A Security Audit of the Corporate Email Gateway

The Ciphertrust Appliance: Ironmail V. 4.0

A Security Analyst's Perspective

Option 1
GSNA Practical Version 3.0

Author: Kris A. Kendrick
Date: July 27th, 2004

Table of Contents

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

Section 2 – Create an Audit Checklist

Section 3 – Audit Fieldwork

Section 4 – Executive Summary

Abstract

According to a recent report published by the FBI, 95% of all attacks go un-detected. This is a staggering percentage especially since a majority of the attacks are generated and sent out across the Internet via e-mail, some requiring user interaction and some not. Electronic mail, or E-mail, has become a critical tool in virtually every business process today. As a network security analyst for a financial institution, part of my daily routine includes the administration of the corporate email gateway and ensuring the company is protected from external threats transmitted through email. A key external threat is commonly known as a virus. A virus is defined as a piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event. (TechTarget 2004) A computer savvy community of computer professionals usually creates these malicious viruses, known as "*black hat hackers*". A black hat hacker is an individual who hacks with malicious intent to gain intimate knowledge of a computer or network. Many black hat hackers use email as a means for distributing malicious content that could compromise an entire network. One way to combat their efforts is to establish a "Defense in Depth" security posture. When referring to "Defense In Depth", securing an email gateway is one of the first lines of defense in achieving layered protection.

This is a technical report of the audit of a corporate email gateway appliance, called Ciphertrust. The Ciphertrust appliance is generally housed in a corporate DMZ, or Demilitarized Zone, network environment. An audit was conducted to determine the technical security of the configuration and to assess the reliability of the service the appliance is planned to provide. The content of this audit is divided into four areas: identify and describe the system to be audited, perform a risk evaluation to the system in its current state of practice, create an audit checklist of subjective and objective tests, and provide a high level management report of the audit results referencing any findings with supported evidence.

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

1.1 Introduction

The technical focus of this security audit is a corporate e-mail gateway appliance, called Ciphertrust. A financial institution, as part of a project to enhance their network security infrastructure, recently purchased the appliance. The appliance' primary function is to provide the company, its assets and its employees a safe environment to send and receive business related emails. This audit is designed to identify internal and external risks associated with the email gateway system, determine vulnerabilities related to those risks, examine how those vulnerabilities can be exploited and provide recommendations to mitigate those risks to ensure a safe and controlled email environment.

1.2 The Environment

1.2.1 Audit Focus

Figure 1 illustrates the network infrastructure in which the Ciphertrust appliance operates. The appliance functions behind two routers and one firewall in a corporate DMZ, or Demilitarized Zone. This appliance is accessed from the Internet and there are known vulnerabilities associated with ports used by the appliance.

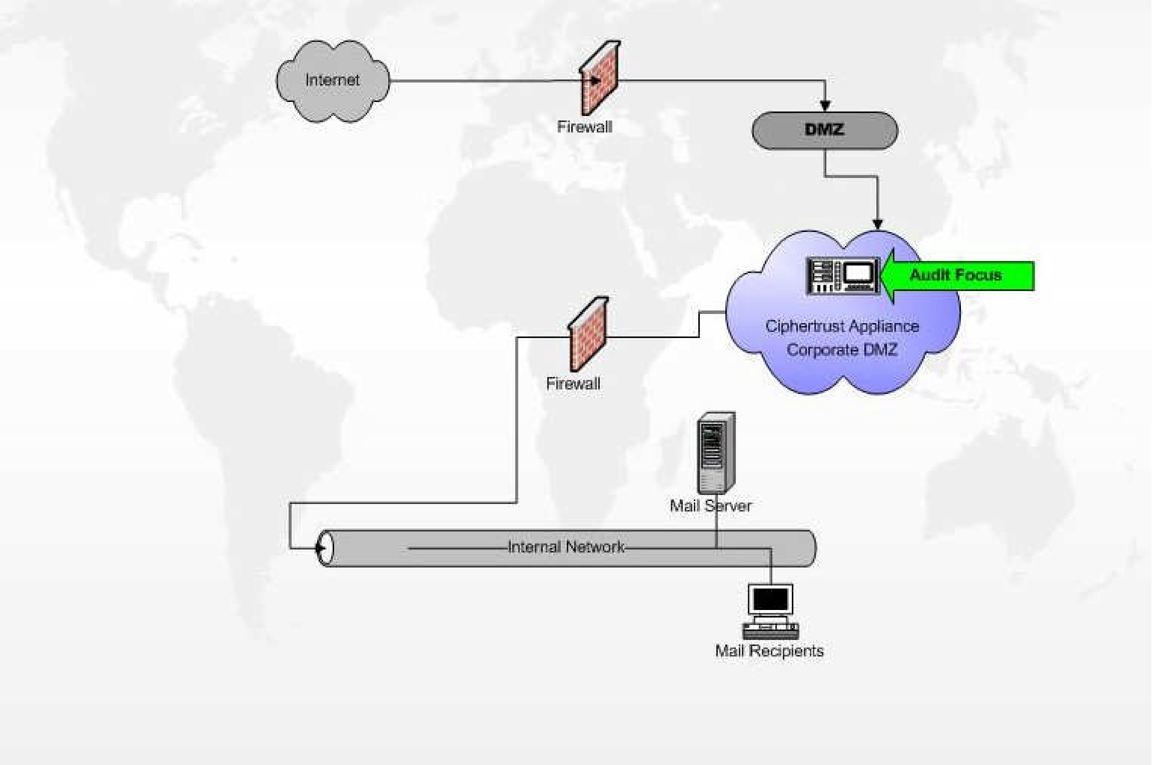


Figure 1 – The network environment in which the Ciphertrust appliance operates.

1.2.2 The Ciphertrust Appliance

Hardware

Make	IBM
Model	345
Processor	2 – 2.4Ghz Intel XEON Processors
Memory	1GB Memory / 3 – 36 GB 10K SCSI Hard Drives

Software

Operating System	Custom build of the UNIX FreeBSD operating system
Application	Ironmail v 4.0

Ironmail, the Ciphertrust appliance's application, was installed on top of a custom version of the FreeBSD UNIX operating system, or OS. The OS used on the appliance is a modified version of the FreeBSD kernel. (FreeBSD, Free Berkeley Software Distribution), as defined at www.newtolinux.org/glossary, is similar the GNU/Linux in that in includes many GNU programs and runs many of the same packages as GNU/Linux. However, some kernel functions are implemented differently as it uses a BSD kernel, and the file system architecture is different.[1] The Ironmail OS is pre-hardened and pre-loaded with encryption software designed specifically for the Ciphertrust appliance. The encryption is used for communication with support and for downloading application and virus updates. In addition, services deemed un-necessary have been removed from the OS to close several ports. Although this appliance was built with a strong security focus, this audit will carry out its objectives and scan for any of the known vulnerabilities that may be associated with the system.

1.2.3 Network Communication

Connections from mail servers and the Internet are necessary for successful mail delivery. The following tables define ports that need to be opened to establish communication links to and from the appliance.

Network Connections (Internal and External)

Ironmail to Internet

Port	TCP/UDP	Protocol	Description
25	TCP	SMTP	Required for mail delivery
53	TCP/UDP	DNS	Optional for an Ironmail/CMC (if your DNS is outside the network, you must open the port allowing Ironmail/CMC to connect to it)
123	**TCP**	**NTP**	**Required if using network time protocol**
6277	**UDP**	**SLS[2]**	**Required if you wish to enable Statistical Lookup Service (SLS) lookup as part of your anti-spam strategy.**
20022	**TCP**	**Ciphertrust**	**Required in order for Ironmail to request software/anti-virus updates**

Figure 2. Ports needed for basic functionality are highlighted in red.

[1] www.newtolinux.org/glossary

[2] According to Ciphertrust, the SLS service is a trusted ring of partners who participate in a collaborative effort to identify spam. (Ciphertrust Manual Release 4)

In the current network environment, ports 123, 6277 and 20022 are the only ports needed to establish communication from the appliance to the Internet. These ports are used for updating purposes.

Internet to Ironmail

Port	TCP/UDP	Protocol	Description
20	TCP	FTP	Optional if using FTP (used to FTP reports and log files to an internal server)
22	TCP	SCP	Optional if using SCP
25	**TCP**	**SMTP**	**Required for Mail Delivery**
80	TCP	HTTP	Optional for Webmail (secure HTTPS on port 443 is preferred)
110	TCP	POP3	Optional (secure POP3S on port 995 is preferred)
143	TCP	IMAP4	Optional (secure IMAPS on port 993 is preferred)
443	TCP	HTTPS	Optional for Webmail (for secure HTTPS proxying)
465	TCP	SMTPS	Optional for secure incoming messages
993	TCP	IMAP4S	Optional (this is the preferred port to securely retrieve email via IMAP4)
995	TCP	POP3S	Optional (you should open port 995 for secure POP3S instead)
20022	**TCP**	**Ciphertrust**	**Required (allows Ciphertrust to connect to your Ironmail for Technical Support)**

Figure 3. *Illustrates the ports required to establish connections from the Internet to the Ironmail. (The ports required for basic functionality are highlighted in red.)*

Ironmail to Internet Mail Server

Port	TCP/UDP	Protocol	Description
21	TCP	FTP	Optional if using FTP
22	TCP	SCP	Optional is using SCP
25	**TCP**	**SMTP**	**Required for mail delivery**
53	UDP	DNS	Optional for an Ironmaiil/CMC (if your DNS is inside the network, you must open the port allowing Ironmail/CMC to connect to it
80	TCP	HTTP	Optional for Webmail (you should open secure port 443 for HTTPS instead)
110	TCP	POP3	Optional (you should open port 995 for secure POP3 instead)
143	TCP	IMAP4	Optional (you should open secure port 993 for IMAP4S instead)
162	TCP	SNMP	Optional if using SNMP Trap Manager
389	TCP	LDAP	Optional if using LDAP
514	UDP		Optional if using Syslog server
443	TCP	HTTPS	Optional for Webmail (for secure HTTPS proxying)
993	TCP	IMAP4S	Optional (this is the preferred port to securely retrieve mail via IMAP4S)
995	TCP	POP3S	Optional (this is the preferred port to securely retrieve mail via POP3S)

Figure 4 - Illustrates the ports required to establish connections from Ironmail to the Internet mail server. (The ports required for basic functionality are highlighted in red.)

Most mail servers use only ports 25, 110, and 143 to send and receive email. Emails transmitted through these ports are unencrypted and attackers are able to retrieve them and ultimately read and obtain information. From a security perspective, it is recommended that the secure ports be opened instead: 995 for POP3S and 993 for IMAP4S.

Internet Mail Server to Ironmail

Port	TCP/UDP	Protocol	Description
22	TCP	CL Interface	Optional (only if you want to access the command line interface from inside the network)
25	**TCP**	**SMTP**	**Required for mail delivery**

Figure 5 - Illustrates the ports required to establish connections from the Internet mail server to Ironmail. (The ports required for basic functionality are highlighted in red.)

The Ironmail 4.0 Application

Protection is divided into 4 main areas, or modules, as they are referred to in the Ciphertrust manual for email systems, anti-spam, anti-virus, secure web mail, and secure delivery. The modules have integrated tools that are used to scan messages to determine if they should be quarantined or delivered. Spammers are notorious for counter striking virtually every method of fighting the spam battle. Spam is an on-going battle. Spammer will always find way to bypass the "latest and greatest" spam fighting tools.

Anti-Virus (Queue)

The best way to stop viruses is at the gateway of a network. With Ironmail, two industry leading anti-virus engines are available to use, Sophos and McAfee. Ironmail is currently configured to automatically check for software updates and virus definition updates every two hours.

Attachment Filtering (Queue)

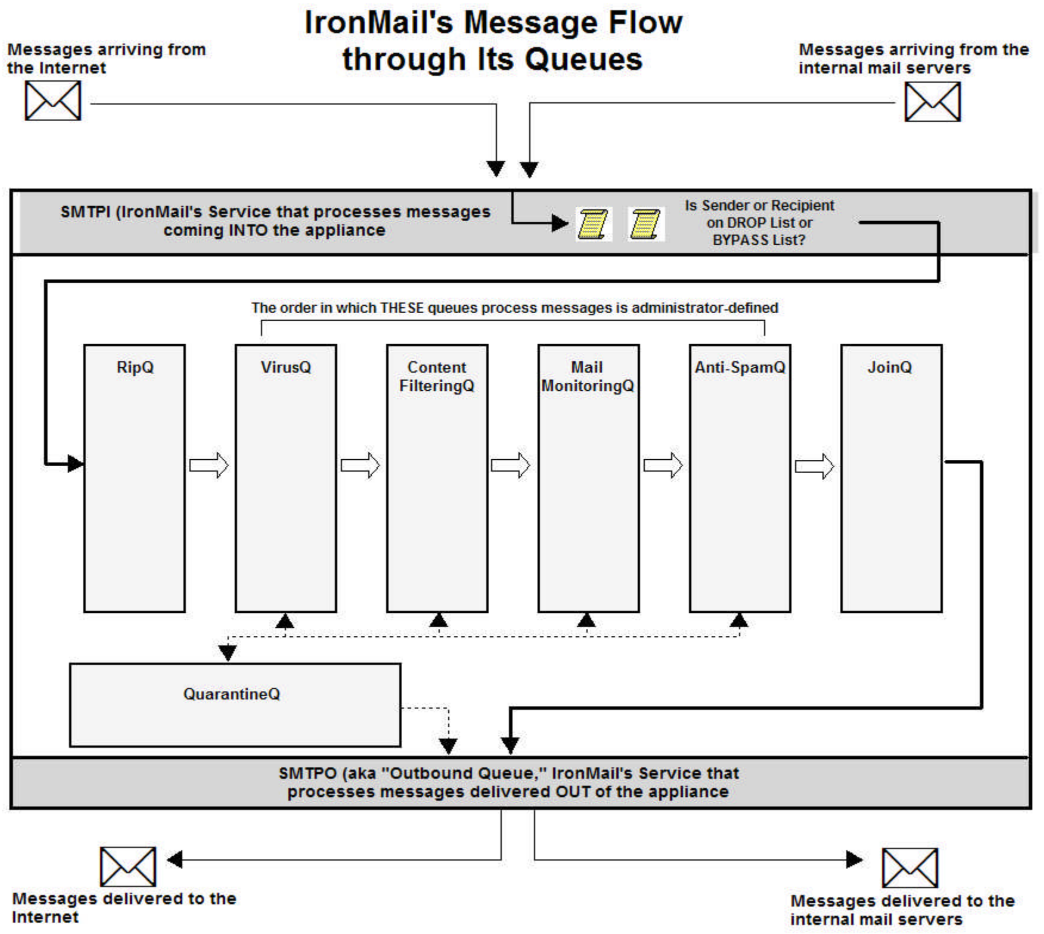
Administrators are allowed to determine what file attachments to block. A strong configuration would be to block all inbound executable. Usually, executable files should not be sent into a network unless they're zipped and the system is able to scan inside the zip files for virus payloads.

Content Filtering (Queue)

Many spammers use a combination of keywords in an effort to bypass content filtering areas. Using foul language in email is against corporate policy, Ironmail has the capability to scan for keywords and phrases and quarantine filthy email if necessary. The content filtering policy was imported from a previous message filtering software the company was using. When an email arrives, Ironmail counts the number of times the words in the dictionary are in the email. Ironmail then gives that message a total numeric value. The total number is then compared to the threshold value pre-defined by the system administrator and an action is taken to quarantine, delete or deliver that particular email. The same process is used to determine if an email is spam, or not.

Anti-Spam (Queue)

Anyone with an email address has at one time or another experienced the annoying advertising emails also known as spam. Though once simply an annoying point, click and delete process, these spam messages are now considered to be a very serious security concern for companies all over the world.


IronMail's Message Flow through Its Queues
Messages arriving from the Internet
Messages arriving from the internal mail servers
SMTPI (IronMail's Service that processes messages coming INTO the appliance
Is Sender or Recipient on DROP List or BYPASS List?
The order in which THESE queues process messages is administrator-defined
RipQ
VirusQ
Content FilteringQ
Mail MonitoringQ
Anti-SpamQ
JoinQ
QuarantineQ
SMTPO (aka "Outbound Queue," IronMail's Service that processes messages delivered OUT of the appliance
Messages delivered to the Internet
Messages delivered to the internal mail servers

The figure above illustrates how the email messages move through the appliance. First, the email is received from the Internet or from internal mail servers. The appliance is not designed to designate external mail (I.E. Internet mail) from internal mail (I.E. Internal mail servers). All mail coming into the appliance is considered “inbound” email. The RipQ is designed to “rip” the email into several parts. The parsed data is then scanned by 4 queues the VirusQ, the ContentFilteringQ, the MailMonitoringQ and the Anti-SpamQ. As the emails move through the queue process, they are weighed by threshold values configured by the mail administrators. These values trigger events that move a message to quarantine, deletion or delivery. The values are subject to change as updates become available.

1.3 Risk Assessment

Risk is a function of the *likelihood* of a given *threat-source's* exercising a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the organization.[3] The following three tables will address, define and determine the potential impact risks have on an organization and its daily business operations.

Threat Analysis

A technological threat is defined as a circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, data modification, and/or Denial of Service (DoS) (Symantec Security Response 2004). Because this system was designed as a network security appliance, threats and impact on business operations are minimal. This table will identify two threats that are associated with any network resource, regardless of its initial design.

Proposed Threat Identification	Impact on Business Operations
Access to the system determined to be un-authorized	An internal or external attacker connects to the appliance without authorization • An attacker could intentionally release viruses into the internal network. • A Trojan could be placed on the appliance to sniff traffic from a remote location. • Financial institutions are a known target for attackers. Information such as account numbers, balances, Social Security Numbers and other sensitive information play an integral role in the day-to-day business activity.
Viruses passing through the appliance to the internal network	The spread of viruses are increasing at an astounding pace. • With the introduction of more sophisticated viruses such as MyDoom, Novrag and variants of Netsky, updating virus engines and definitions should be paramount for all businesses.

[3] NIST (National Institute of Standards and Technology) "Risk Management Guide for Information Technology Systems". Technology Administration – U.S Department of Commerce.

Information Asset – Corporate Email

Corporate email is arguably the fastest growing business tool in recent years (Nexor 2002). Email is an integral part of the communicate link between internal employees, external vendors and potential clients. In the event of a system failure, email would be halted and without a proven backup or disaster recovery plan, a significant loss of production would be the inevitable. System failures can often be avoided by implementing proper controls. The controls are designed to establish a set of standards that will help maintain the most efficient system operability.

Vulnerability Analysis

The following table illustrates vulnerabilities related to the email gateway system configuration, the exposure rating for defined vulnerabilities, and the operational impact that vulnerability would have if exploited successfully by an attacker. The exposure rating is determined by personal experience through administration of the appliance. For example, remote administration is defined through a predefined port on the appliance and only the vendor can authenticate to it. Connections attempted from any other IP address would be immediately rejected. Therefore, the exposure rating for a vulnerability to be exploited successfully through remote administration would be very low (5% to 10%).

Vulnerability	Exposure Rating	Operational Impact
Denial of Service Attack	10%	• The financial institution currently has 2 firewalls in front of the appliance. • Production loss • System unavailable to monitor inbound and outbound email
Unauthorized Remote Administration	10%	• User with malicious intent gaining privileged access to system
System requires re-authentication after session expires	60%	• If the administrator were to leave the workstation and a session is still active, any passerby could have administrative access to the network resource. • The user could unknowingly release infected emails to the internal network.
Virus Protection	65%	• If the IDE files are not updated promptly, viruses could potentially be delivered.

Current State of Practice

The financial institution has recently approved a project to begin implementation of security audit procedures, establish baseline security practices and perform vulnerability assessments on all network security appliances. No documentation will be included to support its current state of practice, as it is an unfinished project.

1.4 Technical Security Tools

In this section, the tools used to perform the technical aspects of the audit will be defined. The tools will assist in determining vulnerabilities in the system configuration and provide evidence to support control objectives and findings reported to senior management. The following is a list of security tools that will be used:

- **SuperScan 4.0** – this is a connect-based TCP port scanner, pinger and host name resolver. In the following audit, this tool will be used to perform banner grabbing on the target system. A copy of Superscan can be downloaded for free at www.foundstone.com

- **EyeE Digital's Retina Security Scanner** - retina is a non-intrusive security scanner that scans network devices for vulnerabilities identified by the application. It also provides the capability to manage security policies from a central location. The latest release of Retina can be downloaded at www.eeye.com/html

- **Nessus** – a tool used to scan networks from a remote location. The Nessus Security scanner was initially built for the MacOS X, FreeBSD, Linux, and Solaris operating systems. The Nessus 2.0 UNIX based tool can be downloaded at http://www.nessus.org/download.html. This release is the most recent stable version of the software. A release of the Windows version of Nessus is now available and can be downloaded at http://www.tenablesecurity.com/newt.html

Section 2 – Audit Checklist

The checklist below was created to assess and determine any potential risks associated with the current configuration of the Ciphertrust appliance. The checklist consists of 12 items including referenced information, the control objective, associated risk, compliance, objective/subjective, the success or failure of the test, audit fieldwork and post test results/audit findings. The checklist criteria are defined as follows:

- **Reference** – Source information for checklist item.
- **Control Objective** – Identifies the audit step.

- **Risk** – States the risk this control objective is related to and determines the potential for an attack.
- **Compliance** – Stated to ensure the control objective satisfies corporate policy or adheres to security best practice.
- **Testing** – Illustrates the security tools, log output, and screen shots necessary to evaluate system operability.
- **Objective/Subjective** – Defined as 1) Objective tests are verifiable, output used to form an objective result. 2) Subjective is based on a conscious evaluation, logic used to determine a result.

Audit Step 1 – Administrator Password Strength

Reference: Novoblisky, Kimberly M. "Audit of an SSL VPN; Secure Remote Email Solution for a Financial Institution"
http://www.giac.org/practical/GSNA/Kimberly_Novoblisky_GSNA.pdf

Control Objective: Verify the administrator password is strong.

Risk: Weak, easy to guess passwords make it significantly easier for an attacker to crack a system administrator's password. If the crack is successful, the attacker could take complete control of the system.

Compliance: Ensure administrator passwords comply with the financial institutions corporate password policy. The policy states administrator passwords must be at least a combination of 8 alphanumeric characters in length.

Testing:

1. Initiate a browsing session to the Ciphertrust appliance.
2. Attempt a series of common Administrator usernames and passwords to login to the appliance.
3. Document any successful tests.
4. In the event a login errors out, determine what error message is displayed. *Security Analyst's Important Note: Ensure the error message does not display unnecessary information such as "Valid Username/Invalid Password. This tells the attacker that the Username was defined in the system. The error message should read, "Username/Password is invalid", which does not volunteer any information.*
5. Document evidence.

Objective/Subjective: Objective
This test is necessary to determine the strength of the system administrator password. In order to effectively complete fieldwork on this audit step, a copy of the corporate password policy would need to be obtained as evidence of security policy compliance. No copy will be included for reasons pertaining to confidentiality and best security practice.

Success/Failure: To be completed during audit fieldwork.

Audit Fieldwork: To be completed during audit fieldwork.

Post Test Results/Audit Findings: To be completed during audit fieldwork.

Audit Step 2 – System Required Re-Authentication After Session Time Out

Reference: Novoblisky, Kimberly M. “Audit of an SSL VPN; Secure remote email solution for a financial institution” http://www.giac.org/practical/GSNA/Kimberly_Novoblisky_GSNA.pdf

Control Objective: Verify system administration is not attainable after 30 minutes of idle time.

Risk: Individual gains un-authorized access with full system privileges by using an authorized session started by an administrator. All users that have accounts on the system are system administrators by default. The accounts have full system privileges to make firewall, local system IDS and service changes. In addition, a user could release malicious viruses into the internal network.

Compliance: The session automatically logs the user out of the system after 30 minutes of inactivity.

Testing:

1. Start a Ciphertrust session using the web browser interface.
2. Login to the system.
3. Allow 30 minutes of idle time. According to the system configuration, the sessions will time out after 30 minutes of idle time. The session minute count can be changed at system administrator’s discretion.
4. Return to the session after 31 minutes. Ensure account login credentials must be re-entered to gain privileged access to the system.
5. Document evidence of test procedures.

Objective/Subjective: Objective
This is an objective test to ensure an un-authorized user is not able to take over the appliance without having an authorized account defined in the system. To give an example, a Ciphertrust system administrator could leave work at 5 p.m. without having logged out of the session. The night janitor with minimal technical “know-how” could take control of the Ciphertrust box without having an authorized login. The system was built for easy navigation and the web interface is very user friendly. The janitor could then simply select the “Quarantine” tab, select “Viruses-Quarantined” and release every virus on the system into the internal network.

Success/Failure: To be completed during audit fieldwork.

Audit Fieldwork: To be completed during audit fieldwork.

Post Test Results/Audit Findings: To be completed during audit fieldwork.

Audit Step 3 – Layered Protection

Reference: The financial institution’s “Defense in Depth” security model. Executive management approved the model and implementation began in September 2002.

Control Objective: Ensure virus-infected emails with an attachment (i.e. .exe, .bat) are quarantined after passing through the anti-virus queue.

Risk: Virtually all emails containing viruses are sent with executable attachments. 0-day exploits take advantage of security vulnerabilities on the same day the vulnerabilities become known to the general public (TechTarget 2004). This generates a significant risk even if the system is updated with the current IDE files and the email passes through the anti-virus queue without being quarantined.

Compliance: In the event an infected email with a payload passes through the anti-virus queue successfully, the email should be quarantined by the attachment-filtering queue.

Testing:

1. Login to the Ciphertrust appliance using the web browser interface.
2. Select the "Queue Manager" tab at the top of the page.
3. Select the "Attachment Filtering" queue area.
4. Provide examples of 2 different quarantined attachments (i.e. exes).
5. Include the list of the blocked attachment extensions.

Objective/Subjective: Objective
This is an objective test that is necessary to determine the strength of the layered security model. Documented evidence will be provided to prove the exchange server quarantines the infected email.

Success/Failure: To be completed during audit fieldwork.

Audit Fieldwork: To be completed during audit fieldwork.

Post Test Results/Audit Findings: To be completed during audit fieldwork.

Audit Step 4 – Physical Security

Reference: Maxwell, Mike. "Auditing an ISP/POP IMAP Email Server: An Independent Auditor's Perspective" (February 2004)
http://www.giac.org/practical/GSNA/Mike_Maxwell_GSNA.pdf

Control Objective: Determine the physical security controls implemented by the security department.

Risk: If the system were damaged, this would initiate a significant window of downtime and result in a loss in production. Without sufficient physical and environmental security controls, the appliance could be compromised or even stolen from the computer room.

Compliance: Access to the computer room should be controlled. Corporate policy requires that all network devices be stored where access to the room is granted only by card key access. Environmental controls should also be present to monitor room temperature etc. Due to confidentiality and security best practices, no copy of the financial institution's corporate policy will be included in this audit. In addition, security logs and computer room access logs will not be included to maintain security best practice.

Testing:

1. Use digital photos to illustrate environmental controls in the facility.
2. Is there a fire control panel located in the facility?
3. In the event of a power failure, are there backup generators to restore power?
4. Determine if the facility controls individuals entering and leaving the facility.

Objective/Subjective: Objective
This is an objective test that requires interaction with various devices to determine the physical and environmental controls in the facility.

Success/Failure: To be completed during audit fieldwork.

Audit Fieldwork: To be completed during audit fieldwork.

Post Test Results/Audit Findings: To be completed during audit fieldwork.

Audit Step 5 – Virus Protection/IDE File Updates

Reference: Novoblisky, Kimberly M. "Audit of an SSL VPN; Secure remote email solution for a financial institution"
http://www.giac.org/practical/GSNA/Kimberly_Novoblisky_GSNA.pdf

Control Objective: Ensure the system is configured to automatically update IDE files when new ones are dispatched from the SOPHOS update site.

Risk: If IDE files, or virus definition files, are not updated in a timely manner for new viruses circulating in the wild, the system will not quarantine the infected emails. Then it becomes possible for the users to receive and execute the payload in the infected messages.

Compliance: Virus definition files should be updated with extreme frequency to ensure the company and its assets are protected from malicious viruses that spread via email.

Testing:

1. Login to the Ciphertrust appliance using the web browser interface.
2. Select the "Anti-Virus" tab.
3. On the left side under Anti-Virus Manager, select Auto Anti-Virus Updates. Ensure the "Automatically Upgrade Anti Virus Software" is checked.
4. On the left side under Anti-Virus Manager, select Current Anti-Virus Information. Include a screen shot to provide evidence the IDE files are being updated.
5. Review the log information and determine if the IDE files are updated.

Objective/Subjective: Objective
This is an objective test. There are many new email viruses released during and after business hours. It's imperative that anti virus engines update their definition files often.

Success/Failure: To be completed during audit fieldwork.

Audit Fieldwork: To be completed during audit fieldwork.

Post Test Results/Audit Findings: To be completed during audit fieldwork.

Audit Step 6 – SSH Tunnel Integrity Check

Reference: Kreuger, Benjamin. [SSL] sshd1 exploit. Many versions.
http://www.ssc.com/pipermail/linux-list/2001-November/010581.html

Control Objective: The Ciphertrust appliance uses the SSH protocol to allow remote connections to the box for administration and support. Perform a "passive" scan on the appliance to determine if the SSH version the appliance is running is subject to any known vulnerabilities.

Risk: There are known vulnerabilities in the wild associated with the SSH protocol. If any of these vulnerabilities were exploited successfully, an attacker could gain root access to the box with full system privileges.

Compliance: The SSH protocol the appliance uses for remote connections should be patched and protected from vulnerabilities circulating in the wild.

Testing:

1. Open the SuperScan 4.0 application.
2. Input the target IP address of the system to scan.
3. Start scan.
4. Determine what version of the SSH protocol the appliance is using.
5. Determine vulnerabilities associated with the SSH protocol?

Objective/Subjective: Objective
This is an objective test. The scan results will determine what version of the SSH protocol the appliance is currently running.

Success/Failure: To be completed during audit fieldwork.

Audit Fieldwork: To be completed during audit fieldwork.

Post Test Results/Audit Findings: To be completed during audit fieldwork.

Audit Step 7 – E-Mail Relay

Reference: Ciphertrust Ironmail 4.0 Manual. https://supportcenter.ciphertrust.com/home.php\4.0Manual.pdf. Ironmail 4.0 User Manual Pg. 52/496. "Allow message relaying to external domains"

Control Objective: Ensure the allow relay feature of the appliance is functioning properly.

Risk: Spammers and malicious virus writers often remotely take over email servers and use them as launching pads for marketing campaigns and targets for viruses. If an attacker compromised the appliance, the attacker could potentially use the internal mail servers to conduct criminal activity.

Compliance: The appliance should only allow email relay from IP addresses in pre-defined subnets on the allow relay list.

Testing:

1. Login to the Ciphertrust appliance using a web browser interface.
2. Select the "Mail Firewall" tab.
3. On the left hand side of the window, select the "Allow Relay" hyperlink.
4. Verify the allow relay is authorized.

Objective/Subjective: Objective
This is an objective test. The screen shots will illustrate the configuration of the allow relay list currently being used.

Success/Failure: To be completed during audit fieldwork.
Audit Fieldwork: To be completed during audit fieldwork.
Post Test Results/Audit Findings: To be completed during audit fieldwork.

Audit Step 8 – Vulnerability Assessment
Reference: Retina Manual Pg 38/83 "Retina Audit Wizard" http://www.google.com/search?hl=en&ie=UTF-8&q=retina+audit+steps
Control Objective: Using the Retina Security Scanner, ensure there are no unnecessary ports active on the appliance. Retina uses a file, called an RTH that contains information about known security vulnerabilities, to scan the target system. This application performs an automatic web update for the RTH file each time a session is started. The scanner is then able to determine if the system has vulnerabilities and reports the feedback in an HTML report.
Risk: Ports open that are not used make it possible for an attacker to exploit any vulnerability associated with those ports and potentially steal confidential information quarantined on the appliance.
Compliance: As defined in section 1, only ports required to send and receive business related emails should be active and listening.
Testing: 1. Start the Retina Security Scanner. 2. In the select targets area, select the target IP address of the system to scan. 3. On the right side, click "start scan" under audit tasks. 4. Document results.
Objective/Subjective: Objective This is an objective test. The results from the retina scan will provide information about open and closed ports on the appliance. The scan will also provide remediation steps to ensure the appliance is secure.
Success/Failure: To be completed during audit fieldwork.
Audit Fieldwork: To be completed during audit fieldwork.
Post Test Results/Audit Findings: To be completed during audit fieldwork.

Audit Step 9 – Built In IDS System Functionality
Reference: The financial institution's "Defense in Depth" security model. Executive management approved the model and implementation began in September 2002.
Control Objective: Ensure the built-in Intrusion Detection System is functioning properly. Launch a DDoS attack against the appliance and document results.
Risk: A successful attack against a critical network resource going unnoticed could allow enough time for an attacker to steal sensitive information.
Compliance: The appliance should have an alerting system to notify information security that an attack has been attempted.
Testing:

1. Using Nessus, launch an attack against the Ciphertrust appliance. 2. Login to the appliance; select the "Mail IDS" tab. On the left side, select Network Level – Analysis Console. 3. Select the hyperlink number next "Unique Alerts". 4. Determine the most frequent 5 alerts. 5. Provide an example of a DDoS alert. 6. Provide the results from the Nessus scan. 7. Document the results.
Objective/Subjective: Objective This is an objective test. The results from the built-in IDS system will provide information regarding the attack.
Success/Failure: To be completed during audit fieldwork.
Audit Fieldwork: To be completed during audit fieldwork.
Post Test Results/Audit Findings: To be completed during audit fieldwork.

Audit Step 10 – Allocation of Administrative Resources
Reference: Frigon, Stephanie. "Auditing a Small Internet Business Hosted by an Internet Service Provider: An Auditor's Perspective" (October 2003) http://www.giac.org/practical/GSNA/Stephanie_Frigon_GSNA.pdf
Control Objective: Verify that an employee of the Network Security Department has been assigned to administer and monitor the appliance on a daily basis.
Risk: Providing resources to effectively monitor and administer the appliance is crucial to identify and respond to attacks in a timely manner. If resources are not available to monitor the system, remote or even internal attacks could go unnoticed for extended periods of time.
Compliance: Information security personnel should be available, trained and prepared to respond to attacks that may occur during or after business hours.
Testing: 1. Consult with the Information Security Manager and determine the department personnel responsible for monitoring and administering the Ciphertrust email gateway appliance. 2. Provide task percentages for daily administration.
Objective/Subjective: Subjective
Success/Failure: To be completed during audit fieldwork.
Audit Fieldwork: To be completed during audit fieldwork.
Post Test Results/Audit Findings: To be completed during audit fieldwork.

Audit Step 11 – Displayed Warning Banner

Reference: Novoblisky, Kimberly M. "Audit of an SSL VPN; Secure remote email solution for a financial institution"
http://www.giac.org/practical/GSNA/Kimberly_Novoblisky_GSNA.pdf

Control Objective: Determine if a warning banner is displayed before access to the logon screen is granted.

Risk: Lawsuits are always supported with documented evidence. Without a warning banner informing potential attackers that un-authorized access to the system is prohibited, there is only substantial evidence to provide in the event a lawsuit is brought against the financial institution. On port 143, the IMAP protocol has a banner that usually contains information about the appliance. This should also be changed and a warning banner be implemented.

Compliance: Corporate issued warning banner should be displayed before a user is able to access the logon screen informing the user that the system is for authorized use only.

Testing:

1. Initiate a browsing session to the Ciphertrust appliance.
2. Determine if the warning banner is displayed.
3. Start a SuperScan session with the target IP address.
4. Document results of the scan.

Objective/Subjective: Objective
This is an objective test. The screen shots and the Superscan results will provide evidence of banners currently displayed on the appliance.

Success/Failure: To be completed during audit fieldwork.

Audit Fieldwork: To be completed during audit fieldwork.

Post Test Results/Audit Findings: To be completed during audit fieldwork.

Audit Step 12 – International Domains

Reference: The financial institution's "Defense in Depth" security model. Executive management approved the model and implementation began in September 2002.

Control Objective: Ensure the Ciphertrust appliance blocks all international domains that are not used for daily business activity.

Risk: Spammers and virus writers are operating all over the world. If international domains are not blocked, this provides yet another avenue for an international attacker to compromise a network resource. By implementing as many mitigating factors as possible, it reduces the risk of a system compromise.

Compliance: All international domains not used on a daily basis should be blocked before emails from those domains reach the policy scan process.

Testing:

1. Provide a list of all domains blocked by the appliance.
2. Provide a list of "accepted" domains.
3. Include instructions on how to setup the rule to block a domain.

Objective/Subjective: Objective
This is an objective test. Screen shots will provide evidence of the blocked international domains.

Success/Failure: To be completed during audit fieldwork.

Audit Fieldwork: To be completed during audit fieldwork.

Post Test Results/Audit Findings: To be completed during audit fieldwork.

Section 3 – Audit Fieldwork

Audit Step 1 – Administrator Password Strength

Reference: Novoblisky, Kimberly M. "Audit of an SSL VPN; Secure Remote Email Solution for a Financial Institution"
http://www.giac.org/practical/GSNA/Kimberly_Novoblisky_GSNA.pdf

Control Objective: Verify the administrator password is strong.

Risk: Weak, easy to guess passwords make it significantly easier for an attacker to crack a system administrator's password. If the crack is successful, the attacker could take complete control of the system.

Compliance: Ensure administrator passwords comply with the financial institutions corporate password policy. The policy states administrator passwords must be at least a combination of 8 alphanumeric characters in length.

Testing:

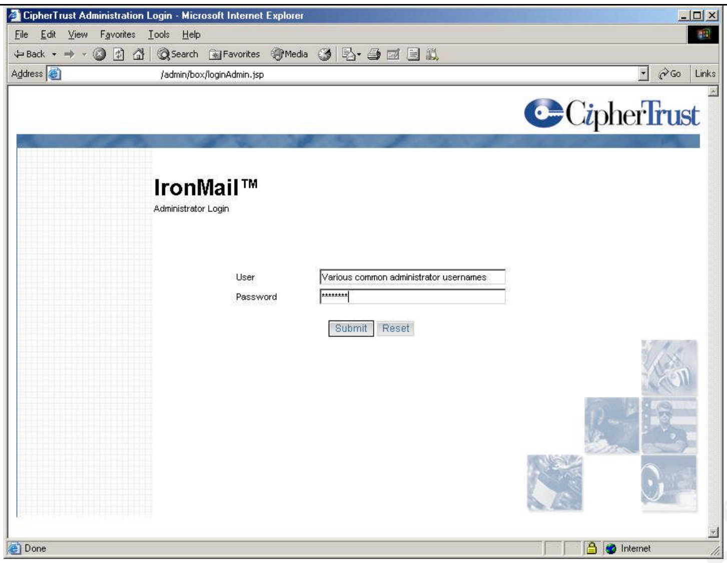
6. Initiate a browsing session to the Ciphertrust appliance.
7. Attempt a series of common Administrator usernames and passwords to login to the appliance.
8. Document any successful tests.
9. In the event a login errors out, determine what error message is displayed. *Security Analyst's Important Note: Ensure the error message does not display unnecessary information such as "Valid Username/Invalid Password. This tells the attacker that the Username was defined in the system. The error message should read, "Username/Password is invalid", which does not volunteer any information.*
10. Document evidence.

Objective/Subjective: Objective
This test is necessary to determine the strength of the system administrator password. In order to effectively complete fieldwork on this audit step, a copy of the corporate password policy would need to be obtained as evidence of security policy compliance. No copy will be included for reasons pertaining to confidentiality and best security practice.

Success/Failure: This was a successful test.

Audit Fieldwork:

1. Initiate a browsing session to the Ciphertrust appliance.


CipherTrust Administration Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address /admin/box/loginAdmin.jsp
Go Links
CipherTrust
Done
Internet

IronMail™

Administrator Login

User Various common administrator usernames

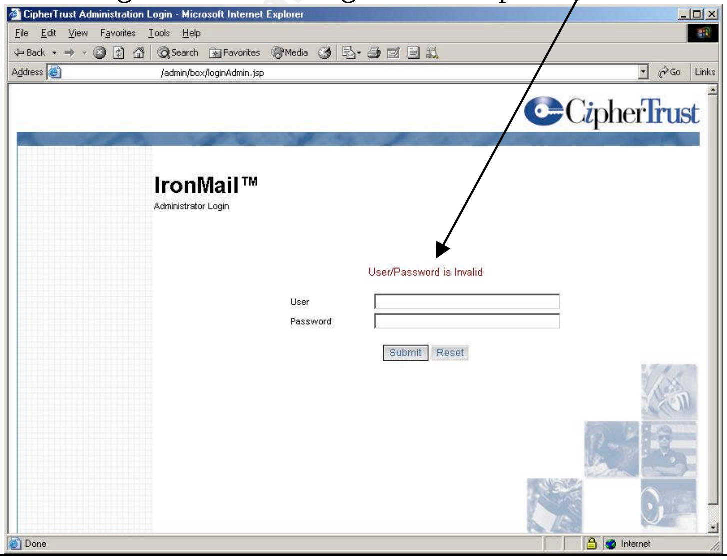
Password ********

Submit Reset

2. Attempt a series of common Administrator usernames and passwords to login to the appliance. The following usernames and passwords were tried:

Username	Password
Administrator	Admin
Admin	Administrator
Ciphertrust	Ciphertrust
Admin	Password
Root	Password
Admin	Ciphertrust
Administrator	Ciphertrust

3. No successful logins.
4. In the event a login errors out, determine what error message is displayed. All tests gave the following invalid response.


CipherTrust Administration Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address /admin/box/loginAdmin.jsp
Go Links
CipherTrust
Done
Internet

IronMail™

Administrator Login

User/Password is Invalid

User

Password

Submit Reset

Post Test Results/Audit Findings:

- There were no successful login tests. Therefore, the username and password used on this appliance are not common in nature. No findings.

Audit Step 2 – System Required Re-Authentication After Session Time Out

Reference: Novoblisky, Kimberly M. "Audit of an SSL VPN; Secure remote email solution for a financial institution"
http://www.giac.org/practical/GSNA/Kimberly_Novoblisky_GSNA.pdf

Control Objective: Verify system administration is not attainable after 30 minutes of idle time.

Risk: Individual gains un-authorized access with full system privileges by using an authorized session started by an administrator. All users that have accounts on the system are system administrators by default. The accounts have full system privileges to make firewall, local system IDS and service changes. In addition, a user could release malicious viruses into the internal network.

Compliance: The session automatically logs the user out of the system after 30 minutes of inactivity.

Testing:

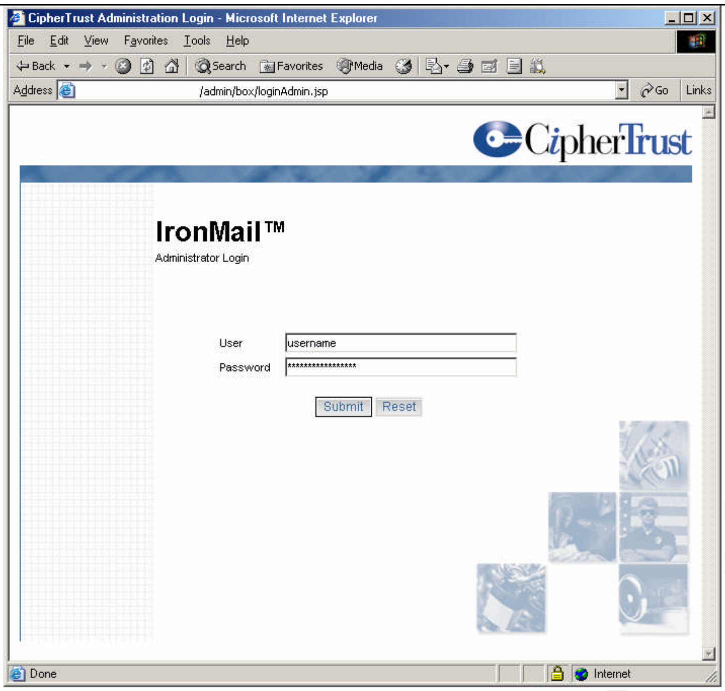
6. Start a Ciphertrust session using the web browser interface.
7. Login to the system.
8. Allow 30 minutes of idle time. According to the system configuration, the sessions will time out after 30 minutes of idle time. The session minute count can be changed at system administrator's discretion.
9. Return to the session after 31 minutes. Ensure account login credentials must be re-entered to gain privileged access to the system.
10. Document evidence of test procedures.

Objective/Subjective: Objective
This is an objective test to ensure an un-authorized user is not able to take over the appliance without having an authorized account defined in the system. To give an example, a Ciphertrust system administrator could leave work at 5 p.m. without having logged out of the session. The night janitor with minimal technical "know-how" could take control of the Ciphertrust box without having an authorized login. The system was built for easy navigation and the web interface is very user friendly. The janitor could then simply select the "Quarantine" tab, select "Viruses-Quarantined" and release every virus on the system into the internal network.

Success/Failure: This was a successful test.

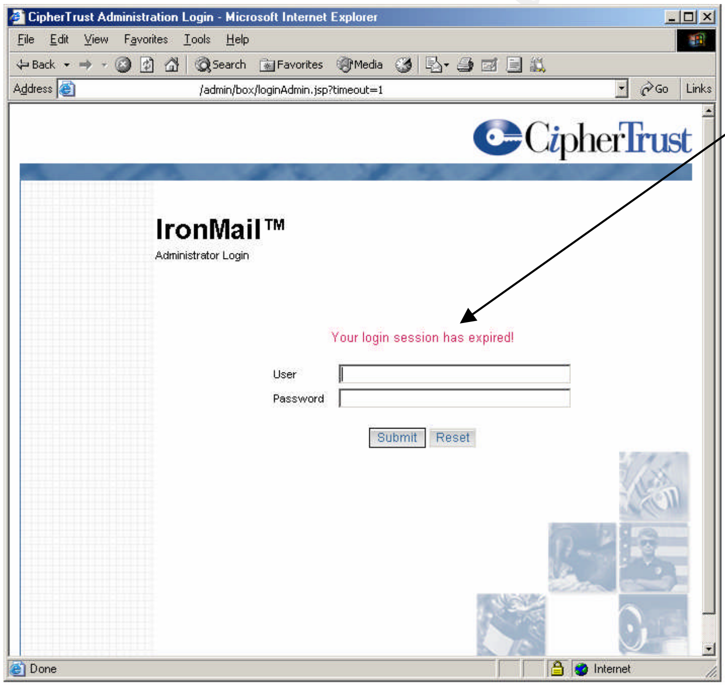
Audit Fieldwork:

1. Start a Ciphertrust session using the web browser interface.
2. Login to the system.



CipherTrust Administration Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address /admin/box/loginAdmin.jsp
Go Links
CipherTrust
IronMail™
Administrator Login
User
username
Password
Submit
Reset
Done
Internet

3. Allow 30 minutes of idle time… … … …
4. The system has automatically logged out of the session after 31 minutes.



CipherTrust Administration Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address /admin/box/loginAdmin.jsp?timeout=1
Go Links
CipherTrust
IronMail™
Administrator Login
User
Password
Submit
Reset
Done
Internet

Your login session has expired!

Post Test Results/Audit Findings:

- After the system is idle for over 30 minutes, the session expires requiring the user to input the login credentials to initiate another session. No findings.

Audit Step 3 – Layered Protection

Reference: The financial institution’s “Defense in Depth” security model. Executive management approved the model and implementation began in September 2002.

Control Objective: Ensure virus-infected emails with an attachment (i.e. .exe, .bat) are quarantined after passing through the anti-virus queue.

Risk: Virtually all emails containing viruses are sent with executable attachments. 0-day exploits take advantage of security vulnerabilities on the same day the vulnerabilities become known to the general public (TechTarget 2004). This generates a significant risk even if the system is updated with the current IDE files and the email passes through the anti-virus queue without being quarantined.

Compliance: In the event an infected email with a payload passes through the anti-virus queue successfully, the email should be quarantined by the attachment-filtering queue.

Testing:

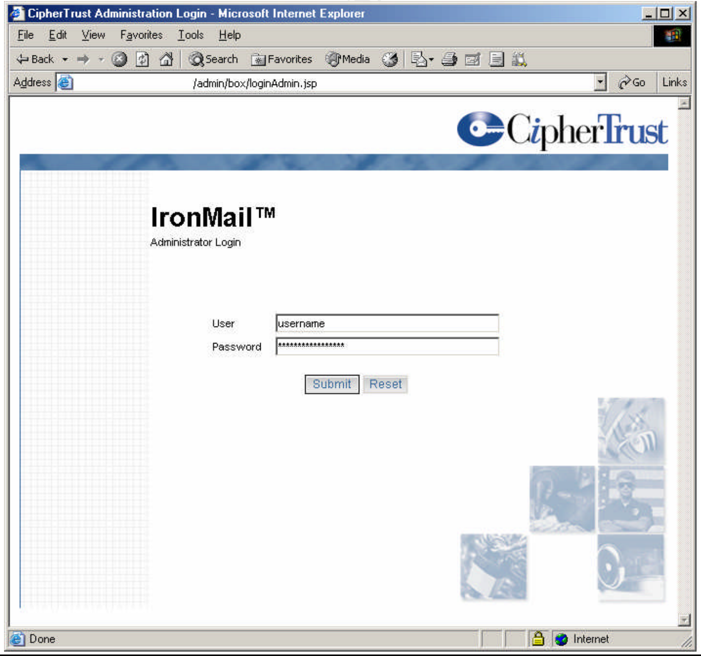
6. Login to the Ciphertrust appliance using the web browser interface.
7. Select the “Queue Manager” tab at the top of the page.
8. Select the “Attachment Filtering” queue area.
9. Provide examples of 2 different quarantined attachments (i.e. exes).
10. Include the list of the blocked attachment extensions.

Objective/Subjective: Objective
This is an objective test that is necessary to determine the strength of the layered security model. Documented evidence will be provided to prove the exchange server quarantines the infected email.

Success/Failure: This was a successful test.

Audit Fieldwork:

1. Login to the Ciphertrust appliance.



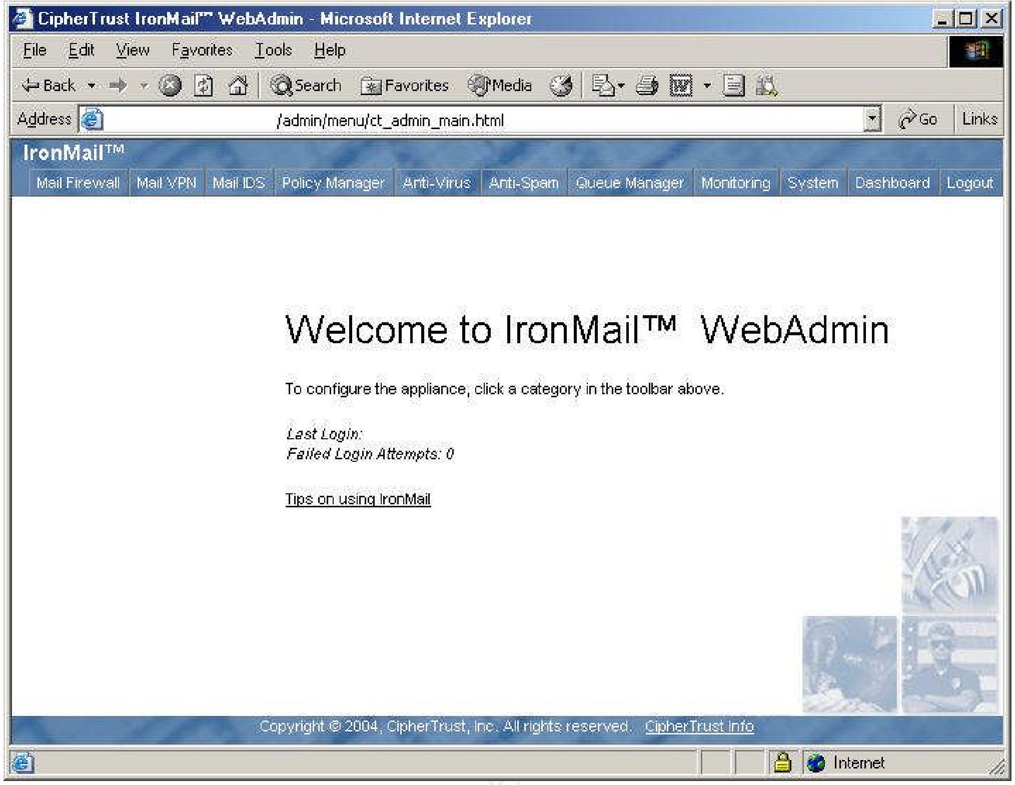
CipherTrust Administration Login - Microsoft Internet Explorer

Address /admin/box/loginAdmin.jsp

IronMail™
Administrator Login

User username
Password ****************

2. Select the “Queue Manager” tab at the top of the page.


CipherTrust IronMail™ WebAdmin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address /admin/menu/ct_admin_main.html Go Links
IronMail™
Mail Firewall Mail VPN Mail IDS Policy Manager Anti-Virus Anti-Spam Queue Manager Monitoring System Dashboard Logout
Internet

Welcome to IronMail™ WebAdmin

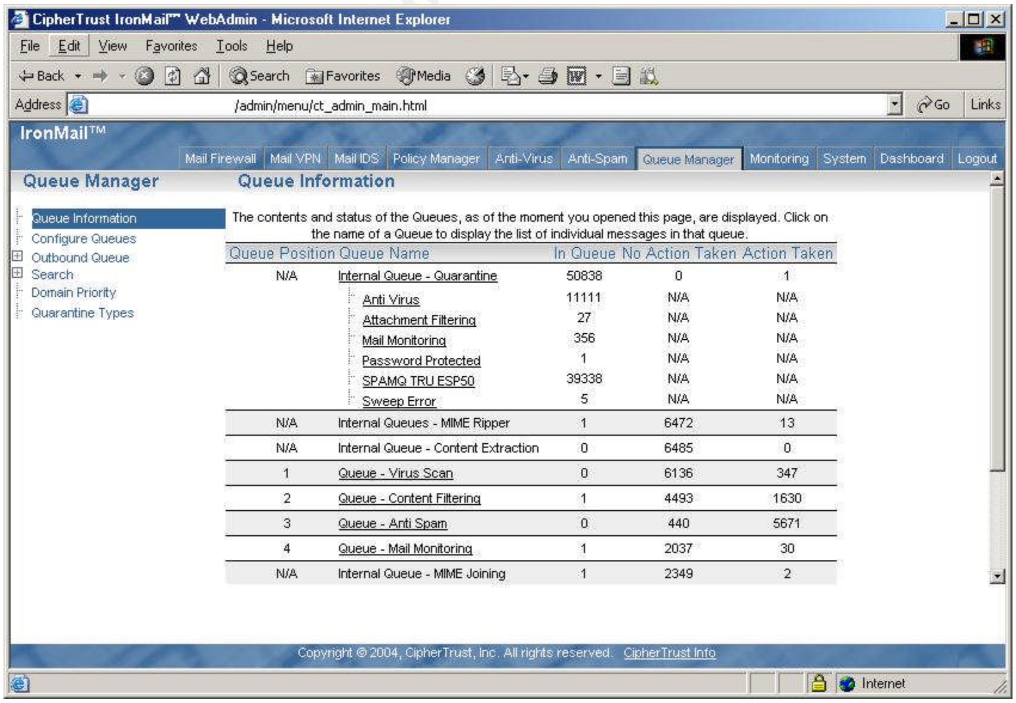
To configure the appliance, click a category in the toolbar above.

Last Login:
Failed Login Attempts: 0

Tips on using IronMail

Copyright © 2004, CipherTrust, Inc. All rights reserved. CipherTrust Info

3. Select the Attachment Filtering queue area. The emails were quarantined in this area.


CipherTrust IronMail™ WebAdmin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address /admin/menu/ct_admin_main.html Go Links
IronMail™
Mail Firewall Mail VPN Mail IDS Policy Manager Anti-Virus Anti-Spam Queue Manager Monitoring System Dashboard Logout
Queue Manager
Queue Information
Configure Queues
Outbound Queue
Search
Domain Priority
Quarantine Types
Internet

Queue Information

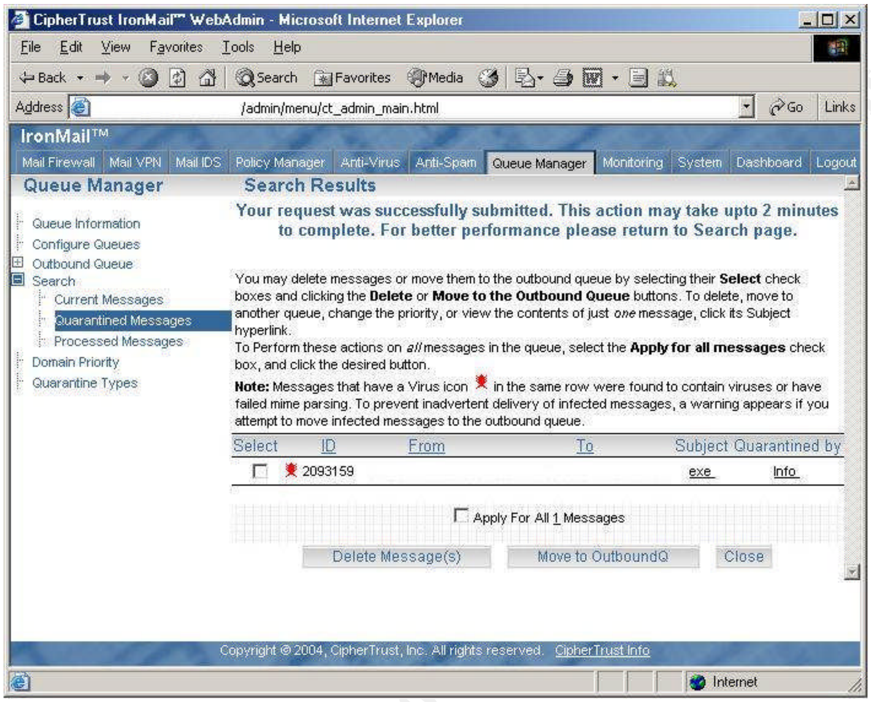
The contents and status of the Queues, as of the moment you opened this page, are displayed. Click on the name of a Queue to display the list of individual messages in that queue.

Queue Position	Queue Name	In Queue	No Action Taken	Action Taken
N/A	Internal Queue - Quarantine	50838	0	1
	Anti Virus	11111	N/A	N/A
	Attachment Filtering	27	N/A	N/A
	Mail Monitoring	356	N/A	N/A
	Password Protected	1	N/A	N/A
	SPAMQ TRU ESP50	39338	N/A	N/A
	Sweep Error	5	N/A	N/A
N/A	Internal Queues - MIME Ripper	1	6472	13
N/A	Internal Queue - Content Extraction	0	6485	0
1	Queue - Virus Scan	0	6136	347
2	Queue - Content Filtering	1	4493	1630
3	Queue - Anti Spam	0	440	5671
4	Queue - Mail Monitoring	1	2037	30
N/A	Internal Queue - MIME Joining	1	2349	2

Copyright © 2004, CipherTrust, Inc. All rights reserved. CipherTrust Info

4. The following 2 emails were sent through the appliance to determine how the system would process the messages.

- 1) The first is an infected email provided by Sophos. The message has the attachment known as the “Eicar-AV-Test”. The payload consists of test material that is not deemed as malicious. The system simply recognizes the email as a possible virus. The latest signature for the Eicar test has been installed.


CipherTrust IronMail™ WebAdmin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address /admin/menu/ct_admin_main.html
Go Links
IronMail™
Mail Firewall Mail VPN Mail IDS Policy Manager Anti-Virus Anti-Spam Queue Manager Monitoring System Dashboard Logout
Queue Manager
Queue Information
Configure Queues
Outbound Queue
Search
Current Messages
Quarantined Messages
Processed Messages
Domain Priority
Quarantine Types
Delete Message(s) Move to OutboundQ Close
Copyright © 2004, CipherTrust, Inc. All rights reserved. CipherTrust Info
Internet

Search Results

Your request was successfully submitted. This action may take upto 2 minutes to complete. For better performance please return to Search page.

You may delete messages or move them to the outbound queue by selecting their **Select** check boxes and clicking the **Delete** or **Move to the Outbound Queue** buttons. To delete, move to another queue, change the priority, or view the contents of just *one* message, click its Subject hyperlink.

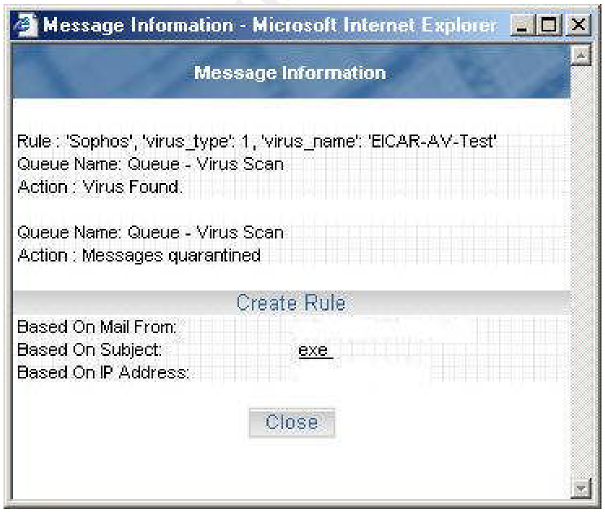
To Perform these actions on *all* messages in the queue, select the **Apply for all messages** check box, and click the desired button.

Note: Messages that have a Virus icon ✱ in the same row were found to contain viruses or have failed mime parsing. To prevent inadvertent delivery of infected messages, a warning appears if you attempt to move infected messages to the outbound queue.

Select	ID	From	To	Subject	Quarantined by
□	✱ 2093159			exe	Info

□ Apply For All 1 Messages

- The following screen shot includes the message details of the infected message identified as by the appliance. The virus scan determined there was a payload that included an executable attachment, and quarantined it in the Anti-Virus Queue.



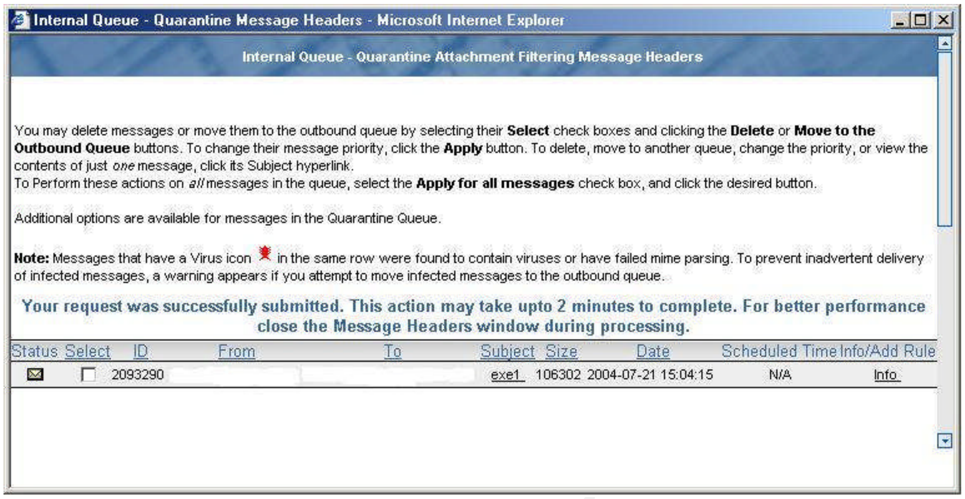
Rule : 'Sophos', 'virus_type': 1, 'virus_name': 'EICAR-AV-Test'
Queue Name: Queue - Virus Scan
Action : Virus Found.

Queue Name: Queue - Virus Scan
Action : Messages quarantined

Create Rule

Based On Mail From:
Based On Subject: exe
Based On IP Address:

- 2) The second test includes a generic message with an executable attachment and no virus payload. The test was performed to ensure the appliance is configured to block attachments that can be executed by unsuspecting users. The following screen shot illustrates the email was quarantined by the attachment filtering queue.


Internal Queue - Quarantine Message Headers - Microsoft Internet Explorer
Internal Queue - Quarantine Attachment Filtering Message Headers

You may delete messages or move them to the outbound queue by selecting their **Select** check boxes and clicking the **Delete** or **Move to the Outbound Queue** buttons. To change their message priority, click the **Apply** button. To delete, move to another queue, change the priority, or view the contents of just *one* message, click its Subject hyperlink.
To Perform these actions on *all* messages in the queue, select the **Apply for all messages** check box, and click the desired button.

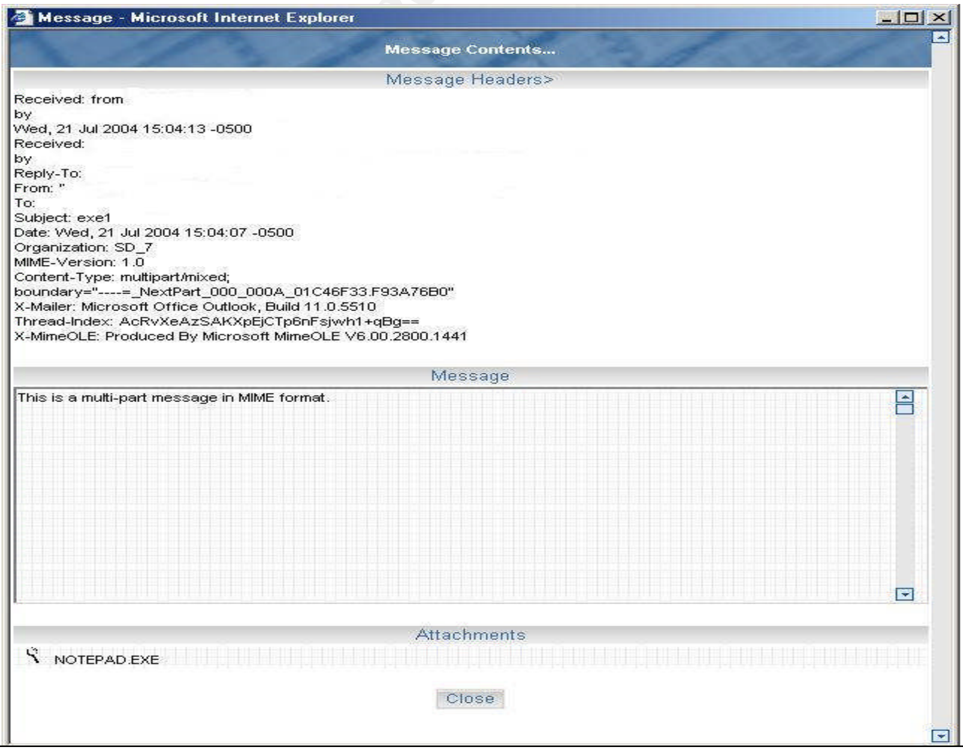
Additional options are available for messages in the Quarantine Queue.

Note: Messages that have a Virus icon ✱ in the same row were found to contain viruses or have failed mime parsing. To prevent inadvertent delivery of infected messages, a warning appears if you attempt to move infected messages to the outbound queue.

Your request was successfully submitted. This action may take upto 2 minutes to complete. For better performance close the Message Headers window during processing.

Status	Select	ID	From	To	Subject	Size	Date	Scheduled Time	Info/Add Rule
✉	□	2093290			exe1	106302	2004-07-21 15:04:15	N/A	Info

- The following screen shot provides the contents of the quarantined attachment, which includes the message headers. The message header provides information pertaining to the origination of the message, who received the message and the date and time stamp. This information will help determine the validity of a suspicious email.



```
Received: from
by
Wed, 21 Jul 2004 15:04:13 -0500
Received:
by
Reply-To:
From: "
To:
Subject: exe1
Date: Wed, 21 Jul 2004 15:04:07 -0500
Organization: SD_7
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="----=_NextPart_000_000A_01C46F33.F93A76B0"
X-Mailer: Microsoft Office Outlook, Build 11.0.5510
Thread-Index: AcRvXeAzSAKXpEjCTp6nFsjwh1+qBg==
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1441
```

This is a multi-part message in MIME format.

NOTEPAD.EXE

- The following list was exported from the appliance to provide evidence of the file extensions that are blocked.

Blocked Attachment List Ciphertrust Config July 2004			
dll	lib	msp	sys
obj	vbe	mde	js
ade	chm	pif	pcd
hta	vb	sea	adp
exe	lnk	shb	scr
url	shs	mdb	reg
crt	hlp	ins	cmd
isp	wsh	msi	com
jse	eml	bat	wsc
vbs	wsf	msc	inf
sct	mst	cpl	

Post Test Results/Audit Findings:

- In the event an infected email with a 0-day exploit is sent, the appliance is prepared to stop the message before it reaches the internal network. The two tests confirm that the appliance is properly configured to block both infected messages with signatures defined in the appliance anti-virus engine and executable attachments with no virus payload. No findings to report.

Audit Step 4 – Physical Security

Reference: Maxwell, Mike. "Auditing an ISP/POP IMAP Email Server: An Independent Auditor's Perspective" (February 2004) http://www.giac.org/practical/GSNA/Mike_Maxwell_GSNA.pdf

Control Objective: Determine the physical security controls implemented by the security department.

Risk: If the system were damaged, this would initiate a significant window of downtime and result in a loss in production. Without sufficient physical and environmental security controls, the appliance could be compromised or even stolen from the computer room.

Compliance: Access to the computer room should be controlled. Corporate policy requires that all network devices be stored where access to the room is granted only by card key access. Environmental controls should also be present to monitor room temperature etc. Due to confidentiality and security best practices, no copy of the financial institution's corporate policy will be included in this audit. In addition, security logs and computer room access logs will not be included to maintain security best practice.

Testing:

5. Use digital photos to illustrate environmental controls in the facility.
6. Is there a fire control panel located in the facility?
7. In the event of a power failure, are there backup generators to restore power?

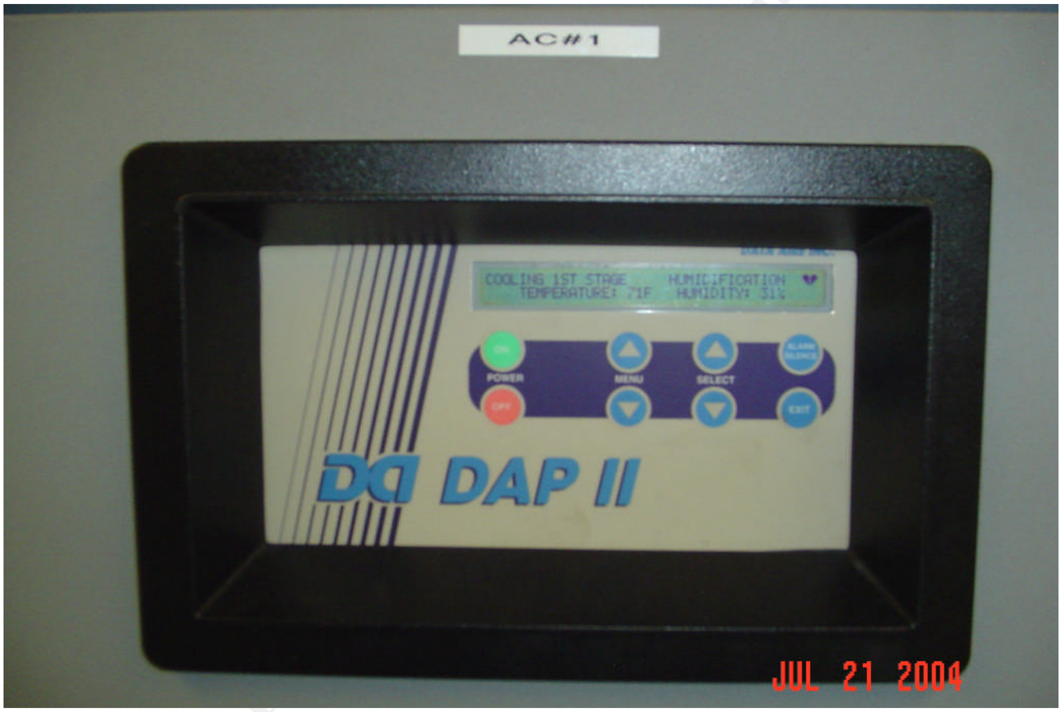
8. Determine if the facility controls individuals entering and leaving the facility.

Objective/Subjective: Objective
This is an objective test that requires interaction with various devices to determine the physical and environmental controls in the facility.

Success/Failure: This was a successful test.

Audit Fieldwork:

- After touring the facility, it was determined there were sufficient controls in place to monitor environmental information such as room temperature and air quality. The following photographs were taken of the two air conditioning units, one unit is located at the entrance and one at the back of the facility.



- The air conditioning unit's monitoring window provides information regarding room temperature and humidity levels. It is essential the room stay at a cool temperature to ensure the network devices do not overheat. The systems are setup to automatically maintain a pre-defined temperature of 70 degrees at all times.

- Verify a fire control console is mounted in the facility. The green tag shows the console was serviced by the fire department in April 2004. Fire suppression devices should have periodic checks by certified personnel to make sure the devices are functioning properly.

- Verify backup generators are available to restore power in the event of a power failure. A picture of the backup devices provided below. The devices are active.

- Performed a visual inspection of access controls for the entrance door of the facility. This door is the only way to access the room and card key access is required. An attempt was made to obtain door access to security logs, however, due to security best practice; they will not be included as evidence. The security department is in the process of upgrading the logging system to a new program with a GUI (or Graphical User Interface) that will allow for HTML reporting.

Post Test Results/Audit Findings:

- ➢ It was determined there were sufficient environmental controls in the facility the appliance is located. No findings.

Audit Step 5 – Virus Protection/IDE File Updates

Reference: Novoblisky, Kimberly M. "Audit of an SSL VPN; Secure remote email solution for a financial institution" http://www.giac.org/practical/GSNA/Kimberly_Novoblisky_GSNA.pdf

Control Objective: Ensure the system is configured to automatically update IDE files when new ones are dispatched from the SOPHOS update site.

Risk: If IDE files, or virus definition files, are not updated in a timely manner for new viruses circulating in the wild, the system will not quarantine the infected emails. Then it becomes possible for the users to receive and execute the payload in the infected messages.

Compliance: Virus definition files should be updated with extreme frequency to ensure the company and its assets are protected from malicious viruses that spread via email.

Testing:

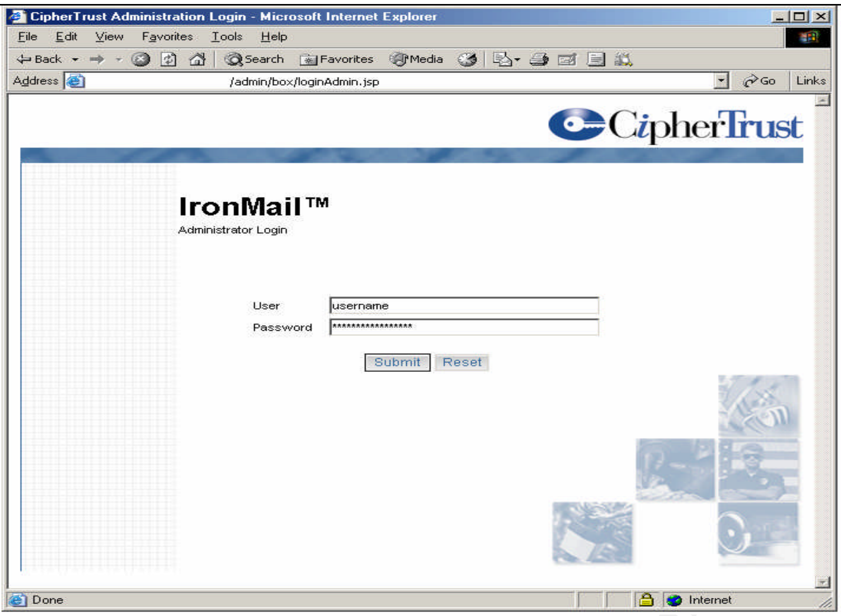
6. Login to the Ciphertrust appliance using the web browser interface.
7. Select the "Anti-Virus" tab.
8. On the left side under Anti-Virus Manager, select Auto Anti-Virus Updates. Ensure the "Automatically Upgrade Anti Virus Software" is checked.
9. On the left side under Anti-Virus Manager, select Current Anti-Virus Information. Include a screen shot to provide evidence the IDE files are being updated.
10. Review the log information and determine if the IDE files are updated.

Objective/Subjective: Objective
This is an objective test. There are many new email viruses released during and after business hours. It's imperative that anti virus engines update their definition files often.

Success/Failure: This was a successful test.

Audit Fieldwork:

1. Login to the Ciphertrust appliance using the web browser interface.


File Edit View Favorites Tools Help
Back Search Favorites Media
Go Links
CipherTrust
Done
Internet

CipherTrust Administration Login - Microsoft Internet Explorer

Address /admin/box/loginAdmin.jsp

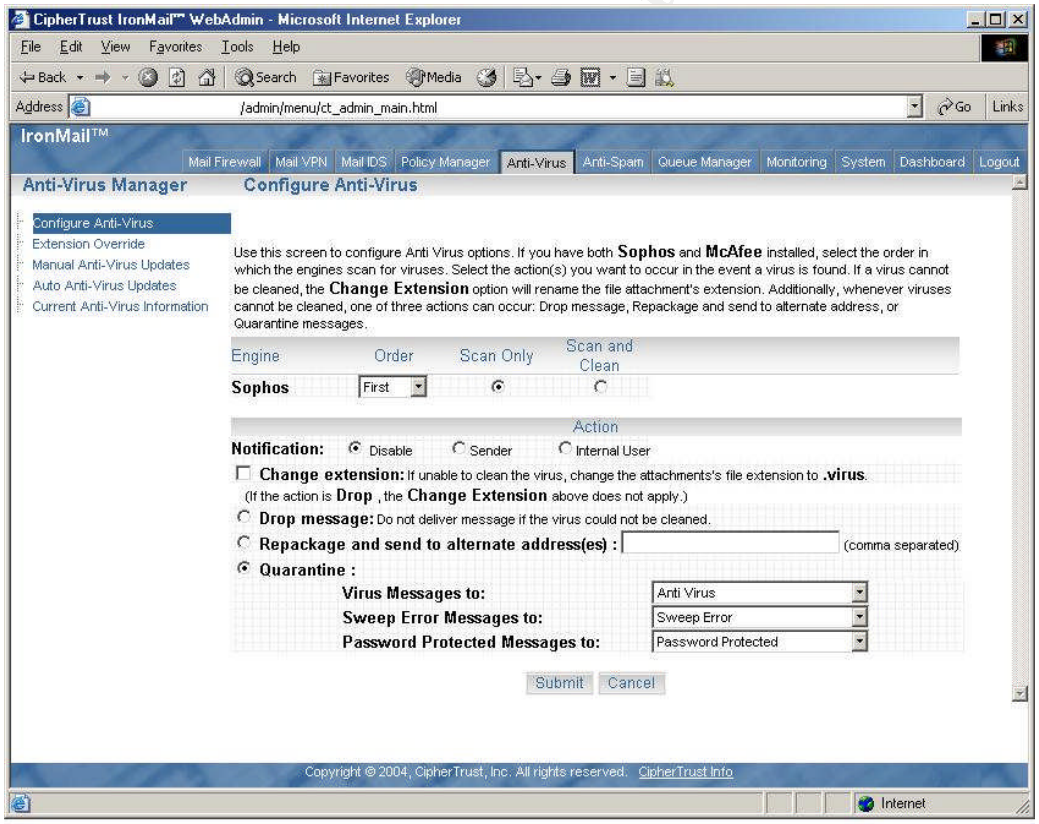
IronMail™

Administrator Login

User	username
Password	****************

Submit Reset

2. Select the “Anti-Virus” tab.



CipherTrust IronMail™ WebAdmin - Microsoft Internet Explorer

Address /admin/menu/ct_admin_main.html

Anti-Virus Manager — Configure Anti-Virus

Use this screen to configure Anti Virus options. If you have both **Sophos** and **McAfee** installed, select the order in which the engines scan for viruses. Select the action(s) you want to occur in the event a virus is found. If a virus cannot be cleaned, the **Change Extension** option will rename the file attachment's extension. Additionally, whenever viruses cannot be cleaned, one of three actions can occur: Drop message, Repackage and send to alternate address, or Quarantine messages.

Engine	Order	Scan Only	Scan and Clean
Sophos	First	●	○

Action

Notification: ● Disable ○ Sender ○ Internal User

□ **Change extension:** If unable to clean the virus, change the attachments's file extension to **.virus**.
(If the action is **Drop** , the **Change Extension** above does not apply.)

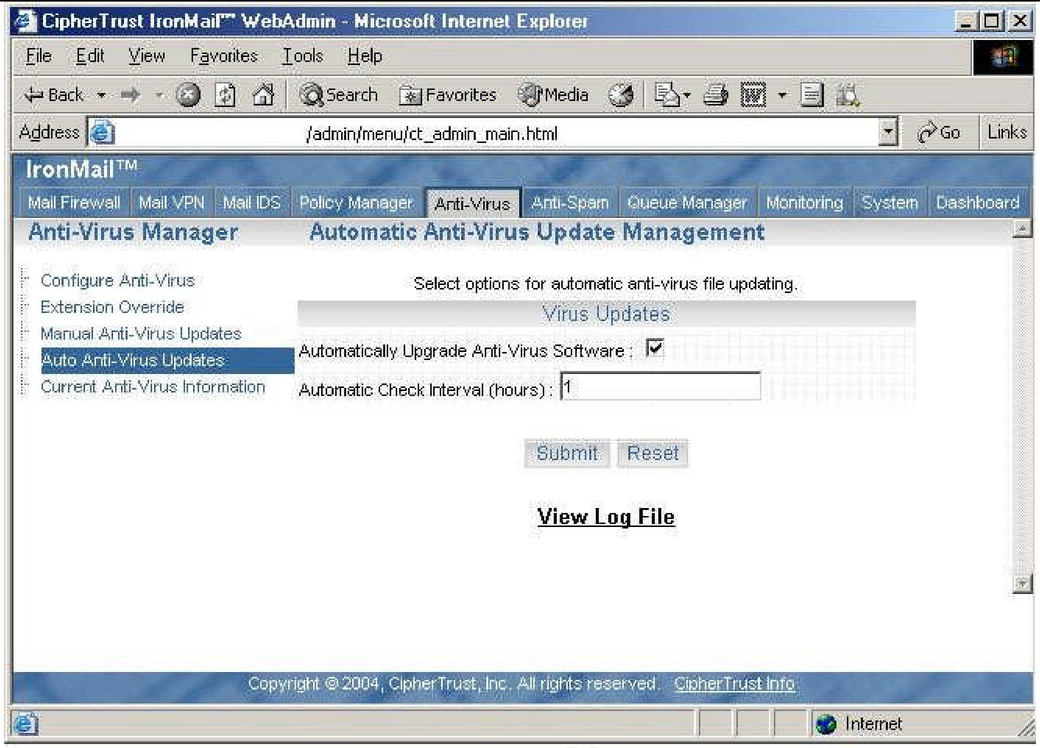
○ **Drop message:** Do not deliver message if the virus could not be cleaned.

○ **Repackage and send to alternate address(es) :** (comma separated)

● **Quarantine :**

Virus Messages to:	Anti Virus
Sweep Error Messages to:	Sweep Error
Password Protected Messages to:	Password Protected

3. On the left side under Anti-Virus Manager, select Auto Anti-Virus Updates.


CipherTrust IronMail™ WebAdmin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address /admin/menu/ct_admin_main.html
Go Links
IronMail™
Mail Firewall Mail VPN Mail IDS Policy Manager Anti-Virus Anti-Spam Queue Manager Monitoring System Dashboard
Anti-Virus Manager
Configure Anti-Virus
Extension Override
Manual Anti-Virus Updates
Auto Anti-Virus Updates
Current Anti-Virus Information
Submit Reset
View Log File
Copyright © 2004, CipherTrust, Inc. All rights reserved. CipherTrust Info
Internet

Automatic Anti-Virus Update Management

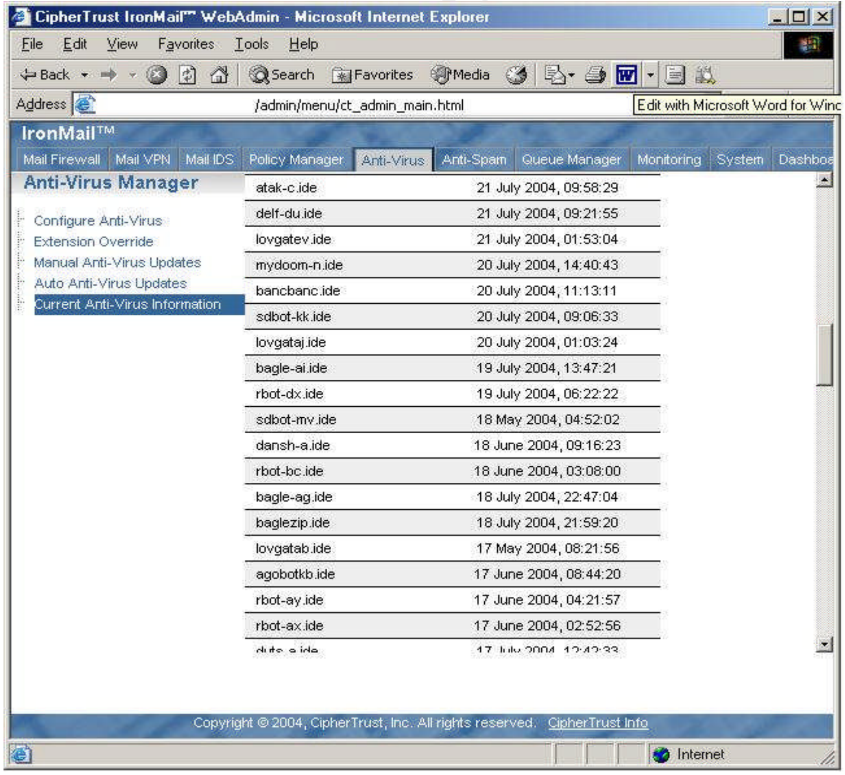
Select options for automatic anti-virus file updating.

Virus Updates

Automatically Upgrade Anti-Virus Software : ☑

Automatic Check Interval (hours) : 1

4. On the left side under Anti-Virus Manager, select Current Anti-Virus Information. Include a screen shot to provide evidence the IDE files are being updated.


CipherTrust IronMail™ WebAdmin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address /admin/menu/ct_admin_main.html
Edit with Microsoft Word for Winc
IronMail™
Mail Firewall Mail VPN Mail IDS Policy Manager Anti-Virus Anti-Spam Queue Manager Monitoring System Dashboa
Anti-Virus Manager
Configure Anti-Virus
Extension Override
Manual Anti-Virus Updates
Auto Anti-Virus Updates
Current Anti-Virus Information
Copyright © 2004, CipherTrust, Inc. All rights reserved. CipherTrust Info
Internet

atak-c.ide	21 July 2004, 09:58:29
delf-du.ide	21 July 2004, 09:21:55
lovgatev.ide	21 July 2004, 01:53:04
mydoom-n.ide	20 July 2004, 14:40:43
bancbanc.ide	20 July 2004, 11:13:11
sdbot-kk.ide	20 July 2004, 09:06:33
lovgataj.ide	20 July 2004, 01:03:24
bagle-ai.ide	19 July 2004, 13:47:21
rbot-dx.ide	19 July 2004, 06:22:22
sdbot-mv.ide	18 May 2004, 04:52:02
dansh-a.ide	18 June 2004, 09:16:23
rbot-bc.ide	18 June 2004, 03:08:00
bagle-ag.ide	18 July 2004, 22:47:04
baglezip.ide	18 July 2004, 21:59:20
lovgatab.ide	17 May 2004, 08:21:56
agobotkb.ide	17 June 2004, 08:44:20
rbot-ay.ide	17 June 2004, 04:21:57
rbot-ax.ide	17 June 2004, 02:52:56
duts-a.ide	17 July 2004, 12:42:33

Post Test Results/Audit Findings:

- The test and evidence confirms the IDE files are being updated in a timely manner.
- No findings.

Audit Step 6 – SSH Tunnel Integrity Check

Reference: Kreuger, Benjamin. [SSL] sshd1 exploit. Many versions. http://www.ssc.com/pipermail/linux-list/2001-November/010581.html

Control Objective: The Ciphertrust appliance uses the SSH protocol to allow remote connections to the box for administration and support. Perform a “passive” scan on the appliance to determine if the SSH version the appliance is running is subject to any known vulnerabilities.

Risk: There are known vulnerabilities in the wild associated with the SSH protocol. If any of these vulnerabilities were exploited successfully, an attacker could gain root access to the box with full system privileges.

Compliance: The SSH protocol the appliance uses for remote connections should be patched and protected from vulnerabilities circulating in the wild.

Testing:

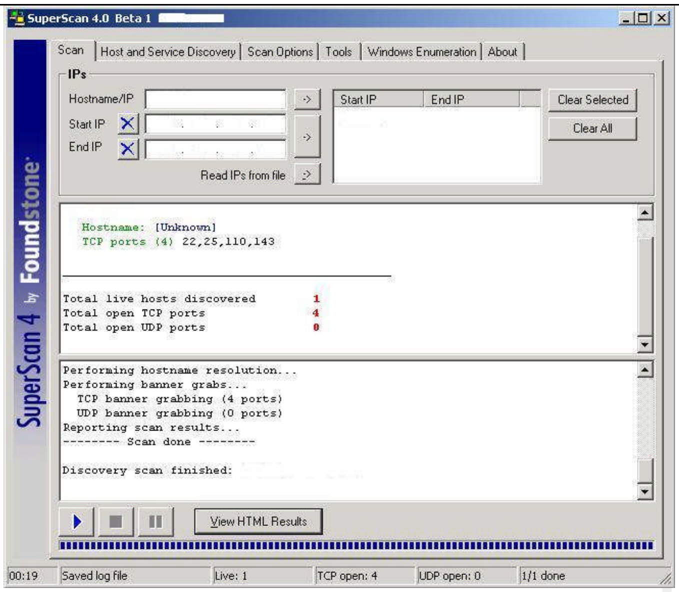
6. Open the SuperScan 4.0 application.
7. Input the target IP address of the system to scan.
8. Start scan.
9. Determine what version of the SSH protocol the appliance is using.
10. Determine vulnerabilities associated with the SSH protocol?

Objective/Subjective: Objective
This is an objective test. The scan results will determine what version of the SSH protocol the appliance is currently running.

Success/Failure: This test failed.

Audit Fieldwork:

- Start the SuperScan 4.0 application. Input the target IP address. Note: If not planning to scan an entire subnet, make sure the IP address is in the start IP and end IP areas.



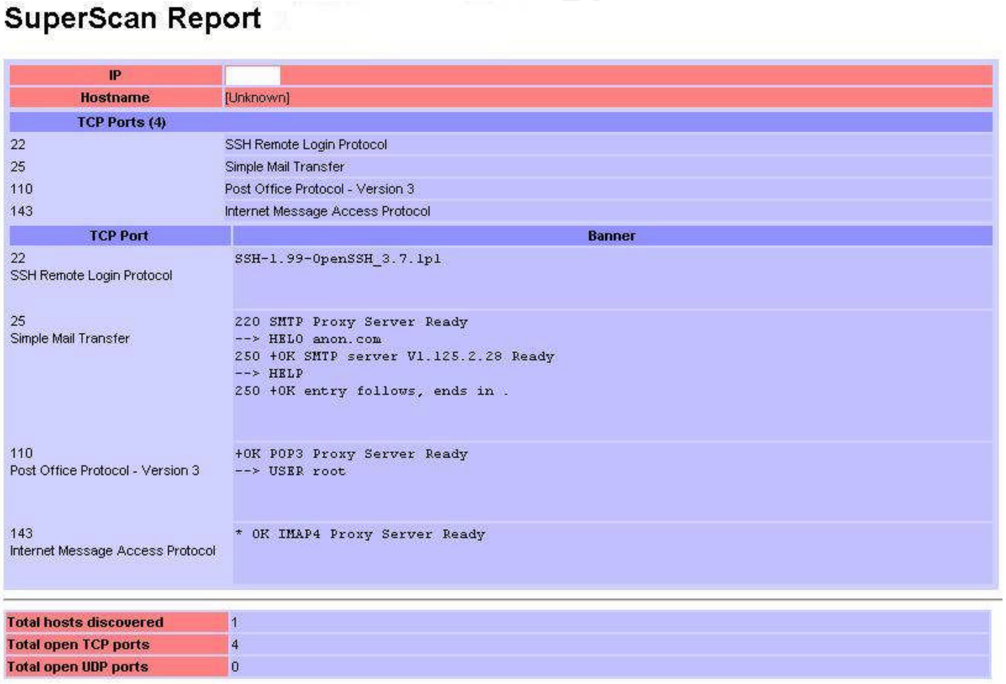
```
Hostname: [Unknown]
TCP ports (4) 22,25,110,143

Total live hosts discovered         1
Total open TCP ports                4
Total open UDP ports                0
```

```
Performing hostname resolution...
Performing banner grabs...
  TCP banner grabbing (4 ports)
  UDP banner grabbing (0 ports)
Reporting scan results...
-------- Scan done --------

Discovery scan finished:
```

00:19 | Saved log file | Live: 1 | TCP open: 4 | UDP open: 0 | 1/1 done

- The scans results show 4 open TCP ports and no open UDP ports.

- The appliance is running SSH 1.99 on port 22.



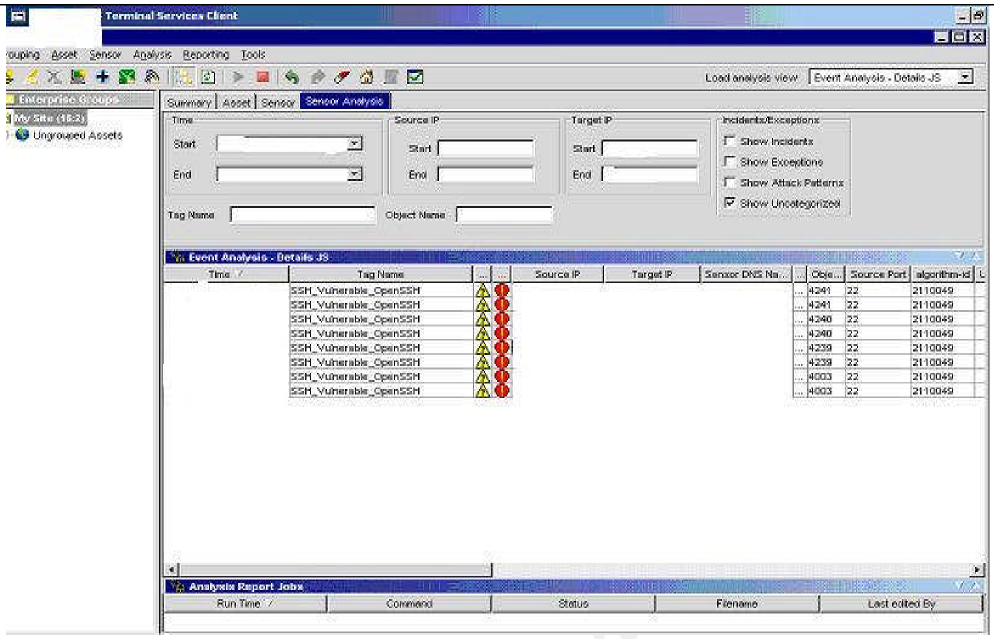
SuperScan Report

IP	[redacted]
Hostname	[Unknown]
TCP Ports (4)	
22	SSH Remote Login Protocol
25	Simple Mail Transfer
110	Post Office Protocol - Version 3
143	Internet Message Access Protocol

TCP Port	Banner
22 SSH Remote Login Protocol	SSH-1.99-OpenSSH_3.7.1p1
25 Simple Mail Transfer	220 SMTP Proxy Server Ready --> HELO anon.com 250 +OK SMTP server V1.125.2.28 Ready --> HELP 250 +OK entry follows, ends in .
110 Post Office Protocol - Version 3	+OK POP3 Proxy Server Ready --> USER root
143 Internet Message Access Protocol	* OK IMAP4 Proxy Server Ready

Total hosts discovered	1
Total open TCP ports	4
Total open UDP ports	0

- In addition to running Superscan, the event logs on the network sensor were monitored to verify the appliance was vulnerable to the SSH protocol it was using. The following screenshot verifies the SSH protocol the appliance is running has a vulnerability.



Load analysis view: Event Analysis - Details JS

□ Show Incidents
□ Show Exceptions
□ Show Attack Patterns
☑ Show Uncategorized

Event Analysis - Details JS

Time	Tag Name	...	...	Source IP	Target IP	Sensor DNS Na...	...	Obje...	Source Port	algorithm-id
	SSH_Vulnerable_OpenSSH	⚠	●				...	4241	22	2110049
	SSH_Vulnerable_OpenSSH	⚠	●				...	4241	22	2110049
	SSH_Vulnerable_OpenSSH	⚠	●				...	4240	22	2110049
	SSH_Vulnerable_OpenSSH	⚠	●				...	4240	22	2110049
	SSH_Vulnerable_OpenSSH	⚠	●				...	4239	22	2110049
	SSH_Vulnerable_OpenSSH	⚠	●				...	4239	22	2110049
	SSH_Vulnerable_OpenSSH	⚠	●				...	4003	22	2110049
	SSH_Vulnerable_OpenSSH	⚠	●				...	4003	22	2110049

Post Test Results/Audit Findings:

- Using an SSH protocol that is vulnerable creates significant risk to company assets.
- Remote connections to the box are not internally monitored and an attacker who successfully exploited the vulnerability could connect to the box via SSH undetected.

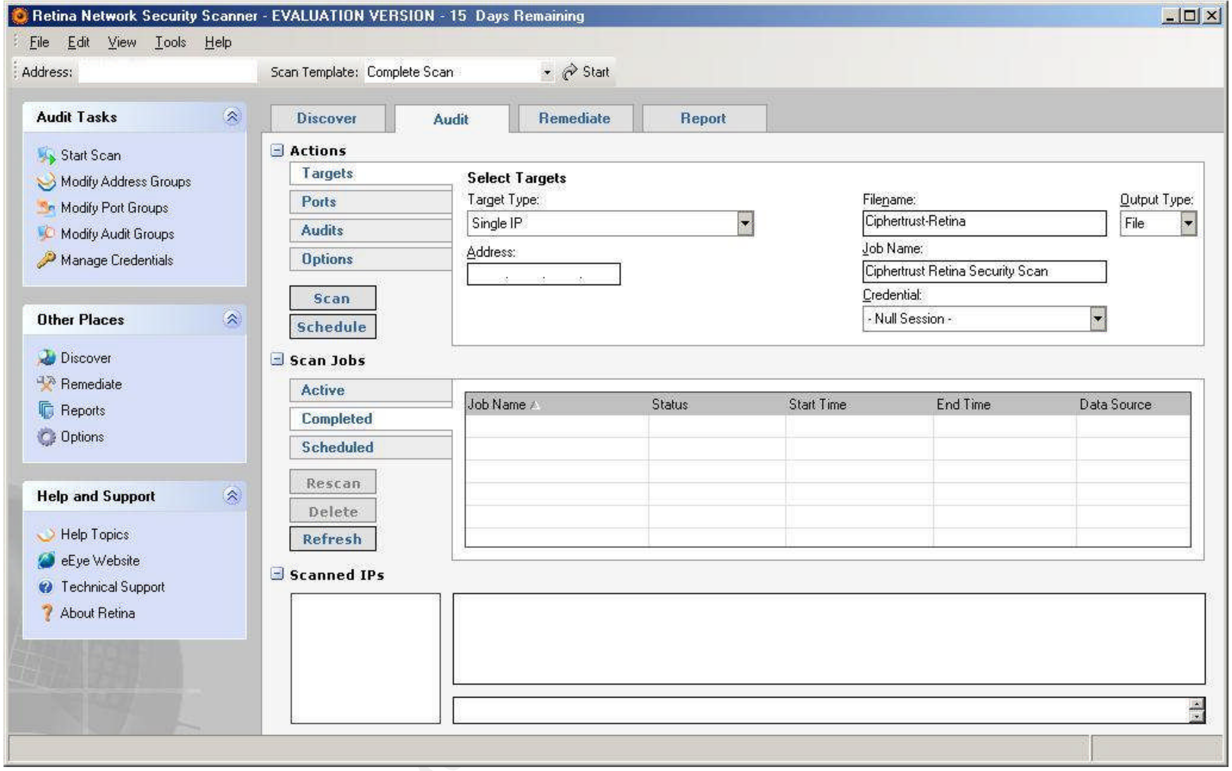
Audit Step 8 – Vulnerability Assessment
Reference: Retina Manual Pg 38/83 “Retina Audit Wizard” http://www.google.com/search?hl=en&ie=UTF-8&q=retina+audit+steps
Control Objective: Using the Retina Security Scanner, ensure there are no unnecessary ports active on the appliance. Retina uses a file, called an RTH that contains information about known security vulnerabilities, to scan the target system. This application performs an automatic web update for the RTH file each time a session is started. The scanner is then able to determine if the system has vulnerabilities and reports the feedback in an HTML report.
Risk: Ports open that are not used make it possible for an attacker to exploit any vulnerability associated with those ports and potentially steal confidential information quarantined on the appliance.
Compliance: As defined in section 1, only ports required to send and receive business related emails should be active and listening.
Testing: 5. Start the Retina Security Scanner. 6. In the select targets area, select the target IP address of the system to scan. 7. On the right side, click “start scan” under audit tasks. 8. Document results.

Objective/Subjective: Objective
This is an objective test. The results from the retina scan will provide information about open and closed ports on the appliance. The scan will also provide remediation steps to ensure the appliance is secure.

Success/Failure: This was a successful test.

Audit Fieldwork:

- Start the Retina Security Scanner



Scan Template: Complete Scan

Target Type: Single IP

Filename: Ciphertrust-Retina

Output Type: File

Job Name: Ciphertrust Retina Security Scan

Credential: - Null Session -

- In the select targets area, select the target IP address of the system to scan.
- On the right side, click "start scan" under audit tasks.

- Results from the Retina Security Scan.

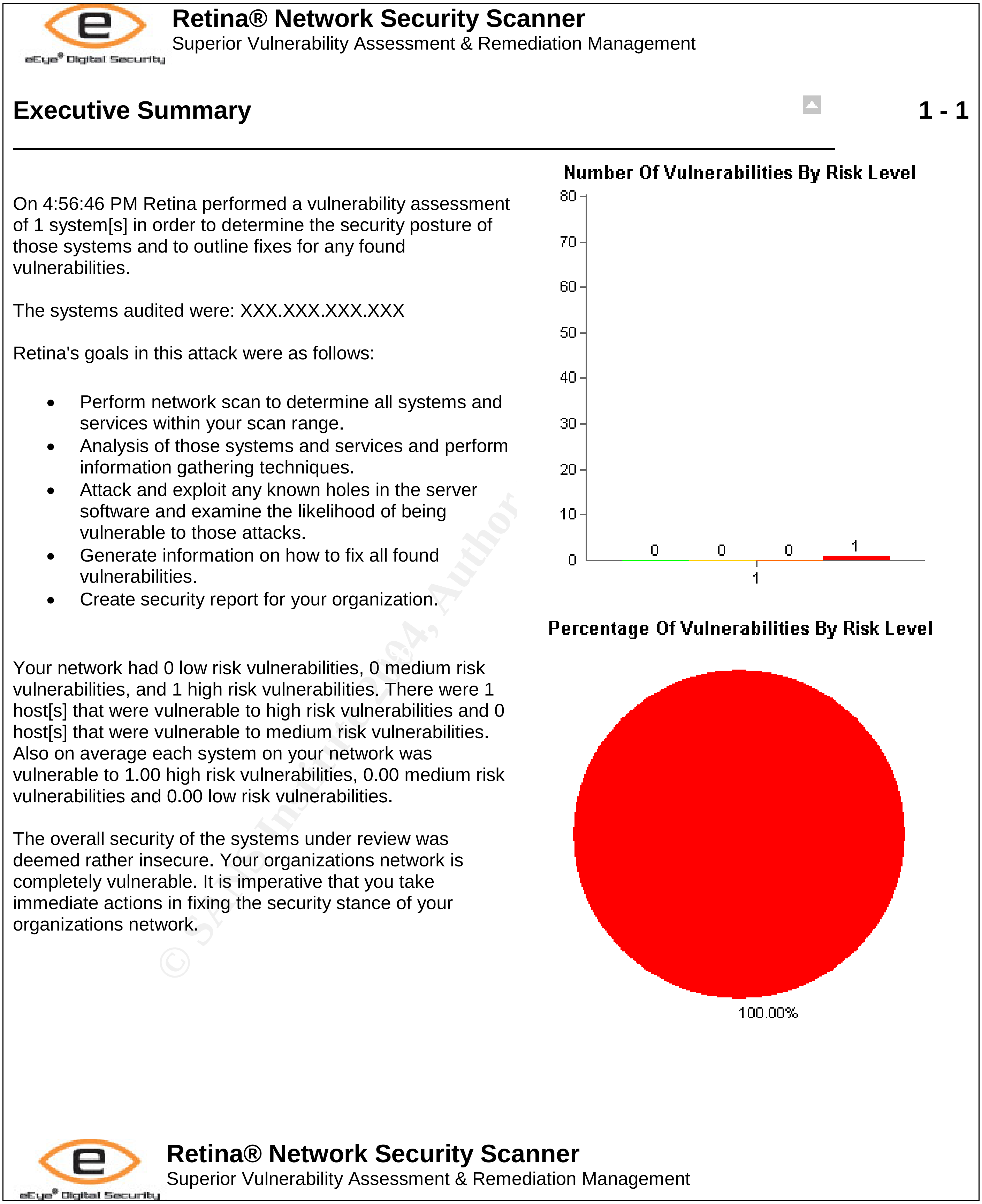
eEye® Digital Security

Retina® Network Security Scanner

Superior Vulnerability Assessment & Remediation Management

Confidential Information

The following report contains confidential information, do not distribute, email, fax or transfer via any electronic mechanism unless it has been approved by our security policy. All copies and backups of this document should be saved on protected storage at all times. Do not share any of the information contained within this report with anyone unless they are authorized to view the information. Violating any of the previous instructions is ground for termination.



Retina® Network Security Scanner

Superior Vulnerability Assessment & Remediation Management

Executive Summary

1 - 1

On 4:56:46 PM Retina performed a vulnerability assessment of 1 system[s] in order to determine the security posture of those systems and to outline fixes for any found vulnerabilities.

The systems audited were: XXX.XXX.XXX.XXX

Retina's goals in this attack were as follows:

- Perform network scan to determine all systems and services within your scan range.
- Analysis of those systems and services and perform information gathering techniques.
- Attack and exploit any known holes in the server software and examine the likelihood of being vulnerable to those attacks.
- Generate information on how to fix all found vulnerabilities.
- Create security report for your organization.

Your network had 0 low risk vulnerabilities, 0 medium risk vulnerabilities, and 1 high risk vulnerabilities. There were 1 host[s] that were vulnerable to high risk vulnerabilities and 0 host[s] that were vulnerable to medium risk vulnerabilities. Also on average each system on your network was vulnerable to 1.00 high risk vulnerabilities, 0.00 medium risk vulnerabilities and 0.00 low risk vulnerabilities.

The overall security of the systems under review was deemed rather insecure. Your organizations network is completely vulnerable. It is imperative that you take immediate actions in fixing the security stance of your organizations network.

Number Of Vulnerabilities By Risk Level

Percentage Of Vulnerabilities By Risk Level

Retina® Network Security Scanner

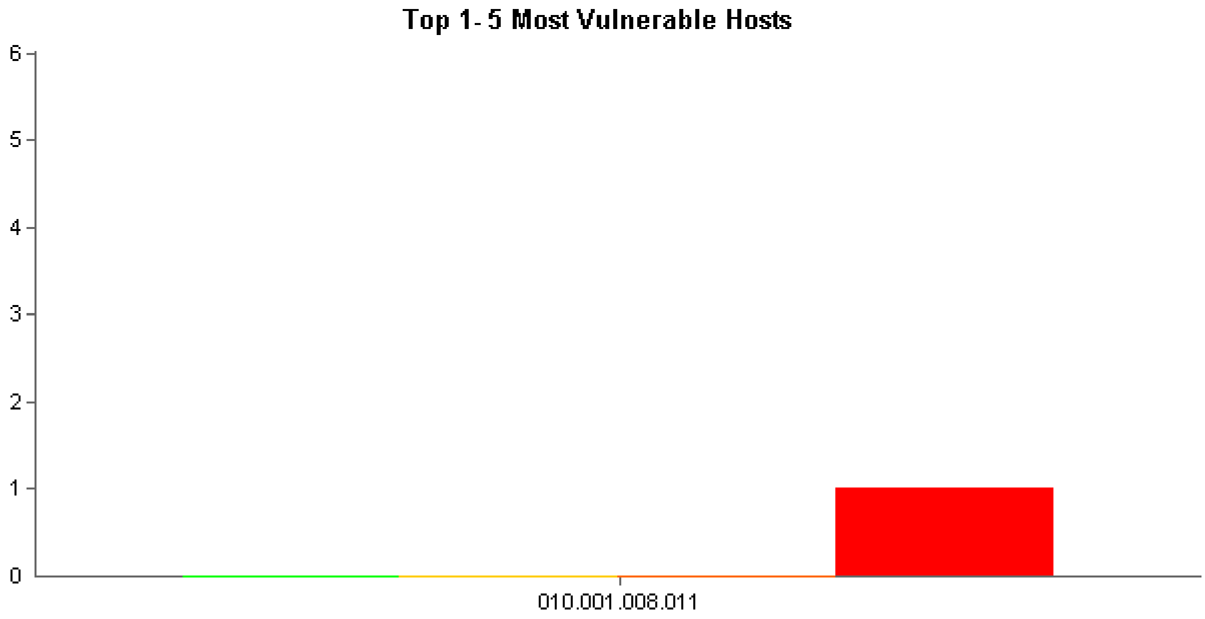
Superior Vulnerability Assessment & Remediation Management

Vulnerability Summary

2 - 1

Introduction

This report was generated on 7/22/2004 9:14:21 AM. Network security scan was performed using the default security policy. Security audits in this report are not conclusive and to be used only as reference, physical security to the network should be examined also. All audits outlined in this report where performed using Retina - The Network Security Scanner, Version 4.9.214



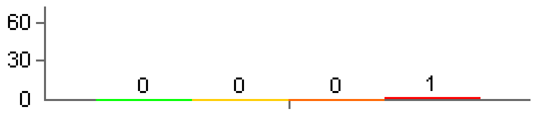
Retina® Network Security Scanner

Superior Vulnerability Assessment & Remediation Management

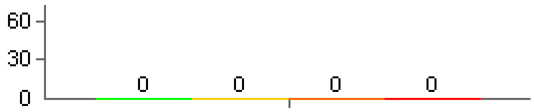
Audits

Audits in Retina the Network Security Scanner are categorized into different sections. The sections are based on the type of services you might be running on your servers and / or workstations.

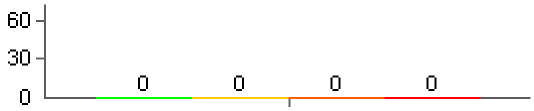
Total Vulnerabilities By Risk Level
The following graph illustrates the total number of vulnerabilities across all machines divided by risk level.

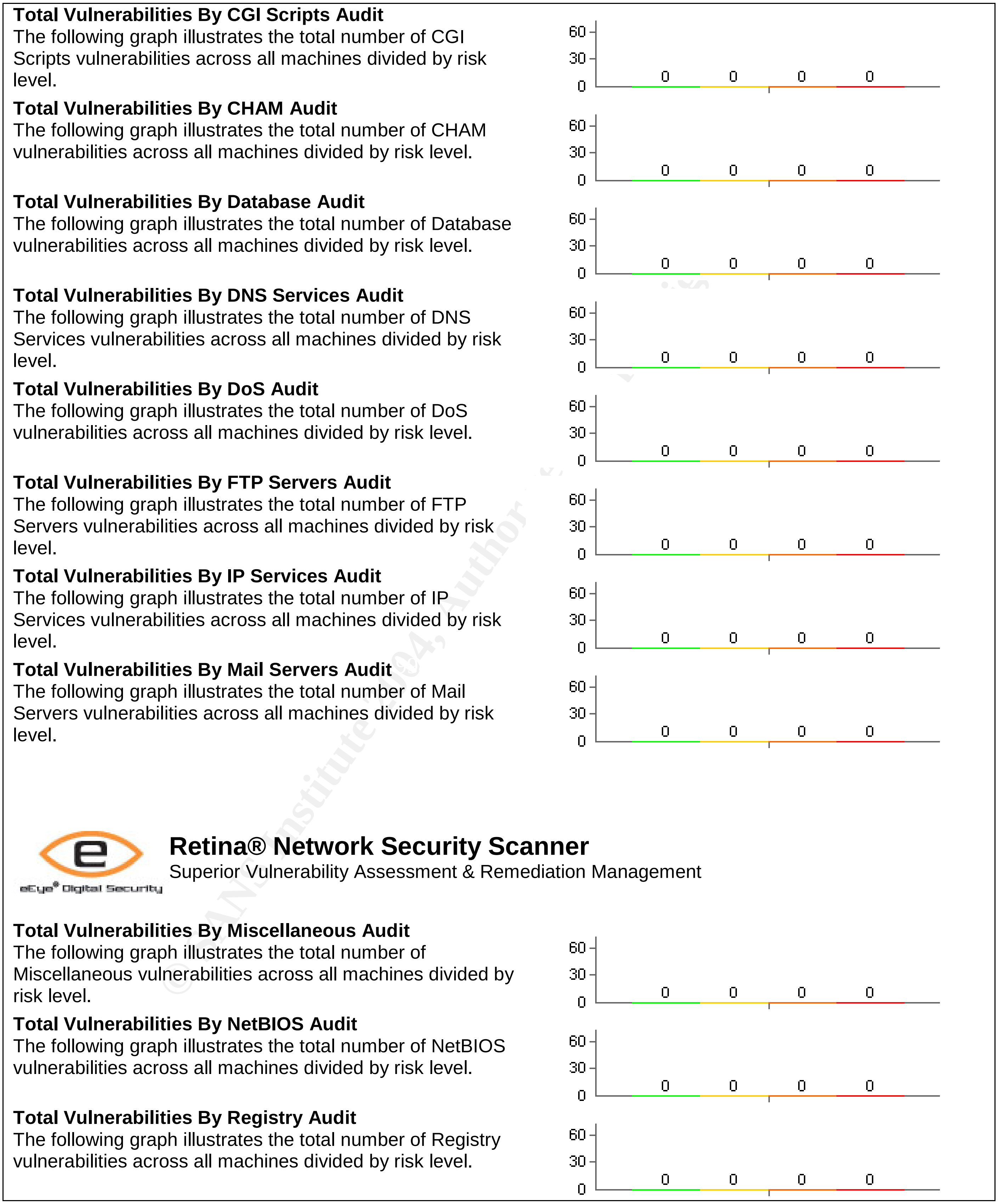


Total Vulnerabilities By Accounts Audit
The following graph illustrates the total number of Accounts vulnerabilities across all machines divided by risk level.



Total Vulnerabilities By Anti-Virus Audit
The following graph illustrates the total number of Anti-Virus vulnerabilities across all machines divided by risk level.





Total Vulnerabilities By CGI Scripts Audit
The following graph illustrates the total number of CGI Scripts vulnerabilities across all machines divided by risk level.

Total Vulnerabilities By CHAM Audit
The following graph illustrates the total number of CHAM vulnerabilities across all machines divided by risk level.

Total Vulnerabilities By Database Audit
The following graph illustrates the total number of Database vulnerabilities across all machines divided by risk level.

Total Vulnerabilities By DNS Services Audit
The following graph illustrates the total number of DNS Services vulnerabilities across all machines divided by risk level.

Total Vulnerabilities By DoS Audit
The following graph illustrates the total number of DoS vulnerabilities across all machines divided by risk level.

Total Vulnerabilities By FTP Servers Audit
The following graph illustrates the total number of FTP Servers vulnerabilities across all machines divided by risk level.

Total Vulnerabilities By IP Services Audit
The following graph illustrates the total number of IP Services vulnerabilities across all machines divided by risk level.

Total Vulnerabilities By Mail Servers Audit
The following graph illustrates the total number of Mail Servers vulnerabilities across all machines divided by risk level.

eEye® Digital Security

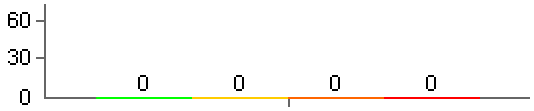
Retina® Network Security Scanner
Superior Vulnerability Assessment & Remediation Management

Total Vulnerabilities By Miscellaneous Audit
The following graph illustrates the total number of Miscellaneous vulnerabilities across all machines divided by risk level.

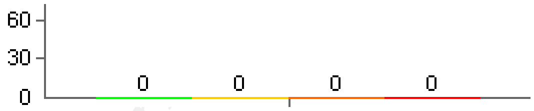
Total Vulnerabilities By NetBIOS Audit
The following graph illustrates the total number of NetBIOS vulnerabilities across all machines divided by risk level.

Total Vulnerabilities By Registry Audit
The following graph illustrates the total number of Registry vulnerabilities across all machines divided by risk level.

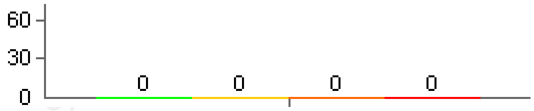
Total Vulnerabilities By Remote Access Audit
The following graph illustrates the total number of Remote Access vulnerabilities across all machines divided by risk level.



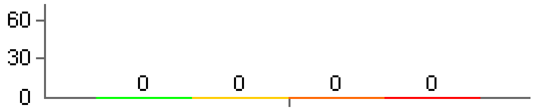
Total Vulnerabilities By Rpc Services Audit
The following graph illustrates the total number of Rpc Services vulnerabilities across all machines divided by risk level.



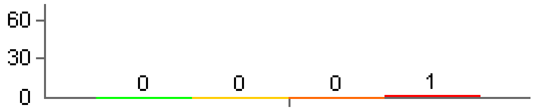
Total Vulnerabilities By Service Control Audit
The following graph illustrates the total number of Service Control vulnerabilities across all machines divided by risk level.



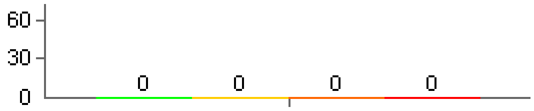
Total Vulnerabilities By SNMP Servers Audit
The following graph illustrates the total number of SNMP Servers vulnerabilities across all machines divided by risk level.



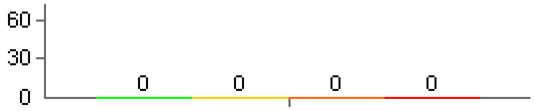
Total Vulnerabilities By SSH Servers Audit
The following graph illustrates the total number of SSH Servers vulnerabilities across all machines divided by risk level.



Total Vulnerabilities By Web Servers Audit
The following graph illustrates the total number of Web Servers vulnerabilities across all machines divided by risk level.



Total Vulnerabilities By Wireless Audit
The following graph illustrates the total number of Wireless vulnerabilities across all machines divided by risk level.



Retina® Network Security Scanner
Superior Vulnerability Assessment & Remediation Management

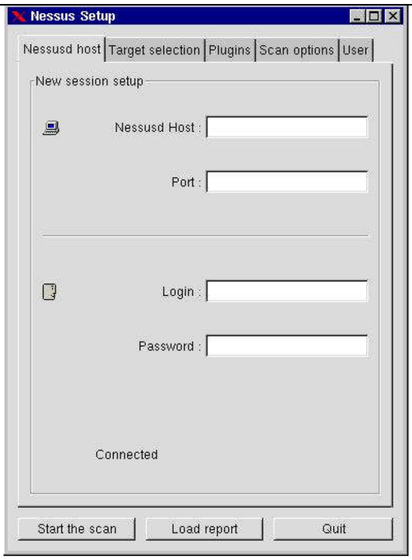
Retina® Network Security Scanner
Superior Vulnerability Assessment & Remediation Management

Address 3 - 1

General:

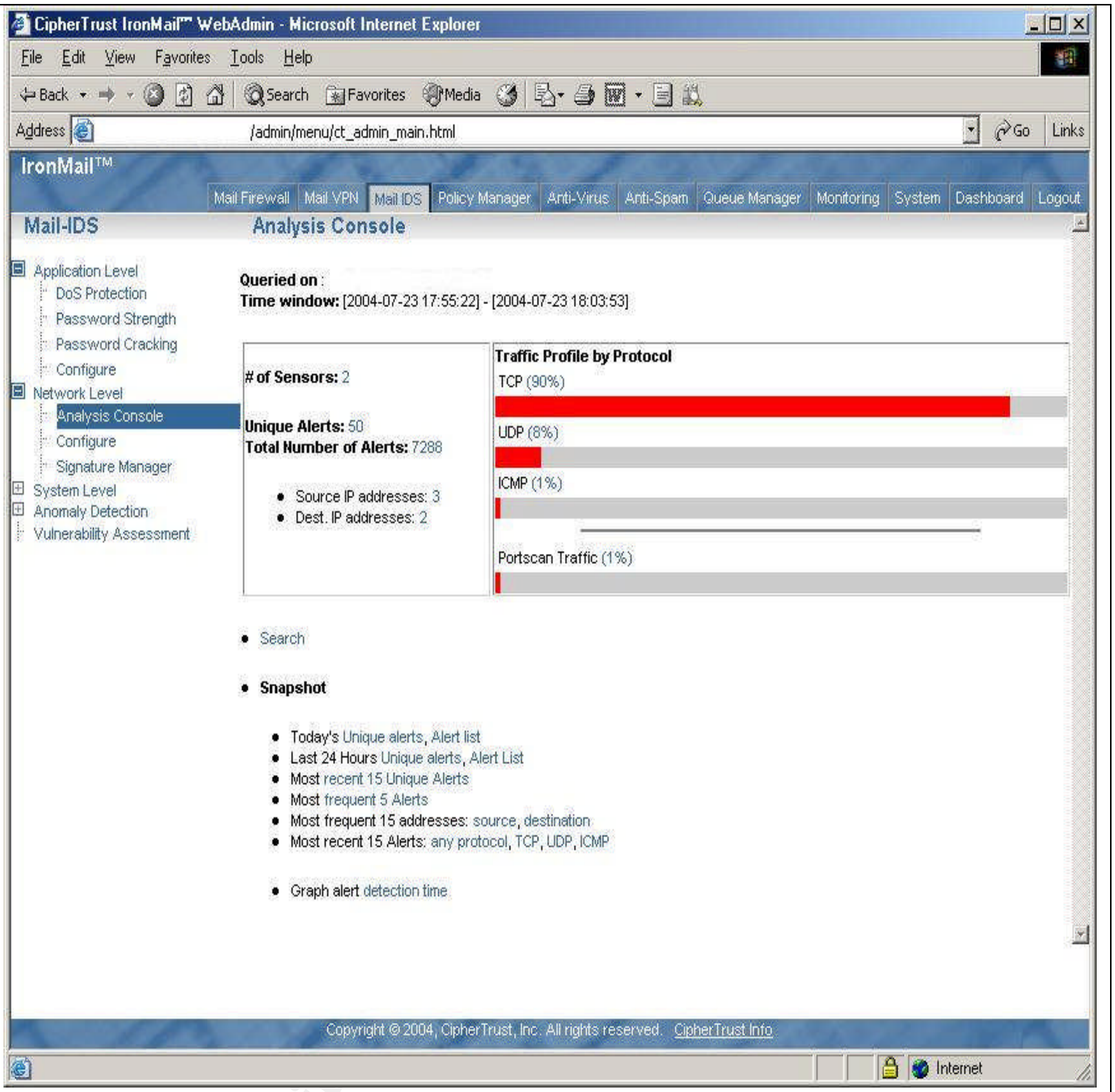
Post Test Results/Audit Findings: ➢ The scan identified 6 open ports; SSH port 22, SMTP port 25, POP3 port 110, IMAP port 143, IMAPS port 993 and POP3S port 995. ➢ The results indicate that the SSH protocol version the appliance is using has multiple vulnerabilities associated with the PAM implementation. ➢ The scan reported 1909 closed ports. ➢ Results show the system is using the FreeBSD 4.5 release for the operating system. No additional information was obtained. This confirms the stripped down version of the OS Ciphertrust has implemented. ➢ All ports that are open are defined in section 1 as required for mail delivery.

Audit Step 9 – Built In IDS System Functionality
Reference: The financial institution's "Defense in Depth" security model. Executive management approved the model and implementation began in September 2002.
Control Objective: Ensure the built-in Intrusion Detection System is functioning properly. Launch a DDoS attack against the appliance and document results.
Risk: A successful attack against a critical network resource going unnoticed could allow enough time for an attacker to steal sensitive information.
Compliance: The appliance should have an alerting system to notify information security that an attack has been attempted.
Testing: 8. Using Nessus, launch an attack against the Ciphertrust appliance. 9. Login to the appliance; select the "Mail IDS" tab. On the left side, select Network Level – Analysis Console. 10. Select the hyperlink number next "Unique Alerts". 11. Determine the most frequent 5 alerts. 12. Provide an example of a DDoS alert. 13. Provide the results from the Nessus scan. 14. Document the results.
Objective/Subjective: Objective This is an objective test. The results from the built-in IDS system will provide information regarding the attack.
Success/Failure: This was a successful test.
Audit Fieldwork: • Start the Nessus application. Insert the Nessus host you want to perform the attack against. Use default selections for other tabs. Include the port on which to make the connection. In this case, the Nessusd and port will not be included for best security practice. Provide the administrator login and password if needed.



- Select start the scan.

- While the scan is running, login to the Ciphertrust appliance and select the "Mail IDS" tab. On the left side, select the Network Level – Analysis Console hyperlink. This provides information about the attack and the percentage for each protocol, TCP, UDP and ICMP.



Queried on :
Time window: [2004-07-23 17:55:22] - [2004-07-23 18:03:53]

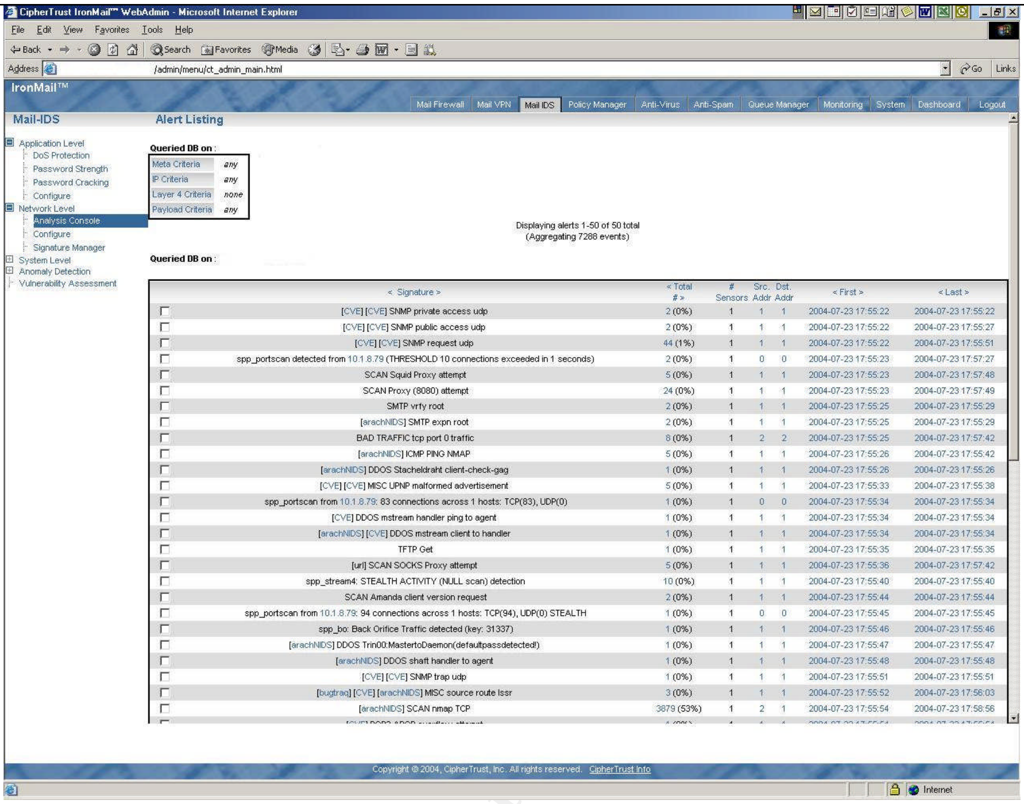
# of Sensors: 2

Unique Alerts: 50
Total Number of Alerts: 7288

- Source IP addresses: 3
- Dest. IP addresses: 2

- Search
- **Snapshot**
  - Today's Unique alerts, Alert list
  - Last 24 Hours Unique alerts, Alert List
  - Most recent 15 Unique Alerts
  - Most frequent 5 Alerts
  - Most frequent 15 addresses: source, destination
  - Most recent 15 Alerts: any protocol, TCP, UDP, ICMP
  - Graph alert detection time

- Next to "Unique Alerts", select the hyperlink number **50**. This area provides information about all the unique attacked defined by the system.



CipherTrust IronMail™ WebAdmin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address /admin/menu/ct_admin_main.html
Go Links
IronMail™
Mail Firewall Mail VPN Mail IDS Policy Manager Anti-Virus Anti-Spam Queue Manager Monitoring System Dashboard Logout
Mail-IDS
Application Level
DoS Protection
Password Strength
Password Cracking
Configure
Network Level
Analysis Console
Configure
Signature Manager
System Level
Anomaly Detection
Vulnerability Assessment
Internet

Alert Listing

Queried DB on :

Meta Criteria	*any*
IP Criteria	*any*
Layer 4 Criteria	*none*
Payload Criteria	*any*

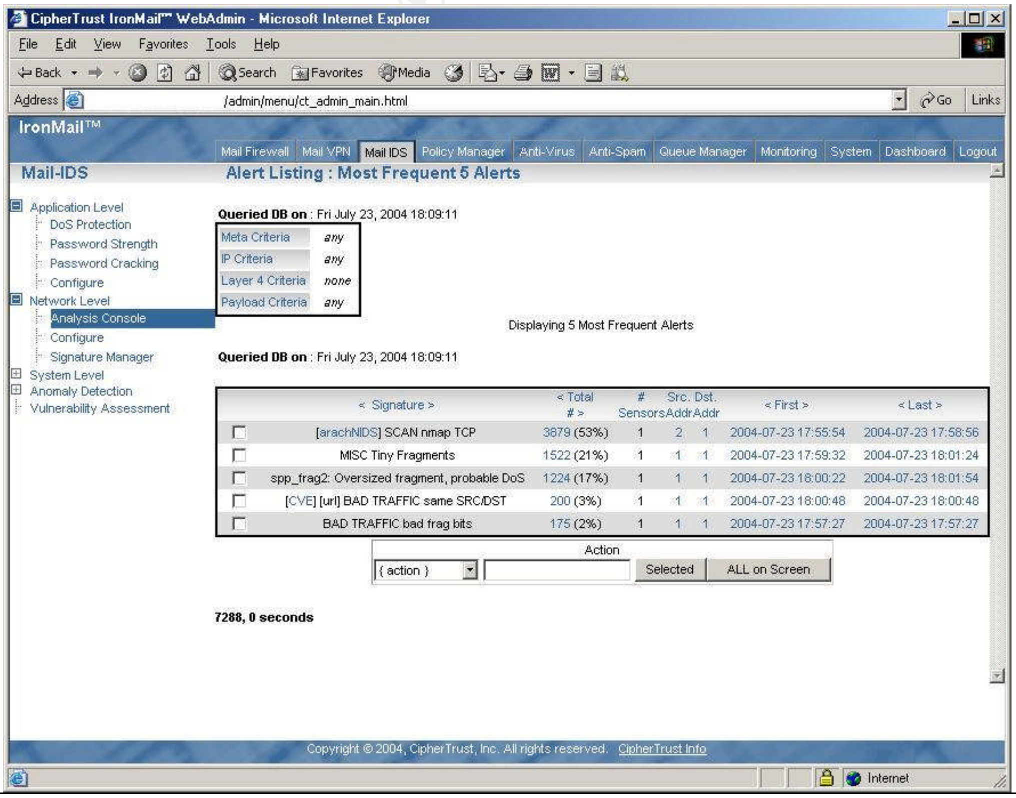
Displaying alerts 1-50 of 50 total
(Aggregating 7288 events)

Queried DB on :

	< Signature >	< Total # >	# Sensors	Src. Addr	Dst. Addr	< First >	< Last >
□	[CVE] [CVE] SNMP private access udp	2 (0%)	1	1	1	2004-07-23 17:55:22	2004-07-23 17:55:22
□	[CVE] [CVE] SNMP public access udp	2 (0%)	1	1	1	2004-07-23 17:55:22	2004-07-23 17:55:27
□	[CVE] [CVE] SNMP request udp	44 (1%)	1	1	1	2004-07-23 17:55:22	2004-07-23 17:55:51
□	spp_portscan detected from 10.1.8.79 (THRESHOLD 10 connections exceeded in 1 seconds)	2 (0%)	1	0	0	2004-07-23 17:55:23	2004-07-23 17:57:27
□	SCAN Squid Proxy attempt	5 (0%)	1	1	1	2004-07-23 17:55:23	2004-07-23 17:57:48
□	SCAN Proxy (8080) attempt	24 (0%)	1	1	1	2004-07-23 17:55:23	2004-07-23 17:57:49
□	SMTP vrfy root	2 (0%)	1	1	1	2004-07-23 17:55:25	2004-07-23 17:55:29
□	[arachNIDS] SMTP expn root	2 (0%)	1	1	1	2004-07-23 17:55:25	2004-07-23 17:55:29
□	BAD TRAFFIC tcp port 0 traffic	8 (0%)	1	2	2	2004-07-23 17:55:25	2004-07-23 17:57:42
□	[arachNIDS] ICMP PING NMAP	5 (0%)	1	1	1	2004-07-23 17:55:26	2004-07-23 17:55:42
□	[arachNIDS] DDOS Stacheldraht client-check-gag	1 (0%)	1	1	1	2004-07-23 17:55:26	2004-07-23 17:55:26
□	[CVE] [CVE] MISC UPNP malformed advertisement	5 (0%)	1	1	1	2004-07-23 17:55:33	2004-07-23 17:55:38
□	spp_portscan from 10.1.8.79: 83 connections across 1 hosts: TCP(83), UDP(0)	1 (0%)	1	0	0	2004-07-23 17:55:34	2004-07-23 17:55:34
□	[CVE] DDOS mstream handler ping to agent	1 (0%)	1	1	1	2004-07-23 17:55:34	2004-07-23 17:55:34
□	[arachNIDS] [CVE] DDOS mstream client to handler	1 (0%)	1	1	1	2004-07-23 17:55:34	2004-07-23 17:55:34
□	TFTP Get	1 (0%)	1	1	1	2004-07-23 17:55:35	2004-07-23 17:55:35
□	[url] SCAN SOCKS Proxy attempt	5 (0%)	1	1	1	2004-07-23 17:55:36	2004-07-23 17:57:42
□	spp_stream4: STEALTH ACTIVITY (NULL scan) detection	10 (0%)	1	1	1	2004-07-23 17:55:40	2004-07-23 17:55:40
□	SCAN Amanda client version request	2 (0%)	1	1	1	2004-07-23 17:55:44	2004-07-23 17:55:44
□	spp_portscan from 10.1.8.79: 94 connections across 1 hosts: TCP(94), UDP(0) STEALTH	1 (0%)	1	0	0	2004-07-23 17:55:45	2004-07-23 17:55:45
□	spp_bo: Back Orifice Traffic detected (key: 31337)	1 (0%)	1	1	1	2004-07-23 17:55:46	2004-07-23 17:55:46
□	[arachNIDS] DDOS Trin00:MastertoDaemon(defaultpassdetected!)	1 (0%)	1	1	1	2004-07-23 17:55:47	2004-07-23 17:55:47
□	[arachNIDS] DDOS shaft handler to agent	1 (0%)	1	1	1	2004-07-23 17:55:48	2004-07-23 17:55:48
□	[CVE] [CVE] SNMP trap udp	1 (0%)	1	1	1	2004-07-23 17:55:51	2004-07-23 17:55:51
□	[bugtraq] [CVE] [arachNIDS] MISC source route lssr	3 (0%)	1	1	1	2004-07-23 17:55:52	2004-07-23 17:56:03
□	[arachNIDS] SCAN nmap TCP	3879 (53%)	1	2	1	2004-07-23 17:55:54	2004-07-23 17:58:56

Copyright © 2004, CipherTrust, Inc. All rights reserved. CipherTrust Info

- List the 5 most frequent alerts generated by the system.



CipherTrust IronMail™ WebAdmin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address /admin/menu/ct_admin_main.html
Go Links
IronMail™
Mail Firewall Mail VPN Mail IDS Policy Manager Anti-Virus Anti-Spam Queue Manager Monitoring System Dashboard Logout
Mail-IDS
Application Level
DoS Protection
Password Strength
Password Cracking
Configure
Network Level
Analysis Console
Configure
Signature Manager
System Level
Anomaly Detection
Vulnerability Assessment
Internet

Alert Listing : Most Frequent 5 Alerts

Queried DB on : Fri July 23, 2004 18:09:11

Meta Criteria	*any*
IP Criteria	*any*
Layer 4 Criteria	*none*
Payload Criteria	*any*

Displaying 5 Most Frequent Alerts

Queried DB on : Fri July 23, 2004 18:09:11

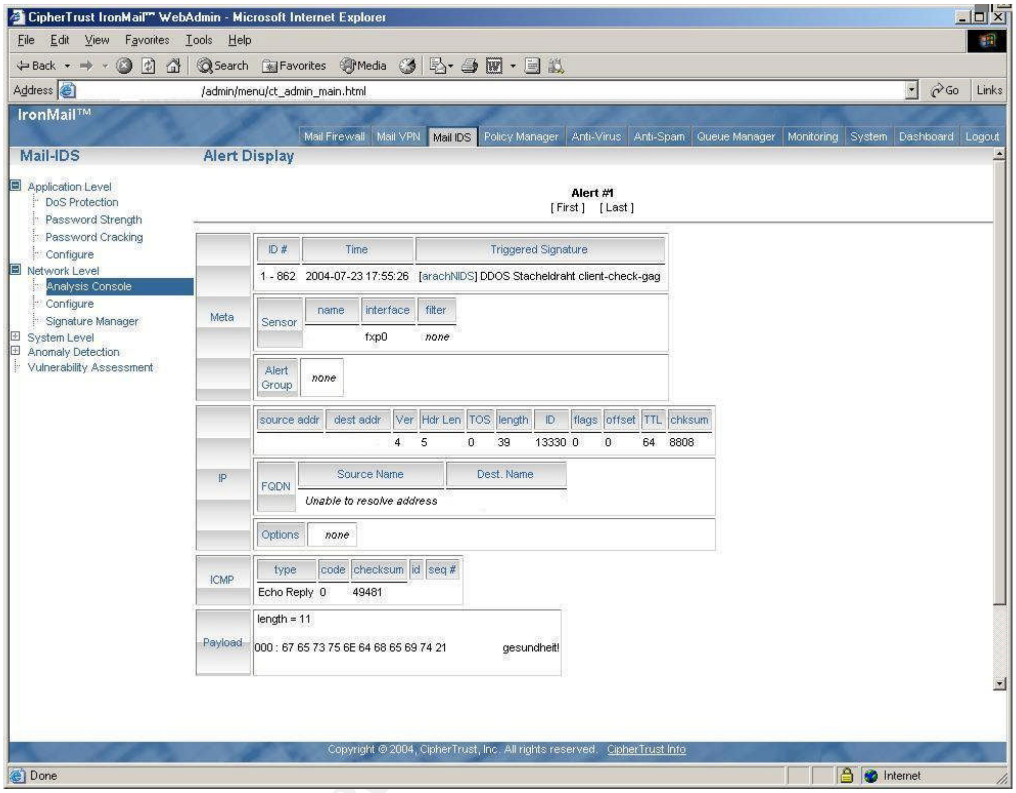
	< Signature >	< Total # >	# Sensors	Src. Addr	Dst. Addr	< First >	< Last >
□	[arachNIDS] SCAN nmap TCP	3879 (53%)	1	2	1	2004-07-23 17:55:54	2004-07-23 17:58:56
□	MISC Tiny Fragments	1522 (21%)	1	1	1	2004-07-23 17:59:32	2004-07-23 18:01:24
□	spp_frag2: Oversized fragment, probable DoS	1224 (17%)	1	1	1	2004-07-23 18:00:22	2004-07-23 18:01:54
□	[CVE] [url] BAD TRAFFIC same SRC/DST	200 (3%)	1	1	1	2004-07-23 18:00:48	2004-07-23 18:00:48
□	BAD TRAFFIC bad frag bits	175 (2%)	1	1	1	2004-07-23 17:57:27	2004-07-23 17:57:27

Action
{ action } | Selected | ALL on Screen

7288, 0 seconds

Copyright © 2004, CipherTrust, Inc. All rights reserved. CipherTrust Info

- Provide an example of an attempt for a distributed denial of service, or DDoS attack. Signatures will trigger these attack alerts if attempts are made on the box. The system is configured to automatically update attack signatures on a daily basis.



Alert Display

Alert #1
[First] [Last]

Meta

ID #	Time	Triggered Signature
1 - 862	2004-07-23 17:55:26	[arachNIDS] DDOS Stacheldraht client-check-gag

Sensor	name	interface	filter
		fxp0	*none*

Alert Group	*none*

IP

source addr	dest addr	Ver	Hdr Len	TOS	length	ID	flags	offset	TTL	chksum
		4	5	0	39	13330	0	0	64	8808

FQDN	Source Name	Dest. Name
	Unable to resolve address	

Options	*none*

ICMP

type	code	checksum	id	seq #
Echo Reply	0	49481		

Payload

```
length = 11

000 : 67 65 73 75 6E 64 68 65 69 74 21          gesundheit!
```

- Provide the Nessus scan results.

Nessus Scan Report

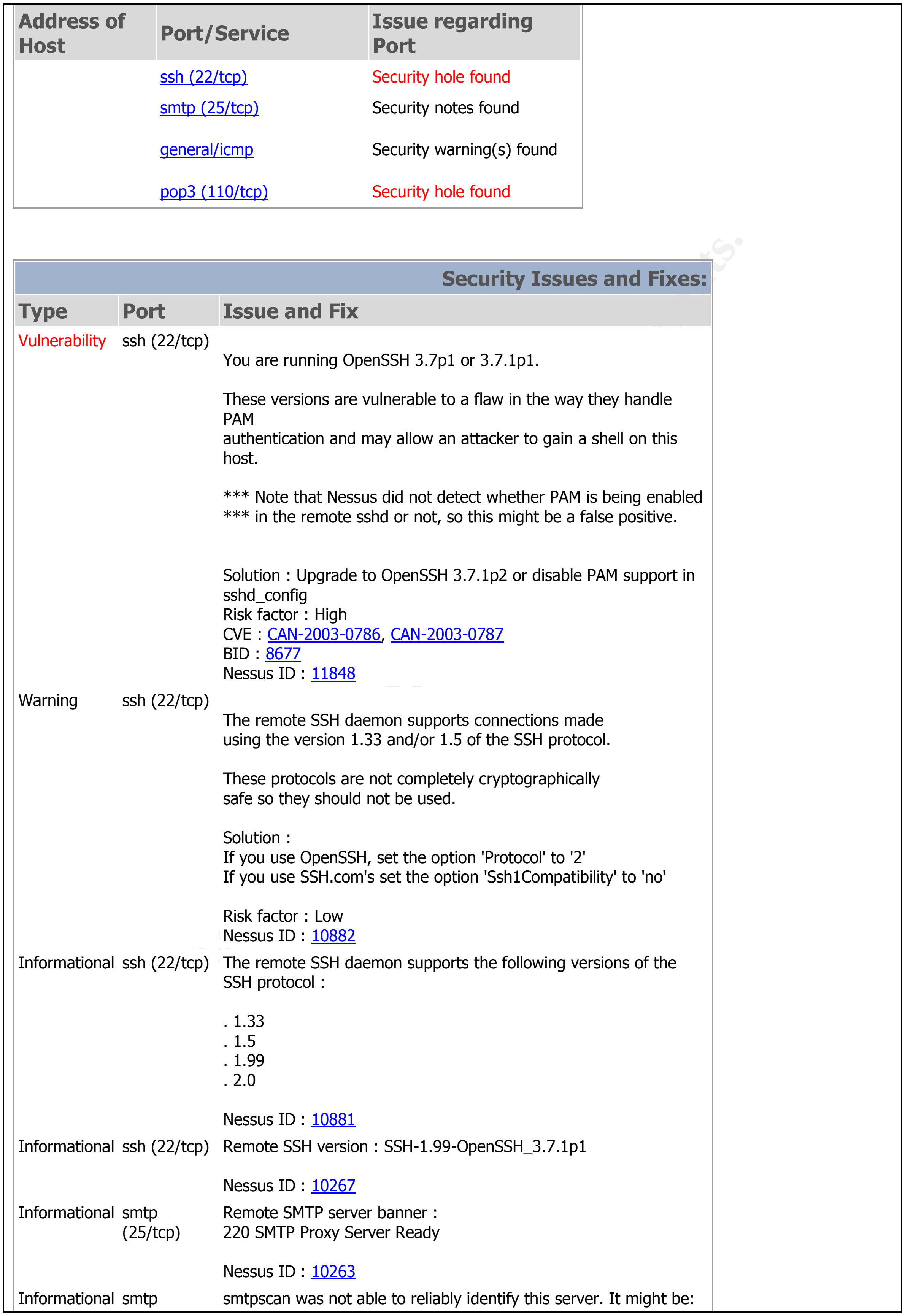
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details	
Hosts which were alive and responding during test	1
Number of security holes found	3
Number of security warnings found	2

Host List

Host(s)	Possible Issue
	Security hole(s) found

Analysis of Host



Address of Host	Port/Service	Issue regarding Port
	ssh (22/tcp)	Security hole found
	smtp (25/tcp)	Security notes found
	general/icmp	Security warning(s) found
	pop3 (110/tcp)	Security hole found

Security Issues and Fixes:

Type	Port	Issue and Fix
Vulnerability	ssh (22/tcp)	You are running OpenSSH 3.7p1 or 3.7.1p1. These versions are vulnerable to a flaw in the way they handle PAM authentication and may allow an attacker to gain a shell on this host. *** Note that Nessus did not detect whether PAM is being enabled *** in the remote sshd or not, so this might be a false positive. Solution : Upgrade to OpenSSH 3.7.1p2 or disable PAM support in sshd_config Risk factor : High CVE : CAN-2003-0786, CAN-2003-0787 BID : 8677 Nessus ID : 11848
Warning	ssh (22/tcp)	The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol. These protocols are not completely cryptographically safe so they should not be used. Solution : If you use OpenSSH, set the option 'Protocol' to '2' If you use SSH.com's set the option 'Ssh1Compatibility' to 'no' Risk factor : Low Nessus ID : 10882
Informational	ssh (22/tcp)	The remote SSH daemon supports the following versions of the SSH protocol : . 1.33 . 1.5 . 1.99 . 2.0 Nessus ID : 10881
Informational	ssh (22/tcp)	Remote SSH version : SSH-1.99-OpenSSH_3.7.1p1 Nessus ID : 10267
Informational	smtp (25/tcp)	Remote SMTP server banner : 220 SMTP Proxy Server Ready Nessus ID : 10263
Informational	smtp	smtpscan was not able to reliably identify this server. It might be:

	(25/tcp)	MDaemon 6.5.2 -20- Sendmail 8.11.6/8.11.6 -286- Sendmail 8.9.1/8.9.1 -37- Sendmail 8.10.2/8.10.2 -248- Sendmail 8.11.6/8.11.6 -227- XMail 1.12 (Win32/Ix86) iMate Mail Server 5.0.0 Lotus SMTP MTA Service Sendmail 8.9.1/8.9.1 -70- MailSite ESMTP Receiver Version 4.5.6.7 Sendmail 8.10.2/8.10.2 -30- Sendmail 8.10.2/8.10.2 -332- eXtremail V1.2 release 2 VopMail Version 5.3.232.0 eXtremail V1.5 release 5 USA.NET-SMTA vC8.MAIN.1.11G MDaemon 6.5.0 Sendmail 8.10.2/8.10.2 -518- Sendmail 8.10.2/8.10.2 -520- WinRoute Pro 4.2.0 Kerio MailServer 5.5.1 Sendmail 8.10.2/8.10.2 -89- Sendmail 8.10.2/8.10.2 -451- Merak 5.5.7 VopMail Version 5.3.232.0 Merak 5.5.7 Sendmail 8.12.9/8.12.8 Sendmail 8.9.1/8.9.1 -86- XMail 1.10 MDaemon 6.5.2 Merak 5.5.5 The fingerprint differs from these known signatures on 5 point(s) If you known precisely what it is, please send this fingerprint to smtp-signatures@nessus.org : :503:501:500:250:250:250:550:250:500:500:500:250:250:250:250 Nessus ID : 11421	
Informational	smtp (25/tcp)	For some reason, we could not send the 42.zip file to this MTA BID : 3027 Nessus ID : 11036	
Warning	general/icmp	 The remote host answers to an ICMP timestamp request. This allows an attacker to know the date, which is set on your machine. This may help him to defeat all your time based authentication protocols. Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). Risk factor : Low CVE : CAN-1999-0524 Nessus ID : 10114	
Vulnerability	pop3 (110/tcp)	 The remote POP3 server might be vulnerable to a buffer overflow bug when it is issued at least one of these commands, with a too long argument : auth user pass	

		If confirmed, this problem might allow an attacker to execute arbitrary code on the remote system, thus giving him an interactive session on this host. Solution : If you do not use POP3, disable this service in /etc/inetd.conf and restart the inetd process. Otherwise, upgrade to a newer version. See also : http://online.securityfocus.com/archive/1/27197 Risk factor : High CVE : CAN-2002-0799, CVE-1999-0822 BID : 789, 790, 830, 894, 942, 1965, 2781, 2811, 4055, 4295, 4614 Nessus ID : 10184
Vulnerability	pop3 (110/tcp)	The remote pop3 server is vulnerable to the following buffer overflow : USER test PASS <buffer> This *may* allow an attacker to execute arbitrary commands as root on the remote POP3 server. Solution : contact your vendor, inform it of this vulnerability, and ask for a patch Risk factor : High CVE : CAN-1999-1511 BID : 791 Nessus ID : 10325

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

Post Test Results/Audit Findings:

- There were a total of 7288 alerts generated in approximately 11 minutes and 38 seconds.
- A total of 3 vulnerabilities were found by the Nessus scan. One vulnerability was in the SSH protocol the appliance is using. Two vulnerabilities were found for the remote pop3 server. The links to fixes for the findings are provided in the Nessus report.

Audit Step 11 – Displayed Warning Banner
Reference: Novoblisky, Kimberly M. "Audit of an SSL VPN; Secure remote email solution for a financial institution" http://www.giac.org/practical/GSNA/Kimberly_Novoblisky_GSNA.pdf
Control Objective: Determine if a warning banner is displayed before access to the logon screen is granted.
Risk: Lawsuits are always supported with documented evidence. Without a warning banner informing potential attackers that un-authorized access to the system is prohibited, there is only substantial evidence to provide in the event a lawsuit is brought against the financial institution. On port 143, the IMAP protocol has a banner that

usually contains information about the appliance. This should also be changed and a warning banner be implemented.

Compliance: Corporate issued warning banner should be displayed before a user is able to access the logon screen informing the user that the system is for authorized use only.

Testing:

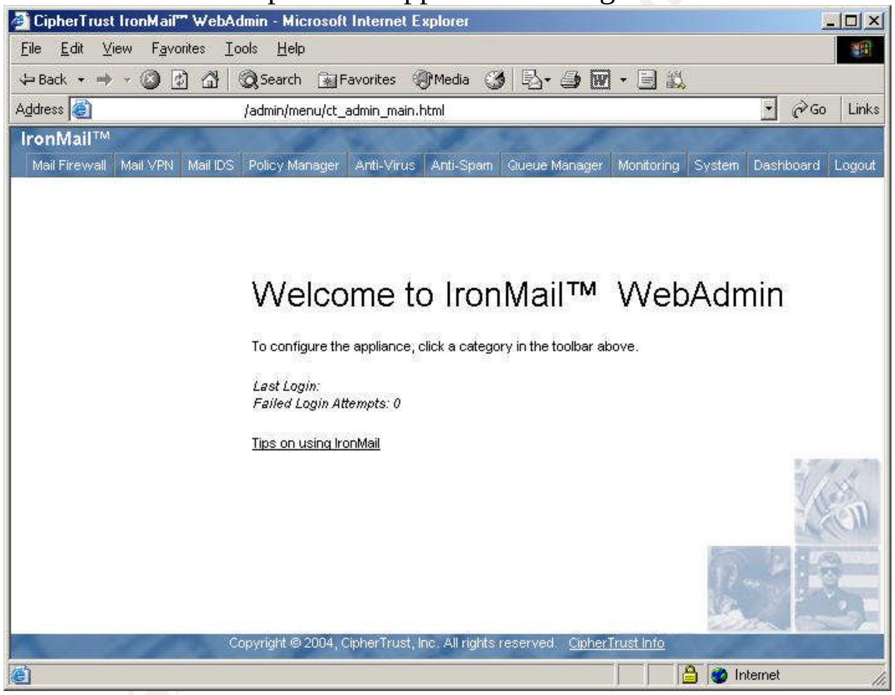
5. Initiate a browsing session to the Ciphertrust appliance.
6. Determine if the warning banner is displayed.
7. Start a SuperScan session with the target IP address.
8. Document results of the scan.

Objective/Subjective: Objective
This is an objective test. The screen shots and the Superscan results will provide evidence of banners currently displayed on the appliance.

Success/Failure: This test failed.

Audit Fieldwork:

- Browse to the Ciphertrust appliance and login.


CipherTrust IronMail™ WebAdmin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address /admin/menu/ct_admin_main.html Go Links
IronMail™
Mail Firewall Mail VPN Mail IDS Policy Manager Anti-Virus Anti-Spam Queue Manager Monitoring System Dashboard Logout
Internet

Welcome to IronMail™ WebAdmin

To configure the appliance, click a category in the toolbar above.

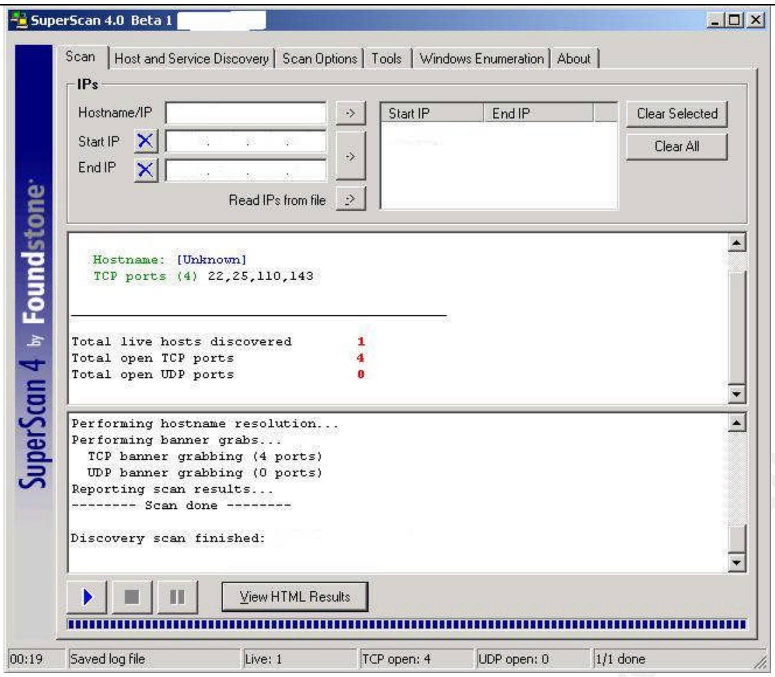
Last Login:
Failed Login Attempts: 0

Tips on using IronMail

Copyright © 2004, CipherTrust, Inc. All rights reserved. CipherTrust Info

- There appeared to be no warning banner displayed before logging into the appliance.

- Start a SuperScan session. Plug the IP address in the Hostname/IP, Start IP and End IP target window.

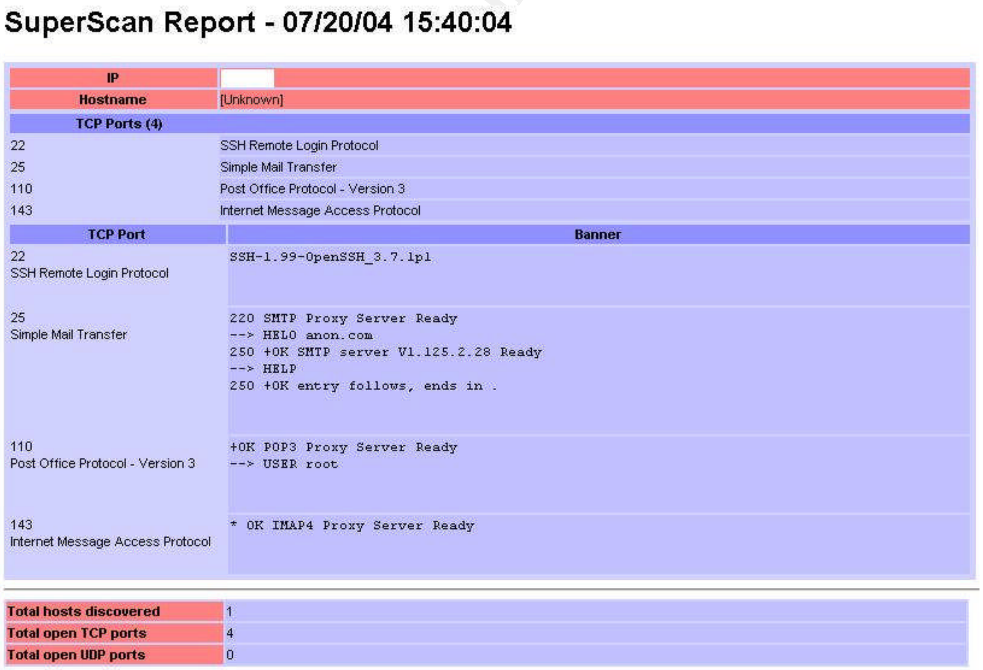


```
Hostname: [Unknown]
TCP ports (4) 22,25,110,143

Total live hosts discovered      1
Total open TCP ports             4
Total open UDP ports             0
```

```
Performing hostname resolution...
Performing banner grabs...
  TCP banner grabbing (4 ports)
  UDP banner grabbing (0 ports)
Reporting scan results...
-------- Scan done --------

Discovery scan finished:
```

00:19 | Saved log file | Live: 1 | TCP open: 4 | UDP open: 0 | 1/1 done

- Provide the Superscan results.



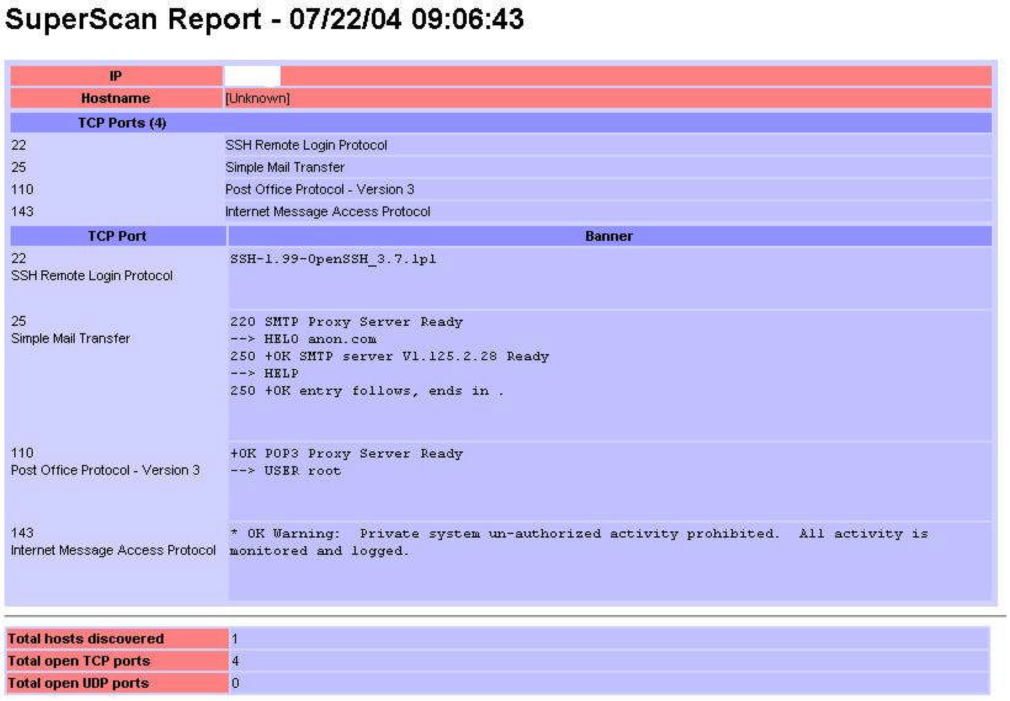
SuperScan Report - 07/20/04 15:40:04

IP	[redacted]
Hostname	[Unknown]
TCP Ports (4)	
22	SSH Remote Login Protocol
25	Simple Mail Transfer
110	Post Office Protocol - Version 3
143	Internet Message Access Protocol

TCP Port	Banner
22 SSH Remote Login Protocol	SSH-1.99-OpenSSH_3.7.1p1
25 Simple Mail Transfer	220 SMTP Proxy Server Ready --> HELO anon.com 250 +OK SMTP server V1.125.2.28 Ready --> HELP 250 +OK entry follows, ends in .
110 Post Office Protocol - Version 3	+OK POP3 Proxy Server Ready --> USER root
143 Internet Message Access Protocol	* OK IMAP4 Proxy Server Ready

Total hosts discovered	1
Total open TCP ports	4
Total open UDP ports	0

- Under TCP port, port 143 provides sensitive information.
- As part of the remediation process, the IMAP banner has been changed and is illustrated in the following screen shot.



SuperScan Report - 07/22/04 09:06:43

IP	[redacted]
Hostname	[Unknown]
TCP Ports (4)	
22	SSH Remote Login Protocol
25	Simple Mail Transfer
110	Post Office Protocol - Version 3
143	Internet Message Access Protocol

TCP Port	Banner
22 SSH Remote Login Protocol	SSH-1.99-OpenSSH_3.7.1p1
25 Simple Mail Transfer	220 SMTP Proxy Server Ready --> HELO anon.com 250 +OK SMTP server V1.125.2.28 Ready --> HELP 250 +OK entry follows, ends in .
110 Post Office Protocol - Version 3	+OK POP3 Proxy Server Ready --> USER root
143 Internet Message Access Protocol	* OK Warning: Private system un-authorized activity prohibited. All activity is monitored and logged.

Total hosts discovered	1
Total open TCP ports	4
Total open UDP ports	0

Post Test Results/Audit Findings:

- A warning banner should be displayed before any user is allowed to login to the appliance.
- The IMAP banner has been changed to read "OK Warning: Private system un-authorized activity prohibited. All activity is monitored and logged."

Audit Step 12 – International Domains

Reference: The financial institution's "Defense in Depth" security model. Executive management approved the model and implementation began in September 2002.

Control Objective: Ensure the Ciphertrust appliance blocks all international domains that are not used for daily business activity.

Risk: Spammers and virus writers are operating all over the world. If international domains are not blocked, this provides yet another avenue for an international attacker to compromise a network resource. By implementing as many mitigating factors as possible, it reduces the risk of a system compromise.

Compliance: All international domains not used on a daily basis should be blocked before emails from those domains reach the policy scan process.

Testing:

4. Provide a list of all domains blocked by the appliance.
5. Provide a list of "accepted" domains.
6. Include instructions on how to setup the rule to block a domain.

Objective/Subjective: Objective

This is an objective test. Screen shots will provide evidence of the blocked international domains.

Success/Failure: This was a successful test.

Audit Fieldwork:

- List all blocked domains.

Blocked International Domains
Information Security - Corp Tech
Financial Institution

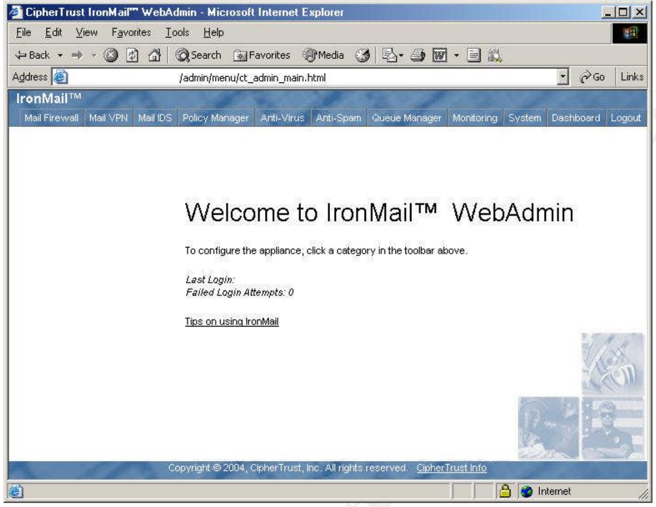
*.ac	*.cy	*.is	*.ne	*.td
*.ad	*.dj	*.je	*.nf	*.tf
*.ae	*.dk	*.jm	*.ng	*.tg
*.af	*.dm	*.jo	*.ni	*.th
*.ag	*.do	*.jp	*.nl	*.tj
*.ai	*.dz	*.ke	*.no	*.tk
*.al	*.ec	*.kg	*.np	*.tm
*.am	*.ee	*.kh	*.nr	*.tn
*.an	*.eg	*.ki	*.nu	*.to
*.ao	*.eh	*.km	*.nz	*.tp
*.aq	*.er	*.kn	*.om	*.tr
*.ar	*.es	*.kp	*.pa	*.tt
*.as	*.et	*.kr	*.pe	*.tw
*.at	*.fi	*.kw	*.pf	*.tz
*.aw	*.fj	*.ky	*.pg	*.ua
*.az	*.fk	*.kz	*.ph	*.ug
*.ba	*.fm	*.la	*.pk	*.uk
*.bb	*.fo	*.lb	*.pl	*.um
*.bd	*.ga	*.lc	*.pm	*.uy
*.be	*.gd	*.li	*.pn	*.uz
*.bf	*.ge	*.lk	*.pr	*.va
*.bg	*.gf	*.lr	*.ps	*.vc
*.bh	*.gg	*.ls	*.pt	*.ve
*.bi	*.gh	*.lt	*.pw	*.vg
*.bj	*.gi	*.lu	*.py	*.vi
*.bm	*.gl	*.lv	*.qa	*.vn
*.bn	*.gm	*.ly	*.re	*.vu
*.bo	*.gn	*.ma	*.ro	*.wf
*.br	*.gp	*.mc	*.ru	*.ws
*.bs	*.gq	*.md	*.rw	*.ye
*.bt	*.gr	*.mg	*.sa	*.yt
*.bv	*.gs	*.mh	*.sb	*.yu
*.bw	*.gt	*.mk	*.sc	*.za
*.by	*.gu	*.ml	*.sd	*.zm
*.bz	*.gw	*.mm	*.se	*.zw
*.cd	*.gy	*.mn	*.sg	
*.cf	*.hk	*.mo	*.si	
*.cg	*.hm	*.mp	*.sj	
*.ch	*.hn	*.mq	*.sk	
*.ci	*.hr	*.mr	*.sl	
*.ck	*.ht	*.ms	*.sm	

*.cl	*.hu	*.mt	*.sn	
*.cm	*.id	*.mu	*.so	
*.cn	*.ie	*.mv	*.sr	
*.co	*.im	*.mw	*.st	
*.cr	*.in	*.my	*.sv	
*.cu	*.io	*.mz	*.sy	
*.cv	*.iq	*.na	*.sz	
*.cx	*.ir	*.nc	*.tc	

- Currently, the following domains are allowed to send mail through the gateway appliance: Australia (AU), Canada (CA), England (EN), France (FR), Germany (DE), Israel (IL), Italy (IT) and Mexico (MX).

Blocked Domain Rule Setup Instructions:

- Login to the Ciphertrust appliance.


CipherTrust IronMail™ WebAdmin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address /admin/menu/ct_admin_main.html
Go Links
IronMail™
Mail Firewall Mail VPN Mail IDS Policy Manager Anti-Virus Anti-Spam Queue Manager Monitoring System Dashboard Logout
Internet

Welcome to IronMail™ WebAdmin

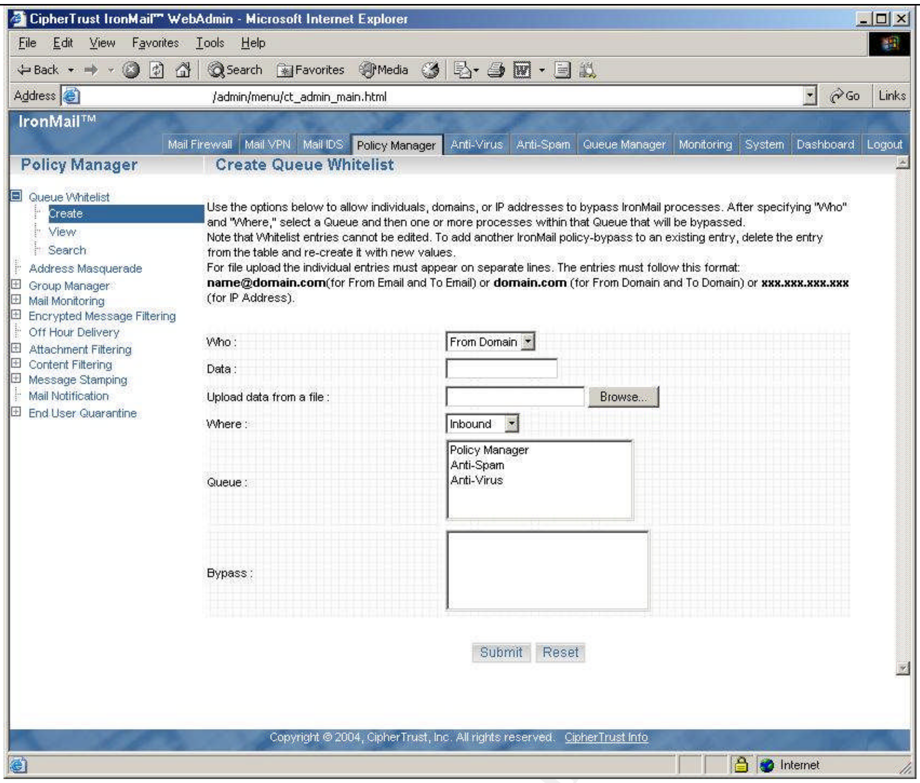
To configure the appliance, click a category in the toolbar above.

Last Login:
Failed Login Attempts: 0

Tips on using IronMail

Copyright © 2004, CipherTrust, Inc. All rights reserved. CipherTrust Info

- Select the Policy Manager tab.


CipherTrust IronMail™ WebAdmin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address /admin/menu/ct_admin_main.html
IronMail™
Mail Firewall Mail VPN Mail IDS Policy Manager Anti-Virus Anti-Spam Queue Manager Monitoring System Dashboard Logout
Policy Manager
Queue Whitelist
Create
View
Search
Address Masquerade
Group Manager
Mail Monitoring
Encrypted Message Filtering
Off Hour Delivery
Attachment Filtering
Content Filtering
Message Stamping
Mail Notification
End User Quarantine
Copyright © 2004, CipherTrust, Inc. All rights reserved. CipherTrust Info
Internet

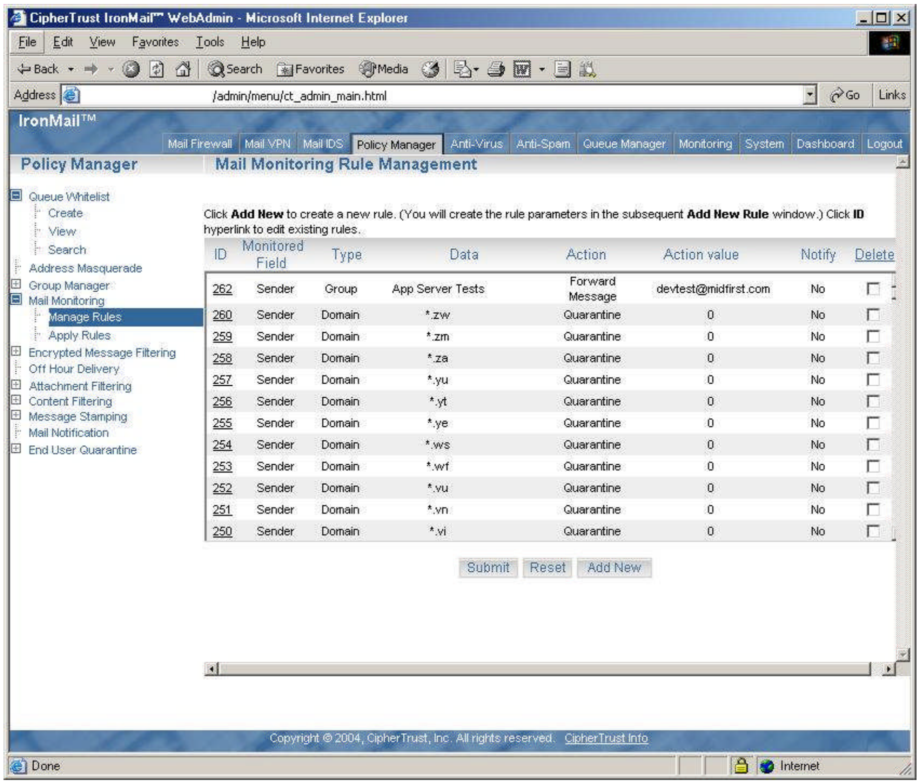
Create Queue Whitelist

Use the options below to allow individuals, domains, or IP addresses to bypass IronMail processes. After specifying "Who" and "Where," select a Queue and then one or more processes within that Queue that will be bypassed.
Note that Whitelist entries cannot be edited. To add another IronMail policy-bypass to an existing entry, delete the entry from the table and re-create it with new values.
For file upload the individual entries must appear on separate lines. The entries must follow this format: **name@domain.com**(for From Email and To Email) or **domain.com** (for From Domain and To Domain) or **xxx.xxx.xxx.xxx** (for IP Address).

Who :	From Domain
Data :	
Upload data from a file :	Browse...
Where :	Inbound
Queue :	Policy Manager Anti-Spam Anti-Virus
Bypass :	

Submit Reset

- On the left side, select the mail monitoring hyperlink, then select "Manage Rules".


CipherTrust IronMail™ WebAdmin - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address /admin/menu/ct_admin_main.html
IronMail™
Mail Firewall Mail VPN Mail IDS Policy Manager Anti-Virus Anti-Spam Queue Manager Monitoring System Dashboard Logout
Policy Manager
Queue Whitelist
Create
View
Search
Address Masquerade
Group Manager
Mail Monitoring
Manage Rules
Apply Rules
Encrypted Message Filtering
Off Hour Delivery
Attachment Filtering
Content Filtering
Message Stamping
Mail Notification
End User Quarantine
Copyright © 2004, CipherTrust, Inc. All rights reserved. CipherTrust Info
Done
Internet

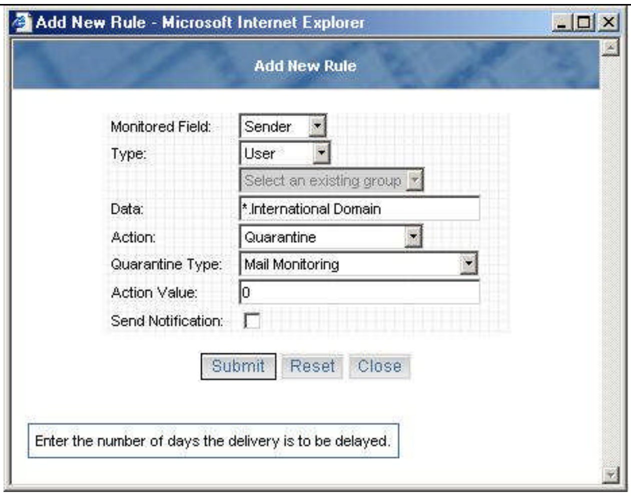
Mail Monitoring Rule Management

Click **Add New** to create a new rule. (You will create the rule parameters in the subsequent **Add New Rule** window.) Click **ID** hyperlink to edit existing rules.

ID	Monitored Field	Type	Data	Action	Action value	Notify	Delete
262	Sender	Group	App Server Tests	Forward Message	devtest@midfirst.com	No	□
260	Sender	Domain	*.zw	Quarantine	0	No	□
259	Sender	Domain	*.zm	Quarantine	0	No	□
258	Sender	Domain	*.za	Quarantine	0	No	□
257	Sender	Domain	*.yu	Quarantine	0	No	□
256	Sender	Domain	*.yt	Quarantine	0	No	□
255	Sender	Domain	*.ye	Quarantine	0	No	□
254	Sender	Domain	*.ws	Quarantine	0	No	□
253	Sender	Domain	*.wf	Quarantine	0	No	□
252	Sender	Domain	*.vu	Quarantine	0	No	□
251	Sender	Domain	*.vn	Quarantine	0	No	□
250	Sender	Domain	*.vi	Quarantine	0	No	□

Submit Reset Add New

- Select "Add New"



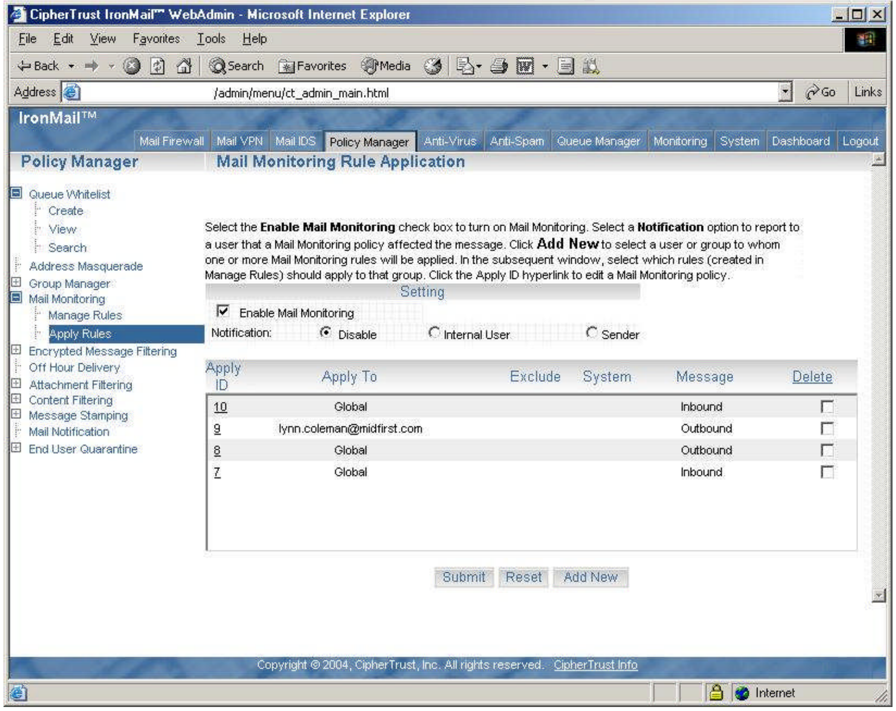
Add New Rule - Microsoft Internet Explorer

Add New Rule

Monitored Field:	Sender
Type:	User
	Select an existing group
Data:	*.International Domain
Action:	Quarantine
Quarantine Type:	Mail Monitoring
Action Value:	0
Send Notification:	□

Enter the number of days the delivery is to be delayed.

- Provide information about the international domain to block.
- Click the submit button.
- At this point, the rule must be applied in order to work. Go back to the Policy Manager – Mail Monitoring Rule Management page.
- On the left side under Mail Monitoring, select the apply rules hyperlink.



CipherTrust IronMail™ WebAdmin - Microsoft Internet Explorer

Address /admin/menu/ct_admin_main.html

Mail Monitoring Rule Application

Select the **Enable Mail Monitoring** check box to turn on Mail Monitoring. Select a **Notification** option to report to a user that a Mail Monitoring policy affected the message. Click **Add New** to select a user or group to whom one or more Mail Monitoring rules will be applied. In the subsequent window, select which rules (created in Manage Rules) should apply to that group. Click the Apply ID hyperlink to edit a Mail Monitoring policy.

Setting

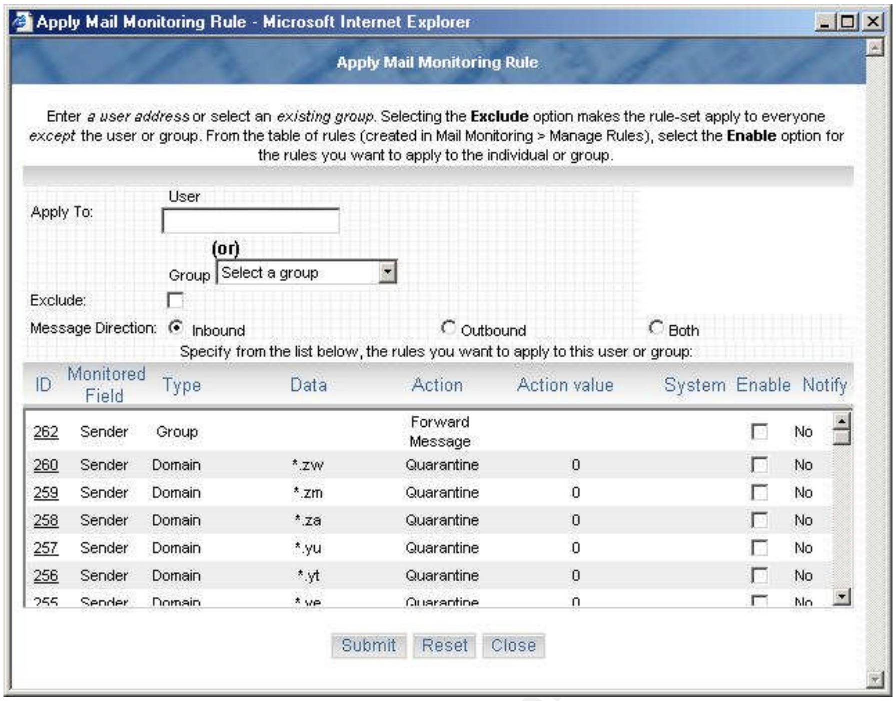
☑ Enable Mail Monitoring

Notification: ● Disable ○ Internal User ○ Sender

Apply ID	Apply To	Exclude	System	Message	Delete
10	Global			Inbound	□
9	lynn.coleman@midfirst.com			Outbound	□
8	Global			Outbound	□
7	Global			Inbound	□

Submit
Reset
Add New
Copyright © 2004, CipherTrust, Inc. All rights reserved. CipherTrust Info
Internet

- Select the “Add New” button.



Apply Mail Monitoring Rule

Enter *a user address* or select an *existing group*. Selecting the **Exclude** option makes the rule-set apply to everyone *except* the user or group. From the table of rules (created in Mail Monitoring > Manage Rules), select the **Enable** option for the rules you want to apply to the individual or group.

Apply To: User [ ]

(or)

Group [Select a group ▾]

Exclude: □

Message Direction: ● Inbound ○ Outbound ○ Both

Specify from the list below, the rules you want to apply to this user or group:

ID	Monitored Field	Type	Data	Action	Action value	System	Enable	Notify
262	Sender	Group		Forward Message			□	No
260	Sender	Domain	*.zw	Quarantine	0		□	No
259	Sender	Domain	*.zm	Quarantine	0		□	No
258	Sender	Domain	*.za	Quarantine	0		□	No
257	Sender	Domain	*.yu	Quarantine	0		□	No
256	Sender	Domain	*.yt	Quarantine	0		□	No
255	Sender	Domain	*.ye	Quarantine	0		□	No

- Ensure the message direction radio button selected is Inbound. Select the rule or rules you want to enable and hit submit.

Post Test Results/Audit Findings:

- The system is currently blocking over 260 international domains.
- This provides a highly restrictive Internet email environment, which helps provide an additional layer of security.
- No findings.

Section 4 – Executive Summary

This audit was performed to assess and determine significant risks pertaining to the Ciphertrust email gateway appliance. The first section defines the system and the environment for which it operates. In the second section, a series of twelve checklist items are included to validate the security measures of the appliance. Section three includes fieldwork, documentation and supporting evidence for any findings related to the checklist items. Finally, section four addresses the findings, mitigating factors, and costs required for the remediation process. During the course of the engagement, the Information Security team found two significant security issues. One finding was in the version of the SSH protocol and the second was the lack of a banner display. The audit was successful in terms of completing all control objectives with supporting evidence.

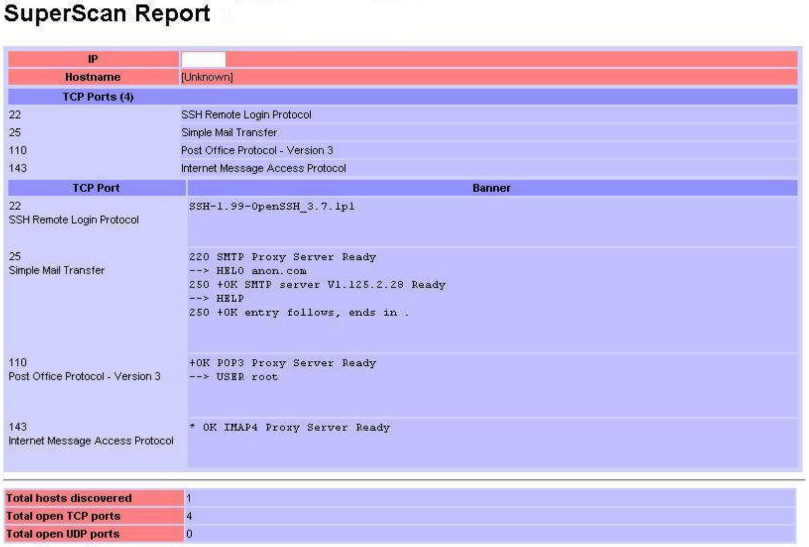
However, there were a few items that need immediate attention and remediation in order to maintain best security practice.

Audit Findings

This section will identify the security audit findings, provide recommendations to resolve the issues presented, and determine the related costs required to fix them.

Audit Step 6 – SSH Tunnel Integrity Check (Page 35)

Issue: Remote connections to the appliance are required for regular administration and monitoring and are also needed for the vendor to provide technical support. After running the SuperScan application against the appliance, there were four TCP ports active and listening, or waiting for connections. The Superscan report indicates the version of the SSH protocol the appliance is running has several vulnerabilities. See screen shot below:



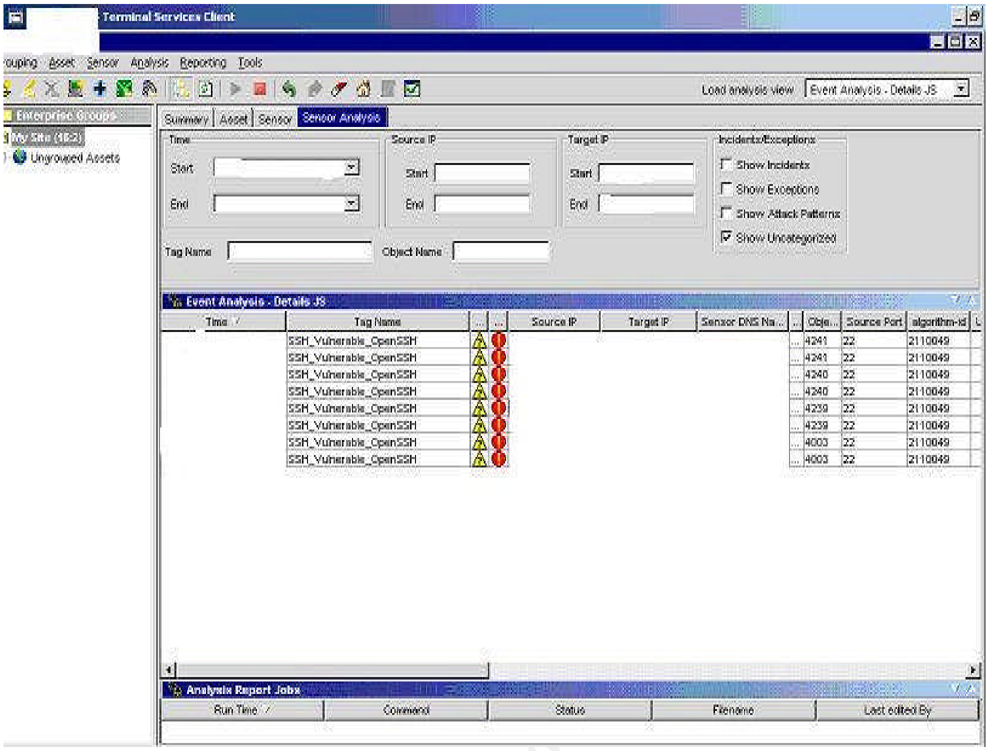
SuperScan Report

IP	[redacted]
Hostname	[Unknown]
TCP Ports (4)	
22	SSH Remote Login Protocol
25	Simple Mail Transfer
110	Post Office Protocol - Version 3
143	Internet Message Access Protocol

TCP Port	Banner
22 SSH Remote Login Protocol	SSH-1.99-OpenSSH_3.7.1p1
25 Simple Mail Transfer	220 SMTP Proxy Server Ready --> HELO anon.com 250 +OK SMTP server V1.125.2.28 Ready --> HELP 250 +OK entry follows, ends in .
110 Post Office Protocol - Version 3	+OK POP3 Proxy Server Ready --> USER root
143 Internet Message Access Protocol	* OK IMAP4 Proxy Server Ready

Total hosts discovered	1
Total open TCP ports	4
Total open UDP ports	0

Included is a screen shot of one of the financial institution’s network sensor confirming the SSH vulnerability



Load analysis view: Event Analysis - Details JS

Incidents/Exceptions
☐ Show Incidents
☐ Show Exceptions
☐ Show Attack Patterns
☑ Show Uncategorized

Event Analysis - Details JS

Time	Tag Name	...	...	Source IP	Target IP	Sensor DNS Na...	...	Obje...	Source Port	algorithm-id
	SSH_Vulnerable_OpenSSH	⚠	●				...	4241	22	2110049
	SSH_Vulnerable_OpenSSH	⚠	●				...	4241	22	2110049
	SSH_Vulnerable_OpenSSH	⚠	●				...	4240	22	2110049
	SSH_Vulnerable_OpenSSH	⚠	●				...	4240	22	2110049
	SSH_Vulnerable_OpenSSH	⚠	●				...	4239	22	2110049
	SSH_Vulnerable_OpenSSH	⚠	●				...	4239	22	2110049
	SSH_Vulnerable_OpenSSH	⚠	●				...	4003	22	2110049
	SSH_Vulnerable_OpenSSH	⚠	●				...	4003	22	2110049

Recommendation: The SSH protocol should be updated to the latest version. The financial institution has a perpetual technical support license that was packaged with the purchase of the appliance. This appliance has full vendor support so the cost would be minimal. Because it is a security appliance, no OS or application changes can be implemented from in-house. The vendor requires clients to send an email regarding the desired change, which they decide, whether or not to implement that change for the quarterly appliance updates. In this particular case, contact the vendor and notify them of the vulnerability and wait for the patch to become available.

Man Hours: 0 **Cost:** $0
(The Ciphertrust programming team would have to implement this change)

Audit Step 8 – Vulnerability Assessment using eEye Retina Security Scanner (Page 37)

Issue: This finding is generally the same as in Audit Step 6. The Retina report provides links to sites to download the update for the protocol. Reference audit step 6 for the complete Retina report (Page 35)

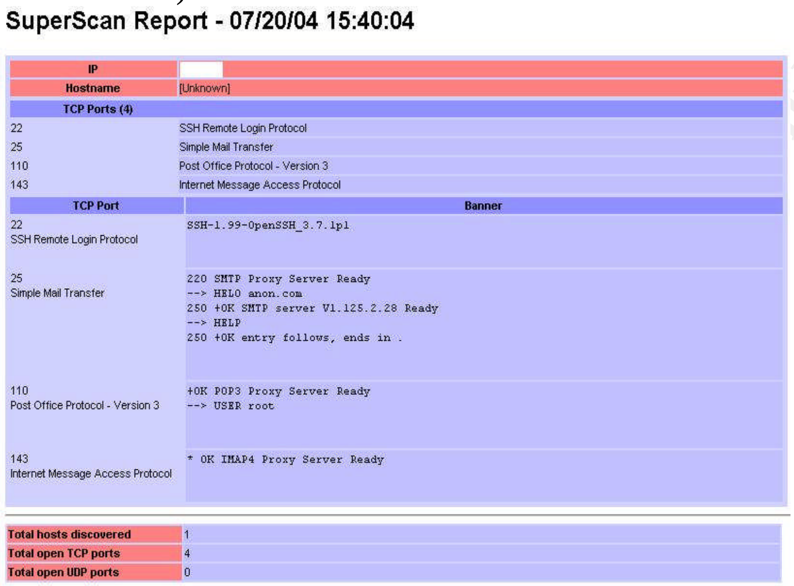
Recommendation: Reference the recommendation for Audit Step 6.

Man Hours: 1 **Cost:** Internal Labor Rate

Audit Step 11 – Warning Banner (Page 53)

Issue: The warning banner adds yet another layer of security to the appliance. It is intended to provide information to the user attempting to logon to the system that it is a private network resource and only authorized personnel are allowed to use it. The banner also allows an administrator to notify the user that all activity on the appliance is logged and monitored, partly to discourage a potential attack. Two screen shots are included. The first screen shot shows no warning banner displayed before logging on to the appliance. The second displays the new banner for the IMAP service. In the event of a lawsuit, it's imperative to provide evidence the system and it's operable environment are secure.

Screen Shot 1) this screen shot illustrates the banner for the IMAP service.

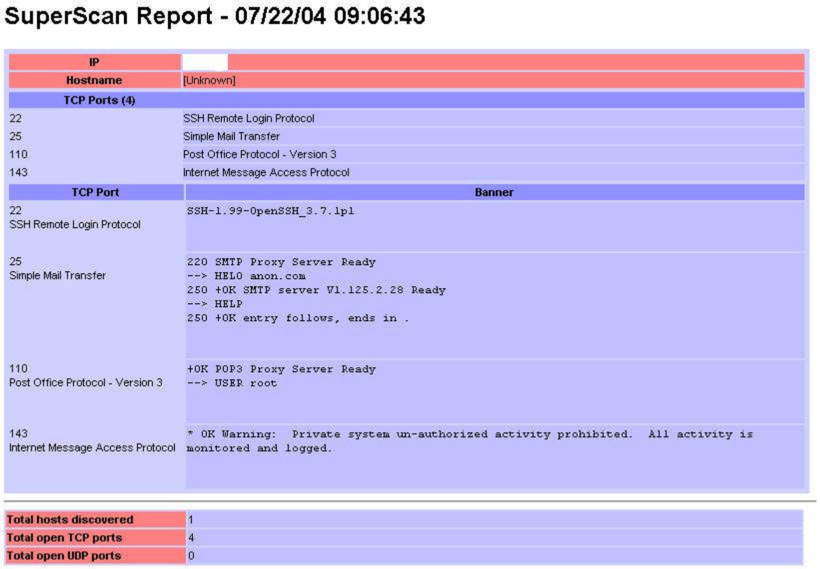


SuperScan Report - 07/20/04 15:40:04

IP	[redacted]
Hostname	[Unknown]
TCP Ports (4)	
22	SSH Remote Login Protocol
25	Simple Mail Transfer
110	Post Office Protocol - Version 3
143	Internet Message Access Protocol
TCP Port	**Banner**
22 SSH Remote Login Protocol	SSH-1.99-OpenSSH_3.7.1p1
25 Simple Mail Transfer	220 SMTP Proxy Server Ready --> HELO anon.com 250 +OK SMTP server V1.125.2.28 Ready --> HELP 250 +OK entry follows, ends in .
110 Post Office Protocol - Version 3	+OK POP3 Proxy Server Ready --> USER root
143 Internet Message Access Protocol	* OK IMAP4 Proxy Server Ready

Total hosts discovered	1
Total open TCP ports	4
Total open UDP ports	0

Screen Shot 2) this screen shot shows the banner has been changed.



SuperScan Report - 07/22/04 09:06:43

IP	[redacted]
Hostname	[Unknown]
TCP Ports (4)	
22	SSH Remote Login Protocol
25	Simple Mail Transfer
110	Post Office Protocol - Version 3
143	Internet Message Access Protocol
TCP Port	**Banner**
22 SSH Remote Login Protocol	SSH-1.99-OpenSSH_3.7.1p1
25 Simple Mail Transfer	220 SMTP Proxy Server Ready --> HELO anon.com 250 +OK SMTP server V1.125.2.28 Ready --> HELP 250 +OK entry follows, ends in .
110 Post Office Protocol - Version 3	+OK POP3 Proxy Server Ready --> USER root
143 Internet Message Access Protocol	* OK Warning: Private system un-authorized activity prohibited. All activity is monitored and logged.

Total hosts discovered	1
Total open TCP ports	4
Total open UDP ports	0

Recommendation: The vendor should be asked to implement a warning banner before being allowing a login to the appliance. Network Security personnel have already changed the warning banner for the IMAP service.

Man Hours: 1 **Cost:** Internal Labor Rate

CONCLUSION

This audit was conducted to establish a baseline for the security audit on similar email gateway appliances. The audit provides a subset to assist with policy deployment. Without policy guidelines, and standards to comply with those policies, it becomes difficult to determine the direction in which a business is going.

Audit References and Support Material

2004 MyDoom and Novrag (Threat Analysis)
http://www.infoplease.com/ipa/A0872842.html

Definition of a Threat
http://securityresponse.symantec.com/avcenter/refa.html#t

Ciphertrust Inc.
www.ciphertrust.com/support

Information Asset – Corporate Email
http://www.nexor.com/media/whitepapers/email%20asset.pdf
www.nexor.com

Network Vulnerability Analysis Project
http://www.isse.gmu.edu/~skaushik/nva/

NIST (National Institute of Standards and Technology) "Risk Management Guide for Information Technology Systems". Technology Administration – U.S Department of Commerce.

Paul Ammann, Duminda Wijesekera, and Saket Kaushik. *Scalable, Graph-Based Network Vulnerability Analysis.* In Proceedings CCS 2002: 9th ACM Conference on Computer and Communications Security, Washington, DC, November 2002. pp 217-224 PDF

Retina Network Security Scanner
http://www.eeye.com/html/products/retina/index.html

Retina Manual Pg 38/83 "Retina Audit Wizard"
http://www.google.com/search?hl=en&ie=UTF-8&q=retina+audit+steps

SANS (Internet Storm Center)
http://isc.sans.org

SSHD1 Exploit web site – Benjamin Krueger
http://www.ssc.com/pipermail/linux-list/2001-November/010581.html

"The Inevitability of Failure: The Flawed Assumptions of Security in Modern Computing Environments." Lososco, Smalley, Muckelbauer, Taylor, Turner and Farrell. NSA

Webster's Dictionary
http://www.webster-dictionary.org/definition/compliance