



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Auditing Systems, Applications, and the Cloud (Audit 507)"
at <http://www.giac.org/registration/gсна>

DNS and SMTP Server Security Audit: An Auditor's Perspective

A GIAC Practical applied toward the GIAC Systems and Network Auditor (GSNA) Certification
GSNA Practical Assignment Version 2.1 (Amended July 5, 2002), Option 1

Prepared By Jeff Pack**June 14, 2003**

© SANS Institute 2003, Author retains full rights.

.....

Table of Contents

Abstract/Summary	1
1 Research in Audit, Measurement Practice and Control	2
1.1 Description of System	2
1.2 Evaluation of Risk	3
1.3 Current State of Practice	8
2 Audit Checklist	9
2.1 Scope	9
2.2 Structure	9
2.3 Conventions	10
2.4 Administration Checklist	10
2.5 Physical Access Control Checklist	12
2.6 Network Checklist	14
2.7 Operating System Checklist	17
2.8 DNS Checklist	24
2.9 SMTP Checklist	29
3 Audit Evidence	42
3.1 Audit Results	42
3.2 Measure Residual Risk	61
3.3 Evaluate the Audit	62
4 Audit Report	64
4.1 Executive Summary	64
4.2 Audit Findings and Risks	64
4.3 Audit Recommendations	68
4.4 Estimated Costs	68
4.5 Compensating Controls	69
References	70

Table of Figures

Figure 1 – Internet Network Design.....	2
Figure 2 – Intranet Search Page for Asset Protection Documents	43
Figure 3 – Search Page Results for Asset Protection Documents	44
Figure 4 – Rack-mounted server for DNS/SMTP (second from top)	45
Figure 5 – Door to Computer Room	46
Figure 6 – Air Conditioning Unit	46
Figure 7 - UPS	46
Figure 8 – Results of nmap scans	48
Figure 9 – Output from the “lsof -l +M” command.....	50
Figure 10 – Output from the “netstat -anp” command.....	50
Figure 11 – Output from “named -v” command	52
Figure 12 – Listing of /etc/named.conf from server	54
Figure 13 – Test lookup from external host	55
Figure 14 – Test lookup from internal host.....	55
Figure 15 – Checking for least privilege and chroot	57
Figure 16 – Output from sendmail debug command to find version	58
Figure 17 – Listing of file ownership and permissions for sendmail.....	60
Figure 18 – Check of PrivacyOptions on sendmail server.....	61

Table of Tables

Table 1 – Summary of Risk Evaluation	5
Table 2 – Administration Checklist	10
Table 3 – Physical Access Control Checklist	13
Table 4 –Network Checklist.....	14
Table 5 –Operating System Checklist	17
Table 6 –DNS Checklist	24
Table 7 –SMTP Checklist.....	29
Table 8 – Estimated Costs	69

Abstract/Summary

Auditing systems and networks is a challenging task. The auditors have several obstacles to overcome even before they start the process. Auditors, for the most part, are not welcomed with open arms by management or staff, are considered to have limited technical and practical knowledge about how the system actually works, typically have to defend their findings in a somewhat hostile environment, and are rarely complimented for finding faults with the system or network. It makes a lot of people wonder if auditing is really worth it.

Auditing, however, is necessary and fundamental to the proper operation of systems and networks. Using the analogy from the SANS "Auditing Networks, Perimeters and Systems" coursework, if your company had never had an information security incident, you might be tempted to not do anything to protect your network [SANS – 03-1]. However, if you were having a new office building designed, disregarding the building codes, would you install a fire suppression system even if you had never had a fire in your buildings before? Of course! It's an easy decision. Also, once you moved into the building, would you test the fire control system even if you have never had a fire before? Yes, of course, because you want to make sure that the fire control system will work when a fire occurs.

System and network auditing provides the same function as testing the fire control system. Without a periodic review of policies, standards, and procedures, network perimeters, critical systems and services, you are never sure if your security controls are going to work when they need to.

This paper discusses the steps required to audit the DNS and SMTP services based on a Linux Intel server for a small to medium-sized organization. The first section describes the system being reviewed, the types of risk inherent for this system and services, and the current state of practice for auditing similar systems. The second section provides a checklist of steps that are used to evaluate the system and determine the level of risk present. The third section details the process taken and the findings from ten of the steps that were defined in the second section. The final section provides an audit report for management, including an executive summary, summary of findings and risk, recommendations, estimated costs and any additional compensating controls.

1 Research in Audit, Measurement Practice and Control

1.1 Description of System

The system being reviewed is the external Domain Name System (DNS) and Simple Mail Transfer Protocol (SMTP) server for an application development company.

The DNS server is providing external (Internet) name resolution for the company's domain name and acts as a forwarder for internal name resolution that is not resolved by the internal DNS servers [Albitz – 01].

The SMTP server provides the gateway function between the Internet and the internal SMTP server. All incoming and outgoing SMTP traffic travels through the gateway.

The company has a dedicated Internet connection and publicly accessible web servers as well as the DNS/SMTP server. The publicly accessible servers are connected in a screened subnet design [Chapman – 00]. This design is shown in Figure 1. The main subject of the audit is circled.

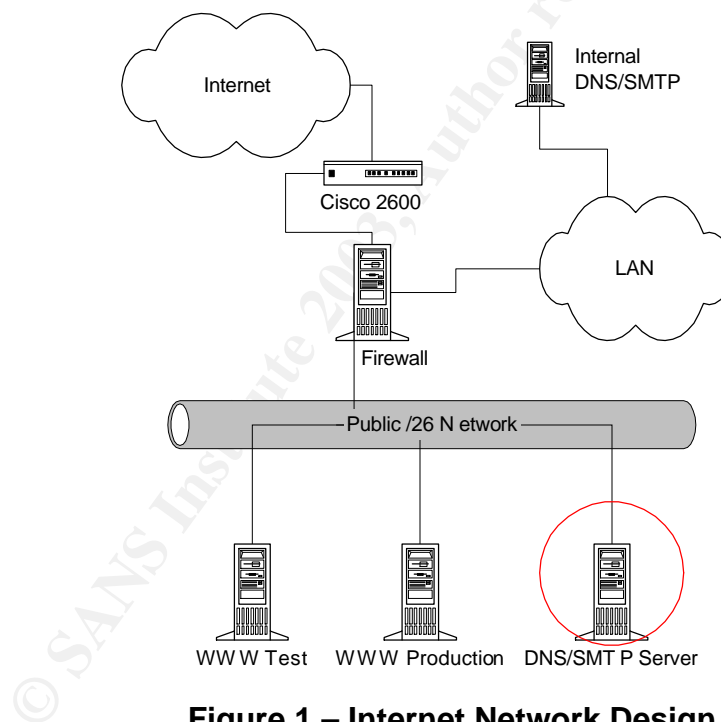


Figure 1 – Internet Network Design

The DNS/SMTP server is an Intel rack-mount server using Red Hat 9.0 as the operating system. The DNS server application is the open source Berkeley Internet Name Domain (BIND) 9.2.1 implementation developed and maintained by the Internet Software Consortium (ISC) as delivered in the Red Hat distribution [ISC – 01]. The SMTP server application is the open source Sendmail 8.12.8 implementation developed and maintained by the Sendmail Consortium also as delivered by Red Hat [Sendmail – 03].

The scope of this audit is primarily concerned with the DNS and SMTP services on the subject server. However, in order to evaluate risk properly, other areas of the network will require review, such as the policies, standards and procedures, the physical location of the server, the router configuration and any access control lists (ACLs), the firewall rules with respect to DNS and SMTP services, and the configuration of the operating system in those areas that relate to the DNS and SMTP services.

For the purposes of maintaining privacy, all company information has been omitted or modified and actual IP addresses have either been deleted or modified to non-routable addresses.

1.2 Evaluation of Risk

The DNS/SMTP server being audited in this report has a relatively high level of risk compared to other information resources at this company due to its location in the network and its function in the proper operation of the organization. The evaluation of risk is partitioned into the risk of improper administration, physical protection, the underlying computing platforms, and the separate services. A summary table is presented at the end of this section.

1.2.1 Administration Risks

Improper administration practices can result in risks to the DNS and SMTP services. Without proper policies, standards and procedures, the system will allow unauthorized access and improper configuration of the services.

1.2.2 Physical Access Control Risks

There is a physical access threat for the DNS/SMTP server as well as the firewall and router. The major threats from physical access are denial-of-service and inappropriate access to the equipment. This equipment should be in a secure location with appropriate physical and environmental controls to protect the equipment from physical threats. With proper controls, this risk can be effectively mitigated.

1.2.3 Network Risks

Network devices in the path of the service connection are also responsible for protecting the service to the extent that they are able to. For example, Internet routers should have ACLs installed to limit incoming DNS requests to the external name servers. Continuing our example, outbound DNS requests should only be allowed from the external name servers, as all other internal hosts should be configured to ask the internal name servers for DNS requests.

1.2.4 Operating System Risks

All network services including DNS and SMTP rely on an underlying operating system to provide a basic structure for the computing platform. Specialized hardware solutions with "hardened" operating systems are increasingly popular for firewalls and intrusion detection systems, but even these suffer from vulnerabilities [CVE – 01]. The major threats to

operating systems are the unauthorized use of the system, denial-of-service attacks on the system, and the improper configuration or maintenance of the system. Proper management of the systems will reduce the risk to acceptable levels.

1.2.5 DNS Risks

DNS has a long and colorful history of security vulnerabilities. Perhaps the most famous DNS vulnerability that had widespread implications was the AlterNIC incident in July 1997 [Albitz – 01]. Eugene Kashpureff, then affiliated with AlterNIC, “poisoned” the caches of major name servers around the world, which in effect redirected all requests for `www.internic.net` to a web server belonging to AlterNIC. The result was a much higher awareness of how vulnerable DNS can be.

The major threats to the DNS service are denial-of-service, unauthorized modification of configuration data, and unauthorized access to the operating system via the DNS service. Proper configuration and maintenance of the DNS configuration files is critical to mitigating the risk associated with these threats. This includes proper administrative policies and procedures for configuration management as well as prudent access controls and separation of duties.

1.2.6 SMTP Risks

If there is one service that has a more colorful history for security vulnerabilities than DNS, it is SMTP, and in particular, the sendmail implementation of SMTP. The Morris worm, unleashed on the Internet in November 1988, exploited a vulnerability in sendmail, along with other weaknesses in Sun and DEC VAX Unix implementations [Boettger – 00]. The consequences of this event were many of the “firsts” in information security. The CERT (Computer Emergency Response Team) Coordination Center at Carnegie Mellon University was founded primarily in response to the worm, and Morris was the first person convicted of violating the 1986 US Federal Computer Fraud and Abuse Act. Many other stories exist regarding the exploitation of SMTP and sendmail [SANS – 03-2].

By far the largest risk associated with SMTP is gaining unauthorized access to the operating system via the SMTP service. There have been numerous buffer overflows exploited against SMTP servers and the vast majority of them provide the intruder with privileged access (i.e., “root” in Unix) to the operating system. Other threats include denial-of-service, improper use of the SMTP service (for example, relaying SMTP traffic), and unauthorized modification of the SMTP configuration data. Configuring the SMTP service to operate as much as possible in a non-privileged mode (as in Sendmail 8.12) mitigates much of the unauthorized access risk. As with DNS, proper configuration and maintenance, as well as administrative policies and procedures, is critical to mitigating the risk.

Table 1 – Summary of Risk Evaluation

Administration Risks				
Threat	Risk	Likelihood	Severity	Consequences
Improper or non-existent policies, standards and procedures for management of services	System administrators have no guidance in managing system for business goals	Medium	Medium to High	Without proper guidance, services do not meet business goals or best industry practices and do not provide proper protection from unauthorized access and use.
Improper configuration and maintenance	System provides erroneous data to customers, allows misuse of service, or allows unauthorized access	Low to Medium	Medium to High	DNS information could be incorrect causing other services (i.e., HTTP) to be unavailable to the Internet. SMTP service could be used to relay inappropriate messages or message delivery could be interrupted possibly resulting in important e-mail not being delivered timely or properly.
Unauthorized access	System is accessed by unauthorized individuals using misconfigured operating system or application	Medium	High	Modify system and service configuration. Use configuration information to launch other attacks. Provides easier access to screened subnet and internal hosts.

Physical Access Control Risks				
Threat	Risk	Likelihood	Severity	Consequences
Denial-of-service	System is physically damaged and unable to provide service	Low	High	DNS and SMTP services will not be available until replacement hardware is installed.
Unauthorized access	System is accessed using console, serial terminal or maintenance port	Low	High	Console access provides higher privileges by default for some systems. Modify system and service configuration. Use configuration information to launch other attacks. Provides easier access to screened subnet and internal hosts.
Network and Operating System Risks				
Threat	Risk	Likelihood	Severity	Consequences
Unauthorized access	System is accessed by unauthorized individuals using vulnerability or misconfigured support service, such as SSH or FTP	Medium	High	Modify system and service configuration. Use configuration information to launch other attacks. Provides easier access to screened subnet and internal hosts.
Denial-of-service	System is unable to provide primary services to customers	Medium	High	DNS and SMTP services will not be available until denial-of-service attack is controlled or is terminated by attacker.

DNS Risks				
Threat	Risk	Likelihood	Severity	Consequences
Denial-of-service	DNS server is unable to provide requested service	Medium	High	DNS service will not be available until denial-of-service attack is controlled or is terminated by attacker.
Unauthorized modification of configuration data	DNS server provides incorrect data or permits unauthorized access and modification of DNS information	Low to Medium	Medium to High	DNS information could be incorrect causing other services (i.e., HTTP) to be unavailable to the Internet. DNS could be directed to incorrect servers for upstream lookups and direct employees to incorrect locations.
Unauthorized access	DNS service provides unauthorized access to operating system using a newly discovered vulnerability (i.e., a buffer overflow)	Medium	High	Modify system and service configuration. Use configuration information to launch other attacks. Provides easier access to screened subnet and internal hosts.
SMTP Risks				
Threat	Risk	Likelihood	Severity	Consequences
Unauthorized access	SMTP service provides unauthorized access to operating system using a newly discovered vulnerability (i.e., a buffer overflow)	Medium	High	Modify system and service configuration. Use configuration information to launch other attacks. Provides easier access to screened subnet and internal hosts.

Denial-of-service	SMTP server is unable to provide requested service	Medium	High	SMTP service will not be available until denial-of-service attack is controlled or is terminated by attacker. Critical e-mail cannot be delivered in a timely manner.
Unauthorized modification of configuration data	SMTP server allows misuse or does not deliver SMTP messages properly	Low to Medium	Medium to High	SMTP service could be used to relay inappropriate messages or message delivery could be interrupted possibly resulting in important e-mail not being delivered timely or properly.

1.3 Current State of Practice

There are several different types of resources available for developing checklists for DNS and SMTP service auditing. The resources used to develop the checklists in the second section are listed below.

1.3.1 Reference Books

Two of the primary resources for DNS and SMTP information are the O'Reilly reference books. DNS and BIND, Fourth Edition, by Paul Albitz and Cricket Liu is the de facto reference guide for BIND. Sendmail, Third Edition, by Bryan Costales with Eric Allman is the de facto reference for the *sendmail* implementation of SMTP. Each of these books has specific chapters dedicated to the secure configuration of the respective service.

1.3.2 Configuration Guides

There are many configuration guides available for low or no cost. The SANS Institute has several "Step-By-Step" guides for various operating systems. Some of them have steps for securing DNS and SMTP services. The SANS Reading Room (<http://www.sans.org/rr>) has several references for securely implementing DNS and SMTP services. CERT (<http://www.cert.org>) has several resources for securing services. The Center for Internet Security (<http://www.cisecurity.org>) also has several resources for configuring routers, firewalls and operating systems.

1.3.3 Web Resources

The millions of Web servers available combined with the search capabilities of a modern search engine provide a large number of resources for developing checklists. There are too many available to provide a complete list. Any specific resources used in this document are referenced in each checklist step and listed in the References section.

2 Audit Checklist

The audit checklist provides the auditor with a systematic, repeatable process for measuring compliance to company policies and standards and industry best practices. This is important for measuring the change in risk to the organization over time.

2.1 Scope

The scope of this audit checklist is primarily concerned with DNS and SMTP services on a screened subnet server. However, in order to evaluate risk properly other areas will require review such as:

- all relevant policies, standards and procedures
- the physical location of the server
- the router configuration and firewall rules with respect to DNS and SMTP services
- the configuration of the operating system in those areas that relate to the DNS and SMTP services.

2.2 Structure

The checklists are organized by the types of risk as described in Section 1. Each checklist step has the following elements.

2.2.1 Identifier

The identifier is a unique name for each step in the checklist.

2.2.2 Objective

The objective is the description and goal of a particular step.

2.2.3 Reference

The reference indicates the source of the step, either from a reference or an original contribution from the auditor.

2.2.4 Risk

The risk identifies which type and element of risk the step is addressing.

2.2.5 Compliance

The compliance element describes the criteria for compliance to the step.

2.2.6 Test

The test describes the action taken to determine if the system passes or fails a particular step.

2.2.7 O/S

The O/S item indicates whether the test is objective or subjective. Objective tests are independently verifiable and repeatable, whereas subjective tests mainly rely on the impression and opinion of the auditor.

2.3 Conventions

System commands and the results returned that are used as part of the testing are referenced in `Courier` font. References are denoted by an author or organization name with a full reference to the References list at the end of the report.

2.4 Administration Checklist

The administration checklist groups the common administrative steps for the DNS/SMTP server and for the organization in general.

Table 2 – Administration Checklist

Identifier	A1
Objective	Check for Information Security Policy.
Reference	[GAO – 98], [Tudor – 01] and original contribution
Risk	No guidance in managing system for business goals or best practices
Compliance	Does an information security policy exist, and more importantly, do the employees know if the policy exists and how it affects them? If not, the system is not compliant.
Tests	Ask system administrator or manager for policy. Also ask other staff members if they are aware of any information security policies. Review internal web site for policies.
O/S	Objective and Subjective: Either the policy exists or it does not, but harder to measure is the effectiveness of the policy. If employees are aware of the policy and their associated responsibilities, then the policy is effective.
Identifier	A2
Objective	Information Asset Management Standards and/or Procedures <ul style="list-style-type: none">• Change Control Standard and/or Procedure• Configuration Management Standard and/or Procedure• System Lifecycle Management Standard and/or Procedure
Reference	[Tudor – 01] and original contribution
Risk	No standards or procedures for managing system to meet business goals or industry best practices

Compliance	Do information asset management standards and/or procedures exist, and more importantly, do the employees responsible for information assets know and follow the standards and/or procedures? If not, the system is not compliant.
Test	Ask system administrator or manager for standards and/or procedures. Also ask other staff members if they are aware of relevant standards and/or procedures. Review internal web site for relevant standards and/or procedures.
O/S	Objective: Either the standards and/or procedures exist or not.
Identifier	A3
Objective	Information Asset Protection Standards and/or Procedures <ul style="list-style-type: none"> • Remote Access Standard and/or Procedure • Encryption Standard and/or Procedure • Availability Protection Standard and/or Procedure • Anti-virus Standard and/or Procedure • Confidentiality Protection Standard and/or Procedure • Access Control Standard and/or Procedure
Reference	[Tudor – 01] and original contribution
Risk	No standards or procedures for protecting information assets to meet business goals or industry best practices
Compliance	Do information asset protection standards and/or procedures exist, and more importantly, do the employees responsible for information assets know and follow the standards and/or procedures? If not, the system is not compliant.
Test	Ask system administrator or manager for standards and/or procedures. Also ask other staff members if they are aware of relevant standards and/or procedures. Review internal web site for relevant standards and/or procedures.
O/S	Objective: Either the standards and/or procedures exist or not.
Identifier	A4
Objective	Threat and Vulnerability Management Standards and/or Procedures <ul style="list-style-type: none"> • Threat Monitoring Standard and/or Procedure • Vulnerability Assessment Standard and/or Procedure • Vulnerability Management Standard and/or Procedure • Incident Response Standard and/or Procedure
Reference	[Tudor – 01] and original contribution

Risk	No standards or procedures for monitoring threats, managing vulnerabilities and response to information security incidents
Compliance	Do threat and vulnerability management standards and/or procedures exist, and more importantly, do the employees responsible for information assets know and follow the standards and/or procedures? If not, the system is not compliant.
Test	Ask system administrator or manager for standards and/or procedures. Also ask other staff members if they are aware of relevant standards and/or procedures. Review internal web site for relevant standards and/or procedures.
O/S	Objective: Either the standards and/or procedures exist or not.
Identifier	A5
Objective	Acceptable Use and Information Security Awareness Standards
Reference	[Tudor – 01] and original contribution
Risk	Employees are unaware of their responsibilities for information security and the threats, vulnerabilities and risks associated with information technology.
Compliance	Do acceptable use and information security awareness standards exist and, more importantly, do the employees know and follow the standards? If not, the system is not compliant.
Test	Ask system administrator or manager for standards. Also ask other staff members if they are aware of relevant standards. Review internal web site for relevant standards.
O/S	Objective: Either the standards exist or not.

2.5 Physical Access Control Checklist

This checklist lists the common steps that should be taken to physically protect the DNS/SMTP server from unauthorized access.

Table 3 – Physical Access Control Checklist

Identifier	P1
Objective	Physical access controls for server, firewall, and router locations.
Reference	[NERC – 03] and original contribution
Risk	Unauthorized access to room that houses DNS/SMTP server or other network devices could cause denial-of-service or unauthorized access to system.
Compliance	List of personnel with key or listing of users allowed access via a card reader or other electronic access control system. If list has terminated or non-essential employees on it, the system is not compliant.
Test	Review physical location of server and determine if access controls (locked door, key card lock system, etc.) are in place to protect server
O/S	Objective and Subjective: the room is locked or it is not; however the list of people that have access to the room should be evaluated for need.
Identifier	P2
Objective	Physical protection for servers, including drives, consoles, maintenance ports, and environmental controls.
Reference	[SANS – 00] and original contribution
Risk	Unauthorized personnel can reboot servers with different operating system, reboot systems with console access or plug into serial or maintenance ports to gain access.
Compliance	Are adequate controls in place for proper operation of the server, including locked rack, air conditioning, regulated power, or alarms for temperature, humidity, water on floor, and unauthorized access after working hours? If not, the system may not be fully compliant.
Test	Review physical security of servers; ideally they should be in a locked cabinet with adequate environmental controls and alarms to maintain system in operating conditions for temperature, humidity, water and power.
O/S	Subjective: The server may have most of these safeguards and be adequately protected; final judgment is subject to costs and overall risk posture of the organization.
Identifier	P3
Objective	Disable “Auto” settings and enable BIOS passwords.
Reference	[SANS – 00] and original contribution

Risk	Server BIOS can automatically reconfigure for new hardware and unauthorized users can change BIOS settings to enable booting from diskette, CD-ROM. Note that these are not the power-on password or other settings that would prevent the server from automatically rebooting after a power outage. Most organizations want the server to reboot automatically after a power outage.
Compliance	Are BIOS passwords set on the server? If not, the system is not compliant.
Test	Review server BIOS for automatic hardware reconfiguration and passwords.
O/S	Objective: Either the settings are correct or they are not.

2.6 Network Checklist

These steps pertain to network security as it pertains to the DNS/SMTP server. This is not a complete checklist for routers or firewalls. These steps are only provided to provide a more complete understanding of the security controls for the DNS and SMTP services that may be in place. A complete checklist for auditing a router or firewall is outside the scope of this audit. Please check the References for a complete checklist for auditing a router or firewall.

Table 4 –Network Checklist

Identifier	N1
Objective	Ingress/egress filtering and other ACLs on Internet router.
Reference	[CIS – 01] and original contribution
Risk	Unauthorized servers could access services and gain restricted knowledge of the system configuration
Compliance	Are ACLs installed to reduce the chance of IP spoofing attacks? Are additional ACLs installed for specific types of traffic? If not, the system may not be compliant.

Test	<p>Have administrator of router provide copy of running configuration of router for review or access router and review running configuration. Typical ACLs that should be in place are listed below.</p> <p>Here are some example ACLs for a Cisco Internet router. List 100 would be applied on the outside interface of the router to all incoming traffic. List 101 would be applied on the outside interface also, but on outbound traffic.</p> <pre>access-list 100 deny ip 10.0.0.0 0.255.255.255 any log access-list 100 deny ip 127.0.0.0 0.255.255.255 any log access-list 100 deny ip 172.16.0.0 0.15.255.255 any log access-list 100 deny ip 192.168.0.0 0.0.255.255 any log access-list 100 deny ip <your public address block> any log access-list 100 deny ip any 10.0.0.0 0.255.255.255 log access-list 100 deny ip any 127.0.0.0 0.255.255.255 log access-list 100 deny ip any 172.16.0.0 0.15.255.255 log access-list 100 deny ip any 192.168.0.0 0.0.255.255 log access-list 100 permit ip any any access-list 101 permit ip <your public address block> any access-list 101 deny ip any any log</pre> <p>Scan router from the Internet with a port scanner (such as nmap) with the source IP address set to an internal address and see if the ACLs reject the traffic on the router.</p>
O/S	<p>Objective and Subjective: This test is objective in that if there are no ACLs on the router, it fails. However, some organizations may prefer to do more filtering on the firewall for logging or other reasons. This test needs to be reviewed in conjunction with the organization's policies, standards and procedures, as well as the firewall rules to determine if adequate protection is in place.</p>
Identifier	N2
Objective	Filter access to servers at the Internet firewall.
Reference	[Albitz – 01], [CERT – 02] and original contribution
Risk	Unauthorized users could access services and gain restricted knowledge of the system configuration.
Compliance	Are the firewall rules configured correctly to accept and deny traffic as designed? If not, the system is not compliant.
Test	Have administrator of firewall provide copy of running configuration of firewall rules for review. Typical firewall rules that should be in place are

listed in the following table.

Number	Function	Description	Source IP	Source Port	Destination IP	Destination Port
1	Public NS	Inbound queries	Any	53/udp 53/tcp >1023/udp >1023/tcp	PubNS	53/udp 53/tcp
2	Public NS	Query replies	PubNS	53/udp 53/tcp	Any	53/udp 53/tcp >1023/udp >1023/tcp
3	Internal NS	Queries from clients	Internal network	>1023/udp >1023/tcp	IntNS	53/udp 53/tcp
4	Internal NS	Replies to clients	IntNS	53/udp 53/tcp	Internal network	>1023/udp >1023/tcp
5	Internal NS	Outbound recursive queries	IntNS	53/udp 53/tcp >1023/udp >1023/tcp	Any	53/udp 53/tcp
6	Internal NS	Replies to recursive queries	Any	53/udp 53/tcp	IntNS	53/udp 53/tcp >1023/udp >1023/tcp
7	Public SMTP	Inbound SMTP	Any	>1023/tcp	PubSMTP	25/tcp
8	Public SMTP	Inbound replies	PubSMTP	25/tcp	Any	>1023/tcp
9	Internal SMTP	Outbound SMTP	Internal Network	>1023/tcp	IntSMTP	25/tcp
10	Internal SMTP	Outbound replies	IntSMTP	25/tcp	Internal Network	>1023/tcp
11	Internal to Public SMTP	Outbound SMTP	IntSMTP	>1023/tcp	PubSMTP	25/tcp
12	Internal to Public SMTP	Outbound replies	PubSMTP	25/tcp	IntSMTP	>1023/tcp

Note the need in Rule 1 to allow inbound queries to 53/TCP. This is used to accommodate query requests that won't fit into a single UDP packet. There is new functionality as defined in RFC 2671 that allows larger UDP

	<p>packet sizes, but not all servers will recognize this enhancement, so the 53/tcp rule will still be required. Stateful firewalls such as iptables or CheckPoint's FireWall-1 will only have to enable the rule required for query initiation. For example, in the case of Rules 1 and 2, the stateful firewalls will only require Rule 1.</p> <p>Use a scanning tool such as nmap to discover which ports are available on the DNS/SMTP server from the Internet. Scan for both TCP and UDP ports.</p>
O/S	<p>Objective and Subjective: This test is objective in that if there are not adequate firewall rules enabled, it fails. However, some organizations may prefer to do more filtering on the router for performance or other reasons. This test needs to be reviewed in conjunction with the organization's policies, standards and procedures, as well as the router rules to determine if adequate protection is in place.</p>

2.7 Operating System Checklist

This checklist provides areas of the operating system that should be checked as they pertain to the DNS/SMTP server. This is not a complete checklist for the Linux operating system. These steps are only provided to provide a more complete understanding of the security controls for the DNS and SMTP services that may be in place. A complete checklist for auditing a Linux server is outside the scope of this audit. Please check the References for a complete checklist for auditing a Linux server.

Table 5 –Operating System Checklist

Identifier	O1
Objective	Verify that shadow passwords with MD5 hashing are used.
Reference	[SANS – 00]
Risk	Password hashes can be easily exposed to intruders who can then run password-cracking software to reveal the clear text password.
Compliance	Are shadow passwords with MD5 hashes installed? If not, the system is not compliant.

Test	<p>On the target server, as root, type:</p> <pre># more /etc/passwd</pre> <p>The result should show no hash entries in the /etc/passwd file, similar to this:</p> <pre>root:x:0:0:root:/root:/bin/bash bin:x: 1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin</pre> <p>On the target server, as root, type:</p> <pre>more /etc/shadow</pre> <p>The /etc/shadow file should look something like this:</p> <pre>root:\$1\$jIyBPLT/\$FfnMaTBfM4sc1tGOzhFRN0:12155:0:99999:7::: bin:*:12155:0:99999:7::: daemon:*:12155:0:99999:7::: adm:*:12155:0:99999:7::: lp:*:12155:0:99999:7:::</pre> <p>Notice the long string (~34 characters) in the second position of the first line in the shadow file. This is the MD5 hash of the clear-text password for root. If the hash is only 13 characters long, it is using the older DES algorithm. The server should be reconfigured to use the MD5 algorithm.</p>
O/S	Objective: The server is either using shadow passwords with MD5 hashes or it is not.
Identifier	O2
Objective	Set or disable passwords for all system accounts associated with DNS and SMTP.
Reference	[SANS – 00] and original contribution
Risk	Unauthorized users could access services and overtake the server.
Compliance	Are the passwords for the system accounts associated with DNS and SMTP disabled so no login is allowed? If not, the system is not compliant.

Test	<p>Use the following command as root for each of the desired user ids:</p> <pre># grep <user id> /etc/shadow</pre> <p>where <user id> is replaced with one of the following each time: root, named, smmsp. The result should look something like this:</p> <pre># grep root /etc/shadow root:\$1\$jIyBPLT/\$FfnMaTBfM4sc1tGOzhFRN0:12155:0:99999:7:::</pre> <pre># grep named /etc/shadow named:!!:12155:0:99999:7:::</pre> <pre># grep smmsp /etc/shadow smmsp:!!:12155:0:99999:7:::</pre> <p>Each user id should either have a hash entry like the root user id above, or it should be disabled like the named and smmsp user ids.</p> <p>Also attempt to login as one of the user ids to see how the system responds. It should not allow access.</p>
O/S	Objective: Either the accounts have passwords or have been disabled, or they haven't.
Identifier	O3
Objective	Review /etc/passwd and /etc/security/access.conf for system account login permissions.
Reference	[SANS – 00], [RedHat-02] and original contribution
Risk	Unauthorized users could access services and overtake the server
Compliance	Are the system accounts associated with DNS and SMTP disabled? If not, the system is not compliant.
Test	<p>Use the following command for each of the desired user ids:</p> <pre># grep <user id> /etc/passwd</pre> <p>where <user id> is replaced with one of the following each time: named, smmsp. The result should look something like this:</p> <pre># grep named /etc/passwd named:x:25:25:Named:/var/named:/sbin/nologin</pre> <pre># grep smmsp /etc/passwd smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin</pre> <p>Each account should have the “/sbin/nologin entry at the end of the line. This is used by the Pluggable Authentication Module (PAM) system to check for login permission.</p> <p>As an additional step that offers more granular control over login access</p>

	<p>permissions, you can use the <code>/etc/security/access.conf</code> file. Use the following command to review the entries in the file:</p> <pre># more /etc/security/access.conf</pre> <p>Depending on the organization's security policies and standards, there may or may not be restrictions on which accounts can log in at particular locations. For example, you may want to limit console access to <code>root</code> only, and also not allow the <code>named</code> and <code>smmsp</code> accounts to log in at all. The entries in the file would be:</p> <pre>-:ALL EXCEPT root:LOCAL -:named smmsp:ALL</pre> <p>In order for the entries to be used by PAM, you also need to review the <code>/etc/pam.d/login</code> file and see if the following entry exists. If it does not exist, it needs to be added.</p> <pre>account required /lib/security/pam_access.so</pre> <p>Also attempt to login as one of the user ids to see how the system responds. It should not allow access.</p>
O/S	Subjective: This step depends on the policies and standards of the organization.
Identifier	O4
Objective	Check for synchronization of system time to NTP service.
Reference	[SANS – 00] and original contribution
Risk	Inaccurate system time makes coordinating events between different devices and examining forensic evidence difficult.
Compliance	Is the system synchronizing time with an NTP server? If not, the system is not compliant.
Test	<p>Ask the system administrator if the system is using NTP in some form to set the system time. It is not necessary for the system to run the NTP daemon to keep accurate time. An hourly cronjob to sync the time to an NTP server is sufficient.</p> <p>Verify the status of the <code>ntp</code> daemon by using the <code>ps</code> command to see if is running.</p> <pre># ps -ef grep ntpd root 8889 7506 0 15:04 pts/0 00:00:00 grep ntpd</pre>
O/S	Objective: Either the system time is synchronized with NTP or it is not.
Identifier	O5

Objective	Check for xinetd services and turn off xinetd daemon.
Reference	[SANS – 00] and original contribution
Risk	The Extended Internet Services Daemon (xinetd) starts network services on request. Services that start only when asked to are unnecessary on a DNS/SMTP server and should be disabled to eliminate unauthorized access or perform a denial-of-service on the server.
Compliance	Are there any services configured to start via xinetd and is the xinetd daemon running? If not, the system is not compliant.
Test	<p>Review all of the files in the <code>/etc/xinetd.d/</code> directory. Each service should be disabled by having the entry <code>disable = yes</code> in the file. Verify that the xinetd daemon is not running by using the <code>ps -ef</code> command. To see if the xinetd daemon is configured to start, use the <code>chkconfig</code> command.</p> <pre># ps -ef grep xinetd root 8889 7506 0 15:04 pts/0 00:00:00 grep xinetd # chkconfig --list xinetd xinetd 0:off 1:off 2:off 3:off 4:off 5:off 6:off</pre>
O/S	Objective: Either the services and the xinetd daemon are disabled or they are not.
Identifier	O6
Objective	Check to see what network services are running.
Reference	[SANS – 00] and original contribution
Risk	Unnecessary services always provide attackers additional ways to gain unauthorized access or perform a denial-of-service on the server.
Compliance	Are any unnecessary network services running? If so, the system may not be compliant.
Test	<p>There are several ways to test this step. The best way, if the utility is available on the system, is to use the <code>lsof</code> command. This command lists all open files, and in our case, the network sockets in use and the programs that have them opened. You can also use the <code>netstat</code> command to list the open sockets if <code>lsof</code> is not available. Depending on the version of <code>netstat</code>, it may display the programs that are associated with the open sockets. Check for the availability of the “p” option.</p> <p>The <code>lsof</code> command:</p> <pre># lsof -i +M</pre>

The results will look similar to this:

```
# lsof -i +M
COMMAND  PID  USER  FD  TYPE  DEVICE  SIZE  NODE  NAME
named    2735  named  6u  IPv4  3078      UDP *:32769
named    2735  named  7u  IPv4  3074      UDP bob:domain
named    2735  named  8u  IPv4  3075      TCP bob:domain (LISTEN)
named    2735  named  9u  IPv4  3076      UDP 10.10.6.25:domain
named    2735  named 10u  IPv4  3077      TCP 10.10.6.25:domain
(LISTEN)
named    2735  named 11u  IPv4  3079      TCP bob:rndc (LISTEN)
sendmail 2782  root   4u  IPv4  3170      TCP bob:smtp (LISTEN)
```

The netstat command:

```
# netstat -anp
```

The results will look similar to this:

```
# netstat -anp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 127.0.0.1:32769         0.0.0.0:*               LISTEN
2764/xinetd
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN
2750/sshd
tcp        0      0 127.0.0.1:631          0.0.0.0:*               LISTEN
32642/cupsd
udp        0      0 0.0.0.0:32768          0.0.0.0:*               2631/
udp        0      0 0.0.0.0:32772          0.0.0.0:*               8846/
udp        0      0 0.0.0.0:687            0.0.0.0:*               2631/

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State       I-Node
PID/Program name  Path
unix    2      [ ACC ]     STREAM    LISTENING   3188
2802/gpm          /dev/gpmctl
unix    4      [ ]       DGRAM                    69643
8790/syslogd      /dev/log
unix    2      [ ]       DGRAM                    69651
8794/klogd
unix    2      [ ]       DGRAM                    56142 8211/
```

	<pre> unix 2 [] DGRAM 3206 2811/crond unix 2 [] DGRAM 3104 2764/xinetd </pre>
O/S	Subjective: Each organization will require different services depending on their policies and standards.
Identifier	O7
Objective	If remote administrative access is required, use <code>ssh</code> instead of <code>telnet</code> or <code>rlogin/rsh/rcp</code> .
Reference	[SANS – 00] and original contribution
Risk	The standard Unix remote access utilities of <code>telnet</code> and <code>rlogin</code> are not adequate in any environment today. <code>Telnet</code> and <code>rlogin</code> send passwords in clear-text over the network. All authentication for remote access should at least be encrypted, and strong, two-factor authentication should be considered for mission-critical systems.
Compliance	Is <code>ssh</code> installed and running? Is it the latest version or is there a valid reason why it is not the latest version? If not, the system is not compliant.
Test	<p>Check to see if <code>ssh</code> is installed and that it is the latest version. If using OpenSSH, check their web site at http://www.openssh.org/ to get the latest released version. Since OpenSSH depends on other applications for use, such as Zlib and OpenSSL, you will need to update those applications also.</p> <p>You can check the version of the OpenSSH server by executing the daemon with an invalid option.</p> <pre> sshd -v sshd: illegal option -- v sshd version OpenSSH_3.5p1 Usage: sshd [options] </pre> <p>For other distributions of <code>ssh</code>, please check with the vendor of the application.</p>
O/S	Objective and Subjective: The use of <code>ssh</code> is easy to judge objectively, but it may be implemented improperly and may not provide sufficient protection. This requires comparison with the organization's policies and standards and is therefore subjective.

2.8 DNS Checklist

This checklist provides the steps that should be performed when auditing the DNS service as implemented using the BIND implementation developed and maintained by the Internet Software Consortium.

Table 6 –DNS Checklist

Identifier	D1
Objective	Check version of BIND distribution.
Reference	[Albitz – 01], [CERT – 02] and original contribution
Risk	Older versions of the BIND distribution have vulnerabilities. It is normally best to run the latest version of the BIND distribution. There are some circumstances where an older version of the software may be required for backward compatibility. In those cases, apply any patches that can be applied to the existing distribution and try to eliminate the reason for the backward compatibility.
Compliance	Is BIND the latest version or is there a valid reason why it is not the latest version? If not, the system is not compliant.
Test	You can usually ask the named program to tell you the version with this command: # named -v The program should respond with a version number and other information, depending on the version.
O/S	Objective and Subjective: The BIND distribution in most cases should be the most current version available. However, the organization may have reasons for running an older version.
Identifier	D2
Objective	Review single points of failure in DNS system design.
Reference	[Albitz – 01], [CERT – 02] and original contribution
Risk	Failure of one component or communications link can cause unavailability of the service or an unintended denial-of-service.
Compliance	Are there single points of failure in the design that could be eliminated with a reasonable effort and cost? If not, the system may not be compliant.
Test	Review DNS system design for single points of failure. Some of these include installing multiple name servers at different physical locations on separate subnets, using the ISP as a slave server, and installing multiple paths to the Internet for the organization.

O/S	Subjective: Elimination of all single points of failure is cost-prohibitive for most organizations. However, if there are simple things that can be done at low cost to reduce this risk, they should be implemented.
Identifier	D3
Objective	Review use of split namespace.
Reference	[Albitz – 01], [CERT – 02] and original contribution
Risk	Improper design of the DNS system will expose internal naming information that should not be exposed to the Internet.
Compliance	Is BIND configured to use a split namespace to reduce exposure of internal naming information? If not, the system is not compliant.
Test	<p>Review DNS system design to determine if split namespace is being used. For BIND 9, the use of views is the easiest way to implement this feature. In the <code>named.conf</code> file, look for statements similar to these:</p> <pre>view "internalview" { match-clients { internal; }; recursion yes; }; view "externalview" { match-clients { any; }; recursion no; };</pre> <p>Test the server by querying for a known internal name from the Internet. The name should not resolve.</p>
O/S	Objective and Subjective: The use of split namespace is objective but the organization may have valid reasons for not using it, so the step is also subjective.
Identifier	D4
Objective	Review dynamic updates and transaction signatures (TSIG) configuration and use for server-to-server communications.
Reference	[Albitz – 01], [CERT – 02], [ISC-01] and original contribution

Risk	Modern DNS servers can use dynamic updates to maintain accurate namespaces, but access controls need to be in place to make sure the updates are not malicious. TSIG provides authentication and data integrity for server-to-server communications such as dynamic updates and zone transfers. Note that this does not encrypt the data, it simply verifies that the two servers are talking to each other and not an imposter.
Compliance	If dynamic updates are required, then TSIG is mandatory. If dynamic updates are not required, then TSIG is recommended, but not required. If these conditions are not met, the system is not compliant.
Test	Review DNS system configuration to determine if dynamic updates are configured and if TSIG is being used. Look for entries similar to these in the <code>named.conf</code> file: <pre>key ns1-isp.example.com. { algorithm hmac-md5; secret "mZiMNOUYQPMNwsDzrX2ENw=="; }; zone "example.com" { type master; file "db.example.com"; allow-transfer { key ns1-isp.example.com; }; };</pre>
O/S	Objective: If dynamic updates are required, then TSIG is required. If dynamic updates are disabled, then TSIG is optional.
Identifier	D5
Objective	Review configuration of query restrictions for internal namespace.
Reference	[Albitz – 01], [CERT – 02], [ISC-01] and original contribution
Risk	BIND 8 and 9 allow the creation of ACLs to limit what IP addresses can make queries to a particular zone or entire server.
Compliance	Internal names should only be available to internal hosts. If an external host is able to resolve an internal name, then the system is not compliant.

Test	<p>Review DNS system configuration to determine if queries to the internal zones are limited to internal hosts. Also attempt to query DNS server for an internal server name. Look for entries similar to these in the <code>named.conf</code> file:</p> <pre>acl internal { 192.168.4.0/24; }; view "internalview" { match-clients { internal; }; recursion yes; };</pre>
O/S	Objective: Either internal zones are limited to internal hosts or they are not.
Identifier	D6
Objective	Review configuration for unauthorized zone transfers.
Reference	[Albitz – 01], [CERT – 02] and original contribution
Risk	BIND 8 and 9 provide the “allow-transfer” parameter to limit which IP addresses are able to receive DNS zone transfers.
Compliance	Zone transfers must be restricted to specific IP addresses. If not, the system is not compliant.
Test	<p>Review DNS system configuration to determine if zone transfers are limited to desired IP addresses. Also attempt to perform a zone transfer from an unauthorized host. Look for the “allow-transfer” parameter in <code>named.conf</code>:</p> <pre>allow-transfer { 192.168.4.20; };</pre>
O/S	Objective: Either zone transfers are limited to specific IP addresses or they are not.
Identifier	D7
Objective	Review configuration for least privilege and chroot environment.
Reference	[Albitz – 01], [CERT – 02], [SANS-00] and original contribution
Risk	BIND 8.1.2 and above provide the option to run the DNS server with least privilege. This option eliminates the need to have the DNS server run with root privileges. In addition, it is also possible to configure the DNS server to operate with a limited view of the filesystem (known as <code>chroot</code> , named after the Unix system call that performs the function), which limits the exposure to an attacker if the DNS server is compromised.

Compliance	Is the DNS server running with least privilege and is it running from a chrooted environment? If not, the system is not compliant.
Test	<p>Review DNS system configuration to determine if the DNS server is configured to run with least privilege and in a chroot environment. Verify that the least privileged account is running the DNS server and then check the privileges of that account. Run the following commands on the DNS server host and review the response. The named process should be owned by a user other than root and the user entry in the password file should not have a uid of zero (0).</p> <pre># ps -ef grep named named 2736 1 0 May13 ? 00:00:00 [named] # grep named /etc/passwd named:x:25:25:Named:/var/named:/sbin/nologin</pre> <p>To check for the chroot environment, restart the DNS server and review the system log to verify that the daemon is using the “-t” option for chroot.</p> <pre>Jun 10 17:59:23 bob named[8665]: starting BIND 9.2.1 -u named -t /var/named Jun 10 17:59:23 bob named[8665]: using 1 CPU Jun 10 17:59:23 bob named[8665]: loading configuration from '/etc/named.conf' Jun 10 17:59:24 bob named[8665]: no IPv6 interfaces found.</pre>
O/S	Objective: Either the DNS server is configured for least privilege and chroot or it is not.
Identifier	D8
Objective	Review measures for preventing cache poisoning.
Reference	[Albitz – 01], [CERT – 02] and original contribution
Risk	Cache poisoning occurs when a DNS server caches incorrect data for a domain name. This can result in denial-of-service or man-in-the-middle attacks.
Compliance	Is the DNS server configured to help prevent cache poisoning? If not, the system is not compliant.

Test	<p>Review DNS system configuration to determine if the following areas in the <code>named.conf</code> file are configured properly.</p> <ul style="list-style-type: none"> • Disable recursion for all external queries. • Enable recursion for internal queries if DNS server is configured for a split namespace. • If DNS server is BIND 9, restricting recursion by defining internal and external views (shown in D3). • Turning off “glue fetching” for BIND 8 and earlier.
O/S	Objective: Either the DNS server is configured to reduce the risk of cache poisoning or it is not.

2.9 SMTP Checklist

This checklist provides the steps that should be taken when auditing an SMTP server that uses the Sendmail distribution developed and maintained by the Sendmail Consortium.

Table 7 –SMTP Checklist

Identifier	S1
Objective	Check version of SMTP server distribution.
Reference	[Costales – 03] and original contribution
Risk	Older versions of the Sendmail distribution have vulnerabilities. It is normally best to run the latest version of the Sendmail distribution. There may be some circumstances where an older version of the software may be required for backward compatibility. In those cases, apply any patches that can be applied to the existing distribution and try to eliminate the reason for the backward compatibility.
Compliance	Is the sendmail program the current version, and if not, is there a valid reason why it is not the latest version? If not, the system is not compliant.
Test	<p>On the Sendmail server, issue the following command:</p> <pre># /usr/sbin/sendmail -d0.1 -bt < /dev/null</pre> <p>The program should respond with a version number and other information, depending on the version.</p>
O/S	Objective and Subjective: The Sendmail distribution in most cases should be the most current version available, however, the organization may have reasons for running an older version.
Identifier	S2

Objective	Review single points of failure in SMTP system design.
Reference	Original contribution
Risk	Failure of one component or communications link can cause unavailability of the service or an unintended denial-of-service.
Compliance	Are there single points of failure in the design that could be eliminated with a reasonable effort and cost? If not, the system may not be compliant.
Test	Review SMTP system design for single points of failure. The SMTP protocol is more forgiving of communications failures and server downtime than DNS. For example, SMTP servers will normally queue messages for later delivery in the case of a communication line failure. However, it is important for the system design to have adequate business continuity planning and backup servers available.
O/S	Subjective: Elimination of all single points of failure is cost-prohibitive for most organizations. However, if there are simple things that can be done at low cost to reduce this risk, they should be implemented.
Identifier	S3
Objective	Review set-user-id root for sendmail.
Reference	[Costales – 03] and original contribution
Risk	In the past, many exploits targeted sendmail because it was a set-user-id program, that is, it ran with root privileges regardless of which user id started it. Beginning with version 8.12, sendmail by default is no longer installed as a set-user-id program.
Compliance	Is the sendmail program installed with set-user-id privileges? If so, the system is not compliant.
Test	<p>Review the file permissions on the sendmail binary. Typically, this is <code>/usr/sbin/sendmail</code> or <code>/usr/lib/sendmail</code>. In the case of RedHat 9.0, the alternatives package is used, so the actual sendmail binary is <code>/usr/lib/sendmail.sendmail</code>. The file permissions should be set-group-id to allow e-mail submitted via the command line on the server to be written to the queue directory. The group should be the same group that owns the <code>/var/spool/clientmqueue</code> directory, by default <code>smmsp</code>.</p> <p>To test, use the <code>ls</code> command to determine the file permissions. The result should be similar to the following:</p> <pre># ls -l /usr/sbin/sendmail.sendmail -r-xr-sr-x 1 root smmsp 3859419 Feb 24 17:15 sendmail.sendmail</pre> <p>If there is an "s" in the fourth position of the permissions list, as shown</p>

	<p>below, the sendmail binary is installed set-user-id and, if the owner is root, vulnerable to attack.</p> <pre># ls -l /usr/sbin/sendmail.sendmail -r-sr-sr-x 1 root smmsp 3859419 Feb 24 17:15 sendmail.sendmail</pre>
O/S	Subjective: Either the sendmail program has the proper file permissions or it does not.
Identifier	S4
Objective	Review set effective user and group id system call support.
Reference	[Costales – 03] and original contribution
Risk	It is still a requirement for sendmail to run as root to perform several functions, such as ~/.forward files, certain mailing list programs, and others. By using the proper system calls, this process is done as safely as possible.
Compliance	Is sendmail compiled with the proper system calls available? If not, the system is not compliant.
Test	<p>Review the operating system defines in the sendmail binary to determine which system calls are used for effective user and group id system calls. The preferred calls are the <code>setreuid</code> and <code>setregid</code> system calls because it allows transfer of both the real and effective user ids to the temporary process. If the <code>seteuid</code> and <code>setegid</code> system calls are listed instead, verify that they are Posix-compliant calls. Most modern Unix implementations either have the <code>setreuid</code> and <code>setregid</code> system calls or their <code>seteuid</code> and <code>setegid</code> system calls are Posix-compliant.</p> <p>On the sendmail server, issue the following command:</p> <pre># /usr/sbin/sendmail -d0.10 -bt < /dev/null</pre> <p>The program should respond with results similar to the following:</p> <pre>Compiled with: DNSMAP HESIOD HES_GETMAILHOST LDAPMAP LOG MAP_REGEX MATCHGECOS MILTER MIME7TO8 MIME8TO7 NAMED_BIND NETINET NETINET6NETUNIX NEWDB NIS PIPELINING SASL SCANF STARTTLS TCPWRAPPERS USERDB USE_LDAP_INIT OS Defines: ADDRCONFIG_IS_BROKEN HASFCHOWN HASFCHMOD HASFLOCK HASRANDOM HASGETDTABLESIZE HASINITGROUPS HASLSTAT HASNICE HASRRESVPORT HASSETREGID HASSETREUID HASSETRLIMIT HASSETSID HASSETVBUF HASURANDOMDEV HASSTRERROR HASUNAME HASUNSETENV HASWAITPID IDENTPROTO NEEDSGETIPNODE REQUIRES_DIR_FSYNC</pre>

	<p>USE_DOUBLE_FORK USE_SIGLONGJMP</p> <p>Verify that the variables HASSETREUID and HASSETREGID or HASSETEUID and HASSETEGID are listed in the "OS Defines" section. If HASSETEUID and HASSETEGID are listed, verify that the system calls are Posix-compliant.</p>
O/S	Objective: The proper system calls are available or they aren't.
Identifier	S5
Objective	Review environmental variables available for delivery agent.
Reference	[Costales – 03] and original contribution
Risk	Older versions of sendmail were vulnerable to environmental variable changes that affected the delivery agent's operation. Beginning with version 8.7 of sendmail, the delivery agent's environment is built from within the sendmail configuration and not from the external variables.
Compliance	Is the sendmail program passing the minimal number of environment variables? If not, the system is not compliant.
Test	<p>Review sendmail configuration to verify that the version is greater than 8.7 and that the environment variables available to the delivery agent(s) are limited.</p> <p>On the sendmail server, issue the following command:</p> <pre># /usr/sbin/sendmail -d0.15 -bt < /dev/null</pre> <p>The program should respond with results similar to the following:</p> <pre>mailer 0 (prog): P=/usr/sbin/smrsh S=EnvFromL/HdrFromL R=EnvToL/HdrToL M=0 U=0:0 F=9DFMeloqsu L=0 E=\n T=X-Unix/X- Unix/X-Unix r=100 A=smrsh -c \$u mailer 1 (*file*): P=[FILE] S=parse/parse R=parse/parse M=0 U=0:0 F=9DEFMPloqsu L=0 E=\n T=X-Unix/X-Unix/X-Unix r=100 A=FILE \$u mailer 2 (*include*): P=/dev/null S=parse/parse R=parse/parse M=0 U=0:0 F=su L=0 E=\n T=<undefined>/<undefined>/<undefined> r=100 A=INCLUDE \$u mailer 3 (smtp): P=[IPC] S=EnvFromSMTP/HdrFromSMTP R=EnvToSMTP/EnvToSMTP M=0 U=0:0 F=DFMXmu L=990 E=\r\n T=DNS/RFC822/SMTP r=100 A=TCP \$h</pre> <p>Review each of the "mailer" lines and verify that the "E" variable is defined. In most cases, it will be set to a newline character, but on some operating systems and mailers, the ISP and SYSTYPE variables may be defined.</p>
O/S	Objective: Either the environment to the delivery agents is limited or it is not.

Identifier	S6
Objective	Review SMTP Debug setting.
Reference	[Costales – 03]
Risk	The SMTP protocol has an option to allow remote debugging of sendmail servers. Remote users can view the contents of the mail queue when this option is enabled. This should be disabled when the program is compiled for production release.
Compliance	Is the SMTP Debug command disabled? If not, the system is not compliant.
Test	<p>Try and enable debug mode on the server. On the server, do the following:</p> <pre># telnet localhost 25</pre> <p>The server will respond with something similar to the following string: Trying 127.0.0.1...</p> <pre>Connected to localhost. Escape character is '^]'. 220 localhost.localdomain ESMTP Sendmail 8.12.8/8.12.8; Mon, 9 Jun 2003 07:11:05 -0600</pre> <p>Next, type the word “debug”.</p> <pre>debug</pre> <p>If the program responds with something similar to the following, the SMTPDEBUG is not defined and the system passes this test.</p> <pre>500 5.5.1 Command unrecognized: "debug"</pre> <p>On the other hand, if the system responds with something similar to this, SMTPDEBUG is enabled and the system fails this test.</p> <pre>200 2.0.0 Debug set</pre> <p>Type “quit” to exit the sendmail program.</p> <pre>quit 221 2.0.0 localhost.localdomain closing connection Connection closed by foreign host. #</pre>
O/S	Objective: Either SMTP Debug is disabled or it is not.
Identifier	S7
Objective	Review configuration of sendmail PrivacyFlags option and the SMTP <code>vrfy</code> and <code>expn</code> commands.
Reference	[Costales – 03], [SANS-00] and original contribution

Risk	<p>SMTP provides commands for remote systems to determine the e-mail address of a particular user or groups of users on an SMTP server. This functionality is used by intruders to determine if a particular username is being used on the server and then the password can be brute-forced to gain access.</p> <p>Use of these commands is primarily controlled by the PrivacyOptions option in the sendmail configuration file. Newer versions of sendmail (versions 8.10 and higher) allow the creation of selective lists of hosts that can use <code>vrfy</code> and <code>expn</code>. In general, however, it is recommended that these services be completely disabled.</p> <p>There are other options for the PrivacyOptions option that limit information exposure and control access. It is recommended that the most restrictive options (<code>goaway</code>, <code>restrictmailq</code>, <code>restrictqrun</code>) be used to start with, and to ease restrictions if necessary. Goaway includes <code>novrfy</code> and <code>noexpn</code>.</p>
Compliance	Are the PrivacyOptions set to at least disable the <code>vrfy</code> and <code>expn</code> commands? If not, the system is not compliant.
Test	<p>On the sendmail server, locate the active sendmail configuration (sendmail.cf) file. On RedHat 9, this location is <code>/etc/mail/sendmail.cf</code>. Use the following command to determine the settings of the PrivacyOptions option.</p> <pre># grep PrivacyOptions /etc/mail/sendmail.cf O PrivacyOptions=authwarnings,novrfy,noexpn,restrictqrun #</pre> <p>Verify that either the "goaway" option is listed or that the options "novrfy" and "noexpn" are listed.</p>
O/S	Objective and Subjective: Either and are disabled or they are not. Other options are dependent on the policies and standards.
Identifier	S8
Objective	Review use of the "F" command in the configuration file.
Reference	[Costales – 03] and original contribution
Risk	Improper use of the "F" command can permit unintended files to be read and interpreted. The "F" command in conjunction with the " " (pipe) prefix to a path can be used to execute external programs.
Compliance	Do the "F" commands in the configuration file point to full paths and files with no " " (pipe) characters? If so, the system is compliant.

Test	<p>On the sendmail server, use the following command to determine how the "F" command is used in the configuration file:</p> <pre># grep "^F" /etc/mail/sendmail.cf Fw/etc/mail/local-host-names FR-o /etc/mail/relay-domains Ft/etc/mail/trusted-users #</pre> <p>Verify that all of the F options are reading full file names with no wildcard characters and that there is no use of the " " (pipe) prefix in front of any of the file names.</p>
O/S	Objective: Either the "F" command is used properly or it is not.
Identifier	S9
Objective	Review use of the "P=" command in the configuration file.
Reference	[Costales – 03] and original contribution
Risk	Improper configuration of the delivery agent definitions can cause the agents to run improper programs with elevated privileges.
Compliance	Are the "P=" commands configured properly? If not, the system is not compliant.
Test	<p>Since the delivery agent definitions are on multiple lines, we cannot use grep to extract the particular lines of interest. On the sendmail server, review the sections of the configuration file that have "P=" in the line. In particular, check to see if the delivery agents have options such as "U=0" or "F=S" in the definitions. These options allow the delivery agent to run as root. Also make sure the paths to any local executables, such as mail or procmail, are the actual paths to the trusted executables. Here are two examples of delivery agent definitions.</p> <pre>Msmtp, P=[IPC], F=mDFMuX, S=EnvFromSMTP/HdrFromSMTP, R=EnvToSMTP, E=\r\n, L=990, T=DNS/RFC822/SMTP, A=TCP \$h Mlocal, P=/usr/bin/procmail, F=lsDFMAw5:/ @qSPfhn9, S=EnvFromL/HdrFromL, R=EnvToL/HdrToL, T=DNS/RFC822/X-Unix, A=procmail -t -Y -a \$h -d \$u</pre>

O/S	Objective: Either the "P=" commands are configured properly or they are not.
Identifier	S10
Objective	File and directory permissions.
Reference	[Costales – 03] and original contribution
Risk	Improper file and directory permissions can allow undesired access to root-owned configuration and executable files. This is true for all system files, not just sendmail-related files, but since sendmail runs as root during startup, it is of particular concern for sendmail.
Compliance	Are the file and directory permissions set to those listed in the Test? If not, the system is not compliant.
Test	<p>The queue file permissions are controlled by setting the TempFileMode and QueueFileMode options in the configuration files. For the MTA daemon, the configuration file is named submit.cf and is usually in the same directory as the sendmail.cf file.</p> <p>On the sendmail server, use the following command to determine how the TempFileMode and QueueFileMode options are set in each configuration file:</p> <pre># grep "FileMode" /etc/mail/sendmail.cf #O QueueFileMode=0600 O TempFileMode=0600 # grep "FileMode" /etc/mail/submit.cf O QueueFileMode=0660 O TempFileMode=0600 #</pre> <p>Verify that the permissions correspond with the settings recommended for the queue files in the table below.</p> <p>There are several files and directories that should be checked for proper permissions. The following list is from [Costales – 03] and is applicable to sendmail versions 8.12 and higher.</p> <p>The "F/path" and "/path/file" entries refer to the files defined by the "F" command in the configuration file that were reviewed earlier. The "include" entries refer to those files which may be included in an /etc/aliases file for mailing list purposes. The owner is listed as either a system username or as a T or R. T refers to the TrustedUser</p>

	<p>option and R refers to the RunAsUser option. These are defined in the sendmail configuration file. When the group ownership is important, the group is also defined with the “:name” convention.</p> <table><tr><th>Path</th><th>Type</th><th>Owner</th><th>Mode</th></tr><tr><td>/</td><td>Directory</td><td>root</td><td>0755</td></tr><tr><td>/usr</td><td>Directory</td><td>root</td><td>0755</td></tr><tr><td>/usr/sbin</td><td>Directory</td><td>root</td><td>0755</td></tr><tr><td>/usr/sbin/sendmail</td><td>File</td><td>root:smmsp</td><td>02555</td></tr><tr><td>/etc</td><td>Directory</td><td>root</td><td>0755</td></tr><tr><td>/etc/mail</td><td>Directory</td><td>root, T</td><td>0755</td></tr><tr><td>/etc/mail/sendmail.cf</td><td>File</td><td>root, T</td><td>0644 or 0640</td></tr><tr><td>/etc/mail/statistics</td><td>File</td><td>root, T, R</td><td>0600</td></tr><tr><td>/etc/mail/helpfile</td><td>File</td><td>root, T</td><td>0444</td></tr><tr><td>/etc/mail/aliases</td><td>File</td><td>root, T</td><td>0644</td></tr><tr><td>/etc/mail/aliases.pag</td><td>File</td><td>root, T, R</td><td>0640</td></tr><tr><td>/etc/mail/aliases.dir</td><td>File</td><td>root, T, R</td><td>0640</td></tr><tr><td>/etc/mail/aliases.db</td><td>File</td><td>root, T, R</td><td>0640</td></tr><tr><td>F/path</td><td>Directory</td><td>root, T</td><td>0755</td></tr><tr><td>/path/file</td><td>File</td><td>T</td><td>0444 or 0644</td></tr><tr><td>/var</td><td>Directory</td><td>root</td><td>0755</td></tr><tr><td>/var/spool</td><td>Directory</td><td>root</td><td>0755</td></tr><tr><td>/var/spool/mqueue</td><td>Directory</td><td>root, R</td><td>0700</td></tr><tr><td>/var/spool/mqueue/files</td><td>Files</td><td>root</td><td>0600</td></tr><tr><td>/var/spool/clientmqueue</td><td>Directory</td><td>smmsp:smmsp</td><td>0770</td></tr><tr><td>/var/spool/clientmqueue/files</td><td>Files</td><td>smmsp:smmsp</td><td>0660</td></tr><tr><td>:include:/path</td><td>Directories</td><td>root</td><td>0755</td></tr><tr><td>:include:/path/list</td><td>File</td><td>n/a</td><td>0644</td></tr><tr><td>~/forward</td><td>File</td><td>Root or user</td><td>0600</td></tr></table>	Path	Type	Owner	Mode	/	Directory	root	0755	/usr	Directory	root	0755	/usr/sbin	Directory	root	0755	/usr/sbin/sendmail	File	root:smmsp	02555	/etc	Directory	root	0755	/etc/mail	Directory	root, T	0755	/etc/mail/sendmail.cf	File	root, T	0644 or 0640	/etc/mail/statistics	File	root, T, R	0600	/etc/mail/helpfile	File	root, T	0444	/etc/mail/aliases	File	root, T	0644	/etc/mail/aliases.pag	File	root, T, R	0640	/etc/mail/aliases.dir	File	root, T, R	0640	/etc/mail/aliases.db	File	root, T, R	0640	F/path	Directory	root, T	0755	/path/file	File	T	0444 or 0644	/var	Directory	root	0755	/var/spool	Directory	root	0755	/var/spool/mqueue	Directory	root, R	0700	/var/spool/mqueue/files	Files	root	0600	/var/spool/clientmqueue	Directory	smmsp:smmsp	0770	/var/spool/clientmqueue/files	Files	smmsp:smmsp	0660	:include:/path	Directories	root	0755	:include:/path/list	File	n/a	0644	~/forward	File	Root or user	0600
Path	Type	Owner	Mode																																																																																																		
/	Directory	root	0755																																																																																																		
/usr	Directory	root	0755																																																																																																		
/usr/sbin	Directory	root	0755																																																																																																		
/usr/sbin/sendmail	File	root:smmsp	02555																																																																																																		
/etc	Directory	root	0755																																																																																																		
/etc/mail	Directory	root, T	0755																																																																																																		
/etc/mail/sendmail.cf	File	root, T	0644 or 0640																																																																																																		
/etc/mail/statistics	File	root, T, R	0600																																																																																																		
/etc/mail/helpfile	File	root, T	0444																																																																																																		
/etc/mail/aliases	File	root, T	0644																																																																																																		
/etc/mail/aliases.pag	File	root, T, R	0640																																																																																																		
/etc/mail/aliases.dir	File	root, T, R	0640																																																																																																		
/etc/mail/aliases.db	File	root, T, R	0640																																																																																																		
F/path	Directory	root, T	0755																																																																																																		
/path/file	File	T	0444 or 0644																																																																																																		
/var	Directory	root	0755																																																																																																		
/var/spool	Directory	root	0755																																																																																																		
/var/spool/mqueue	Directory	root, R	0700																																																																																																		
/var/spool/mqueue/files	Files	root	0600																																																																																																		
/var/spool/clientmqueue	Directory	smmsp:smmsp	0770																																																																																																		
/var/spool/clientmqueue/files	Files	smmsp:smmsp	0660																																																																																																		
:include:/path	Directories	root	0755																																																																																																		
:include:/path/list	File	n/a	0644																																																																																																		
~/forward	File	Root or user	0600																																																																																																		
O/S	Objective: Either the directories and files have the proper permissions or they do not.																																																																																																				
Identifier	S11																																																																																																				
Objective	Review use of the “DontBlameSendmail” command in the configuration file.																																																																																																				

Reference	[Costales – 03] and original contribution
Risk	System management policies should not be enforced using exceptions to the default configuration of the “DontBlameSendmail” command. Current versions of sendmail (version 8.12 and above) are very restrictive regarding file and directory permissions. Sometimes system administrators use the “DontBlameSendmail” command to allow group management of alias files without breaking the functionality of sendmail. It is recommended that other mechanisms be used to provide the desired functionality and that the “DontBlameSendmail” command be left undefined.
Compliance	Is the “DontBlameSendmail” variable undefined or set to “Safe”? If not, the system is not compliant.
Test	On the sendmail server, use the following command to determine how the “DontBlameSendmail” command is used in the configuration file: <pre># grep "DontBlameSendmail" /etc/mail/sendmail.cf #O DontBlameSendmail=safe #</pre>
O/S	Objective: Either the “DontBlameSendmail” command is configured properly or it is not.
Identifier	S12
Objective	Review aliases file for decode and other executable files.
Reference	[Costales – 03] and original contribution
Risk	The sendmail aliases file can define an executable program to be run when mail for a particular alias arrives. This can create opportunities for intruders to e-mail malicious code to an alias and have the code executed on the sendmail server.
Compliance	Is the “decode” alias set to execute the program and are there any aliases that have executable resolution? If so, the system is not compliant.

Test	<p>On the sendmail server, use the following command to determine how the "decode" alias is defined and if any executables are defined:</p> <pre># grep decode /etc/aliases # trap decode to catch security attacks decode: root # grep " " /etc/aliases #</pre>
O/S	Objective: Either the aliases file is configured properly or it is not.
Identifier	S13
Objective	Review configuration file for Trusted Users as defined by the "T" command, the /etc/mail/trusted-users file, the "RunAs" option (versions 8.8 and above) and the TrustedUser option (versions 8.10 and above).
Reference	[Costales – 03] and original contribution
Risk	The sendmail program only allows users as defined by the "T" command, the /etc/mail/trusted-users file, and the TrustedUser option (in version 8.10 and above) to rebuild the alias database. If ordinary users could rebuild the alias database, they could insert malicious code that would be executed when mail was sent to a particular user. The "RunAs" option is available, but not normally used when running versions 8.12 or above. If it is used, it should be set to an unprivileged user such as smmsp or sendmail.
Compliance	Are the "T" commands, the "RunAs" option, and the "TrustedUser" option set properly? If not, the system is not compliant.
Test	<p>On the sendmail server, use the following commands to determine which users are defined as trusted:</p> <pre># grep "^T" /etc/mail/sendmail.cf Troot Tdaemon Tuucp # cat /etc/mail/trusted-users # trusted-users - users that can send mail as others without a warning # apache, mailman, majordomo, uucp, are good candidates # grep RunAs sendmail.cf #O RunAsUser=sendmail</pre>

	<pre># grep "TrustedUser" /etc/mail/sendmail.cf O TrustedUser=smmisp #</pre> <p>Verify that the trusted users don't include ordinary or untrusted users. In most cases, root and daemon are the only ones listed with the "T" option or in the <code>/etc/mail/trusted-users</code> file, and for versions 8.12 and higher, smmisp should be defined with the "TrustedUser" option. The "RunAs" option is disabled with a comment in this example.</p>
O/S	Objective and Subjective: Minimizing the trusted users is the goal, but some sites may have legitimate needs for additional trusted users.
Identifier	S14
Objective	Review LogLevel option in configuration file.
Reference	[Costales – 03] and original contribution
Risk	The sendmail program can log a wide variety of information during its operation. The level is defined from 0 to 98 with the verbosity increasing with the level. For security purposes, it is desirable to log both sides of all SMTP conversations. The minimum level for this level of log information is 12.
Compliance	Is the LogLevel option set to at least 12? If not, the system may not be compliant.
Test	<p>On the sendmail server, use the following command to determine the logging level:</p> <pre># grep LogLevel /etc/mail/sendmail.cf O LogLevel=9 #</pre> <p>Verify that the logging level is sufficient to meet security policies and standards.</p>
O/S	Subjective: Increased logging is usually better, but if there is not a policy of reviewing log files, the data is of little use.
Identifier	S15
Objective	Review SafeFileEnvironment option in configuration file.
Reference	[Costales – 03] and original contribution

Risk	The SafeFileEnvironment option provides additional protection for mail delivery to regular files only. If it is defined with a "/", it protects writing mail to devices and directories. If it defined with a "/path" it will only deliver mail to regular files underneath that path (using chroot).
Compliance	Is the SafeFileEnvironment option set to at least the "/"? If not, the system may not be compliant.
Test	<p>On the sendmail server, use the following command to determine the SafeFileEnvironment option:</p> <pre># grep SafeFileEnvironment /etc/mail/sendmail.cf O SafeFileEnvironment=/ #</pre> <p>Verify that the SafeFileEnvironment option is set according to policies and standards.</p>
O/S	<p>Subjective: Security is improved at the cost of an additional administrative function to make sure that mail is delivered correctly. Some sites will use it and others will just use it to deny writing to devices and directories.</p>

3 Audit Evidence

3.1 Audit Results

The following ten test results were selected from the full list of audit results to present as the most significant findings for this audit. Each result is identified by its test identifier, whether the test passed or failed, the tests performed, the findings from the tests, and the test type.

3.1.1 A3 - Information Asset Protection Standards and/or Procedures

Test Identifier	A3 - Information Asset Protection Standards and/or Procedures
Pass/Fail	Failed
Test	Ask system administrator or manager for standards and/or procedures. Also ask other staff members if they are aware of relevant standards and/or procedures. Review internal web site for relevant standards and/or procedures.
Findings	<p>The organization has an information security policy, but it does not cover any aspect of asset protection.</p> <p>The system administrator did not have formal standards or procedures for asset protection. She does maintain informal procedures of several processes that apply to asset protection (i.e., she has a checklist of how to add, modify and delete an e-mail user), but it doesn't specifically address access control or confidentiality protection.</p> <p>In speaking with other personnel, they were not aware of any centralized standards or procedures that addressed asset protection.</p> <p>The internal web site was reviewed and searched for standards and/or procedures for information asset protection with no pages matching. Several different combinations of searches were performed with similar results. An example of the search page and results are shown below.</p>
Test type: Stimulus/Response Objective/Subjective	<p>Interview and Observation</p> <p>This test is mostly a subjective measure to determine if standards or procedures exist. Two interviews and observations of search results from the internal web site yielded no documentation.</p>

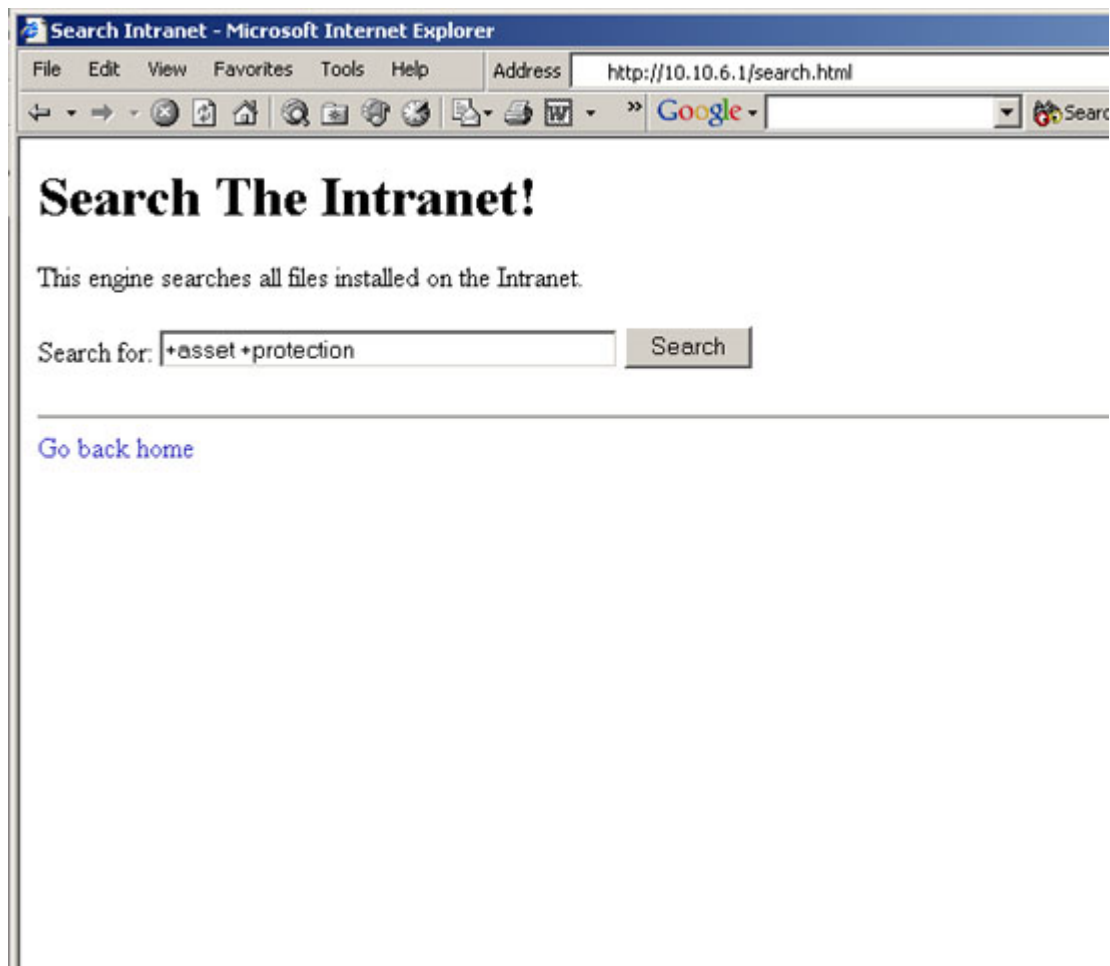


Figure 2 – Intranet Search Page for Asset Protection Documents

© SANS Institute

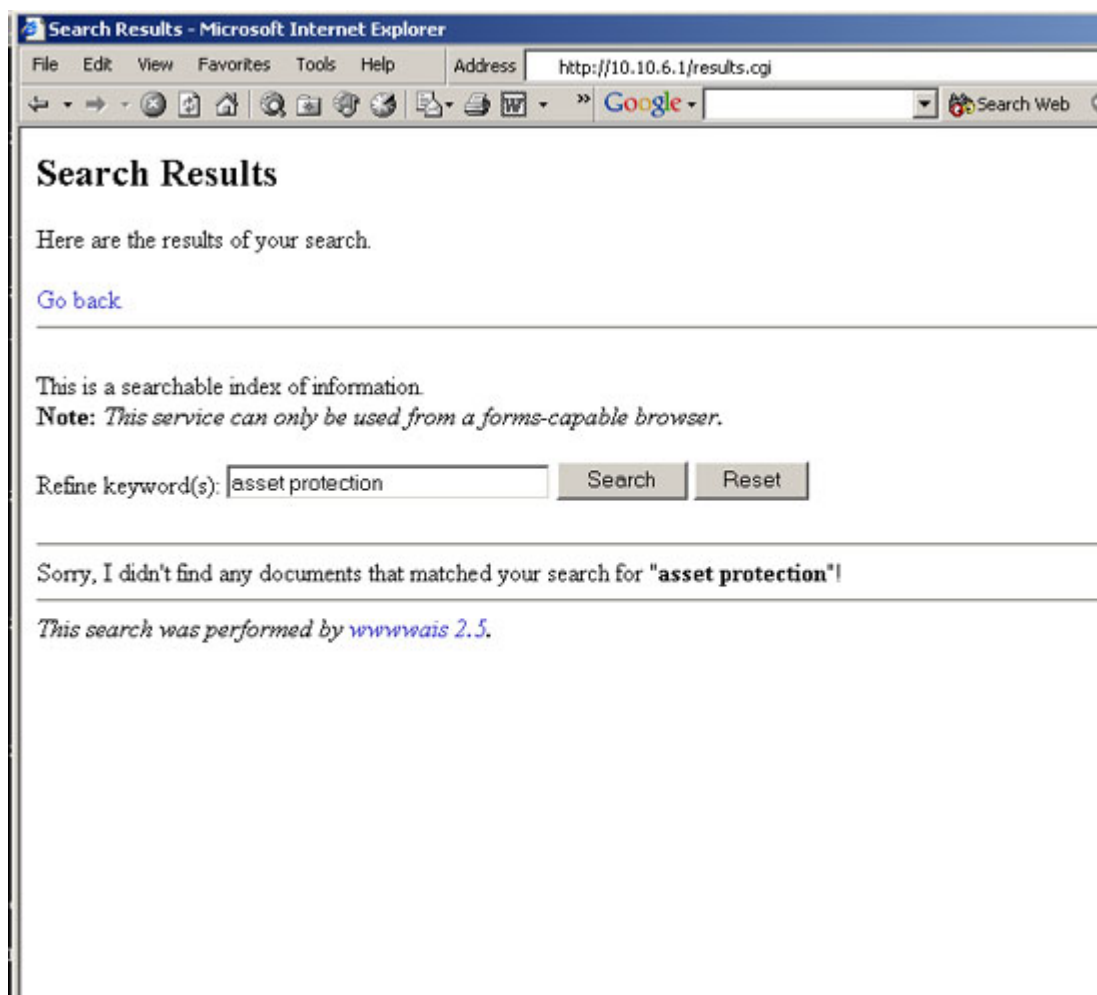


Figure 3 – Search Page Results for Asset Protection Documents

3.1.2 P2 - Physical protection for server

Test Identifier	P2 - Physical protection for server
Pass/Fail	Passed
Test	Review physical security of servers; ideally they should be in a locked cabinet with adequate environmental controls to maintain system in operating conditions for temperature, humidity, and power.

Findings	The DNS/SMTP server is located in a locked room with separate air conditioning and an uninterruptible power supply. The server is rack mounted and the console is left with no one logged in. The rack is not locked but the room is locked and the personnel that have access are limited to the system administrator, the information security manager, and the building security force that does regular inspections of the room during off hours. There were no alarms for temperature or humidity aberrations.
Test type: Stimulus/Response Objective/Subjective	Observation This test is mostly objective as to the level of physical security required to adequately protect the server. Some judgment is required on the lack of alarms for temperature and humidity extremes, but the regular security guard inspections mitigate this risk. The observations show an acceptable level of protection.



Figure 4 – Rack-mounted server for DNS/SMTP (second from top)



Figure 5 – Door to Computer Room



Figure 6 – Air Conditioning Unit



Figure 7 - UPS

3.1.3 N2 – Filter access to server at the Internet firewall

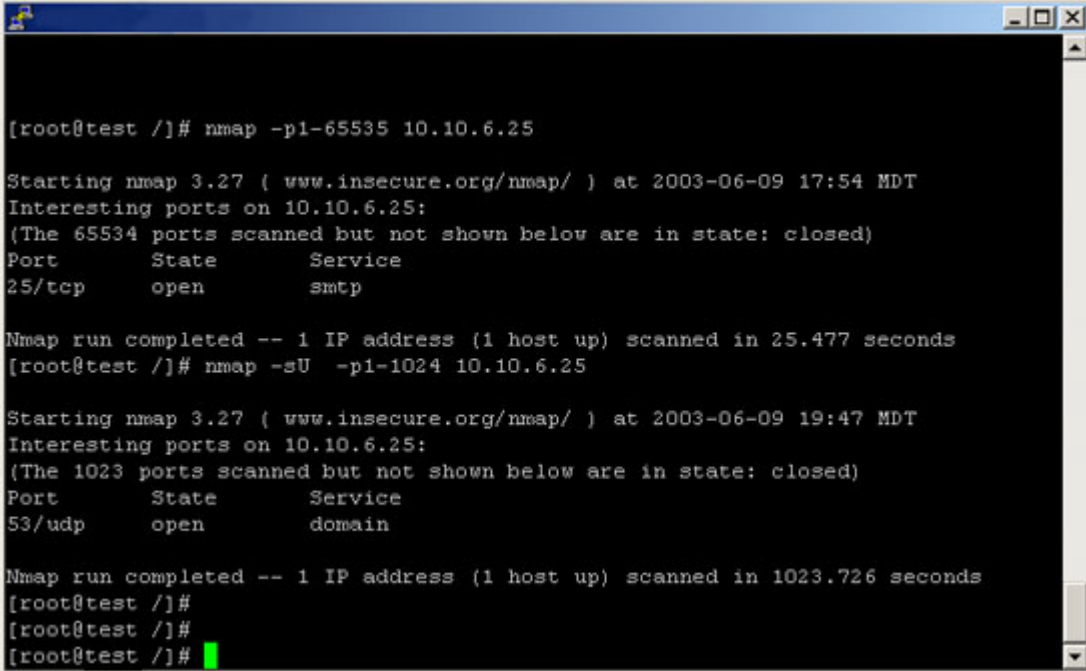
Test Identifier	N2 – Filter access to server at the Internet firewall.
Pass/Fail	Passed

Test	Have administrator of firewall provide copy of running configuration of firewall rules for review. Use a scanning tool such as nmap to discover which ports are available on the DNS/SMTP server from the Internet. Note that only the privileged UDP ports (1-1024) were scanned due to the length of time required to scan all UDP ports. All TCP ports were scanned.
Findings	<p>The rules pertaining to the DNS/SMTP server are correct for the most part. There was one configuration error in the rules, but it is not strictly a security issue, as described below.</p> <p>One common rule that is not properly defined is the need to allow TCP port 53 from anywhere to the DNS server. This is used to accommodate DNS query requests that won't fit into a single UDP packet. There is new functionality as defined in RFC 2671 that allows larger UDP packet sizes, but not all servers will recognize this enhancement, so the 53/tcp rule is still required. As DNS queries get larger due to enhancements such as DNSSec and dynamic updates, this issue will become more apparent.</p>
Test type: Stimulus/Response Objective/Subjective	<p>Documentation and Testing</p> <p>This test is objective and provides the stimulus and response required to objectively test the firewall rules. Note that the test is not to try and "break in" through the firewall but to verify that the firewall rules are working as designed.</p>

The iptables firewall rules as they pertain to the DNS/SMTP server as provided by the system administrator are listed below:

```
-A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -s 0.0.0.0/0 -d 10.10.6.25 -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -p tcp -s 0.0.0.0/0 -d 10.10.6.25 --dport 25 -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -p udp -s 0.0.0.0/0 -d 10.10.6.25 --dport 53 -j ACCEPT
-A INPUT -i eth2 -m state --state ESTABLISHED,RELATED -s 10.10.7.0/24 -d 10.10.6.25 -j ACCEPT
-A INPUT -i eth2 -m state --state NEW -p tcp -s 10.10.7.0/24 -d 10.10.6.25 --dport 25 -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -p udp -s 10.10.7.0/24 -d 10.10.6.25 --dport 53 -j ACCEPT
```

```
-A INPUT -s 0.0.0.0/0 -d 0.0.0.0/0 -j DROP
-A OUTPUT -o eth0 -s 10.10.6.25 -d 0.0.0.0/0 -j ACCEPT
-A OUTPUT -o eth2 -s 10.10.6.25 -d 10.10.7.0/24 -j ACCEPT
-A OUTPUT -s 0.0.0.0/0 -d 0.0.0.0/0 -j DROP
-A FORWARD -i eth0 -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT
-A FORWARD -i eth2 -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT
-A FORWARD -i eth1 -o eth0 -j ACCEPT
-A FORWARD -i eth1 -o eth2 -j ACCEPT
-A FORWARD -j DROP
```



```
[root@test /]# nmap -p1-65535 10.10.6.25

Starting nmap 3.27 ( www.insecure.org/nmap/ ) at 2003-06-09 17:54 MDT
Interesting ports on 10.10.6.25:
(The 65534 ports scanned but not shown below are in state: closed)
Port      State      Service
25/tcp    open       smtp

Nmap run completed -- 1 IP address (1 host up) scanned in 25.477 seconds
[root@test /]# nmap -sU -p1-1024 10.10.6.25

Starting nmap 3.27 ( www.insecure.org/nmap/ ) at 2003-06-09 19:47 MDT
Interesting ports on 10.10.6.25:
(The 1023 ports scanned but not shown below are in state: closed)
Port      State      Service
53/udp    open       domain

Nmap run completed -- 1 IP address (1 host up) scanned in 1023.726 seconds
[root@test /]#
[root@test /]#
[root@test /]#
```

Figure 8 – Results of nmap scans

3.1.4 O6 – Check to see what network services are running

Test Identifier	O6 – Check to see what network services are running.
Pass/Fail	Failed

Test	<p>The best test, if the utility is available on the system, is to use the <code>lsof</code> command. This command lists all open files, and in our case, the network sockets in use and the programs that have them opened. You can also use the <code>netstat</code> command to list the open sockets if <code>lsof</code> is not available. Depending on the version of <code>netstat</code>, it may display the programs that are associated with the open sockets. Check for the availability of the “p” option.</p>										
Findings	<p>There are several network services running on the server that should be disabled.</p> <table> <tr> <th>Name</th><th>Description</th></tr> <tr> <td>portmap</td><td>Maps RPC program numbers to TCP/IP ports</td></tr> <tr> <td>rpc.statd</td><td>Network status monitor for RPC programs, specifically, NFS</td></tr> <tr> <td>Xinetd</td><td>Extended Internet services daemon, used to start services on demand</td></tr> <tr> <td>Cupsd</td><td>The scheduling daemon for CUPS (Common UNIX printing system)</td></tr> </table> <p>In talking with the system administrator, she used the DNS server configuration as provided by RedHat during the install process. She added the packages required for sendmail configuration but assumed that RedHat had provided a secure configuration “out of the box.” This was a reasonable but bad assumption. Linux distribution vendors have made great strides in securing their default distributions but there is still a need for the system administrator to verify that the server is configured properly.</p>	Name	Description	portmap	Maps RPC program numbers to TCP/IP ports	rpc.statd	Network status monitor for RPC programs, specifically, NFS	Xinetd	Extended Internet services daemon, used to start services on demand	Cupsd	The scheduling daemon for CUPS (Common UNIX printing system)
Name	Description										
portmap	Maps RPC program numbers to TCP/IP ports										
rpc.statd	Network status monitor for RPC programs, specifically, NFS										
Xinetd	Extended Internet services daemon, used to start services on demand										
Cupsd	The scheduling daemon for CUPS (Common UNIX printing system)										
Test type: Stimulus/Response Objective/Subjective	<p>Testing</p> <p>This test is objective and provides the stimulus and response required to determine what network services are running on the server.</p>										

```

root@bob:/var/log
[ root@bob log ] #
[ root@bob log ] #
[ root@bob log ] #
[ root@bob log ] # lsof -i +M
COMMAND      PID      USER   FD   TYPE DEVICE SIZE NODE NAME
portmap      2612     rpc     3u   IPv4  2434      UDP *:sunrpc[portmapper]
portmap      2612     rpc     4u   IPv4  2457      TCP *:sunrpc[portmapper] (LISTEN)
rpc.statd    2631    rpcuser  4u   IPv4  2512      UDP *:32768[status]
rpc.statd    2631    rpcuser  5u   IPv4  2475      UDP *:687
rpc.statd    2631    rpcuser  6u   IPv4  2515      TCP *:32768[status] (LISTEN)
named        2736     named    6u   IPv4  3095      UDP *:32769
named        2736     named    7u   IPv4  3067      UDP bob:domain
named        2736     named    8u   IPv4  3068      TCP bob:domain (LISTEN)
named        2736     named    9u   IPv4  3087      UDP 10.10.6.25:domain
named        2736     named   10u   IPv4  3088      TCP 10.10.6.25:domain (LISTEN)
named        2736     named   11u   IPv4  3096      TCP bob:rndc (LISTEN)
sshd         2750     root     3u   IPv4  3065      TCP *:ssh (LISTEN)
xinetd       2764     root     5u   IPv4  3109      TCP bob:32769[sgi_fam] (LISTEN)
sshd         7504     root     4u   IPv4  53226     TCP 10.10.6.25:ssh->10.10.6.102
:1043 (ESTABLISHED)
sendmail     8202     root     4u   IPv4  56129     TCP bob:smtp (LISTEN)
cupsd        32642    root     0u   IPv4  45820     TCP bob:ipp (LISTEN)
[ root@bob log ] #

```

Figure 9 – Output from the “lsof -l +M” command

```

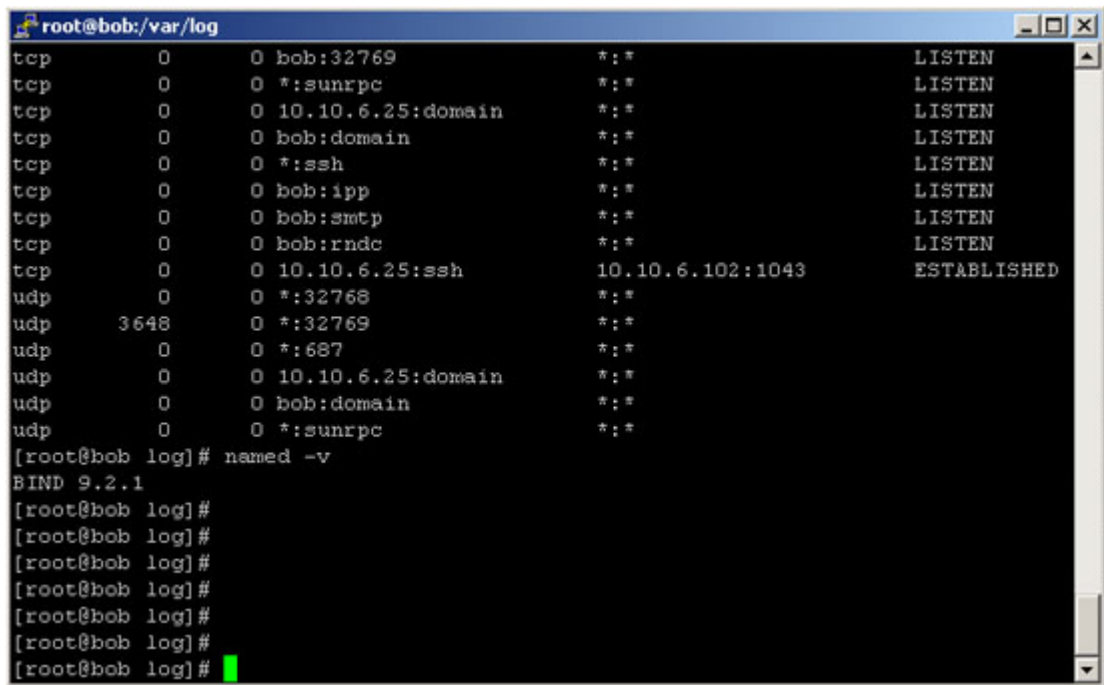
root@bob:~
[ root@bob root ] # netstat -anp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:32768           0.0.0.0:*               LISTEN      2631/
tcp        0      0 127.0.0.1:32769         0.0.0.0:*               LISTEN      2764/xinetd
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      2612/
tcp        0      0 10.10.6.25:53           0.0.0.0:*               LISTEN      8846/
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      8846/
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2750/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      32642/cupsd
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      8846/
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      8202/
tcp        0      0 10.10.6.25:22           10.10.6.116:1837       ESTABLISHED 9796/sshd
udp        0      0 0.0.0.0:32768           0.0.0.0:*               2631/
udp        0      0 0.0.0.0:32772           0.0.0.0:*               8846/
udp        0      0 0.0.0.0:687             0.0.0.0:*               2631/
udp        0      0 10.10.6.25:53           0.0.0.0:*               8846/
udp        0      0 127.0.0.1:53            0.0.0.0:*               8846/
udp        0      0 0.0.0.0:111             0.0.0.0:*               2612/
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State       I-Node PID/Program name    Path
unix   2      [ ACC ] STREAM    LISTENING   3188   2802/gpm            /dev/gpmctl
unix   2      [ ACC ] STREAM    LISTENING   3303   2880/                /tmp/.font-unix/fs7100
unix   4      [ ]        DGRAM                     69643  8790/syslogd        /dev/log
unix   2      [ ]        DGRAM                     72886  8846/
unix   2      [ ]        DGRAM                     69651  8794/klogd
unix   2      [ ]        DGRAM                     56142  8211/
unix   2      [ ]        DGRAM                     56128  8202/
unix   2      [ ]        DGRAM                     3357   2880/
unix   2      [ ]        DGRAM                     3206   2811/crond
unix   2      [ ]        DGRAM                     3104   2764/xinetd
unix   2      [ ]        DGRAM                     2604   2698/apmd
unix   2      [ ]        DGRAM                     2459   2631/
[ root@bob root ] #

```

Figure 10 – Output from the “netstat -anp” command

3.1.5 D1 – Check version of BIND distribution

Test Identifier	D1 – Check version of BIND distribution.
Pass/Fail	Failed
Test	<p>You can usually ask the named program to tell you the version with this command:</p> <pre># named -v</pre> <p>The program should respond with a version number and other information, depending on the version.</p>
Findings	<p>The version of BIND installed on the server is BIND 9.2.1. This is the version that shipped with RedHat 9. Unfortunately, soon after the release of RedHat 9, a vulnerability was found in BIND 9.2.1 (libbind buffer overflow) and BIND 9.2.2 was released and as of this writing is the current version.</p> <p>I asked the system administrator if there was a particular reason why BIND had not been upgraded. She stated that she was unaware that there was a newer version and if she had known, that she would have upgraded the software.</p> <p>As seen in earlier tests, there is still a need for the system administrator to be aware of developments that may cause a new release of software and to verify that the applications are updated and current.</p>
Test type: Stimulus/Response Objective/Subjective	<p>Interview and Testing</p> <p>This test is objective and provides the stimulus and response required to determine what version of BIND is installed and running on the server.</p>



```
root@bob:/var/log
tcp      0      0 bob:32769                *:*      LISTEN
tcp      0      0 *:sunrpc                  *:*      LISTEN
tcp      0      0 10.10.6.25:domain         *:*      LISTEN
tcp      0      0 bob:domain                *:*      LISTEN
tcp      0      0 *:ssh                     *:*      LISTEN
tcp      0      0 bob:ipp                   *:*      LISTEN
tcp      0      0 bob:smtp                  *:*      LISTEN
tcp      0      0 bob:rndc                  *:*      LISTEN
tcp      0      0 10.10.6.25:ssh            10.10.6.102:1043 ESTABLISHED
udp      0      0 *:32768                   *:*      LISTEN
udp      3648    0 *:32769                   *:*      LISTEN
udp      0      0 *:687                     *:*      LISTEN
udp      0      0 10.10.6.25:domain         *:*      LISTEN
udp      0      0 bob:domain                *:*      LISTEN
udp      0      0 *:sunrpc                  *:*      LISTEN
[root@bob log]# named -v
BIND 9.2.1
[root@bob log]#
[root@bob log]#
[root@bob log]#
[root@bob log]#
[root@bob log]#
[root@bob log]#
[root@bob log]#
```

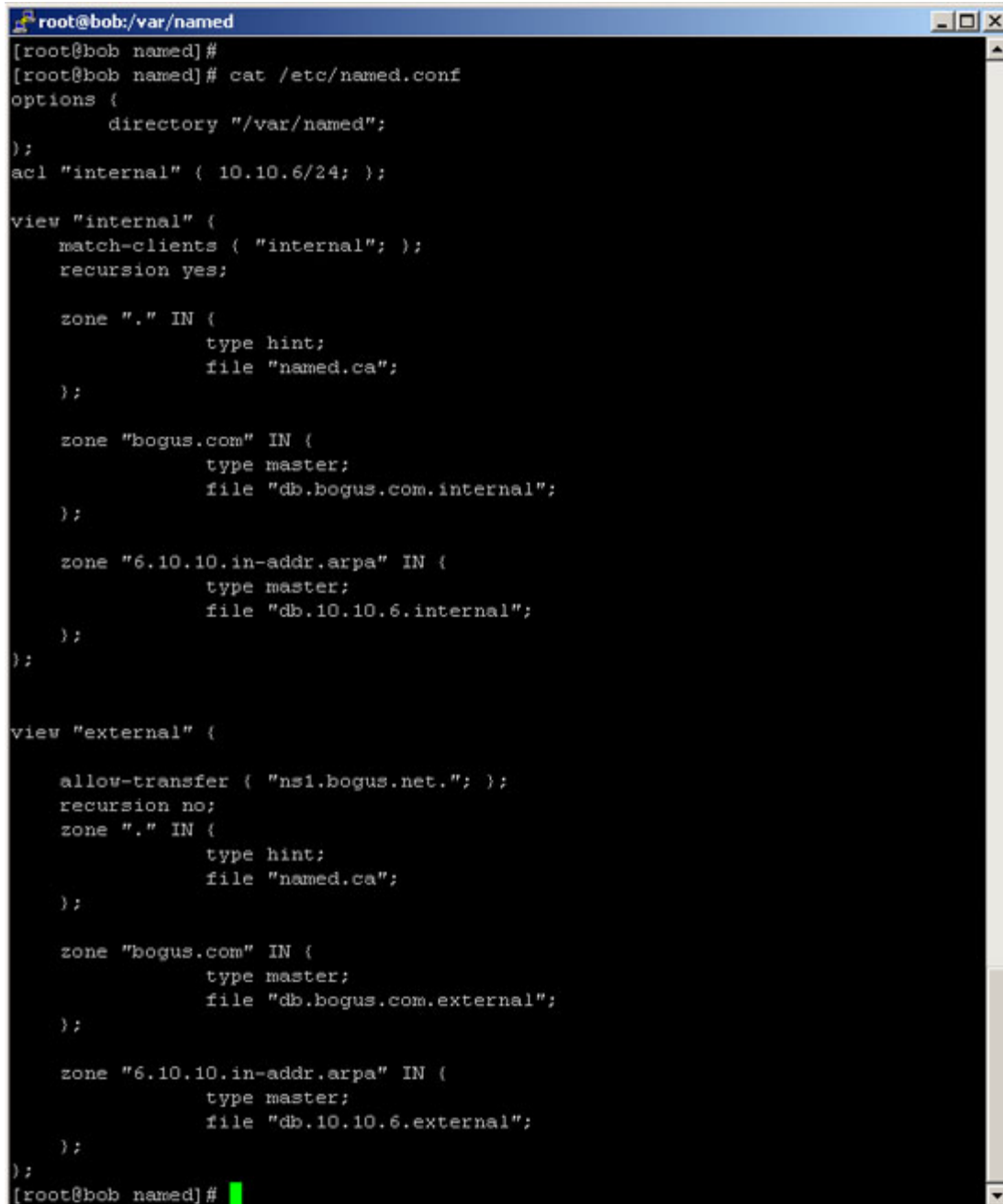
Figure 11 – Output from “named -v” command

3.1.6 D3 – Review use of split namespace

Test Identifier	D3 – Review use of split namespace.
Pass/Fail	Passed
Test	<p>Review DNS system design to determine if split namespace is being used. For BIND 9, the use of views is the easiest way to implement this feature. In the <code>named.conf</code> file, look for statements similar to these:</p> <pre>view "internalview" { match-clients { internal; }; recursion yes; }; view "externalview" { match-clients { any; }; recursion no; };</pre> <p>Also test the server by querying for a known internal name from the Internet. The name should not resolve.</p>

Findings	The <code>named.conf</code> file does have internal and external views defined and separate zone files for internal and external use. When querying the DNS server from the Internet for a known internal name, the name server responds with an error. The same query from the inside returns the name as expected.
Test type: Stimulus/Response Objective/Subjective	Documentation and Testing This test is objective and provides the stimulus and response required to determine if the internal and external views are working as designed.

© SANS Institute 2003, Author retains full rights

A terminal window titled 'root@bob:/var/named' displays the output of the command 'cat /etc/named.conf'. The window has a blue title bar and standard window controls. The terminal text shows the configuration for two views: 'internal' and 'external'. The 'internal' view is for the 10.10.6/24 network and includes zones for the root, bogus.com, and 6.10.10.in-addr.arpa. The 'external' view is for ns1.bogus.net and includes similar zones. The prompt '[root@bob named]#' is visible at the top and bottom of the terminal output.

```
root@bob:/var/named
[root@bob named]#
[root@bob named]# cat /etc/named.conf
options {
    directory "/var/named";
};
acl "internal" { 10.10.6/24; };

view "internal" {
    match-clients { "internal"; };
    recursion yes;

    zone "." IN {
        type hint;
        file "named.ca";
    };

    zone "bogus.com" IN {
        type master;
        file "db.bogus.com.internal";
    };

    zone "6.10.10.in-addr.arpa" IN {
        type master;
        file "db.10.10.6.internal";
    };
};

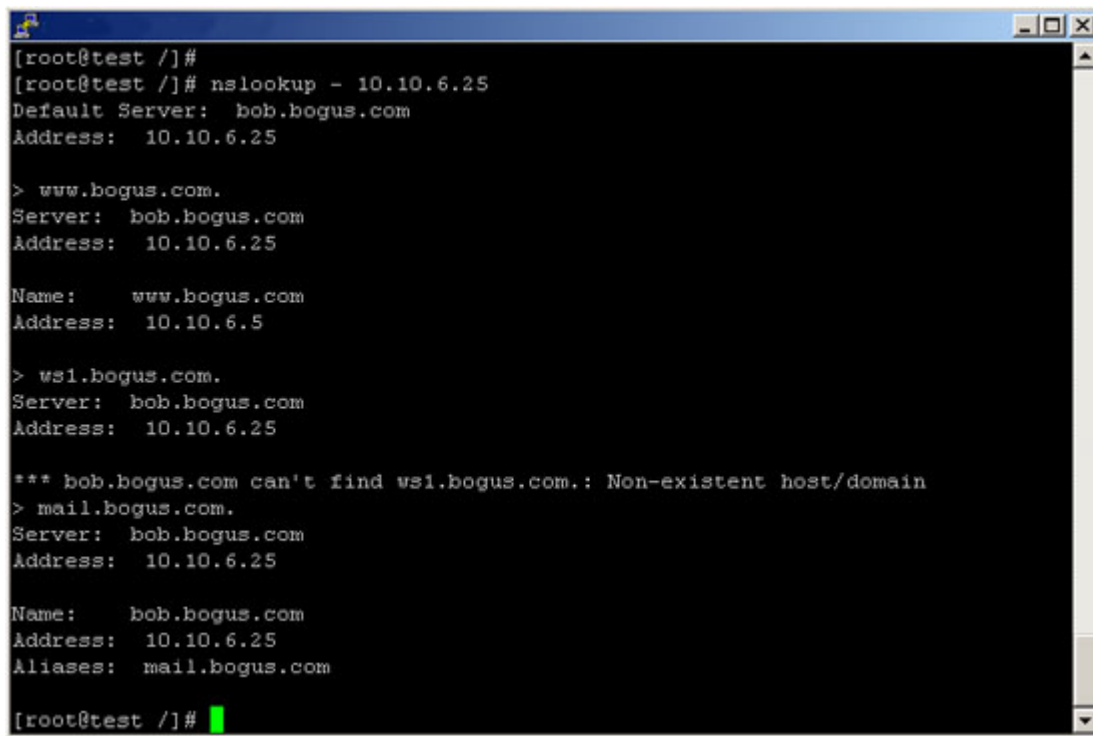
view "external" {

    allow-transfer { "ns1.bogus.net."; };
    recursion no;
    zone "." IN {
        type hint;
        file "named.ca";
    };

    zone "bogus.com" IN {
        type master;
        file "db.bogus.com.external";
    };

    zone "6.10.10.in-addr.arpa" IN {
        type master;
        file "db.10.10.6.external";
    };
};
[root@bob named]#
```

Figure 12 – Listing of /etc/named.conf from server



```
[root@test /]#
[root@test /]# nslookup - 10.10.6.25
Default Server:  bob.bogus.com
Address:  10.10.6.25

> www.bogus.com.
Server:  bob.bogus.com
Address:  10.10.6.25

Name:    www.bogus.com
Address:  10.10.6.5

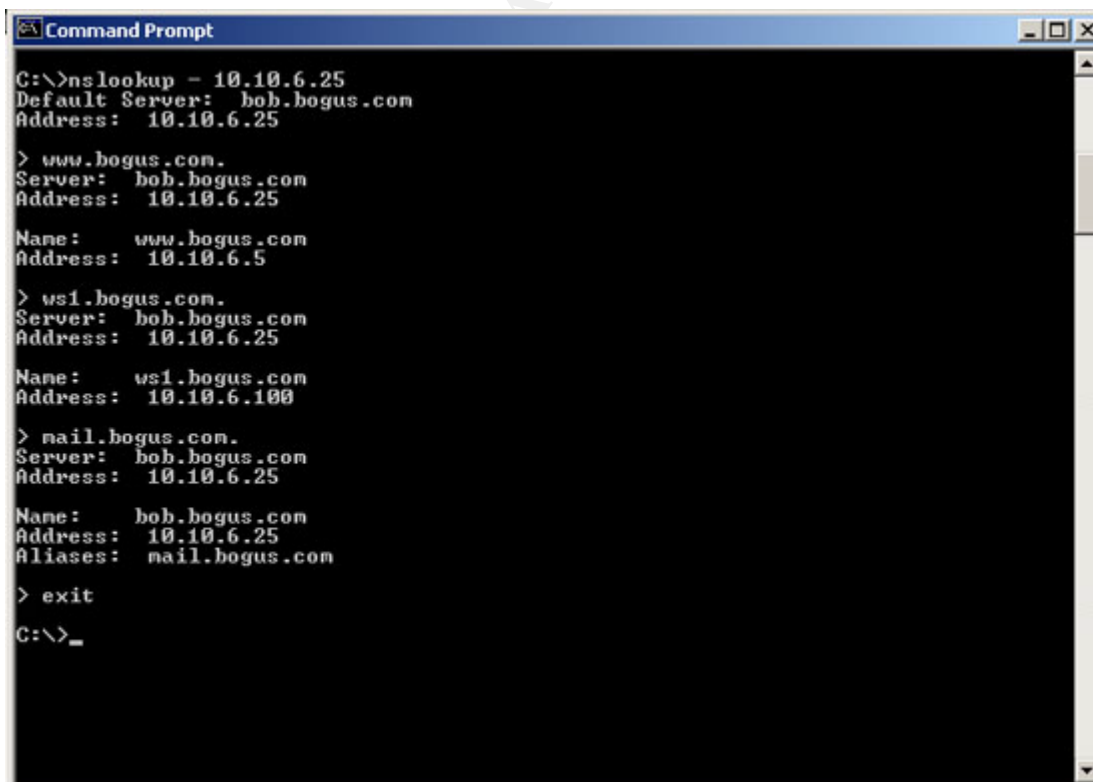
> ws1.bogus.com.
Server:  bob.bogus.com
Address:  10.10.6.25

*** bob.bogus.com can't find ws1.bogus.com.: Non-existent host/domain
> mail.bogus.com.
Server:  bob.bogus.com
Address:  10.10.6.25

Name:    bob.bogus.com
Address:  10.10.6.25
Aliases:  mail.bogus.com

[root@test /]#
```

Figure 13 – Test lookup from external host



```
C:\>nslookup - 10.10.6.25
Default Server:  bob.bogus.com
Address:  10.10.6.25

> www.bogus.com.
Server:  bob.bogus.com
Address:  10.10.6.25

Name:    www.bogus.com
Address:  10.10.6.5

> ws1.bogus.com.
Server:  bob.bogus.com
Address:  10.10.6.25

Name:    ws1.bogus.com
Address:  10.10.6.100

> mail.bogus.com.
Server:  bob.bogus.com
Address:  10.10.6.25

Name:    bob.bogus.com
Address:  10.10.6.25
Aliases:  mail.bogus.com

> exit
C:\>_
```

Figure 14 – Test lookup from internal host

3.1.7 D7 – Review configuration for least privilege and chroot environment

Test Identifier	D3 – Review configuration for least privilege and chroot environment.
Pass/Fail	Failed
Test	<p>Review DNS system configuration to determine if the DNS server is configured to run with least privilege and in a chroot environment. Verify that the least privileged account is running the DNS server and then check the privileges of that account. Run the following commands on the DNS server host and review the response. The named process should be owned by a user other than root and the user entry in the password file should not have a uid of zero (0).</p> <pre># ps -ef grep named named 2736 1 0 May13 ? 00:00:00 [named] # grep named /etc/passwd named:x:25:25:Named:/var/named:/sbin/nologin</pre> <p>To check for the chroot environment, restart the DNS server and review the system log to verify that the daemon is using the “-t” option for chroot.</p> <pre>Jun 10 17:59:23 bob named[8665]: starting BIND 9.2.1 -u named -t /var/named Jun 10 17:59:23 bob named[8665]: using 1 CPU Jun 10 17:59:23 bob named[8665]: loading configuration from '/etc/named.conf' Jun 10 17:59:24 bob named[8665]: no IPv6 interfaces found . . .</pre>
Findings	<p>The DNS service is running under the named account. The named account does not have extra privileges on the system. However, the service is not running in a chroot environment. When the service is started, the log file indicates that it is running at the root directory level.</p>
Test type:	Documentation and Testing
Stimulus/Response	This test is objective and provides the stimulus and response required to determine if the DNS service is running as a non-privileged user and if the service is running in a chroot environment.
Objective/Subjective	

```
root@bob:/var/named
[root@bob named]#
[root@bob named]# ps -ef | grep named
named      8817      1  0 13:17 ?        00:00:00 [named]
root       8829   7506  0 13:28 pts/0    00:00:00 grep named
[root@bob named]# grep named /etc/passwd
named:x:25:25:Named:/var/named:/sbin/nologin
[root@bob named]# grep named /etc/group
named:x:25:
[root@bob named]# kill 8817
[root@bob named]# ps -ef | grep named
root       8833   7506  0 13:29 pts/0    00:00:00 grep named
[root@bob named]# /etc/init.d/named start
[root@bob named]# tail -25 /var/log/messages OK ]
Jun 10 13:17:04 bob named[8817]: zone bogus.com/IN: sending notifies (serial 200306101)
Jun 10 13:17:04 bob named[8817]: zone bogus.com/IN: sending notifies (serial 200306101)
Jun 10 13:17:04 bob named[8817]: zone 6.10.10.in-addr.arpa/IN: sending notifies (serial 200306101)
Jun 10 13:17:04 bob named[8817]: zone 6.10.10.in-addr.arpa/IN: sending notifies (serial 200306101)
Jun 10 13:29:06 bob named[8817]: shutting down
Jun 10 13:29:06 bob named[8817]: stopping command channel on 127.0.0.1#953
Jun 10 13:29:06 bob named[8817]: no longer listening on 127.0.0.1#53
Jun 10 13:29:06 bob named[8817]: no longer listening on 10.10.6.25#53
Jun 10 13:29:06 bob named[8817]: exiting
Jun 10 13:29:16 bob named[8846]: starting BIND 9.2.1 -u named
Jun 10 13:29:16 bob named[8846]: using 1 CPU
Jun 10 13:29:16 bob named[8846]: loading configuration from '/etc/named.conf'
Jun 10 13:29:16 bob named[8846]: no IPv6 interfaces found
Jun 10 13:29:16 bob named[8846]: listening on IPv4 interface lo, 127.0.0.1#53
Jun 10 13:29:16 bob named[8846]: listening on IPv4 interface eth0, 10.10.6.25#53
Jun 10 13:29:16 bob named[8846]: command channel listening on 127.0.0.1#953
Jun 10 13:29:16 bob named[8846]: zone 6.10.10.in-addr.arpa/IN: loaded serial 200306101
Jun 10 13:29:16 bob named[8846]: zone bogus.com/IN: loaded serial 200306101
Jun 10 13:29:16 bob named[8846]: zone 6.10.10.in-addr.arpa/IN: loaded serial 200306101
Jun 10 13:29:16 bob named[8846]: zone bogus.com/IN: loaded serial 200306101
Jun 10 13:29:16 bob named[8846]: running
Jun 10 13:29:16 bob named[8846]: zone bogus.com/IN: sending notifies (serial 200306101)
Jun 10 13:29:16 bob named[8846]: zone bogus.com/IN: sending notifies (serial 200306101)
Jun 10 13:29:16 bob named: named startup succeeded
Jun 10 13:29:16 bob named[8846]: zone 6.10.10.in-addr.arpa/IN: sending notifies (serial 200306101)
[root@bob named]#
```

Figure 15 – Checking for least privilege and chroot

3.1.8 S1 - Check version of SMTP server distribution

Test Identifier	S1 – Check version of SMTP server distribution.
Pass/Fail	Failed

Test	<p>On the Sendmail server, issue the following command:</p> <pre># /usr/sbin/sendmail -d0.1 -bt < /dev/null</pre> <p>The program should respond with a version number and other information, depending on the version.</p>
Findings	<p>The version of sendmail installed on the server is 8.12.8. This is the version that shipped with RedHat 9. Unfortunately, soon after the release of RedHat 9, a vulnerability was found in sendmail 8.12.8 (CERT Advisory CA-2003-12 Buffer Overflow in sendmail). Sendmail 8.12.9 was released and as of this writing is the current version.</p> <p>I asked the system administrator if there was a particular reason why sendmail had not been upgraded. As was the case with BIND, she was unaware that there was a newer version and if she had known, that she would have upgraded the software. The system administrator needs to be aware of developments that may cause a new release of software and to verify that the applications are updated and current.</p>
<p>Test type:</p> <p>Stimulus/Response</p> <p>Objective/Subjective</p>	<p>Documentation and Testing</p> <p>This test is objective and provides the stimulus and response required to determine what version of the SMTP service is installed and running on the server.</p>

```

root@bob:/var/named
[root@bob named]#
[root@bob named]#
[root@bob named]# /usr/sbin/sendmail -d0.1 -bt < /dev/null
Version 8.12.8
  Compiled with: DNSMAP HESIOD HES_GETMAILHOST LDAPMAP LOG MAP_REGEX
                MATCHGECOS MILTER MIME7TO8 MIME8TO7 NAMED_BIND NETINET NETINET6
                NETUNIX NEWDB NIS PIPELINING SASL SCANF STARTTLS TCPWRAPPERS
                USERDB USE_LDAP_INIT

----- SYSTEM IDENTITY (after readcf) -----
  (short domain name) $w = mail
  (canonical domain name) $j = mail.localdomain
  (subdomain name) $m = localdomain
  (node name) $k = bob
-----

ADDRESS TEST MODE (ruleset 3 NOT automatically invoked)
Enter <ruleset> <address>
[root@bob named]#

```

Figure 16 – Output from sendmail debug command to find version

3.1.9 S3 - Review set-user-id root for sendmail

Test Identifier	S3 – Review set-user-id root for sendmail.
Pass/Fail	Passed
Test	<p>Review the file permissions on the sendmail binary. Typically, this is <code>/usr/sbin/sendmail</code> or <code>/usr/lib/sendmail</code>. In the case of RedHat 9.0, the alternatives package is used, so the actual sendmail binary is <code>/usr/sbin/sendmail.sendmail</code>. The file permissions should be set-group-id to allow e-mail submitted via the command line on the server to be written to the queue directory. The group should be the same group that owns the <code>/var/spool/clientmqueue</code> directory, by default <code>smmsp</code>.</p> <p>To test, use the <code>ls</code> command to determine the file permissions. The result should be similar to the following:</p> <pre># ls -l /usr/sbin/sendmail.sendmail -r-xr-sr-x 1 root smmsp 3859419 Feb 24 17:15 sendmail.sendmail</pre> <p>If there is an “s” in the fourth position of the permissions list, as shown below, the sendmail binary is installed set-user-id and, if the owner is root, vulnerable to attack.</p> <pre># ls -l /usr/sbin/sendmail.sendmail -r-sr-sr-x 1 root smmsp 3859419 Feb 24 17:15 sendmail.sendmail</pre>
Findings	The sendmail binary is installed with the proper ownership and permissions.
Test type: Stimulus/Response Objective/Subjective	Testing This test is objective and provides the stimulus and response required to determine what the permissions are on the sendmail program.

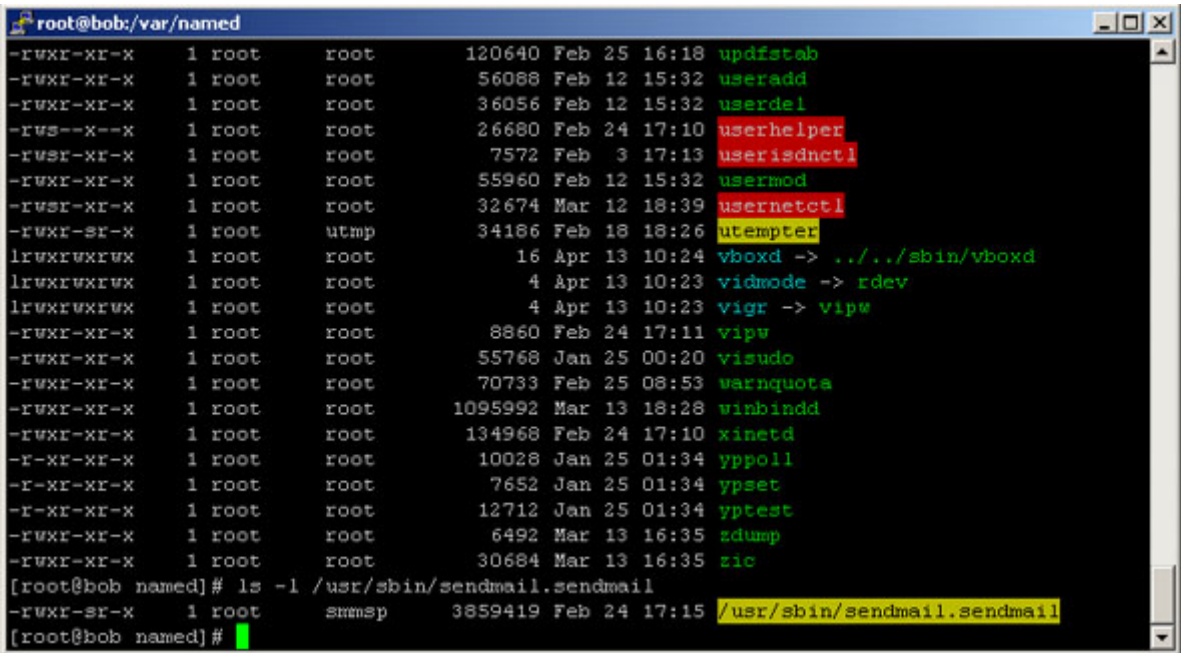
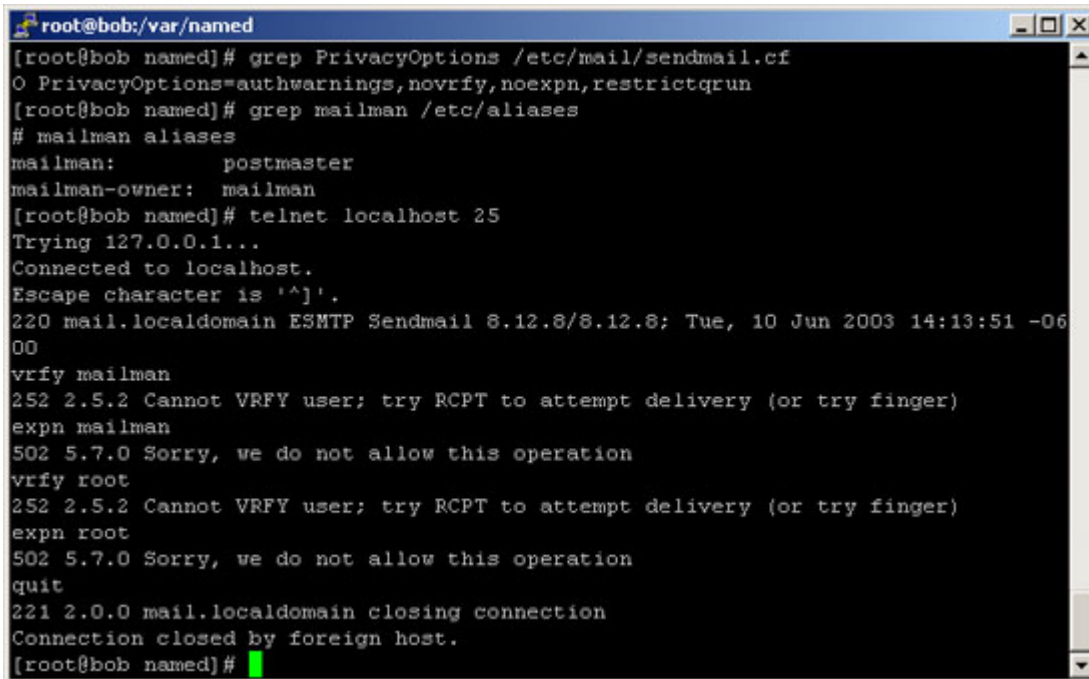


Figure 17 – Listing of file ownership and permissions for sendmail

3.1.10 S7 - Review configuration of PrivacyFlags option

Test Identifier	S7 – Review configuration of PrivacyFlags option.
Pass/Fail	Passed
Test	<p>On the sendmail server, locate the active sendmail configuration (sendmail.cf) file. On RedHat 9, this location is /etc/mail/sendmail.cf. Use the following command to determine the settings of the PrivacyOptions option.</p> <pre># grep PrivacyOptions /etc/mail/sendmail.cf O PrivacyOptions= #</pre> <p>Verify that the options "novrfy" and "noexpn" are listed. If "goaway" is listed, then "novrfy" and "noexpn" are included.</p> <p>You can also telnet to the sendmail server port, 25, and try to verify and expand known mail aliases.</p>
Findings	<p>The sendmail configuration file has adequate settings to prevent the vrfy and expn SMTP commands. Testing with telnet to the sendmail server verifies that the server does not interpret these commands.</p>

Test type:	Testing
Stimulus/Response	This test is objective and provides the stimulus and response required to determine that the PrivacyOptions are set adequately to prevent the
Objective/Subjective	



```
root@bob:/var/named
[root@bob named]# grep PrivacyOptions /etc/mail/sendmail.cf
O PrivacyOptions=authwarnings,noverify,noexpn,restrictqrun
[root@bob named]# grep mailman /etc/aliases
# mailman aliases
mailman:                postmaster
mailman-owner:          mailman
[root@bob named]# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.localdomain ESMTP Sendmail 8.12.8/8.12.8; Tue, 10 Jun 2003 14:13:51 -06
00
vrfy mailman
252 2.5.2 Cannot VRFY user; try RCPT to attempt delivery (or try finger)
expn mailman
502 5.7.0 Sorry, we do not allow this operation
vrfy root
252 2.5.2 Cannot VRFY user; try RCPT to attempt delivery (or try finger)
expn root
502 5.7.0 Sorry, we do not allow this operation
quit
221 2.0.0 mail.localdomain closing connection
Connection closed by foreign host.
[root@bob named]#
```

Figure 18 – Check of PrivacyOptions on sendmail server

3.2 Measure Residual Risk

Overall, the residual risk exposure for the DNS/SMTP server is not substantial compared to what it could be. However, this audit only covered one server located in a screened subnet of a much larger network. Other areas of the company will require auditing that will reveal additional risks. These areas are outside the scope of this report.

There are several findings in this report that reveal the need for the organization to invest in a long-term modification of how they manage information systems, but there are also several areas that can be addressed for a small amount of time and cost that will reduce the risk exposure for the DNS/SMTP server.

3.2.1 Management direction and oversight

A key piece of any information security program is the policies, standards and procedures. Policies provide executive management's intent with respect to how information systems are administered. There is a general policy in place that mostly deals with acceptable use of company resources. There was no evidence of policies or standards that provided guidance in areas such as configuration management, access control, threat and vulnerability

assessment, or incident response. All of these areas and others need policies, standards and procedures available and approved by executive management in order for an information security program to be effective.

The recommendation is to implement a comprehensive set of policies, standards and procedures that clearly identify executive management's intent for the management of information systems. This will not be an easy task and it will be expensive, but it is required if the organization's goal is to have an effective information security program.

The control objectives regarding administrative steps were adequately measured and the audit objectives were met.

3.2.2 Awareness of threats and vulnerabilities

Another key finding concerns the need to have system and network administrators aware of new vulnerabilities in the services they are managing. Both primary services covered in this audit did not have the latest version of software installed and had no valid reason why they were not current.

This is easy to fix short term; just install the latest software. However, the root cause of this finding is due to the lack of effective management processes. The administrators, in the lack of management direction, need to take responsibility and maintain the services using industry best practices and common sense.

The control objectives in the steps that relate to threats and vulnerabilities were measured with sufficient tests and the audit results reflect the importance of these objectives.

3.2.3 Managing the overall system, not just the individual services

Other findings focused on the underlying operating system and the location of the server. Some of these findings may be due to having inexperienced system administrators that simply didn't have enough knowledge, or trusting the operating system vendor to "harden" the server based on selections made at installation. Again, however, the root cause of these findings is due to the lack of effective management processes. If management will not provide effective oversight, the administrators need to become involved by participating in on-line seminars or attending user group meetings to increase their knowledge and implement internal procedures.

The related control objectives concerning the entire system, especially the operating system controls, were measured and meet on of the goals of the audit, to demonstrate the need to look at the entire system.

3.3 Evaluate the Audit

Ideally, the audit process would be completely objective, with only one right answer to each question. In reality, there are always subjective areas that require the auditor to make a judgment call. The overall goal in creating the checklist is to make the tests as objective as possible.

Overall, the audit checklist for this audit has a high number of objective tests that are auditable and stimulus/response actions that provide proof for the result. Most, if not all, of

these tests concern the technical implementation of the services. In this audit, however, the major findings have more to do with the lack of effective management practices. These types of findings are often difficult to measure and evaluate due to human nature and the need for the auditor to make that judgment call.

In summary, the audit results are provable and those tests that require a subjective answer have a great deal of evidence that indicates the finding is accurate.

© SANS Institute 2003, Author retains full rights.

4 Audit Report

4.1 Executive Summary

The organization requested a security audit of their DNS and e-mail server that provides these services to the Internet. The objective of the audit was to determine the risk associated with these services and the steps required to remediate the risk. Our company was retained to provide the audit and present the findings in this report.

Overall, the risk to the services is judged to be medium. There are several findings that can be easily and economically addressed that will lower the immediate risk. There are other findings that will require the executives to approve fundamental changes in the way that information assets are managed. These are long-term goals that are becoming increasingly important in keeping the organization compliant with Federal regulations such as the Sarbanes-Oxley Act, among others.

The top three findings as seen by the auditor are:

- Information Security Policies, Standards and Procedures

The organization does not have an effective governance model for information security. Without policies, standards and procedures sanctioned by executive management, the information security program will not be effective.

- Application Versions

The two services targeted by this audit are implemented with software that has known vulnerabilities. The services need to be updated with the latest software.

- Operating System Configuration

The operating system has several findings associated with unnecessary services and incorrect configuration.

The objectives of the audit were met and the technical risks associated with these services can be mitigated to an acceptable level in a timely manner. The underlying management issues are more problematic and will take a major commitment from the executives to implement an effective information security program for the organization.

4.2 Audit Findings and Risks

This section provides a summary of the findings from each of the areas reviewed by the auditor.

4.2.1 Administration Checklist

These tests pertain to the governance model for managing information systems and determine the existence of policies, standards and procedures.

The validation methods include interviews with personnel, reviews of documentation, and searching the organization's internal web server.

As shown in Section 3.1.1, the existence of relevant policies, standards or procedures was limited. There was an information security policy that mostly pertained to Acceptable Use of information resources but did not adequately address all information security topics. There was no indication that policies, standards or procedures exist in the areas of asset management, asset protection, threat and vulnerability management, and incident response. The system administrator had created some procedures for her personal use, but they are not approved or reviewed by management. Extensive searches on the internal web site provided only the one information security policy.

The associated risk in not having an adequate governance model for information security, and information systems in general, is that management of the information systems of the company will not be done with management's business objectives or goals as part of the model. Also, increasing emphasis on publicly traded companies will force executive management to establish adequate controls to verify that the organization's resources are being managed with due care. Finally, the lack of measurable configuration management and vulnerability assessment standards for the DNS/SMTP server was not acceptable given the importance that these services play in the success of the organization.

All five of the tests in this section were listed as failed.

4.2.2 Physical Access Control Checklist

These tests review the protection that the system has from physical access, environmental controls, and other external threats.

The validation methods include a visual inspection of the location of the system, a review of the key sign-out process or the configuration of the access card system, and testing of the alarms for temperature and humidity.

The tests were reviewed and evidence of the door locks and environmental controls is provided in Section 3.1.2. There were no alarms installed to notify personnel of temperature or humidity extremes, but this threat is mitigated to sufficient degree by the presence of guards who perform regular inspections of the room.

The risk of physical damage to the server is quite low given the controls in place. There is always the chance of a disgruntled internal employee or security guard who could cause harm. For security guards, background checks are an effective screening tool.

The physical access controls were determined to be adequate for the system and the three tests were listed as passed.

4.2.3 Network Checklist

These tests review the configuration of routers and firewalls as they pertain to the DNS and SMTP services. A complete assessment of the network devices is recommended for the future, but is outside of the scope of this audit.

The validation methods include a review of the running configuration on the devices, review of the documentation associated with the devices, and the use of a port scanner and packet fabricator to determine the effectiveness of the configuration of each device.

As shown in Section 3.1.3, the firewall rules were reviewed and the firewall was scanned with a port scanner to verify proper operation. One minor issue with the firewall rules was shared with the administrator to improve the configuration, but the test overall was listed as passed.

The risk associated with the network devices is mostly caused by the lack of policies, standards and procedures as noted earlier. The network administrators seem to be doing the right things, but they need the support of management in the form of standards and procedures to keep the systems managed properly.

The two network checklist tests were listed as passed.

4.2.4 Operating System Checklist

These tests review the configuration of the operating system as it pertains to the DNS and SMTP services. A complete assessment of the operating system is recommended for the future, but is outside of the scope of this audit.

The validation methods are mostly objective tests that display the results for review. Some of the review of the results, however, can be subjective, such as the system processes and network services that are enabled. The organization may have a valid reason for running the service. If so, that will be noted in the findings and the auditor will have to decide if the test passes or fails.

As shown in Section 3.1.4, the network services available on the server are not acceptable. These services are not required to run DNS or SMTP and have a history of being vulnerable to attack.

The highest risk findings of this audit are associated with the operating system. Due to the additional services installed and operating, the likelihood that this system could be compromised and then used to attack internal servers is quite high. Since the firewall rules are based on IP source and destination addresses, the firewall will be less effective if a server in the screened subnet is compromised than if the attacker is using a server from the Internet.

Overall, the audit found that three out of seven tests on the operating system failed.

4.2.5 DNS Checklist

These tests review the installation and configuration of the DNS server and assorted files.

The validation methods for most of these tests are objective. The test results provide proof of compliance or no compliance. The tests involve reviewing configuration files and then using query tools to verify that the configuration is working as designed. For the subjective tests, the auditor must determine if the test is valid for this audit. If so, then the auditor must determine if the organization has passed or failed and provide the reasons for the determination.

An example of an objective and subjective test is shown in Section 3.1.5. After determining the version of BIND installed on the server and the current version, the auditor needs to interview the administrator and manager to determine if there is a valid reason for running the outdated version. If there is, the reason is noted and the auditor determines if the test

passed or failed. If there is no valid reason for running the outdated version, the test must be given a failed result.

Another example is shown in Section 3.1.6. This test is more objective with the review showing the external and internal views configured in the `named.conf` file. The verification test also shows that the external client was unable to resolve an internal name and the internal client was able to resolve it correctly. This test result was given a passing result.

Finally, a similar example of how the service is configured is shown in Section 3.1.7. In this case, the `named` daemon is running with least privilege, but the daemon is not running in a chroot environment, which provides additional protection for the server if the `named` daemon is somehow compromised. So, the overall result for this test is failed.

Overall, the risk associated with these findings is fairly low. The items that did not pass can be mitigated quickly and inexpensively.

For the DNS tests, two tests out of eight failed.

4.2.6 SMTP Checklist

These tests review the installation and configuration of the SMTP server (sendmail) and assorted files.

The validation methods for most of these tests are similar to the DNS tests, a review of the configuration followed by an objective test. The test results provide proof of compliance or non compliance. For the subjective tests, the auditor must determine if the test is valid for this audit. If so, then the auditor must determine if the organization has passed or failed and provide the reasons for the determination.

An example of an objective and subjective test is shown in Section 3.1.8. This test is similar to the BIND version test. After determining the version of sendmail installed on the server and the current version, the auditor needs to interview the administrator and manager to determine if there is a valid reason for running the outdated version. If there is, the reason is noted and the auditor determines whether the test passed or failed. If there is no valid reason for running the outdated version, the test must be failed, as was the case in this audit. In this particular case, the sendmail program in production is vulnerable to a buffer overflow that ranked a CERT Advisory (CA-2003-12).

The next example shows an objective test that reviews the file permissions of the sendmail executable. Sendmail is somewhat unique in that some of the actions it needs to perform require it to temporarily act like the privileged user in Unix known as root. In the past, sendmail would be installed set-user-id as root. That way, regardless of who ran the program, it would run with root privileges. This was not a good way to maintain a secure system, however. In the latest version of the sendmail program, it is installed with set-group-id and, with some proper file permissions, this setting provides the required functionality without the need for set-user-id root. In Section 3.1.9, the screen shots demonstrate the permissions of the sendmail program that passed the test.

Our last example shows the tests to verify that the SMTP `vrfy` and `expn` commands have been disabled. These commands can be used to extract e-mail addresses from the server.

In Section 3.1.10, the tests demonstrate that the server does not provide the e-mail address requested and therefore passes the test.

The overall risk to the SMTP service is medium, with the biggest risk item being the use of the older software release. Implementing a new version of sendmail and changing a few configuration settings will minimize the risk to the SMTP service.

For the SMTP tests, three out of fifteen tests failed.

4.3 Audit Recommendations

The following recommendations come from the findings presented earlier. Each recommendation is cross-referenced to the test identifier that demonstrated the need for the recommendation.

4.3.1 Update Software Packages

Test Identifiers: D1, S1

The finding of both DNS and SMTP software packages being out of date points to a lack of awareness of new vulnerabilities and associated patches at the organization. Of course, the immediate recommendation is to update the packages to the current versions to patch vulnerabilities. But an additional recommendation is to implement a procedure to evaluate the services for vulnerabilities and to keep the services up to date. This is not a replacement for the required standards and procedures that should cover all vulnerabilities in the organization.

4.3.2 Configuration Changes

Test Identifiers: O4, O5, O6, D7, S14, S15

There are several areas that require configuration changes in order to bring the areas of concern. These changes are normally one-time changes that will reduce the immediate risk. Any changes should be incorporated into the change control and configuration management procedures that should be implemented as part of the policy, standard and procedure recommendations.

4.3.3 Policy, Standard and Procedure Development

Test Identifiers: A1 through A5

The root cause of many of the findings in this audit can be traced to a lack of a governance model that provides a framework of policies, standards and procedures. This recommendation will take the most time and cost the most money, but when implemented will result in reduced risk and the required foundation for an effective information security program.

4.4 Estimated Costs

The following table provides estimated costs for implementing the recommendations listed in Section 4.3.

Table 8 – Estimated Costs

Recommendation	Description	Labor Costs
4.3.1 – Update Software Packages	Development of vulnerability detection and patch installation procedures Installation of current software packages	80 hours for procedure development 16 hours for new application testing and installation
4.3.2 – Configuration Changes	Implementation of changes for various findings Development and incorporation of changes into change control and configuration management processes	40 hours for testing and implementing configuration changes 120 hours for procedure development
4.3.3 – Policy, Standard and Procedure Development	Development of comprehensive set of policies, standards and procedures	600 hours for development, approval and implementation

4.5 Compensating Controls

The cost of development of the comprehensive set of policies, standards and procedures is a significant investment for any organization. These controls are long-term and necessary for the overall information security program. During the development of these documents, some compensating controls should be implemented to mitigate the immediate risk. Some recommended compensating controls are:

- Use existing individual procedures developed by system and network administrators as templates for managing systems
- Use example policies, standards and procedures available from reputable sources such as SANS, CERT, and the Center for Internet Security
- Perform a periodic internal audit to measure progress on eliminating existing findings

Other compensating controls that could be used include host and network intrusion detection systems, but these controls will incur more costs and management issues that may create more issues than they solve at this particular organization.

References

[Albitz – 01] Albitz, Paul and Liu, Cricket. DNS and BIND, 4th Edition. O'Reilly and Associates, 2001.

[Boettger – 00] Boettger, Larry. "The Morris Worm: How it Affected Computer Security and Lessons Learned by It". 2000. URL:
<http://www.wbglinks.net/pages/reads/misc/morrisworm.html> (10 June, 2003).

[CERT – 02] Householder, Allen and King, Brian. "Securing an Internet Name Server". CERT® Coordination Center. August 2002. URL: <http://www.cert.org/archive/pdf/dns.pdf> (12 June 2003).

[Chapman – 00] Chapman, Brent and Zwickey, Elizabeth. Building Internet Firewalls, 2nd Edition. O'Reilly and Associates, 2000.

[CIS – 03] The Center for Internet Security. "Benchmark for Cisco IOS - Level 1 and 2 Benchmarks, Version 2.0", March 2003. URL: http://www.cisecurity.org/bench_cisco.html (12 June 2003).

[Costales – 03] Costales, Bryan and Allman, Eric. Sendmail, 3rd Edition. O'Reilly and Associates, 2003.

[CVE – 01] Common Vulnerabilities and Exposures. "CVE-2001-0299", May 2001. URL: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0299> (12 June 2003).

[GAO – 98] United States General Accounting Office, Accounting and Information Management Division. "Executive Guide, Information Security Management", May 1998. URL: <http://www.gao.gov/special.pubs/ai9868.pdf> (12 May 2003).

[ISC – 01] Internet Software Consortium. "BIND 9 Administrator Reference Manual", 2001. URL: <http://www.nominum.com/content/documents/bind9arm.pdf> (12 June 2003)

[NERC – 03] North American Electric Reliability Council. "Urgent Action Standard 1200 - Cyber Security", April 9, 2003. URL: ftp://ftp.nerc.com/pub/sys/all_updl/standards/Draft-Urgent-Req-CyberStd-3-3121.pdf (12 May 2003).

[RedHat – 02] Red Hat, Inc. “Red Hat Linux 9, Red Hat Linux Security Guide”, 2002. URL: <http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/> (12 June 2003).

[SANS – 00] The SANS Institute. Securing Linux Step-by-Step, Version 1.0. The SANS Institute, 2000.

[SANS – 03-1]..The SANS Institute. Auditing Networks, Perimeters, And Systems 7.1, Auditing Principles and Concepts. The SANS Institute, 2003.

[SANS – 03-2] The SANS Institute. “SANS/FBI Top 20 List”, May 2003. URL: <http://www.sans.org/top20/> (10 June 2003).

[Sendmail – 03] Sendmail Consortium. “Sendmail Release Notes”, March 2003. URL: http://www.sendmail.org/ftp/RELEASE_NOTES (10 June 2003).

[Tudor – 01] Tudor, Jan Killmeyer. Information Security Architecture. Auerbach, 2001.

© SANS Institute 2003, Author retains full rights.