Global Information Assurance Certification Paper

Auditing Apache Secure Reverse Proxy On HP-UX in a Large Scale Production Environment: An Auditor's Perspective

Kelly M. Hertel
November 2003

Practical Assignment Submitted in Partial Requirement for the
SANS Global Information Assurance Certification (GIAC) program for
GIAC Systems and Network Auditor (GSNA) Certification
GSNA Practical Version 2.1

Abstract:
This paper is written from an auditor's perspective and shows the complete audit process based on an Apache Reverse Proxy, configured on HP-UX v11.11 with HP Apache Bundle in reverse proxy mode in a large-scale production environment. Controls for this environment will be identified by researching current threats and vulnerabilities. A baseline security checklist will be developed that is appropriate for this configuration. Finally, an audit will be performed based on the checklist developed from these security requirements and a report developed that will detail the findings and recommendations for risk mitigation. The style and structure of this paper are meant to conform to the standards set forth for GIAC certification practical assignments.

Table of Contents

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

1.1 Objective of the Audit

The objective of this audit is to specify the configuration of a Secure Reverse Proxy (SRP) in a large-scale production environment, including the platform and operating system the SRP is configured on; identify threats and vulnerabilities that pertain to this configuration and to create an audit checklist. The checklist will then be used to ensure appropriate controls are in place to mitigate and identified risk. A technical review will be conducted against the SRP using the checklist. Finally, a report will be developed that will detail the findings and recommendations for risk mitigation.

This audit will be designed to be repeatable so that the audit and security community can apply the documented learning gained by this practical and improve the state of practice in similar environments.

1.2 Role and Purpose of a SRP

A reverse proxy is the "technology that acts as an intermediate agent between two remote and distinct computing agents and requires no client-side proxy engine or configuration."[i] In this audit, the two remote agents are the web browser and web server. For the purposes of this audit, an SRP is a reverse proxy with authentication and authorization. The SRP will grant or deny access to the user using a web browser to the web-based application based on the response from the authentication and authorization infrastructure. The SRP will proxy the web page to the web browser and maintain session state until the session is terminated.

1.3 How a SRP Works in an Large-Scale Enterprise Environment

A user requests a web page using their web browser. The web browser passes the request to the SRP via SSL. The SRP then passes the request to a SiteMinder Policy Server for authentication and authorization based on the user's credentials. The SiteMinder policy server validates the user's credentials (either certificate or username/password) using an LDAP directory server and, based on the response from the LDAP directory server, SiteMinder policy server will respond to the SRP with either a rejection or approval for authorization to the requested web page. If authentication and authorization is granted, the SRP will pass the request to the web server and the web server will serve up the webpage back to the SRP. The SRP will then proxy the web page back to the web

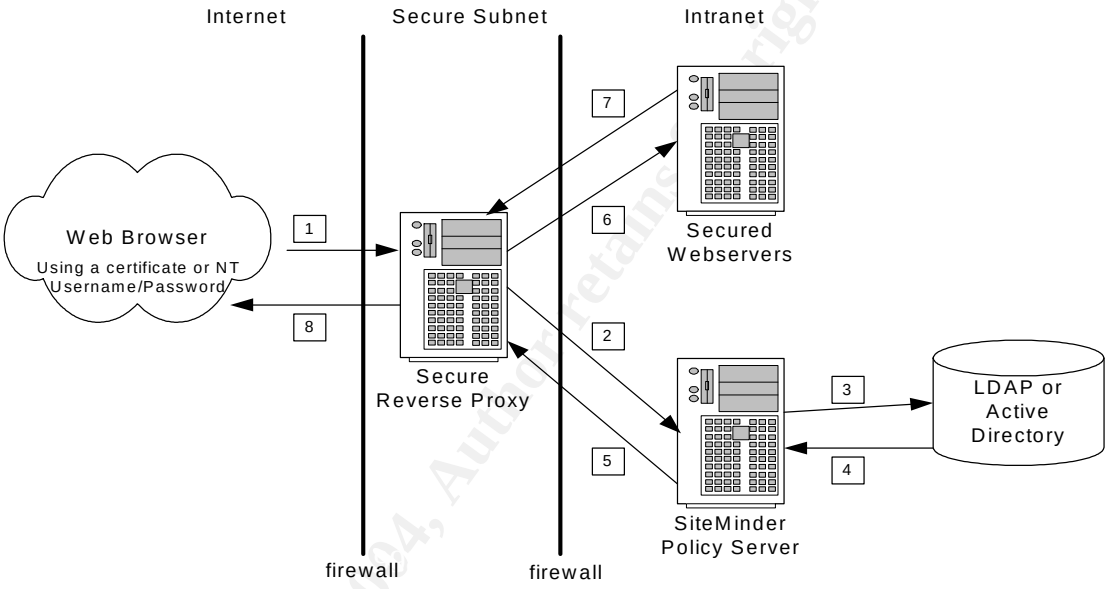
browser and appear to the web browser as serving the web page. The web browser will not see any information on the URL indicating the originating web server. SSL is used for end-to-end session encryption throughout.

In summary:

1. User requests web page through their web browser.
2. Web browser passes request to the SRP.
3. SRP makes a call the SiteMinder policy server.
4. SiteMinder Policy makes a call to the LDAP server to validate the credentials.
5. LDAP responds.
6. SiteMinder Policy server approves or rejects the request.
7. Approval or rejection is passed to the SRP.
8. SRP passes the request to the WEB server if access is granted (note: at this point all traffic between client and SRP is encrypted via HTTPS). If access is denied, the SRP responds to the web agent with a rejected URL request.
9. WEB server serves the web page to SRP.
10. SRP proxies the web page to the web browser.
11. User receives WEB page.

Note: SSL is used for end-to-end session encryption.

Figure 1: Data Flow of SRP in an Large-Scale Enterprise Environment



1.4 System Identified for the Audit

1.4.1 Components that are In-Scope for This Audit

The SRP system to be audited is based on HP-UX v11.11 with the HP Apache Bundle in reverse proxy mode. It is important to understand the baseline configuration of the components of the SRP for developing an appropriate audit checklist. In summary, the following will be the target of this audit:

Table 1: SRP Major Components for Audit:

	Major Components	Model/versions
1	Hardware	PA-RISC (rp2470)
2	HP-UX	11.11
3	Apache	HP 1.3.27 bundle

For the platform, HP-UX 11.11 will be used on the latest PA-RISC version. HP-UX Bastille is a security hardening/lockdown tool for the HP-UX 11.11 operating system and will be used to establish the baseline security-hardened configuration for the SRP. HP-UX Bastille accommodates the various degrees of hardening required of servers used for webs, applications and databases. For the SRP, the server will be locked down using the appropriate hardening settings for web servers. This will include configuring the daemons and system settings appropriately and turning off unneeded services. HP-UX Bastille also creates "'chroot jails' that help limit the vulnerability of common Internet services, such as Web server" [ii] which applies to this SRP configuration.

For the reverse proxy, Apache web server, which is part of the HP 1.3.27 bundle, will be used in this configuration. HP-UX Apache-based Web Server combines numerous modules from Open Source projects and provides the following features for the HP-UX platform including -

- "Scripting capabilities: PHP, mod_perl, CGI;
- Content management: WebDAV;
- Security: authentication through an LDAP server, SSL and TLS support" [iii]

A full list of the product specifications is necessary to understand the configuration capabilities of the SRP. This list will be used to assist in researching vulnerabilities of Apache Web Server on HP-UX 11.11; however only those features required for the SRP configuration will be included in the list of vulnerabilities and threats.

The following is a full list of the product specifications of the Apache Web Server and the added features provided by the HP 1.3.27 bundle:

Table 2: Product Specifications for Apache Web Server[iv]

- **Apache Web Server v.1.3.27**
  Modules statically included http_core, mod_so
  Other standard modules dynamically included mod_access, mod_actions, mod_alias, mod_asis, mod_auth, mod_auth_anon, mod_auth_dbm, mod_autoindex, mod_cern_meta, mod_cgi, mod_define, mod_digest, mod_dir, mod_env, mod_expires, mod_headers, mod_imap, mod_include, mod_info, mod_log_config, mod_mime, mod_mime_magic, mod_negotiation, mod_proxy*,mod_rewrite, mod_setenvif, mod_speling, mod_status, mod_unique_id, mod_userdir, mod_usertrack, mod_vhost_alias
  Note for HP-UX 11i Version 1.6 (IPF) only: mod_proxy is currently not supported in this release.

HP Added Features:

- **Modules dynamically included:** auth_ldap, mod_jk, mod_jserv,

mod_perl, mod_php, mod_ssl

- **RSA's BSAFE Crypto-C Library** v.5.2 (PA-RISC) and v.5.2.1 (IPF) has U.S. Commerce approval for worldwide export of 128-bit strong encryption.
- **OpenSSL** v.0.9.6i is an Open Source toolkit that implements the SSL/TLS security protocols.
- **mod_ssl** v.2.8.11 provides strong cryptography for Apache over SSL using OpenSSL toolkit and BSAFE Crytpo-C libraries.
- **auth_ldap** v.1.6 is the connector between Apache and an LDAP directory server module allowing Apache to authenticate HTTP clients by using entries in an LDAP directory. Auth_ldap supports iPlanet (Netscape) Directory Server and OpenLDAP Server and can be configured to use the stunnel program for secure SSL queries to the LDAP server. Stunnel is started and stopped using the bin/stunnel_ctl.sh utility.
- **mod_perl** v.1.27 is a server plug-in that glues together the Perl runtime library, server software and an object oriented Perl interface to the server's C language API. This makes it possible to write Apache modules entirely in Perl. It is configured for Perl v.5.6.1.
- **mod_jk** v.1.2.0 is the servlet connector to Tomcat in addition to the mod_jserv servlet connector found in previous versions of HP Apache-based Web Server. mod_jk can use either the original ajpv12 protocol or the newer ajpv13 protocol.
- **Apache JServ** v.1.1.1 is a Java servlet engine compliant with Java Servlet Development Kit 2.0. HP Apache-based Web Server uses mod_jserv as the connector.
- **Tomcat** v.3.3.1a is a servlet container which is compliant with Java Servlets 2.2 and JavaServer Pages 1.1.
- **PHP** v.4.2.2 is a popular, server-side, cross-platform, HTML-embedded, full-featured language with a Java/C++ syntax. It also supports many databases.
- **Webmin** v.1.070 is a web-based administration and configuration tool from Webmin. It has been enhanced to handle administration and configuration for the Apache Web Server.
- Support for loading customized **Apache modules implemented in C++**
- **Third Party Support:** BroadVision plug-in provides out-of-the box support for BroadVision e-commerce application suite.
- **Automatic Restart of Apache/Tomcat/Webmin** on reboot. More information on customization/configuration of this feature can be found in the Config Notes.
- **Chroot** causes the named directory to become the root directory, the starting point for path searches. A malicious user cannot get to the root file system. Our chroot includes SSL enhancements. For example pass phrase exits in 60 seconds and limits retries. We include a script for copying OS files under your chroot directory.
- **MM** v.1.2.1 is a 2-layer abstraction library which simplifies the usage of shared memory between forked (and in this way strongly related)

processes under Unix platforms. MM support allows the httpd.conf SSLSessionCache directives shm:/opt/apache/logs/ssl_scache(512000) to be used.

- **certmig** (for PA-RISC only) makes sharing of certificates between the Netscape Enterprise Server and any server that supports PKCS#12 formats possible. The certmig utility is an extension of the pk12util utility, provided by the Mozilla community. In addition to the pk12util functionality, certmig lists and extracts certificates from Netscape certificate databases.
- **Helper utilities** make creating certificates (mkcert.sh) and starting and stopping stunnel (stunnel_ctl.sh) much easier. These two utilities can be found in the /opt/apache/bin/ directory.

Source: http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B9415AA132702

The HP 1.3.27 bundle release was made available in October 2002 with minor releases to address security vulnerabilities. At the time of this audit, Apache v2 was released but was not considered due to core infrastructure dependencies that prohibit the use of it with the existing enterprise environment (specifically the dependency on SiteMinder v5.5).

1.4.2 Components that are Out-Of-Scope for This Audit

This audit will focus specifically on the HP 1.3.27 bundle including HP-UX 11.11 and Apache web server 1.3.27.02 and will not include end-to-end data flow of a full SRP offering. Therefore, the backend authentication and authorization infrastructure using SiteMinder Policy server, ActiveDirectory or LDAP and any backend servers that are addressed by the SRP will not be audited. In addition, network device components (such as routers, switches, hubs) are not part of this audit.

1.5 Risk Evaluation and Security Control Objectives

1.5.1 Overview of Security Controls and Objectives

The objective of securing the reverse proxy is to secure the system itself. This includes providing appropriate access controls and network security as well as to ensure appropriate authentication and authorization controls for granting or denying access to the web applications served by the SRP. Securing the SRP itself is necessary because it is one of the most critical components in the overall service architecture and design used to enable access to intranet web-based

applications from the hostile Internet. Failure to properly secure the SRP could lead to loss of confidential data; loss of brand image and loss of sales (see Section 4.3: Risk Related to Findings).

1.5.2 Audit Control Objectives

Control objectives, both procedural and technical, for audit of the SRP include -

- Identify security level requirements for the SRP.
- Appropriate documentation for the technical configuration of the SRP exists.
- Appropriate documentation of system administration procedures of the SRP exists.
- Operational and administrative responsibilities are clearly defined and documented.
- Least privilege principle is documented in policy and procedures and is implemented appropriately.
- Separation of duty principle is documented in policy and procedures and is implemented appropriately.
- System administrator accounts are traced to unique individuals.
- System administrative access controls are appropriate for the SRP.
- Remote access to SRP is appropriately secured.
- Appropriate documentation for disaster recovery exists, including appropriate backup procedures and storage.
- SRP has appropriate physical security.
- System is appropriately hardened to meet the security level requirements.
- Applicable vendor security announcements are reviewed and acted upon in timely fashion.
- Testing and application of appropriate patches of the SRP system occurs.
- Appropriate log files are generated, maintained, secured and periodically reviewed.
- Monitoring of services and events with notification occurs.
- Alerting exists for indication of system compromise.
- Verify appropriate client access control and channel security exists.
- Appropriate vendor support is available.

1.5.3 System Vulnerabilities, Threats, Risk and Controls for Mitigation

The control objectives listed above mitigate the following risks to an acceptable level of risk for the SRP –

Table 3: System Threats, Vulnerabilities, Risk and Controls for Mitigation:

	Threat	Vulnerability	Consequences	Risk	Control(s)

			/ Impact	**Level**	
1.	Misconfiguration of SRP, allowing inappropriate access to systems and applications protected by SRP	- configuration error or a flawed configuration	- loss of confidentiality, integrity and availability (CIA) of info asset(s) - loss of intellectual property	High	- documented configuration - change management
2.	Misuse of sys admin privileges compromises a system	- malicious sys admin - accidental usage - O/S that does not allow for granularity of privilege	- loss of CIA - loss of intellectual property	Medium	- controlled use of system administrator privileges - system administrator account and tasks are traceable to unique individual
3.	Attacker compromises a system by exploiting a platform/OS vulnerability(s)	- unpatched platform/OS vulnerability(s) - varying vendor notification mechanisms (HP, Apache)	- loss of CIA of info asset(s) - loss of intellectual property - loss of IA of computing resource(s)	Medium	- systematic tracking of vendor security announcements - patching process documented and used - platform vulnerability assessment & notification - monitoring of events and notification
4.	Attacker compromises an improperly maintained system	- configuration error or a flawed configuration	- loss of CIA of info asset(s) - loss of intellectual property - loss of IA of computing resource(s)	Medium	- system administrators must be properly trained - documented configuration - change management - monitoring of

					events and notification
5.	Attacker compromises system by exploiting unnecessary, unmanaged, or default accounts	- well-known default accounts - application accounts	- loss of CIA of info asset(s) - loss of intellectual property - loss of IA of computing resource(s)	Medium	- only required accounts permitted on the system - accounts traceable to a unique individual or to the system administrator(s) - monitoring of events and notification
6.	Attacker compromises system by exploiting unnecessary services	- system OS and application complexity	- loss of CIA of info asset(s) - loss of intellectual property - loss of IA of computing resource(s)	Medium	- unnecessary services, protocols, etc must be disabled
7.	Attacker compromises system by gaining physical access to the system	- system stored/operated in public areas vs. managed data center - media available in public access area - media not sanitized prior to disposal	- loss of CIA of info asset(s) - loss of intellectual property - loss of IA of computing resource(s)	Medium	- system must not be operated or left unattended in any manner that allows unauthorized access - backup media securely stored or destroyed prior to reuse - systems must be protected against interference with configuration or continued operation
8.	Network-based denial of service attack against	- system exists in an improperly	loss of availability of computer	High	- use of host and network IDS

	Internet facing system	configured network environment	resources and data		- O/S hardening
9.	Vendor support of product	- no vendor support of product resulting in unpatched vulnerabilities	- loss of availability of service and data	High	- system must be running a version of product supported by vendor
10.	No ability to recover from system compromise or disaster	- no disaster recovery plan or procedure, including backup procedures	- loss of availability of service and access to data	Medium	- disaster recovery plan must be documented - system administrators have training and knowledge of disaster recovery plans and procedures - backups procedure must be documented and followed

1.5.4 SANS Top 10 UNIX Vulnerabilities

The most critical vulnerabilities to HP-UX can be found at the SANS website http://www.sans.org/top20/. The following table provides the top 10 vulnerabilities:

Table 4: The Twenty Critical Internet Security Vulnerabilities. Version 3.23 May 29, 2003[v]

- U1 Remote Procedure Calls (RPC)
- U2 Apache Web Server
- U3 Secure Shell (SSH)
- U4 Simple Network Management Protocol (SNMP)
- U5 File Transfer Protocol (FTP)
- U6 R-Services -- Trust Relationships
- U7 Line Printer Daemon (LPD)
- U8 Sendmail
- U9 BIND/DNS
- U10 General Unix Authentication -- Accounts with No Passwords or Weak Passwords

Source: http://www.sans.org/top20/

For the SRP, it is important to understand which services are required for the SRP configuration and verify that only services that are required are enabled, specifically: RPC, Apache Web Server, SSH, SNMP and General UNIX Authentication. Vulnerabilities related to these services have been reviewed and are addressed in Table 5: Vendor Vulnerabilities, Threats, Risk and Controls for Mitigation. Services, such as FTP, R-Services, LPD, Sendmail and BIND/DNS are not required and should be disabled.

1.5.5 Vendor Vulnerabilities, Threats, Risk and Controls for Mitigation

This audit looks at how well the SRP (in this case Apache SRP on HP-UX) mitigates risk in a Large Scale Production Environment. It is important to understand the risks associated with Apache SRP on HP-UX 11.11. The following is a table of risks identified on this configuration:

Table 5: Vendor Vulnerabilities, Threats, Risk and Controls for Mitigation

Vulnerabilities for Apache on HP-UX	Threat	Risk Level	Controls for Resolution / Mitigation
Java Virtual Machine (J2SE) and Java Secure Socket Extension (JSSE) potential vulnerability Ref 1: HPSBUX0309-280	Vulnerability exists in Java Secure Socket Extension (JSSE) where it may be possible to gather information about the data transmitted over a secure sockets layer (SSL) or a transport layer security (TLS) channel with CBC encryption. A second vulnerability exists where it may be possible to extract private keys from an SSL server. No known exploits.	Medium	Update to version of Java with security fixes (for details, reference java.sun.com/products/jsse/index-103.html)
HP-UX 11.11 DCE potential vulnerability Ref 1: HPSBUX0309-276	PHNE_27063 introduced new behavior that can	Medium	Install libcma.1 and libcma.2.

	cause DCE libraries to fail. The behavior is present in the superseding patches PHNE_28089 and PHNE_28895. The worm referred to as 'Blaster' or 'W32.Blaster.Worm' creates network traffic, which can lead to the DCE failure when these patches are installed. As the worm attempts to find new systems to infect, it can cause programs to fail. HP-UX is impacted as a side effect of the network traffic generated by the worm.		
Apache web server HTTP TRACE enabled by default. Ref 1: HPSBUX0309-279	HTTP TRACE method returns the contents of client HTTP requests in the entity-body of the trace response. This behavior could be exploited by attackers to access sensitive information. No known exploits		If site requirements allow, disable HTTP TRACE.
wu-ftpd off by one vulnerability Ref 1: bugtraq 8315 (www.securityfocus.com/bid/8315) Ref 2: cve CAN-2003-0466 Ref 3: HPSBUX0309-277	Vulnerability reported to effect the implementation of realpath () in wu-ftpd has led to discovery that the C library is also vulnerable. HP announced that the wu-ftpd program is potentially vulnerable to a buffer overflow but does not affect realpath (3) supplied	Medium	Apply patch specified in HPSBUX0309-277 or ensure FTP daemon/service is not running.

	with HP-UX (only ftpd). Exploits available at http://downloads.securityfocus.com/vulnerabilities/exploits/0x82-wu262.c http://downloads.securityfocus.com/vulnerabilities/exploits/lukemftp.pl http://downloads.securityfocus.com/vulnerabilities/exploits/0x82-WOOoou~happy_new.c		
UNIX shell redirection race condition vulnerability Ref 1: bugtraq 2006 (www.securityfocus.com/bid/2006) Ref 2: cve CAN-2000-1134 Ref 3: HPSBUX0308-275	Vulnerability in UNIX shell may allow local attacker to corrupt files or elevate privileges resulting in a symbolic link attack and could be used to corrupt any file that the owner of the redirecting shell has access to write to. Requires local or telnet access. Exploits available at http://downloads.securityfocus.com/vulnerabilities/exploits/bashack.c	Medium	Apply patch specified in HPSBUX0308-275.
Apache Basic Authentication Module Valid User Login Denial Of Service Vulnerability Ref 1: bugtraq 7725 (www.securityfocus.com/bid/7725) Ref 2: cve CAN-2003-0189 Ref 3: HPSBUX0307-269 (REV 1)	Improper use of spread-safe functions. An attacker may be able to create a circumstance that prevents users from logging into restricted areas with valid user credentials. No known exploits	Low	Install hp-ux apache-based web server bundle v.1.0.06.01 or later. Not vulnerable – SRP for this audit is HP Bundle *v.1.3.27.02.* Verify the HP Bundle installed is greater than v.1.0.06.01.

Apache APR_PSPrintf memory corruption Ref 1: bugtraq 7723 (www.securityfocus.com/bid/7723) Ref 2: cve CAN-2003-0245 Ref 3: HPSBUX0304-256	Potential memory management issue could allow for exploit of mod_dev or other components and could allow for execution of arbitrary code Exploit available at http://downloads.securityfocus.com/vulnerabilities/exploits/Apache-Knacker.pl	Medium	Install hp-ux apache-based web server bundle v.1.0.06.01 or later. Not vulnerable – SRP for this audit is HP Bundle *v.1.3.27.02.* Verify the HP Bundle installed is greater than v.1.0.06.01.
Apache web server linefeed memory allocation denial of service Ref 1: bugtraq 7254 (www.securityfocus.com/bid/7254 Ref 2: cve CAN-2003-0132 Ref 3: HPSBUX0304-256	DoS is due to how Apache allocates large amounts of memory to handle the excessive consecutive line feed characters Exploits available at http://downloads.securityfocus.com/vulnerabilities/exploits/apache-massacre.c http://downloads.securityfocus.com/vulnerabilities/exploits/th-apachedos.c	Medium	Install hp-ux apache-based web server bundle v.1.0.03.01 or later. Not vulnerable – SRP for this audit is HP Bundle *v.1.3.27.02.* Verify the HP Bundle installed is greater than v.1.0.06.01.
Potential vulnerability regarding miniserv.pl Ref 1: bugtraq 6915 (www.securityfocus.com/bid/6915) Ref 2: cve CAN-2003-0101 Ref 3: HPSBUX0303-250	Vulnerability exists in the 'miniserv.pl' script used to invoke both webmin and usermin. Due to insufficient sanitazation of client-supplied BASE64 encoded input, it is possible to inject a Session ID into the access control list. Successful exploit may allow an attacker to bypass typical authentication	Medium	Install hp-ux apache-based web server bundle v.1.3.27.02. Not vulnerable – SRP for this audit is HP Bundle *v.1.3.27.02.* Verify the HP Bundle installed is greater than v1.3.27.00.

	procedures, gaining administrator access to webmin/usermin interface. Exploit available at http://downloads.securityfocus.com/vulnerabilities/exploits/webmin-expliot.pl		
OpenSSL CBC Error Information Leakage Weakness Ref 1: bugtraq 6884 (www.securityfocus.com/bid/6884) Ref 2: cve CAN-2003-0078 Ref 3: HPSBUX0303-248	Requires the target be a man-in-the-middle, attack is difficult to exploit Exploit available at - http://downloads.securityfocus.com/vulnerabilities/exploits/omen-1.1.tar.gz	Low	Upgrade to mod_ssl 2.8.11 or install HP Upgrade Apache-Based Web Server 1.3.27.01 Not vulnerable – SRP for this audit is HP Bundle *v.1.3.27.02.* Verify the HP Bundle installed is greater than *v.1.3.27.02*.
HP-UX 11.11 strlimit() Kernel Panic Vulnerability Dated 12/02/02 Ref 1: bugtraq 4094 (www.securityfocus.com/bid/6884) Ref 2: cve CAN-2002-0279	No known exploits	Medium	Apply HP patch PHKL_26233 Verify HP patch PHKL_26233 is applied

1.6 Current State of Practice

The current state of practice for securing and auditing HP-UX is well defined with published references, guidelines, whitepapers and checklists; however the current state of practice for securing and auditing a reverse proxy is not well defined with little information published in the form of an audit checklist. This is the primary reason for choosing this topic and publishing this practical as it will benefit the security community.

Audit of the SRP will primarily be based on two things: (1) the operating system and (2) the Apache web application running in reverse proxy mode. There are several published papers, articles and guidelines available for HP-UX 11i and several checklists available for auditing and securing UNIX. Checklists such as the 'SANS Audit Checklists, Track 7' a handout provided from the SANS Audit Track, 'UNIX System Security Checklist' available at

http://www-arc.com/security/checklist.html and 'AusCERT - UNIX Security Checklist v2.0 – The Essentials' available at http://www.auscert.org.au/render.html will be used to create an appropriate checklist for this configuration. In regards to Apache Web Server and the HP 1.3.27 bundle, there is product information available but not in the form of a security audit checklist for this specific configuration. One reference, written by Gary Bahadur and Mike Shema, *"Features of Web Server: Improving Apache*; InfoSecurity Magazine"[vi] provides recommendations for improving the security of Apache web server and will be used as a reference when creating a checklist for the SRP. Additional references including vendor product information will be used. The following links are to vendor websites that apply to the SRP configuration - http://www.hp.com/products1/unix/operating/security/index.html, http://www.hp.com/go/webserver and http://www.hp.com/products1/unix/webservers/apache/index.html. These sources of information specifically pertaining to HP-UX 11.11 and Apache web server 1.3.27 will be used to create a comprehensive and repeatable checklist.

There are several audit tools available for auditing the SRP configuration. The auditor will use a selection of these tools to audit the SRP configuration. The tools that were discovered, and are applicable, while researching this configuration include –

- Application scanner, such as SpiDynamic's WebInspect product to audit the web server. Available at http://www.spidynamics.com/productline/WE_over.html
- Bastille for HP-UX, used by administrators to harden HP-UX for the web can be used to determine the current state of security for the operating system and web service. Available at http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6849AA
- Medusa (Master Environment for Detection of UNIX System Anomalies), for monitoring and maintaining security and auditability of HP-UX. The Spy function of Medusa can be used to perform security analyses of user accounts, file systems, network services and software integrity. Available at http://sectools.hp.com/medusa/medusa.htm, and should be installed along with LSOF (LiStOpenFiles), available at ftp://uxcoews5.bbn.hp.com/pub/lsof
- Software Patch Tool for HP-UX, to test installation of security patches required for the SRP configuration. Available at http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA
- SuperScan, for port scanning. Free scanner, available at http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/freetools.htm
- Symantec Enterprise Security Manager for HP-UX, for auditing security policy and system configuration and for host-based IDS. Available at http://enterprisesecurity.symantec.com

- Vendor product commands, such as httpd –lx to view what is installed on the Apache server.

Assignment 2 – The Audit Checklist

Product: Apache Reverse Proxy provided in HP 1.3.27 bundle on HP-UX 11.11
Checklist Version: OCT2003-09
Auditor: Kelly Hertel
Audit Date: _____

2.1 Control Objectives:

- Identify security level requirements for the SRP.
- Appropriate documentation for the technical configuration of the SRP exists.
- Appropriate documentation of system administration procedures of the SRP exists.
- Operational and administrative responsibilities are clearly defined and documented.
- Least privilege principle is documented in policy and procedures and is implemented appropriately.
- Separation of duty principle is documented in policy and procedures and is implemented appropriately.
- System administrator accounts are traced to unique individuals.
- System administrative access controls are appropriate for the SRP.
- Remote access to SRP is appropriately secured.
- Appropriate documentation for disaster recovery exists, including appropriate backup procedures and storage.
- SRP has appropriate physical security.
- System is appropriately hardened to meet the security level requirements.
- Applicable vendor security announcements are reviewed and acted upon in timely fashion.
- Testing and application of appropriate patches of the SRP system occurs.
- Appropriate log files are generated, maintained, secured and periodically reviewed.
- Monitoring of services and events with notification occurs.
- Alerting exists for indication of system compromise.
- Verify appropriate client access control and channel security exists.
- Appropriate vendor support is available.

2.2 Audit Tests

1. Test: Determine the data integrity, system availability and confidentiality requirements of the SRP.	Analysis: Subjective
Control Objective: Identify security requirements for the SRP	
Risk: Compromise to data integrity, system availability and confidentiality (CIA) of the systems or application protected by the SRP due to inadequate security controls; or risk to data availability due to excessive security controls beyond business requirements. For example, a hacker could gain access or control of a system by gaining unauthorized access to the password file due to inadequate security controls.	
Reference: • Bishop, Matt (2003). Computer Security, p.481-494 • Auditor's general knowledge / best practice	
Procedure: 1. Interview SRP Service Manager to determine the security level requirements for the SRP. 2. Interview system administrator to determine basic system level requirements for a general Apache Web Server implementation 3. Compare SRP requirements with generic requirements to determine what additional security requirements need to exist for this SRP configuration.	
Compliance: Test passes if the SRP system architecture meets business security requirements without adding undue costs to the business by overly exceeding these requirements. Pass / Fail	
Comments:	

2. Test: Technical documentation exists and is properly implemented.	Analysis: Subjective
Control Objective: Appropriate documentation for the technical configuration of the SRP exists and that these procedures are adhered to.	
Risk: Attacker compromises an improperly configured system or gains inappropriate access to systems and applications protected by SRP through a misconfigured system. For example, Telnet service is enabled and hacker gains unauthorized system administrator access.	
Reference: • Dayton, Doug (1997). Information Technology Audit Handbook. p.187-189	
Procedure:	

1. Interview system administrator and ask them to produce the SRP technical documentation. 2. Ask questions that pertain to the SRP technical documentation for proof of knowledge of contents.
Compliance: Test passes if system administrator demonstrates sufficient knowledge of the SRP configuration and this knowledge is validated against the SRP technical documentation. Pass / Fail
Comments:

3. Test: SRP configuration change control process is documented and changes are implemented as documented.	Analysis: Objective
Control Objective: Appropriate documentation of change management procedure exists, is adhered to and all changes are documented in the change control log.	
Risk: A change could be applied without proper documentation; therefore a subsequent change could be made to the system causing a system failure resulting from a change conflict and causes a loss in system availability or data integrity.	
Reference: • Tipton & Ruthberg (1993). Handbook of Information Security, p.399-401	
Procedure A: 1. View change control records 2. Validate the changes on record were completed Procedure B: 3. View patch level on SRP. 4. Select a sample of patches applied on SRP. 5. Verify change was properly documented in change control documentation.	
Compliance: Test passes if change control records exist and a sampling of recent changes are validated against the current system configuration. Pass / Fail	
Comments:	

4. Test: SRP system administrative procedures exist and are followed.	Analysis: Objective
Control Objective: Operational and administrative responsibilities of maintaining the SRP are clearly defined and documented.	
Risk: Attacker compromises the system or the applications it is protecting as a result of improper procedures or lack of following appropriate, documented system administrative procedures.	
Reference: • Garfinkel & Spafford (1996). Practical Unix & Internet Security, p.819-840	
Procedure: 1. View documentation for system administrative procedures. 2. Interview administrator based on documented procedures. 3. Observe system administrator conducting sample of system administrative tasks, as documented. An example of this is the creation of a user account is done by following the documented procedures. (Note: The documentation shows that the corporation's internal Virtual Security Manager (VSM) tool is required for this task.	
Compliance: Test passes if system administrator produces documentation and validates knowledgeable of the procedures by answering questions based on the content of the documentation. Demonstration of Add User task is followed, as documented. Pass / Fail	
Comments:	

5. Test: Documentation exists for least privilege and auditor observes this control.	Analysis: Objective Stimulus / Response
Control Objective: Least privilege principle is documented in policy and procedures and is implemented appropriately.	
Risk: Single user compromise of system due to this person having excessive privileges or privileges beyond time needed.	
Reference: • Summers, Rita (1997). Secure Computing: Threats and Safeguards, p.105-106	
Procedure: 1. View documented policy and procedures for existence of least privilege control. 2. Observe system administrator conduct of normal duties for evidence of this controls. 3. Test least privilege by observing the backup administrator attempting to gain access to a file requiring elevated privileges, such as http.conf.	

Compliance: Test passes if system administrator produces documentation and evidence is observed of least privilege by operator's failure to edit the httpd.conf file which requires elevated privileges beyond those granted an operator. Pass / Fail
Comments:

6. Test: Documentation exists for separation of duty and auditor observes this control.	Analysis: Objective Stimulus / Response
Control Objective: Separation of duty principles are documented in policy and procedures and are implemented appropriately.	
Risk: Single user compromise of system due to this person having multiple roles. For example, a database administrator, who has root privileges on the system, could gain access and compromise the password file.	
Reference: • Summers, p.105-106	
Procedure: 1. View documented policy and procedures for existence of separation of duty. 2. Observe system administrator doing conduct of normal duties for existence of evidence of this control. 3. Test separation of duty exists by observing a backup operator attempting to rebuild the kernel, an operation a backup operator would not have permissions to do in his/her role.	
Compliance: Test passes if system administrator produces documentation and demonstrates control exists for separation of duty. Pass / Fail	
Comments:	

7. Test: View sample of all the system accounts and validate accounts are either associated with a unique individual or are locked and associated with a system daemon (e.g. daemon, bin, sys).	Analysis: Objective Stimulus / Response
Control Objective: System administrator accounts are traced to unique individuals or associated with a system process.	
Risk: Attacker compromises the system or the applications it is protecting as a result of improper account administration. For example, an attacker gains unauthorized access to the system through a guest account.	

Reference: • Garfinkel, p.823-824
Procedure: 1. Observe system administrator viewing accounts and validate that the accounts are associated with an authorized user or system process. 2. View the passwd file to validate accounts are assigned to a unique individual or are locked down (i.e. 'lk' is observed after the account). 3. Attempt access to a locked account, expected response is a failure to access account.
Compliance: Test passes if all system accounts and other valid accounts are either associated with a unique individual or are locked and associated with a system daemon. Attempt to access a locked account should fail. Pass / Fail
Comments:

8. Test: SRP administrative access controls exist and are properly implemented.	Analysis: Objective Stimulus / Response
Control Objective: System administrative access controls are appropriate for the SRP.	
Risk: Attacker compromises the system or the applications it is protecting as a result of improper access controls for administrators. For example, an attacker gains unauthorized access by remotely accessing the root account.	
Reference: • Garfinkel, p.820-821	
Procedure: 1. Interview administrator about administrative access controls. 2. Observe system administrator in using these access controls. 3. Observe system administrator using Powerbroker for privileged access. 4. Observe user attempting to elevate privileges without use of Powerbroker (logged in as user, attempting to execute 'su'– thus overriding Powerbroker to gain elevated privileges).	
Compliance: Test passes if system administrator is aware of appropriate administrative access controls and demonstrates they are implemented appropriately, such as attempt to gain privileged access without use of powerbroker. Pass / Fail	
Comments:	

9. Test: Demonstrate appropriate remote access security.	Analysis: Objective Stimulus / Response
Control Objective: Remote access to SRP is appropriately secured (e.g. use of SSH).	
Risk: Attacker compromises the system or the applications it is protecting as a result of improper remote access security.	
Reference: • Van der Walt, Charl (2002). Assessing Internet Security Risk (http://www.securityfocus.com/infocus/1612)	
Procedure: 1. View documented procedures for remote access. 2. Interview administrator on documented remote access procedures. 3. Validate procedure is followed by direct observation of remote access to SRP following documented procedures by use of SSH. 4. Validate remote access to SRP cannot be obtained by undocumented process (i.e. remote access to SRP by Telnet).	
Compliance: Test passes if system administrator demonstrates appropriate remote access security is implemented, can appropriately gain remote access as documented and cannot gain access by use of Telnet. Pass / Fail	
Comments:	

10. Test: SRP backup procedures are documented and are followed.	Analysis: Subjective
Control Objective: Appropriate documentation of backup procedure exists and adherence to procedure is demonstrated.	
Risk: No ability to recover data.	
Reference: • Garfinkel, p.822-823	
Procedure A: 1. View documentation for backup procedures. 2. Interview administrator based on documented procedures, including frequency of backups, storage of backups and procedure for recovery of data. 3. Ask administrator to attest to following the procedures.	
Compliance: Test passes if system administrator produces documentation of backup procedures, validates knowledge of the procedures by answering questions based on the content of the documentation and attests to these procedures being followed.	

Pass / Fail
Comments:

11. Test: Disaster recovery plan (DRP) exists and SRP is part of it.	Analysis: Subjective
Control Objective: Appropriate documentation exists for disaster recovery plan and the SRP is part of the systems included in the DRP plan	
Risk: No ability to recover from a disaster.	
Reference: • Kaplan, Jim (2002). Disaster Recovery Business Continuity Audits (http://www.auditnet.org/drp.htm)	
Procedure: Interview system administrator or data center manager and verify that 1. DRP exists for the data center 2. SRP system is included as part of the DRP 3. SRP is appropriately prioritized in the DRP for recovery based on business requirements.	
Compliance: Test passes if system administrator or data center manager produces documented DRP, validates knowledge of the procedures by answering questions based on the content of the DRP and attests that the SRP is part of the DRP documentation and appropriately prioritized based on business requirements. Pass / Fail	
Comments:	

12. Test: Validate the SRP is a secured environment with appropriate physical access controls.	Analysis: Objective or Subjective
Control Objective: SRP is located in a physically secure environment.	
Risk: Attacker compromises system by gaining physical access to the system.	
Reference: • Garfinkel, p.827-828	
Procedure: - Conduct a physical security review of the SRP location (Objective); OR - Ask system administrator to describe the environment and to attest to the fact that it is physically secured (Subjective).	
Compliance:	

Test passes if the SRP is physically secured from inappropriate access, OR the system administration attests to the fact that the SRP is physically secured from inappropriate access. This should include appropriate physical access controls such as "server located in locked room with restricted access, access to the server room forces the individual entering to distinguish himself or herself from anyone else, ID of security card recorded as well as date and time of entry and exit."[vii] Pass / Fail
Comments:

13. Test: Produce log files, verify they are kept for minimum amount of time, properly secured from inappropriate access and periodically reviewed.	Analysis: Objective
Control Objective: Appropriate log files are generated, maintained, secured and periodically reviewed.	
Risk: Do not have appropriate logs to provide documentation for a forensic investigation.	
Reference: • Garfinkel, p.825-826	
Procedure: 1. Ask system administrator to view a sampling of log files (syslog, btmp, sulog as examples) and view the history or retention setting for those log files 2. Witness system administrator access for appropriate access controls to the log files 3. Ask system administrator to show that the log files were recently reviewed by displaying entries of such in the appropriate log files.	
Compliance: Test passes if system administrator demonstrates log retention capability with appropriate access controls and that log files have been periodically reviewed. Pass / Fail	
Comments:	

14. Test: Verify relevant security events are monitored.	Analysis: Objective
Control Objective: Monitoring of security relevant services and events.	
Risk: Significant security event occurs and no one is aware, thereby no incident response can occur. An attacker compromise to a system would go	

undetected.
Reference: • Garfinkel, p.819-840
Procedure: 1. Ask system administrator how monitoring of relevant security events is accomplished. 2. Ask system administrator to produce a list of relevant security events. 3. Ask system administrator to demonstrate monitoring occurs and compare output to list of relevant security events.
Compliance: Test passes if system administrator can show that monitoring exists for relevant security events. Pass / Fail
Comments:

15. Test: Determine if alerting exists for relevant security events and test alerting process by generating a security event.	Analysis: Objective Stimulus / Response
Control Objective: Alerting exists for relevant security events.	
Risk: System is compromised; no immediate alerting or notification occurs thereby an attacker could gain unauthorized access for an excessive period of time and use the system for their own nefarious purposes.	
Reference: • Wong, Chris (2002). HP-UX 11i Security, p.401-405	
Procedure: 1. Ask the system administrator what the alerting process is. 2. Ask system administrator to log into the host, show that alerting agent is installed and configured properly. 3. Verify alerting process exists by having the system administrator generate a security event, such as failed attempt to gain elevated privileges, and validate that the event triggered appropriate notification.	
Compliance: Test passes if system administrator can demonstrate alerting agent is installed and alerting of security relevant events exists and can be demonstrated. Pass / Fail	
Comments:	

16. Test: Verify SRP operating system is sufficiently secured based on requirements and best practices.	Analysis: Objective Stimulus / Response
Control Objective: System is appropriately hardened to meet the security level requirements	
Risk: Loss of confidentiality, integrity and availability due to exploitation of the system, such as an attacker compromising the system by exploiting vulnerability in a non-essential service or exploits a misconfigured system, allowing inappropriate access to systems and applications protected by SRP.	
Reference: • Garfinkel, p.831-833	
Procedure: 1. Auditor will run port scanner against SRP server to determine what services are running. 2. Review the output for any non-essential services running.	
Compliance: Test passes if output from port scanner indicates no inappropriate services are running. Pass / Fail	
Comments:	

17. Test: Verify that appropriate mitigating controls are applied for Apache web server as they apply to the SRP configuration.	Analysis: Objective
Control Objective: Applicable Apache web server vendor security announcements including patch releases are reviewed and acted upon in timely fashion.	
Risk: Attacker compromises a system by exploiting Apache web server vulnerability(s). This could allow an attacker to conduct a sql-injection attack or other known exploits.	
Reference: • SRP Blueprint document. • IT Resource Center Technical Knowledge Base (http://www1.itrc.hp.com/service/cki/search.do?category=c0&mode=text&searchString=apache+security&searchCrit=allwords&docType=Security&docType=Patch&docType=EngineerNotes&docType=BugReports&docType=Hardware&docType=ReferenceMaterials&docType=ThirdParty&search.x=11&search.y=13)	
Procedure:	

1. Ask system administrator how they track Apache web server vulnerability announcements (such as bugtraq, vendor notification lists, vendor website). 2. Review recent vulnerability notifications and select sample that apply to this configuration 3. Review change control documentation for existence of application of mitigating control (such as a patch or manual configuration change to mitigate risk). 4. View system information for existence of patches applied.
Compliance: Test passes if SRP configuration has appropriate mitigating controls applied to the SRP system based on Apache vulnerability announcements and recommendations for remediation (i.e. patch installation) have been performed. Pass / Fail
Comments:

18. Test: Verify that appropriate mitigating controls are applied for HP-UX 11.11 as they apply to the SRP configuration.	Analysis: Objective
Control Objective: Applicable HP-UX 11.11 security announcements including patch releases are reviewed and acted upon in timely fashion.	
Risk: Attacker compromises a system by exploiting platform/OS vulnerability(s).	
Reference: • SRP Blueprint document • Garfinkel, p.819-840	
Procedure: 1. Ask system administrator how they track specific HP-UX vulnerability announcements (such as bugtraq, vendor notification lists, vendor website). 2. Review recent vulnerability notifications and select sample that apply to this configuration 3. Review change control documentation for existence of application of mitigating control (such as a patch or manual configuration change to mitigate risk). 4. View system information for existence of patches applied.	
Compliance: Test passes if SRP configuration has appropriate mitigating controls applied to	

the SRP system based on HP-UX vulnerability announcements and recommendations for remediation (i.e. patch installation) have been performed. Pass / Fail
Comments:

19. Test: Verify the current version of product (HP-UX 11.11 and Apache Web Server 1.3.x) is supported by vendor.	Analysis: Objective
Control Objective: Appropriate vendor support is available for the current version of product.	
Risk: Compromise to availability of data.	
Reference: • HP-UX (http://www.hp.com/products1/unix/operating/infolibrary/) • Apache HP Bundle (http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B9415AA132702)	
Procedure: 1. Check current versions of product used. 2. Validate that these versions are supported by vendor by reviewing vendor website.	
Compliance: Test passes if vendor website indicates support of current product(s) used. Pass / Fail	
Comments:	

20. Test: Verify appropriate client access control and channel security exist.	Analysis: Objective
Control Objective: Ensure appropriate end-to-end security controls are in place.	
Risk: Compromise to confidentially and data integrity.	
Reference: • Bishop, p.805-807 • Auditor's general knowledge / best practice	
Procedure:	

1. Ask system administrator to create an account for the auditor. 2. On a client system on the same subnet as either the client or the server, run a network analyzer (sniffer). 3. Verify that web pages are only displayed with appropriate authentication and authorization using this account. 4. Attempt to access the same webpage with invalid credentials.
Compliance: Test passes if, based on the client's authentication and authorization credentials, only appropriate information is displayed back to the client's web browser. Valid credentials should display appropriate data and invalid credentials should produce an error. Pass / Fail
Comments:

Assignment 3 – Audit Evidence – Conducting the Audit

This section of the audit takes the developed checklist and applies the methodology to the SRP in an enterprise environment. A complete audit was performed based on the checklist developed in 'Assignment 2'. Twelve of the tests, of which eight are stimulus-response tests, were taken from the completed checklist and are presented in this section.

The 'Comments' section of each step shows the details of the information gathered through observations and interviews during the actual audit. These comments support the 'Pass' or 'Fail' rating of each audit step.

The 'Compliance' section will indicate Pass or Fail for the test. If the test passes, this section will be highlighted in **GREEN** and labeled '**PASSED'**. If the test fails, this section will be highlighted in **RED** and labeled '**FAILED'**.

3.1 Audit Tests

1. Test: Determine the data integrity, system availability and confidentiality requirements of the SRP.	Analysis: Subjective
Control Objective: Identify security requirements for the SRP	
Risk: Compromise to data integrity, system availability and confidentiality (CIA) of the systems or application protected by the SRP due to inadequate security controls; or risk to data availability due to excessive security controls beyond business requirements. For example, a hacker could gain access or control of a system by gaining unauthorized access to the password file due to inadequate security controls.	
Reference: • Bishop, Matt (2003). Computer Security, p.481-494 • Auditor's general knowledge / best practice	
Procedure: 1. Interview SRP Service Manager to determine the security level requirements for the SRP. 2. Interview system administrator to determine basic system level requirements for a general Apache Web Server implementation 3. Compare SRP requirements with generic requirements to determine what additional security requirements need to exist for this SRP configuration.	
Compliance: Test passes if the SRP system architecture meets business security requirements without adding undue costs to the business by overly exceeding these requirements. **PASSED**	

Comments: To determine what level of system security is required for the SRP we needed to determine the confidentiality requirements of the data, system integrity requirements and system availability requirements. The service manager was identified as the best candidate to provide this information as the SRP was developed for multiple businesses with multiple business sponsors all with similar access requirements to their web-based applications. The system administrator was identified to provide the basic system security requirements of an HP-UX 11.11 server running Apache as an Internet facing host. During the interview it was discovered that the SRP, as an Internet-facing server, would be required to follow stringent host security policy and standards. The policy and standards that apply to the SRP include such things as formal change management processes; changes to the SRP including enabling application and services require approval by the system manager, service manager and application owners; logging required for authentication, denied access, installation and removal of accounts; access to accounts with administrative privileges must be authenticated; physical access to peripherals and media must be secured; formal documented process for backup/recovery, backups must be protected against unauthorized disclosure and process must be tested; system must be registered in corporate registration database. The data accessed by the SRP is labeled by the data owner and will require the most stringent access controls based on the highest level of data label. For the data served by the SRP, the highest data label is 'Confidential' per the guidelines of data labeling for this company. The data must be restricted to a specific group or department and cannot be posted in plain sight on the Intranet or Internet. Authentication requirements include certificates at the SRP and a minimum of username/password at the application. The SRP Blueprint document specified the requirements noted during this interview and is the document used to install and configure the SRP. It was verified that the document includes stringent host security configuration requirements as well as integration with SiteMinder for authentication and authorization requirements. The SRP Blueprint also includes additional security measures such as IPFilters configuration for access control lists to further control access by limiting access to explicitly specified IP addresses only. This is not considered to be exceeding the security and business requirements of the SRP as it is at adds no additional cost and aids in limiting access to the SRP and the data it is protecting and is considered a best practice for this configuration.

2. Test: Technical documentation exists and is properly implemented.	Analysis: Subjective
Control Objective: Appropriate documentation for the technical configuration of the SRP exists and that these procedures are adhered to.	
Risk: Attacker compromises an improperly configured system or gains	

inappropriate access to systems and applications protected by SRP through a misconfigured system. For example, Telnet service is enabled and hacker gains unauthorized system administrator access.
Reference: • Dayton, Doug (1997). Information Technology Audit Handbook. p.187-189 • SRP Blueprint (internal document)
Procedure: 1. Interview system administrator and ask them to produce the SRP technical documentation. 2. Ask questions that pertain to the SRP technical documentation for proof of knowledge of contents.
Compliance: Test passes if system administrator demonstrates sufficient knowledge of the SRP configuration and this knowledge is validated against the SRP technical documentation. **FAILED**
Comments: 1. The interview was conducted with the engineer and the system administrator. They produced the SRP technical documentation (i.e. SRP Blueprint). 2. The system administrator had knowledge of the contents in the document but was not sufficiently familiar with the HP-UX Hardening Blueprint referenced by the document. The HP-UX Hardening Blueprint is a key internal reference document system administrators use to harden a server, either manually or through the use of HP's Bastille found at http://software.hp.com.

3. Test: SRP configuration change control process is documented and changes are implemented as documented.	Analysis: Objective
Control Objective: Appropriate documentation of change management procedure and adherence to procedure	
Risk: A change could be applied without proper documentation; therefore a subsequent change could be made to the system causing a system failure resulting from a change conflict and causes a loss in system availability or data integrity.	
Reference: • Tipton & Ruthberg (1993). Handbook of Information Security, p.399-401	
Procedure A: 1. View change control records 2. Validate the changes on record were completed	

3. View patch level on SRP

Procedure B:

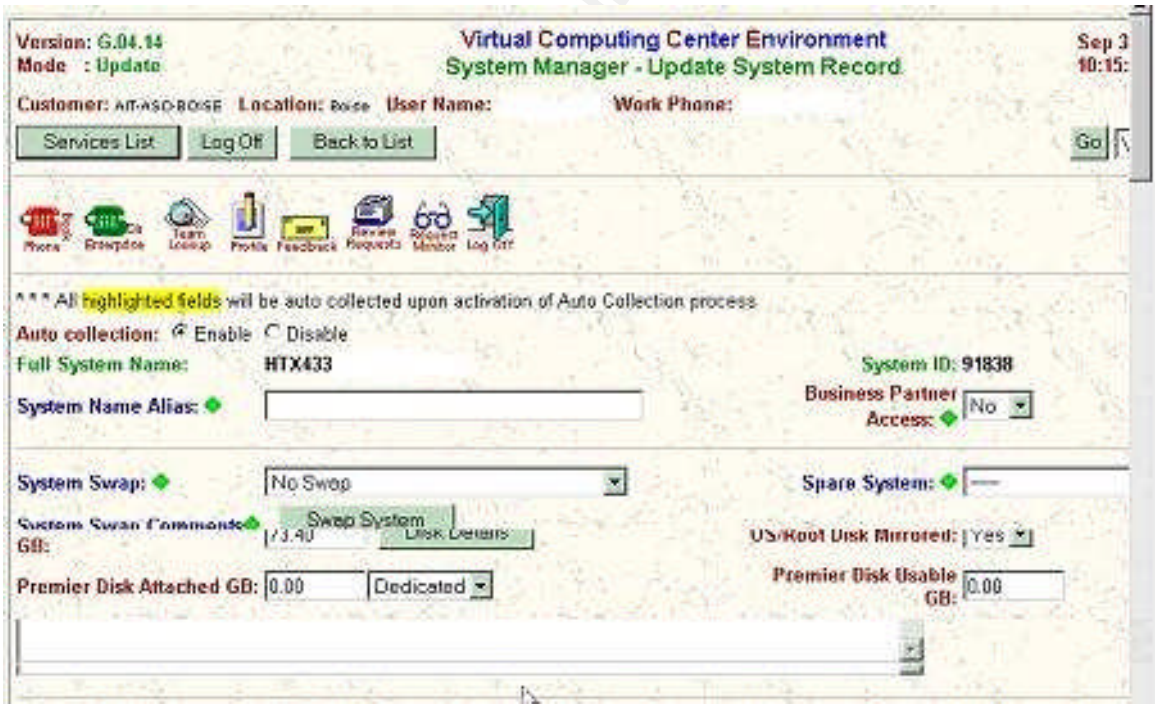
4. Select a sample of patches applied on SRP.
5. Verify change was properly documented in change control documentation.

Compliance: Test passes if change control records exist and a sampling of recent changes are validated against the current system configuration.

FAILED

Comments:
Change control is managed through a centralized system and the process is documented. The system administrator demonstrated sufficient knowledge of this process and the auditor observed the system administrator accessing the change control system (VCCE) and demonstrating the tool and process. It was noted that the SRP system is newly configured and just entering the pilot phase of the development lifecycle. Current configuration information exists for the SRP servers in VCCE.

Screenshot sample of system administrator using VCCE tool and demonstrating that the SRP servers exists in the tool:



No formal changes have occurred since the servers entered pilot, therefore the audit steps for this checklist item could not be completed.

4. Test: SRP system administrative procedures exist and are followed.	Analysis: Objective
Control Objective: Operational and administrative responsibilities of maintaining the SRP are clearly defined and documented.	
Risk: Attacker compromises the system or the applications it is protecting as a result of improper procedures or lack of following appropriate, documented system administrative procedures.	
Reference: • Garfinkel & Spafford (1996). Practical Unix & Internet Security, p.819-840	
Procedure: 1. View documentation for system administrative procedures. 2. Interview administrator based on documented procedures. 3. Observe system administrator conducting sample of system administrative tasks, as documented. An example of this is the creation of a user account is done by following the documented procedures. (Note: The documentation shows that the corporation's internal VSM tool is required for this task.	
Compliance: Test passes if system administrator produces documentation and validates knowledgeable of the procedures by answering questions based on the content of the documentation. Demonstration of Add User task is followed, as documented. **PASSED**	
Comments: 1. System administrator documentation was provided. 2. Several procedures were demonstrated as part of this audit by the system administrator. 3. System administrator showed knowledge and understanding of Account Creation process. Screen shot of system administrator creating a user account:	

Note: some fields have been blanked out intentionally.

5. Test: Documentation exists for least privilege and auditor observes this control.	Analysis: Objective Stimulus / Response
Control Objective: Least privilege principle is documented in policy and procedures and is implemented appropriately.	
Risk: Single user compromise of system due to this person having excessive privileges or privileges beyond time needed.	
Reference: • Summers, Rita (1997). Secure Computing: Threats and Safeguards, p.105-106	
Procedure: 1. View documented policy and procedures for existence of least privilege control. 2. Observe system administrator conduct of normal duties for evidence of this controls. 3. Test least privilege by observing the backup administrator attempting to gain access to a file requiring elevated privileges, such as http.conf.	
Compliance: Test passes if system administrator produces documentation and evidence is observed of least privilege by operator's failure to edit the httpd.conf file which requires elevated privileges beyond those granted an operator.	

PASSED

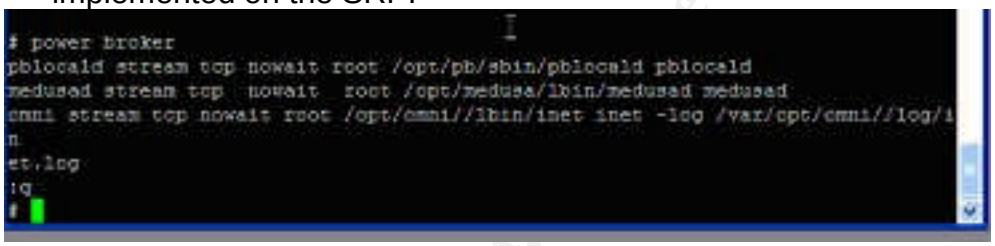
Comments:

1. It was observed that processes are in place and documented to comply with least privilege requirements and the system administrator and engineer has knowledge of least privilege.

   During the interview with the system administrator and system engineer, they answered questions regarding least privilege. They demonstrated knowledge and use of Symark Powerbroker, which is documented and used in the HP-UX environment in this enterprise. This is an example of least privilege tool which "enables system administrators to delegate administrative privileges and authorization without disclosing the root password and to grant selective access"[viii].

2. Observe system administrator for evidence of this control:

   a. Screen shot of Powerbroker from configuration file, indicating it is implemented on the SRP:



   b. Successful attempt of Powerbroker as used by the system administrator on SRP server:

```
****************************************
Last login:  26 Sep 08:52
$ pbrun ksh
#
```

   Note: the command 'pbrun ksh' gives root access for uniquely identified user account.

   c. Failed attempt to use Powerbroker by a user who does not have permissions to run Powerbroker.

```
htx433:/home/tmiller $ id
uid=2183(tmiller) gid=20(users)
htx433:/home/tmiller $ pbrun ksh
Request rejected by pbmasterd on xxxxxx.xxx.xx.com
```

3. Failed attempt to by operator to access the /opt/apache/conf/httpd.conf file. Specifically, operators are only granted access to conduct specific backup operations. For example, operators do not have privileges to edit

Apache configuration files. Attempt to edit httpd.conf resulted in a failure message, as expected.

```
htx433:/home/tmiller $ id
uid=2183(tmiller) gid=20(users)
htx433:/home/tmiller $ pbrun -u www vi /opt/apache/conf/httpd.conf
Request rejected by pbmasterd on xxxxxx.xxx.xx.com
htx433:/home/tmiller $ _
```

7. Test: View sample of all the system accounts and validate accounts are either associated with a unique individual or are locked and associated with a system daemon (e.g. daemon, bin, sys).	Analysis: Objective Stimulus / Response

Control Objective: System administrator accounts are traced to unique individuals or associated with a system process.

Risk: Attacker compromises the system or the applications it is protecting as a result of improper account administration. For example, an attacker gains unauthorized access to the system through a guest account.

Reference:

- Garfinkel, p.823-824

Procedure:

1. Observe system administrator viewing accounts and validate that the accounts are associated with an authorized user or system process.
2. View the passwd file to validate accounts are assigned to a unique individual or are locked down (i.e. 'lk' is observed after the account).
3. Attempt access to a locked account, expected response is a failure to access account.

Compliance: Test passes if all system accounts and other valid accounts are either associated with a unique individual or are locked and associated with a system daemon. Attempt to access a locked account should fail.

PASSED

Comments:

1. It was observed through the use of `#more passwd` that all accounts were associated with a unique individual. The system administrator attested to this. The server is also in pilot and it was noted that only a few individual user accounts existed.
2. It was observed through the use of `#passwd -s -a` conducted by the system administrator that 'Important Users' (e.g. root, daemon, bin, sys, adm, uucp, lp, etc)[ix] accounts were locked and individual accounts were uniquely identified.

Screen shot of 'passwd –s –a' output:

```
root  PS    07/17/03    0  182
daemon  LK
bin  LK
sys  LK
adm  LK
uucp  LK
lp  LK
nuucp  LK
hpdb  LK
www  LK
bkpadmnh  PS    06/05/03    0  182
bkpadmsh  PS    05/02/02    0  182
bkpadmjh  PS    05/08/03    0  182
bkpadmch  PS    06/12/03    0  182
bkpadmin  PS    04/11/02    0  182
mnagel  PS    06/20/02    0  182
rsimnitt  PS    01/02/03    0  182
bbowden  PS    07/11/02    0  182
kstites  PS    07/11/02    0  182
```

3. Attempt access to a locked account (adm). Expected response is a failure to access account.

```
$ telnet htx433
Trying…
Connected to htx433
Escape character is '^]'.
Local flow control on
Telnet TERMINAL-SPEED option ON
login: adm
Password:
Login incorrect
login: adm
Password:
Login incorrect
login: adm
Password:
Connection closed by foreign host.
```

8. Test: SRP administrative access controls exist and are properly implemented.	Analysis: Objective Stimulus / Response
Control Objective: System administrative access controls are appropriate for the SRP.	
Risk: Attacker compromises the system or the applications it is protecting as a result of improper access controls for administrators.	
Reference: • Garfinkel, p.820-821	
Procedure: 1. Interview administrator about administrative access controls.	

2. Observe system administrator in using these access controls.
3. Observe system administrator using Powerbroker for privileged access.
4. Observe user attempting to elevate privileges without use of Powerbroker (logged in as user, attempting to execute 'su'– thus overriding Powerbroker to gain elevated privileges).

Compliance: Test passes if system administrator is aware of appropriate administrative access controls and demonstrates they are implemented appropriately, such as attempt to gain privileged access without use of powerbroker.

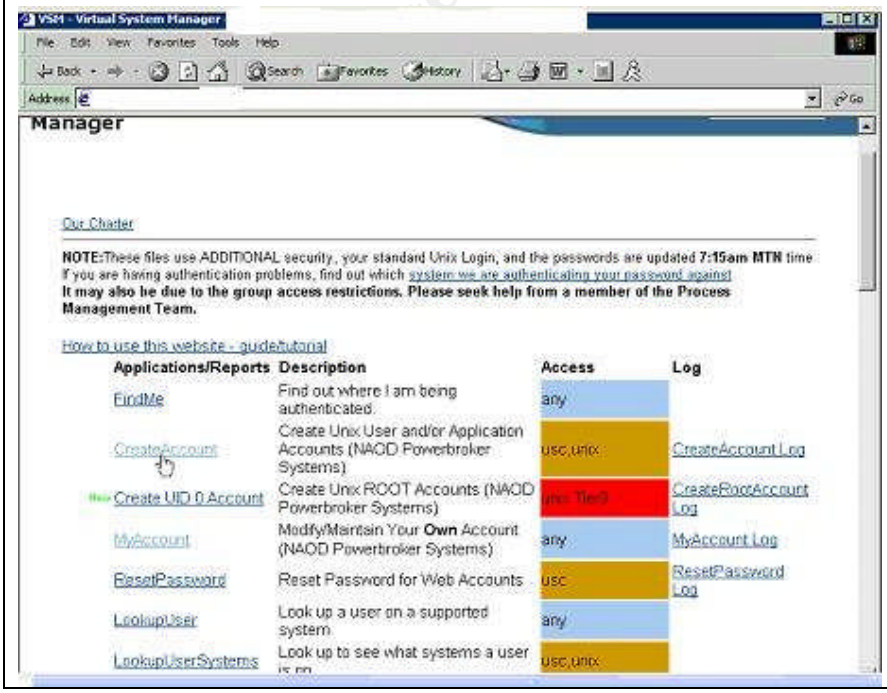
PASSED

Comments:

1. System administrator was able to provide information about administrative access controls; specific examples were given in relation to root access and Powerbroker.
2. System administrator explained, and then demonstrated knowledge of the administrative access control process and use of powerbroker to delegate privilege authorization and selective access (reference Test 5: Documentation exists for least privilege and auditor observes this control).

   System administrator was also familiar with new account access control process for system administrators – from initial request in the VSM tool. This included validating user access request with management through granting access based on management approval.

Screenshot of VSM tool used for various user administrator tasks and logging of such tasks:



3. See #2 above.
4. Observe user attempting to elevate privileges without use of Powerbroker (logged in as user, attempting to execute 'su'– thus overriding Powerbroker to gain elevated privileges).

```
htx433:/home/tmiller $ id
uid=2183(tmiller) gid=20(users)
htx433:/home/tmiller $ su
Request rejected
htx433:/home/tmiller $
```

Additional administrative access control test :
From a user account authorized in Powerbroker to only perform web administrator actions, attempt to execute a command as 'su':

```
htx433:home/pfroj $ pbrun su sysinfo
Request rejected by pbmasterd on xxxxxx.xxx.xx.com
htx433:home/pfroj $
```

From a user account authorized in Powerbroker to execute same command:

```
htx433:home/rkelly $ pbrun ksh
htx433:home/rkelly $ su sysinfo
htx433:home/rkelly $ id
uid=2062(sysinfo) gid=20(users)
htx433:home/rkelly $
```

9. Test: Demonstrate appropriate remote access security.	Analysis: Objective Stimulus / Response
Control Objective: Remote access to SRP is appropriately secured (e.g. use of SSH).	
Risk: Attacker compromises the system or the applications it is protecting as a result of improper remote access security.	
Reference: • Van der Walt, Charl (2002). Assessing Internet Security Risk (http://www.securityfocus.com/infocus/1612)	
Procedure: 1. View documented procedures for remote access. 2. Interview administrator on documented remote access procedures. 3. Check for compliance of remote access procedures (use of SSH). 4. Validate remote access to SRP cannot be obtained by undocumented or insecure process (i.e. remote access to SRP by Telnet or FTP).	

Compliance: Test passes if system administrator demonstrates appropriate remote access security is implemented, can appropriately gain remote access as documented and cannot gain access by use of Telnet.

FAILED

Comments:

1. Documentation was provided and reviewed, including references to related Security policy and standards.
2. Security policy and standards require the use of Secure Shell (SSH) for remote access.
3. SSH was not enabled.

```
htx433:/home/tmiller ->/usr/bin/ssh -V
/usr/bin/ksh: /usr/bin/ssh: not found
htx433:/home/tmiller ->
```

4. Telnet and FTP were enabled and used.
   During the interview with the system administrator it was found that Telnet was being used instead of SSH because the set of cryptographic keys had not been issued yet.

```
htx433:/home/tmiller $ /usr/bin/netstat -af inet | /usr/bin/grep telnet
tcp   0   0  *.telnet           *.*                    LISTEN
tcp   0   2  htx433.telnet      15.71.112.100.2038     ESTABLISHED
tcp   0   0  htx433.telnet      15.71.112.100.2043     ESTABLISHED
htx433:/home/tmiller $ /usr/bin/netstat -af inet | /usr/bin/grep ftp
tcp   0   0  *.ftp              *.*                    LISTEN
```

Note: IP address modified for protection of host.

14. Test: Verify relevant security events are monitored.	Analysis: Objective
Control Objective: Monitoring of security relevant services and events.	
Risk: Significant security event occurs and no one is aware, thereby no incident response can occur. An attacker compromise to a system would go undetected.	
Reference: • Garfinkel, p.819-840	
Procedure: 1. Ask system administrator how monitoring of relevant security events is accomplished. 2. Ask system administrator to produce a list of relevant security events. 3. Ask system administrator to demonstrate monitoring occurs and compare output to list of relevant security events.	
Compliance:	

Test passes if system administrator can show that monitoring exists for relevant security events.

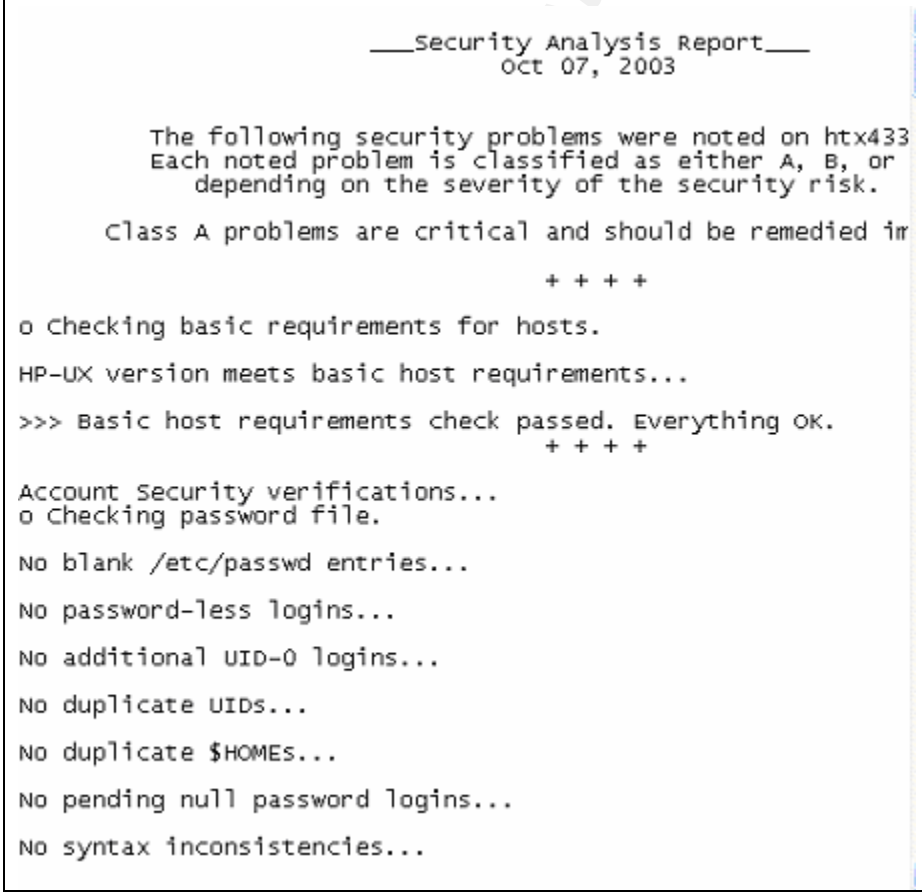
FAILED

Comments:

1. System administrator explained how monitoring of relevant security events occurs. It is based on a series of process steps. Medusa is used to monitor the system and generate reports. These reports are centrally logged into a database for the enterprise and managed through the corporation's internal VSM tool. This is done by the 'gather sysinfo' script and scheduled through crontab to send system information collected by the 'gather sysinfo' script to the VSM central repository. The VSM tool will show system configuration, patch and security-related information but does not do notification other than to the VSM tool. A system administrator needs to monitor the status of the system through the VSM GUI.

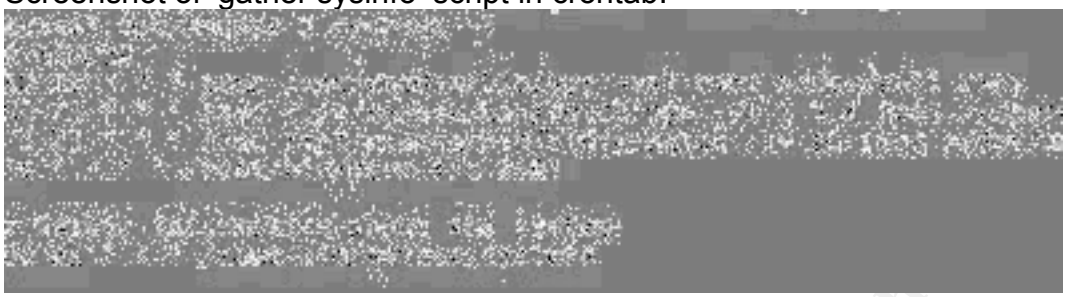
   Medusa is used for security analysis and diagnostic report, by default, the report is located at /usr/local/medusa/etc/spy.report.

   Sample output from spy.report:



```
                    ___Security Analysis Report___
                              Oct 07, 2003


         The following security problems were noted on htx433
         Each noted problem is classified as either A, B, or
            depending on the severity of the security risk.

      Class A problems are critical and should be remedied im

                                  + + + +

o Checking basic requirements for hosts.

HP-UX version meets basic host requirements...

>>> Basic host requirements check passed. Everything OK.
                                  + + + +

Account Security verifications...
o Checking password file.

No blank /etc/passwd entries...

No password-less logins...

No additional UID-0 logins...

No duplicate UIDs...

No duplicate $HOMEs...

No pending null password logins...

No syntax inconsistencies...
```

Screenshot of 'gather sysinfo' script in crontab:



2. Relevant security events are included in the VSM tool and updated as necessary.
3. System administrator could not demonstrate monitoring occurs to the VSM tool for the SRP servers. This had not been established yet and therefore comparing the output to the list of relevant security events was not possible.

15. Test: Determine if alerting exists for relevant security events and test alerting process by generating a security event.	Analysis: Objective Stimulus / Response
Control Objective: Alerting exists for relevant security events.	
Risk: System is compromised; no immediate alerting or notification occurs thereby an attacker could gain unauthorized access for an excessive period of time and use the system for their own nefarious purposes.	
Reference: • Garfinkel, p.819-840	
Procedure: 1. Ask the system administrator what the alerting process is. 2. Ask system administrator to log into the host, show that alerting agent is installed and configured properly. 3. Verify alerting process exists by having the system administrator generate a security event, such as failed attempt to gain elevated privileges, and validate that the event triggered appropriate notification.	
Compliance: Test passes if system administrator can demonstrate alerting agent is installed and alerting of security relevant events exists and can be demonstrated.	

FAILED

Comments:

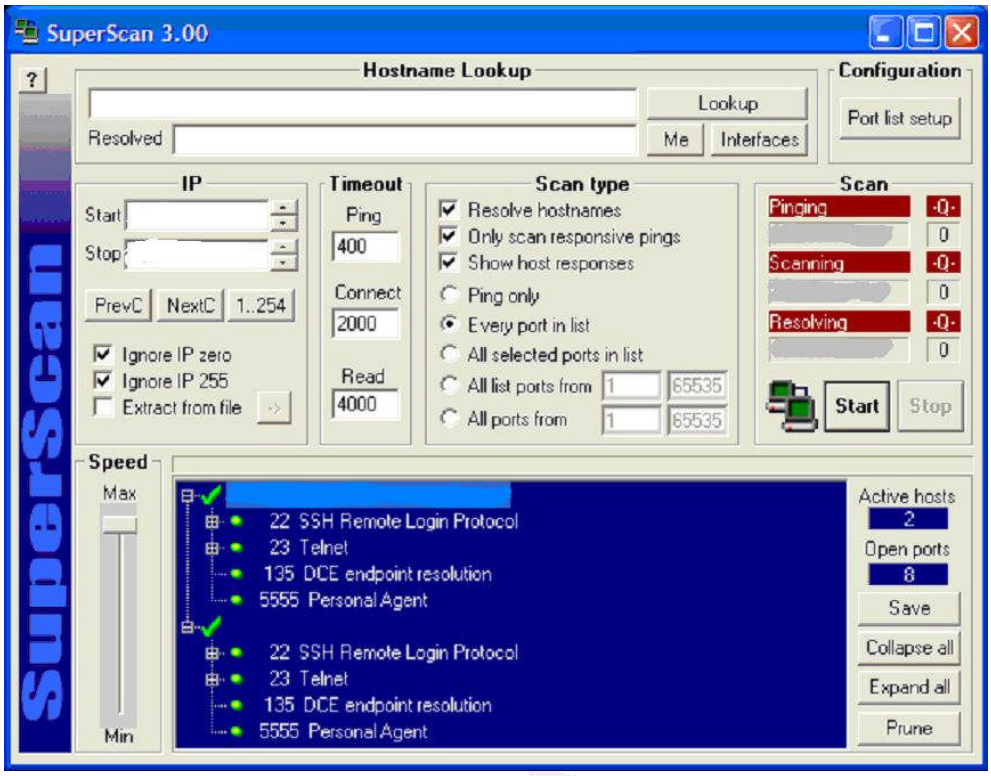
1. Alerting process did not exist therefore steps 2 & 3 could not be completed. Investigating this audit step, it was observed that a privileged powerbroker account was left logged onto the Console for an excessive time period (overnight, totally +11 hours). Further evidence that no alert notification process exist.

Evidence of console logged on for excessive period of time:

```
# date
Fri Sep 26 09:23:52 CDT 2003
# wc -l /etc/passwd
219 /etc/passwd
# w
  9:24am  up 14:44,  3 users,  load average: 0.00, 0.01, 0.01
User     tty           login@  idle   JCPU   PCPU  what
dannyr   console      10:07pm  5:12                 pbrun ksh
mjohnson pts/0         8:54am                      pbrun ksh
root     ttyp2         8:54am                      w
#
```

16. Test: Verify SRP system is sufficiently secured based on requirements	Analysis: Objective Stimulus / Response
Control Objective: System is appropriately hardened to meet the security level requirements	
Risk: Loss of confidentiality, integrity and availability due to exploitation of the system, such as an attacker compromising the system by exploiting vulnerability in a non-essential service or exploits a misconfigured system, allowing inappropriate access to systems and applications protected by SRP.	
Reference: • Garfinkel, p.831-833	
Procedure: 1. Auditor will run port scanner against SRP server to determine what services are running. 2. Review the output for any non-essential services running.	
Compliance: Test passes if output from port scanner indicates no inappropriate services are running. **FAILED**	
Comments: 1. Auditor ran the SuperScan port scanner.	

Screenshot of enabled services on SRP:



Note: Server IP addresses and host names have been removed from the image.

2. System is not appropriately hardened to meet the security level requirements. At the time of the audit, it was observed that unnecessary services were enabled (Telnet and Personal Agent).

17. Test: Verify that appropriate mitigating controls are applied for Apache web server as they apply to the SRP configuration.	Analysis: Objective
Control Objective: Applicable Apache web server vendor security announcements including patch releases are reviewed and acted upon in timely fashion.	
Risk: Attacker compromises a system by exploiting Apache web server vulnerability(s). This could allow an attacker to conduct a sql-injection attack or other known exploits.	
Reference: • SRP Blueprint document. • IT Resource Center Technical Knowledge Base	

(http://www1.itrc.hp.com/service/cki/search.do?category=c0&mode=text&searchString=apache+security&searchCrit=allwords&docType=Security&docType=Patch&docType=EngineerNotes&docType=BugReports&docType=Hardware&docType=ReferenceMaterials&docType=ThirdParty&search.x=11&search.y=13)

Procedure:

1. Ask system administrator how they track Apache web server vulnerability announcements (such as bugtraq, vendor notification lists, vendor website).
2. Review recent vulnerability notifications and select sample that apply to this configuration
3. Review change control documentation for existence of application of mitigating control (such as a patch or manual configuration change to mitigate risk).
4. View system information for existence of patches applied.

Compliance:

Test passes if SRP configuration has appropriate mitigating controls applied to the SRP system based on Apache vulnerability announcements and recommendations for remediation (i.e. patch installation or manual remediation as documented by vendor) have been performed.

FAILED

Comments:

1. Web and system administrators receive notification and track vulnerabilities through Apache. HP is the vendor for the Apache bundle and there are processes established for notification, applicability of patch to the environment, testing and installation of patches. There are dedicated security resources that manage this process with the operations team.
2. Auditor reviewed published Apache vulnerabilities. HTTP Trace (Reference HPSBUX0309-279, http://cirrus.cxo.cpqcorp.net/ssrt/securitybulletins/2003/SSRT3515.txt) was found to be vulnerability with Apache 1.3.27. There is no published patch for this vulnerability however a manual process is documented. The manual process to resolve this is to disable HPPT Trace with the following mod_rewrite syntax in the Apache server's httpd.conf file:

   ```
   RewriteEngine On
   RewriteCond %{REQUEST_METHOD} ^TRACE
   RewriteRule .* - [F]
   ```

3. There were no changes documented for the SRP.
4. Viewing the system showed that HTTP Trace vulnerability was not mitigated:

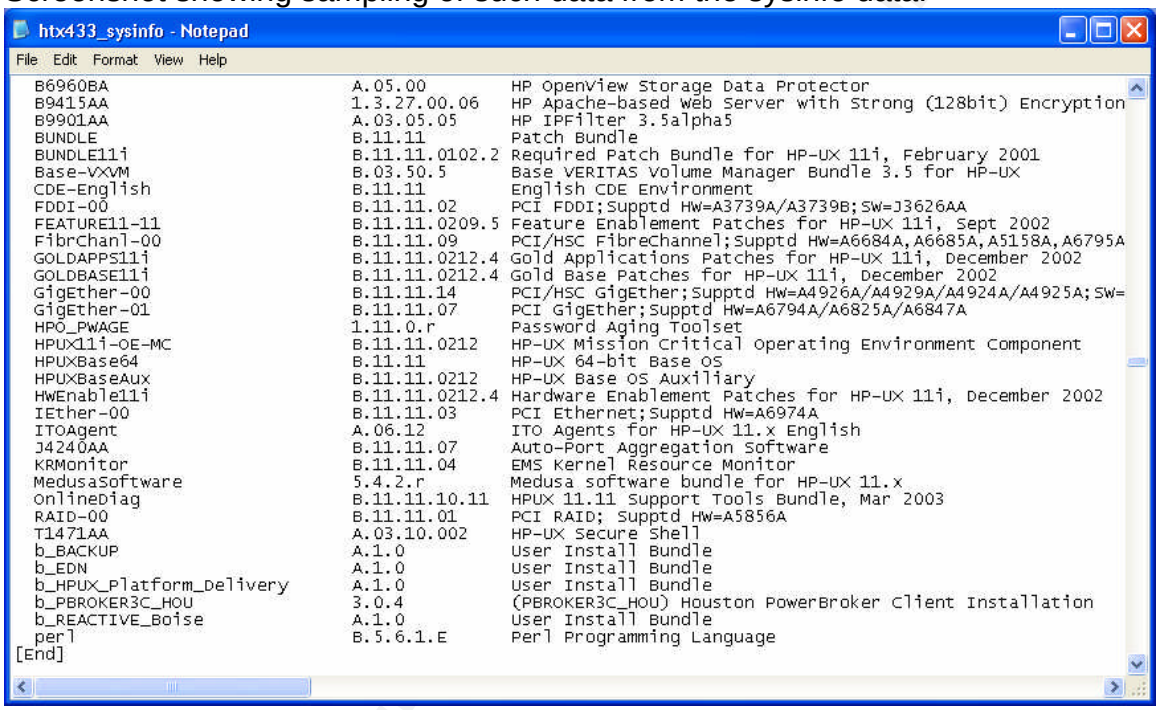
```
htx433:/opt/apache/conf $ grep –i trac /httpd.conf
LoadModule usertrack_module   libexec/mod_usertrack.so
AddModule mod_usertrack.c
htx433:/opt/apache/conf $
```

18. Test: Verify that appropriate mitigating controls are applied for HP-UX 11.11 as they apply to the SRP configuration.	Analysis: Objective
Control Objective: Applicable HP-UX 11.11 security announcements including patch releases are reviewed and acted upon in timely fashion.	
Risk: Attacker compromises a system by exploiting platform/OS vulnerability(s).	
Reference: • SRP Blueprint document • Garfinkel, p.819-840	
Procedure: 1. Ask system administrator how they track specific HP-UX vulnerability announcements (such as bugtraq, vendor notification lists, vendor website). 2. Review recent vulnerability notifications and select sample that apply to this configuration 3. Review change control documentation for existence of application of mitigating control (such as a patch or manual configuration change to mitigate risk). 4. View system information for existence of patches applied.	
Compliance: Test passes if SRP configuration has appropriate mitigating controls applied to the SRP system based on HP-UX vulnerability announcements and recommendations for remediation (i.e. patch installation) have been performed. **FAILED**	
Comments: 1. System administrators receive notification and track vulnerabilities through the vendor, HP. There are processes established for notification, applicability of patch to the environment, testing and installation of patches. There are dedicated security resources that manage this process with the operations team. 2. Auditor reviewed current vulnerabilities to HP-UX 11.11. One such vulnerability is to the DCE service which was found to be enabled on the	

server (Reference HPSBUX0309-276, http://cirrus.cxo.cpqcorp.net/ssrt/securitybulletins/2003/R2SSRT3620UX.txt). The resolution is to apply patch PHNE_28895 and then libcma.1 and libcma.2.

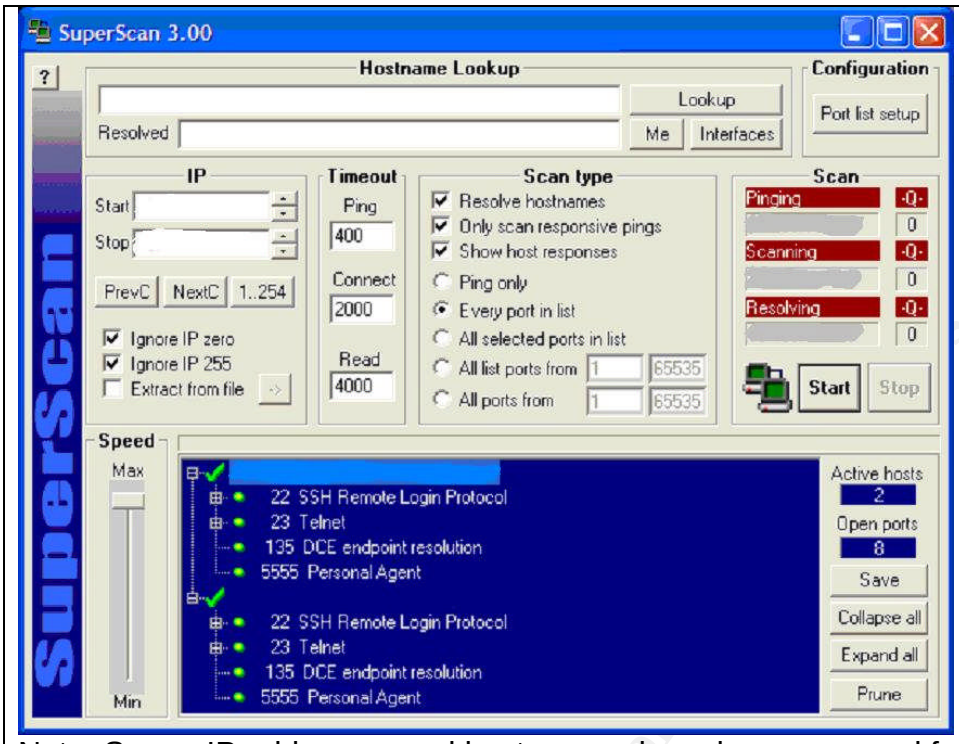
3. Change control documentation did not exist yet for the SRP due to the pilot state of the server.
4. The system administrator used the Medusa tool and 'gather sysinfo' script to show the current patches applied to the SRP server.

Screenshot showing sampling of such data from the sysinfo data:



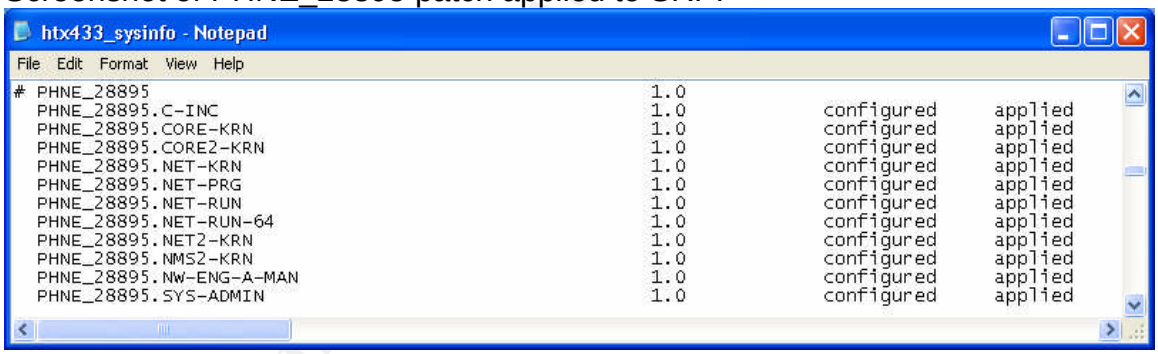
Although critical patches were applied, the audit discovered that DCE was enabled and patch PHNE_28895 was observed to be applied however there was no evidence that libcma.1 and libcma.2 were applied, which is the resolution/risk mitigation control for the DCE vulnerability listed in Section 1.5.5.

Screenshot of DCE enabled:



Note: Server IP addresses and host names have been removed from the image.

Screenshot of PHNE_28895 patch applied to SRP:



Note: no evidence that libcma.1 and libcma.2 was applied.

19. Test: Verify the current version of product (HP-UX 11.11 and Apache Web Server 1.3.x) is supported by vendor.	Analysis: Objective
Control Objective: Appropriate vendor support is available for the current version of product.	
Risk: Compromise to availability of data due to no vendor support for product. In addition, if new vulnerabilities are discovered, no commitment from vendor to provide security patch to vulnerability.	

Reference:

- HP-UX (http://www.hp.com/products1/unix/operating/infolibrary/)
- Apache HP Bundle (http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B9415AA132702)

Procedure:

1. Check current versions of product used.
2. Validate that these versions are supported by vendor by reviewing vendor website.

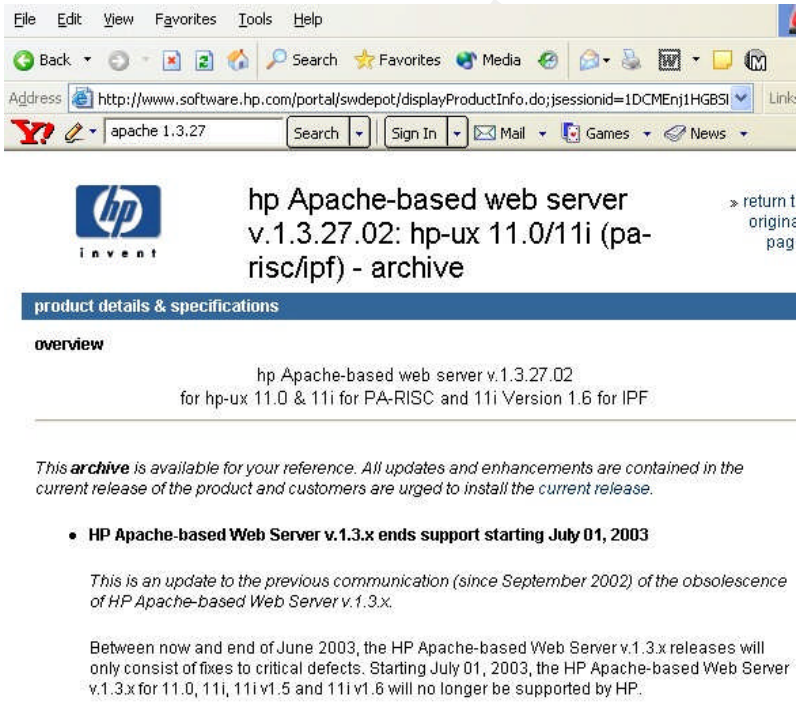
Compliance:
Test passes if vendor website indicates support of current product(s) used.

FAILED

Comments:

1. Current versions are HP-UX 11.11 and HP-Apache-based Web Server 1.3.27 bundle.
2. Current version of HP-UX is supported. Current version of HP-Apache-based Web bundle was found to be end-of-life, effective July 2003.

Screenshot from vendor website:



3.2 Residual Risk

Residual risk is measured by determining the exposure to risk, determining the controls necessary to reduce or eliminate the risk and then evaluating the risk remaining and making recommendations to reduce the residual risk.

The following table summarizes the audit results and rates the exposure to risk. The risk ratings are classified as follows:

> **High** vulnerabilities and risks pose an immediate threat to the information security and must be addressed before SRP goes into production.
>
> **Medium** vulnerabilities and risks must be addressed promptly (before, or within one month after production) and pose threats to the information security.
>
> **Low** vulnerabilities and risks are issues that do not pose an immediate or critical threat, but should be addressed as soon as practical.
>
> **None** indicates that there is no applicable risk.

Table 6: Audit Tests, Findings and Exposure to Risk:

Checklist Item	Risk Rating	Pass	Fail
Test #1: Determine the data integrity, system availability and confidentiality requirements of the SRP.	None	✓	
Test #2: Technical documentation exists and is properly implemented.	Low		✗
Test #3: SRP configuration change control process is documented and changes are implemented as documented.	Low		✗
Test #4: SRP system administrative procedures exist and are followed.	None	✓	
Test #5: Documentation exists for least privilege and auditor observes this control.	None	✓	
Test #7: View all system accounts and validate accounts are either associated with a unique individual or are locked and associated with a system daemon (e.g. daemon, bin, sys).	None	✓	

Test #8: SRP administrative access controls exist and are properly implemented.	None	✓	
Test #9: Demonstrate appropriate remote access security.	High		✓
Test #14: Test passes if system administrator can show that monitoring occurs for relevant security events.	High		✓
Test #15: Determine if alerting exists for relevant security events and test alerting process by generating a security event.	High		✓
Test #16: Verify SRP system is sufficiently secured based on requirements	High		✓
Test #17: Verify that appropriate mitigating controls are applied for Apache web server as they apply to the SRP configuration.	Medium		✓
Test #18: Verify that appropriate mitigating controls are applied for HP-UX 11.11 as they apply to the SRP configuration.	Medium		✓
Test #19: Verify the current version of product (HP-UX 11.11 and Apache Web Server 1.3.x) is supported by vendor.	High		✓

The business requires that the SRP servers, which are Internet-facing, be sufficiently secured to mitigate the risk of a compromise which could result in loss of confidentiality, integrity and availability of data. The data the SRP is protecting is labeled confidential and has defined data protection requirements including system availability and data integrity (see checklist item #1).

It was discovered during the audit that the SRP did not meet several control objectives that would prevent the SRP from going into production. The high and medium risks include;

- remote access to SRP not appropriately secured (checklist item #9),
- monitoring and alerting did not exist (checklist item #14 $ 15),
- SRP not appropriately hardened to meet the security level requirements (checklist item #16),
- appropriate mitigating controls, such as vendor security patches, are applied for Apache web server 1.3.27 in a timely fashion (checklist item #17),

- appropriate mitigating controls, such as vendor security patches, are applied to the HP-UX 11.11 operating system (checklist item #18),
- appropriate vendor support is not available (checklist item #19).

Mitigation of high and medium risks includes;

- disable Telnet, FTP and enable SSH (checklist item #9),
- complete configuration of SRP servers in VSM tool for monitoring or security relevant events (checklist item #14)
- establish alerting process (checklist item #15),
- disable unnecessary services, including Telnet and Personal Agent (checklist item #16),
- establish patch management process tied into the change control process. Train system administrators in process. Include a periodic review of system to ensure system administrators are following the process (checklist item #17 & #18),
- migrate to supported version of Apache v2.0.

Costs of these mitigation recommendations are included in Section 4.4: Audit Recommendations, Costs and Compensating Controls.

In the SRP current implementation state, the control objectives were not achieved. Compromise to the SRP could occur. This could result in loss of confidentiality, data integrity as well as system availability further resulting in a "measurable impact on the organization's missions, functions, image or reputation"[x], as defined by SANS.

3.3 System Auditability

The SRP is currently in a pre-production state of the system development life cycle and is not currently auditable. Several control objectives were not implemented at the time of this audit as a result. The system should be re-audited using this checklist at a time when the system is production-ready but before production implementation.

Assignment 4 – Audit Report

4.1 Executive Summary

The primary objective was to audit the Secure Reverse Proxy (SRP), evaluate risk and recommend mitigating controls. As part of this audit it was important to first understand the function of the Secure Reverse Proxy (SRP) in this large-scale enterprise environment. Then to gain knowledge of the configuration details of the SRP, identify the threats and vulnerabilities that pertain to this configuration and, based on this information, create an audit checklist. Finally, the audit was conducted to identify any existing vulnerabilities that have not been appropriately mitigated and to make recommendations to the business and system owner to remediate the findings.

It was advantageous to conduct the audit in its current state and provide this feedback to management and the support personnel so that the mitigating controls can be addressed before production implementation, thereby reducing the risk to an acceptable level.

At the time of this audit the likelihood of a security event occurring to the SRP in its current configuration is 'medium'. This rating takes into account the findings listed below and ability to exploit the vulnerability related to the finding (reference Section 1.5.3 and 1.5.5). If no remediation steps are taken before the SRP is implemented in production, there is a risk that the business could experience loss of confidentiality, data integrity and system availability. This can potentially lead to loss of brand image - the highest value to the corporation.

The cost and time to implement the remediation recommendations listed below will require little-to-no cost for all findings except the recommendation to upgrade to Apache v2. The recommendation is based on three factors:

1. Likelihood of a security event occurring,
2. Cost to the business as a result of such an event, and
3. Cost to proactively remediate the findings.

Therefore, the auditor recommends that the remediation steps found in Section 4.4: Audit Recommendations, Costs and Compensating Controls be completed before the SRP is put into production and business confidential data is made available.

4.2 Audit Background and Findings

1. Remote access to SRP is not appropriately secured (see checklist item #9). Secure remote access to the SRP is critical to prevent unauthorized access to the SRP and the applications it is protecting. Enabling telnet

can allow a hacker to compromise a system by learning the username and password from sniffing the network. FTP could allow anonymous access to the server.

The configuration of the SRP showed that Telnet and FTP were enabled. The interview led to the discovery that telnet is enabled in order to administer the application until keys are distributed for Secure Shell (SSH) "Telnet is a protocol for communicating between a client and a host. All telnet traffic, by default is sent across the network in clear text, including username and password."[xi] A hacker using a network sniffer could learn the username and password and gain access to the server. In addition, some system vulnerabilities require the use of Telnet to be exploited - such as the UNIX shell redirection race condition vulnerability.

2. Monitoring of services and events with notification did not exist (see checklist item #14 & #15). Monitoring of services and events with notification is critical for key Internet-facing servers used in an enterprise environment. As a result this finding, monitoring and alerting of significant security events would not occur. As a result, an attacker compromise to an improperly maintained system could occur undetected. Based on concepts from Winn Schwartau (2001) "Time-Based Security"[xii], the fortress can no longer be trusted to protect the system from an attacker. The worst case scenario should be considered. The worst case assumes that there is zero-time when the environment is secure. Therefore, the defense of the SRP should be based upon how fast it can detect and alert of an attacker or intrusion attempt. With this concept, the importance of monitoring of services and events with notification is vital in reducing risk. In addition, the example of a privileged user logged onto the console for an excessive period of time presents a risk through the unattended session.

   Although documentation exists for the installation and configuration of the SRP, including the configuration of Medusa for logging security events to a central repository, the central repository was not configured to receive these events from the SRP servers. In an enterprise environment, monitoring systems through a central security management system and timely alerts to server managers is essential. It was also observed that a privileged account was left logged onto the Console for an excessive time period (overnight, totally +11 hours).

3. System is not appropriately hardened to meet the security level requirements (see checklist item #16). Appropriately hardening the SRP servers is critical as these servers are Internet-facing and provide access to confidential data. At the time of the audit, it was observed that unnecessary services were running (Telnet and Personal Agent).

a. Personal Agent enabled on port 5555 (aka rplay or Real Player): there is a known TCP Trojan called "ServeMe"[xiii] available for that port.
b. Telnet enabled: All telnet traffic, by default is sent across the network in clear text, including username and password. A hacker could sniff the network, learn username and password combinations and gain unauthorized access to the SRP server.

4. Applicable vendor security announcements including patch releases are not always reviewed and acted upon in timely fashion (see checklist item #17 & #18). It is essential to ensure that vulnerabilities are mitigated in a timely fashion. It was observed that sampling of security patches were installed on the SRP, however the DCE vulnerability was discovered that did not appear to be mitigated. DCE was observed to be enabled, patch PHNE_28895 was observed to be applied however there was no evidence that libcma.1 and libcma.2 were applied, which is the resolution/risk mitigation control for the DCE vulnerability. It was further observed that HTTP Trace was not disabled.

5. Appropriate vendor support is not available (see checklist item #19). This may affect system availability of the SRP and data availability from the application data the SRP is serving to the businesses, partner or customers. At the time of the audit the SRP was running HP-Apache-based Web Server 1.3.27 bundle and this version was found to be end of life, effective July 01, 2003.

4.3 Risk Related to the Findings

All of the findings listed in Section 4.2: Audit Background and Findings can allow an attacker to compromise the SRP system and the applications it is protecting. This could cause negative impact to the business by loss of brand image resulting in loss of customer confidence. This can directly impact sales wins and stock price. Therefore, it is the auditor's recommendation that the remediation identified in Section 4.4: Audit Recommendations, Costs and Compensating Controls be executed before the SRP is implemented in production.

4.4 Audit Recommendations, Costs and Compensating Controls

4.4.1 Overarching observation and recommendation:

This is the first instance of SRP in production for this enterprise based on the documented SRP blue print. In addition, the process for hardening the operating system is recently transitioned to the support team for the SRP.

Due to these two factors, several security risks were discovered that might not otherwise exist in a more mature production process and in a better-developed support organization providing support for system hardening. As a result of this, the auditor recommends overall system administration and server hardening training based on documented procedures (Items #1, 2, 4, 5, 6, 7, 8 and 9). In addition, cross training of the system administrators with the pre-existing support administrator team is highly recommended.

Costs of such training would include system administrator time to participate in training and pre-existing support administrator time to conduct cross training. This training should be conducted as new members join the support administrator team and periodic refresher training should be conducted for all existing members.

4.4.2 Secure remote access:

Properly secure remote access to SRP (Item #9). Use of Secure Shell (SSH) is recommended for remote access and telnet should be disabled (Item #9). "SSH utilizes cryptography for authentication and provides protection from IP and DNS spoofing, as well as source routing attacks while allowing for a wide variety of user authentication schemes including SSH allows a wide variety of user authentication schemes including rhosts, RSA symmetric key exchange, Kerberos and others".[xiv] Another feature of SSH is its ability to perform port forwarding. Using this feature, a service that sends data across the network in the clear can now be sent encrypted.

This recommendation will not add additional cost as SSH is provided on HP-UX at no cost. In addition, enterprise security standard requires SSH and disablement of telnet.

4.4.3 Monitoring of services and events with notification:

Enable monitoring of services and events with notification (Item #14 & #15). The recommendation is to complete the logging and monitoring configuration of the SRP servers by configuring the servers to send reports to the central database that the VSM tool accesses. Also, adding the servers to HP's Virtual Central Computer Management system used by the enterprise to centrally monitor the configuration of HP-UX servers is recommended. Further, HP OpenView (http://www.openview.hp.com/) could also be configured for monitoring security events and sending alerts (aka 'traps) via email, paging system or alerting systems. To reduce the risk of unattended sessions (i.e. failure of a user to log off the system), training should be given to the system administrators on the documented security policy and standards that prohibit this, encourage the use of the lock function of UNIX to suspend the session and password protect it, or

automate a process to terminate a session if a user takes no action for a time interval specified by the system manager or by security.

The recommendation for monitoring will not add additional cost as the SRP is part of the enterprise environment and such controls (i.e. centralized monitoring of security events) are already established and used. Establishing an appropriate notification process for these servers could be established with minimal costs and time through the use of HP Openview. This would sufficiently mitigate the risk identified. It is noted that the SRP servers are part of an enterprise environment and an appropriate notification and alerting process should be established for the enterprise, requiring additional time, resources and funding. Symantec's Enterprise Security Manager (http://enterprisesecurity.symantec.com) is already implemented in the Microsoft Window's environment and could be extended in the enterprise to include HP-UX. Leveraging the enterprise license would primarily only cost the company the additional resources to manage the notifications and alerts.

Training of the system administrators on security policy and standards will require a small amount of resource time. These documents are published online and can be viewed by the system administrators as time permits. This should also be documented in the system administrator's responsibilities and measured against during performance reviews.

4.4.4 Server hardening:

Appropriately hardening the SRP servers (Item #16) is critical as these servers are Internet-facing and provide access to confidential data. The recommendation is to disable all unnecessary services on the SRP servers, including Telnet and Personal Agent. With change control management (Item #3) and monitoring established on these servers (Item #14) such changes in the configuration of the SRP (such as enabling a service) will be controlled to ensure that unnecessary services are not enabled.

This recommendation will not add additional cost, as the SRP is part of an enterprise environment and such controls (i.e. change control management and centralized monitoring) are already established and used throughout the enterprise.

4.4.5 Vendor patch application:

Applicable vendor security announcements including patch releases are reviewed and acted upon in timely fashion (Item #17 & #18) is critical to ensure vulnerabilities are mitigated to reduce or remove risk. Recommend that the established process for patch management be followed that includes a periodic review conducted to ensure system administrators are following the process.

The recommendation will not add additional cost, as the patch management process is established in this enterprise and includes monitoring and reviewing of security patches.

4.4.6 Vendor support:

Appropriate vendor support for the current version of product (Item #19) is critical to system availability of the SRP and data availability from the application data the SRP is serving to the businesses, partner or customers. The recommendation is to migrate to a supported version of Apache.

This recommendation will add additional cost for Apache web server upgrade. It could require newer hardware, additional support and maintenance costs and time to test with all dependent infrastructure components (e.g. SiteMinder). It should be noted that the test for this audit was conducted in a production-pilot environment. The solution architect informed the auditor that their plans were to complete the upgrade of SiteMinder 5.5 and then upgrade Apache to v2 before entering full, global production. This upgrade would not require additional funds for hardware and licenses for Apache v2 were already purchased by the sponsor. The only cost would be for internal resources to upgrade the existing pilot environment after SiteMinder 5.5 became available.

Some research was conducted on Apache v2.0. The following table illustrates the published known vulnerabilities to-date, including threats, risk and controls for Apache v2.0. It is recommended that the controls for resolution be applied when v.2 is installed.

Table 7: Known vulnerabilities, threats, risk and controls for Apache v2.0:

Vulnerabilities for Apache on HP-UX	Threat	Risk Level	Controls for Resolution / Mitigation
Apache web server prefork MPM denial of service vulnerability Ref 1: bugtraq 8137 (www.securityfocus.com/bid/8137) Ref 2: cve CAN-2003-0253 Ref 3: HPSBUX0309-278	Vulnerability in the prefork MPM (multi-processing module) that could result in a temporary DoS condition. No known exploits	Medium	Apply patch specified in HPSBUX0309-278.
Apache web server	Issue may occur when	Medium	Apply

sslciphersuite weak ciphersuite renegotiation weakness Ref 1: bugtraq 8134 (www.securityfocus.com/bid/8134) Ref 2: cve CAN-2003-0192 Ref 3: HPSBUX0309-278	sslciphersuite directive is used to upgrade a ciphersuite. Particular sequences of per-directory renegotiations may cause this condition to occur, resulting in a weaker ciphersuite being used in place of the upgraded one. No known exploits		patch specified in HPSBUX0309-278.

APPENDIX A:
HP-UX 11i System Security Features and Benefits[xv]

hp-ux 11i system security features and benefits

hp-ux secure shell	• encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks • provides a myriad of secure tunneling capabilities • protects a variety of authentication methods • secure remote logins • secure file transfer • secure remote commands execution • authenticate users using keys and agents • access control • port forwarding (tunneling)
hp-ux bastille	• answer security questions • answer usability questions • lock-down appropriate to hp-ux server use • produce a profile script • use the script to harden many servers in the same category
stack buffer overflow protection	• uses a combination of highly efficient software and existing memory management hardware to protect against both known and unknown stack buffer overflow attacks. Eliminates need to modify a program's code to get stack buffer overflow protection, unlike other products that require time-consuming program modifications, recompilation or relinking • provides a "trial mode" that can be used to gain confidence that it will not interfere with legitimate applications • provides a "zone bypass" feature that allows application owners to mark their binaries as having a legitimate need to execute code located on their stack(s) • programs so marked are exempt from the HP-UX stack buffer overflow protection
security_patch_check	• Perl script that performs analysis of file sets and patches installed on an HP-UX machine and generates a report of recommended security patches
access control list (ACL)	• stores a series of entries that identify specific users or groups and their access privileges for a directory or file • specifies detailed access permissions for multiple users and groups • supports Journaled File System (JFS 3.3)
generic security services application programming interface (GSS API)	• contains all the GSS APIs in RFC 2743 and is implemented as C programming language interfaces • provides security services for client/server applications independent of various underlying security mechanisms and communication protocols, including authentication, integrity and confidentiality services • enables application developers writing secure applications to write code only once, eliminating need to change it whenever the underlying security mechanism changes
sendmail-8.9.3	• uses the first sendmail release to include anti-spam rule sets, which give mail administrators significantly more

hp-ux 11i network security features and benefits

hp-ux IPSec	• provides secure and private communication over the Internet and within the enterprise-without modifying existing applications • incorporates Internet Key Exchange (IKE) as an automated protocol for dynamically negotiating the IPSec parameters. IKE provides dynamic secret key generation and exchange for IPSec and allows for scalability • interoperates with over 25 other IPSec implementations, including those of Cisco Systems and Microsoft®
hp-ux IPFilter	• a stateful inspection host-based firewall system that provides filtering of selected IP traffic and streaming UDP protocols into or out of the system
hp-ux Kerberos server	• provides key distribution facilities to implement the Kerberos authentication protocol in network-distributed enterprises • provides strong authentication for client/server applications by using secret-key cryptography • enables encryption of all communications to assure privacy and data integrity • provides the foundation for secure single sign-on to applications and multi-platform resources
hp-ux AAA server	• provides authentication, authorization and accounting services using the RADIUS protocol • enables service providers or enterprises to authenticate users and then account for time and billing use of network services • supports EAP (Extensible Authentication Protocol) for Wireless LAN Security
pluggable authentication modules (PAM)	• industry-standard authentication framework gives system administrators the flexibility to choose any authentication service available on the system • allows new authentication service modules to be plugged in and made available without modifying the applications
BIND9.2.0	• provides data integrity and authentication to applications using cryptographic digital signature • prevents non-authorized access to DNS and prevents name-to-address mapping tampering over the wire • restricts DHCP updates to those authorized to perform them • guarantees the integrity of zone data using digital signatures

References

1. Auditing the Perimeter: Firewalls, Border Routers, VPNs and Perimeters (2003). SANS GSNA Courseware.
2. Bahadur, Gary and Shema, Mike (April 2001). Features of Web Server. *Improving Apache*. InfoSecurity Magazine, retrieved August 2003 from the World Wide Web: http://infosecuritymag.techtarget.com/articles/april01/features1_web_server_sec.shtml
3. Chun, Jon (February 2002). Application-Level Reverse Proxies and VPNs: *A Brief Technical Discussion*. Safe Web. Retrieved August 2003 from the World Wide Web: www.safeweb.com/pr_infosec.html.
4. Dayton, Doug (1997). Information Technology Audit Handbook. New Jersey: Prentice Hall.
5. Features of HP-UX Web Server Suite. HP. Retrieved August 2003 from the World Wide Web http://www.hp.com/products1/unix/webservers/apache/.
6. Garfinkel & Spafford (1996). Practical Unix & Internet Security. Cambridge, MA: O'Reilly & Associates, Inc.
7. HP Apache-based Web Server v.1.3.27.02: HP-UX 11.0/11i (pa-risc/ipf). HP. Retrieved August 2003 from the World Wide Web: http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B9415AA132702
8. HP-UX Information Library. HP. Retrieved August 2003 from the World Wide Wed: http://www.hp.com/products1/unix/operating/infolibrary/
9. Kaplan, Jim (August 2002). Disaster Recovery Business Continuity Audits. Retrieved August 2003 from the World Wide Web: http://www.auditnet.org/drp.htm
10. Key features of PowerBroker. Symark. Retrieved August 2003 from the World Wide Web: http://www.symark.com/powerbroker.htm
11. SANS Top Vulnerabilities 2003. SANS. Retrieved August 2003 from the World Wide Web: http://www.sans.org/top20/
12. Schwartau, Winn (2001). Time-Based Security. Retrieved October 2003 from the World Wide Web: http://www.chi-publishing.com/portal/backissues/pdfs/ISB_2001/ISB0610/ISB0610WS.pdf.
13. Summers, Rita (1997). Secure Computing: Threats and Safeguards. New York:McGraw-Hill
14. TCP/IP Port Numbers. Delamere Services. Retrieved August 2003 from the World Wide Web: http://www.delamereservices.co.uk/ports3501to7000%5B1%5D.html
15. Technical Knowledge Base. IT Resource Center. Retrieved August 2003 from the World Wide Web: http://www2.itrc.hp.com/

16. Tipton, H. & Ruthberg, Z. (1993). Handbook of Information Security. New York: Auerbach Publications.
17. Van der Walt, Charl (July 30, 2002). Assessing Internet Security Risk. Security Focus. Retrieved August 2003 from the World Wide Web: http://www.securityfocus.com/infocus/1612
18. Wong, Chris (2002). HP-UX 11i Security. New Jersey: Prentice Hall. Also available and referenced during August 2003 from World Wide Web: http://www.hp.com/products1/unix/operating/security/index.html

Endnotes

[i] Chun, Jon (February 2002). Application-Level Reverse Proxies and VPNs: *A Brief Technical Discussion*. Safe Web. Retrieved August 2003 from the World Wide Web: www.safeweb.com/pr_infosec.html. Note: SafeWeb, Inc was recently acquired by Symantec on Oct 15, 2003 and this link is likely to change in the near future.

[ii] Wong, Chris (2002). HP-UX 11i Security. New Jersey: Prentice Hall. Retrieved August 2003 from World Wide Web: http://www.hp.com/products1/unix/operating/security/index.html.

[iii] Features of HP-UX Web Server Suite. HP. Retrieved August 2003 from the World Wide Web http://www.hp.com/products1/unix/webservers/apache/.

[iv] HP Apache-based Web Server v.1.3.27.02: HP-UX 11.0/11i (pa-risc/ipf). HP. Retrieved August 2003 from the World Wide Web: http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B9415AA132702

[v] SANS Top Vulnerabilities 2003. SANS. Retrieved August 2003 from the World Wide Web*:* http://www.sans.org/top20/

[vi] Bahadur, Gary and Shema, Mike (April 2001). Features of Web Server. *Improving Apache*. InfoSecurity Magazine, retrieved August 2003 from the World Wide Web: http://infosecuritymag.techtarget.com/articles/april01/features1_web_server_sec.shtml

[vii] Wong, Chris (2002). HP-UX 11i Security. New Jersey: Prentice Hall. Page 450.

[viii] Key features of PowerBroker. Symark*.* Retrieved August 2003 from the World Wide Web: http://www.symark.com/powerbroker.htm

[ix] Wong. *HP-UX 11i Security*. "Passwords, Users, and Groups", page 76.

[x] Auditing the Perimeter: Firewalls, Border Routers, VPNs and Perimeters (2003). SANS GSNA Courseware, page 156.

[xi] Wong, Chris (2002). HP-UX 11i Security. New Jersey: Prentice Hall. Page 269.

[xii] Schwartau, Winn (2001). Time-Based Security. Retrieved October 2003 from the World Wide Web: http://www.chi-publishing.com/portal/backissues/pdfs/ISB_2001/ISB0610/ISB0610WS.pdf

[xiii] TCP/IP Port Numbers. Delamere Services. Retrieved August 2003 from the World Wide Web: http://www.delamereservices.co.uk/ports3501to7000%5B1%5D.html

[xiv] Wong, Chris (2002). HP-UX 11i Security. New Jersey: Prentice Hall. Page 184.

[xv] Wong, Chris (2002). HP-UX 11i Security. "HP-UX 11i System Security Features and Benefits". Retrieved August 2003 from World Wide Web: http://www.hp.com/products1/unix/operating/security/index.html