



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/gsna>

Auditing Internet Security System's Real Secure: A Solaris-based Network Intrusion Detection System

An Auditor's Perspective

GSNA Assignment Version: 2.1
David Manley

© SANS Institute 2003, Author retains full rights.

Table of Contents

1	RESEARCH IN AUDIT, MEASUREMENT PRACTICE, AND CONTROL	4
1.1	IDENTIFY THE SYSTEM TO BE AUDITED	4
1.1.1	<i>Purpose</i>	4
1.1.2	<i>Primary Security Mechanisms</i>	4
1.2	EVALUATE THE RISK TO THE SYSTEM	7
1.2.1	<i>Consequences of a Compromise</i>	8
1.2.2	<i>Security Control Objectives</i>	8
1.3	CURRENT STATE OF PRACTICE (AUDIT)	8
1.3.1	<i>Operating System Auditing</i>	8
1.3.2	<i>Auditing Network Intrusion Detection Systems</i>	9
2	CREATE AN AUDIT CHECKLIST	10
2.1	INTRODUCTION	10
2.2	ADMINISTRATIVE TASKS RELATED TO THE AUDIT	10
2.3	AUDIT CHECKLIST	11
3	CONDUCT THE AUDIT	35
3.1	ITEM 3 – VERIFICATION OF NETWORKING INFORMATION	35
3.2	ITEM 6 – OPERATING SYSTEM: VERIFICATION OF HARDENING	39
3.3	ITEM 7 – OPERATING SYSTEM: START SCRIPTS	41
3.4	ITEM 9 – OPERATING SYSTEM: ACCOUNTS	42
3.5	ITEM 10 – OPERATING SYSTEM: /ETC/DEFAULT/LOGIN SETTINGS	44
3.6	ITEM 11 – OPERATING SYSTEM: /ETC/DEFAULT/PASSWD SETTINGS	46
3.7	ITEM 16 – OPERATING SYSTEM: SCHEDULED OPERATIONS (CRON JOBS)	47
3.8	ITEM 19 – OPEN SSH CONFIGURATION	48
3.9	ITEM 20 – NETWORK IDS: VERIFICATION OF STEALTH INTERFACE	51
3.10	ITEM 21 – ISS REAL SECURE NETWORK SENSOR: CONFIGURATION	52
3.11	ITEM 22 – NETWORK-BASED ASSESSMENT	56
3.12	ITEM 23 – ANOMALOUS TRAFFIC ASSESSMENT	58
3.13	MEASURE RESIDUAL RISK	59
3.14	IS THE SYSTEM AUDITABLE?	60
4	AUDIT REPORT	60
4.1	EXECUTIVE SUMMARY	60
4.2	AUDIT FINDINGS	61
4.2.1	<i>Verification of Networking Information (Section 3.1)</i>	61
4.2.2	<i>Operating System: Verification of Hardening (Section 3.2)</i>	61
4.2.3	<i>Operating System: Accounts (Section 3.4)</i>	62
4.3	AUDIT RECOMMENDATIONS	62
	REFERENCES	63

Abstract

This document is intended to fulfill the practical assignment (version 2.1) of the GIAC Auditing Networks, Perimeters and Systems (GSNA) certification. For the assignment, the role of independent auditor was chosen, as well as the option to perform an audit. The Real Secure network intrusion detection system was chosen as the system to be audited.

This particular system was chosen because of its extremely vulnerable location in the network (i.e., external to the border firewall) and the requirement that it be very well secured. The document outlines in further detail the reasons this system was chosen including the risks it is exposed to; based on these, an appropriate audit checklist was developed with which to conduct a thorough audit of the system.

Finally, the audit was conducted and an analysis made of the results of the individual audit items. The audit checklist, the audit results, and a summary of the audit findings are all included within this document.

© SANS Institute 2003, Author retains full rights.

1 Research in Audit, Measurement Practice, and Control

1.1 Identify the System to be Audited

The system to be audited is Real Secure version 6.5, a Network Intrusion Detection System from Internet Security Systems (ISS). It is running on a Sun Microsystems Server, Solaris version 8, on Sun Ultra 10 hardware.

The system is currently in a test environment that simulates a corporate production environment; the intent is to place the IDS between network segments, primarily on the links between the corporate network and its branch offices, and also external to Internet-facing firewalls. Once it is implemented, several identical systems will be incorporated into the network. The hardware platform will be changed to more robust Sun hardware; the operating system version and IDS software, as well as their installation and configuration details, should remain the same for the foreseeable future.

For the purposes of this audit and this document, one system will be taken as a standard system and evaluated.

1.1.1 Purpose

The Intrusion Detection System's intended role is to detect abnormal and anomalous traffic, including scans, probes, worms, and other malicious activity, as well as attempted intrusions. It will not be an intrusion prevention system, or configured to drop or reject any of these questionable connections, but rather to recognize, log and provide an alerting mechanism for the suspect traffic. The system will act in concert with the security defences already in place, particularly firewalls. The data obtained by the network IDS (NIDS) will also be correlated with that of the logs of other systems, including operating system log files and firewall logs.

1.1.2 Primary Security Mechanisms

The process of securing the system was done using a bottom-up, security-in-depth approach. First, a Core installation of Solaris version 8 was performed, which is the option that installs the minimum components. It was further hardened and fully patched. Then ISS Real Secure (version 6.5) software was installed and the latest updates were applied. Finally, the interface that would be listening to and analyzing the network traffic was placed into stealth mode, meaning it is configured not to have an IP address.

The IDS has two interfaces. As mentioned, one is configured as a stealth interface, and will listen to and analyze the traffic passing on the network. The second interface is connected to a screened subnet of the firewall, through which there is a connection to the ISS Real Secure Management Console. This management network is physically isolated from the rest of the internal network. The diagram on the next page depicts the network configuration.

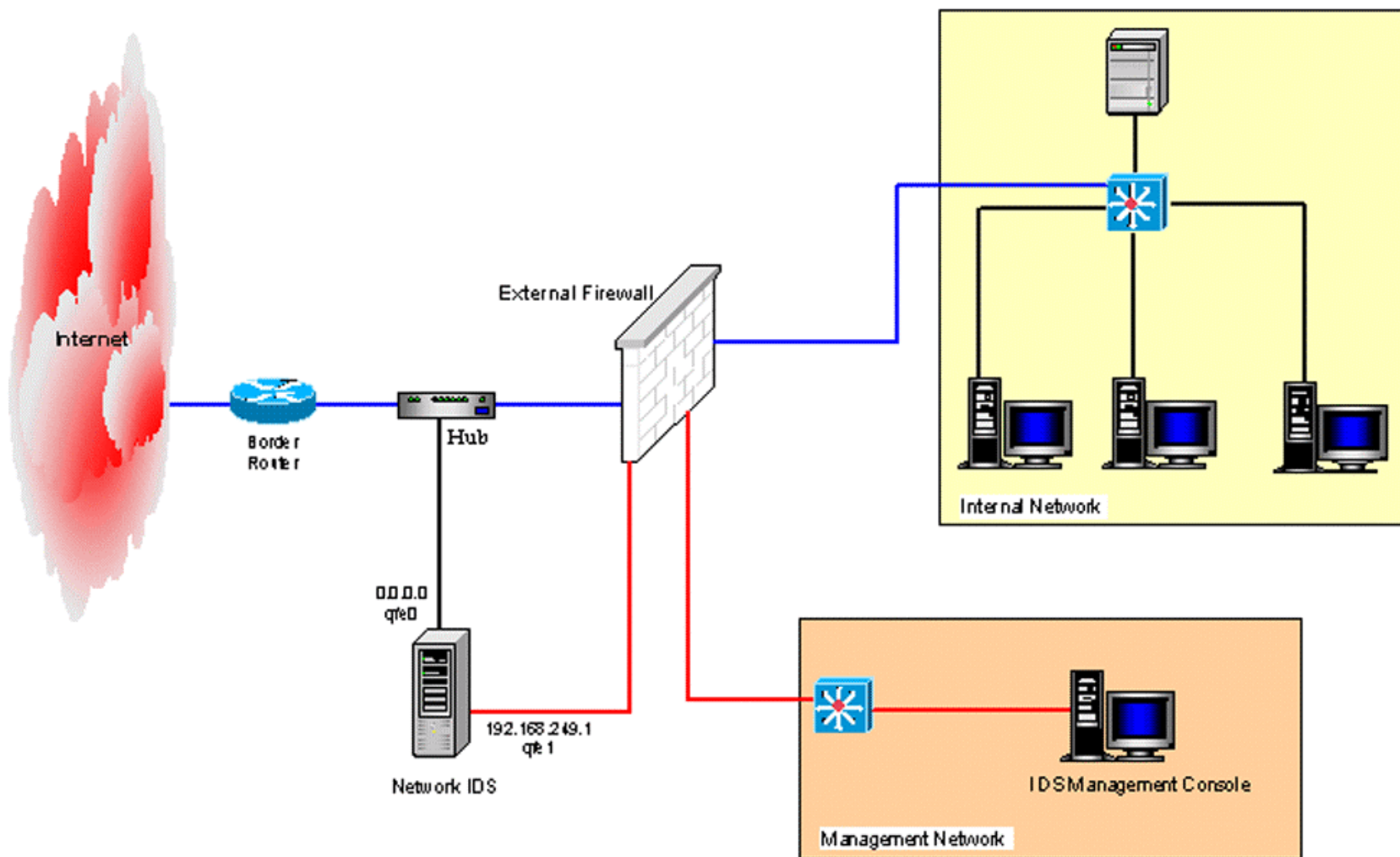


Figure 1: IDS Network Design (Proposed)

The Management Console itself (operating system configuration and hardening, etc.) will not be included in the scope of this audit (because of the time and document length constraints of the assignment), although it is quite important from a security perspective.

In addition to the IDS software, the only additional software installed is Open SSH, version 3.51p, which is used to administer the system.

1.2 Evaluate the Risk to the System

Because this system will reside outside of trusted networks, the risks to the system if it is not secured properly are very high, and therefore a thorough audit is warranted and deserves a high priority.

The only method of accessing the IDS from an external network will be via the stealth interface, so its configuration and security are paramount. As it has no IP address, its security is based on the fact that it is unreachable, and indeed should be virtually invisible. A recent discussion that took place on the Security Focus IDS mailing list (located at <http://online.securityfocus.com/archive/96/306346/2003-01-11/2003-01-17/1>) addressed the issue of the stealth interface. There was general agreement of those contributing to the discussion, including Kurt Seifried (<http://seifried.org/security>), Talisker (<http://www.networkintrusion.co.uk>) and M. Dodge Mumford, an NFR employee, that the stealth interface has not recently been exploited or used as a means of breaching any well-known IDS system.

Three means of exploiting the stealth interface, according to Mr. Mumford, would be through vulnerabilities in the kernel of the OS, a buffer overflow or vulnerability in the IDS software, or a similar vulnerability in any additional software used on the system.

Therefore, the stealth interface should be secure, provided it is configured properly and that no known vulnerabilities in the OS, IDS software, or other software on the system exist that have not been patched.

The primary means of securing the operating system are through its "Spartan" installation and very well-hardened configuration, and by maintaining a current patch level. The IDS software is from a respected vendor, and updates to the software are released periodically.

Because the IDS device will be external to the trusted network, if breached it could possibly provide a means of accessing the internal management network. Therefore, the management network is physically isolated from the rest of the internal network, located off of a screened subnet of the firewall. Communication between the network IDS sensor and the Management Console takes place over ports 2998/tcp and 901/tcp. Further, SSH is installed on the IDS, and configured to use its standard port for communication, 22/tcp.

So, these combined attributes mean that while the IDS is in a highly vulnerable location, it should have a low probability of being attacked or breached, and should, in fact, be virtually invisible.

1.2.1 Consequences of a Compromise

If the system were to be compromised, there are several consequences that could be critical. First, the basic function of the system in detecting intrusions and other nefarious traffic could be disabled if an intruder has interrupted, bypassed, or is in control of the system. If this is carried out surreptitiously, an intruder could attempt to breach, or even enter, the network, undetected by the IDS.

Further, the administrator, potentially not knowing of the compromise of the IDS, would continue to rely on the accuracy of the information received from it, and be unaware of the malevolent activities taking place.

Also, as mentioned previously, if the system were to be compromised and administrative access obtained, an intruder could potentially use the IDS as an access point into other areas of the network, which is highly undesirable.

1.2.2 Security Control Objectives

The security control objectives therefore are clear: the operating system must be installed and configured in a very secure fashion, and a current patch-level maintained; the security of the network configuration is paramount; and finally, the ISS Real Secure and SSH software must be installed and configured to be as secure as possible, and must be kept up-to-date with patches and security updates.

The network configuration control objective, however, has been somewhat limited in scope due to the time and length constraints of this assignment. The Management Console device itself, additional devices found within the management network, and the firewall configuration will not be considered. Also not within the scope are the border router and switch configurations.

The scope of the network portion of the audit will be limited to the network configuration of the IDS, the basic design of the management network, and the SSH and ISS communication between the Management Console and the IDS.

1.3 Current State of Practice (Audit)

The security of the Network Intrusion Detection System being audited can be broken down into two parts: the operating system and the Network IDS itself.

1.3.1 Operating System Auditing

The current state of practice for securing and auditing a Solaris system is quite good. There is a wealth of material available on the Internet that discusses hardening a Solaris operating system, which can then be modified to create a thorough audit checklist.

There are also tools available for free, such as the one available from the Center for Internet Security, which will check multiple configuration settings on a Solaris system and generate a list of positive and negative responses so that these may be investigated and/or changed.

These documents and tools have been culled over years of dealing with Solaris systems; there are new documents and resources becoming available regularly. In addition to

personal knowledge and experience, the following table lists the resources used to create the Solaris operating system audit checklist items in this document:

Resource	Link
SANS Institute: Solaris Security Step-by-Step	http://store.sans.org/store_item.php?item=21
The Center for Internet Security Solaris Benchmark	http://www.cisecurity.org
How to Strip Down a UNIX OS – Check Point Guide	http://support.checkpoint.com/kb/docs/public/os/solaris/pdf/strip-sunserver.pdf
Australian Computer Emergency Response Team: UNIX Security Checklist	http://www.uscert.org.au/Information/Auscert_info/papers.html
Security Focus - Hardening Solaris: Creating a Diamond in the Rough, Parts I and II	http://www.securityfocus.com/infocus/1365 and http://www.securityfocus.com/infocus/1366
The UNIX Auditor's Practical Handbook	http://www.nii.co.in/tuaph1.html

1.3.2 Auditing Network Intrusion Detection Systems

The resources available for auditing Network Intrusion Detection Systems are somewhat more limited. Most of the information available relating to NIDS is from the standpoint of comparing multiple products to determine which has the best performance; this is based not only on whether or how well the systems detect attacks, but also upon their ability to handle high volumes of traffic without becoming overwhelmed and dropping packets or missing significant events.

While it is important that the NIDS be able to analyze and detect anomalous traffic even when much of the bandwidth is being consumed and the system is under heavy load, it is outside the scope of the audit to conduct such tests on the system.

There are, however, many resources available for conducting vulnerability assessments and scanning of networks, which should be detected and identified by an IDS. Additionally, many of these tools (such as netcat, nessus and nmap) allow the creation of packets or traffic which should appear suspicious to an IDS and therefore trigger an alert.

In addition to personal knowledge and experience, the following table lists resources used to develop further audit checklist items:

Resource	Link
Intrusion Detection Systems Group Test: An NSS Group Report	http://www.nss.co.uk
SANS Reading Room: Proactive Vulnerability Assessments with Nessus	http://www.sans.org/rr/audit/proactive.php
SANS Reading Room: Auditing Inside the Enterprise via Port Scanning & Related Tools	http://www.sans.org/rr/audit/inside.php
SANS Reading Room: An Introduction to NMAP	http://www.sans.org/rr/audit/nmap2.php
Hacking Exposed by Stuart McClure, Joel Scambray and George Kurtz	http://www.foundstone.com/knowledge/books.html

2 Create an Audit Checklist

2.1 Introduction

The goal of the following Audit Checklist will be to verify the security control objectives outlined in section 1.2.2, namely a secure operating system configuration, a secure network configuration, and that the software on the system has also been securely installed and configured.

As the security of the operating system is of primary importance, the majority of the audit items will deal with verifying its security. The network portion of the audit will be limited in scope as outlined in section 1.2.2.

2.2 Administrative Tasks Related to the Audit

There are a number of administrative tasks that go hand-in-hand with conducting an audit, including preparing a detailed audit plan including timelines and objectives, scheduling time with the personnel involved in the audit, conducting interviews with various parties, and so on, that will not be included in the Audit Checklist.

The Audit Checklist, with these omissions, will attempt to narrow the focus down to the best items possible to determine the objectives outlined in the previous section.

2.3 Audit Checklist

Check the appropriate box for each item: **Yes** if true, **No** if false, or **N/A** if it does not apply.

Important: Do not make configuration changes based on this audit document! Certain systems may require configuration settings that differ from those in this document. Please make note of any variances between actual system information and this checklist in the “notes” sections. Include plans and timeframe for remediation (if applicable).

System Hostname: _____ Date: _____

Item 1 – Documentation and Administration

Verify that appropriate documentation and administrative information exists for the Intrusion Detection System, including the following:

Yes	No	N/A	Item
			Inventory Information – including:
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Hardware type, manufacturer, serial number, current firmware/BIOS information
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Hardware configuration information (CPU, memory, network interfaces, etc.)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Operating system type, manufacturer, version, and current patch information
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	All installed applications, manufacturer, version, and current patch information
			Support Information – including:
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	License information for hardware, operating system, and IDS software vendors
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Contact information (e.g., telephone numbers, addresses) for hardware, operating system, IDS and other software vendors
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Support contract information (e.g., support numbers, expiration) for hardware, operating system, IDS and other software vendors

Reference: Personal Knowledge and Experience.

Control Objective: To verify that system hardware, software, and support information is available, complete and up-to-date.

Risk: Well-maintained and regularly updated documentation (e.g., support contract expiration dates) can aid in quickly contacting the appropriate support personnel and providing them with the correct information.

Compliance: The information requested should be readily available.

Testing: Verify documentation, contract numbers, telephone numbers, etc.

Objective/Subjective: Objective. It should be apparent whether the information is current and complete.

Notes:

Item 2 – Operating System and Network Documentation

Verify that appropriate operating system and network configuration documentation exists for the Intrusion Detection System environment, including the following:

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Operating System Installation Procedures
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Hardening Information - the procedures and documentation used in hardening the operating system
			Network Documentation – including:
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	MAC Address(es), network interface, IP Address(es), subnet mask(s), default gateway, DNS servers, and hostname information
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Network routing tables, diagrams, other relevant network configuration information
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Account Documentation - includes administrator and all other account information
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Backup Procedures - includes procedures and plans for continuity of operations
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Patching - includes procedures for assessment, testing and system downtime and rollback scenarios

Reference: Personal Knowledge and Experience.

Control Objective: To verify that system configuration, hardening, and maintenance information is well-documented and readily available.

Risk: Well-maintained and regularly updated documentation is vital to proper system maintenance; all changes made to a system, beginning from the operating system installation and hardening, should be documented and kept current.

Compliance: The information requested should be readily available.

Testing: Verify that documentation is regularly maintained and available.

Objective/Subjective: Objective. It should be apparent whether the information is current and complete.

Notes:

Item 3 – Verification of Networking Information

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Actual system network information including MAC Address, hostname, network interface, IP address, subnet mask, default gateway, and DNS information matches the documentation.
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Routing tables, network diagrams, and other network information in the operating system documentation matches the actual system configuration

Reference: Personal knowledge and experience.

Control Objective: To verify that system documentation is the same as the actual system network configuration.

Risk: Out of date, poorly maintained, or inaccurate documentation may lead to mistakes or misunderstandings of the configuration of a system, or what has or has not been done on a system.

Compliance: Actual system network configuration matches documentation.

Testing:	
Command:	Results:
# ifconfig -a	Displays MAC address, IP address, interface, and subnet mask
# cat /etc/hostname.interface (e.g. /etc/hostname.hme0); or # cat /etc/hosts	Displays hostname information; the hostname.interface file will contain the hostname; the hostname and corresponding IP address will be in the hosts file
# cat /etc/defaultrouter	Displays default router information
# cat /etc/nsswitch.conf	Displays information about which network services (e.g., DNS, hostname file) will be consulted in which order
# netstat -rn	Displays routing table information; routing information may also be configured in start scripts – verify with system administrator.
# netstat -an	Displays listening network ports on the system as well as current connections
Other:	Verify that information on diagrams (IP addresses, interface names, cables connected to switches, etc., match the physical connections in the network

Objective/Subjective: Objective. The information should be verifiable via the commands listed.

Item 4 – Verification of Physical Network Connections

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Unused network cards are disabled or removed and no cabling is attached to unused interfaces
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Physical network configuration matches that of the network documentation

Reference: Personal knowledge and experience.

Control Objective: To verify that the physical connections match those of the network diagrams.

Risk: Network diagramming should be physically verified to insure accuracy. The security risks of this are minimal, but the benefits are numerous, especially when troubleshooting connections or when looking up information about the physical configuration of the network.

Compliance: Actual cabling/network configuration matches what has been documented.

Testing: Physically verify that cabling is connected to correct interfaces, that unused interfaces are not attached to cabling, and that network connections are accurately portrayed in the documentation.

Objective/Subjective: Objective. Any discrepancies between physical connections and diagrams should be clear.

Notes:

Item 5 – Operating System: Verification of Patching

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The latest vendor operating system patches have been applied
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A utility (such as Sun's Patch Check) is used to maintain current patch level

Reference: Personal knowledge and experience.

Control Objective: To verify that the operating system patch level is current.

Risk: Not applying patches in a timely fashion can leave the system exposed to known vulnerabilities.

Compliance: Review of patch information on the system matches list of current patches available from Sun Microsystems.

Testing: The contents of the /var/sadm/patch directory may be compared with a list of current patches (available from Sun at <http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage>); the command **showrev -p** will also display a list of patches applied to the system.

Objective/Subjective: Objective. A comparison of the list of patches available versus those applied to the system should reveal any disparity between the two.

Notes:

Item 6 – Operating System: Verification of Hardening

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A utility (such as CIS-SCAN from The Center for Internet Security) is used to verify system hardening

Reference: The Center for Internet Security.

Control Objective: To apply an objective, 3rd party tool as a review of system hardening.

Risk: Hardening actions may be accidentally overlooked, which may be revealed by using a tool such as this.

Compliance: Results of a scanning tool (such as the one from The Center for Internet Security) will provide information about hardening steps that were or were not performed on the system.

Testing: Run a 3rd party tool to verify hardening.

Testing:	
Command:	Results:
# cd /opt/CIS/	Change to the directory where the CIS tool is installed
# ./cis-scan	Runs the scan

Objective/Subjective: Subjective. A review of the output of the CIS scan (or other 3rd party tool) will reveal both positive and negative items; not all items found as negative by the tool are necessarily required for good hardening of a system, but this will provide a good overview and a chance to discuss each item with the systems administrator responsible for hardening the system.

Notes:

Item 7 – Operating System: Start Scripts

Unnecessary services have been disabled at all run levels (/etc/rc*.d), especially:

Yes	No	N/A	Item	Yes	No	N/A	Item	Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	afbinit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	lifbinit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	rpc
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	asppp	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	llc2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	savecore
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	autofs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	lp	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	sendmail
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	autoinstall	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	mipagent	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Slpd
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	bdconfig	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	ncad	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	snmpdx
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	cachefs.daemon	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	ncalogd	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Spc
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	cacheos.finish	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	nfs.client	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	sysid.net
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	dmi	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	nfs.server	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	sysid.sys
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	dtlogin	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	nscd	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Uucp
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	power	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	wbem	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	ldap.client
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	PRESERVE	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	flashprom	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Xntpd

Reference: SANS Institute: Solaris Security Step-by-Step, version 2.0; The Center for Internet Security Solaris Benchmark v1.0.1b; How to Strip Down a UNIX OS – Check Point Guide; Australian Computer Emergency Response Team: UNIX Security Checklist v2.0; Hardening Solaris: Creating a Diamond in the Rough, Parts I and II; The UNIX Auditor's Practical Handbook; Personal Knowledge and Experience.

Control Objective: To verify what services will or will not be started at various run levels.

Risk: Certain items which are installed and started by default under Solaris 8, such as sendmail or NFS, contain multiple vulnerabilities and are widely considered to be security risks.

Compliance: A review of the run level directories will determine which scripts are configured to start automatically at which run level.

Testing:	
Command:	Results:
# cd /etc/init.d/rc*.d	The * in the command indicates the run level. Run level 2 (rc2.d) and 3 (rc3.d) are the “multi-user” run levels.
# ls	Lists the contents of the directory. If the script is to start automatically during boot, it will be preceded by the letter “S”. Any other character will prevent the script from starting – many administrators use a different convention.
# ps -ef	Will list the currently running processes on the server; verify that no unidentified processes are active

Objective/Subjective: Subjective. Each system has different requirements that will determine whether a startup script can be safely disabled. The list in Item 7 above contains most scripts that are not necessary on a bastion host.

A review of start scripts will give the administrator an opportunity to explain why each script is necessary for the requirements of the system. This network intrusion detection system should be very well hardened. Therefore, even though this is a somewhat subjective item, any start scripts other than network routing, SSH, IDS software, etc., which are enabled should be noted and explained.

Notes:

Item 8 – Operating System: Inetd.conf

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	All unnecessary services have been removed from /etc/inetd.conf

Reference: SANS Institute: Solaris Security Step-by-Step, version 2.0; The Center for Internet Security Solaris Benchmark v1.0.1b; How to Strip Down a UNIX OS – Check Point Guide; Australian Computer Emergency Response Team: UNIX Security Checklist v2.0; Hardening Solaris: Creating a Diamond in the Rough, Parts I and II; The UNIX Auditor’s Practical Handbook; Personal Knowledge and Experience.

Control Objective: Inetd, or the Internet services daemon, starts standard Internet services; the contents of this file should be reviewed carefully to verify that no unnecessary services are started by this daemon

Risk: Certain services that are started by Inetd, such as telnet, ftp, and finger, may leave the system open to known vulnerabilities or open additional points from which the system may be attacked. Any unnecessary services should be disabled.

Compliance: A review of this file will reveal which services will be automatically started by the daemon.

Testing:	
Command:	Results:
# more /etc/inetd.conf	The file will be displayed a page at a time. A # symbol in the file indicates lines that are commented out, and that the service will not be started. Any services that are not preceded by a # symbol will be started automatically during the system boot process.

Objective/Subjective: Subjective. Each system has different requirements that will determine whether an item in the /etc/inetd.conf file can be disabled. A review of the file will give the administrator an opportunity to explain why each is necessary for the function of the system.

Because of the requirements for this system to be secure and the fact that it need not offer any additional services other than intrusion detection, it is highly unlikely that any services need to be started by this file.

Notes:

Item 9 – Operating System: Accounts

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Individual, unique accounts have been created for each administrator (/etc/passwd)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Unnecessary accounts, including the following, have been removed (accounts may be removed or NP in password field of /etc/shadow):

Yes	No	N/A	Item	Yes	No	N/A	Item	Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	sys	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	uucp	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	lp
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	listen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	nuucp	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	smtp
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	nobody4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A /dev/null or false shell has been created for any of these users remaining on the system (/etc/passwd)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The files /etc/passwd and /etc/group have permissions 644 and are owned by root and group sys
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The file /etc/shadow has permissions 400 and is owned by root and group sys

Reference: SANS Institute: Solaris Security Step-by-Step, version 2.0; The Center for Internet Security Solaris Benchmark v1.0.1b; How to Strip Down a UNIX OS – Check Point Guide; Australian Computer Emergency Response Team: UNIX Security Checklist v2.0; Hardening Solaris: Creating a Diamond in the Rough, Parts I and II; The UNIX Auditor's Practical Handbook; Personal Knowledge and Experience.

Control Objective: To verify that individual accounts exist for each administrator on the system, and that default system accounts have been removed, disabled, and/or been given a false shell; and to verify that the related files have appropriate permissions and ownership.

Risk: An unused account on the system may be used as a means of gaining unauthorized access to the system; verification of the file permissions, whether the accounts have been deleted or disabled and given false shells are several means of securing the default accounts created during OS installation against misuse.

Testing:	
Command:	Results:
# more /etc/passwd	The file will be displayed a page at a time. The first item in each line is an individual user account. Verify that the accounts exist for individual administrators, and that the accounts listed in Item 9 have been removed. If they exist, verify that an NP or an LK is in the password field of /etc/shadow

Testing:	
Command:	Results:
# more /etc/passwd	The last item (items are separated by colons) is the path of the login shell. For disabled users, verify that no valid shell exists (e.g., a disabled user may have a null shell, or /dev/null).
# more /etc/shadow	The file will be displayed a page at a time. The second item (items are separated by colons) is the password field. An NP indicates that the account owns processes but cannot be used to log into the system. An *LK* indicates that the account is locked.
# ls -la /etc/passwd	Verify that the permissions are 644 (rw- r-- r--); root should be the owner and sys the group
# ls -la /etc/group	Verify that the permissions are 644 (rw- r-- r--); root should be the owner and sys the group

# ls -la /etc/shadow	Verify that the permissions are 400 (r-- --- ---); root should be the owner and sys the group
----------------------	---

Compliance: The tests should verify whether the accounts have been properly deleted or disabled and given false or null login shells, and whether the files have the correct permissions and ownership.

Objective/Subjective: Objective. The accounts indicated should be able to be safely disabled, and the appropriate permissions applied to the files. Any variances should be noted and explained.

Notes:

Item 10 – Operating System: /etc/default/login Settings

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Root login has been restricted to the console (CONSOLE=/dev/console)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Timeout has been set (TIMEOUT=60)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Failed logins are logged (SYSLOG_FAILED_LOGINS=0)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The number of failed login attempts has been limited (RETRIES=3)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Syslog is enabled (SYSLOG=YES)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	An appropriate UMASK has been set (UMASK=027)

Reference: SANS Institute: Solaris Security Step-by-Step, version 2.0; The Center for Internet Security Solaris Benchmark v1.0.1b; How to Strip Down a UNIX OS – Check Point Guide; Australian Computer Emergency Response Team: UNIX Security Checklist v2.0; Hardening Solaris: Creating a Diamond in the Rough, Parts I and II; The UNIX Auditor's Practical Handbook; Personal Knowledge and Experience.

Control Objective: To verify the settings contained in the file /etc/default/login, which controls root login access, whether and after how many failed login attempts a log entry will be made, how many seconds after failed login attempts before another attempt is allowed, whether syslog is enabled, and default system umask settings.

Risk: The configuration settings in this file should be modified to further restrict access to the system, to increase the level of logging performed by the system, and to set an appropriate default umask value to set permissions for future files created on the system.

Testing:	
Command:	Results:
#more /etc/default/login	<p>The file will be displayed a page at a time. As with other files, a # indicates that a value has been commented out and is not used. Verify that the following entries exist, and are not commented out:</p> <p>CONSOLE=/dev/console TIMEOUT=60 SYSLOG_FAILED_LOGINS=0 RETRIES=3 SYSLOG=YES UMASK=027</p>

Compliance: The tests should verify whether the settings in the file are correct.

Objective/Subjective: Objective. The settings indicated should be the minimum settings in the file. Any variances should be noted and explained.

Notes:

Item 11 – Operating System: /etc/default/passwd Settings

Yes	No	N/A	Item
			Maximum expiration, minimum change period, and minimum password length have been set in the /etc/default/passwd file. Verify the following settings:
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	MAXWEEKS = 8 (at most 12 weeks)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	MINWEEKS = 2
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	PASSLENGTH = 8 (at least 8 characters)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	WARNWEEKS = 1

Reference: SANS Institute: Solaris Security Step-by-Step, version 2.0; The Center for Internet Security Solaris Benchmark v1.0.1b; How to Strip Down a UNIX OS – Check Point Guide; Australian Computer Emergency Response Team: UNIX Security Checklist v2.0; Hardening Solaris: Creating a Diamond in the Rough, Parts I and II; The UNIX Auditor's Practical Handbook; Personal Knowledge and Experience.

Control Objective: To verify the settings contained in the file /etc/default/passwd, which controls the amount of time between password expiration, the amount of time before a password may be changed, and the minimum length of the password.

Risk: The configuration settings in this file should be modified to control the behavior of password expiration, length of password, etc. Passwords that never expire, or are very short, may be significant security risks.

Testing:	
Command:	Results:
# cat /etc/default/passwd	Verify that the settings are as indicated.

Compliance: The tests should verify whether the settings in the file are correct.

Objective/Subjective: Objective. The settings indicated should be the minimum settings in the file. Any variances should be noted and explained.

Notes:

Item 12 – Operating System - Network: /etc/system Settings

Yes	No	N/A	Item
			The file /etc/system contains the following lines:

Yes	No	N/A	Item	Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	set noexec_user_stack = 1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	set noexec_user_stack_log = 1
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	set sys:coredumpsize = 0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	set nfssrv:nfs_portmon = 1
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	set maxuprc = 128				

Reference: SANS Institute: Solaris Security Step-by-Step, version 2.0; The Center for Internet Security Solaris Benchmark v1.0.1b; How to Strip Down a UNIX OS – Check Point Guide; Australian Computer Emergency Response Team: UNIX Security Checklist v2.0; Hardening Solaris: Creating a Diamond in the Rough, Parts I and II; The UNIX Auditor's Practical Handbook; Personal Knowledge and Experience.

Control Objective: To prevent some buffer overflow attacks, set limits on resource consumption and prevent core dumps, and force NFS clients to use ports in the privileged port range.

Risk: These settings will improve the security of the system, for instance by protecting against some types of buffer overflows, which may allow arbitrary code to be executed on a system, and by preventing core dumps, which may contain privileged system information.

Testing:	
Command:	Results:
# cat /etc/system	Verify that the settings are as indicated.

Compliance: The tests should verify whether the settings in the file are correct.

Objective/Subjective: Objective. The settings indicated should be contained within the file. Any variances should be noted and explained. (The “coredump” option may be considered to be subjective, as it would be required for forensics activity and for this reason it may be decided to allow core dumps on the system.)

Notes:

Item 13 – Operating System - Network: Miscellaneous

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The file /etc/default/inetinit contains the line TCP_STRONG_ISS=2
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	If necessary, static routes exist, and are included in a startup file; the current routing table in use is consistent with the routes in the startup file
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	If necessary, /etc/defaultrouter exists and contains the IP of the default gateway
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The file /etc/notrouter exists to prevent IP forwarding
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The server is not used as a DNS, DHCP, NIS, or WINS server, or for any other purpose than as intended; No web servers are running on the system; a list of currently open ports on the server has been reviewed and only authorized ports are open

Reference: SANS Institute: Solaris Security Step-by-Step, version 2.0; The Center for Internet Security Solaris Benchmark v1.0.1b; How to Strip Down a UNIX OS – Check Point Guide; Australian Computer Emergency Response Team: UNIX Security Checklist v2.0; Hardening Solaris: Creating a Diamond in the Rough, Parts I and II; The UNIX Auditor’s Practical Handbook; Personal Knowledge and Experience.

Control Objective: To verify various network configuration settings.

Risk: The line TCP_STRONG_ISS sets initial sequence number parameters; 2 is the most secure setting, creating unique sequence numbers per connection ID; static routes should be configured and set within a startup file; the defaultrouter file is used to define the default gateway if necessary; the notrouter file will prevent IP forwarding; and the server should not be used for any other purpose than intended.

These settings will improve the security of the system, for instance by generating unique sequence numbers, increasing the difficulty of an attacker predicting the initial sequence

number. Setting static routes in a startup file will make the routes used consistent with each boot, and verifying that the ones currently in use correspond with the startup file will prevent non-permanent routes configured at the command line from being used. The defaultrouter (if necessary) and notrouter files will set the default router, and prevent the system from being used as a router, respectively.

It should be verified that the system is only configured for the intended use, as adding additional services, such as web servers, increase the risk to the system.

Testing:	
Command:	Results:
# cat /etc/default/inetinit	Verify that the settings are as indicated.
# cat /etc/init.d/Snstaticroutes	Note: staticroutes file name and start number may vary.
# netstat -rn	Prints current routing table for comparison with staticroutes file
# cat /etc/defaultrouter	Will display the contents of the file, if it exists
Command:	Results:
# ls /etc/notrouter	Will list the file if it exists; if the file exists, it will be an empty file
# netstat -an	Will display listening ports on the system; any open ports should be verified against a port list to verify that they are authorized to be open. (The command will also display current connection information.)

Compliance: The tests should verify whether the settings are correct.

Objective/Subjective: Objective. The desired settings should be verified against the system configuration, comparisons made between routing tables and the static routes file, and that only authorized ports are open should be confirmed.

Notes:

Item 14 – Operating System – Network: /etc/init.d/inetinit file

Yes	No	N/A	Item
			The file /etc/init.d/inetinit contains the following lines (note: some administrators prefer to add these settings in a different file):
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/tcp tcp_conn_req_max_q0 10240 (note: min 4096)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/ip ip_ire_arp_interval 60000
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/arp arp_cleanup_interval 60000

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/ip ip_forward_directed_broadcasts 0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/ip ip_forward_src_routed 0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/ip ip6_forward_src_routed 0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/ip ip_forwarding 0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/tcp tcp_ip_abort_cinterval 60000
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp 0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/ip ip_respond_to_address_mask_broadcast 0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/ip ip6_forwarding 0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/ip ip_strict_dst_multihoming 1
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/ip ip6_strict_dst_multihoming 1
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/ip ip_send_redirects 0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/ip ip6_send_redirects 0
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/ip ip_ignore_redirect 1
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/usr/sbin/ndd -set /dev/ip ip6_ignore_redirect 1

Reference: SANS Institute: Solaris Security Step-by-Step, version 2.0; The Center For Internet Security Solaris Benchmark v1.0.1b; How to Strip Down a UNIX OS – Check Point Guide; Australian Computer Emergency Response Team: UNIX Security Checklist v2.0; Hardening Solaris: Creating a Diamond in the Rough, Parts I and II; The UNIX Auditor's Practical Handbook; Personal Knowledge and Experience.

Control Objective: To verify settings in the /etc/init.d/inetinit file.

Risk: The indicated settings in the inetinit file will modify different network parameters within the operating system kernel, modifying how the system reacts to various network stimuli.

Testing:	
Command:	Results:
# more /etc/init.d/inetinit	Note: The settings may be modified in a different start script. Verify that the settings are as indicated.

Compliance: The tests should verify whether the settings in the file are correct.

Objective/Subjective: Subjective. The settings indicated are recommendations to enhance the security of the system. Some of these configuration settings may not be able to be implemented due to interference with other software installed on the system. Any variances should be noted and explained.

Notes:

Item 15 – Operating System: Auditing and Logging

Yes	No	N/A	Item
			The file /etc/security/audit_control contains the following lines:
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	naflags: lo, ad flags: lo, ad, fc, fm, fd
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The file /etc/syslog.conf contains the entry: auth.info /var/log/authlog
			The following files exist, and have permissions 600 and are owned by root and group sys:
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/var/log/loginlog
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	/var/log/authlog
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The Sun Basic Security Module (BSM) has been enabled to audit Kernel activity
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The operating system log files are backed up on a daily basis and stored for a minimum of 12 months

Reference: SANS Institute: Solaris Security Step-by-Step, version 2.0; The Center For Internet Security Solaris Benchmark v1.0.1b; How to Strip Down a UNIX OS – Check Point Guide; Australian Computer Emergency Response Team: UNIX Security Checklist v2.0; Hardening Solaris: Creating a Diamond in the Rough, Parts I and II; The UNIX Auditor's Practical Handbook; Personal Knowledge and Experience.

Control Objective: To verify that appropriate logging is being done on the system.

Risk: The indicated settings in the /etc/security/audit_control will audit logins, logouts, administrative activities, file creation, modification, and deletion (viewed through the praudit command). The loginlog and authlog files will capture information about failed login attempts, su attempts, and reboot information. BSM captures comprehensive information about system activity.

Improper system auditing means that important security events may go unnoticed. The caveat, of course, is that the logs must be reviewed on a regular and recurring basis to look for potential security events.

Testing:	
Command:	Results:
# cat /etc/security/audit_control	Verify that the settings are as indicated
# cat /etc/syslog.conf	Verify that the auth.info entry exists as indicated
# ls -la /var/log/loginlog	Verify that the file exists with appropriate permissions and ownership
# ls -la /var/log/authlog	Verify that the file exists with appropriate permissions and ownership
# ps -ef or: # /usr/sbin/auditconfig -getcond	Verify that the auditd process is running to verify that BSM has been enabled
	Look for "condition = auditing" to verify that BSM has been enabled

Compliance: The tests should verify whether the settings are correct, the files exist, and that BSM has been enabled.

Objective/Subjective: Objective. The system settings are recommended to improve the auditing of the system and provide a valuable audit trail.

Notes:

Item 16 – Operating System: Scheduled operations (cron and at jobs)

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Unused crontab files have been deleted (/var/spool/cron/crontabs – especially adm and lp)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The files /etc/cron.d/cron.allow and /etc/cron.d/at.allow exist with the permissions 400, owned by root and group sys, and contain only an entry for user root or other allowed user(s)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The files /etc/cron.d/cron.deny and /etc/cron.d/at.deny do not exist (only if the files cron.allow and at.allow exist with appropriate permissions)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The file /etc/default/cron contains the entry: CRONLOG=YES

Reference: SANS Institute: Solaris Security Step-by-Step, version 2.0; The Center For Internet Security Solaris Benchmark v1.0.1b; How to Strip Down a UNIX OS – Check Point Guide; Australian Computer Emergency Response Team: UNIX Security Checklist v2.0; Hardening Solaris: Creating a Diamond in the Rough, Parts I and II; The UNIX Auditor's Practical Handbook; Personal Knowledge and Experience.

Control Objective: To verify that unnecessary crontabs have been deleted, that only authorized users are allowed to schedule cron jobs, and to verify that cron activity is being logged.

Risk: The settings will verify that no unscheduled cron activity is taking place on the system, that only authorized users may schedule cron jobs, and that all cron activity is logged. It is undesirable to have unauthorized users to be able to schedule jobs to run on the system.

Testing:	
Command:	Results:
# ls /var/spool/cron/crontabs	Verify that unused crontab files have been deleted, especially adm and lp.
# ls -la /etc/cron.d/cron.allow and # ls -la /etc/cron.d/at.allow	Verify that the file exists with the appropriate permissions and ownership.
# ls -la /etc/cron.d/cron.deny and # ls -la /etc/cron.d/at.deny	Verify that the files do not exist.
# cat /etc/cron.d/cron.allow and # cat /etc/cron.d/at.allow	Verify that only authorized users are in the file.
# cat /etc/default/cron	Verify that the entry CRONLOG=YES is in the file.

Compliance: The tests should verify whether the settings are correct.

Objective/Subjective: Objective. The settings, file permissions and ownership, and logging settings are appropriate to verify that only proper cron activity is taking place on the system.

Notes:

Item 17 – Operating System: /etc/vfstab Mount Options

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The /usr partition is mounted read-only

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Other file systems are mounted “nosuid” where possible

Reference: SANS Institute: Solaris Security Step-by-Step, version 2.0; The Center For Internet Security Solaris Benchmark v1.0.1b; How to Strip Down a UNIX OS – Check Point Guide; Australian Computer Emergency Response Team: UNIX Security Checklist v2.0; Hardening Solaris: Creating a Diamond in the Rough, Parts I and II; The UNIX Auditor’s Practical Handbook; Personal Knowledge and Experience.

Control Objective: To verify that file systems are mounted with restrictive options.

Risk: The /usr directory contains operating system binaries which may be replaced with Trojan or rootkit versions; to prevent this, the /usr directory should be mounted read-only. Set user-id (SUID) can be used to allow an executable file to run with permissions of the user or group owner instead of those of the user that created the process. This can be used by a malicious user to elevate privileges, and should be secured against where possible.

Testing:	
Command:	Results:
# cat /etc/vfstab	Verify that the mount options for the various file systems.

Compliance: The tests outlined should verify compliance.

Objective/Subjective: Objective. The settings can be verified through the tests outlined; however, there may be reasons why the particular file systems should not be mounted with more restrictive options.

Notes:

Item 18 – Operating System: Miscellaneous

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Time synchronization (NTP) is used on the server
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The directory /tmp has the “sticky-bit” set so that only file owners may remove files (chmod + t /tmp)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The file /etc/hosts.equiv does not exist, or an empty file exists with permissions 000

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	TCP Wrappers software is installed
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	File integrity checking software is installed
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Unauthorized access warning messages have been created (/etc/issue, /etc/motd, /etc/issue.net and eeeprom oem-banner) with permissions 644 and owned by root and group sys
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	EEPROM security has been enabled and password protected

Reference: SANS Institute: Solaris Security Step-by-Step, version 2.0; The Center For Internet Security Solaris Benchmark v1.0.1b; How to Strip Down a UNIX OS – Check Point Guide; Australian Computer Emergency Response Team: UNIX Security Checklist v2.0; Hardening Solaris: Creating a Diamond in the Rough, Parts I and II; The UNIX Auditor's Practical Handbook; Personal Knowledge and Experience.

Control Objective: To verify that various additional measures have been taken to improve security on the system.

Risk: Secure time synchronization will help with correlation of the IDS logs with other system logs; setting the “sticky bit” on the /tmp directory will restrict removal of files to their owners; the file hosts.equiv allows hosts identified within this file to access the system without authentication via password; TCP Wrappers allows for more granular control over which hosts can use which available services, and provides additional logging capabilities; file integrity software takes a snapshot of selected files and monitors if they are modified; warning messages upon login are a notice to users that their activities may be monitored and may provide some legal benefit in case of system breach; EEPROM passwords help protect a system in the event physical access protections are defeated.

Testing:	
Command:	Results:
# ls -la /	Verify that the long listing displays a “t” at the end of the list of permissions for the tmp directory
# ls -la /etc/hosts.equiv	Verify that the file does not exist, or has permissions of 000
# ls -la /etc/motd # ls -la /etc/issue # ls -la /etc/issue.net	Verify that the files exist with appropriate permissions and ownership (644 and root owner and group sys).
# cat /etc/motd # cat /etc/issue # cat /etc/issue.net	Verify that the banner warning messages contained in the files contain appropriate text.

Testing (continued): Log onto the system and verify that a banner message appears. Verify with the administrator whether or not file integrity software is installed, TCP Wrappers is installed and in use. Reboot the system and verify whether an EEPROM-level password is in place.

Compliance: The tests outlined should verify compliance.

Objective/Subjective: Objective and Subjective. Certain items, such as the “sticky bit” setting are objective; others, such as whether the text of the /etc/issue file is appropriate, or whether file integrity software is in use, are subjective.

Notes:

Item 19 – Open SSH: Configuration

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A current version of Open SSH is in use.
			The /etc/sshd_config file contains the following parameters (parameters are indicated after the = sign, but it should not appear in the sshd_config file):

Yes	No	N/A	Item	Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	ListenAddress = non-stealth interface IP address	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LoginGraceTime = 120
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Protocol = 2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	KeyRegenerationInterval = 3600
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	PermitRootLogin = no	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IgnoreRhosts = yes
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	StrictModes = yes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IgnoreUserKnownHosts = yes
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LogLevel = INFO	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	SyslogFacility = AUTH
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	RhostsRSAAuthentication = no	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	RhostsAuthentication = no
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	RSAAuthentication = no	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	HostbasedAuthentication = no
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	PasswordAuthentication = no	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	PermitEmptyPasswords = no

Reference: Personal Knowledge and Experience; CERT® Coordination Center SSH Implementation Guide (http://www.cert.org/security-improvement/implementations/i062_01.html)

Control Objective: To verify a secure configuration of Open SSH on the Network Intrusion Detection System.

Risk: The risk of an incorrectly configured Open SSH installation, in particular allowing the use of older, weaker encryption algorithms or access to SSH on the incorrect interface, are that it may reduce the effectiveness of using a secure alternative to Telnet

or FTP for remote access, thereby exposing the system to access by unauthorized individuals.

Testing:	
Command:	Results:
# /usr/local/bin/ssh -V	Command will display the version of Open SSH in use. Current Open SSH version: _____ Version in use on system: _____
# more /usr/local/etc/sshd_config	Verify that the settings match those outlined in Item 19.

Compliance: The version of Open SSH should be the latest available, and the configurations settings should match those indicated in item 19.

Objective/Subjective: Objective.

Notes:

Item 20 – Network IDS: Verification of Stealth Interface

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The stealth interface is configured with no IP address.

Reference: Personal Knowledge and Experience.

Control Objective: To verify that the stealth interface is configured correctly, that is, with no IP address.

Risk: The risks of an incorrectly configured stealth interface are that the system may be compromised. These risks are outlined in detail in the portion of this document regarding consequences of a system compromise, section 1.2.1.

Testing:	
Command:	Results:
# ifconfig - a	The command will display the network parameters for all interfaces; it should be verified that the interface to be the stealth interface should be configured with no IP address (i.e., an IP address of 0.0.0.0).

Testing (continued): From the Real Secure Workgroup Manager GUI, select the network sensor from the list of **Managed Assets** and then view the **Properties** of the sensor. Click the **Adapters** tab and verify that the correct interface is listed with no IP address (i.e., an IP address of 0.0.0.0).

Compliance: The tests outlined should verify that the stealth interface is configured correctly.

Objective/Subjective: Objective.

Notes:

Item 21 – ISS Real Secure Network Sensor: Configuration

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The most current version of the ISS Real Secure network sensor is in use, and the latest ISS Real Secure X-Press Update has been applied.
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Verify the current ISS Real Secure network sensor policy.

Reference: Personal Knowledge and Experience.

Control Objective: To verify that the ISS Real Secure network sensor is using the latest available sensor engine and attack signatures, and that the policy installed on the sensor is appropriate.

Risk: The risks of an out of date sensor configuration are the same as with any software that is not kept current, i.e., software bugs and vulnerabilities may exist on the system which could be exploited to disrupt service or take control of the system. An appropriate sensor configuration is largely subjective, but the system must be configured such that it is effective at detecting network anomalies that may be indicative of attempted intrusions.

Testing: The current version and X-Press Update (XPU) and the current policy may be verified from the Workgroup Manager console.

Compliance: The current version of the software and the latest XPU should be installed. The Real Secure network sensor policy should be effective at detecting potential intrusions or other malicious network traffic.

Objective/Subjective: Current version: Objective; Policy: Subjective.

Notes:

Item 22 – Network-based Assessment

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The ISS Real Secure Network Sensor detects various scans from tools such as NMAP.

Reference: Personal Knowledge and Experience.

Control Objective: To verify that the ISS Real Secure network sensor detects various scans including OS fingerprinting and stealth scanning, etc.

Risk: A scan of the network is typically the first phase (reconnaissance) of an attack. It is therefore important that the IDS detect this activity.

Testing: Scan systems on the network on which the IDS is located using various options available with NMAP.

Compliance: The IDS should detect the traffic.

Objective/Subjective: Objective.

Notes:

Item 23 – Anomalous Traffic Assessment

Yes	No	N/A	Item
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The ISS Real Secure Network Sensor detects various forms of anomalous traffic.

Reference: Personal Knowledge and Experience.

Control Objective: To verify that the ISS Real Secure network sensor detects anomalous traffic.

Risk: The purpose of the IDS device is to detect anomalous traffic. If it does not, nefarious activity may occur unnoticed.

Testing: Configure systems external and internal to the network monitored by the IDS and determine whether potentially malicious traffic between the two systems is detected.

Compliance: The IDS should detect the nefarious traffic.

Objective/Subjective: Objective.

Notes:

3 Conduct the Audit

The full audit was conducted on the system as outlined in section 2. The following items represent the more critical security concerns for the Network IDS.

3.1 Item 3 – Verification of Networking Information

Control Objective: To verify that the documented network information, including IP addresses, hostname, routing tables, and network diagrams, match that of the actual configuration.

Documentation of the system network configuration was provided to the auditor beforehand, and a comparison made during the audit.

Yes	No	N/A	Item
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Actual system network information including MAC Address, hostname, network interface, IP address, subnet mask, default gateway, and DNS information matches the documentation.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Routing tables, network diagrams, and other network information in the operating system documentation matches the actual system configuration

Testing:

Command: `ifconfig -a`

Output:

```
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
hme0: flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 0.0.0.0 netmask 0
    ether 8:0:20:d1:5b:e9
hme1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
    inet 10.200.200.150 netmask ff000000 broadcast 10.255.255.255
    ether 8:0:20:d1:5b:e9
```

Analysis:

The results of the command show that the interfaces are configured as documented, with the exception of the subnet mask. The subnet mask is ff000000 (255.0.0.0) for the hme1 address, which should be modified to 255.255.255.0 as is indicated in the documentation.

Testing:**Command:** `cat /etc/hosts`**Output:**

```
#  
# Internet host table  
#  
127.0.0.1    localhost    loghost  
10.200.200.150    ISS1
```

Analysis:

The results of the command show the same information as the documentation.

Testing:**Command:** `cat /etc/defaultrouter`**Output:**

```
10.200.200.1
```

Analysis:

The results of the command show that the default router configuration matches the documentation.

Testing:**Command:** `cat /etc/nsswitch.conf`**Output:**

```
#  
# /etc/nsswitch.files:  
#  
# An example file that could be copied over to /etc/nsswitch.conf; it  
# does not use any naming service.  
#  
# "hosts:" and "services:" in this file are used only if the  
# /etc/netconfig file has a "-" for nametoaddr_libs of "inet" transports.  
  
passwd:      files  
group:       files  
hosts:       files  
ipnodes:     files  
networks:    files  
protocols:   files  
rpc:         files  
ethers:      files  
netmasks:    files  
bootparams:  files  
publickey:   files  
# At present there isn't a 'files' backend for netgroup; the system will  
# figure it out pretty quickly, and won't use netgroups at all.  
netgroup:    files  
automount:   files  
aliases:     files  
services:    files  
sendmailvars: files  
printers:    user files  
  
auth_attr:   files  
prof_attr:   files  
project:     files
```

Analysis:

The results of the command match that of the documentation; the nsswitch file indicates that only files will be consulted for resolution.

Testing:**Command:** `netstat -rn`**Output:**

```
Routing Table: IPv4
  Destination      Gateway         Flags   Ref       Use    Interface
  -----
10.0.0.0           10.200.200.150    U        1         0     hme1
224.0.0.0          127.0.0.1        U        1         0     lo0
127.0.0.1          127.0.0.1        UH       1         0     lo0
```

Analysis:

The results of the command indicate that only one route exists; the route should be further constrained, perhaps to only the 10.200.200.0 network, or even further, to a single IP. The entry above is due to the improperly configured subnet mask. The routing tables were undocumented.

Testing:**Command:** `netstat -an`**Output:**

See screenshot – figure 2.

Analysis:

The results of the command show that ports listening on the system are those required by Real Secure for communication between the Workgroup Manager and the network sensor (i.e., 901/tcp and 2998/tcp), and port 22/tcp for SSH communication. Additionally, in the screenshot connections to and from the localhost can be seen (e.g., 32768 – 327769). These are not ports open and listening on the system.

Additionally, port 514/udp, which allows syslog to receive logs from remote systems, is listening. This port is not required and should be closed.

```
# netstat -an

UDP: IPv4
  Local Address      Remote Address      State
  -----
    *.514
127.0.0.1.32768      Idle
127.0.0.1.32769      Idle
127.0.0.1.32770      Idle
127.0.0.1.32771      Idle
127.0.0.1.32772      Idle
127.0.0.1.32773      Idle
127.0.0.1.32774      Idle
127.0.0.1.32775      Idle
127.0.0.1.32776      127.0.0.1.32770    Connected
    *.*
    *.*              Unbound

TCP: IPv4
  Local Address      Remote Address      Swind Send-Q Rwind Recv-Q  State
  -----
    *.*              *.*                0      0 24576      0 IDLE
10.200.200.150.22    *.*                0      0 24576      0 LISTEN
    *.2998           *.*                0      0 24576      0 LISTEN
127.0.0.1.32768      *.*                0      0 24576      0 LISTEN
10.200.200.150.22    10.200.200.3.1550  63580   43 24820      0 ESTABLISHED
127.0.0.1.32769      *.*                0      0 24576      0 LISTEN
127.0.0.1.32770      *.*                0      0 24576      0 LISTEN
127.0.0.1.32771      *.*                0      0 24576      0 LISTEN
127.0.0.1.32772      *.*                0      0 24576      0 LISTEN
127.0.0.1.32773      *.*                0      0 24576      0 LISTEN
    *.901            *.*                0      0 24576      0 LISTEN
10.200.200.150.901    10.200.200.3.1551  63493   0 24820      0 ESTABLISHED
127.0.0.1.32774      127.0.0.1.32769    32768   0 32768      0 ESTABLISHED
127.0.0.1.32769      127.0.0.1.32774    32768   0 32768      0 ESTABLISHED
    *.*              *.*                0      0 24576      0 IDLE
```

Connected to 10.200.200.150 SSH2 - 3des-cbc - hmac-sha1 - none 86x36 3, 51 00:10:22

Figure 2: Output of the netstat -an command

Testing:

Command: **Other:** Verify that information on diagrams (IP addresses, interface names, cables connected to switches, etc.) match the physical connections in the network

Analysis:

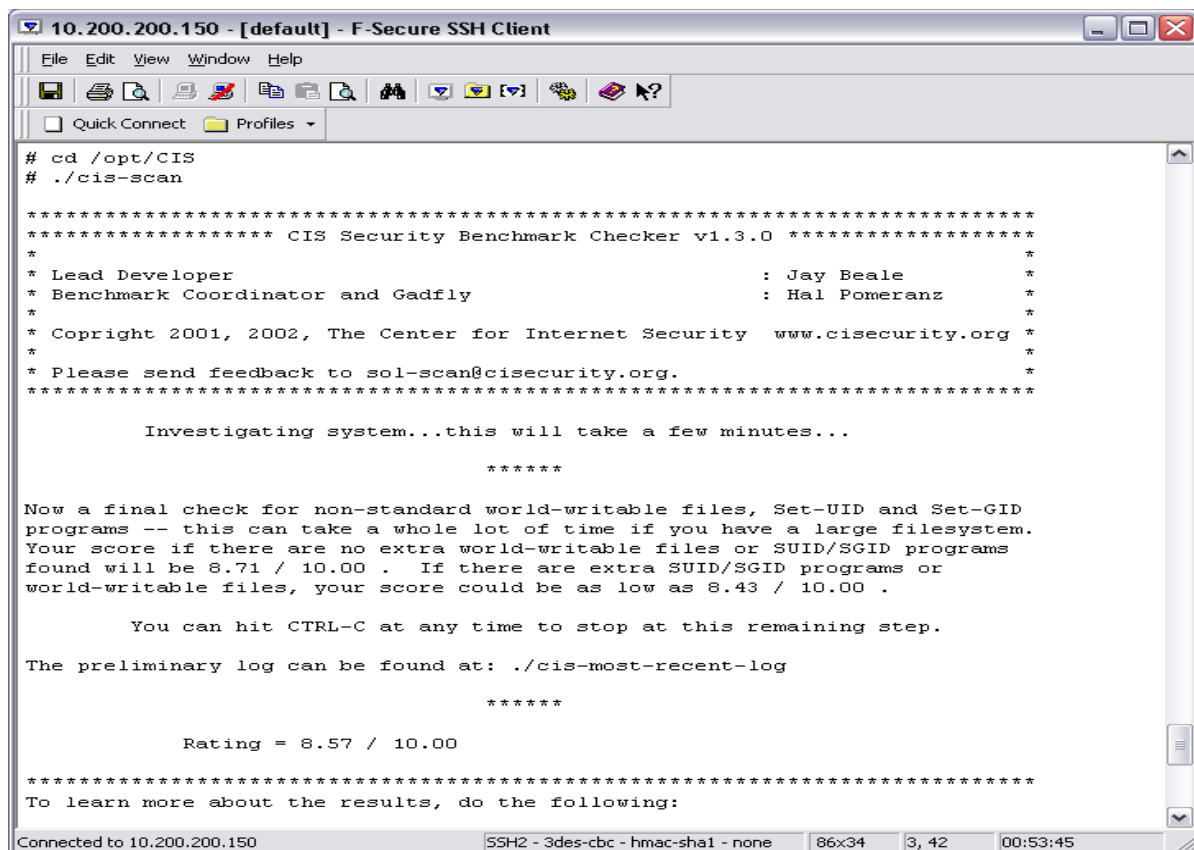
The main network diagram (see figure 1 on page 5 of this document) is lacking information such as firewall interface (e.g., hme0, qfe0) and IP address information, switch port information, etc. This information would be very useful not only in conducting the audit, but also potentially when troubleshooting problems.

3.2 Item 6 – Operating System: Verification of Hardening

Control Objective: To apply an objective, 3rd party tool as a review of system hardening

Yes	No	N/A	Item
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A utility (such as CIS-SCAN from The Center For Internet Security) is used to verify system hardening.

Testing:	
Command:	Results:
# cd /opt/CIS/	Change to the directory where the CIS tool is installed
# ./cis-scan	Runs the scan
Output:	
See screenshots – figures 3 and 4.	
Analysis:	
The results of the scan were very good, an overall score of 8.57 out of a possible 10. The individual items found to be negative would require only minor configuration changes to become positive items.	
An example would be that inetd was found to be active; while this is certainly the case, the inetd.conf file is empty and therefore does not start any services. This could therefore easily be disabled entirely.	
A further example would be that the /etc/shells file, which lists the known accepted shells allowed on the system, does not exist. If this file does not exist then any program can be used as a valid user shell. It would be a fairly routine task to rectify this.	



10.200.200.150 - [default] - F-Secure SSH Client

```
# cd /opt/CIS
# ./cis-scan

*****
***** CIS Security Benchmark Checker v1.3.0 *****
*
* Lead Developer                      : Jay Beale
* Benchmark Coordinator and Gadfly    : Hal Pomeranz
*
* Copright 2001, 2002, The Center for Internet Security www.cisecurity.org
*
* Please send feedback to sol-scan@cisecurity.org.
*****

Investigating system...this will take a few minutes...

*****

Now a final check for non-standard world-writable files, Set-UID and Set-GID
programs -- this can take a whole lot of time if you have a large filesystem.
Your score if there are no extra world-writable files or SUID/SGID programs
found will be 8.71 / 10.00 . If there are extra SUID/SGID programs or
world-writable files, your score could be as low as 8.43 / 10.00 .

You can hit CTRL-C at any time to stop at this remaining step.

The preliminary log can be found at: ./cis-most-recent-log

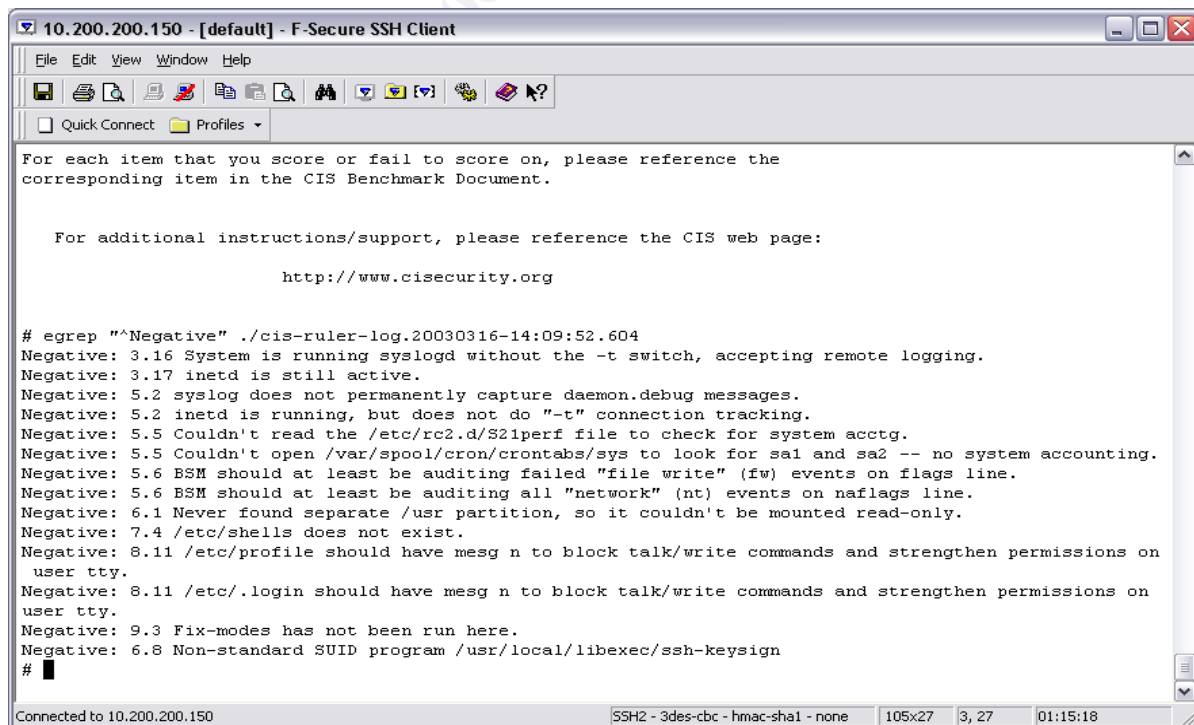
*****

Rating = 8.57 / 10.00

*****
To learn more about the results, do the following:
*****
```

Connected to 10.200.200.150 SSH2 - 3des-cbc - hmac-sha1 - none 86x34 3, 42 00:53:45

Figure 3: CIS Scan Results Overview



10.200.200.150 - [default] - F-Secure SSH Client

```
For each item that you score or fail to score on, please reference the
corresponding item in the CIS Benchmark Document.

For additional instructions/support, please reference the CIS web page:

http://www.cisecurity.org

# egrep "^Negative" ./cis-ruler-log.20030316-14:09:52.604
Negative: 3.16 System is running syslogd without the -t switch, accepting remote logging.
Negative: 3.17 inetd is still active.
Negative: 5.2 syslog does not permanently capture daemon.debug messages.
Negative: 5.2 inetd is running, but does not do "-t" connection tracking.
Negative: 5.5 Couldn't read the /etc/rc2.d/S21perf file to check for system acctg.
Negative: 5.5 Couldn't open /var/spool/cron/crontabs/sys to look for sa1 and sa2 -- no system accounting.
Negative: 5.6 BSM should at least be auditing failed "file write" (fw) events on flags line.
Negative: 5.6 BSM should at least be auditing all "network" (nt) events on naflags line.
Negative: 6.1 Never found separate /usr partition, so it couldn't be mounted read-only.
Negative: 7.4 /etc/shells does not exist.
Negative: 8.11 /etc/profile should have mesg n to block talk/write commands and strengthen permissions on
user tty.
Negative: 8.11 /etc/.login should have mesg n to block talk/write commands and strengthen permissions on
user tty.
Negative: 9.3 Fix-modes has not been run here.
Negative: 6.8 Non-standard SUID program /usr/local/libexec/ssh-keysign
#
```

Connected to 10.200.200.150 SSH2 - 3des-cbc - hmac-sha1 - none 105x27 3, 27 01:15:18

Figure 4: CIS Scan - Detailed Results

3.3 Item 7 – Operating System: Start Scripts

Control Objective: To verify that unnecessary services have been disabled at all run levels (/etc/rc*.d), especially:

Yes	No	N/A	Item	Yes	No	N/A	Item	Yes	No	N/A	Item
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	affbinit	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	lifbinit	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	rpc
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	asppp	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	llc2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	savecore
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	autofs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	lp	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	sendmail
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	autoinstall	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	mipagent	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	slpd
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	bdconfig	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	ncad	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	snmpdx
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	cacheofs.daemon	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	ncalogd	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	spc
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	cacheofs.finish	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	nfs.client	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	sysid.net
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	dmi	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	nfs.server	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	sysid.sys
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	dtlogin	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	nscd	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	uucp
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	power	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	wbem	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	ldap.client
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	PRESERVE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	flashprom	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	xntpd

Testing:

Command: `cd /etc/init.d/rc*.d`

Command: `ls`

Command: `ps -ef`

Output:

See screenshots – figures 5 and 6.

Analysis:

The results indicate that only necessary services are started at system boot, and listing of currently running processes corroborates this finding.

```

10.200.200.150 - [default] - F-Secure SSH Client
File Edit View Window Help
[Icons]
[Quick Connect] [Profiles]
# cd /etc/rc2.d
# ls
K28nfs.server      S74syslog          dS30sysid.net      dS75savecore
README             S75cron            dS71ldap.client    dS76nscd
S01MOUNTFSYS       S88utmpd           dS71rpc            dS88sendmail
S05RMTMPFILES      S98sshd            dS71sysid.sys      dS93cacheofs.finish
S20syssetup        S99audit           dS72autoinstall    dSautofs
S69inet            S99realsecure      dS73cacheofs.daemon
S72inetsvc         d80PRESERVE        dS73nfs.client
# cd ../rc3.d
# ls
README             dS15nfs.server
#

```

Connected to 10.200.200.150 | SSH2 - 3des-cbc - hmac-sha1 - none | 81x14 | 3, 13 | 00:12:38

Figure 5: Listing of run levels rc2.d and rc3.d

Figure 6: Output of ps -ef command

3.4 Item 9 – Operating System: Accounts

Control Objective: To verify that individual accounts exist for each administrator, that unnecessary default system accounts have been removed, disabled and/or given a false shell, and to verify that the related files have appropriate permissions and ownership.

Yes	No	N/A	Item
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Individual, unique accounts have been created for each administrator (/etc/passwd)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Unnecessary accounts, including the following, have been removed (accounts may be removed or NP in password field of /etc/shadow):

Yes	No	N/A	Item	Yes	No	N/A	Item	Yes	No	N/A	Item
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	sys	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	uucp	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	lp
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	listen	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	nuucp	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	smtp
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	nobody4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Yes	No	N/A	Item
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A /dev/null or false shell has been created for any of these users remaining on the system (/etc/passwd)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The files /etc/passwd and /etc/group have permissions 644 and are owned by root and group sys
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The file /etc/shadow has permissions 400 and is owned by root and group sys

Testing:

Command: cat /etc/passwd

Command: ls -la /etc/passwd

Command: ls -la /etc/group

Command: ls -la /etc/shadow

Output:

See screenshot – figure 7.

Analysis:

Multiple users will be administering the system, but only one administrative account has been created. Unnecessary system accounts have been removed from the system; additional user accounts have /dev/null shells. The files have the appropriate modes and ownership.

The screenshot shows an F-Secure SSH Client window titled "10.200.200.150 - [default] - F-Secure SSH Client". The terminal displays the output of the following commands:

```
# cat /etc/passwd
root:x:0:1:Super-User:/:/sbin/sh
daemon:x:1:1:/:/dev/null
bin:x:2:2:/:usr/bin:/dev/null
adm:x:4:4:Admin:/var/adm:/dev/null
nobody:x:60001:60001:Nobody:/:/dev/null
noaccess:x:60002:60002:No Access User:/:/dev/null
sshd:x:100:100:sshd privsep:/var/empty:/dev/null
dcm:x:101:1:~/home/dcm:/bin/sh
# ls -la /etc/passwd /etc/group /etc/shadow
-rw-r--r--  1 root    sys      271 Mar 12 12:42 /etc/group
-r--r--r--  1 root    sys      294 Mar 16 15:02 /etc/passwd
-r-----  1 root    sys      188 Mar 13 17:10 /etc/shadow
#
```

The status bar at the bottom indicates the connection is established to 10.200.200.150 using SSH2 with 3des-cbc, hmac-sha1, and none for compression. The window size is 67x14 and the cursor is at line 3, column 14.

Figure 7: Review of system accounts

3.5 Item 10 – Operating System: /etc/default/login Settings

Control Objective: To verify the settings in the /etc/default/login file, which controls where root may login from, whether failed logins are logged, whether syslog should be enabled, and also sets the default UMASK on the system.

Yes	No	N/A	Item
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Root login has been restricted to the console (CONSOLE=/dev/console)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Timeout has been set (TIMEOUT=60)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Failed logins are logged (SYSLOG_FAILED_LOGINS=0)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The number of failed login attempts has been limited (RETRIES=3)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Syslog is enabled (SYSLOG=YES)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	An appropriate UMASK has been set (UMASK=027)

Testing:

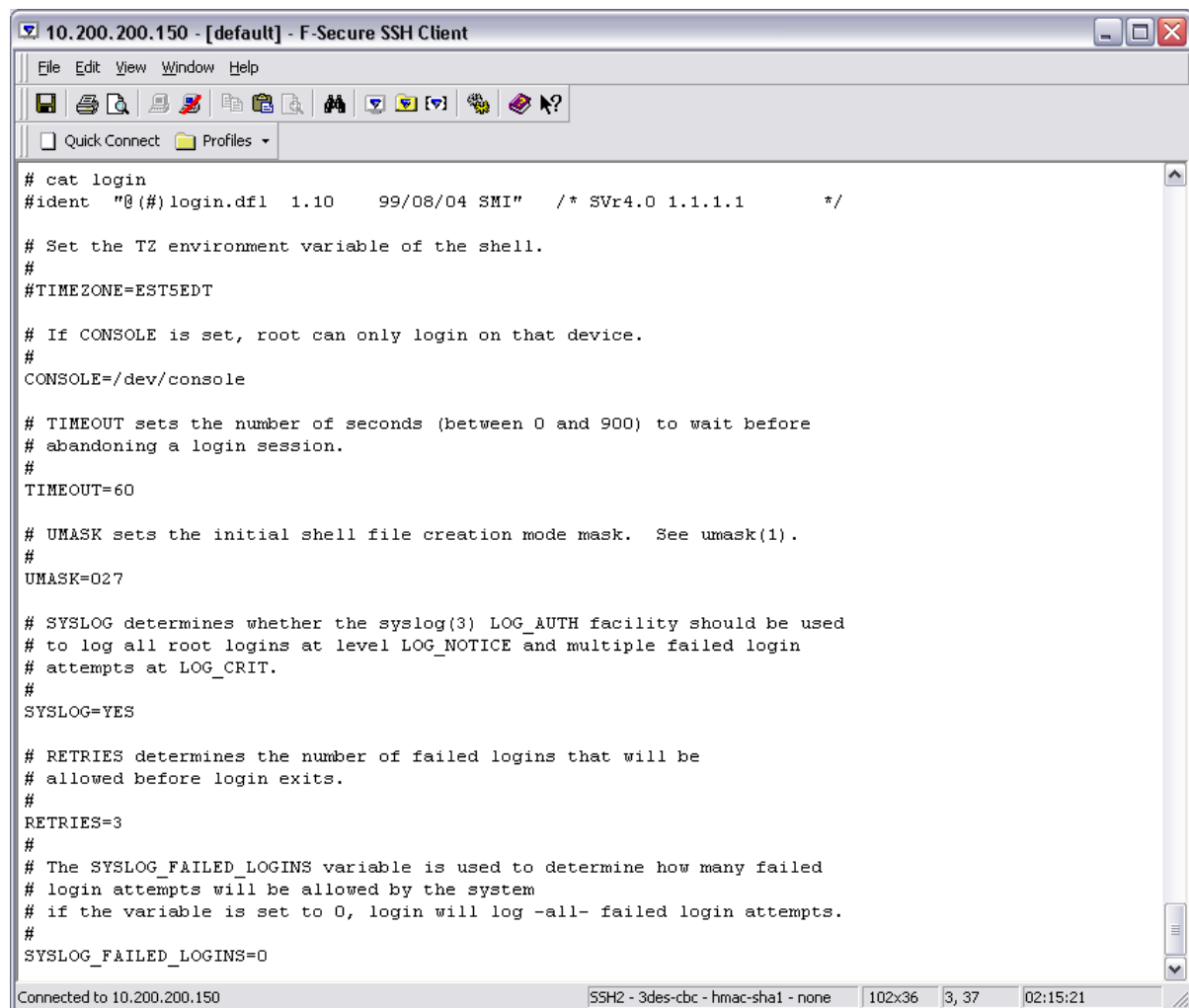
Command: cat /etc/default/login

Output:

See screenshots - figure 8.

Analysis:

The settings in the /etc/default/login file match those recommended.



```
# cat login
#ident  "(#)login.dfl  1.10    99/08/04 SMI"   /* SVr4.0 1.1.1.1    */

# Set the TZ environment variable of the shell.
#
#TIMEZONE=EST5EDT

# If CONSOLE is set, root can only login on that device.
#
CONSOLE=/dev/console

# TIMEOUT sets the number of seconds (between 0 and 900) to wait before
# abandoning a login session.
#
TIMEOUT=60

# UMASK sets the initial shell file creation mode mask.  See umask(1).
#
UMASK=027

# SYSLOG determines whether the syslog(3) LOG_AUTH facility should be used
# to log all root logins at level LOG_NOTICE and multiple failed login
# attempts at LOG_CRIT.
#
SYSLOG=YES

# RETRIES determines the number of failed logins that will be
# allowed before login exits.
#
RETRIES=3
#
# The SYSLOG FAILED_LOGINS variable is used to determine how many failed
# login attempts will be allowed by the system
# if the variable is set to 0, login will log -all- failed login attempts.
#
SYSLOG_FAILED_LOGINS=0
```

Connected to 10.200.200.150 SSH2 - 3des-cbc - hmac-sha1 - none 102x36 3, 37 02:15:21

Figure 8: /etc/default/login settings

3.6 Item 11 – Operating System: /etc/default/passwd Settings

Control Objective: Review of the settings in /etc/default/passwd, which controls the time between password expiration, the time allowed between password changes, minimum password length, and number of weeks of notification before the password expires.

Yes	No	N/A	Item
			Maximum expiration, minimum change period, and minimum password length have been set in the /etc/default/passwd file. Verify the following settings:
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	MAXWEEKS = 8 (at most 12 weeks)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	MINWEEKS = 2
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	PASSLENGTH = 8 (at least 8 characters)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	WARNWEEKS = 1

Testing:

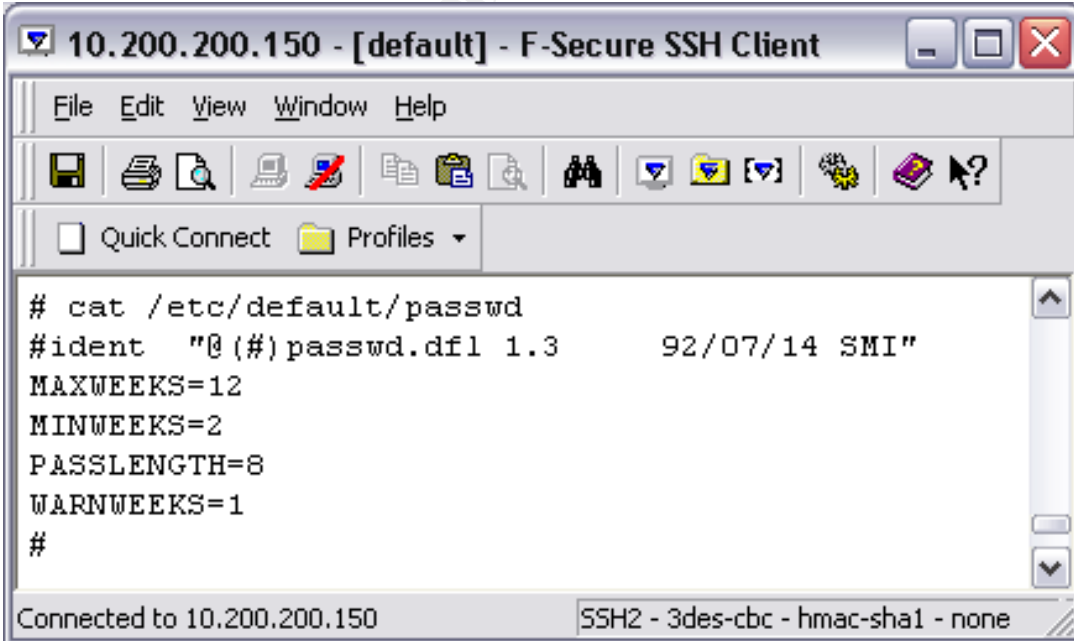
Command: cat /etc/default/passwd

Output:

See screenshot – figure 9.

Analysis:

The settings in the /etc/default/login file match those recommended.



The screenshot shows an F-Secure SSH Client window titled "10.200.200.150 - [default] - F-Secure SSH Client". The window has a menu bar (File, Edit, View, Window, Help) and a toolbar with various icons. Below the toolbar, there is a "Quick Connect" checkbox and a "Profiles" dropdown menu. The main area of the window displays the output of the command "cat /etc/default/passwd" in a terminal-like font. The output is as follows:

```
# cat /etc/default/passwd
#ident  "@(#)passwd.dfl 1.3      92/07/14 SMI"
MAXWEEKS=12
MINWEEKS=2
PASSLENGTH=8
WARNWEEKS=1
#
```

At the bottom of the window, there is a status bar that reads "Connected to 10.200.200.150" and "SSH2 - 3des-cbc - hmac-sha1 - none".

Figure 9: /etc/default/passwd settings

3.7 Item 16 – Operating System: Scheduled operations (cron jobs)

Control Objective: To verify that only authorized users are allowed to schedule automated jobs, that unused crontab files have been deleted, and to verify that cron activity is being logged.

Yes	No	N/A	Item
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Unused crontab files have been deleted (/var/spool/cron/crontabs – especially adm and lp)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The files /etc/cron.d/cron.allow and /etc/cron.d/at.allow exist with the permissions 400, owned by root and group sys, and contain only an entry for user root or other allowed user(s)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The files /etc/cron.d/cron.deny and /etc/cron.d/at.deny do not exist (only if the files in the previous step exist with appropriate permissions)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The file /etc/default/cron contains the entry: CRONLOG=YES

Testing:

Command: `ls -la /var/spool/cron/crontabs`

Command: `ls -la /etc/cron.d/cron.allow /etc/cron.d/at.allow`

Command: `cat /etc/cron.d/cron.allow`

Command: `cat /etc/cron.d/at.allow`

Command: `ls -la /etc/cron.d/cron.deny /etc/cron.d/at.deny`

Command: `cat /etc/default/cron`

Output:

See screenshot – figure 10.

Analysis:

No unnecessary automated jobs exist on the system, appropriate files to restrict authority to create automated jobs exist with appropriate permissions and ownership, and cron activity is being logged.

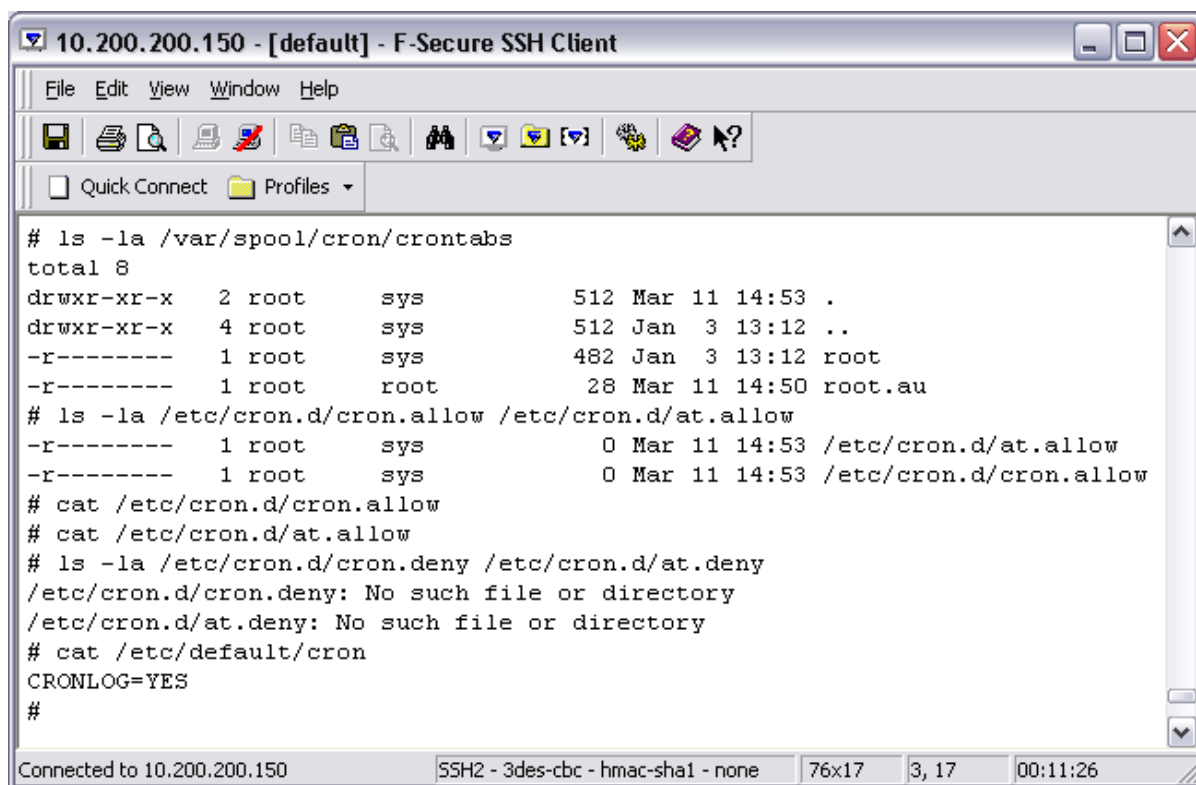


Figure 10: Scheduled Operations (Cron and at)

3.8 Item 19 – Open SSH Configuration

Control Objective: To verify a secure configuration of Open SSH on the Network Intrusion Detection system.

Yes	No	N/A	Item
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A current version of Open SSH is in use.
			The /etc/sshd_config file contains the following parameters (parameters are indicated after the = sign, but it should not appear in sshd_config file):

Yes	No	N/A	Item	Yes	No	N/A	Item
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	ListenAddress = non-stealth interface IP address	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LoginGraceTime = 120
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Protocol = 2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	KeyRegenerationInterval = 3600
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	PermitRootLogin = no	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IgnoreRhosts = yes
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	StrictModes = yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IgnoreUserKnownHosts = yes

Yes	No	N/A	Item	Yes	No	N/A	Item
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LogLevel = INFO	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	SyslogFacility = AUTH
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	RhostsRSAAuthentication = no	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	RhostsAuthentication = no
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	RSAAAuthentication = no	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	HostbasedAuthentication = no
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	PasswordAuthentication = no	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	PermitEmptyPasswords = no

Testing:

Command: `ssh -V`

Output:

See screenshots – figures 11 and 12.

Analysis:

The version of Open SSH in use, version 3.51p, is the latest available.

Testing:

Command: `more /usr/local/etc/sshd_config`

Output:

See screenshot – figure 12.

Analysis:

The configuration of SSH matches that of the recommended configuration.

```
# ./ssh -V
OpenSSH_3.5p1, SSH protocols 1.5/2.0, OpenSSL 0x0090609f
# more /usr/local/etc/sshd_config
#      $OpenBSD: sshd_config,v 1.59 2002/09/25 11:17:16 markus Exp $

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

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

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

Port 22
Protocol 2
ListenAddress 10.200.200.150
#ListenAddress ::

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

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

Figure 11: SSH version information and configuration (part 1)

```
ServerKeyBits 768

# Logging
#obsoletes QuietMode and FascistLogging
SyslogFacility AUTH
LogLevel INFO

# Authentication:

LoginGraceTime 120
PermitRootLogin no
StrictModes yes

RSAAuthentication no
#PubkeyAuthentication yes
#AuthorizedKeysFile      .ssh/authorized_keys

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

Figure 12: SSH Configuration (cont.)

3.9 Item 20 – Network IDS: Verification of Stealth Interface

Control Objective: To verify that the stealth interface is configured correctly, that is, without an IP address.

Yes	No	N/A	Item
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The stealth interface is configured without an IP address.

Testing:

Command: `ifconfig -a`

Output:

See screenshot – figure 13.

Analysis:

The stealth interface, hme0, is configured correctly.

Testing continued:

Other: From the Real Secure Workgroup Manager GUI, select the network sensor from the list of **Managed Assets** and then view the **Properties** of the sensor. Click the **Adapters** tab and verify that the correct interface is listed without an IP address (i.e., an IP address of 0.0.0.0).

Output:

See screenshot – figure 14.

Analysis:

The configuration of the stealth address, hme0, is correctly configured on the IDS sensor.

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
hme0: flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
    inet 0.0.0.0 netmask 0
    ether 8:0:20:d1:5b:e9
hme1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
    inet 10.200.200.150 netmask ff000000 broadcast 10.255.255.255
    ether 8:0:20:d1:5b:e9
#
```

Figure 13: Stealth Interface Configuration

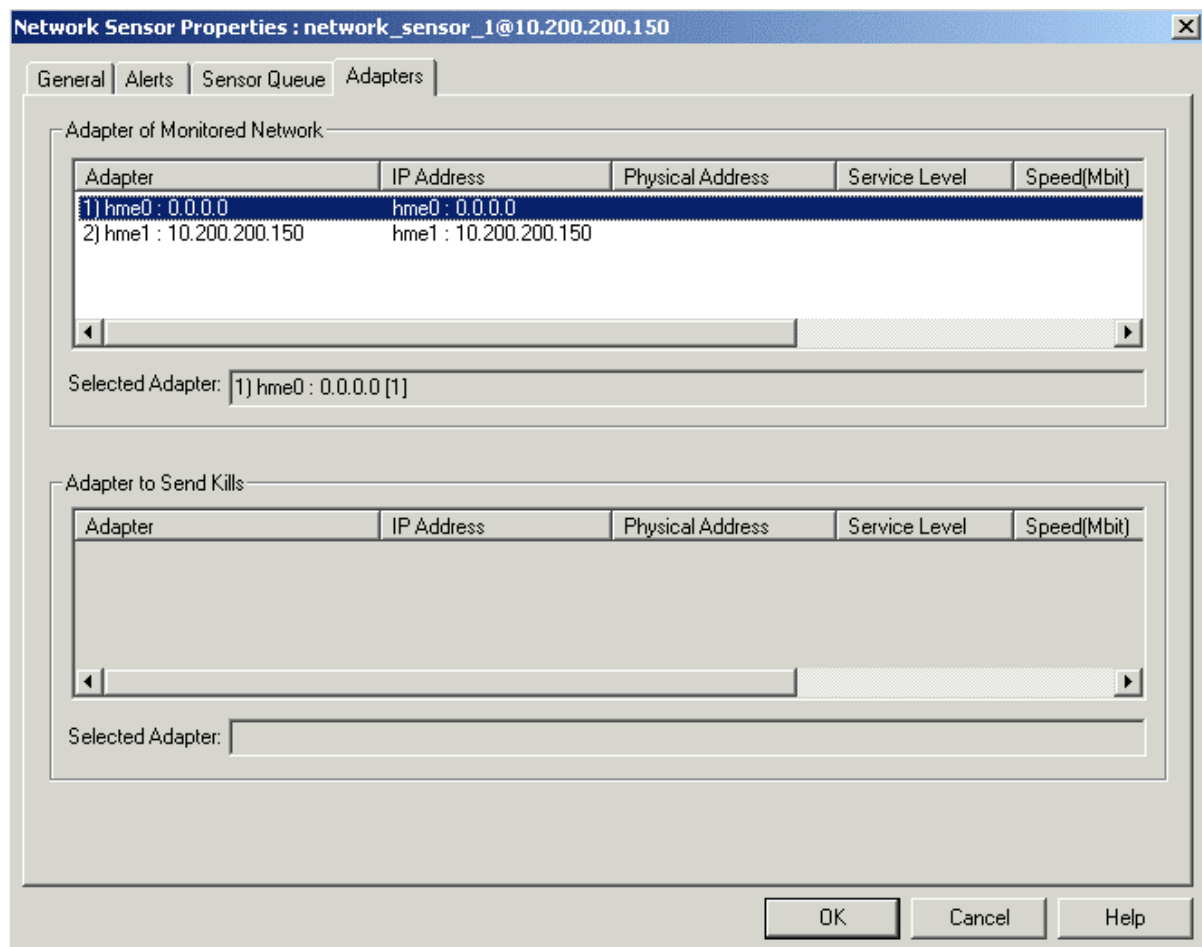


Figure 14: Workgroup Manager Stealth Interface Configuration

3.10 Item 21 – ISS Real Secure Network Sensor: Configuration

Control Objective: To verify that the ISS Real Secure network sensor is using the latest available sensor engine and that the policy installed on the sensor is appropriate.

Yes	No	N/A	Item
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The most current version of the ISS Real Secure network sensor is in use, and the latest ISS Real Secure X-Press Update has been applied.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Verify that the current ISS Real Secure network sensor policy is appropriate.

Testing:

The current version, X-Press Update (XPU) level, and the current policy may be verified from the Workgroup Manager console in the Managed Assets section under the “Version” field.

Output:

See screenshots – figures 15, 16 and 17.

Analysis:

Version information for the network sensor can be seen from the Management Console; the current version of the sensor is 6.5.2003.44. The “Micro Update”, or MU version, is 5.9.

This may be verified against the current version available for download at <http://www.iss.net/downloads> under the Real Secure Network Protection section; the latest X-Press Updates, which contain the “most current attack signatures”.

Testing:

The policy currently in use by the IDS sensor can also be viewed from the Management Console.

Output:

See screenshot – figure 18.

Analysis:

The current policy is the default “Maximum Coverage” policy. This provides a broad range of attack signatures, as seen in the screenshot. During the audit, it was learned that it will continue to be tested and refined to produce the most effective coverage.

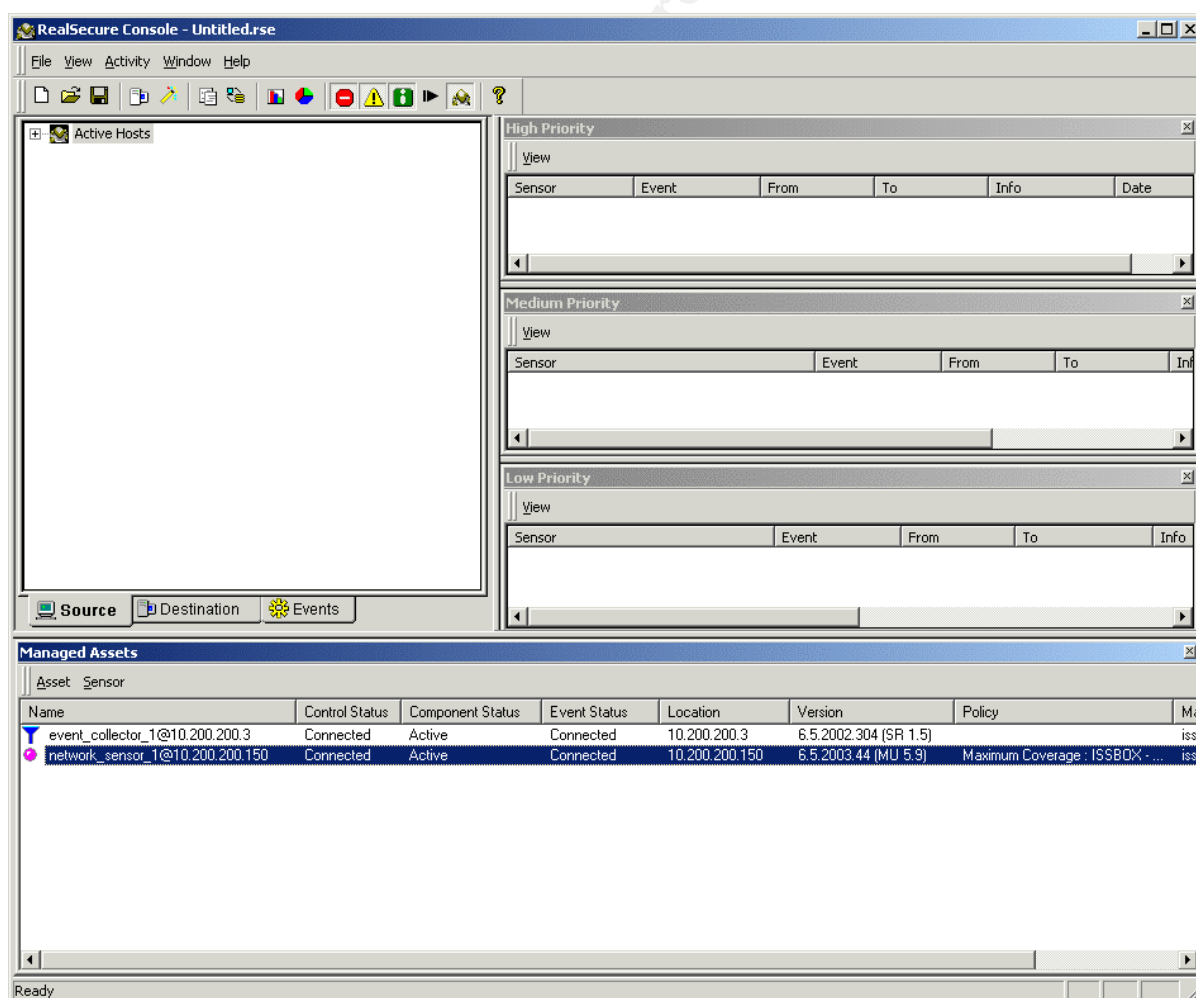


Figure 15: Real Secure Version Information

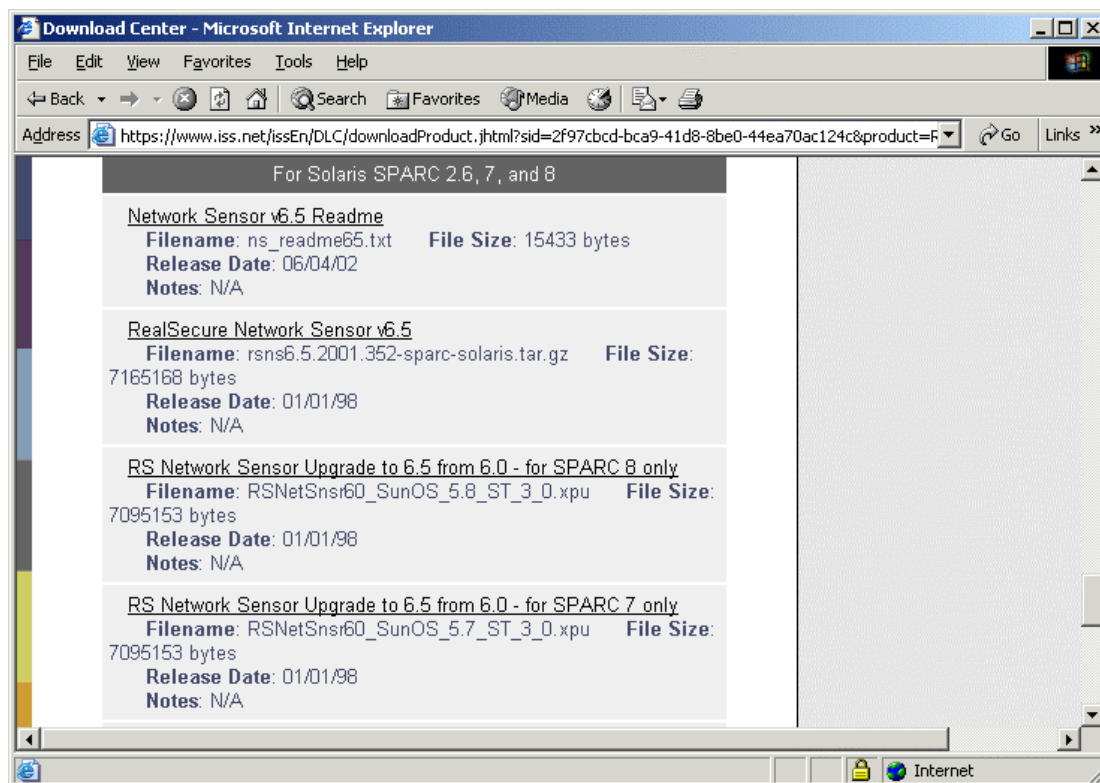


Figure 16: Network Sensor Version - <http://www.iss.net/downloads>

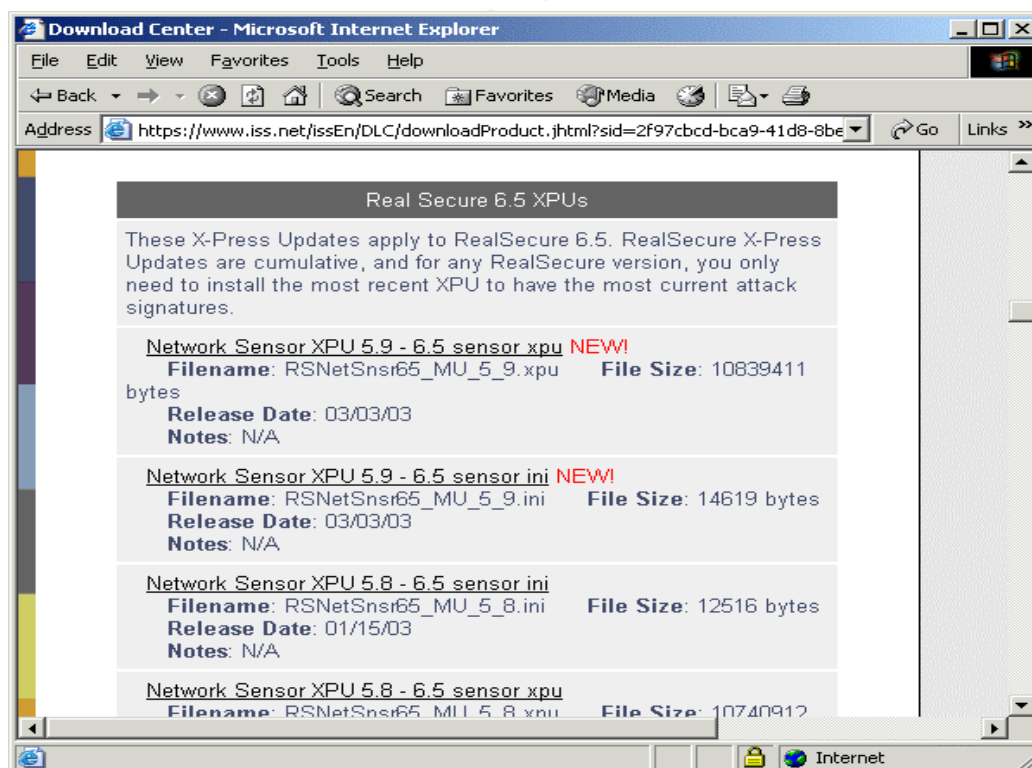


Figure 17: Current XPU - <http://www.iss.net/downloads>

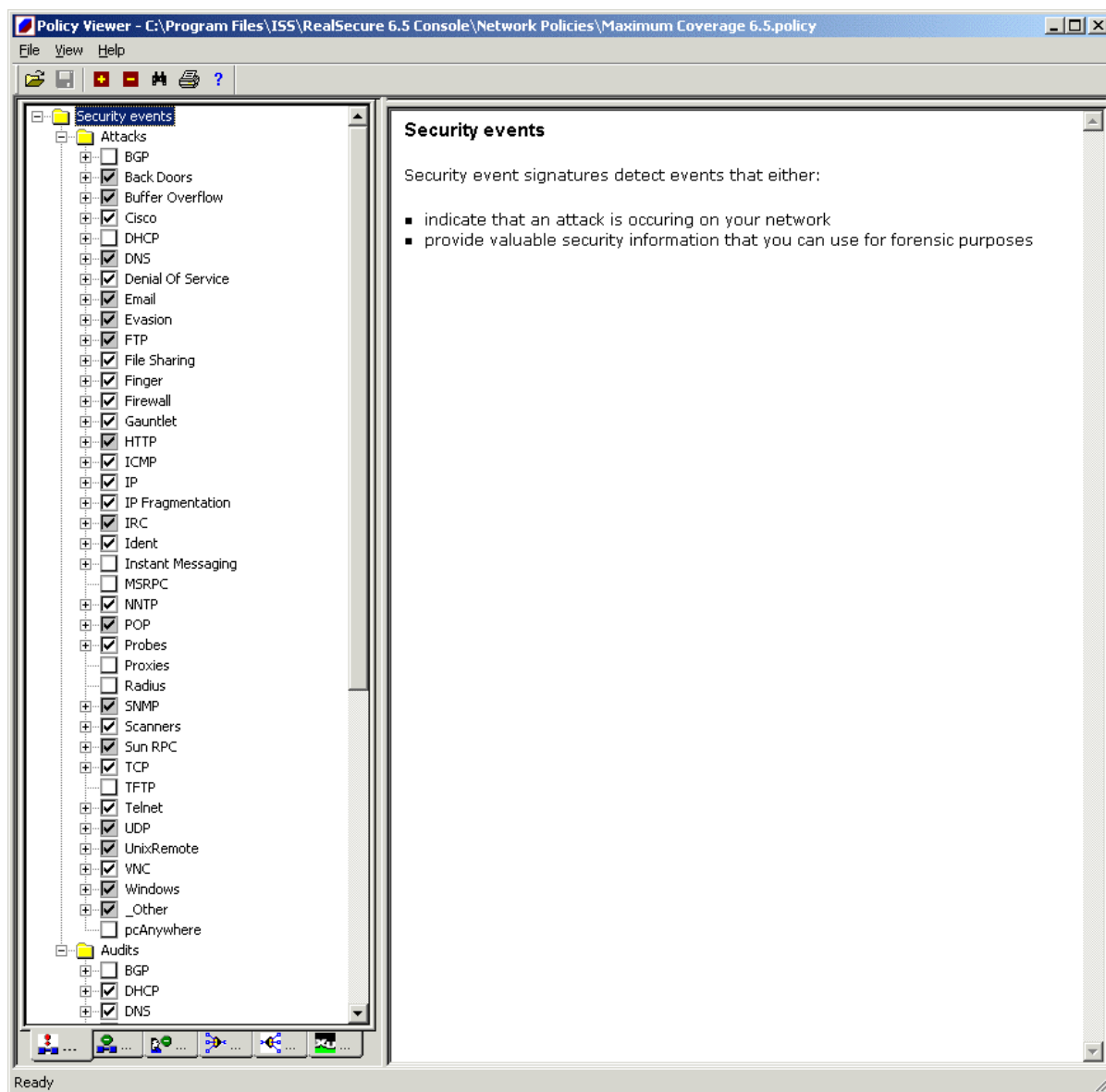


Figure 18: Network Sensor Policy – Detail

3.11 Item 22 – Network-based Assessment

Control Objective: To verify that the ISS Real Secure network sensor detects various scans including OS fingerprinting and stealth scanning.

Yes	No	N/A	Item
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The ISS Real Secure Network Sensor detects various scans from tools such as NMAP.

Testing:

Testing: The host scanned is a Windows XP workstation running Back Officer Friendly software, which simulates the Back Orifice Trojan, as well as simulating open telnet, FTP, and SMTP ports, and a web server. The host also has a Sub Seven Trojan server installed.

The scans completed were a simple NMAP scan, an OS detection scan, and a Stealth scan.

Output:

See screenshots – figures 19, 20, and 21.

Analysis:

The network sensor detected all of the scans, including the OS scan and the Stealth scan.

© SANS Institute 2003, Author retains full rights.

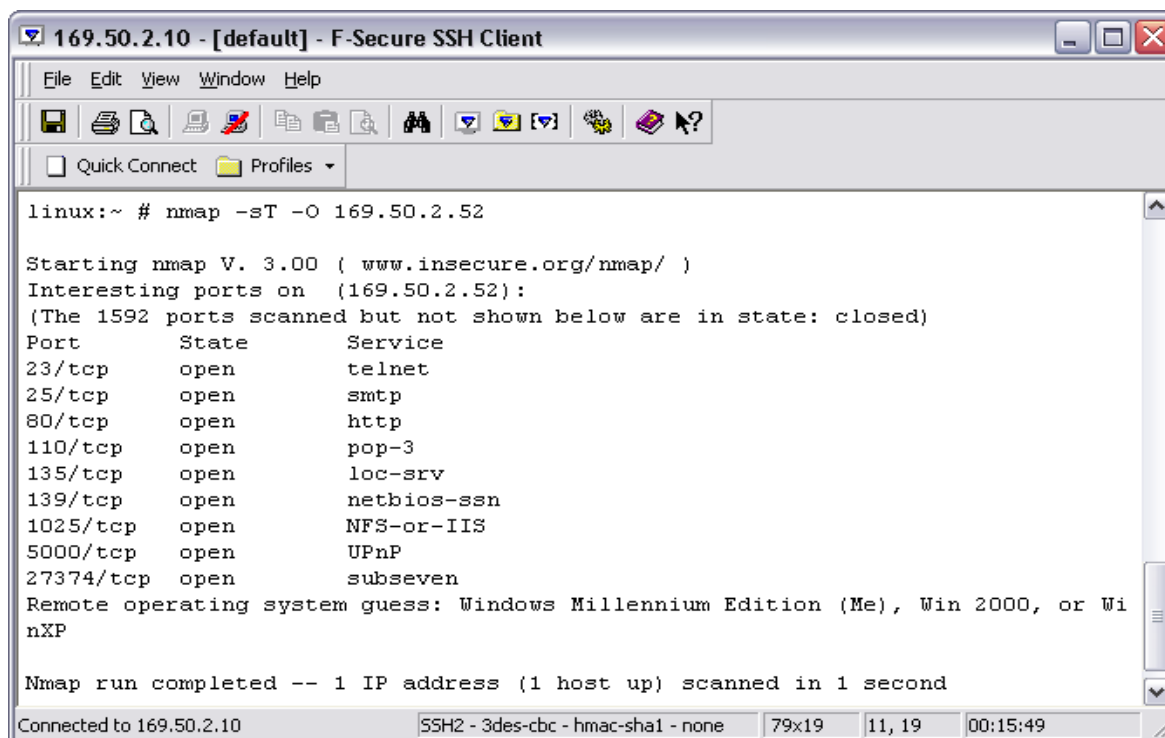


Figure 19: Nmap OS Detection Scan

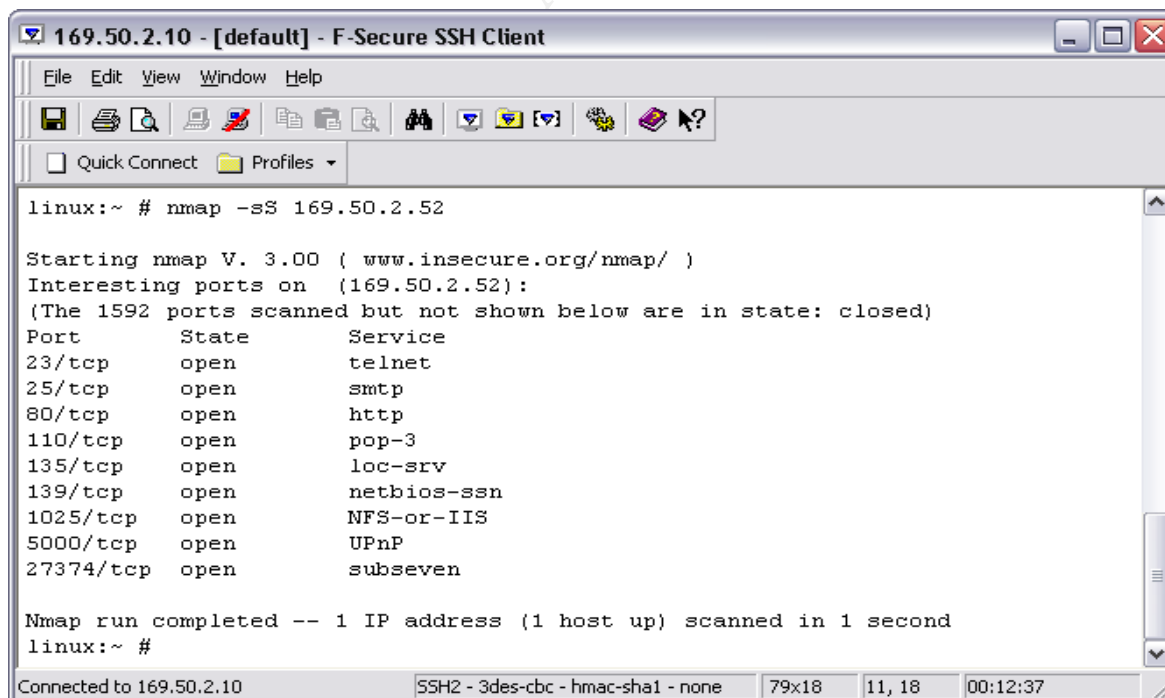


Figure 20: Nmap Stealth Scan

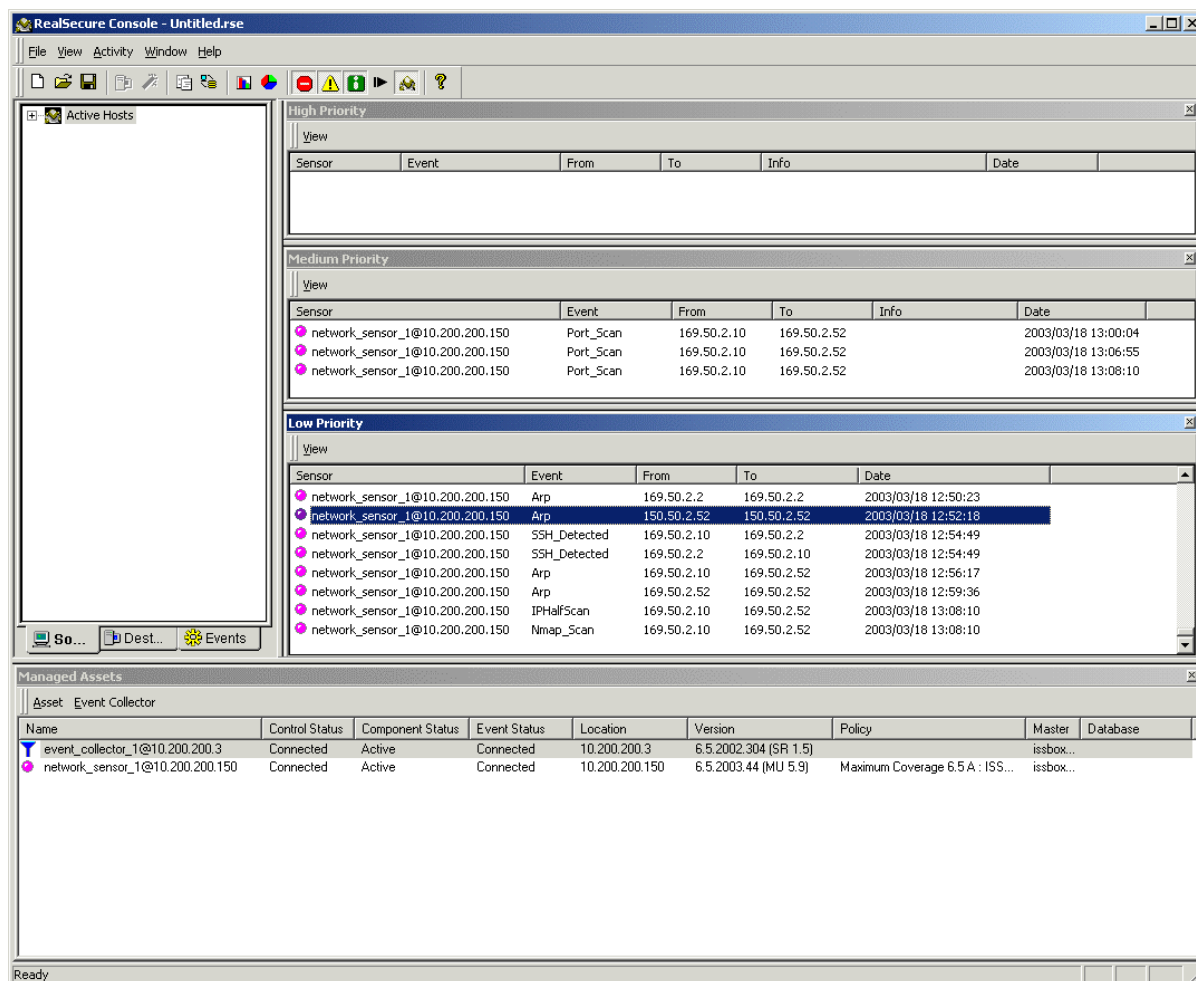


Figure 21: Network IDS Console - Detection of Nmap Scans

3.12 Item 23 – Anomalous Traffic Assessment

Control Objective: To verify that the ISS Real Secure network sensor detects anomalous traffic.

Yes	No	N/A	Item
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	The ISS Real Secure Network Sensor detects various forms of anomalous traffic.

Testing:

Testing: A host running Windows XP Professional was scanned using various options with the Nessus vulnerability assessment tool. The scans included a wide range of vulnerabilities.

Output:

See screenshot – figure 22.

Analysis:

The network sensor detected a wide array of anomalous traffic, in concurrence with the options used in the Nessus scan.

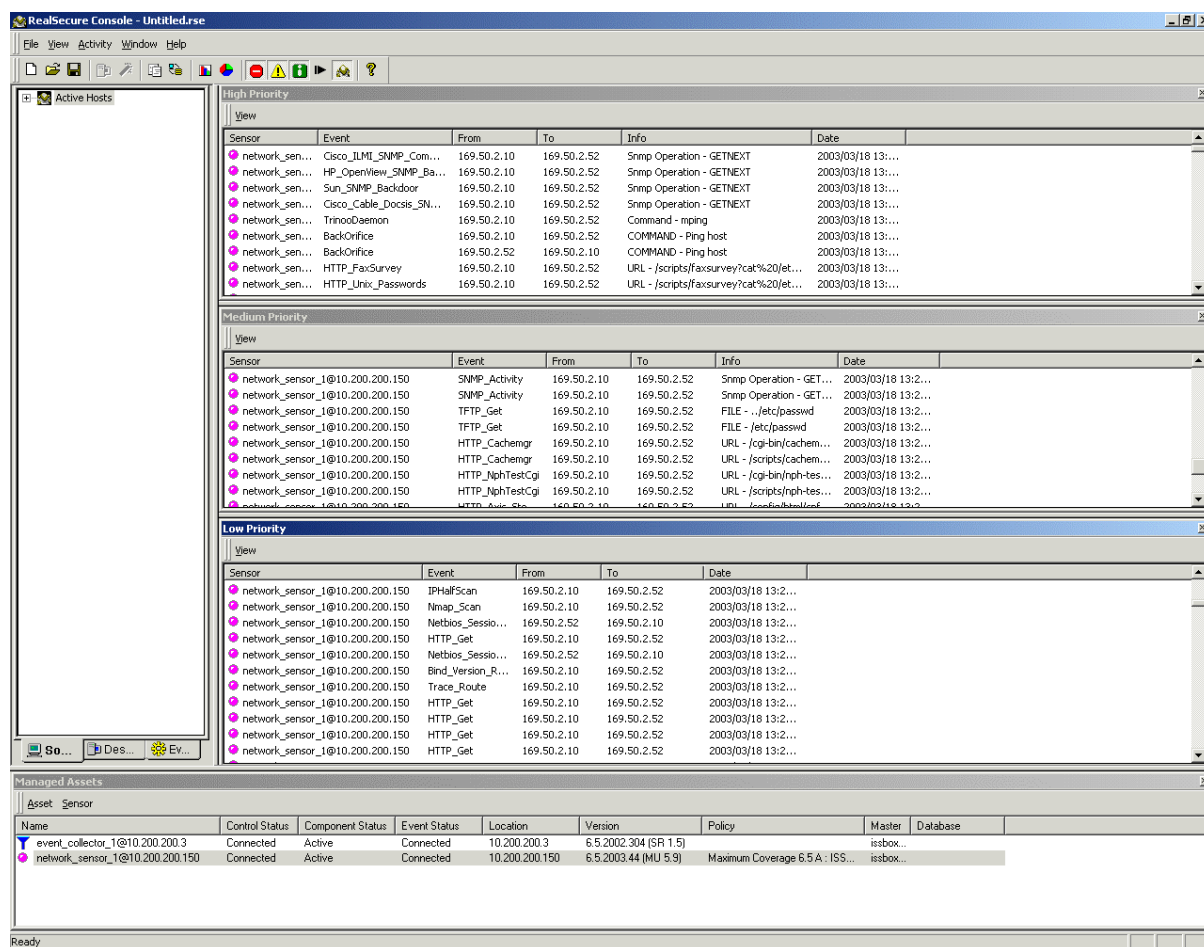


Figure 22: Network IDS - Detection of Nessus Vulnerability Scan

3.13 Measure Residual Risk

While the system itself is in a very vulnerable location, located externally to the network and outside of the protection of the border firewalls, it can be secured in such a way that the risk is greatly reduced. The controls discussed, hardening the system as a bastion host and using a stealth interface as the listening interface, go a long way toward reducing the residual risk to the system.

However, there are risks that remain, potentially from a flaw in either the operating system or software installed on the system (Real Secure or Open SSH). Additional security may be obtained through further measures, for instance using a network tap to connect the listening interface to the network or using a "one-way cable". These devices physically prevent traffic from leaving the network IDS host via the stealth interface, further increasing the security. On the downside, network taps are quite expensive.

The main security control objectives outlined in the beginning of this document were:

- A well-hardened base operating system with a current and regularly maintained patch-level
- A secure network configuration (i.e., stealth interface)
- Real Secure and Open SSH software installed and configured securely with a current patch-level

These items were thoroughly investigated, within the outlined scope, in the audit of the network IDS. The results of the audit clearly indicate that the security control objectives were achieved.

3.14 Is the system auditable?

The network IDS itself is clearly auditable, as it is somewhat limited in its configuration (i.e., bastion host, stealth interface, software configuration). However, it is one piece of the overall intrusion detection puzzle. Additional items involved include the network communication between the sensor and the Workgroup Manager, the configuration of the firewall and other network devices in-between, the encryption of the communication between the devices, the Management Console's underlying operating system, the IDS policy and attack signature configuration, and so on. When these additional items are taken into consideration, the complexity of the audit increases dramatically.

4 Audit Report

4.1 Executive Summary

Because of the future intention to implement network intrusion detection systems into the network, an audit was conducted of Real Secure, the Network Intrusion Detection System from Internet Security Systems, which is the product that has been chosen for this function. Because the network IDS is intended to be placed outside border firewalls of the network, the security of its configuration is of paramount importance.

Due to the constraints of time and length of this report, the audit was limited in scope to the network IDS device itself and its network configuration, although some limited consideration was given to other components, such as the Management Console, which is used to administer the sensor. Outside of the scope of the audit were the additional network components such as the firewall, border router, and switches, as well as an in-depth audit of the Management Console component of the IDS or the design of the management network.

The items audited ranged from a review of the documentation of the system and a thorough examination of the operating system configuration and hardening (with particular attention to its network configuration) to a review of the IDS policy, i.e., attack signature configuration, and a test of its ability to detect various types of anomalous traffic.

The results of the audit were very positive, and the security of the network IDS device was found to be quite good. There were some items found that should be modified to further increase the security of the IDS, however, these were generally minor issues or easily corrected.

4.2 Audit Findings

As stated, the findings of the audit were generally very positive. However, there were a few items that could be modified to improve the overall security of the network IDS environment.

4.2.1 Verification of Networking Information (Section 3.1)

One of the first activities made during the audit process was to conduct a thorough review of the documentation of the installation and configuration of the IDS device itself, as well as the network configuration.

It was observed during the subsequent comparison of this documentation with the actual situation that there were a few minor discrepancies, including a mismatch between the documented and actual network configuration, and a lack of documentation of items such as routing tables. Also, specifics such as IP addresses and interface information were not included in the network diagrams (figure 1), which would hinder efforts to compare the actual physical configuration versus what was documented.

Additionally, the output of the listening ports on the system revealed that the system was listening on the syslog port, UDP/514.

Background/Risk

Documentation is typically an afterthought in many IT endeavors, as troubleshooting problems and attempting to get components to communicate with one another take priority. Documentation, the necessary evil, has its benefits, especially during troubleshooting or when trying to remember how or why something was configured a particular way. For example, it would be very useful to know the port of the switch a particular interface of a firewall was plugged into from the documentation rather than determining this information by physically tracing a cable.

Regarding the finding of the listening syslog port, UDP/514, this is a relatively minor finding. However, as the system will not be receiving remote log files, this port need not be open and is easily closed. While it is not a huge security risk, open UDP ports may be vulnerable to UDP flooding, which creates a Denial of Service (DoS).

4.2.2 Operating System: Verification of Hardening (Section 3.2)

During the audit, the CIS Scan tool was used to verify the hardening of the operating system. While the results were excellent overall, there were a few items found to be negative. They were the following:

- Syslog accepts remote logging
- Inetd is still active and does not do connection tracking
- /etc/rc2.d/S21perf does not exist
- BSM does not audit various events
- No /usr partition was found/not mounted read-only
- /etc/shells does not exist
- /etc/.profile permissions on user tty lacking
- /etc/.login permissions on user tty lacking
- fix-modes has not been run
- ssh-keygen is a non-standard SUID program

Background/Risk

Among these items, some are of no consequence, such as the /usr partition not being mounted read-only. This is not an issue because there is no /usr partition on the system. The /usr directory is contained within the root partition on the system.

Syslog listening on port UDP/514 was discussed in Section 4.2.1.

As discussed in the analysis of Section 3.2, the /etc/shells file prevents non-authorized programs from being used as valid user shells on the system, and should exist in order to prevent this.

BSM, Sun's Basic Security Module, allows an increased level of system auditing than is available by default, and the recommendation of The Center for Internet Security is that BSM be configured to audit these additional system events.

The fix-modes application changes various file ownership and permission settings within the Solaris operating system. Fix-modes is available at:

http://www.sun.com/solutions/blueprints/tools/FixModes_license.html

SSH-keygen is required as part of the Open SSH software installed on the system.

4.2.3 Operating System: Accounts (Section 3.4)

While various aspects of user account configuration were found to be excellent, including the fact that default system accounts had either been removed or given a false shell, during the audit it was discovered that only one administrative account existed on the system.

Background/Risk

In order to determine the activities of various administrators on a system, individual, unique accounts for each administrator should exist on the system.

4.3 Audit Recommendations

The audit revealed a few minor outstanding issues as discussed in the previous section. It is recommended that the findings and the background/risks sections be reviewed and weighed against the effort of modifying the various items. Many of the items are very minor and very easily corrected, such as the lack of an /etc/shells file or the open syslog port.

As this system is not yet in production, some of the items were not completed as thoroughly as they would be before the actual implementation into the productive environment. Among these are the documentation of the various network configuration items and diagrams. It is recommended that these items found outstanding be reviewed again before the network IDS is implemented into the production environment.

Also of concern are the maintenance of the versions and patch-level of the operating system and software components such as Real Secure and Open SSH. A patch-maintenance plan should be drawn up with specific procedures for maintenance of the system.

As discussed in the “residual risk” section, other items may be investigated to improve the security of the system. Among these is the use of a network tap for the stealth interface of the IDS device. However, this item may not provide enough of a concrete security benefit to justify its cost.

Costs

Most of the items found in the audit would require costs only in terms of effort and time. It is believed that the benefits of taking the time to rectify the outstanding items would provide enough of a benefit to be worthwhile.

Compensating controls

There were no items found that would be of such considerable cost as to require other mitigating factors.

Next Steps

As discussed in the “residual risk” section, the audit undertaken was of a portion of the proposed network IDS infrastructure. While it is understood that the network sensor itself is of highest risk and therefore deserves the highest priority for an audit, other aspects of the proposed infrastructure should also be audited.

It is recommended that a thorough audit of other components of the proposed IDS environment be conducted. In particular, an audit of the Management Console should be conducted, with particular focus upon the operating system hardening. The database which collects detected network events runs on MSDE, which is based on Microsoft SQL server and was vulnerable to the recent Slammer worm. This is of concern and should rate a high priority for review.

Further items which should be investigated include the configuration of the management network, the border firewall and router, and networking aspects within the environment including items surrounding the encrypted communication between the management console and the network sensor.

References

Australian Computer Emergency Response Team. “UNIX Security Checklist.” Version 2.0. May 2002. http://www.uscert.org.au/Information/Auscert_info/papers.html

Center for Internet Security, The. “Solaris Benchmark.” Version 1.1.0. 2001-2002. <http://www.CISecurity.org>

CERT® Coordination Center. “Installing, configuring, and operating the secure shell (SSH) on systems running Solaris 2.x. December 2000.” http://www.cert.org/security-improvement/implementations/i062_01.html

Corcoran, Tim. “An Introduction to NMAP.” October 2001. <http://www.sans.org/rr/audit/nmap2.php>

Flynn, Hal. “Focus on Sun: Hardening Solaris – Creating a Diamond in the Rough, Part One.” October 2000. <http://www.securityfocus.com/infocus/1365>

Flynn, Hal. "Focus on Sun: Hardening Solaris – Creating a Diamond in the Rough, Part Two." November 2000. <http://www.securityfocus.com/infocus/1366>

Konigsberg, Bob. "Auditing Inside the Enterprise via Port Scanning and Related Tools." January 2002. <http://www.sans.org/rr/audit/inside.php>

Laggui, Dexter D. "How to Strip Down a UNIX OS – Check Point Guide." <http://support.checkpoint.com/kb/docs/public/os/solaris/pdf/strip-sunserver.pdf>

McClure, Stuart, Scambray, Joel, Kurtz, George. Hacking Exposed: Network Security Secrets and Solutions. Third Edition. 2001. <http://www.foundstone.com/knowledge/books.html>

Mitchell, Jason. "Proactive Vulnerability Assessments with Nessus." April 2002. <http://www.sans.org/rr/audit/proactive.php>

Mookhey, K. K. "Unix Auditor's Practical Handbook, The." <http://www.nii.co.in/tuaph1.html>

NSS Group, The. "Intrusion Detection Systems, Group Test". Edition 3. June 2002. <http://www.nss.co.uk>

SANS Institute, The. "Solaris Security Step By Step". Version 2.0. 2001. http://store.sans.org/store_item.php?item=21

Security Focus. Focus-IDS Mailing List Discussion. <http://online.securityfocus.com/archive/96/306346/2003-01-11/2003-01-17/1>

Wassom, Darrin. "Auditing a Distributed Intrusion Detection System: An Auditor's Perspective. GSNA Practical Version 2.0." February 2002. <http://www.giac.org/GSNA.php>

Software Resources:

Fix-modes. http://www.sun.com/solutions/blueprints/tools/FixModes_license.html

Internet Security Systems. <http://www.iss.net>

NMAP. NT Version: <http://www.eeye.com/html/Research/Tools/nmapNT.html> Linux version: http://www.insecure.org/nmap/nmap_download.html

Nessus. <http://www.nessus.org>

Sun Microsystems. Current patches for Solaris. <http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage>