fault tolerance.

The MTA (Mail Transfer Agent) running on the system is Qmail version 1.03. Qmail was chosen for its improved security over sendmail. Instead of running the entire mail delivery process as a single user (root), Qmail breaks the process

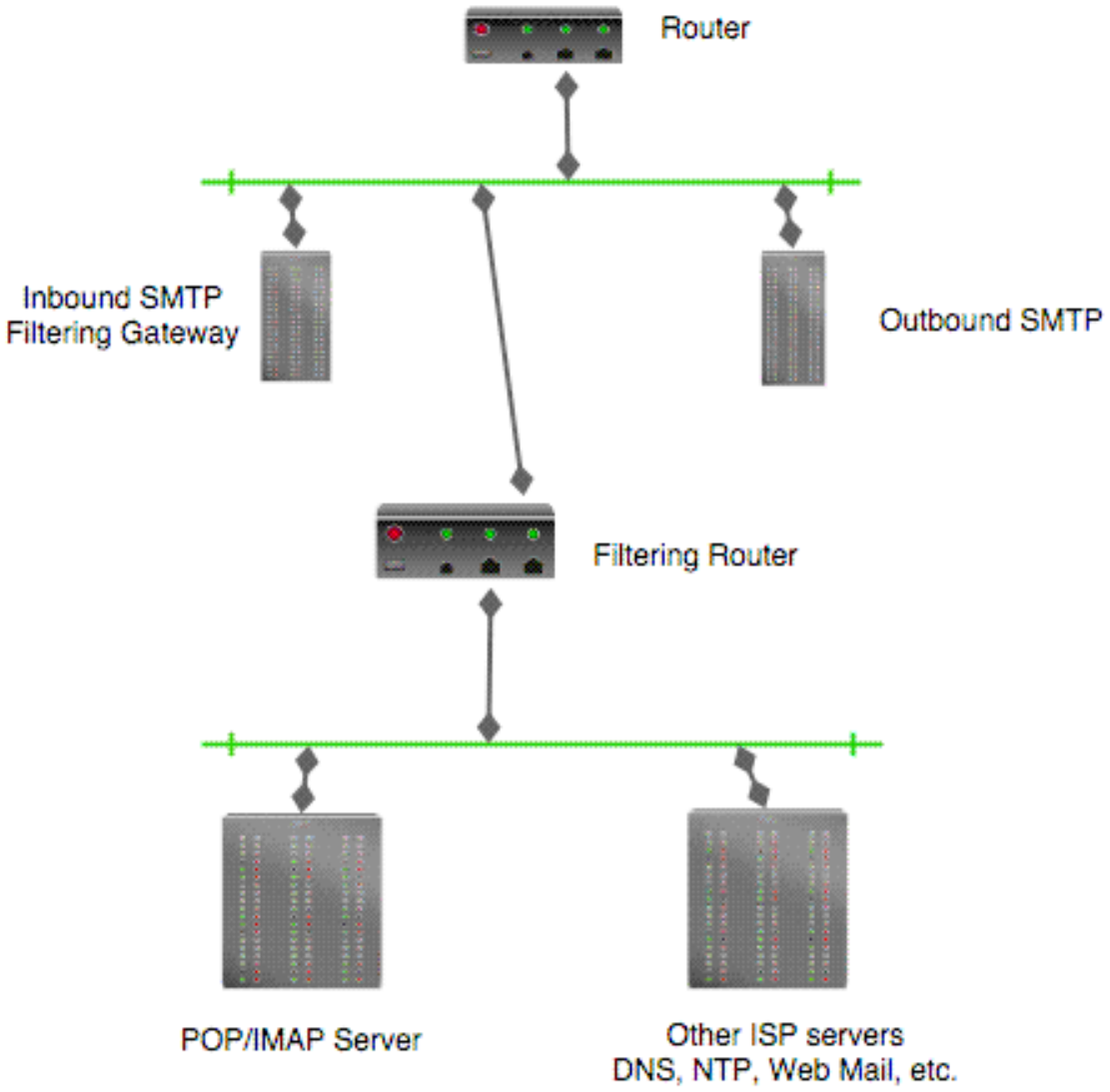
of delivery into multiple sections controlled by separate users with the minimal level of privilege necessary to complete their respective tasks. In fact there is still an outstanding $500 reward to anyone who can publish a substantiated vulnerability relating to the Qmail software. [1]

The POP/IMAP server being used is the most current version of the University of Washington IMAP daemon provided with the RedHat distribution (imap-2002d-2 at the time of this writing).

The System's Role in the Organization

The ISP counts on this server to be available and functioning at all times. This system is responsible for providing POP/IMAP email services to all of the ISP's employees and customers. Any unscheduled downtime results in almost immediate complaints from paying customers of the company. Many of the ISP's customers are business that outsource all email functions to the ISP and rely on timely and reliable communications.

Simplified Network Diagram



Network Level Access and Input Controls

As mentioned earlier, all network level controls are done using ACL's on a Cisco 3640 router. A router was chosen over a firewall when the network was setup to help keep down startup costs for the ISP. As time has progressed, the administrator has realized an increasing need for a firewall and has plans to deploy one in the near future. The following is the relevant part of the access list that controls traffic to the POP/IMAP server.

```
access-list 150 permit tcp any host 192.168.2.35 eq 110
access-list 150 permit tcp host 192.168.1.30 host 192.168.2.35 eq 25
access-list 150 permit tcp host 10.0.1.32 host 192.168.2.35 eq 22
access-list 150 deny ip any any log
```

As you can see, there is very little inbound traffic allowed to reach the server. All other necessary services, including DNS, NTP, and Syslog, are provided to the system on its own subnet. As you can see, even IMAP traffic is not permitted from the outside in. This is because the IMAP service is only being run to provide Web Mail services to the ISP's customers, and the Web Mail systems resides on this subnet as well.

The SMTP rule from above allows SMTP connections only from the ISP's email filtering gateway machine. There is no DNS MX record for this server, and it therefore has no need to receive email directly from anywhere but the filtering server. The SSH rule permits on the system administrator's management workstation access to the system. The account used for this access is the only user on the system that has an actual shell. All other user accounts are configured with /bin/false as their default shell.

The only outbound filtering being done on the router at this time is a simple egress filter prohibiting address spoofing.

The software in use on this system to provide network services are the latest available versions from the vendor, and are know to handle exceptions properly. As mentioned above, Qmail handles permissions and exceptions very well, and to this date there have been no known published vulnerabilities. The system logs show the system handling malformed packets and messages in an acceptable manner.

There have been several vulnerabilities with earlier versions of Open SSH, but this risk is mitigated by the access list on the router. The only system permitted to communicate with the server using this protocol is the administration console, which is also always kept up to date from the vendor, and resides behind a firewall at the business office.

All exception handling for the POP and IMAP services is being done by the Washington University IMAP daemon provided from by Red Hat with the distribution. There have been many published vulnerabilities with theses services over the years, but the latest version is always in use on this system. While this is not a perfect scenario, it is all that is available at this time.

There are no other listening ports on the system, and all other input controls for necessary services are being performed by the systems providing the services.

Evaluate the Risk to the System

The success of the ISP's business depends on providing high quality, high availability services. With many businesses and individuals relying on email communications to make their living, it is imperative that the POP/IMAP server be available at all times. There are several factors that could cause this system to

become unavailable, resulting in potential loss of revenue and damage to the business. The following are the four main categories of risk that this system is exposed to at all times; physical threats, software vulnerabilities, network access, and administrator misconfiguration and/or error. While this is not meant to be an exhaustive description of vulnerabilities and threats to the system, it will provide the framework for the focus of the audit.

Physical Threats

What could go wrong: If someone malicious were able to gain physical access to the machine they could cause a great deal of damage, or even worse, complete loss of the system. With powerful computing resources becoming smaller every year, it has become a lot more feasible for someone to enter a data center and remove hardware without a great deal of physical exertion. It is also possible to do a great deal of physical and logical damage to a system if console level access is obtained. Fire and water damage would also be catastrophic to the proper operation of this system.

How likely is it: The POP/IMAP server is housed in the ISP's main data center. Physical access to the facility is controlled with keypads on all external doors and there are no windows at this location. During business hours, company personnel are responsible for ensuring that no unauthorized physical access to any systems is permitted. After hours, the door keypads and a monitored alarm system are in place to prevent access to the facility. The building is equipped with both a computer safe fire suppression system, and a water notification system to prevent damage from these sources. Overall, physical security of the system is not too bad. However, it is not outside the realm of possibility that physical access could be obtained.

What are the consequences: If physical access to the system was obtained, and damage to the system occurred it could be catastrophic to the business. Down time and customer data loss could both have long term financial and business reputation consequences to the ISP.

Software Vulnerabilities

What could go wrong: The server is running several software packages that could expose it to attack. The Washington University IMAP daemon in use currently has no published vulnerabilities, but there have been many over the years. Because it is in widespread use on the Internet, it has long been an attractive target for attackers. Due to the nature of the service this system provides, this software is accessible from the entire Internet. Open SSH is also in use on this system, and there have been many attacks directed at it as well. The current version has no known issues, but new problems are developing all the time. The risk to this particular service is reduced by the access list on the

router restricting traffic to only a known “trusted” system. The Linux distribution is provided by Red Hat, Inc., and is kept up to date using the RHN [2] service provided by the vendor. Proper operation of this system is also dependent on several other services provided by other systems under the ISP’s control. If vulnerabilities in any of the software in use were exploited, system uptime, performance, and data integrity could all be at risk.

How likely is it: Because new vulnerabilities are discovered in software on a very regular basis, the risk to this system from software vulnerability should be considered very high. It is quite common for vendors to require several days after a particular vulnerability is discovered to patch, test, and distribute a new version of their software. With the exposure of this system to the entire Internet, it is quite likely that someone could take advantage of this window of opportunity and gain access to this system.

What are the consequences: Because this is a mission critical system to the ISP, any unauthorized access, use, or otherwise could be potentially devastating to the business.

Network Access

What could go wrong: While access to certain services is tightly restricted by the router access list, there is also access to this system available from anywhere on the Internet. This exposes the system to a great deal of potential risk. Many of the other services necessary for proper operation (DNS, NTP, SMTP) are also exposed to the Internet, thereby increasing the level of risk exposure. It would be quite simple for an attacker to launch a Denial of Service attack against this system, or any of it’s supporting systems, rendering it essentially useless. Because of the widespread access to services on these systems, and the lack of any Intrusion Detection at all, it would also be fairly easy for someone to compromise these systems and go unnoticed.

How likely is it: With the dramatic rise of security incidents over the past few years, it is very likely that someone will, or already has, compromise any or all of the systems on this subnet due to the high level of Internet exposure they have.

What are the consequences: A Denial of Service attack or unauthorized access and damage to any of the systems on the subnet would result in a potentially high level of damage to the ISP’s business.

Administrator Misconfiguration and/or Error

What could go wrong: With all access controls to the system being done with a Cisco ACL, if an error was made in the list, the system would be exposed to greater risk. It is also possible that because all of the systems on the ISP’s network are under the control of a single individual, that an alert about a

vulnerability could be overlooked, exposing the system to increased risk.

How likely is it: As we all know, system administrators are typically under a great deal of pressure, and overworked. It is highly possible that a mistake could be made exposing the system to greater threat.

What are the consequences: Any unknown exposure to threat and/or attack could result in loss of service to the ISP's customers, and thus result in loss or damage of business to the company.

As an Internet Service Provider, many of the systems in use are there to provide service to their customer base. This exposes the business to a great deal of risk that many private companies are not exposed to. It is not feasible for the ISP to restrict access to services to company employees on trusted networks, because those services are for hire.

The POP/IMAP server has been chosen for this audit for a particular reason. Many of the services the ISP provides are redundant in nature. For example, there are multiple DNS servers available for use by the customer base. The web servers are designed so that any one could provide service to all hosting customers if the need arose. The outbound SMTP server could provide filtering services if need be, and vice versa. The POP/IMAP system is the only mission critical service that cannot be replaced without a great deal of down time and lost data.

What is the Current State of Practice?

While doing research on different auditing methods and procedures, I quickly found that there is very little in the way of documented auditing of the Qmail MTA. Therefore, all of the checks and test that will be performed that deal specifically with securing Qmail will be based on my own experience with the software. I have been running Qmail on my own systems for almost five years now and have become very comfortable with setting up a secure email platform using Qmail.

Unlike the shortage of information available on Qmail audits, I was able to find a great deal of documentation on Linux audits. Over the past several years, Linux has become a very popular Internet operating system, and therefore a great deal of time and effort has been spent coming up with security best practices. A good place to start when looking for information on Linux security is the Linux Security website, available at http://www.linuxsecurity.com. There are links to many documents, articles, how to guides, and books dealing with Linux security; from basic introductions to advanced level technical documents on setting up secure application jails.

There have also been tools developed by several groups to help automate the

process of auditing and securing your Linux operating system. The most prevalent return from a Google [3] search on Linux security auditing tools is the Linux Security Auditing Tool (LSAT). LSAT is a post install tools designed to look for configuration and setting problems on a Linux system and recommend changes. The LSAT project homepage can be found at http://usat.sourceforge.net, and is available as a free download for many Linux distributions, as well as for Solaris.

Another good resource for Audit related reading and how to information is available at http://www.linux-sec.net/Audit/. With many links to other resources I find this site to be quite useful when researching security issue for Linux in general.

The SANS Institute also has published a great deal of information on the topic of Linux Auditing. I found a great deal of useful information that I translated into parts of my checklist in the following few documents.

How-To Make Linux System Auditing a Little Easier, Paul J. Santos, URL: http://www.sans.org/rr/papers/index.php?id=81

Linux Security Auditing, Paul Whelan, URL: http://rr.sans.org/audit/linux_sec.php

Auditing Linux, Krishni Naidu, URL: http://www.sans.org/score/checklists/AuditingLinux.doc

Because the ISP does not have a published security policy dealing with the server being audited, I did not spend a great deal of time researching auditing security policies. I will put an item in the checklist about policy, but already know the result and plan on addressing it in my audit report in section four of this document.

Assignment 2 – Create an Audit Checklist

The following checklist tries to deal with key issues specific to the server being audited. Many common security best practice issues have not been included because they are not relevant to the particular configuration of the email server.

For example:
We will not be looking at password security because all of the end users are paying customers and do not have shell access to the system. The only shell access is for administration, and is controlled with the use of RSA keys.

Item 1 – Physical Security

Reference	Own contribution
Control Objective	Determine whether or not the physical security of the system is up to best standards.
Risk	Ensure that physical damage and/or access to the system is difficult or impossible. If the system were physically damaged down time would occur resulting in loss to the business. If physical access is obtainable, down time or data loss could occur resulting in loss to the business.
Compliance	Can access to the building be obtained during business hours and/or after hours without proper permission? Is the server console accessible without logging in? Is it possible to remove the system from the facility without being noticed? Does the alarm company provide sufficient controls/checks when verifying the identity of a caller when the alarm is set off?
Testing	1. Attempt to brute force the door key pad system 2. Set off the alarm and contact the alarm company. Do they require sufficient proof of identity to ensure proper system security? 3. Ctrl+Alt+Del at the system console and try to enter different run levels without authentication. 4. Visually inspect the facility to determine if the system could be removed unnoticed. 5. Is the console logged out when a visit happened unannounced?
Objective/Subjective	This item falls into both categories. Some of the checks, like brute forcing the key pads and trying to obtain access without authentication are objective, while deciding whether or not sufficient care is taken by the alarm company and determining whether or not I could leave the building with the system easily are subjective in nature.

Item 2 – Ensure that all patches have been applied

Reference	SANS Press, Securing Linux Guide, Chapter 1, page 3
Control Objective	Ensure that all OS and software patches have been applied.
Risk	Software vulnerabilities account for a large number of successful system compromises on the Internet today. If all patches are not applied the system will be exposed to unnecessary risks.
Compliance	If the system is up to date, the Red Hat Network will indicate it as such. If it is not there will be notices of which errata apply.
Testing	1. up2date –register 2. Register the system to an account managed by the auditor by following the on screen instructions. 3. Log in to RHN and ensure that all patches have been applied, or run update –u and ensure that it reports that all packages are currently up to date 4. Visit the Qmail website to ensure that newer releases are not available. (http://www.qmail.org)
Objective/Subjective	Objective

Item 3 –Ensure that SSH is in use

Reference	Auditing Linux, Krishni Naidu
Control Objective	Ensure that the only shell level access to the box is secured with SSH and that SSH has been properly configured to not allow any access that is not controlled with secure keys
Risk	If unencrypted access is permitted, or SSH is not configured properly it would be possible for an attacker to obtain shell access on the server.
Compliance	If the system is running SSH and it is properly configured, the system will be deemed compliant. Because there are several ways in which SSH can be

	misconfigured, it is possible that SSH could be in use and the system would still not be compliant. For the purpose of this audit compliance will be satisfied if SSH is in use, and does not allow login without an RSA key.
Testing	1. Attempt to telnet to the system and see if access can be obtained 2. ps –aux |grep sshd 3. ls –la /etc/init.d/sshd 4. ls –la /etc/rc.d/rc3.d/ and look for a symbolic link to the /etc/init.d/sshd file 5. Move /home/sysadmin/.ssh directory on administration machine to a backup location and attempt to ssh to the server and get a password prompt 6. cd /etc/ssh a. grep protocol sshd_config b. grep syslog sshd_config c. grep PermitRoot sshd_config d. grep PasswordAuth sshd_config
Objective/Subjective	Objective

Item 4 –Ensure remote syslog is in use and working properly

Reference	Many Linux Best Practices sources as well as own knowledge
Control Objective	Ensure that all critical syslog information is being sent to a remote syslog server
Risk	If the system were compromised, history has shown that many attackers will attempt to cover their tracks by removing the logs from the system. If remote syslog is in use there will still be logs of the attack even if the local logs are removed.
Compliance	If syslog is configured to use a remote syslog server than compliance will be obtained.
Testing	1. View /etc/syslog.conf and ensure that there are entries for all critical logs

	that look like @remotesyslogserver note: this is to include all “kern” level logging. 2. verify the presence of log entries from this system on the remote syslog server a. grep giant /var/log/messages b. grep giant /var/log/secure
Objective/Subjective	Objective

Item 5 –Ensure xinetd is only running necessary services

Reference	Own contribution
Control Objective	Ensure that only POP and IMAP are being run via xinetd
Risk	If an unnecessary service is running via xinetd, access could be obtained due to an vulnerability in an unknown service
Compliance	There should not be any extra files in the /etc/xinetd.d directory besides what are needed for POP and IMAP
Testing	1. ls –la /etc/xinetd.d 2. ensure that only ipop3 and imap are returned
Objective/Subjective	Objective

Item 6 –Ensure SMTP service only receives traffic from filtering server

Reference	Own contribution. I obtained this information from my interview of the system administrator. During the interview I was told this system does not accept SMTP traffic from any system other than the filtering gateway.
Control Objective	Confirm that SMTP traffic is restricted to the filtering gateway system only
Risk	If this is not configured properly, the system would be able to receive mail that has not been properly scanned for viruses and SPAM. This could expose the end users to unexpected risk. It is also possible that the system could be used as a relay server for spammers to

	send messages out to the Internet.
Compliance	The tcpserver database file should contain only the IP address of the filtering gateway and a deny statement. Connecting to port 25 should return no positive response.
Testing	1. View the tcpserver template file /etc/rules.txt and ensure that only filterserver:allow and :deny are present 2. ls –la /etc/tcp.smtp.cdb and note file size 3. tcprules tcp.smtp.cdb temp<rules.txt 4. ls –la /etc/tcp.smtp.cdb and compare file size to previous file size 5. attempt to telnet to port 25 on the system to see whether or not a response is given
Objective/Subjective	Objective

Item 7 –Verify that all end user accounts have /bin/false shell

Reference	Interview with system administrator
Control Objective	Confirm that no end user accounts have shell access to the server
Risk	Because the end users are paying customers, there is no enforceable password policy for their accounts. Without strong passwords, it would be trivial to obtain shell access to the system and then launch a privilege elevation attack.
Compliance	All end user accounts will have /bin/false as their shell
Testing	1. grep the /etc/passwd file for all other shell type installed on the system and ensure that none of the accounts returned belong to end users 2. investigate the “user_add” PERL script that is used for adding and removing accounts from the system and ensure that it sets the user shell to /bin/false whenever an account is added

Objective/Subjective	Objective

Item 8 –Verify that shadow passwords are in use for all accounts

Reference	Auditing Linux, Krishni Naidu
Control Objective	Ensure that shadow passwords are in use on the system for all accounts
Risk	Unix systems that store the password in the /etc/passwd system are no longer considered secure. This file is readable by all users on the system to allow for login. If someone were to gain "user level" access to the system, they would have all accounts and their associated password. Even if they were encrypted, they could copy the file to a remote system and crack them at their leisure. The use of shadow passwords moves the encrypted passwords to a separate file that is only readable by the "root" user, making it much less trivial to obtain access to the system.
Compliance	All user accounts will have their passwords stored in the /etc/shadow file.
Testing	1. verify that the password field in the /etc/passwd file contains an "x" for all accounts 2. verify that all user accounts have an encrypted password in the /etc/shadow file by viewing the contents of the file.
Objective/Subjective	Objective

Item 9 –Verify that only "root" has console login permissions

Reference	Auditing Linux, Krishni Naidu
Control Objective	Make sure that only the root account has the ability to login to the system at the console.
Risk	The end user accounts may have weak passwords due to the nature of the system, therefore obtaining console access with one of these accounts could potentially be trivial.
Compliance	Console access will be restricted in

	/etc/security/access.conf
Testing	1. Review /etc/security/access.conf and verify that console access has been restricted to only the root account 2. If access controls are in place, verify by attempting to login as the sysadmin user at the console
Objective/Subjective	Objective

Item 10 –Verify that the host based IDS Portsentry is in use

Reference	Own contribution obtained from interview with the system administrator indicating use of Portsentry host based IDS
Control Objective	Ensure that all connection attempts to dangerous ports not in use on the system are monitored and logged
Risk	All attempts to connect to a system could potentially indicate that access had been obtained. Without a way to monitor for connections and notify the administrator when they take place, access to the system could go unnoticed.
Compliance	Portsentry will be installed and configured to monitor all non-production ports, and will log this information the the syslog facility locally and remotely. These logs will be reviewed on a regular basis by the system administrator.
Testing	1. Verify the presence of Portsentry in /usr/local/psionic/portsentry 2. Verfiy there are startup scripts to run Portsentry on system startup in "/etc/init.d" and "/etc/rc.d/rc3/d" 3. execute 'ps –aux |grep portsentry' and make sure two running processes are returned 4. Ensure the package is configured to listen in "really anal" mode by reviewing the /usr/local/psionic/portsentry/portsentry.conf file 5. Ensure the IDS is logging to the local syslog facility by connecting to a monitored port and reviewing the

	/var/log/messages file locally and on the remote syslog server
Objective/Subjective	Objective

Item 11 –Verify that original sendmail package has been removed

Reference	Own contribution based on years of running Qmail as an MTA, and the best practices involved with it.
Control Objective	Verify that sendmail has been removed from the system to ensure that the extra security of running Qmail is not compromised
Risk	Leaving the original sendmail daemon installed exposes the system to all risks associated with using sendmail, thus partially defeating the purpose of choosing a more secure MTA.
Compliance	Sendmail will no longer be installed
Testing	1. rpm –q sendmail should return package not installed message 2. find / -name sendmail and record all returned locations of sendmail 3. ls –la /all_locations/sendmail besides /var/qmail/bin/sendmail and verify they are all symbolic links back to /var/qmail/bin/sendmail
Objective/Subjective	Objective

Item 12 –Verify that change documentation is maintained for the server

Reference	Own contribution based on best practice knowledge of system change controls
Control Objective	Verify that change log is kept and all changes and updates to the server are recorded
Risk	If a log of all updates and changes is not kept it is difficult to roll back a change or update that causes problems. It is also impossible to verify who made a configuration change and why it was done if all changes are not fully documented
Comliance	Logs will exist and be kept up to date
Testing	1. Obtain change log from system

	administrator and review from start date to current date 2. Compare all configuration options in logs with what is actually configured and running on the server. 3. Ensure update syslog messages correspond to the server change log
Objective/Subjective	Subjective. It is going to be impossible to ensure that every update and change has been documented, but if the records are detailed and all configurations seem to be in order it is safe to assume that server changes are documented well.

Item 13 –Test network level controls from outside the server segment

Reference	Own contribution from interview with system administrator about network level filtering done at the gateway router.
Control Objective	Verify that network access to the server matches the access controls reported to be in place.
Risk	If access to the server from outside it's network is not tightly controlled, services accidentally running will be exposed to potential attack from the Internet.
Compliance	Port scans of the server IP address should return only permitted responses
Testing	1. Obtain copy of running config from gateway router and ensure that an access list is configured and applied to the inbound interface of the router 2. nmap –p 1-65535 192.168.2.35 3. Verify that only port 110 (POP) is listed by nmap as listening and responding.
Objective/Subjective	Objective

Item 14 –Verify all listening services on the system

Reference	Own contribution from knowledge of best practices for running an Internet

	connected system
Control Objective	Ensure that system is only listening on ports that are in use by production services.
Risk	If the system is listening on a port that is not used by a production service that has been properly configured the system is at risk for remote exploit
Compliance	Only ports in use by production services should reply to the stimuli
Testing	1. netstat –al and ensure that no ports are returned for non production services 2. nmap –p 1-65535 192.168.2.35 from another machine on the server segment and verify that only ports 110 (POP), 25 (SMTP), 143 (IMAP), and 22 (SSH) are reported as responding.
Objective/Subjective	Objective

Item 15 –Verify system backups are performed regularly and valid

Reference	Own contribution based on interview with VP of Information Systems indicating that backups are supposed to be performed
Control Objective	Verify backups are being done and perform a test restore to ensure information is current.
Risk	If backups are not taken of critical system configuration files, restoration of the system would result in longer than necessary down time.
Compliance	System logs will show regular backups jobs being run and tapes or backup disks will contain up to date information.
Testing	1. Verify that local and remote /var/log/messages files contain records indicating start and finish of backup jobs. 2. Review list of files to be backed up and ensure that all critical configuration files are included. 3. Restore several randomly

	selected backed up files and compare them to the ones in production to ensure that they are identical. 4. crontab –l to verify backup schedule is consistent with expectations of leadership
Objective/Subjective	Objective

Item 16 –Ensure logs are monitored and notification procedure is in place

Reference	Auditing Linux, Krishni Naidu
Control Objective	Is there a log monitoring facility in place on the system and is it configured to notify the system administrator
Risk	If the system logs are not monitored errors, configuration changes/problems, and illegal access attempts/successes will go unnoticed.
Compliance	A syslog monitoring program will be installed and in use and cnooifgured to notify the administrator of any problems as they arise.
Testing	If Swatch is in use, verify the swatchrc file is configured to monitor all system logs and that the expressions in use are sufficient If Logcheck is in use verify that the expressions in logcheck.ignore are feasible for this system Ensure that whatever software is in use is listed when a ps –aux is executed or is in the root users crontab If service is run as daemon and not with crontab, ensure proper startup scripts are present in the rc.d directories and /etc/init.d/
Objective/Subjective	Both. The software will either be present and in use or not, but the expressions in the config files being appropriate or not is generally up to the person doing the review. Some people are comfortable with what is expected of their system more than others and

	therefore may ignore a few more notifications that someone who is not so sure of him/herself.

Item 17 –Verify that regular vulnerability scans are performed

Reference	Own contribution based on security best practices
Control Objective	Ensure that periodic testing is done to ensure that no chages have been made or taken place that negatively affect the security of the system.
Risk	If periodic vulnerability tests don't get performed a service update or change could expose the system to risk and go unnoticed
Compliance	Logs of vulnerability test dates and the associated results should be present in the system documentation
Testing	Obtain documentation on periodic scans from system administrator and review.
Objective/Subjective	Subjective.

Item 18 –Are the Qmail packages installed the latest available versions

Reference	Own contribution from years of experience running and maintaining Qmail
Control Objective	Ensure that packages that are not being kept up to date from the Linux vendor are being updated and have no known/published vulnerabilities
Risk	Because most of the software in use on this system is kept updated using the Red Hat Network system, it is important to ensure that all software not provided by Red Hat has been kept up to date. Often times individual packages that are ot maintained by a vendor do not have the notification systems in place that someone like Red Hat does. These packages are critical to the security stance of the machine as they are all publicly facing.
Compliance	All Qmail related software installed will be the latest version available on the www.qmail.org website

Testing	1. Obtain version of qmial package running 2. Obtain version of ucspi package running 3. Verify they are the latest available from the Qmail website.
Objective/Subjective	Objective

Item 19 –Does the server comply with written security policies for the system?

Reference	Own contribution based on experience
Control Objecive	To determine whether or not the server complies with all written policies regarding configuration and security.
Risk	If there are not strict guidelines in place to define proper security measures and configuration options, the security of the system is not being properly managed.
Compliance	All aspects of the servers configuration should comply exactly with the written policy specific to this system
Testing	Go through all policies regarding this particular system and ensure that each and every guideline specified in the documents is in place and properly setup
Objective/Subjective	Objective. Either the server will adhere to the guidelines set forth in the policies or it will not.

Item 20 –Is NTP in use for time synchronization

Reference	Own contribution
Control Objective	Determine if time synchronization is being run and is working properly
Risk	While not having accurate time on the system will not affect the proper operation of the system, it will make determining exactly when events take place more difficult. When trying to investigate potential incidents it is important to be able to accurately establish a time frame for the event.
Compliance	NTP should be installed, configured to run automatically, and properly

	synchronized with the remote time server.
Testing	1. rpm- q ntpd 2. review /etc/ntp.conf is setup to use the correct time server 3. ntpstat 4. /usr/sbin/ntptrace 5. date
Objective/Subjective	Objective

Assignment 3 –Audit Evidence

Conduct the Audit

The actual audit of the email system was conducted with the assistance of the system administrator. All tests requiring login to the machine were executed in front of the auditor by the system administrator. Because the system needs to be available 24/7, all tests conducted were "safe" in nature. Any vulnerability testing that could potentially disturb the operation of the system was left out of the tests to ensure proper operation during the entire audit process. All commands executed on the system were done so with "root" privileges unless otherwise noted in the results below.

Checklist item 3 – Ensure that SSH is in use

Control Objective
Ensure that the only shell level access to the box is secured with SSH and that SSH has been properly configured to not allow any access that is not controlled with secure keys

Testing

1. Attempt to telnet to the system and see if access can be obtained
2. ps –aux |grep sshd
3. ls –la /etc/init.d/sshd
4. ls –la /etc/rc.d/rc3.d/ and look for a symbolic link to the /etc/init.d/sshd file
5. Move /home/sysadmin/.ssh directory on administration machine to a backup location and attempt to ssh to the server and get a password prompt
6. cd /etc/ssh
    a. grep protocol sshd_config
    b. grep syslog sshd_config
    c. grep PermitRoot sshd_config
    d. grep PasswordAuth sshd_config

Actual Results

1.
audit:~ mmaxwell$ telnet 192.168.2.35
Trying 192.168.2.35...
telnet: connect to address 192.168.2.35: Connection refused
telnet: Unable to connect to remote host
audit:~ mmaxwell$

2.
[root@giant sysadmin]# ps aux | grep sshd
root 21282 0.0 0.0 3560 428 ? S 2003 0:00 /usr/sbin/sshd
root 7969 0.0 0.0 6764 1748 ? S 09:40 0:00 sshd: sysadmin [priv]
sysadmin 7973 0.0 0.0 6776 1996 ? S 09:40 0:00 sshd: sysadmin@pts/1
root 22974 0.0 0.0 3684 648 pts/1 S 09:54 0:00 grep sshd

3.
[root@giant sysadmin]# ls -la /etc/init.d/sshd
-rwxr-xr-x 1 root root 2647 Sep 17 12:13 /etc/init.d/sshd
[root@giant sysadmin]#

4.
[root@giant sysadmin]# ls -la /etc/rc.d/rc3.d/
lrwxrwxrwx 1 root root 14 Oct 22 09:38 S55sshd -> ../init.d/sshd

5.
audit:~ mmaxwell$ ssh -l sysadmin 192.168.2.35
Permission denied (publickey,keyboard-interactive).
audit:~ mmaxwell$

6.
[root@giant /]# cd /etc/ssh/
[root@giant ssh]# grep Protocol sshd_config
Protocol 2
[root@giant ssh]# grep Syslog sshd_config
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
[root@giant ssh]# grep PermitRoot sshd_config
PermitRootLogin no
[root@giant ssh]# grep PasswordAuth sshd_config
PasswordAuthentication no

[root@giant ssh]#

Score

Pass
All tests results support the proper configuration and operation of the SSH daemon.

Checklist Item 4 -- Ensure remote syslog is in use and working properly

Control Objective
Ensure that all critical syslog information is being sent to a remote syslog server

Testing

1. View /etc/syslog.conf and ensure that there are entries for all critical logs that look like

@remotesyslogserver

note: this is to include all “kern” level logging.

2. Verify the presence of log entries from this system on the remote syslog server.

grep giant /var/log/secure
grep giant /var/log/messages

Actual Results

[root@giant etc]# cat 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;mail.none;authpriv.none;cron.none @syslog.isp.net

The authpriv file has restricted access.
authpriv.* /var/log/secure
authpriv.* @syslog.isp.net

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
[root@giant etc]#


[root@syslog log]# grep giant secure
Feb 23 04:02:00 giant xinetd[13704]: START: pop3 pid=7556
from=192.168.76.232
Feb 23 04:02:00 giant xinetd[13704]: EXIT: pop3 pid=7556 duration=0(sec)
Feb 23 04:02:00 giant xinetd[13704]: START: pop3 pid=7557
from=192.168.80.101
Feb 23 04:02:01 giant xinetd[13704]: EXIT: pop3 pid=7557 duration=1(sec)
Feb 23 04:02:01 giant xinetd[13704]: START: pop3 pid=7576
from=192.168.74.95
Feb 23 04:02:01 giant xinetd[13704]: EXIT: pop3 pid=7576 duration=0(sec)
Feb 23 04:02:01 giant xinetd[13704]: START: pop3 pid=7587 from=69.54.2.205
Feb 23 04:02:01 giant xinetd[13704]: START: pop3 pid=7588
from=192.168.76.199
Feb 23 04:02:01 giant xinetd[13704]: EXIT: pop3 pid=7587 duration=0(sec)
Feb 23 04:02:02 giant xinetd[13704]: EXIT: pop3 pid=7573 duration=1(sec)
Feb 23 04:02:02 giant xinetd[13704]: EXIT: pop3 pid=7588 duration=1(sec)
Feb 23 04:02:02 giant xinetd[13704]: START: pop3 pid=7624
from=192.168.76.57
Feb 23 04:02:03 giant xinetd[13704]: EXIT: pop3 pid=7624 duration=1(sec)
Feb 23 04:02:03 giant xinetd[13704]: START: pop3 pid=7630
from=192.168.75.65
Feb 23 04:02:03 giant xinetd[13704]: START: pop3 pid=7635
from=192.168.65.74
Feb 23 04:02:03 giant xinetd[13704]: EXIT: pop3 pid=7630 duration=0(sec)
Feb 23 04:02:03 giant xinetd[13704]: START: pop3 pid=7636
from=192.168.75.65
Feb 23 04:02:03 giant xinetd[13704]: EXIT: pop3 pid=7636 duration=0(sec)
Feb 23 04:02:04 giant xinetd[13704]: EXIT: pop3 pid=7635 duration=1(sec)
Feb 23 04:02:04 giant xinetd[13704]: START: pop3 pid=7674
from=192.168.76.13
```

```
Feb 23 04:02:04 giant xinetd[13704]: EXIT: pop3 pid=7674 duration=0(sec)
Feb 23 04:02:04 giant xinetd[13704]: START: pop3 pid=7695
from=192.168.76.142
Feb 23 04:02:04 giant xinetd[13704]: START: pop3 pid=7696
from=192.168.73.213
Feb 23 04:02:05 giant xinetd[13704]: EXIT: pop3 pid=7695 duration=0(sec)
Feb 23 04:02:05 giant xinetd[13704]: START: pop3 pid=7697
from=192.168.76.142
Feb 23 04:02:05 giant xinetd[13704]: EXIT: pop3 pid=7697 duration=0(sec)
Feb 23 04:02:05 giant xinetd[13704]: START: pop3 pid=7698
from=192.168.79.98
Feb 23 04:02:05 giant xinetd[13704]: START: pop3 pid=7699
from=192.168.73.182
Feb 23 04:02:06 giant xinetd[13704]: START: pop3 pid=7700 from=192.168.79.9
Feb 23 04:02:06 giant xinetd[13704]: EXIT: pop3 pid=7699 duration=0(sec)
Feb 23 04:02:06 giant xinetd[13704]: EXIT: pop3 pid=7698 duration=1(sec)
Feb 23 04:02:06 giant xinetd[13704]: EXIT: pop3 pid=7700 duration=1(sec)
Feb 23 04:02:06 giant xinetd[13704]: START: pop3 pid=7705
from=192.168.79.98
Feb 23 04:02:06 giant xinetd[13704]: START: pop3 pid=7706
from=192.168.76.134
Feb 23 04:02:07 giant xinetd[13704]: EXIT: pop3 pid=7705 duration=1(sec)
Feb 23 04:02:07 giant xinetd[13704]: START: pop3 pid=7715
from=192.168.70.109
Feb 23 04:02:07 giant xinetd[13704]: EXIT: pop3 pid=7715 duration=0(sec)
Feb 23 04:02:08 giant xinetd[13704]: START: pop3 pid=7716 from=69.54.2.135
Feb 23 04:02:08 giant xinetd[13704]: EXIT: pop3 pid=7706 duration=2(sec)
Feb 23 04:02:08 giant xinetd[13704]: START: pop3 pid=7717
from=192.168.76.61
```

Cut for space

[root@syslog log]# grep giant messages

Because a great deal of the information retured by this search was sensitive customer information, the actual results have not been included here. It is evident however that there was a great deal of syslog information on the reomte syslog server for this system.

Score

Fail
While remote syslog is setup for some syslog facilities, kernel level messages are not being logged remotely (or locally). Because of this, the requirement for this objective is not being met at this time.

Checklist Item 5 –Ensure xinted is only running necessary services

Control Objective
Ensure that only POP and IMAP are being run via xinetd

Testing

1. ls –la /etc/xinetd.d
2. ensure that only ipop3 and imap are returned

Actual Results

1.
```
[root@giant xinetd.d]# ls -la
drwxr-xr-x    2 root     root        4096 Feb 23 11:06 .
drwxr-xr-x   48 root     root        4096 Feb 23 10:40 ..
-rw-r--r--    1 root     root         387 Nov 26 11:36 imap
-rw-r--r--    1 root     root         376 Nov 26 11:37 ipop3
-rw-r--r--    1 root     root         430 Oct 24 12:32 rsh
[root@giant xinetd.d]#
```

Score

Fail
The results show that in addition to IMAP and POP, RSH is being run by xinetd. The is an insecure service that is not being run for any particluar reason at this time. The system adminstrator informed me they used to manage parts of the system with this service and must have forgotten to disable it when they changed their management strategies.

Checklist Item 6 –ensure SMTP service only receives traffic from filtering server

Control Objective
Confirm that SMTP traffic is restricted to the filtering gateway system only

Testing

1. View the tcpserver template filre /etc/rules.txt and ensure that on filterserver:allow and :deny are present
2. ls –la /etc/tcp.smtp.cdb and note file size
3. tcprules tcp.smtp.cdb temp<rules.txt
4. ls –la /etc/tcp.smtp.cdb and compare file size to previous result. The file sizes should be identical.
5. attempt to telnet to port 25 (SMTP) on the system to see whether or not a response is given.

Actual Results

1.
[root@giant xinetd.d]# cd /etc/
[root@giant etc]# cat rules.txt
192.168.1.30:allow
:deny

2.
[root@giant etc]# ls -la tcp.smtp.cdb
-rw-r--r-- 1 root root 2214 Jan 20 10:08 tcp.smtp.cdb

3.
[root@giant etc]# tcprules tcp.smtp.cdb temp<rules.txt

4.
[root@giant etc]# ls -la tcp.smtp.cdb
-rw-r--r-- 1 root root 2214 Feb 23 12:01 tcp.smtp.cdb

5.
audit:~ mmaxwell$ telnet 192.168.2.35 25
Trying 192.168.2.35...
Connected to giant.isp.net.
Escape character is '^]'.
Connection closed by foreign host.

Score

Pass
All controls are in place to restrict SMTP traffic, and attempting to connect to port 25 results in failure.

Checklist Item 9 –Verify that only "root" has console login permissions

Control Objective
Make sure that only the "root" account has the ability to loginto the system at the console.

Testing

1. Review /etc/security/access.conf and verify that console access has been restricted to only the root account.
2. If access controls are in place, verify by attempting to login with the sysadmin account at the console.

Actual Results

1.

```
[root@giant security]# cat access.conf
# Login access control table.
#
# When someone logs in, the table is scanned for the first entry that
# matches the (user, host) combination, or, in case of non-networked
# logins, the first entry that matches the (user, tty) combination.  The
# permissions field of that table entry determines whether the login will
# be accepted or refused.
#
# Format of the login access control table is three fields separated by a
# ":" character:
#
#       permission : users : origins
#
# The first field should be a "+" (access granted) or "-" (access denied)
# character.
#
# The second field should be a list of one or more login names, group
# names, or ALL (always matches). A pattern of the form user@host is
# matched when the login name matches the "user" part, and when the
# "host" part matches the local machine name.
#
# The third field should be a list of one or more tty names (for
# non-networked logins), host names, domain names (begin with "."), host
# addresses, internet network numbers (end with "."), ALL (always
# matches) or LOCAL (matches any string that does not contain a "."
# character).
#
# If you run NIS you can use @netgroupname in host or user patterns; this
# even works for @usergroup@@hostgroup patterns. Weird.
#
# The EXCEPT operator makes it possible to write very compact rules.
#
# The group file is searched only when a name does not match that of the
# logged-in user. Both the user's primary group is matched, as well as
# groups in which users are explicitly listed.
#
##############################################################################
###############
#
# Disallow console logins to all but a few accounts.
#
```

```
#-:ALL EXCEPT wheel shutdown sync:LOCAL
#
# Disallow non-local logins to privileged accounts (group wheel).
#
#-:wheel:ALL EXCEPT LOCAL .win.tue.nl
#
# Some accounts are not allowed to login from anywhere:
#
#-:wsbscaro wsbsecr wsbspac wsbsym wscosor wstaiwde:ALL
#
# All other accounts are allowed to login from anywhere.
#
```

Score

Fail
No access controls are in place for console logins. There is no reason to complete test 2 due to this fact.

Checklist Item 10 –Verify that the host based IDS Portsentry is in use

Contol Objective
Ensure that all connection attempts to dangerous ports not in use on the system are monitored and logged.

Testing

1. Verify the presence of Portsentry in /usr/local/psionic/portsentry
2. Verfiy there are startup scripts to run Portsentry on system startup in "/etc/init.d" and "/etc/rc.d/rc3/d"
3. execute 'ps –aux |grep portsentry' and make sure two running processes are returned
4. Ensure the package is configured to listen in "really anal" mode by reviewing the /usr/local/psionic/portsentry/portsentry.conf file
5. Ensure the IDS is logging to the local syslog facility by connecting to a monitored port and reviewing the /var/log/messages file locally and on the remote syslog server

Actual Results

1.
```
[root@giant security]# ls -la /usr/local/psionic/portsentry/
total 256
drwx------    2 root     root        4096 Oct 24 13:24 .
drwx------    3 root     root        4096 Oct 24 04:44 ..
-rwx------    1 root     root       35914 Oct 24 04:44 portsentry
```

```
-rw-r--r--    1 root     root        91282 Feb 23 12:51 portsentry.blocked.stcp
-rw-r--r--    1 root     root          660 Jan 19 18:43 portsentry.blocked.sudp
-rw-------    1 root     root        11196 Oct 24 04:44 portsentry.conf
-rw-------    1 root     root        93166 Feb 23 12:51 portsentry.history
-rw-------    1 root     root          480 Oct 24 04:44 portsentry.ignore
```

2.

```
[root@giant security]# cat /etc/init.d/portsentry
#! /bin/sh

/usr/local/psionic/portsentry/portsentry -stcp
/usr/local/psionic/portsentry/portsentry –sudp
```

```
[root@giant security]# ls -la /etc/rc.d/rc3.d/
lrwxrwxrwx    1 root     root           22 Oct 24 12:45 S98portsentry ->
/etc/init.d/portsentry
```

3.

```
[root@giant security]# ps -aux |grep portsentry
root      2107  0.0  0.0  1672  548 ?        S     2003 154:17
/usr/local/psionic/portsentry/portsentry -stcp
root      2109  0.0  0.0  1672  496 ?        S     2003  32:05
/usr/local/psionic/portsentry/portsentry -sudp
root     21318  0.0  0.0  3684  656 pts/1    S    12:56   0:00 grep portsentry
```

4.

relevant part of file

```
[root@giant security]# more /usr/local/psionic/portsentry/portsentry.conf
# PortSentry Configuration
#
# $Id: portsentry.conf,v 1.23 2001/06/26 15:20:56 crowland Exp crowland $
#
# IMPORTANT NOTE: You CAN NOT put spaces between your port arguments.
#
# The default ports will catch a large number of common probes
#
# All entries must be in quotes.


#########################
# Port Configurations #
#########################
#
#
# Some example port configs for classic and basic Stealth modes
#
```

```
# I like to always keep some ports at the "low" end of the spectrum.
# This will detect a sequential port sweep really quickly and usually
# these ports are not in use (i.e. tcpmux port 1)
#
# ** X-Windows Users **: If you are running X on your box, you need to be sure
# you are not binding PortSentry to port 6000 (or port 2000 for OpenWindows
users).
# Doing so will prevent the X-client from starting properly.
#
# These port bindings are *ignored* for Advanced Stealth Scan Detection Mode.
#

# Un-comment these if you are really anal:
TCP_PORTS="1,7,9,11,15,21,23,70,79,80,109,111,119,138,139,512,513,514,51
5,540,635,1080,1524,2000,2001,4000,4001,5742,6000,6001,6667,12345,12346,
20034,27665,30303,32771,32772,32773,32774,31337,40421,40425,4972
4,54320"
UDP_PORTS="1,7,9,53,66,67,68,69,111,137,138,161,162,474,513,517,518,635,
640,641,666,700,2049,31335,27444,34555,32770,32771,32772,32773,32774,31
337,54321"
```

5.
local syslog facility
Feb 23 12:31:09 giant portsentry[2107]: attackalert: TCP SYN/Normal scan from host: audit.isp.net to TCP port: 32773
Feb 23 12:31:09 giant portsentry[2107]: attackalert: Host: audit.isp.net is already blocked Ignoring

Remote syslog server
Feb 23 12:31:09 giant portsentry[2107]: attackalert: TCP SYN/Normal scan from host: audit.isp.net to TCP port: 32773
Feb 23 12:31:09 giant portsentry[2107]: attackalert: Host: audit.isp.net is already blocked Ignoring

Score

Pass
Portsentry is installed, configured, and in use on the system and connecting to a monitored port immediately is recorded in both the local and remote syslog facilities.

Checklist Item 11 –Verify that original sendmail package has been removed

Control Objective
Verify that sendmail has been removed from the system to ensure that the extra security of running Qmail is not compromised.

Testing

1. 'rpm –q sendmail' should return package not installed message
2. 'find / -name sendmail' and record all returned locations of sendmail
3. 'ls –la /all_locations/sendmail' besides '/var/qmail/bin/sendmail' and verify they are all symbolic links back to '/var/qmail/bin/sendmail'

Actual Results

1.
[root@giant security]# rpm -q sendmail
package sendmail is not installed

2.
[root@giant security]# find / -name sendmail
/var/qmail/bin/sendmail
/usr/sbin/sendmail
/usr/lib/sendmail

3.
[root@giant security]# ls -la /usr/sbin/sendmail
lrwxrwxrwx 1 root root Oct 22 10:15 sendmail -> /var/qmail/bin/sendmail

[root@giant security]# ls -la /usr/lib/sendmail
lrwxrwxrwx 1 root root Oct 22 10:15 sendmail -> /var/qmail/bin/sendmail

Score

Pass
All tests show that the original sendmail package has been removed and the proper symbolic links to the Qmail sendmail binary have been setup.

Checklist Item 13 –Test network level controls from outside the server segment

Control Objective
Verify that network access to the server matches the access controls reported to be in place.

Testing

1. Obtain a copy of running config from gateway router and ensure that an access list is configured and applied to the inbound interface of the router
2. 'nmap –p 1.65535 192.168.2.35'
3. Verify that only port 110 (POP) is listed by nmap as listening and

responding.

Actual Results

1.
```
access-list 150 deny   ip 10.0.0.0 0.255.255.255 any
access-list 150 deny   ip 127.0.0.0 0.255.255.255 any
access-list 150 deny   ip 169.254.0.0 0.0.255.255 any
access-list 150 deny   ip 172.16.0.0 0.15.255.255 any
access-list 150 deny   ip 192.0.2.0 0.0.0.255 any
access-list 150 deny   ip 192.168.0.0 0.0.255.255 any
access-list 150 deny   ip 224.0.0.0 15.255.255.255 any
access-list 150 deny   ip 240.0.0.0 7.255.255.255 any
access-list 150 deny   ip 248.0.0.0 7.255.255.255 any
access-list 150 deny   ip 192.168.2.0 0.0.0.255 any log
access-list 150 permit tcp any host 192.168.2.35 eq 110
access-list 150 permit tcp host 192.168.1.30 host 192.168.2.35 eq 25
access-list 150 permit tcp host 10.0.1.32 host 192.168.2.35 eq 22
access-list 150 deny ip any any log

interface FastEthernet 0/0
ip address 192.168.1.126
ip access-group 150 in
```
2.
```
[root@scanner admin]# nmap -p 1-65535 192.168.2.35

Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on giant.greenmountainaccess.net (65.19.68.35):
(The 65534 ports scanned but not shown below are in state: closed)
Port       State       Service
110/tcp    open        pop-3

Nmap run completed -- 1 IP address (1 host up) scanned in 7 seconds
```

Score

Pass
The only listening port reported by the NMAP portscan was 110(POP)

Checklist Item 14 –Verify all listening services on the system

Control Objective
Ensure that the system is only listening on ports that are in use by production services.

Testing

1. 'netstat –al' and ensure that no ports are returned for non production services
2. 'nmap –p 1-65535 192.168.2.35' from another machine on the server segment and verify that only ports 110 (POP), 25 (SMTP), 143 (IMAP), and 22 (SSH) are reported as responding.

Actual Results

1.
[root@giant security]# netstat -al
Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	*:shell	*:*	LISTEN
tcp	0	0	*:pop3	*:*	LISTEN
tcp	0	0	*:imap	*:*	LISTEN
tcp	0	0	*:ssh	*:*	LISTEN
tcp	0	0	*:smtp	*:*	LISTEN

2.
[root@friend sysadmin]# nmap -p 1-65535 65.19.68.35

Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/)
Interesting ports on giant.greenmountainaccess.net (65.19.68.35):
(The 65530 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh
25/tcp	open	smtp
110/tcp	open	pop-3
143/tcp	open	imap2
514/tcp	open	shell

Nmap run completed -- 1 IP address (1 host up) scanned in 7 seconds

Score

Fail
Port 514 (shell), which is associate with the rsh service is listening on the server and is not used as part of any production service.

Checklist Item 19 –Does the server comply with written security policies for the system?

Control Objective
To determine whether or not the server complies with all written policies

regarding configuration and security.

Testing

Go through all policies regarding this particular system and ensure that each and every guideline specified in the documents is in place and properly setup.

Actual Results

No security policies or written configuration guidelines exist for this system.

Score

Fail
See actual results above.

Measure Residual Risk

Summary of Audit Results

The following is a summary list of the results presented in the previous section, as well as any possible mitigation, controls, and an overall residual risk score for each item.

Check
Ensure that SSH is in use

Result
Pass

Controls/Mitigation
SSH is in use and properly configured for all remote access to the system.

Residual Risk
None

Check
Ensure remote syslog is in use and working properly

Result
Fail

Controls/Mitigation
Kernel level logging must be configured to log to the remote syslog server. Currently no kernel level logging is being done. To setup kernel logging:

*kern @syslog.isp.net

Residual Risk
Medium

Check
Ensure xinetd is only running necessary services

Result
Fail

Controls/Mitigation
The RSH service was found to be running on the system, and in talking with the system administrator it was discovered that certain management tasks were done using this method in the past. Not only was the service running, but was setup and configured for root access to be permitted from the main control server used by the ISP to manage its accounts on the system. The simplest way to deal with this is to simply remove the rsh file from /etc/xinetd.d and restart the daemon, which would completely remove the risk.

Residual Risk
Low

Check
Ensure SMTP service only receives traffic from fitlering server

Result
Pass

Controls/Mitigation
No control/mitigation is needed

Residual Risk
None

Check
Verify that only root has console login permissions

Result
Fail

Controls/Mitigation
To remove this risk from the system the /etc/security/access.conf file need to be edited to disallow console access for all accounts on the system other than root.

Residual Risk
Low

Check
Verify that the host based IDS Portsentry is in use

Result
Pass

Controls/Mitigation
The “really anal” setting in Portsentry is being used to monitor unused ports on the system. To be completely aware of all connection attempts to the system you would want to include every port from 1-65535 that is not in use by a production service. Monitoring this many ports may be a drain on system resources however and is probably going a little over board.

Residual Risk
Very Low

Check
Verify that original sendmail package has been removed

Result
Pass

Controls/Mitigation
None

Residual Risk
None

Check
Test network level controls from outside the server segment
Result
Pass

Controls/Mitigation
All steps possible are being taken to keep the risk of providing POP services to an absolute minimum. The only way to remove this risk completely would be to not allow POP from the Internet, which would essentially defeat the primary purpose of the system.

Residual Risk
Low

Check
Verify all listening services on the system

Result
Fail

Controls/Mitigation
This failure is directly related to the rsh process being run by xinetd. If that process file is removed from the directory and the daemon is restarted the risk will be completely mitigated for the purposes of this audit.

Rediual Risk
Low

Check
Does the server comply with written security policies for the system?

Result
Fail

Controls/Mitigation
The ISP currently does not have any written security policies for the system. Because of this, the audit had to measured against only best practices. It would take considerable time and effort to create these documents, but to ensure the ongoing security of this system it is absolutely necessary. This audit should have provided a framework to build these policies and there are many resources available on the Internet to help this process along. Without policies in place the future security of this sytem will be incredibly difficult to maintain. Since this server is essential to the successful operation of the organization, it is imperative that this process be started immediately.

Residual Risk
High

Evaluate the Audit

The lack of any written policies concerning the server's security configuration took the audit in a unique direction. Typically an audit is performed to ensure a system is following the guidelines defined in the corporate security policies. In this case, the audit served as an instrument to help develop a security strategy for the system going forward. Because there are a great deal of resources dealing with best practices and Linux auditing available on the Internet, the customer and I feel that the audit has been an overall success.

Until this audit was performed, the ISP relied on the system administrator's own knowledge and skills to secure the system. While this has worked until now, they

realise that a formal strategy needs to be put in place going forward. With the results from this audit, and audits of all other systems on their network that were performed during the same time period, they are feeling better prepared to address the task of writing detailed security policies regarding all their Internet connected systems.

Assignment 4 –Audit Report

Executive Summary

Overall, the audit of the POP/IMAP email server was a success. All of the objectives set forth at the start of the project have been met. Because the primary goal of the audit was to establish a baseline framework for developing a security policy for the system, most of the checks were based on Linux best practice recommendations. The checklist created for the audit, located in section 2 of this document, will make an excellent guideline for developing a comprehensive security policy for this system. There were some unexpected issues discovered during the course of the audit that should be addressed prior to the completion of security policy, but the costs associated are fairly minimul.

Audit Findings

The following is a description of the problems discovered during the audit and recommendations for resovling them, including the associated costs.

Checklist Item 4 (page 27)

Logging all system log information, including kernel messages, is recommended best practice for all systems, and is an excellent example of defense in depth. It has been discovered that often times attackers will erase the log entires generated by their activities to cover their tracks upon successful compromise of a system. By logging to both the local system and a secure remote syslog server, you make it much more difficult, or even near impossible, to completely cover the tracks of an attack.

The email server is logging some of its information to the remote syslog server, but the kernel messages are not being sent to the server. I would recommend configuring the syslog daemon to log all kermel messages to the local system and secure syslog server to remediate this issue. The associated costs to resolve the issue are almost non-existent. It will take the system administrator only a few minutes to configure and restart the daemon, and there should be no additional remote storage needed on the syslog server.

Checklist Item 5 (page 30)

During our tests to ensure that no unecessary software is running on the system,

the RSH service was found to be running. RSH is a service that allows access to the server based on an established trust relationship. Because this service was originally used by the system administrator for system management, the trust relationship established was done using the “root” account on the system. What this means is that the central server responsible for updating user accounts and settings on the email system has a trust relationship established with the email server as the “root” user. Any remote command issued from the account management server will be executed by the email server as the “root” user. This means that if the management server was to be become compromised, the attacker would by default have complete control of the email server as well. As with the previous item, the recommended course of action is to remove this service from the system immediately. As with the syslog changes, the costs associated with removing this service and completely removing the risk are less than one hour of the system administrators time.

Checklist Item 9 (page 31)

Console access to any system should be restricted to only the “root” user account. Console access provides “normal” users access to hardware resources that are not to be taken lightly. While a company may have a content filtering system in place to scan all traffic to a from a system that travels over the network, if a user has console access, sensitive information can easily be removed from the system with the use of the floppy drive or any other physically connected writeable media. With the Linux operating system, it is fairly simple to restrict console access to only the “root” user. All the system administrator needs to do is edit the /etc/security/access.conf file and place the following line at the end:

-:ALL EXCEPT root:LOCAL

Once again, the cost to remove this risk from the system is simply a very small amount of the system administrator’s time, and should not be cause for any financial concern to the business.

Checklist Item 14 (page 37)

This item is essentially identical to Item 9 listed above. The steps to remove this risk entirely from the system can be reviewed above.

The most time consuming recommendation, writing security policies, was actually the primary goal of the audit. I will not go into great detail in this section on why it is necessary to have good security policies, because the business has already spent time and money performing this audit to help them accomplish that, and is well aware of the reasons good policies are necessary. I can speak from experience though, that coming up with comprehensive security policies that can be agreed on by all decision makers in a business can be a difficult and time

consuming process. It is my hope that this audit has provided a great deal of useful information about the system and its' current state of security, that your job in creating a security policy has been made easier. I would also recommend looking at the Security Policy Template project that is sponsored by the SANS Institute. There a policy examples available that can be modified to suit just about any business' specific needs. It is difficult to estimate the cost of completing the security policies for this system, because they tend to be an ongoing an evolving process. As the needs of the business and the role of the system change, the policy will need to be modified or updated to take into consideration any changes to accommodate these business needs.

References

1. "The Qmail Security Guarantee", D.J. Bernstein, URL:
http://cr.yp.to/qmail/guarantee.html

2. Red Hat Network, Red Hat, Inc., URL:
http://rhn.redhat.com

3. Google, URL:
http://www.google.com

4. How-To Make Linux System Auditing a Little Easier, Paul J. Santos, URL:
http://www.sans.org/rr/papers/index.php?id=81

5. Linux Security Auditing, Paul Whelan, URL:
http://rr.sans.org/audit/linux_sec.php

6. Auditing Linux, Krishni Naidu, URL:
http://www.sans.org/score/checklists/AuditingLinux.doc

7. LinuxSecurity.com, Excellent source of many Linux related security topics,URL:
http://www.linuxsecurity.com

8. Linux Security Auditing Tool, Post install audit tool for Linux, URL:
http://usat.sourceforge.net

9. Linux-sec.net, Great source of how to information and security patches and software, URL:
http://www.linux-sec.net

10. SANS Reading Room, Valuable source of security publications, URL:
http://www.sans.org/rr/

11. The SANS Security Policy Project, The SANS Institute, URL:
http://www.sans.org/resources/policies/