



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
"Securing Linux/Unix (Security 506)"
at <http://www.giac.org/registration/gcux>

Practical Assignment

• ASSIGNMENT VERSION: 3.0 • ASSIGNMENT OPTION: 2

Secure Web Search for a Solaris Intranet File Server

GIAC Certified
UNIX Administrator

Tom Simcock, GSEC, GCIH, GCYW

1 March, 2005

Table of Contents

Abstract.....	1
Operating Environment.....	2
New Software to be Added	4
Security Issues Introduced by the New Software.....	6
Solution.....	8
Step-by-Step Guide	8
Audit Protocol	19
Ongoing Maintenance Plan / Policy	23
Summary and Research	25
Glossary.....	26
References	27
Appendix A	30
Appendix B	33
Appendix C	34
Appendix D	35
Appendix E	36
Appendix F.....	38

List of Tables

Table 1. GIAC Enterprises: File Server's Current Operating Environment.....	3
Table 2. GIAC Enterprises: Web Server Prerequisites	5

List of Figures

Figure 1. Sun Java System Web Server's Web Administration Interface.....	10
Figure 2. Filevault's Web Search Interface (Customized)	12
Figure 3. Filevault's Access Control List	14

Abstract

GIAC Enterprises, a fictitious research company, had the requirement for an improved, secure file searching capability for their Solaris 8 research intranet file server. In order to manage the multitude of research documents contained on the file server, a web search interface was deemed the best solution to search for and search inside the company's documents. This requirement was addressed through the implementation of the Sun Java System Web Server application to provide a webpage interface through which users could query the file server for documents. This paper discusses GIAC Enterprises current file server's environment, the proposed changes and the potential security issues that could result from installing the Web server. It then addresses these issues by providing a step-by-step solution and an audit protocol to test the solution. An ongoing maintenance plan was also developed to ensure that the file server would remain secure over time. The resulting system provided an effective secure search capability while maintaining the file server's high level of security.

© SANS Institute 2000 - 2005, Author retains full rights.

Operating Environment

Introduction

GIAC Enterprises is a fictitious research company that conducts specialized computer research. It is important that its research information remains protected from its competitors. GIAC Enterprises maintains a Solaris 8 file server (filevault) to store its important research documentation, proprietary data, and additional reference material acquired from the Internet.

Initial Installation

The file server's initial installation was based on the Sun BluePrints Online guide, "Minimizing the Solaris™ Operating Environment for Security"¹. This guide was used to install a minimal bootable 64-bit Solaris 8 operating system with no graphical user interface. The file server was then hardened using the Centre for Internet Security's Solaris Benchmark v1.3.0 and tested using the CISscan scoring tool², which scored the file server at 10.00/10.00 (Appendix A) against the benchmark.

Current Environment

A number of security mechanisms were put in place to ensure the security of the file server while providing secure access to it. The file server has no direct connection to the Internet and is accessed through the OpenSSH³ (a free implementation of the Secure Shell suite) application, which provides encrypted communications between users' computers and the file server. Users only have access to the file server's documents partition called /docs. TCP Wrappers⁴, an application level filter, has been installed to control incoming connection requests to the file server. TCP Wrappers has been configured to log all authorized and unauthorized connection attempts, deny connections from unauthorized hosts, and restrict access to the OpenSSH service. A host based IP level firewall, IP Filter⁵, has also been installed to only allow connections to port 22 (OpenSSH).

The file server is administered locally inside GIAC Enterprises secured server room. Root logins are not permitted but the administrator can use the "su"⁶ command to obtain root privileges. The file server operates on a total of thirty-four packages and has no security holes according to the Nessus vulnerability scanner⁷. The file server's current operating environment is listed in the table below (Table 1).

Component	Description	
Hardware	Sun Blade 150 ⁸	
Processor	550 MHz UltraSPARC III	
Physical Memory	1024 MB SDRAM	
Operating System	Solaris 8 (SunOS 5.8) ⁹	
Patch Levels	Latest Solaris 8 Recommended Patch Cluster ¹⁰	
Hard Disk Drives	2x 200 GB HDD	
Software	TCP Wrappers 7.6	
	OpenSSH 3.7.1p2 w/ BSM patch	
	Tripwire 4.0 for Servers ¹¹	
	CISscan v1.5.0 (scoring tool for the Solaris Benchmark)	
	Sophos Anti-virus ¹²	
	fix-modes ¹³	
	IP Filter 4.1.3	
Number of Packages	34 (Appendix B)	
CISscan Score	Final rating = 10.00 / 10.00 (Appendix A)	
Nessus Scan (Appendix C)	Services	ssh (22/tcp)
	Security Holes	0
	Security Warnings	0

Table 1. GIAC Enterprises: File Server's Current Operating Environment

New Software to be Added

Sun Java System Web Server

The new software being added is the “Sun Java System Web Server”¹⁴, version 6.1, Service Pack 4 (see Table 2, for Solaris 8 system requirements). The purpose for installing the Sun Java System Web Server application is to provide a secure web based search capability for users of GIAC Enterprises file server. The Sun Java System Web Server application provides a search function to search for and search inside various types of documents (e.g. HTML, ASCII, Adobe PDF, and WordPerfect) and then display a list of relevant results based on the search criteria. The availability of the search function will save GIAC Enterprises time over the current process of looking through masses of (often poorly labelled) filenames with limited descriptions.

Web Server Security Features

The Sun Java System Web Server includes the following security features:¹⁵

- Protects the operating system from potential Web server exploits
- Installs a secure-by-default configuration with services turned off
- Supports SSL (Secure Socket Layer) v2 & v3, and TLS (Transport Layer Security) v1.0*
- Supports X.509 digital certificates*
- Supports various security standards including PKCS #11*, FIPS-140*, and 168-bit step-up certificates*
- Allows server headers to be obfuscated or hidden
- Supports digital certificate-to-LDAP mapping*
- Supports DIGEST* authentication
- Access Control Lists (ACLs)
- Includes plug-in support for reverse-proxy functionality

Support for a number of the security features listed above requires access to a Directory server for the management of users and groups, and digital certificates for SSL encryption. GIAC Enterprises uses a Sun ONE Directory Server for user and group authentication, and issue its own digital certificates.

* Refer to Glossary, Page 25.

Web Server Prerequisites

The prerequisites for installing the Sun Java System Web Server on a Solaris 8 SPARC computer are listed below (Table 2).

Requirement	Description
Web Server Software	Sun Java System Web Server 6.1, SP4
Java Software	JDK release: 1.4.1_03 (minimum) (Bundled with Sun Java System Web Server)
Physical Memory	128 MB (minimum) 512 MB (recommended)
Hard Disk Space	150 MB (minimum), 200 MB (recommended)
Additional Packages to be Added ¹⁶	SunWlibC Sun Workshop Compilers Bundled libC
	SunWlibCx Sun Workshop Compilers Bundled libCx (64-bit)
Web Browser	GUI Administration requires one of the following compatible Web browsers: <ul style="list-style-type: none"> • Netscape™ 7.0 • Netscape™ 6.2.1 • Netscape™ 4.79 • Microsoft Internet Explorer 6.0 • Microsoft Internet Explorer 5.5

Table 2. GIAC Enterprises: Web Server Prerequisites¹⁷

Security Issues Introduced by the New Software

The addition of the Web server application to GIAC Enterprises file server introduces new security considerations that must be addressed. These considerations are listed below with possible steps to address them. The following section will provide a step-by-step guide with procedures to mitigate these issues.

Additional Services = Increased Attack Vectors

The Web server is installed with an Administration server used to configure the Web server. Together, these servers will provide additional services and listening ports resulting in an increased number of potential attack vectors against the file server. The Administration server must be run with root privileges to be able to turn the Web server on and off, but the Web server can be run as an unprivileged user. The availability of these services provides additional entry points into the file server.

Solution: Install the Sun Java System Web Server and run it under a user with the minimum required privileges. Run the servers on non assigned ports other than their default ports, port 80 and port 8888 to obfuscate their functions. The Administration server will be running with root privileges and should only be turned on when needed. Obfuscate the default Web server response header and modify the default error pages. Remove any unnecessary files and change default homepage. Update GIAC Enterprises ongoing maintenance to ensure the latest patches and security configurations are applied.

Authentication and Access

Currently, users (except for the Administrator) can only access the file server through their OpenSSH clients. The Web server's web search interface will allow users another way to access the file server. Additional security controls will need to be put in place to authenticate users and constrain user access to the file server through the web interface.

Solution: Configure the search function to only display files in the /docs partition. Only allow authorized users to access the /docs partition. Turn off virtual directory listings and support for symbolic links. Implement a secure authentication scheme for file server and Web server access. Update the IP Filter configuration file to allow the additional ports to have access through the firewall.

Remote Administration Vulnerabilities

A compatible Web browser (Table 2) is required to use the Sun Java System Web Server's Administration server webpage interface. The file server has no graphical capabilities for heightened security and therefore cannot run a graphical Web browser. Web browser administration will need to be managed through a remote Web browser running on the Administrator's computer. Potential vulnerabilities exist in the communications between the administrating computer the Web server. These communications must be secured.

Solution: Enable SSL to encrypt communications between the administrator and the file server.

Unsecured Access to Web server

By default all transactions between GIAC Enterprises users and the Web server will be unencrypted. This defeats the purpose of using OpenSSH and leaves the file server open to sniffing, session hi-jacking, and data modification. Communications must be encrypted between authorized users and the Web server.

Solution: Enable SSL to encrypt communications between authorized GIAC Enterprises users and the Web server.

Increased Monitoring Overhead

The Web server will require increased monitoring for accesses, server state, and anomalous activity.

Solution: Enable monitoring of error and access activity. Update the administration procedures. Update the Tripwire database.

Solution

Step-by-Step Guide

Agenda

- Install the Sun Java System Web Server
- The Administration Server's Web Based Interface
- Configure the Search Function
- Create a "Collection" for searching based on files in the /docs partition
- The Web Search Interface
- Secure the Web server
 - Enable SSL (Secure Socket Layers) to encrypt communications
 - Restrict user access to the /docs partition only
 - Enable monitoring of server error and access activity
 - Obfuscate unnecessary information and turn off dangerous file types

Installation of the Sun Java System Web Server

(Adapted from Sun Microsystems, Inc. 2004¹⁸)

Prerequisites

For a minimal bootable 64-bit Solaris 8 operating system two additional packages, SUNWlibC (Sun Workshop Compilers Bundled libC) and SUNWlibCx (Sun Workshop Compilers Bundled libCx 64-bit), are required for the installation of the Sun Java System Web Server. These packages are located on the Solaris 8 Software CD-ROM (1 of 2). Certain procedures, beyond the scope of this paper, have been referenced where appropriate.

Step	Action
1	<u>Download the Sun Java System Web Server 6.1(SP4)</u> ¹⁹
2	<p><u>Create an Unprivileged User and Group to run the Web server</u></p> <p>To mitigate potential damage from unauthorized use, an unprivileged user and group should be used to run the Web server rather than running it with root privileges.</p> <p>e.g. # useradd²⁰ wd (Web server daemon) -g 60001 (the existing nobody group) -s /bin/pfsh (shell) -u 1025 (a user id above 1024)</p>

3	<p><u>Install the Sun Java System Web Server</u></p> <p>Follow the installation guide available from the Sun website using a custom or typical install, (Sun Microsystems, Inc. Installing Sun ONE Web Server on UNIX. 2004), using the following settings:</p> <table border="1" data-bbox="379 472 1342 1010"> <thead> <tr> <th>Installation Setting</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Install Location</td> <td>/opt/SUNWwbsvr</td> </tr> <tr> <td>Administration Port</td> <td>61234 (default 8888)</td> </tr> <tr> <td>Administration URL</td> <td>http://10.0.0.10:61234</td> </tr> <tr> <td>Run Admin User as Root</td> <td>Yes</td> </tr> <tr> <td>HTTP Port Number</td> <td>60 (default 80)</td> </tr> <tr> <td>Document Root</td> <td>/docs (same document partition already used for documents on the file server)</td> </tr> <tr> <td>UNIX User to Run Server</td> <td>wd (created in step 2)</td> </tr> <tr> <td>Subcomponents</td> <td>Install both subcomponents: <ul style="list-style-type: none"> • Server Core • Java Development Kit </td> </tr> </tbody> </table> <p>An Administration server is also installed to manage and configure the Web server. An administration port, URL, username and password are specified during installation and are used to connect to the Administration server's webpage interface. The Administration server is run with root privileges in order to start and stop the Web server and should only be running when needed.</p> <p>The servers can be accessed by using their:</p> <ul style="list-style-type: none"> • IP address and port number e.g. 10.0.0.10:60 or • Short name and port number e.g. http://filevault:60 or • Fully qualified domain name and port number e.g. http://filevault-giac-enterprises.com:60 (using port 61234 for Administration server) <p>The HTTP and administration ports have been changed to random non assigned ports²¹, ports 60 and 61234, as a basic obfuscation technique.</p>	Installation Setting	Value	Install Location	/opt/SUNWwbsvr	Administration Port	61234 (default 8888)	Administration URL	http://10.0.0.10:61234	Run Admin User as Root	Yes	HTTP Port Number	60 (default 80)	Document Root	/docs (same document partition already used for documents on the file server)	UNIX User to Run Server	wd (created in step 2)	Subcomponents	Install both subcomponents: <ul style="list-style-type: none"> • Server Core • Java Development Kit
Installation Setting	Value																		
Install Location	/opt/SUNWwbsvr																		
Administration Port	61234 (default 8888)																		
Administration URL	http://10.0.0.10:61234																		
Run Admin User as Root	Yes																		
HTTP Port Number	60 (default 80)																		
Document Root	/docs (same document partition already used for documents on the file server)																		
UNIX User to Run Server	wd (created in step 2)																		
Subcomponents	Install both subcomponents: <ul style="list-style-type: none"> • Server Core • Java Development Kit 																		
4	<p><u>Start the Administration Server</u></p> <pre># /opt/SUNWwbsvr/https-admserv/start</pre>																		
5	<p><u>Connect to the Web Server's Administration Server</u></p> <p>The file server has no graphical capabilities, but a compatible Web browser (Table 2) is required to connect to the Administration server's webpage interface. Administration will be managed through a Web browser on the administrator's remote computer.</p>																		

	<p>Connect to the Administration server through a Web browser. URL: <code>http://10.0.0.10:61234</code></p> <p>Enter the correct username and password (created during the installation phase) when prompted to authenticate.</p>
▶	The Sun Java System Web Server can now be administered through the Administration server's web page interface using a compatible Web browser.

Administration Server's Web Based Interface

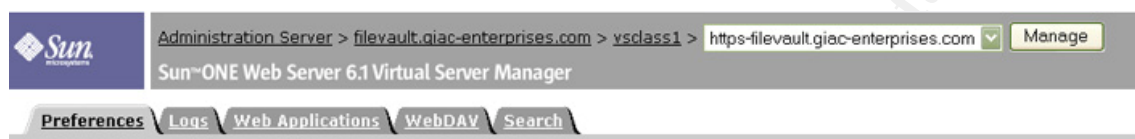


Figure 1. Sun Java System Web Server's Web Administration Interface

The web-based administration interface comprises multiple sets of tabs (Figure 1 shows a subset of the available tabs). Due to the number of configuration options available, web-based administration is a viable alternative to the command line. This majority of the steps that follow use the web administration interface to configure the Web server.

The following steps assume that the administrator is connected to the Administration server through a Web browser. Some steps require the administrator to click on a hyperlink called "Apply" before configuration changes take affect, and certain steps require a server restart. Though not discussed here, the Administration server will prompt the administrator to "Apply" changes or restart a server when required.

Configure the Search Function

(Adapted from Sun Microsystems, Inc. 2004²²)

Step	Action						
1	Select the virtual server to configure (<code>https-filevault.giac-enterprises.com</code>) and click "Manage".						
2	Select the "Search" tab.						
3	Click on the "Search Configuration" link. <table border="1" data-bbox="379 1765 1342 1937"> <thead> <tr> <th>Configuration Setting</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Max Hits</td> <td>Enter Maximum results to display from a search query e.g. 20</td> </tr> <tr> <td>Enabled</td> <td>Select to enable the search function</td> </tr> </tbody> </table>	Configuration Setting	Value	Max Hits	Enter Maximum results to display from a search query e.g. 20	Enabled	Select to enable the search function
Configuration Setting	Value						
Max Hits	Enter Maximum results to display from a search query e.g. 20						
Enabled	Select to enable the search function						

4	Click "OK" to save configuration settings.
---	--

Create a Collection for Searching Based on the /docs Partition

(Adapted from Sun Microsystems, Inc. 2004²³)

The search function requires an index of documents called a "Collection" to be created before documents can be searched for. The /docs partition is currently used to store users' documents on the file server, so the Web server will be configured to create an index of documents based on the /docs partition. The search function only allows users to see documents that have been indexed.

Step	Action																
1	Select the virtual server to configure (https-filevault.giac-enterprises.com) and click "Manage".																
2	Select the "Search" tab.																
3	Click on the "Create Collection" link. <table border="1" style="margin-left: 20px;"> <thead> <tr> <th style="text-align: center;">Configuration Setting</th> <th style="text-align: center;">Value</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">Directory to Index</td> <td>/docs</td> </tr> <tr> <td style="text-align: center;">Collection Name</td> <td>Enter a name e.g. "Research-Documents"</td> </tr> <tr> <td style="text-align: center;">Display Name</td> <td>Collection name to appear on search query page (defaults to collection name)</td> </tr> <tr> <td style="text-align: center;">Description</td> <td>Optional text to describe the new collection</td> </tr> <tr> <td style="text-align: center;">Include Subdirectories</td> <td>Yes</td> </tr> <tr> <td style="text-align: center;">Pattern</td> <td>e.g. *.pdf, *.html, *.*</td> </tr> <tr> <td style="text-align: center;">Default Encoding</td> <td>Latin-1 (ISO-8859-1) (default)</td> </tr> </tbody> </table>	Configuration Setting	Value	Directory to Index	/docs	Collection Name	Enter a name e.g. "Research-Documents"	Display Name	Collection name to appear on search query page (defaults to collection name)	Description	Optional text to describe the new collection	Include Subdirectories	Yes	Pattern	e.g. *.pdf, *.html, *.*	Default Encoding	Latin-1 (ISO-8859-1) (default)
Configuration Setting	Value																
Directory to Index	/docs																
Collection Name	Enter a name e.g. "Research-Documents"																
Display Name	Collection name to appear on search query page (defaults to collection name)																
Description	Optional text to describe the new collection																
Include Subdirectories	Yes																
Pattern	e.g. *.pdf, *.html, *.*																
Default Encoding	Latin-1 (ISO-8859-1) (default)																
4	Click "OK" to create the collection.																
▶	A document search (Figure 2) can now be performed through a Web browser by entering the URL: http://10.0.0.10:60/search																

Web Search Interface

The figure below shows the web-based search interface for the file server. The search interface can be customized from the default as in the example below.

GIAC Enterprises: Filevault

Search the site [Help](#)

Research-Documents

[Advanced](#)

1 Results Found, Sorted by Relevance [Sort by Date](#) 1 - 1

1. **CIS Solaris Ruler V1**
 17, 2004 Copyright 2001-2004, The Center for Internet Security (**CIS**) TERMS OF USE AGREEMENT Background. The Center for Internet Security ("...
 TERMS OF USE AGREEMENT Background. The Center for Internet Security ("**CIS**") provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and ...
<http://10.0.0.10:60/solarisbenchmark.pdf> - Feb 21, 2005 3:37:55 PM NZDT - 1138 KB

1

Authorized uses only. All Activity may be monitored and reported.

Figure 2. Filevault's Web Search Interface (Customized)

Note: Information on managing collections and customizing the search interface can be found in the Sun ONE Web Server 6.1 Administrator's Guide²⁴.

Secure the Web server

The Sun Java System Web Server supports a number of security features to secure both the Web and Administration Servers. Certain security features can only be enabled in conjunction with a Directory server and through the use of digital certificates. GIAC Enterprises use a Sun ONE Directory server for user and group authentication and generate their own digital certificates.

For user access to the Web server a user-group called "docs" has been created in the Directory server. The "docs" user-group contains only those users authorized to access the Web server's search function. The term user in the following steps refers to a user who is a member of the "docs" user-group. The security requirements for GIAC Enterprises are to mitigate the issues identified in section three, "Security Issues Introduced by the New Software".

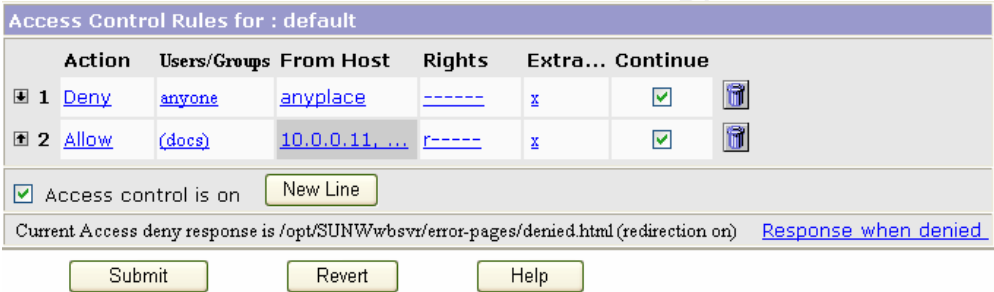
Enable SSL to Encrypt Communications

SSL encryption will be enabled to ensure that the integrity, confidentiality and non-repudiation of communications between authorized users' browsers and the servers will remain secure.

Step	Action
1	<p><u>Create a Trust Database, Request and Install Digital Certificates</u></p> <p>This process requires the administrator to:</p> <ul style="list-style-type: none"> • Create and initialize a trust database, to store public and private key-pairs, for each server. • Request digital certificates from a certificate authority (CA) by making certificate signing requests for each server (GIAC Enterprises is its own internal CA). • Install the signed digital certificates to enable SSL encryption. <p>The procedure for this step is detailed in the Sun ONE Web Server 6.1 Administrator's Guide. (Sun Microsystems, Inc. Security Tab. 2004²⁵).</p> <p>Note: Certificates were created to enable SSL for the Web server, Administration server, and Directory server. This guide only focuses on enabling SSL for the first two servers, as other administrators may use different Directory servers, but the process is generally the same. SSL was enabled for secure lookups to the Directory server. The SSL configuration options only become visible after a valid certificate has been installed for a particular server. For SSL client authentication additional, user certificates must also be created.</p>
2	<p><u>Enable SSL for Administration Server Transactions</u></p> <p>Select: Preferences > Edit Listen Socket > Select the listening socket for port 61234 > Enable Security > Choose SSL version and ciphers to use (SSL3 will be enabled using certain ciphers by default) > Click "OK"</p>
3	<p><u>Enable SSL for Web Server Transactions</u></p> <p>Select: Servers > Manage (filevault.giac-enterprises.com) > Edit Listen Socket > Select the listening socket for port 60 > Enable Security > Choose SSL version and ciphers to use (SSL3 will be enabled using certain ciphers by default) > Click "OK"</p>
▶	<p>Connections to the Web and Administration servers are now encrypted using SSL v3 (SSL was also set up on the Directory server through its own Administration interface). Communications are now facilitated using the secure http protocol (https), http encrypted using SSL.</p>

Restrict User Access to the /docs Partition

By default users can only see files that have been indexed by the search function. An access control list allows for more granular control over which users can and cannot access files on the file server. Two rules will be configured to restrict users to the /docs partition. Symbolic links and virtual directory listings will also be turned off.

<p>1</p>	<p><u>Configure Two Access Rules</u></p> <p>Select: Servers > Manage (filevault.giac-enterprises.com) > Preferences > Restrict Access > OK > Pick a resource > The entire server > Click “Edit Access Control” > Edit the two default rules already available</p> <p>The completed steps will look like this (Figure 3).</p>  <p style="text-align: center;">Figure 3. Filevault’s Access Control List</p>
<p>1a</p>	<p><u>Rule 1:</u> Deny anyone from anyplace and remove all file rights.</p> <ul style="list-style-type: none"> • Click on the first “Action” hyperlink and select “Deny” • Click on the “Rights” hyperlink and uncheck all permissions
<p>1b</p>	<p><u>Rule 2:</u> Only allow members, from the “docs” group, connecting from authorized internal IP addresses, who can be authenticated, to access the search interface and files.</p> <ul style="list-style-type: none"> • Click on the second “Action” hyperlink and select “Allow” • Click on the “From Host” hyperlink and enter all allowed IP addresses that will be allowed to access the /docs partition • Click on the “Rights” hyperlink and only enable “read” permission (allows users to request, view, and save files) • Click on the second “User/Groups” hyperlink and enter the following details (see next page)

Configuration Setting	Value
Authenticated People Only	Enable this option
Only Allow the Following People	Under "Group" enter "docs"
Prompt For Authentication	Enter a descriptive message to appear to users in the prompt e.g. Filevault Secure Search. Authorized Uses Only.
Authentication Methods	Use Basic or SSL

Basic authentication is unencrypted by default, but becomes encrypted once encryption has been enabled on the server.²⁶ The SSL option uses certificate-to-LDAP mapping and requires authorized digital certificates for each user to be created first. These certificates must map to valid users in the Directory server. Both options will encrypt a user's authentication details.

2 Turn Off Symbolic Links

Turning off symbolic links for the /docs partition, minimizes the possibility of users accessing files outside of the /docs partition that have symbolic links to them.

Select: Servers > Manage (filevault.giac-enterprises.com) > Virtual Server Class > Manage > Content Management > Symbolic Links >

Configuration Setting	Value
Allow soft file system links	Never
Allow hard file system links	No
From Directory	/docs

Click "OK"

3 Turn off Virtual Directory Listings

Users should not be allowed to browse the file server's directories via the Web server. To disable users browsing the file system turn off virtual directory listings.

Select: Servers > Manage (filevault.giac-enterprises.com) > Virtual Server Class > Manage > Content Management > Document Preferences > Directory Indexing >

Configuration Setting	Value
Directory Indexing	None
File to use for error response when indexing is set to none	Enter a path to a custom error response page e.g. /opt/SUNWwbsvr/error-pages/vdlisting.html
Index Filenames	Enter same path as above

	<table border="1"> <tr> <td>Homepage</td> <td>Enter a path to a custom home page</td> </tr> </table> <p>Click "OK"</p>	Homepage	Enter a path to a custom home page
Homepage	Enter a path to a custom home page		
▶	<p>Now only members from the "docs" group who authenticate with a valid username and password (stored in the Directory server) and are connecting from an allowed IP address have the ability to use the search interface to access documents. Authentication information is encrypted and users only have "read" privileges enabled. Symbolically linked files will not be accessible from inside the /docs partition and users will be unable to gain virtual directory listings of the file server.</p>		

Enable Monitoring of Access and Error Activity

The Sun Java System Web Server supports the logging of access and error activity. For administrators these logs can provide useful information on the status of the Web server, access attempts, files requested, http methods used, errors, and other activity of interest.

1	<p><u>Configure Access Logs</u></p> <p>Select: Servers > Manage (filevault.giac-enterprises.com) > Logs > Access Log Preferences</p> <table border="1"> <thead> <tr> <th>Configuration Setting</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Log Client Accesses</td> <td>Yes</td> </tr> <tr> <td>Record</td> <td>IP Addresses</td> </tr> <tr> <td>Format</td> <td>Select all options</td> </tr> </tbody> </table> <p>Click "OK"</p>	Configuration Setting	Value	Log Client Accesses	Yes	Record	IP Addresses	Format	Select all options
Configuration Setting	Value								
Log Client Accesses	Yes								
Record	IP Addresses								
Format	Select all options								
2	<p><u>Configure Error Logs</u></p> <p>Select: Servers > Manage (filevault.giac-enterprises.com) > Logs > Error Log Preferences</p> <table border="1"> <thead> <tr> <th>Configuration Setting</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Log Level</td> <td>Finest (provides most verbosity about an error)</td> </tr> </tbody> </table> <p>Click "OK"</p>	Configuration Setting	Value	Log Level	Finest (provides most verbosity about an error)				
Configuration Setting	Value								
Log Level	Finest (provides most verbosity about an error)								
3	<p><u>Log Rotation and Archive</u></p> <p>Log files can be rotated and archived at specific times. Select the time and date preferences for log archiving and rotation to run.</p> <p>Select: Servers > Manage (filevault.giac-enterprises.com) > Logs > Archive Log > Select time and date preferences > Click "OK"</p>								

Obfuscate Unnecessary Information and Turn Off Dangerous File Types

Unnecessary information given out by the default web server installation could be of potential use to an attacker. Certain steps can be taken to configure what information is given out by the server. Unneeded and potentially dangerous file types should also be turned off.

1	<p><u>Obfuscate the Default Web Server Response Header²⁷</u></p> <p>Edit the magnus.conf file located in /opt/SUNWwbsvr/https-filevault.giac-enterprises.com/config/</p> <p>Add the following line:</p> <pre>ServerString " " (an empty string or any other obfuscating string).</pre>				
2	<p><u>Remove Unnecessary Files and Change Default Homepage</u></p> <p>When the Web server is installed a default webpage and associated files are installed into the search directory e.g. /docs. These files are used as the default webpage when a user browses the Web server's homepage. Remove these files and replace with a custom html webpage, or turn off homepage.</p>				
3	<p><u>Modify Error Pages</u></p> <p>Custom html pages can be specified for unauthorized, forbidden, not found, and server error responses. Each error page needs to be created manually first.</p> <p>Select: Servers > Manage (filevault.giac-enterprises.com) > Virtual Server Class> Manage > Content Management > Document Preferences > Error Reponses > Enter the file paths for each custom error response webpage > Click "OK"</p>				
4	<p><u>Check CGI File Type is Turned Off</u></p> <p>GIAC Enterprises have no requirement for potentially dangerous CGI programs to be executed. Confirm that CGI file types are disabled.</p> <p>Select: Servers > Manage (filevault.giac-enterprises.com) > Virtual Server Class> Manage > Programs > CGI File Type ></p> <table border="1" data-bbox="379 1675 1337 1756"> <thead> <tr> <th>Configuration Setting</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Activate CGI as a filetype?</td> <td>No (default)</td> </tr> </tbody> </table>	Configuration Setting	Value	Activate CGI as a filetype?	No (default)
Configuration Setting	Value				
Activate CGI as a filetype?	No (default)				

Configuration Updates

1	<p><u>Create an Updated Tripwire Database Benchmark</u>²⁸</p> <p>An updated Tripwire database benchmark will need to be created to reflect the changes that have been made to the file server. Tripwire will then be able to report integrity violations based on the new benchmark.</p> <p>Run a Tripwire integrity check.</p> <pre># tripwire --check</pre> <p>A report is generated and violations are expected because the current benchmark does not know about the addition of new software.</p> <p>Use the report to create an updated database benchmark that encompasses the new software.</p> <pre># tripwire --update --twrfile /var/lib/tripwire/report/filevault.twr</pre>
▶	<p>Tripwire will now report on the integrity of the file system based on the updated benchmark.</p>
2	<p><u>Update IP Filter Rule Set to Only Allow Connections to Port 60 and 61234 from Authorized Computers</u></p> <p>Note: IP Filter has already been configured to log all connections.</p> <p># Allow Port 60 Connections (Web Server)</p> <pre>pass in quick proto tcp from (authorized IP Address) to 10.0.0.10 port = 60 keep state</pre> <p># Allow Port 61234 Connections (Administration Server)</p> <pre>pass in quick proto tcp from (authorized IP Address) to 10.0.0.10 port = 61234 keep state</pre> <p>If using IP Filter with a deny-all-inbound and deny-all-outbound rule set, the Web server will need to be able to access the Directory server for user and group lookup authentication. This step would need to be implemented prior to connecting to the Directory server.</p> <p># Allow secure connections to Port 636 (Directory Server)</p> <pre>pass out quick proto tcp from 10.0.0.10 to (Directory server IP Address) port = 636 keep state</pre>

Audit Protocol

A battery of tests was constructed to audit the strength of the modified system.

Agenda

- Perform a CISscan to test the security of the system and compare against the previous CISscan benchmark recorded in Appendix A
- Perform a Nessus scan to verify any new services and vulnerabilities on system (Appendix D)
- Test secure authentication to Web and Administration servers
- Verify search is working and is secure
- Check custom error pages and directory access
- Verify Web server access and error logging is working

CISscan

Action: Rerun the CISscan tool and compare to the pre-installation of the Sun Java System Web Server CISscan scan (Appendix A).


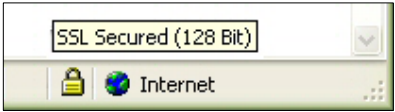
Outcome: The post CISscan resulted in no change to the results recorded in Appendix A, maintaining the file servers CISscan level of 10.00/10.00. This confirms that the modified system maintains its prior security level in accordance with the benchmark.

Nessus Scan

Action: Rerun a Nessus scan (Appendix D) and compare the results with the pre-installation of the Sun Java System Web Server Nessus scan (Appendix C).

Outcome: The Nessus scan (Appendix D) reports that in addition to port 22 (OpenSSH), two additional ports are now open, port 60 and port 61234. Nessus identifies that a Web server (Administration server) is running on port 61234 but did not identify the service running on port 60. The default Web server response header did not appear confirming that it has been successfully masked. No new security holes were discovered.

Test Secure Authentication to Web and Administration Servers

Step	Action										
1	The packet sniffing tool “Ethereal” ²⁹ will be run to ensure that all traffic is encrypted. Configure Ethereal to begin capturing packets.										
2	Open a browser and enter Web server URL <code>https://10.0.0.10:60/search</code>										
3	<p>A username and password dialogue will appear.</p>  <p>Enter the following combinations to determine that only a valid username and password will authenticate a user.</p> <table border="1"> <thead> <tr> <th>Enter</th> <th>And</th> </tr> </thead> <tbody> <tr> <td>Invalid Username</td> <td>Invalid Password</td> </tr> <tr> <td>Invalid Username</td> <td>Valid Password</td> </tr> <tr> <td>Valid Username</td> <td>Invalid Password</td> </tr> <tr> <td>Valid Username</td> <td>Valid Password</td> </tr> </tbody> </table>	Enter	And	Invalid Username	Invalid Password	Invalid Username	Valid Password	Valid Username	Invalid Password	Valid Username	Valid Password
Enter	And										
Invalid Username	Invalid Password										
Invalid Username	Valid Password										
Valid Username	Invalid Password										
Valid Username	Valid Password										
4	If the Web server search interface appears, the connection has been authenticated, otherwise an unauthorized response will appear.										
5	<p>Ensure that SSL encryption is turned on by checking that the Web browsers lock icon (usually located in the bottom right corner of the Web browser) is locked. Placing the mouse cursor over the locked icon displays a “SSL Secured” message, with the level of encryption in brackets.</p> 										
6	Repeat this procedure for the Administration server using the Administration server URL <code>https://10.0.0.10:61234</code>										
▶	Additional tests were performed to test that TCP Wrappers and IP Filters were filtering requests as configured. To test that each authentication mechanism was working as required, the other mechanisms had to be disabled for each test.										

Outcome: Only authenticated users can connect to the Web server and Administration server. The browser displayed the locked icon and presented a message stating that the search page was using SSL secured (128 Bit) encryption. The packets captured from Ethereal were encrypted and TCP Wrappers and IP Filters were filtering connections correctly.

Verify Search is Working and is Secure

Step	Action
1	Configure Ethereal to begin capturing packets.
2	Connect to the secure search page (https://10.0.0.10:60/search) using a valid username and password. Check the page is using encryption (lock icon).
3	From the secure search page make a search request for a known file e.g. <code>solarisbenchmark.pdf</code>
4	The results of the search query appear displaying a hyperlink to the Solaris Benchmark PDF file. Click on this link.
5	A prompt appears asking whether to open the file, save the file or cancel. Select save file and save to the local computer.
6	Stop Ethereal from capturing packets. Analyze the packets to check for encryption. See Appendix E for the results.
7	Additional test: Rerun the test with encryption disabled to verify the results from the packet capture. Select: Servers > Manage (filevault.giac-enterprises.com) > Edit Listen Socket > Select the listening socket for port 60 > Disable Security See Appendix E for the results.
8	Analyze the packets to check for unencrypted data. See Appendix E for the results.

Outcome: The browser displayed the locked icon and presented a message stating that the search page was using SSL secured (128 Bit) encryption. The search query (Step 3), query results (Step 4 and 5) confirm that the search function is working correctly. The results (Appendix E) show that SSL sessions are being encrypted with SSL v3 and (as expected) are using the SSL Handshake³⁰ to set up the session.

Custom Error Pages and Directory Access

1	Try to gain a virtual directory listing by entering the URL https://10.0.0.10:60 , check error response.
2	Enter a non existent URL, check error response.
3	Search for non existent files, check error response.

4	Search for known files outside of /docs directory (the /docs partition), check error response.
5	Place a symbolic link in the /docs partition to a file outside of the /docs partition and index it for searching. Use the search page to find it and try to traverse outside the /docs partition.

Outcome: Virtual directory listings have been turned off. Custom error pages are working and users are limited to the /docs partition. Symbolic links are turned off.

Test Web Server Logging

If logging is working, a large number of access and error logs will have been generated and recorded from the previous steps, e.g. the Nessus scan (Appendix D), authentication activity and errors response testing.

Step	Action
1	Select the virtual server to configure (https://filevault.giac-enterprises.com) and click "Manage".
2	<u>Viewing Access Log</u> Select: Logs > View Access Log See Appendix F for sample output of the access log.
3	<u>Viewing Error Log</u> Select: Logs > View Error Log See Appendix F for sample output of the error log.
4	<u>Report Generation</u> The Web server also supports a configurable report generation function which generates server statistics for a given time period. Reports can be in either html or plain text format. Select: Servers > Manage (filevault.giac-enterprises.com) > Logs > Generate A Report > Select items to report on > Click "OK" The report is generated and displayed and can then be saved if necessary.

Outcome: Logging is turned on and is functioning correctly. A sampling of the access and error logs generated from the Nessus scan is recorded in Appendix F. The logs suggest that a Nessus scan was run from the IP address 10.0.0.11. The scan tried to get and post files that did not exist which resulted in errors recorded to error log. Report generation works correctly.

Ongoing Maintenance Plan / Policy

An on-going maintenance plan has been developed to ensure that the file server will remain secure over time.

Up-To-Date Operating System and Software

- All necessary patches are applied to keep the file server's operating system and applications secure. A check for new updates is made at least once a week.
- Security bulletins and mailing lists are monitored for new vulnerabilities and exploits that may affect GIAC Enterprises network. Steps are then taken to update or modify the network to maintain its security.

Anti-virus

- Anti-virus scans are made on all files before they are transferred to the file server. Anti-virus scans run over entire file server from the "cron" scheduler at least once a day.

Log Monitoring

- Operating system, service, firewall and router logs are monitored and archived on a daily basis.
- The Sun Java System Web Server's access and error logs will also need to be monitored and archived. Log activity to watch for includes:
 - Valid and invalid login attempts and login times
 - Attempts to access unauthorized files and non existent files
 - Server errors and core dumps
 - Attacks against the server
 - Unexpected stops or starts of the Web and Administration servers
- All computers on the GIAC Enterprises network are checked weekly to ensure that logging is functioning properly.

Backups

- The file server uses 2 x 200 GB hard disk drives. The primary hard disk drive is duplicated each night to the secondary drive via a backup script.
- A full backup is recorded to tape weekly.
- Backup tapes are stored offsite in a secured fireproof vault.

- Backups are restored periodically to test file integrity.

Physical Security

- GIAC Enterprises servers are housed in a protected temperature controlled room, inside lockable server racks. A UPS is also installed for business continuity in the case of a power failure.
- Only authorised personnel have access to the server room.
- Sensitive printed documents for disposal are shredded.

Security Policy / Audits

- GIAC Enterprises security policy is reviewed periodically. Security audits are undertaken to ensure policy compliance.
- File, user and group permissions are monitored to ensure that correct privileges are maintained.
- Password cracking tools are run periodically to test user and server password strength.

© SANS Institute 2000 - 2005, Author retains full rights.

Summary and Research

Summary

The focus of this paper was to provide a solution to GIAC Enterprises requirement for a secure search capability on its intranet file server. This requirement was addressed through the installation of the Sun Java System Web Server and a step-by-step guide to securing it. Test plans were developed and executed to ensure the file server retained a high level of security. The Sun Java System Web Server demonstrated an excellent search function with support for a range of security mechanisms. The security steps employed in this paper focussed on the requirements of GIAC Enterprises, but did not exhaust the entire range of security mechanisms available to the Sun Java System Web Server. The steps discussed in this paper are also applicable to an Internet facing file server.

Documentation

Improvements to the Sun Java System Web Server documentation could be made. System installation requirements differ depending on what webpage one refers to and there are a number of technical mistakes in the vendor documentation. The documentation still refers to the Sun Java System Web Server as the Sun ONE Web Server, which is also true of the Administration Server's interface. Sun Microsystems does release a list of known issues and certain workaround solutions with each build, but any updates to the Web server should be reflected in the documentation. It would also be useful to see more administration reference material outside of the vendor documentation.

Additional Software: Reverse Proxy Plug-in

Additional security software for consideration is the use of the reverse-proxy plug-in. The plug-in adds an additional layer of security between Internet or intranet traffic and the Web server. The proxy acts on behalf of the Web server, accepting connection requests and then passing them to the Web server through a firewall. The Web server's responses are then passed back through the proxy. SSL (Secure Socket Layer) encryption can also be used to secure the sessions. More information on reverse proxies can be found in Sun BluePrints Online guide "Securing Web Applications Through a Secure Reverse Proxy."³¹

Glossary

Secure Sockets Layer

“Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols which provide secure communications on the Internet. The protocols allow client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery.”(Wikipedia)³².

X.509 digital certificates

“X.509 is a standard for public key infrastructure (PKI). X.509 specifies, amongst other things, standard formats for public key certificates and a certification path validation algorithm.” (Wikipedia)³³.

PKCS #11

“PKCS refers to a group of Public Key Cryptography Standards devised and published by RSA laboratories in California. PKCS #11 (Cryptographic Token Interface or cryptoki) is an API defining a generic interface to cryptographic tokens”(Wikipedia)³⁴.

FIPS-140

“FIPS-140 refers to the Federal Information Processing Standards Publication 140-1, which defines a standard of security requirements for cryptographic modules” (NIST)³⁵.

Step-up certificates

“Step-up certificates (also known as global server ID's), allow a server to override export policy. When a step-up certificate is installed on a server, it allows an export client that has step-up capabilities to renegotiate the SSL cipher and use domestic-strength encryption.” (Sun Microsystems)³⁶.

Digital Certificate-to-LDAP mapping

Certificate-to-LDAP mapping is a client authentication mechanism used to determine user access to a server. Access is determined by matching a user's digital certificate with an associated entry in a LDAP (Lightweight Directory Application Protocol) server. The Sun One Directory Server supports LDAP. (Netscape Communications Corporation)³⁷.

DIGEST Authentication

“DIGEST authentication is a security mechanism in which a Web application authenticates itself to a Web server by sending the server a message digest along with its HTTP request message. The digest is computed by employing a one-way hash algorithm to a concatenation of the HTTP request message and the client's password.”(Sun Microsystems)³⁸.

References

- ¹ Noordergraaf, Alex. "Minimizing the Solaris™ Operating Environment for Security." Sun BluePrints™ OnLine. Rev 1.0. November 2002. <<http://www.sun.com/solutions/blueprints/1102/816-524.pdf>>.
- ² The Centre for Internet Security. "CIS Level-1 Benchmark and Scoring Tool for Solaris." August 2004. <http://www.cisecurity.org/bench_solaris.html>.
- ³ OpenSSH. Version 3.7.1p2 w/ BSM patch. <<ftp://ftp.CISecurity.org/pub/pkgs/Solaris>>.
- ⁴ TCPWappers. Version 7.6. <ftp://ftp.sunfreeware.com/pub/freeware/sparc/5.8/tcp_wrappers-7.6-sol8-sparc-local.gz>.
- ⁵ IP Filter. Version 4.1.3. <<http://coombs.anu.edu.au/~avalon/>>.
- ⁶ Sun Microsystems, Inc. "su(1M) - become super user or another user." Solaris 8 Reference Manual Collection. 17 Aug 1999. <<http://docs.sun.com/app/docs/doc/806-0625/6j9vfim0k?a=view>>.
- ⁷ Nessus. Version 1.2.6 for Mac OS X. <<http://www.nessus.org>>.
- ⁸ Sun Microsystems, Inc. "Sun Blade 150 Workstation Overview." 2005. <<http://www.sun.com/desktop/workstation/sunblade150/>>.
- ⁹ Sun Microsystems, Inc. "Solaris 8 Operating System." <<http://www.sun.com/software/solaris/8/>>.
- ¹⁰ Sun Microsystems, Inc. "SunSolve Patch Access." <<http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access>>.
- ¹¹ Tripwire. Version 4.0 for Servers. <<http://www.tripwire.com/products/servers/index.cfm>>.
- ¹² Sophos Antivirus. <<http://www.sophos.com>>.
- ¹³ fix-modes. <<http://www.sun.com/software/security/downloads.html>>.
- ¹⁴ Sun Microsystems, Inc. "Sun Java System Web Server 6.1." <http://www.sun.com/software/products/web_srvr/datasheet.xml>.

- 15 Sun Microsystems, Inc. "Sun Java System Web Server 6.1."
<http://www.sun.com/software/products/web_srvr/datasheet.xml>.
- 16 Noordergraaf, Alex. "Minimizing the Solaris™ Operating Environment for Security." Sun BluePrints™ OnLine. Rev 1.0. November 2002.
<<http://www.sun.com/solutions/blueprints/1102/816-524.pdf>>.
- 17 Sun Microsystems, Inc. "Before You Install Sun ONE Web Server." Sun ONE Web Server 6.1 Installation and Migration Guide. 2004.
<<http://docs.sun.com/source/819-0131/preinst.html>>.
- 18 Sun Microsystems, Inc. "Installing Sun ONE Web Server on UNIX." Sun ONE Web Server 6.1 Installation and Migration Guide. 2004.
<<http://docs.sun.com/source/819-0131/unix.html#wp13215>>.
- 19 Sun Microsystems, Inc. "Product Downloads Sun Java System Web Server 6.1 Service Pack 4." 2005.
<<http://www.sun.com/download/products.xml?id=420aabbd>>.
- 20 Sun Microsystems, Inc. "useradd(1M) - administer a new user login on the system" Solaris 8 Reference Manual Collection. 24 Sep 1999.
<<http://docs.sun.com/app/docs/doc/806-0625/6j9vfm26?a=view>>.
- 21 IANA. "PORT NUMBERS. 17 February 2005.
<<http://www.iana.org/assignments/port-numbers>>.
- 22 Sun Microsystems, Inc. "Using Search." Sun ONE Web Server 6.1 Administrator's Guide. 2004.
<<http://docs.sun.com/source/819-0130/agsearch.html>>.
- 23 Sun Microsystems, Inc. "Using Search: Creating a Collection." Sun ONE Web Server 6.1 Administrator's Guide. 2004.
<<http://docs.sun.com/source/819-0130/agsearch.html#wp999023>>.
- 24 Sun Microsystems, Inc. "Using Search." Sun ONE Web Server 6.1 Administrator's Guide. 2004.
<<http://docs.sun.com/source/819-0130/agsearch.html>>.
- 25 Sun Microsystems, Inc. "The Security Tab." Sun ONE Web Server 6.1 Administrator's Guide. 2004.
<<http://docs.sun.com/source/819-0130/agapuirf7.html>>.
- 26 Sun Microsystems, Inc. "Controlling Access to Your Server: Specifying Users and Groups." Sun ONE Web Server 6.1 Administrator's Guide. 2003.
<<http://docs.sun.com/source/817-1831-10/agaccess.html#wp1004448>>.

- ²⁷ Sun Microsystems, Inc. "Sun Software Forums - Changing Serverstring." January 17, 2005.
<<http://swforum.sun.com/jive/thread.jspa?threadID=50840&tstart=30>>
- ²⁸ Tripwire, Inc. Tripwire for Servers User Guide. Portland. 2001.
- ²⁹ Ethereal. Version 0.10.9.
<<http://www.ethereal.com>>.
- ³⁰ Microsoft Corporation. "Description of the Secure Sockets Layer (SSL) Handshake." July 16, 2004.
<<http://support.microsoft.com/kb/q257591/>>.
- ³¹ Nguyen, Anh-Duy. "Securing Web Applications through a Secure Reverse Proxy." Sun BluePrints™ OnLine. November 2003.
<<http://www.sun.com/blueprints/1103/817-4402.pdf>>.
- ³² Wikipedia. "Transport Layer Security." 4 March 2005.
<http://en.wikipedia.org/wiki/Transport_Layer_Security>.
- ³³ Wikipedia. "X.509." 10 February 2005.
<<http://en.wikipedia.org/wiki/X.509>>.
- ³⁴ Wikipedia. "PKCS." 17 December 2004.
<<http://en.wikipedia.org/wiki/PKCS>>.
- ³⁵ NIST. "Security Requirements For Cryptographic Modules." Federal Information Processing Standards Publication. January 11 1994.
<<http://csrc.nist.gov/publications/fips/fips1401.htm>>.
- ³⁶ Sun Microsystems, Inc. "SSL Strength Tool: Export Policy and Step-up." iPlanet Certificate Management System Command-Line Tools Guide. 2001.
<<http://docs.sun.com/source/816-5542-10/sslstren.htm#13139>>.
- ³⁷ Netscape Communications Corporation. "Authentication and Certificates: Mapping Client Certificates to LDAP." 12 December 1997.
<<http://library.n0i.net/netscape/certificate/ne-cmpg/intro.htm>>.
- ³⁸ Sun Microsystems, Inc. "digest authentication." J2EE v1.4 Glossary. 8 October 2004.
<<http://java.sun.com/j2ee/1.4/docs/glossary.html#120183>>.

Appendix A

Pre-installation of new software: CISscan

*** CIS Ruler Run ***

Starting at time 20041220-14:27:27

Positive: 1.1 System appears to have been patched within the last month.
Positive: 1.2 inetd is not running, so tcpd isn't necessary.
Positive: 1.3 System is running sshd and it's configured well.
Positive: 2.1 inetd is not listening on any of the miscellaneous ports checked in this item.
Positive: 2.2 telnet is deactivated.
Positive: 2.3 ftp is deactivated.
Positive: 2.4 rsh, rcp and rlogin are deactivated.
Positive: 2.5 tftp is deactivated.
Positive: 2.6 BSD-compatible printer server is deactivated.
Positive: 2.7 rquotad is deactivated.
Positive: 2.8 CDE-related daemons are deactivated.
Not applicable: 2.9 Not applicable on Solaris versions prior to 9.
Not applicable: 2.10 Not applicable on Solaris versions prior to 9
Positive: 2.11 kerberos network daemons are deactivated.
Positive: 2.12 kerberos network daemons are deactivated.
Positive: 3.1 Serial login prompt is disabled.
Positive: 3.2 Found a good daemon umask of 022 in /etc/default/init.
Positive: 3.3 inetd/xinetd not activated.
Positive: 3.4 Mail daemon is not listening on TCP 25.
Positive: 3.5 in.rarpd and rpc.bootparamd have been disabled..
Positive: 3.6 Miscellaneous scripts are all turned off.
Not applicable: 3.7 Not applicable to Solaris versions prior to 9.
Positive: 3.8 NFS Server script nfs.server is deactivated.
Positive: 3.9 This machine isn't being used as an NFS client.
Positive: 3.10 This machine isn't running the automount daemon.
Positive: 3.11 rpc rc-script is deactivated.
Not applicable: 3.12 This item is not applicable to releases prior to Solaris 9.
Not applicable: 3.13 This item is not applicable to releases prior to Solaris 9.
Positive: 3.14 LDAP cache manager is deactivated.
Positive: 3.15 The printer init scripts are deactivated.
Positive: 3.16 volume manager is deactivated.
Positive: 3.17 Graphical login scripts are all deactivated.
Positive: 3.18 Web server is deactivated.
Positive: 3.19 SNMP daemon is deactivated.

- Not
Applicable: 3.20 Not applicable to Solaris versions prior to 9.
- Positive: 4.1 coredumps, if activated, are written to a well-permissioned directory.
- Positive: 4.2 Stack is set non-executable and logs violations.
- Positive: 4.3 NFS clients use privileged ports.
- Positive: 4.4 Network parameters are set well.
- Positive: 4.5 Network parameters are set well.
- Positive: 4.6 TCP sequence numbers strong enough.
- Positive: 5.1 inetd is not running, so connection logging is unnecessary.
- Positive: 5.3 Syslog is capturing daemon.debug messages.
- Positive: 5.4 syslog captures auth messages.
- Positive: 5.5 /var/adm/loginlog exists to track failed logins.
- Positive: 5.6 cron usage is being logged.
- Positive: 5.7 System accounting appears to be enabled.
- Positive: 5.8 kernel-level auditing is enabled and flags meet or exceed minimum values.
- Positive: 5.9 All logfile permissions and owners match benchmark recommendations.
- Positive: 6.1 logging option is set on root file system
- Positive: 6.2 /etc/rmmount.conf mounts all file systems nosuid.
- Positive: 6.3 password and group files have right permissions and owners.
- Positive: 6.8 Fix-modes has been run on this system.
- Positive: 7.1 sadmind, if present in inetd.conf, passes sadmind the -S 2 argument.
- Positive: 7.2 Nobody access for secure RPC is disabled or the keyser daemon is disabled.
- Positive: 7.3 pam.conf appears to have rhost auth deactivated.
- Positive: 7.4 All users necessary are present in /etc/ftpusers
- Positive: 7.5 System is not running syslogd, thus syslogd is not listening to the network.
- Positive: 7.6 Global X-terminal login is denied or not available.
- Not
Applicable: 7.7 Not applicable to Solaris versions prior to 9.
CDE is either not present or locks the screen after a set timeout period.
- Positive: 7.8 cron.allow and at.allow are configured correctly.
- Positive: 7.10 crontabs all have good ownerships and modes
- Positive: 7.11 Root is only allowed to login on console
- Positive: 7.12 /etc/default/login allows 3 login attempts.
- Positive: 8.1 All system accounts are locked/deleted
- Positive: 8.2 All users have passwords
- Positive: 8.3 All active users have passwords set to expire within reasonable timeframes.
- Positive: 8.4 There were no +: entries in passwd, shadow or group maps.
- Positive: 8.5 Only one UID 0 account AND it is named root.
- Positive: 8.6 The root account's gid is 0.

- Positive: 8.7 root's PATH is clean of group/world writable directories or the current-directory link.
- Positive: 8.8 No user's home directory is world or group writable.
- Positive: 8.9 No group or world-writable dotfiles!
- Positive: 8.10 No user has a .netrc file.
- Positive: 8.11 Umask in all global shell configuration files appears to be good.
- Positive: 8.12 Umask in all global shell configuration files appears to be good.
- Positive: 8.13 User shells default to mesg n, blocking talk/write.
- Positive: 9.1 Authorized-use-only warning banners are in place on the OEM banner page, /etc/motd and /etc/issue.
- Positive: 9.2 The telnetd authorized-use-only warning banners is in place if required.
- Positive: 9.3 The telnetd authorized-use-only warning banners is in place if required.
- Positive: 9.4 The ftpd authorized-use-only warning banners is in place if required.

Preliminary rating given at time: Mon Dec 20 14:27:29 2004

Preliminary rating = 9.75 / 10.00

- Positive: 6.4 All world-writable dirs have their sticky bit set.
- Positive: 6.5 No non-standard world-writable files.
- Positive: 6.6 No non-standard SUID/SGID programs found.
- Positive: 6.7 No unowned files.

Ending run at time: Mon Dec 20 14:28:01 2004

Final rating = 10.00 / 10.00

Appendix B

Pre-installation of new software: GIAC Enterprises file server package listing

system	SUNWadmfw	System & Network Administration Framework
system	SUNWadmr	System & Network Administration Root
system	SUNWauaos	Australasia OS Support
system	SUNWauaow	Australasia OW Support
system	SUNWbzip	The bzip compression utility
system	SUNWcar	Core Architecture, (Root)
system	SUNWcarx	Core Architecture, (Root) (64-bit)
system	SUNWcsd	Core Solaris Devices
system	SUNWcsl	Core Solaris, (Shared Libs)
system	SUNWcslx	Core Solaris Libraries (64-bit)
system	SUNWcsr	Core Solaris, (Root)
system	SUNWcsu	Core Solaris, (Usr)
system	SUNWcsxu	Core Solaris (Usr) (64-bit)
system	SUNWeridx	Sun RIO 10/100 Mb Ethernet Drivers (64-bit)
system	SUNWesu	Extended System Utilities
system	SUNWesxu	Extended System Utilities (64-bit)
system	SUNWkey	Keyboard configuration tables
system	SUNWkvm	Core Architecture, (Kvm)
system	SUNWkvmx	Core Architecture (Kvm) (64-bit)
system	SUNWlibms	Sun WorkShop Bundled shared libm
system	SUNWlmsx	Sun WorkShop Bundled 64-bit shared libm
system	SUNWloc	System Localization
system	SUNWlocx	System Localization (64-bit)
system	SUNWpd	PCI Drivers
system	SUNWpdx	PCI Drivers (64-bit)
system	SUNWscpu	Source Compatibility, (Usr)
system	SUNWswmt	Install and Patch Utilities
system	SUNWusb	USB device drivers
system	SUNWusbx	USB device drivers (64-bit)
system	SUNWvolr	Volume Management, (Root)
system	SUNWvolu	Volume Management, (Usr)
system	SUNWvolux	Volume Management (Usr) (64-bit)
system	ipf	IP Filter
system	ipfx	IP Filter (64-bit)

Appendix C

Pre-installation of new software: Nessus scan

Nessus Scan Report

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

Scan Details

Hosts which were alive and responding during test 1
 Number of security holes found 0
 Number of security warnings found 0

Host List

Host(s)	Possible Issue
10.0.0.10	Security note(s) found

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
10.0.0.10	ssh (22/tcp)	Security notes found
10.0.0.10	general/tcp	Security notes found
10.0.0.10	general/udp	Security notes found

Security Issues and Fixes: 10.0.0.10

Type	Port	Issue and Fix
Informational	ssh (22/tcp)	An ssh server is running on this port
Informational	ssh (22/tcp)	Remote SSH version : SSH-2.0-OpenSSH_3.7.1p2
Informational	ssh (22/tcp)	The remote SSH daemon supports the following versions of the SSH protocol : . 1.99 . 2.0 <u>The Nessus scan has correctly identified that OpenSSH 3.7.1p2 is listening on port 22. OpenSSH uses its version number when negotiating with other ssh clients.</u>
Informational	general/udp	For your information, here is the traceroute to 10.0.0.10 : 10.0.0.10

Appendix D

Post-installation of new software: Nessus scan

Nessus Scan Report

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

Scan Details

Hosts which were alive and responding during test 1
 Number of security holes found 0
 Number of security warnings found 0

Host List

Host(s)	Possible Issue
10.0.0.10	Security note(s) found

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
10.0.0.10	unknown (61234/tcp)	Security notes found
10.0.0.10	unknown (60/tcp)	No Information
10.0.0.10	ssh (22/tcp)	Security notes found
10.0.0.10	general/udp	Security notes found

Security Issues and Fixes: 10.0.0.10

Type	Port	Issue and Fix
Informational	unknown (61234/tcp)	A web server is running on this port
Informational	ssh (22/tcp)	An ssh server is running on this port
Informational	ssh (22/tcp)	Remote SSH version : SSH-2.0-OpenSSH_3.7.1p2
Informational	ssh (22/tcp)	The remote SSH daemon supports the following versions of the SSH protocol : . 1.99 . 2.0
Informational	general/udp	For your information, here is the traceroute to 10.0.0.10 : 10.0.0.10

Appendix E

Results of Ethereal packet capture.

SSL Encrypted Session

Sample output from the encrypted SSL session.

```

.....8æîßI-fÁEË.ûÑ.ä /.-'ú.kµøöP"Æ!' )R.è-"...PB*W=-
;3.Î.H.v{..ê..#. =.fè¾.ë@.;°k±èTè..£÷.àAxCy)àääÀŽN'¼.à
  A&*}..û.êž.kx¼æñËÖäl)Åö...vÅ¿F'AdÖ._.jèÖ¾û..ÎXãxÀ2Úçd
åžZ~.~.2.5pìe...•ÇH«J.ªT..SrÖB±g«µâ- >nn..[.If´.-
.»'.ÄÛô9Y".n.°m.^_à-\ÛÑGG.:ç-
„i°j]H°~4.ý÷".°pö<Î\îØDfnCt.÷KªR¿„.ûMŠI.-@r.pà.".<NqÂ&.\KØ
Ó.}.r^VÃ.±.G.,f.À >pXO -»>rÄSJü.A±°-+ß´ÿÆhŠ.+@.%. w.ýÖL
9ní}.ç.3î©]þQ.Ã.eäæ..ÛävaÃç÷¿.î9h.Áf,À4.ö°ý{öàW."go•Šá†'_¶
.ç{W@ [éÃ°.¬„Ò¼Û..t€"¶»c..M.Å.Ö>,Iy.SKCÿ#Ž!., †ŽxSöÄ
à& +.!....Xd".þÂ÷ä.QW%,7IØc•...föŽ²îá©Î.
    
```

SSL Handshake

This table shows the SSL handshake that occurred when the client's browser (IP address 10.0.0.11 from port 1621) requested the document from the Web server. It also suggests that the encrypted session was using SSL v3, the expected result.

No	Time	Source	Destination	Protocol	Info
1	0.000000	10.0.0.11	10.0.0.10	TCP	1621 > https [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
2	0.000327	10.0.0.10	10.0.0.10	TCP	https > 1621 [SYN, ACK] Seq=0 Ack=1 Win=24820 Len=0 MSS=1460
3	0.000397	10.0.0.11	10.0.0.10	TCP	1621 > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
4	0.000726	10.0.0.11	10.0.0.10	SSLv3	Client Hello
5	0.001005	10.0.0.10	10.0.0.11	TCP	https > 1621 [ACK] Seq=1 Ack=103 Win=24820 Len=0
6	0.003616	10.0.0.10	10.0.0.11	SSLv3	Server Hello, Change Cipher Spec, Encrypted Handshake Message
7	0.003954	10.0.0.11	10.0.0.10	SSLv3	Change Cipher Spec, Encrypted Handshake Message
8	0.004899	10.0.0.11	10.0.0.10	SSLv3	Application Data
9	0.008121	10.0.0.10	10.0.0.11	TCP	https > 1621 [Ack] Seq=147 Ack=170 Win=24820 Len=0
10	0.008188	10.0.0.10	10.0.0.11	SSLv3	Application Data
11	0.160672	10.0.0.11	10.0.0.10	TCP	1621 > https [ACK] Seq=811 Ack=293 Win=65243 Len=0

Non-Encrypted Session

```
GET //solarisbenchmark.pdf HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg,
image/pjpeg, application/vnd.ms-excel, application/vnd.ms-
powerpoint, application/msword, application/x-shockwave-
flash, */*
Referer:
http://10.0.0.10:60/search/index.jsp?search=1&si=1&ns=10&s
t=relevance&c=Research-Documents&qt=*
Accept-Language: en-nz
Accept-Encoding: gzip, deflate
Range: bytes=306024-
Unless-Modified-Since: Fri, 25 Feb 2005 21:21:43 GMT
If-Range: "115eff-422a22e7"
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1; SV1)
Host: 10.0.0.10:60
Connection: Keep-Alive
Cookie: JSESSIONID=D0432EDE8A802F67921A50A03B2B2232

... (solarisbenchmark.pdf content)
```


Appendix F

Web server access and error log sample.

Appendix F shows a sampling of three access logs and their corresponding error logs recorded during the Nessus scan (Appendix D). Note: Not all access logs will have an error associated with them.

Access Logs

```
10.0.0.11 - - [20/Feb/2005:13:39:38 +1300] "GET /fcgi-bin/echo.exe?foo=<SCRIPT>alert(document.domain)</SCRIPT> HTTP/1.1" 405 124 "-" "-" GET /fcgi-bin/echo.exe foo=<SCRIPT>alert(document.domain)</SCRIPT> "HTTP/1.1" https-filevault.giac-enterprises.com
```

```
10.0.0.11 - - [20/Feb/2005:13:39:39 +1300] "POST /FormHandler.cgi HTTP/1.1" 405 124 "-" "Nessus" POST /FormHandler.cgi - "HTTP/1.1" https-filevault.giac-enterprises.com
```

```
10.0.0.11 - - [20/Feb/2005:13:39:42 +1300] "GET /xsql/demo/airport/airport.xsql?xml-stylesheet=none HTTP/1.0" 404 292 "-" "-" GET xsql/demo/airport/airport.xsql xml-stylesheet=none "HTTP/1.0" https-filevault.giac-enterprises.com
```

Error Logs

```
[20/Feb/2005:13:39:38] config (442):  
for host 10.0.0.11 trying to GET /fcgi-bin/echo.exe, handle-processed reports: HTTP2205: The request method is not applicable to the requested resource.
```

```
[20/Feb/2005:13:39:39] config (442):  
for host 10.0.0.11 trying to POST /FormHandler.cgi, handle-processed reports: HTTP2205: The request method is not applicable to the requested resource.
```

```
[20/Feb/2005:13:39:42] warning (442):  
for host 10.0.0.11 trying to GET  
/xsql/demo/airport/airport.xsql, send-file reports:  
HTTP4142: can't find /docs/xsql/demo/airport/airport.xsql  
(File not found)
```

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced