IT Audit:
Security Beyond the Checklist

Copyright SANS Institute

Author Retains Full Rights

This paper is from the SANS IT Audit site. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"20 Critical Security Controls: Planning, Implementing and Auditing (SEC440)"
at http://it-audit.sans.orghttp://it-audit.sans.org/events/

Security Audit of an HP-UX 11i Server: An Auditor's Perspective

A practical submitted in pursuit of the
GIAC Systems and Network Auditor Certification
GSNA Practical version 2.1, Option 1

Prepared by: Timothy D. O'Brien

Submitted on: September 19, 2003

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table of Contents

1 Introduction and Research in Audit, Measurement Practice, and Control.....5
1.1 Abstract/Summary.....5
1.2 Description of audit target.....5
1.3 Scope of the audit.....5
1.3.1 Scope Description.....5
1.3.2 Exclusions from scope.....6
1.4 Risk Evaluation.....6
1.4.1 Assets to be protected.....6
1.4.2 Threats to the assets.....6
1.4.3 Risk = vulnerability + threat.....8
1.4.4 Goal of this audit.....9
1.5 Research on the current state of practice.....9
1.5.1 Internet resources relating to IT auditing and control.....9
1.5.2 Resources specifically relating to auditing HP-UX.....10
1.5.3 Current state of audit practice.....10
2 Audit Checklist.....12
2.1 Control Objective: Verify the system's network services are configured securely.....12
2.1.1 Checklist item #01: System time synchronization.....12
2.1.2 Checklist item #02: Unnecessary services being started.....14
2.1.3 Checklist item #03: Internet daemon logging.....16
2.1.4 Checklist item #04: Services brokered by the Internet daemon.....17
2.1.5 Checklist item #05: TCP Wrappers.....20
2.1.6 Checklist item #06: Internet daemon security file.....22
2.1.7 Checklist item #07: Secure Shell.....23
2.1.8 Checklist item #08: Trust relationships.....25
2.1.9 Checklist item #09: Sendmail configuration.....27
2.1.10 Checklist item #10: CDE access.....29
2.1.11 Checklist item #11: Banners.....30
2.1.12 Checklist item #12: Modems.....32
2.2 Control Objective: Verify that the system is patched regularly according to the company's patching strategy.....34
2.2.1 Checklist item #13: Security patches.....34
2.2.2 Checklist item #14: Operating system patches.....36
2.3 Control Objective: Verify that access to the system is properly controlled 38
2.3.1 Checklist item #15: Shadow Passwords.....38
2.3.2 Checklist item #16: Minimum password length.....39
2.3.3 Checklist item #17: Empty passwords.....41
2.3.4 Checklist item #18: Weak passwords.....42
2.3.5 Checklist item #19: Duplicate superuser accounts.....43
2.3.6 Checklist item #20: Root login restricted.....44
2.3.7 Checklist item #21: Unneeded system accounts.....45
2.3.8 Checklist item #22: PATH variable for root.....47

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.4 Control Objective: Verify that access and modification are properly controlled for sensitive files 48
2.4.1 Checklist item #23: Change Control 48
2.4.2 Checklist item #24: User directory security 49
2.4.3 Checklist item #25: Sticky bit on temporary directories 51
2.4.4 Checklist item #26: Root's home directory 53
2.4.5 Checklist item #27: Default umask 53
2.4.6 Checklist item #28: Global "chown" privileges 55
2.4.7 Checklist item #29: SUID/SGID files 56
2.4.8 Checklist item #30: File integrity software 59
2.4.9 Checklist item #31: Log file and configuration file permissions 61
2.4.10 Checklist item #32: Use of cron/at 63
2.4.11 Checklist item #33: Buffer overflow protection mechanism 66
2.4.12 Checklist item #34: Retirement of old media 67
2.5 Control Objective: Verify that the administrators are monitoring the system. 68
2.5.1 Checklist item #35: Root's mail must be read in a timely manner 68
2.5.2 Checklist item #36: System logs must be reviewed on a regular schedule 69
2.5.3 Checklist item #37: Regular vulnerability assessments 70
3 Audit Evidence 73
3.1 Execution of the audit 73
3.1.1 Audit Results Summary Table 73
3.1.2 Audit Results of Checklist item #02: Unnecessary services being started 75
3.1.3 Audit Results of Checklist item #04: Services brokered by the Internet daemon 80
3.1.4 Audit Results of Checklist item #05: TCP Wrappers 82
3.1.5 Audit Results of Checklist item #07: Secure Shell 84
3.1.6 Audit Results of Checklist item #11: Banners 85
3.1.7 Audit Results of Checklist item #13: Security patches 87
3.1.8 Audit Results of Checklist item #15: Shadow Passwords 88
3.1.9 Audit Results of Checklist item #17: Empty passwords 89
3.1.10 Audit Results of Checklist item #18: Weak passwords 90
3.1.11 Audit Results of Checklist item #20: Root login restricted 91
3.1.12 Audit Results of Checklist item #27: Default umask 93
3.1.13 Audit Results of Checklist item #28: Global "chown" privileges 94
3.1.14 Audit Results of Checklist item #30: File integrity software 95
3.1.15 Audit Results of Checklist item #34: Retirement of old media 96
3.1.16 Audit Results of Checklist item #35: Root's mail must be read in a timely manner 97
3.1.17 Audit Results of Checklist item #36: System logs must be reviewed on a regular schedule 98
3.2 Measurement of residual risk 99
3.2.1 Original risk 99
3.2.2 First steps toward remediation 100

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3.2.3 Risk remaining after remediation 101
3.2.4 Were the stated control objectives met? 102
3.2.5 Summary of residual risk 103
3.3 Evaluation of the audit 103
4 Audit Report 104
4.1 Executive Summary 104
4.2 Audit Findings 104
4.2.1 Findings for Objective: Verify the system's network services are configured securely 104
4.2.2 Findings for Objective: Verify that the system is patched regularly according to the company's patching strategy 105
4.2.3 Findings for Objective: Verify that access to the system is properly controlled 106
4.2.4 Findings for Objective: Verify that access and modification are properly controlled for sensitive files 107
4.2.5 Findings for Objective: Verify that administrators are monitoring the system 108
4.3 Audit Recommendations 109
4.4 Cost summary 110
4.5 Compensating controls 110
4.6 Summary 111
References 112

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1 Introduction and Research in Audit, Measurement Practice, and Control

1.1 Abstract/Summary

The goal of this paper is to communicate a method for performing an objective security audit of a production server running the HP-UX 11i operating system. This paper contains a checklist of important items to consider when auditing an operating system of this type, an analysis of the results of several checklist items from an actual audit, and a report of the findings from the audit.

1.2 Description of audit target

System Description: Hardware is an HP rp5470 running HP-UX 11i v1 with the operating system pre-installed at the factory.

Environment: The audit target is located in the datacenter of a small manufacturing company, XYZ Manufacturing (hereafter referred to as "XYZ Mfg." or "XYZ"). The system to be audited shares a local network with several Windows NT machines that provide e-mail, file storage, and printing services. Users connect to the system via various X-Windows packages from PCs in the shop and in offices around the plant. Operating system patches are said to be applied semi-annually through custom patch analyses provided by the company's support contract on this server.

Role: The audit target runs a heavily modified manufacturing/shop floor control package upon which the manufacturing plant depends. It also runs a second instance of the database used for testing and development.

Considerations: This system is not running in "Trusted Systems"[1] mode. With the small number of system administrators (two), security has come in behind other considerations. However, as unplanned downtime of this server results in the production floor reverting to manual processes for production and the filling and tracking of orders, this system is receiving increased scrutiny. With this in mind, XYZ's management selected this system as a starting point in a larger security effort.

1.3 Scope of the audit

1.3.1 Scope Description

The audit of this system will be limited to an examination of the operating system configuration for the target server only. Attention will not be paid to the systems and other devices that share the LAN with the audit target nor to auditing the actions of users once within the application. Supporting policies to which the IT department should conform will only be examined where they directly relate to operating system configuration (such as password composition).

[1] "Administering Your Trusted System"

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1.3.2 Exclusions from scope

There will be an assumption that the server resides within a controlled environment with no unauthorized physical access or modification to the server. Thus the audit will not include an evaluation of physical security or environmental concerns (water, electrical, geological, etc.).

Note: This paper describes the audit of an HP-UX server's operating system, with a simple definition of auditing being "measuring against a standard". As there is no existing benchmark showing an initial secure configuration for this system, this audit will be conducted using current "best practices" as discovered during the research phase of this project. There are many well-written and complete documents available on installing HP-UX securely and "locking down" existing installation of HP-UX. The goal of this paper is to audit an existing installation, not to change or secure it. Where appropriate, references may be provided for further study. The reader is strongly encouraged to research methods of addressing the concerns raised by this audit.

1.4 Risk Evaluation

This audit is a first step in a broader effort at XYZ Mfg. to develop a focus on security within their organization. The larger project will encompass audits of the NT systems, local PCs, corporate policies, etc. As XYZ views this server as critical, they are "starting from the inside and moving out" in evaluating this server first.

Given the role of this system within the organization as their sole database server and primary test/development platform, the risk to the company is severe should the server be rendered inoperable.

1.4.1 Assets to be protected

From a purely physical viewpoint, the asset to be protected is the rp5470 server itself. From a more business-minded perspective, the assets to be protected (within the scope of this audit) are:

- The integrity of the manufacturing and production data
- The integrity of both the operating system and the manufacturing software
- The availability of both the operating system and the manufacturing software

The server alone does the business little good if users and other systems cannot connect to it reliably and get accurate information.

1.4.2 Threats to the assets

A threat can be defined as "The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability."[2] In this definition we see that threats can be intentional or accidental, these "threat-sources" can also be classified as external or internal in origin.

[2] Stoneburner, p.12.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1.4.2.1 External Threat

What could go wrong? – Recent news articles have illustrated that while many companies place great faith in the firewalls they have purchased, the existence of a firewall does not preclude unauthorized access from the Internet[3]. Often, connections to business partners or other departments circumvent firewalls and other protective devices. Whether they are simply "joy riders" or malicious crackers, if unauthorized intruders from outside the company gained access to the audit target, they could use its resources for launching attacks on other hosts on the Internet, for storing possibly illegal content for retrieval by others, to browse for interesting information, or just to cause mischief.

How likely is it to happen? – In the initial data-gathering phase of this engagement, there were no indications that this system is "visible" from the Internet. The system is understood by management not to be running mail, web or FTP servers. Patches are not downloaded directly to this server and no web surfing is performed from here. Examination of external threats will not be ignored in this audit; however, given the environment, threats from within the company and network are considered more likely.

What are the consequences if it does go wrong? – If unauthorized intruders were to gain access to the system and damage data upon which the company depends, the results would be critical for XYZ Mfg. If not detected in time, the corrupted data could be backed-up as valid data and once discovered confidence in the data on tape would be lost.

1.4.2.2 Determined Insider

What could go wrong? – As the economy has gone through some difficulty, there have been several rounds of layoffs at XYZ in the past two years. This brings up the possibility that an employee could decide to damage the company by causing a disruption in the manufacturing/shop floor system. With access to the PCs on the shop floor, the determined insider could perform a "denial of service" attack on the audit target, or with more time to prepare could try to break out of the application menu on the server and attempt to cause data corruption.

How likely is it to happen? – Given XYZ's current workforce of older manufacturing workers and their experience in non-computer professions, it seems more likely that a disgruntled employee would take out his frustrations in more physical ways than to subtly attack the IT systems.

What are the consequences if it does go wrong? – In the previous paragraph, ***assumptions*** were made that could prove incorrect. If a determined insider had the experience (or a web browser and an desire to acquire the experience), he could attempt to corrupt data or perform a "denial of service" attack. With the dependence of XYZ Mfg. on this system, the consequences of a successful attack could range from light to severe impact.

[3] Poulsen

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

An example of “light impact” would be several hours of downtime and recovery time due to a denial of service attack. An example of “severe impact” would be several days of downtime, lost productivity, and man-hours to recover the server and verify the integrity of the existing data once restored. It is not likely that a determined insider has the ability to affect the quality of material being produced by corrupting the IT system, but it is possible that XYZ Mfg’s customer relations could be affected by delayed shipments to customers.

1.4.2.3 Untrained administration

What could go wrong? – There are two existing technical staff who are managing all IT-related needs including UNIX and NT system administration and support, printer management, database programming and support, network management and support, and “other duties as assigned”. Although, these administrators have performed admirably while learning-on-the-job, they have not received system administration training or system security training. Mistakes and oversights are bound to happen. A few examples of what could go wrong from a security perspective are that systems could be put into place without being locked down, vulnerable network services could be left on and accessible, and security events and other system events could go undetected due to lack of experience and time for proper monitoring.

How likely is it to happen? – Given the number and types of systems the IT staff is expected to administer, misconfigurations are likely. There is a probability that some systems will be configured to allow trust relationships that might be exploitable or network services will be left open due to lack of training on the administrator’s part.

What are the consequences if it does go wrong? – Consequences of misconfigurations would be the same as those in the “Determined Insider” section; downtime, lost productivity, and man-hours to recover the server and verify the integrity of the operating system, application software, and data.

With untrained administrators there is also the consequence that recovery may be hampered by lack of monitoring and/or recovery procedures. If the auditing system is misconfigured or not enabled, tracking what went wrong will be more difficult. If file integrity software is not being used, discovering what has changed will also be difficult.

1.4.3 Risk = vulnerability + threat

Risk assessment can be defined as, “an analysis of potential vulnerabilities and threats taken together to produce an overall picture of the potential for loss or harm to the organization.”[4] Given this definition, one goal of this audit is to identify controls that should be in place on the system to ensure its secure operation (control objectives) and to test those controls to determine their adequacy for the task.

[4] Hoelzer, p.2-23

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1.4.4 Goal of this audit

The primary goal of this audit is to verify that the control objectives for the system are being met. Those control objectives we would like to see on this system are:

- Verify the system's network services are securely configured
- Verify that the system is patched regularly according to company policies
- Verify that access to the system is properly controlled
- Verify that access and modification are properly controlled for sensitive files
- Verify that the administrators are monitoring the system

As noted in section 1.3.2 "Exclusions from scope" on page 6, the goal of this audit is to evaluate the security configuration of this server, not to secure it or "lock it down" (although that effort should certainly follow, if needed).

1.5 Research on the current state of practice

In preparing for this paper, many methods were used to discover the current state of practice for securing and auditing HP-UX. Search engines (primarily Google.com) were used extensively with search strings such as "hp-ux unix security auditing" and "hp-ux unix audit controls" to discover checklists, discussion groups, and other relevant information on the topic.

Resources abound on topics such as physical security auditing, detailed process accounting, and comprehensive policy review which, while interesting, are not within the scope of this project.

1.5.1 Internet resources relating to IT auditing and control

There are many useful sources of IT auditing information available on the Internet.

- Information Systems Audit and Control Association (ISACA http://www.isaca.org/) is a membership organization that provides research and standards publications to its membership of auditors.
- AuditNet (http://www.auditnet.org) is an excellent free resource for best practice documents, checklists, risk analysis worksheets, sample policies, and other information about a broad range of auditing topics (everything from financial accounting and inventory systems to physical security and corporate policies).
- CERT Coordination Center (http://www.cert.org/) is a federally funded research and development center operated by Carnegie Mellon University and is a well-respected source of security alerts and advisories.
- The Federal Computer Incident Response Center (FedCIRC http://www.fedcirc.gov/). Their website describes the organization as "a federal civilian government's trusted focal point for computer security incident reporting, providing assistance with incident prevention and response." They provide information and research on vulnerabilities.
- Computer Security Resource Center (CSRC http://csrc.nist.gov/) division of the National Institute of Standards and Technology contains a wealth of general security information, as well as checklists, security implementation guides for specific hardware, and special publications on security topics ranging from

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

wireless and e-mail security to firewall policies and PKI infrastructures. Specifically, the CSRC's "Special Publications" are good overviews of many technologies: http://csrc.nist.gov/publications/nistpubs/index.html.

- SANS Institute (http://www.sans.org/resources/) provides training, certification, and research to the security community. Their security projects are too numerous to list here, a short list includes:
  - SANS/FBI Top 20 Vulnerabilities List (http://www.sans.org/top20)
  - SANS Security Policy Samples (http://www.sans.org/resources/policies/)
  - Information Security Reading Room (http://www.sans.org/rr)
- No discussion of on-line resources would be complete without mention of the ICAT Metabase. It is a searchable database of vulnerabilities. It is also downloadable to allow the user more flexibility in searching. (http://icat.nist.gov/icat.cfm)

1.5.2 Resources specifically relating to auditing HP-UX

In addition to the general auditing and security resources listed above, the following are resources dealing specifically with auditing and securing HP-UX

- "Building a Bastion Host Using HP-UX 11". 08/2000. http://www.hp.com/products1/unix/operating/infolibrary/whitepapers/building_a_bastion_host.pdf
- "HP-UX 11i System Security White Paper". 05/2003. http://www.hp.com/products1/unix/operating/infolibrary/whitepapers/hpux11isecuritywp.pdf
- "HP-UX Checklist" retrieved on 08/10/2003 from http://www.auditnet.org/docs/HPUX.doc
- Bastille for HP-UX (http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6849AA)
- The Center for Internet Security's Level-1 Benchmark and Scoring Tool for HP-UX (http://www.cisecurity.org/bench_HPUX.html)
- Various HP-UX "security and manageability tools" (such as Bastille, SSH, Shadow Passwords, etc.) http://www.software.hp.com/ISS_products_list.html
- Wong, Chris. HP-UX 11i Security. New Jersey: Prentice Hall PTR, 2002

1.5.3 Current state of audit practice

As HP-UX is a mature operating system, there are many documents that can be used to install HP-UX securely. The above-mentioned "Bastille for HP-UX" and "The Center for Internet Security's Scoring Tool" can also be used to verify the system is locked down after installation.

There are many standards and methodologies for conducting IT audits and expressing management and control concerns. Three of the more popular include:

- COBIT: Control Objectives for Information and related Technology is a framework used by organizations around the world to manage IT processes. It contains principles and guidelines for management and for auditors.
- Time Based Security: A popular security model based on the premise that "The amount of time offered by the Protection device or system must be greater than

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

the amount of time it takes to detect the attack plus the amount of time it takes to react to the detection."[5]

- ITIL: Information Technology Infrastructure Library[6] is a method of IT service management developed in Europe and gaining worldwide attention. Although it is a framework for managing IT, parts of the practice lend themselves well to the auditing disciplines as they focus on controls and procedures.

© SANS Institute 2003, Author retains full rights.

[5] Schwartau, p.34.
[6] http://www.itil.co.uk/

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2 Audit Checklist

The following is a checklist developed for auditing the operating system of the target machine at XYZ Mfg. Each checklist item endeavors to support one of the stated control objectives for this machine. Each item contains comments on the risk of the item if exploited, criteria for compliance with the audit (what we are measuring), testing steps (command lines where applicable), expected output, a comment on whether the test is objective or subjective and whether the test is a "stimulus/response" type test, and finally space for the auditor to indicate his findings and a "pass or fail" grade for the item.

Risk will be evaluated in terms of vulnerabilities and threats specific to this system. Risk for any given checklist item will be rated on a scale of 1 to 10. A rating of "1" or "5" does not mean that the checklist item is not important. Risk ratings are used as a method of prioritizing efforts and focusing resources. Use of this checklist for evaluation of other systems is encouraged, but the threats and likelihood of exploitation will be different for every system.

For clarity and ease of reading the following conventions will be used:

- A "\" will be used to continue any command lines that may wrap to the next line due to length.
- Smaller fonts will be used in some cases to prevent text from wrapping to the next line.
- Any command lines to be typed by the auditor will be written without quotation marks, will be represented in blue, and will be bold as in the following: **`/usr/bin/ls -l /etc/issue`**
- Any expected output will be represented in green and will be bold as in the following:

`*** WARNING: This system is for authorized use only. All activity will be monitored. ***`

- As this project is assuming the role of an auditor, most tests will be performed as an unprivileged user. However, some tests will require superuser access. Any such requirements will be noted.

2.1 Control Objective: Verify the system's network services are configured securely

2.1.1 Checklist item #01: System time synchronization

System time Synchronization	Is NTP being used to synchronize the system time with a reliable time source?

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

System time Synchronization	Is NTP being used to synchronize the system time with a reliable time source?
References	• Rehman, p.669 • Personal experience
Risk Evaluation	Precise synchronization of system time among all systems in an environment is useful for such tasks as incremental backups and integrated scheduled jobs, but it is critical for correlating evidence in the case of a security event. For example, an investigator may be required to prove that an event on the firewall coincided with a related event on the audit target. Without synchronized system times, evidence to be used in a prosecution could be ruled inadmissible preventing the company from proving its case and possibly receiving insurance settlements. **Risk Rating="4".** Although it is good administrative practice, a lack of time synchronization is not likely to lead to a system compromise.
Compliance	"xntpd" is the daemon in HP-UX that controls the time synchronization. It must be configured, running, and actually working.
Testing	Test 1) To test that xntpd is configured to start, type `/usr/bin/grep XNTPD= /etc/rc.config.d/netdaemons` Test 2) To test that xntpd is running, type `/usr/bin/ps -ef | /usr/bin/grep xntpd` Test 3) To test that xntpd is working, type `/usr/sbin/ntpq -p`

Expected Output	Output 1) `export XNTPD=1`. A "1" indicates that XNTPD is configured to start at boot time.
	
	Output 2) `root 9148 1 26 19:25:35 ? 0:00 /usr/sbin/xntpd`
	
	Output 3) A report similar to the following should show the servers we are retrieving time from…
	`remote refid st t when poll reach delay offset jitter`
	`==========`
	`timeserver.name 0.0.0.0 16 u - 64 0 0.000 0.000 4000.00`

Objective / Subjective	Objective (Stimulus/Response)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

System time Synchronization	Is NTP being used to synchronize the system time with a reliable time source?
Findings	
Pass / Fail	

2.1.2 Checklist item #02: Unnecessary services being started

Unnecessary services being started	Are any services being allowed to start from the scripts in /etc/rc.config.d which are not needed by the system and are disallowed by company policy?
References	• "Center for Internet Security: Level-1 Benchmark (v1.0.4) for HP-UX", p.13. • http://www.sans.org/top20/#U1 • Personal experience
Risk Evaluation	Many services may be started at boot time that are not necessary to the intended use of this server. More services being provided means more opportunities for misconfigurations and increased possibility of attacks against less-used network services. The configuration files in /etc/rc.config.d should be evaluated by the system administrator to determine their usefulness to the organization. Services not being used should be disabled and replacements should be found for services with a history of known-vulnerabilities. **Risk Rating="9".** A company assumes a high level of risk when running unused services in general and several services in particular that have a history of well-known vulnerabilities (sendmail, rpc, snmp, to name a few). Attacks against less-used network services are popular and the impact could vary from a short outage to a lengthy denial-of-service attack.
Compliance	Compliance will be measured against the company's documented list of acceptable services. In the absence of such a document, the exception will be noted and a few of the services known to have a history of vulnerability will be examined.
Testing	Test 1) Examine copies of any company policies and procedures detailing acceptable services. Test 2) As root, type `/usr/bin/grep -v "^#" /etc/rc.config.d/* | /usr/bin/grep "=1" | /usr/bin/more`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Unnecessary services being started	Are any services being allowed to start from the scripts in /etc/rc.config.d which are not needed by the system and are disallowed by company policy?
	Test 3) As root, type `/usr/bin/grep -v "^#" /etc/rc.config.d/* | /usr/bin/grep "=0" | /usr/bin/more`
Expected Output	Output 1) Relevant policy and procedure documents should detail which services are acceptable within the organization and under which circumstances they can be provided. Output 2) The entries which end in "=1" are services configured to start at boot time. Output 3) The entries which end in "=0" are services not configured to start at boot time. **Note:** Only services listed in the company's list of acceptable services should be configured to start at boot. In the absence of such a list the following is a list of services that should probably not be starting at boot time. This is just a sample, care should be taken to examine each service and only disable those for which there is no recognized business need: • Rpcd (RPC services have a long and distinguished history of exploits and are usually best disabled). These services are responsible for the #1 vulnerability in the SANS/FBI Top 20 Most Critical Internet Security Vulnerabilities for UNIX systems (http://www.sans.org/top20/#U1) • Mailsrvs (Unless the server is providing mail to users, this probably does not need to be enabled). This is #8 in the Top 20 list referenced above. • Nfsconf (NFS has a history of being exploitable, if it must be used research should be done to make it secure as possible). • SnmpMaster, SnmpHpunix, SnmpMib2, SnmpTrpDst (SNMP is used for some network management tools, but it has the potential to leak valuable system information to network clients). This is #4 in the Top 20 list referenced above.
Objective / Subjective	Subjective
Findings	

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Unnecessary services being started	Are any services being allowed to start from the scripts in /etc/rc.config.d which are not needed by the system and are disallowed by company policy?
Pass / Fail	

2.1.3 Checklist item #03: Internet daemon logging

Internet daemon logging	Is logging enabled for inetd?
References	• Ellis, p.10. • Wong, p.259. • Personal experience
Risk Evaluation	If the Internet Daemon (inetd) is configured to log incoming connections, some level of audit trail is established and patterns of use can be established. **Risk Rating="5".** Although logging these connections aids in evidence gathering, lack of logging does not necessarily contribute to a system compromise.
Compliance	Compliance will be measured by the existence of "INETD_ARGS="-l" (lowercase L) in the /etc/rc.config.d/netdaemons file and evidence of logged connections in the /var/adm/syslog/syslog.log file.
Testing	Test 1) Type `/usr/bin/grep INETD_ARGS= /etc/rc.config.d/netdaemons` Test 2) Type `/usr/bin/grep inetd /var/adm/syslog/syslog.log`
Expected Output	Output 1) `export INETD_ARGS="-l"` Output 2) Grep should result in many lines similar to the following line: `Aug 26 15:54:43 audittarget inetd[4814]: telnet/tcp: Connection from incominghost.net (10.0.0.105) at Tue Aug 26 15:54:43 2003`
Objective / Subjective	Objective
Findings	

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Internet daemon logging	Is logging enabled for inetd?
Pass / Fail	

2.1.4 Checklist item #04: Services brokered by the Internet daemon

Services brokered by the Internet daemon	Are any services being started by the inetd daemon that are not necessary to the function of this server and are disallowed by company policy?
References	• Jones, p.18. • "HP-UX Networking Ports Reference Guide" • Ellis, p.10. • Wong, p.259. • Personal experience
Risk Evaluation	The Internet Daemon (inetd) spawns many network services in response to network requests, some of these services have histories of security vulnerabilities. Any services that are not compliant with company policy should not be enabled or there should be a waiver signed by an upper-level manager acknowledging the risk. **Risk Rating="9".** Unsecured or obscure network services tend to not have much attention paid to them and many can easily be used to extract information about the system, cause a denial-of-service attack on the system, or they could even be the avenue an attacker uses to initially gain access. Even at XYZ Mfg. this would likely be one of the first areas examined for vulnerabilities by a determined internal or external threat.
Compliance	Compliance will be measured against the company's documented list of acceptable services. In the absence of such a document, the exception will be noted and a few of the services known to have a history of vulnerability will be examined (bootps, chargen, daytime, discard, echo, exec, finger, ident, ntalk, login, rpc, shell, tftp, time, uucp). ftp and telnet may be required by business need, but should be replaced with ssh as soon as possible. Use of ftp and telnet will not constitute non-compliance with this checklist item.
Testing	Test 1) Examine any company policies which address acceptable network services.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Services brokered by the Internet daemon	Are any services being started by the inetd daemon that are not necessary to the function of this server and are disallowed by company policy?
	Test 2) To get a list of services currently being brokered by inetd, type: `/usr/bin/grep -v "^#" /etc/inetd.conf`

Expected Output	Output 1) Company policy and procedure documents should list services that are acceptable and the conditions under which they may be provided.
	
	Output 2) One line per service per protocol will be displayed. Output will be similar to the following:
	`echo stream tcp nowait root internal`
	`echo dgram udp nowait root internal`
	`discard stream tcp nowait root internal`
	`discard dgram udp nowait root internal`
	`chargen stream tcp nowait root internal`
	`chargen dgram udp nowait root internal`
	
	Output 3) Only services that are allowed (or not disallowed) by company policy should be enabled. In the absence of company policy that addresses network services, the following can be used as a bare-minimum guide to services that should be disabled. Due to space constraints of this document each service will not be examined in detail.
	
	A good rule of thumb for deciding which services should be enabled is "Deny by default, allow by exception" (i.e. only enable services that are absolutely needed). A person securing a system **must** research whether these settings are valid for any particular system.
	
	The following lists were compiled using section 4.2 of Walt Jones' "How-to" secure HPUX 11i for use in a DMZ environment and pages 26 through 38 of the "HP-UX Networking Ports Reference Guide" (also written by Walt).
	
	Ensure these services are disabled:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Services brokered by the Internet daemon	Are any services being started by the inetd daemon that are not necessary to the function of this server and are disallowed by company policy?

	`#bootps dgram udp wait root /usr/lbin/bootpd bootpd`
	`#chargen dgram udp nowait root internal`
	`#chargen stream tcp nowait root internal`
	`#daytime dgram udp nowait root internal`
	`#daytime stream tcp nowait root internal`
	`#discard dgram udp nowait root internal`
	`#discard stream tcp nowait root internal`
	`#echo dgram udp nowait root internal`
	`#echo stream tcp nowait root internal`
	`#exec stream tcp nowait root /usr/lbin/rexecd rexecd`
	`#finger stream tcp nowait bin /usr/lbin/fingerd fingerd`
	`#ident stream tcp wait bin /usr/lbin/identd identd`
	`#login stream tcp nowait root /usr/lbin/rlogind rlogind`
	`#ntalk dgram udp wait root /usr/lbin/ntalkd ntalkd`
	`#printer stream tcp nowait root /usr/sbin/rlpdaemon rlpdaemon -i`
	`#recserv stream tcp nowait root /usr/lbin/recserv recserv -display :0`
	`#rpc dgram udp wait root /usr/lib/netsvc/rstat/rpc.rstatd 100001 2-4 rpc.rstatd`
	`#rpc dgram udp wait root /usr/lib/netsvc/rusers/rpc.rusersd 100002 1-2 rpc.rusersd`
	`#rpc dgram udp wait root /usr/lib/netsvc/rwall/rpc.rwalld 100008 1 rpc.rwalld`
	`#rpc dgram udp wait root /usr/lib/netsvc/spray/rpc.sprayd 100012 1 rpc.sprayd`
	`#rpc dgram udp wait root /usr/sbin/rpc.rquotad 100011 1 rpc.rquotad`
	`#rpc stream tcp nowait root /usr/sbin/rpc.rexd 100017 1 rpc.rexd`
	`#shell stream tcp nowait root /usr/lbin/remshd remshd`
	`#tftp dgram udp wait root /usr/lbin/tftpd tftpd`
	`#time dgram udp nowait root internal`
	`#time stream tcp nowait root internal`
	`#uucp stream tcp nowait root /usr/sbin/uucpd uucpd`
	
	These may be required by business need, but should be replaced with SHH as soon as possible:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Services brokered by the Internet daemon	Are any services being started by the inetd daemon that are not necessary to the function of this server and are disallowed by company policy?
	`ftp stream tcp nowait root /usr/lbin/ftpd ftpd -l` `telnet stream tcp nowait root /usr/lbin/telnetd telnetd`
Objective / Subjective	Subjective
Findings	
Pass / Fail	

2.1.5 Checklist item #05: TCP Wrappers

TCP Wrappers	Is the system making use of TCP Wrappers to secure network services?
References	• http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=TCPWRAP • "Center for Internet Security: Level-1 Benchmark (v1.0.4) for HP-UX", p.38. • Wong, p.262. • Personal experience
Risk Evaluation	Use of the "TCP Wrappers" product to manage access to network services based on IP address has been a security standard for years. For services that must be used regardless of a poor security history (telnet, ftp, etc.) using TCP Wrappers is one way to mitigate that risk. TCP Wrappers allows access to be granted (and denied) based on IP address (with built-in spoofing protection), provides for the startup of additional checking or logging programs upon connection, and provides for additional banner messages. **Risk Rating="9".** TCP Wrappers is a "preventative control" in that it is configurable to *prevent* intrusions through spoofing protection and access control lists. Preventative controls are preferable over detective or corrective controls in that the intrusion or compromise is prevented instead of just detected and hopefully fixed. The risk rating on this item is high because any network services that are left configured due to business needs must have access to them controlled to prevent abuse.
Compliance	Compliance will be determined by verifying several component programs are on the system, checking for

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

TCP Wrappers	Is the system making use of TCP Wrappers to secure network services?
	tcpwrap usage in inetd.conf, examining the allow/deny files, and attempting to connect to a service that the configuration files indicate is protected.
Testing	Test 1) Type `/usr/bin/ls -l /usr/lbin/tcpd  /usr/bin/tcpdchk /opt/tcpwrap/bin/tcpd` Test 2) Type `/usr/bin/grep tcpwrap /etc/inetd.conf` Test 3) Type `/usr/bin/more /etc/hosts.allow /etc/hosts.deny` **Note:** Chris Wong notes on page 266 of her book that TCP Wrapper follows these two rules: • Search the /etc/hosts.allow file. If a match is found, service is allowed. If no match is found, continue to next rule. • Search the /etc/hosts.deny file. If a match is found, service is denied. If no match is made, *the service is allowed*. **This default "fall through" and the use of wildcard words such as "ALL: ALL" must be considered when building allow/deny files.** Test 4) Given the two rules listed above and the output of Test 3) try to connect to a service that is protected by TCP Wrappers from a host that is not allowed.

Expected Output	Output 1) Output must be three lines similar to the following (some details will be different):
	`-r-xr-xr-x  1 bin  bin  36864 Nov 19  2002 /usr/lbin/tcpd`
	`-r-xr-xr-x  1 bin  bin  84343 Nov 19  2002 /usr/bin/tcpdchk`
	`-r-xr-xr-x  1 bin  bin  43256 Nov 19  2002 /opt/tcpwrap/bin/tcpd`
	
	Output 2) Several lines should show similar to the following:
	`ftp  stream  tcp  nowait  root  /opt/tcpwrap/bin/tcpd  /usr/lbin/ftpd -l`
	
	Output 3) The contents of the hosts.allow and hosts.deny files should show specific services and hosts that are allowed and denied respectively.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

TCP Wrappers	Is the system making use of TCP Wrappers to secure network services?

	Output 4) After an attempted connection from a disallowed host, results should be similar to the following:
	`421 Service not available, remote server has closed connection`
	`ftp>`

Objective / Subjective	Objective (Stimulus/Response test)
Findings	
Pass / Fail	

2.1.6 Checklist item #06: Internet daemon security file

Internet daemon security file	Is /var/adm/inetd.sec being used to restrict access to inetd services?
References	• Wong, p.261 • Personal experience
Risk Evaluation	Access to services brokered by inetd can be granted or denied through entries in the /var/adm/inetd.sec file. TCP Wrappers allows finer granularity of control over access than inetd.sec does. This check for inetd.sec is part of this audit because not all systems use TCP Wrappers. **Risk Rating="7".** If TCP Wrappers is in use, the risk of not using inetd.sec is low. If TCP Wrappers is not in use, the risk of also not using inetd.sec is considered high.
Compliance	Compliance will be measured by examining the contents of the /var/adm/inetd.sec file in context of the results of "Checklist item #05: TCP Wrappers" and correlating the results with the services brokered by inetd as found in "Checklist item #04: Services brokered by the Internet daemon".
Testing	Type `/usr/bin/grep -v "^#" /var/adm/inetd.sec`

Expected Output	Output should consist of at least one line for each service being managed by the inetd daemon. Lines will have the general appearance of:
	`ftp  deny`
	`telnet  allow 10.0.0.101 10.0.5.*`

Objective /	Objective

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Internet daemon security file	Is /var/adm/inetd.sec being used to restrict access to inetd services?
Subjective	
Findings	
Pass / Fail	

2.1.7 Checklist item #07: Secure Shell

Secure Shell	Is ssh used instead of telnet and ftp?
References	• http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=T1471AA • Ryan, p.26. • Personal experience
Risk Evaluation	The risks of telnet and ftp can hardly be overstated. Both services have a history of vulnerabilities and both transfer passwords in clear-text over the network making it very possible for another user of the network to retrieve the passwords. Secure Shell (ssh) does not send passwords in clear-text over the network, and it allows encrypted network traffic and increased access control. As with most other programs, ssh has had several security patches issued. It is wise to install the most recent copy of ssh. At the time of this writing, the most recent copy of HP-UX Secure Shell is A.03.50.000. This is based on OpenSSH 3.5p1. When installing ssh it is best to configure it to use version 2 of the ssh protocols instead of version 1 as there are recognized weaknesses in version 1. **Risk Rating=”10”.** With the vulnerabilities in telnet and ftp, use of ssh as a secure replacement has become a standard. Continuing to use the legacy services opens the system to attack from a network user retrieving the passwords from sniffed network traffic or from one of the exploits available on the Internet for these services. **Note:** If telnet and ftp are required for business reasons, effort should be given to securing them with TCP

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Secure Shell	Is ssh used instead of telnet and ftp?
	Wrappers and use of the /etc/ftpd/ftpaccess file.
Compliance	Compliance will be measured by confirming that there are no telnetd or ftpd daemons listening, that ssh is installed and accessible from the network.
Testing	Test 1) Type `/usr/bin/netstat -af inet | /usr/bin/grep telnet` Test 2) Type `/usr/bin/netstat -af inet | /usr/bin/grep ftp` Test 3) Type `/usr/bin/ssh -V` (capital V) Test 4) From a different host, try to use ssh to connect to the audit target. Type `ssh username@audittarget.xyzmfg.com`

Expected Output	Output 1) There should be no telnetd listening and no established connections, so there should be no output from the test command.
	
	Output 2) There should be no ftpd listening and no established connections, so there should be no output from the test command.
	
	Output 3) `OpenSSH_3.5p1, SSH protocols 1.5/2.0, OpenSSL 0x0090609f`
	
	Output 4) Output should consist of evidence of successful login to the audit target machine.
	`$ ssh username@audittarget`
	`username@audittarget's password:`
	`Last login: Tue Aug 26 21:36:54 2003 from somewhereelse`
	`(c)Copyright 1983-2000 Hewlett-Packard Co., All Rights Reserved.`
	`<snip all the copyright stuff>`
	`(c)Copyright 1991-2000 Isogon Corporation, All Rights Reserved.`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Secure Shell	Is ssh used instead of telnet and ftp?
	RESTRICTED RIGHTS LEGEND Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in sub-paragraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013. Hewlett-Packard Company 3000 Hanover Street Palo Alto, CA 94304 U.S.A. Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).
Objective / Subjective	Objective (Stimulus/Response test)
Findings	
Pass / Fail	

2.1.8 Checklist item #08: Trust relationships

Trust relationships	Are trust relationships allowed between the audit target and other systems using hosts.equiv and .rhosts files?
References	• Jones, p.16. • Personal experience
Risk Evaluation	Files such as /etc/hosts.equiv and .rhosts files in users' directories establish equivalencies between users on the remote system and users on the local system allowing them to potentially login to the local system without supplying a password. These equivalencies establish trust relationships between this system and other systems over which the administrator of this system may have no control. Exploiting trust relationships between systems is a popular method for gaining unauthorized access to a machine. A company policy should exist to address the trust relationships the company is willing to allow. The use

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Trust relationships	Are trust relationships allowed between the audit target and other systems using hosts.equiv and .rhosts files?
	of .rhosts files is discouraged by many practicing system security as they are susceptible to spoofing. **Risk Rating="9".**
Compliance	If a company policy exists which addresses the use of these files, compliance will be measured by examining the system for the presence of these files and determining the usefulness of the files (One practice is to create the files and change their permissions to not allow anyone to access them. This prevents them from being created in the future.) If a company policy does not exist, these files will be assumed to be undesirable for a secure system and compliance will be measured as if company policy disallowed them (they must not exist or must be rendered inaccessible).
Testing	Test 1) Examine any company policies and procedures that address trust relationships. Test 2) Type `/usr/bin/ls -l /etc/hosts.equiv` Test 3) Type `/usr/bin/grep -v "^#"  /etc/hosts.equiv` Test 4a) Type `/usr/bin/find / -name .rhosts -exec /usr/bin/ls -ld {} \;` Test 4b) Any files discovered in Test 4a should be examined to ensure they are abiding by company policy (or in the absence of that, do not have "+" wildcards).
Expected Output	Output 1) Company documents should define the conditions under which trust relationships and their accompanying files are or are not allowed. Output 2) If the hosts.equiv file is disallowed by company policy (or by best practices), the output will be nonexistent or can also be similar to the following which indicates a file that exists, but is not usable `----------  1 root  sys  0 Jan 27 00:29 /etc/hosts.equiv`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Trust relationships	Are trust relationships allowed between the audit target and other systems using hosts.equiv and .rhosts files?
	Output 3) Output should be empty or show hostnames/usernames in accordance with policy. Output 4a) Output should be empty or in accordance with policy. Output 4b) Output should not have any lines with "+".
Objective / Subjective	Subjective
Findings	
Pass / Fail	

2.1.9 Checklist item #09: Sendmail configuration

Sendmail configuration	Is this system intended to be a sendmail server?
References	• Jones, P.25. • Wong, p.444. • Personal experience
Risk Evaluation	"Checklist item #02: Unnecessary services being started" dealt with unnecessary services being started from the /etc/rc.config.d directory. Sendmail (/etc/rc.config.d/mailservs) is one of those services, but due to its popularity and history of security issues, it deserves its own checklist item. Sendmail is the most common mail server and comes installed on most flavors of UNIX. Unless the audit target is intended to provide mail services to its users, sendmail does **not** need to be running in daemon mode (listening on port 25 to service mail requests). With sendmail's history of security issues, it should only be run if needed, if brought up to the most recent stable version, and if patched with all current patches. **Risk Rating="7".** If necessary for the purposes of this server (and allowed in company policies), sendmail should be secured against leaking too much information about the system and it's users.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Sendmail configuration	Is this system intended to be a sendmail server?
Compliance	Compliance will be measured according to company policy and business needs of this server. If sendmail is required and authorized, it will be considered compliant if the "goaway" privacy option is used to disable EXPN and VRFY commands (among others) as they leak information about the users of the system. If sendmail is not required or authorized, this item will be compliant only if sendmail is shown not to be running. **Note:** There are entire books written about configuring sendmail. The tests in this checklist item are basic measures to keep sendmail from leaking too much information about the system's users.
Testing	Test 1) Are company policies available which address the use of sendmail? Test 2a) Type `/usr/bin/grep SENDMAIL_SERVER /etc/rc.config.d/mailservs` Test 2b) Type `/usr/bin/grep "sendmail -" /sbin/init.d/sendmail` Test 2c) Type `/usr/bin/ps -ef | /usr/bin/grep sendmail` Test 3) Type `/usr/bin/grep PrivacyOptions /etc/mail/sendmail.cf`

Expected Output	Output 1) Review any company policies on use of sendmail.
	
	Output 2a) If sendmail is configured to not start at boot time, following should be the output:
	`export SENDMAIL_SERVER=0`
	`export SENDMAIL_SERVER_NAME=`
	
	Output 2b) If sendmail's "-bd" argument has been removed to prevent sendmail from running as a daemon[7], output will be:
	`/usr/sbin/sendmail -q30m && echo "sendmail"`

[7] Jones, p.25

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Sendmail configuration	Is this system intended to be a sendmail server?

	otherwise, it will be: `/usr/sbin/sendmail -bd -q30m && echo "sendmail"`
	
	Output 2c) If sendmail is running, output will be similar to:
	`root 12532 1  0 14:40:48 ?  0:00 sendmail:accepting connections on port 25`
	
	Output 3) If Test 1 indicated that the company allows use of sendmail, the following line should show the following strict settings in the sendmail configuration options:
	`O PrivacyOptions=goaway,restrictmailq,restrictqrun`

Objective / Subjective	Objective
Findings	
Pass / Fail	

2.1.10 Checklist item #10: CDE access

CDE access	Is access to CDE from the network limited by the /etc/dt/config/Xaccess file?
References	• Ellis, p.21.
Risk Evaluation	The main application used at XYZ Mfg. requires users to login via CDE. Providing X-Window services on the network introduces risks of malicious users exploiting CDE or X-Windows vulnerabilities. But, listing the specific hostnames in /etc/dt/config/Xaccess that are allowed to receive a CDE login screen can reduce this risk. **Risk Rating="8".** The benefits of restricting CDE access to only authorized systems far outweigh the cost of the time investment of maintaining a list of authorized hostnames in Xaccess. Given the relatively small number of clients requiring access to this server, maintaining the list should not be prohibitively difficult.
Compliance	The /etc/dt/config/Xacess file must exist and contain valid hosts that are allowed or disallowed by the file (A "!" in front of a hostname denies that host access, whereas the hostname by itself grants the host access. Wildcards granting whole networks access are also possible.)
Testing	Test 1) Type `/usr/bin/ls -l /etc/dt/config/Xaccess`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

CDE access	Is access to CDE from the network limited by the /etc/dt/config/Xaccess file?
	Test 2) Type `/usr/bin/grep -v "^#" /etc/dt/config/Xaccess`

Expected Output	Output 1) `-r--r--r--  1 bin  bin  4500 Nov 14  2000 /etc/dt/config/Xaccess`
	
	Output 2) A list of hosts allowed (or disallowed) access should be similar to the following:
	`workstation1.xyzmfg.com`
	`admin.xyzmfg.com`
	`shopfloor.xyzmfg.com`
	`!storageroom.xyzmfg.com`

Objective / Subjective	Objective
Findings	
Pass / Fail	

2.1.11 Checklist item #11: Banners

Banners	Do system banners provide version numbers or are unnecessarily welcoming?
References	• "Center for Internet Security: Level-1 Benchmark (v1.0.4) for HP-UX", p.32. • Jones, p.42. • Personal experience
Risk Evaluation	Text presented to users when logging in to a system or connecting to a network service frequently leaks valuable information about the system including versions of programs, the operating system version itself, and clues to the use of the system. Best practice standards call for removal of all information welcoming the user in favor of verbiage cautioning that the system is for official use only, all activity is subject to monitoring, and violations will be prosecuted. **Risk Rating="5".** Leaking information may not directly cause a system intrusion, but it can definitely contribute to a reconnaissance effort by those with malicious intent.
Compliance	The auditor will examine the /etc/motd, /etc/issue, /etc/ftpd/ftpaccess, and /etc/inetd.conf files as well as attempt connections to the ftp and telnet services. Compliance will be measured by assuring there are no

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Banners	Do system banners provide version numbers or are unnecessarily welcoming?
	version numbers of the operating system or system services and there is verbiage indicating that access to the system is for authorized users and for official purposes only.

Testing	Test 1) Type `/usr/bin/cat /etc/motd` and `/usr/bin/cat /etc/issue`
	
	Test 2a) If ftp is being used, test that a banner is configured by typing:
	`/usr/bin/grep banner /etc/ftpd/ftpaccess`
	
	Test 2b) If ftp is being used, verify the banner by attempting to connect to the machine.
	
	Test 3a) If telnet is being used, test that the daemon is configured to not display a banner by typing:
	`/usr/bin/grep telnetd /etc/inetd.conf`
	
	Test 3b) If telnet is being used, verify the banner is turned off by attempting to connect to the machine via telnet.

Expected Output	Output 1) The output of both commands should warn against unauthorized use. Output 2a) If the ftpaccess file exists, a line specifying a banner file should be the result of Test 2a. Output will be similar to the following: `banner /etc/motd`. Output 2b) If ftp is used, attempts to connect to the ftp service should result in the banner specified in the preceding test being presented to the user. Output 3a) If telnet is being used and uncommented in the /etc/inetd.conf file, the output of Test 3a should be: `telnet stream tcp nowait root /usr/lbin/telnetd telnetd -b` (the "-b" option should be on the command line) Output 3b) If telnet is being used, attempts to connect to the telnet service should result in only the prompt: `login:` (no identifying lines).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Banners	Do system banners provide version numbers or are unnecessarily welcoming?
Objective / Subjective	Objective (Stimulus/Response test)
Findings	
Pass / Fail	

2.1.12 Checklist item #12: Modems

Modems	If modem access is allowed by company policy, have the modem devices been secured?
References	• Ellis, p.20. • Wong, p.136. • Personal experience
Risk Evaluation	Many companies are surprised to learn that their system may be providing logins via enabled modems. This is an older access method that is often overlooked. Page 20 of Ellis and page 136 of Wong give steps for securing modem access. **Risk Rating="8".** This item is rated high due to the fact that modem access bypasses any firewalls or other network defenses and is frequently overlooked. Although it is less likely that the company will be "war dialed" than it may have been in the past, there is still the threat and initial conversations with the system administrators at XYZ indicate that such war dialing may be taking place at this location.
Compliance	Any applicable company policies and procedures must be reviewed. The /etc/inittab file must be reviewed to determine if the lines for getty providing logins to tty devices are commented out and the /etc/dialups and /etc/d_passwd files must be examined to determine if they are being used to require passwords for modem logins.
Testing	Test 1) Review company policy documents which address modem use on servers. Any steps outlined for securing modems must be examined. Test 2a) Type `/usr/bin/grep getty /etc/inittab` Test 2b) Type `/usr/sbin/ioscan -FunC tty`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Modems	If modem access is allowed by company policy, have the modem devices been secured?
	Test 3) Type **/usr/bin/cat /etc/dialups** Test 4) Type **/usr/bin/cat /etc/d_passwd**
Expected Output	Output 1) Policies must be shown to approve or disapprove of modem usage. Output below must be examined for compliance with any existing company policy. Output 2a) If policy disallows modem usage, any lines like the ttyp1 through ttyp5 lines below should be commented out. **cons:123456:respawn:/usr/sbin/getty console console # system console** **#ttp1:234:respawn:/usr/sbin/getty -h tty0p1 9600** **#ttp2:234:respawn:/usr/sbin/getty -h tty0p2 9600** **#ttp3:234:respawn:/usr/sbin/getty -h tty0p3 9600** **#ttp4:234:respawn:/usr/sbin/getty -h tty0p4 9600** **#ttp5:234:respawn:/usr/sbin/getty -h tty0p5 9600** Output 2b) Output of ioscan should show any modem devices. **pci:wsio:F:T:F:-1:1:0:tty:asio0:10/0/14/1/1:16 11 0 14 0 26 224 116 :0:root.sba.lba.superio.asio0:asio0:CLAIMED:INTERFACE:Built-in RS-232C:0** **/dev/diag/mux0 /dev/mux0 /dev/tty0p0** **pci:wsio:F:T:F:-1:1:65536:tty:asio0:10/0/14/1/2:16 11 0 14 0 26 224 116 :1:root.sba.lba.superio.asio0:asio0:CLAIMED:INTERFACE:Built-in RS-232C:1** **/dev/diag/mux1 /dev/mux1 /dev/tty1p0** Output 3) If policy allows modem usage, there should be an /etc/dialups file containing a list of modem devices as shown in the output from Test 2a. Output of Test 3 would be similar to the following: **/dev/tty0p0** **/dev/tty1p0** Output 4) If policy allows modem usage, there should be an /etc/d_passwd file containing the shell from the /etc/passwd file with an encrypted password. Output will be similar to the following:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Modems	If modem access is allowed by company policy, have the modem devices been secured?
	`/usr/bin/sh:xw0MgTdwgSU:comment`
Objective / Subjective	Objective
Findings	
Pass / Fail	

2.2 Control Objective: Verify that the system is patched regularly according to the company's patching strategy.

2.2.1 Checklist item #13: Security patches

Security patches	Is HP's Security Patch Checker tool run regularly?
References	• http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA • Wong, p.438. • Personal experience
Risk Evaluation	Proactive installation of security patches is critical for keeping a system secure. Many well-known vulnerabilities are exploited simply because system administrators are slow in patching their systems (not only through neglect, frequently they have too many or complex systems to keep current on all of them). If the system administrators are not applying security patches *proactively*, by definition, they are applying them *reactively* or not at all. **Risk Rating="10".** Given the frequency with which security patches are released, the risk for not keeping current with security patches earns this item its high rating.
Compliance	Compliance will be measured by the determination that HP's Security Patch Checker is installed on the audit target, configured to run regularly (at least weekly), and configured to mail the results to an administrator.
Testing	Test 1) As root, type `/usr/bin/ls -l /opt/sec_mgmt/spc/bin/security_patch_check` Test 2) As root, type `/usr/bin/grep security_patch_check /var/spool/cron/crontabs/*`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Security patches	Is HP's Security Patch Checker tool run regularly?
	Test 3) Examine evidence that the security_patch_check tool successfully sent mail to the administrator(s) regarding available security patches.

Expected Output	Output 1) `-r-xr-xr-x  1 bin  bin  7880 Oct 18  2001 /opt/sec_mgmt/spc/bin/security_patch_check`
	
	Output 2) `0 3 * * * /opt/sec_mgmt/spc/bin/security_patch_check -r | /usr/bin/mail root`
	
	Output 3) Evidence of a mail message sent to an administrator, similar to the following:
	`From root@audittarget Tue Aug 26 12:15:14 EDT 2003`
	`Received: (from root@localhost)`
	`  by audittarget (8.9.3/8.9.3) id MAA09000`
	`  for root; Tue, 26 Aug 2003 12:15:14 -0400 (EDT)`
	`Date: Tue, 26 Aug 2003 12:15:14 -0400 (EDT)`
	`From: root@audittarget`
	`Message-Id: <200308261615.MAA09000@audittarget >`
	
	`*** BEGINNING OF SECURITY PATCH CHECK REPORT ***`
	`Report generated by: /opt/sec_mgmt/spc/bin/security_patch_check.pl, run as root`
	`Analyzed localhost (HP-UX 11.11) from audittarget`
	`Security catalog: /var/opt/sec_mgmt/security_catalog`
	`Security catalog created on: Mon Aug 25 21:34:01 2003`
	`Time of analysis: Tue Aug 26 12:15:14 2003`
	
	`List of recommended patches for most secure system:`
	
	`#  Recommended  Bull(s) Spec? Reboot? PDep? Description`
	`----------`
	`1  PHCO_23492  159  No  Yes  No  Kernsymtab`
	`2  PHCO_23909  167  No  No  No  cu(1)`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Security patches	Is HP's Security Patch Checker tool run regularly?
	3 PHCO_24839 191 No No Yes libpam_unix cumulative <edited for length> 24 PHSS_28470 228 No No No X Font Server 25 PHSS_28676 263 Yes No No CDE Base Periodic 26 PHSS_28677 263 Yes No Yes CDE Applications Periodic ---------- *** END OF REPORT *** NOTE: Security bulletins can be found ordered by number at http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin
Objective / Subjective	Objective
Findings	
Pass / Fail	

2.2.2 Checklist item #14: Operating system patches

Operating system patches	Are operating system patches applied regularly according to the company's patching strategy?
References	• Ellis, p.32. • Personal experience
Risk Evaluation	Every operating system is constantly being updated as vulnerabilities in its components are discovered. For any system that has been installed for more than a few months, there are usually extensive lists of patches that are recommended or required by the vendor. The company that does not keep current with patches runs the risk of being compromised unnecessarily through a vulnerability for which a patch already exists. Systems such as Internet-facing servers should be kept up-to-date with the most recent patches while, for stability sake, many companies choose to adopt a more conservative approach for critical internal database servers. For these more protected servers, a quarterly patch application may be best.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Operating system patches	Are operating system patches applied regularly according to the company's patching strategy?
	Risk Rating="9".
Compliance	A listing of installed patches on the system as well as an examination of the software installation logs would show if patches are being applied. Evidence from a change management process would also indicate compliance. A complete discussion of patch management processes is outside of the scope of this audit. However, individual patches as well as patch bundles can be downloaded for free from http://itrc.hp.com (Due to load balancers, it is best to go to the main page and navigate in.) Custom patch bundles are available to customers with a current HP support contract. The goal is to show application of patches in accordance with corporate policy. In the absence of a patch policy, evidence of an application within the past three months would indicate compliance.
Testing	Test 1) Acquire copies of company policies addressing operating system patching. Test 2) To get a list of individual patches, type `/usr/sbin/swlist -l patch` Test 3) To get a list of patch bundles, type `/usr/sbin/swlist -l bundle | /usr/bin/grep Patch` Test 4) Examine most recent dates in "/var/adm/sw/swinstall.log" for evidence of regular patching. Strings such as "QPK", "PHKL", "PHCO", "PHSS", and "PHNE" indicate quality bundles and individual patches.
Expected Output	Due to the manual nature of these tests and the volume of output, full "expected output" is not provided. Output 1) If company policies regarding patching exist, they must detail the frequency of patching that is expected and any criteria for evaluating patches (maturity, criticality, etc.)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Operating system patches	Are operating system patches applied regularly according to the company's patching strategy?
	Output 2) Output may consist of hundreds of individual patches. Output 3) Results should indicate current bundles such as: `GOLDQPK11i  B.11.11.0306.4 HP-UX 11i Quality Pack, June 2003` Output 4) Results of searches for strings indicated in Test 4 should be toward the end of the swinstall.log with recent dates (as specified in "Compliance" section).
Objective / Subjective	Subjective
Findings	
Pass / Fail	

2.3 Control Objective: Verify that access to the system is properly controlled

2.3.1 Checklist item #15: Shadow Passwords

Shadow Passwords	Are Shadow Passwords used on this machine?
References	• http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=ShadowPassword • Personal experience
Risk Evaluation	On older UNIX systems all passwords were kept in a "hashed" format (commonly referred to as "encrypted") all in one file, /etc/passwd. A much safer alternative (the standard in most current UNIX and UNIX-like operating systems) is to store the hashed passwords in a separate file readable only by root, /etc/shadow. This shadow password functionality is shipped with HP-UX 11i v1.6 and can be added to HP-UX 11i versions 1.0 and 1.5 with software downloaded from the address in the references section above. **Risk Rating="9".** If the system is not a "Trusted System" and not running Shadow Passwords, any user on the system can read the /etc/passwd file, copy it off-line, and use a password cracker to discover weak

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Shadow Passwords	Are Shadow Passwords used on this machine?
	passwords for later exploitation. Except in cases where Shadow Passwords would break an application, they should be used on every system.
Compliance	Compliance will be measured by the meeting of the following two criteria: • Existence of the /etc/shadow file (with file size larger than 0). • Existence of a single "x" in every user's password field in the /etc/passwd file.
Testing	Test 1) Type `/usr/bin/ls -l /etc/shadow` Test 2) Type `/usr/bin/awk -F: '{print $2}' /etc/passwd | /usr/bin/sort -u`
Expected Output	Output 1) Output similar to the following showing a file size larger than zero: `-rw-r-----  1 root  sys  2598 Aug 13 18:46 /etc/shadow` Output 2) The test command line outputs contents of every user's password field and sorts it with a "unique" modifier to eliminate duplicates. If shadow passwords are in use, the output should consist of a single "x" representing all user's hashed passwords being in the /etc/shadow file.
Objective / Subjective	Objective
Findings	
Pass / Fail	

2.3.2 Checklist item #16: Minimum password length

Minimum password length	Does this system enforce a minimum password length (either one specified in company policies or recommended length of 8)?
References	• http://docs.hp.com/hpux/onlinedocs/B2355-90696/00/01/111-con.html (Man page for /etc/default/security in HP-UX 11i v1) • http://www.sans.org/top20/#U10 • Personal experience
Risk	Some users choose shorter passwords in order to remember them more easily. This also makes them

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Minimum password length	Does this system enforce a minimum password length (either one specified in company policies or recommended length of 8)?
Evaluation	easier for a password cracker to discover. **Risk Rating="8".** The use of blank or weak user passwords is very common (number 10 on the SANS/FBI Top Vulnerabilities to Unix Systems list). The risk of allowing short passwords is increased when "Shadow Passwords" are not used (see Checklist item #15: Shadow Passwords).
Compliance	"MIN_PASSWORD_LENGTH" must be set in /etc/default/security and a non-complying password change must be attempted.
Testing	Test 1) Examine any company policies governing password composition. Test 2) Type `/usr/bin/grep MIN_PASSWORD_LENGTH /etc/default/security` Test 3) Login as non-privileged user and type the command: `passwd` Then attempt to change the password to less characters than are called for in company policy (or less than 8 in absence of a company policy).

Expected Output	Output 1) Policies must detail the criteria for password composition.
	
	Output 2) Output should be `MIN_PASSWORD_LENGTH=8`
	(Valid values for systems that are not Trusted Systems are 6, 7, or 8).
	
	Output 3) Output should be similar to the following three lines:
	`Changing password for username`
	`Old password:  <something short>`
	`Password too short - must be at least 8 characters`

Objective / Subjective	Objective (Stimulus/Response test)
Findings	

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Minimum password length	Does this system enforce a minimum password length (either one specified in company policies or recommended length of 8)?
Pass / Fail	

2.3.3 Checklist item #17: Empty passwords

Empty passwords	Are there any users in the password file with empty or null passwords?
References	• "Center for Internet Security: Level-1 Benchmark (v1.0.4) for HP-UX", p.35. • http://www.sans.org/top20/#U10 • Personal experience
Risk Evaluation	According to the SANS/FBI Top 20 List, weak or nonexistent passwords are the tenth most common vulnerability on UNIX systems. In effect, having empty passwords on one or more accounts is handing out anonymous access to the machine. Once on the machine, an attacker can implement additional methods to escalate their privileges to superuser. **Risk Rating="9".** This item earns a high risk rating as it hands access to the system to any attacker or casual observer (the attacker still has to discover a valid username to attempt a null password). If someone is attempting to access the system, it is likely that this will be one of the first avenues of attack.
Compliance	No accounts on this machine should have empty passwords.
Testing	While logged in as root, type `/usr/sbin/logins -p`
Expected Output	As this command lists users without passwords, there should be **NO** output.
Objective / Subjective	Objective
Findings	
Pass / Fail	

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.3.4 Checklist item #18: Weak passwords

Weak passwords	Are the users of this system choosing passwords that are not easy to guess and are not found in any dictionary?
References	• http://www.sans.org/top20/#U10 • Personal experience
Risk Evaluation	As in Checklist item #17: Empty passwords, weak passwords are on the SANS/FBI Top 20 list of most common vulnerabilities on UNIX systems. The collection of passwords is part of the chain keeping the system safe and any chain is only as strong as its weakest link. Especially for systems not using Shadow Passwords (discussed elsewhere in the checklist), the /etc/passwd file is huge target for those wishing to elevate their privileges on a system. **Risk Rating="9".** The likelihood for exploitation of weak passwords is high on systems that are not using Shadow Passwords and are not Trusted Systems. **Note:** Due to the sensitivity of this test, the auditor will not view the results in a way that will associate a vulnerable password with a specific user. Also, the test must not be run on the system under review. Recommended practice is to run this test on a machine that is not connected to the network during the test. The results will be removed from the machine before users other than the auditor are allowed back on.
Compliance	Compliance for this test will be measured by the use of the tool "John the Ripper" to attempt to crack passwords in the /etc/passwd file over the course of one hour. To preserve the objectivity of the test, this item will be considered non-compliant (failed) if any passwords are successfully cracked. Although many systems fail this test, full compliance is not impossible. John the Ripper is a well-known tool available at http://www.openwall.com/john/. Configuration and execution of this tool is outside the scope of this document. It could be argued that one hour is not long enough to make a valid test. As we are only looking for the weakest of passwords, we will continue with a one hour test.
Testing	Type `./john copy-of-passwd-file > /dev/null` After one hour, terminate the program with a ^C (CTRL-C) and type the following:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Weak passwords	Are the users of this system choosing passwords that are not easy to guess and are not found in any dictionary?
	`./john -show copy-of-passwd-file | /usr/bin/awk '{print $2}' ; \` `/usr/bin/rm john.pot restore`

Expected Output	As we are checking for **the existence** of weak passwords, we expect John the Ripper not to report any cracked passwords. All that is required for the actual cracking to take place is the "./john passwdfile" command. If the test is run as listed above, passwords are sent to /dev/null as they are discovered (and also stored in the john.pot file). The results are then filtered through awk to remove any actual passwords and output only the names of users with cracked (or empty) passwords. By immediately removing the status files, the auditor prevents himself from seeing any identifiable passwords.
	
	A fictitious example of normal John the Ripper output when finding weak passwords is:
	`Loaded 45 passwords with 45 different salts (Standard DES [24/32 4K])`
	`Secret01 (username)`
	`Bogey999 (manager)`
	`Session aborted`
	
	An example of possible output from our test if typed as listed above:
	`aborted`
	`45`
	`(username)`
	`(manager)`

Objective / Subjective	Objective
Findings	
Pass / Fail	

2.3.5 Checklist item #19: Duplicate superuser accounts

Duplicate superuser accounts	Are there more than one UID "0" accounts in the /etc/passwd (or /etc/shadow) file?

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Duplicate superuser accounts	Are there more than one UID "0" accounts in the /etc/passwd (or /etc/shadow) file?
References	• "Center for Internet Security: Level-1 Benchmark (v1.0.4) for HP-UX", p.35. • Personal experience
Risk Evaluation	There should be only one superuser (root) account on the system (user ID of zero). Existence of an additional UID "0" account indicates possible backdoor activity and effectively doubles the chances of an attacker gaining superuser privileges. System administrators occasionally create extra root-level users to ease administrative responsibilities, but this is considered very risky and insecure administration and is strongly discouraged. **Risk Rating="7".**
Compliance	There should be no duplicate UID "0" accounts in the /etc/passwd file.
Testing	While logged in as root, type `/usr/sbin/logins -d | /usr/bin/grep ' 0 '`
Expected Output	As this command lists users with duplicate user IDs and looks for " 0 ", there should be **NO** output.
Objective / Subjective	Objective
Findings	
Pass / Fail	

2.3.6 Checklist item #20: Root login restricted

Root login restricted	Is root restricted to logging in on the console only?
References	• "Center for Internet Security: Level-1 Benchmark (v1.0.4) for HP-UX", p.32. • Jones, p.13. • Personal experience
Risk Evaluation	In environments where more than one person logs in as root, there is often no way to tell who was behind a specific login (no audit trail). Also, system administrators occasionally get used to always logging in as root to save time. Restricting root to logging in directly only on the console is one way to encourage all

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Root login restricted	Is root restricted to logging in on the console only?
	system administrators to login as themselves and then “su” to root only when required. **Risk Rating=”6”.**
Compliance	The /etc/securetty file must exist, contain only the word “console”, and have no write permissions for any user other than root. Root must not be able to login from another terminal.
Testing	Test 1) As root, type `/usr/bin/ls -l /etc/securetty` Test 2) As root, type `/usr/bin/cat /etc/securetty` Test 3) Attempt to login as root from somewhere other than the console.
Expected Output	Output 1) `-r--------  1 root  sys  8 Jan 11 2000 /etc/securetty` (root’s permissions can also be “rw”) Output 2) Should consist of the word “`console`” on a line by itself. Output 3) Login should fail.
Objective / Subjective	Objective (Stimulus/Response test)
Findings	
Pass / Fail	

2.3.7 Checklist item #21: Unneeded system accounts

Unneeded system accounts	Have all unneeded system accounts been locked?
References	• “Center for Internet Security: Level-1 Benchmark (v1.0.4) for HP-UX”, p.34. • Jones, p.14. • Personal experience

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Unneeded system accounts	Have all unneeded system accounts been locked?
Risk Evaluation	Like many versions of UNIX, HP-UX is installed with several legacy accounts in the /etc/passwd and/or /etc/shadow file that do not require direct login access. **Risk Rating="5".** These unneeded accounts are best disabled to prevent possible abuse.
Compliance	A review of /etc/passwd (and /etc/shadow if in use) should show locked passwords in the second field (delimited by ":") and "/usr/bin/false" in the seventh field for each of the following users: uucp, nuucp, adm, bin, daemon, lp, nobody, noaccess, hpdb, useradm. (they may not all exist on every system)

Testing	Type the following lines:
	`for user in uucp nuucp adm bin daemon lp nobody noaccess hpdb useradm`
	`do`
	`  /usr/bin/grep "^$user" /etc/passwd`
	`done`
	
	Note: If Shadow Passwords are not in use, the above command can be executed to view the second field (password) and seventh field (shell) of the /etc/passwd file. If Shadow Passwords are in use, the command must be run a second time substituting /etc/shadow for /etc/passwd to view the hashed passwords (second field).

Expected Output	Output of the command run against a sample /etc/passwd (on a system without Shadow Passwords):
	
	`uucp:*:5:3::/var/spool/uucppublic:/usr/lbin/uucp/uucico`
	`nuucp:*:11:11::/var/spool/uucppublic:/usr/lbin/uucp/uucico`
	`adm:*:4:4::/var/adm:/usr/bin/false`
	`bin:*:2:2::/usr/bin: /usr/bin/false`
	`daemon:*:1:5::/: /usr/bin/false`
	`bin:*:2:2::/usr/bin: /usr/bin/false`
	`lp:*:9:7::/var/spool/lp: /usr/bin/false`
	`nobody:*:-2:-2::/:`
	`hpdb:*:27:1:ALLBASE:/: /usr/bin/false`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Unneeded system accounts	Have all unneeded system accounts been locked?
Objective / Subjective	Objective
Findings	
Pass / Fail	

2.3.8 Checklist item #22: PATH variable for root

PATH variable for root	Does root's PATH contain "." or any world writable/group writable directories?
References	• "Center for Internet Security: Level-1 Benchmark (v1.0.4) for HP-UX", p.35. • Personal experience
Risk Evaluation	One way a local user may try to elevate his privileges is to trick the superuser into running a command containing Trojan horse code. Many system administrators put a period ("." Meaning "current directory") in their PATH statement to save themselves keystrokes when running scripts in their home directories. This practice as well as the existence of world or group writable directories referenced in root's PATH statement makes the superuser more vulnerable to Trojan code. **Risk Rating="5".** Other vulnerabilities must be combined with this one to create the risk.
Compliance	Root's PATH variable must not contain a "." by itself (separated by field separators, of course), and may not reference any directories found to be group writable or world writable.
Testing	This test must be conducted while logged in as root: Test 1) Type `/usr/bin/echo $PATH`. Examine output for "." by itself. Test 2) Perform a `/usr/bin/ls -ld` on each entry in the PATH variable **OR** to get a list, type the following: `/usr/bin/ls -ld `/usr/bin/echo $PATH | /usr/bin/awk -F: '{for (x=1;x<=NF;x++){print $x}}'`
Expected Output	Output 1) Must not find "." by itself.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

PATH variable for root	Does root's PATH contain "." or any world writable/group writable directories?
	Output 2) No directories should have write permissions for the group or world.
Objective / Subjective	Objective
Findings	
Pass / Fail	

2.4 Control Objective: Verify that access and modification are properly controlled for sensitive files

2.4.1 Checklist item #23: Change Control

Change Control	Are changes to the system tracked with a formal change control process?
References	• "Change Management". Retrieved on 8/22/2003 from http://www.itil-itsm-world.com/itil-3.htm • Personal experience
Risk Evaluation	A formal process requiring any system changes to be documented and authorized is an effective way to assure continuing documentation takes place, assist people coming up-to-speed on a system to be aware of the current configuration, and reduce downtime due to misconfiguration by reviewing changes before implementing them. Although not strictly an operating system control, change control is vital to the supportability of a system. Hardware and software changes made outside of a formal review and implementation process have a greater likelihood of causing system outages especially in an environment with extremely busy system administrators. **Risk Rating="3".** While a change control process allows for finer control of system configuration, the lack of such a process does not *directly* make a compromise possible.
Compliance	Change Control processes come in many levels. Some companies simply require all changes to be requested on a one-page form with all changes being performed by one administrator after review by another. Other companies have teams of change administrators, reviewers, and implementers along with

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Change Control	Are changes to the system tracked with a formal change control process?
	formal change control approval meetings and firm change windows (special times for implementing approved changes). An example of compliance would be the presentation of documents describing the process this company uses and copies of change log books and recent change request forms.
Testing	Auditor must review the company's change management documentation and examine evidence that the process was followed on at least one recent change.
Expected Output	At a minimum there should be a description of the change, reason for the change, steps to implement the change, a back out plan, signoff that the change was completed, and possibly a "results" statement.
Objective / Subjective	Subjective
Findings	
Pass / Fail	

2.4.2 Checklist item #24: User directory security

User directory security	Users' home directories and personal startup files ("dot" files) should have restrictive permissions.
References	• "Center for Internet Security: Level-1 Benchmark (v1.0.4) for HP-UX", p.36.
Risk Evaluation	When a malicious user begins to try to escalate his privileges to superuser, he will frequently try to exploit poor permissions on other user's home directories and/or their individual startup files such as ~/.profile, ~/.cshrc, or ~/.exrc in an attempt to gain that user's privileges or to trick a system administrator into creating a backdoor unintentionally. **Risk Rating="6".** Exploiting weak user directory permissions requires more technical ability than simply using a pre-packaged exploit program, but weak permissions can be a building block to more serious issues.
Compliance	Compliance for this item will be two-fold:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

User directory security	Users' home directories and personal startup files ("dot" files) should have restrictive permissions.
	• Home directories for users as reported by the **`/usr/sbin/logins -ox`** command (or examination of the /etc/passwd file) must be owned by the user and have permissions mode of 755 or better (more restrictive). • For the same list of users (/etc/passwd), all "dot" files must not be group or world writable.

Testing	**Note:** The following script will produce a single file (/tmp/audit-dotfiles.txt) to make reviewing the below tests easier (must be logged in as root).
	----- snip below -----
	`/usr/sbin/logins -ox | /usr/bin/awk -F: '{print $1,$6}' | while /usr/bin/read user home`
	`do`
	`  /usr/bin/echo $user\'s home is:`
	`  /usr/bin/ls -ld  $home`
	`  /usr/bin/echo "  and dot files are:"`
	`  /usr/bin/ls -ld "$home/".[!.]*`
	`  /usr/bin/echo " "`
	`done > /tmp/audit-dotfiles.txt`
	----- snip above -----
	
	Test 1) (If not using the above script) For every user in the output of the **`/usr/sbin/logins -ox`** command (must be logged in as root), perform **`/usr/bin/ls -ld <dirname>`** on the user's home directory (field six).
	
	Test 2) (If not using the above script) To get a list of all "dot" files in the user's home directory, using the same list, perform **`/usr/bin/ls -l <dirname>/.[!.]*`**

Expected Output	Output 1&2) Using the script provided above, each user should have output similar to the following:
	`username's home is /home/username, the permissions are:`
	`drwxr-xr-x  3 username users  8192 Aug 26 21:34 /home/tdob`
	`  and dot files are:`
	`-rw-r--r--  1 username  users  832 May 28  2002 /home/username/.cshrc`
	`-rw-r--r--  1 username  users  347 May 28  2002 /home/username/.exrc`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

User directory security	Users' home directories and personal startup files ("dot" files) should have restrictive permissions.

	`-rw-r--r--  1 username  users  334 May 28  2002 /home/username/.login`
	`-rw-r--r--  1 username  users  439 May 28  2002 /home/username/.profile`
	`-rw-------  1 username  users  1402 Aug 27 17:04 /home/username/.sh_history`
	
	Note 1: For users with no home directory, the output will look like this:
	`john's home is /home/john, the permissions are:`
	`  and dot files are:`
	
	These users should definitely be modified to set their home directory to a specific, private directory.
	
	Note 2: ***NO*** users should have "/" as their home directory. If root or other users are set this way, it should be changed immediately. Root should be changed to "/root" (not "/home/root" as /home is frequently moved to different filesystem).

Objective / Subjective	Objective
Findings	
Pass / Fail	

2.4.3 Checklist item #25: Sticky bit on temporary directories

Sticky bit on temporary directories	Is the sticky bit set on temporary directories?
References	• "Center for Internet Security: Level-1 Benchmark (v1.0.4) for HP-UX", p.24. • Jones, p.30. • Rehman, p.111. • Personal experience
Risk Evaluation	Many users create files in temporary directories for sharing with other users or temporary storage. Programs also create files in temporary directories for such purposes as creating a linkage between processes. With the default permissions of directories like "/tmp" and "/var/tmp", any user can delete

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Sticky bit on temporary directories	Is the sticky bit set on temporary directories?
	files in these directories. This becomes a vulnerability when it is realized that the malicious user can also create replacements with the same name. If done quickly enough, the potential exists for several abuses ranging from data modification to exploitation of "race conditions" (where users take advantage of pauses in execution time to modify behavior of programs). **Risk Rating="3".** The skill required to exploit this vulnerability is beyond the abilities of most users of the audit target. Risk still remains, as there is always the possibility of external intruders.
Compliance	Compliance will be measured by examining the permissions on several temporary directories for the existence of a "t" in the last position. If one or more directories are not found, this does not constitute failure of the test. The test passes as long as the directories that do exist have the proper permissions.
Testing	Type `/usr/bin/ls -ld /tmp /var/tmp /var/preserve /var/stm/logs \ /var/stm/catalog /var/spool/cron/tmp`[8]

Expected Output	Output should be similar to the following:
	`/var/stm/catalog not found`
	`drwxrwxrwt 7 bin bin 8192 Aug 27 22:21 /tmp`
	`drwxrwxrwt 2 bin bin 96 Jan 11 2003 /var/preserve`
	`drwxrwxrwt 2 root root 96 Aug 27 22:15 /var/spool/cron/tmp`
	`drwxrwxrwt 5 root other 8192 Aug 26 15:43 /var/stm/logs`
	`drwxrwxrwt 5 bin bin 8192 Aug 27 22:27 /var/tmp`

Objective / Subjective	Objective
Findings	
Pass / Fail	

[8] Jones, p.30

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.4.4 Checklist item #26: Root's home directory

Root's home directory	Has root's home directory been changed from "/"?
References	• Jones, p.15. • Personal Experience
Risk Evaluation	The default home directory for root on many systems is "/". Best practice is to have root's home directory be in a separate location such as "/root". This lessens the possibility that a mistyped command could destroy critical system directories and removes root's personal startup files (.profile, .exrc, etc) to a location where they can be better protected. **Risk Rating="2".** The risk for this item is rated low because it is more of a systems management issue that has security implications.
Compliance	Examine the output of "/usr/sbin/logins –xl root" to determine root' home directory.
Testing	As root, type `/usr/sbin/logins -xl root`

Expected Output	The second line of output indicates the home directory:
	
	`root 0 sys 3`
	`/root`
	`/sbin/sh`
	`PS 000000 -1 -1 -1`

Objective / Subjective	Objective
Findings	
Pass / Fail	

2.4.5 Checklist item #27: Default umask

Default umask	Is the default file mode creation mask 022 or more restrictive?
References	• Personal experience
Risk	The file creation mask governs whether a newly created file can be read from or written to by users other

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Default umask	Is the default file mode creation mask 022 or more restrictive?
Evaluation	than the file's owner. Many system administrators change the default umask value to 022 or something more restrictive. Relaxed permissions on a system create many opportunities for malicious or inattentive users to damage other users' files. **Risk Rating="5".**
Compliance	Compliance will be measured by logging in as root and as a regular user and confirming the umask value is 022 or stricter.
Testing	Test 1a) Login as root and type `/usr/bin/umask` Test 1b) While logged in as root, type `/usr/bin/touch /tmp/testfile.$$; /usr/bin/ls -l /tmp/testfile.$$` Test 2a) Login as regular user and type `/usr/bin/umask` Test 2b) While logged in as a regular user, type `/usr/bin/touch /tmp/testfile.$$; /usr/bin/ls -l /tmp/testfile.$$`
Expected Output	Output 1a) Output must indicate `022` or more restrictive. Output 1b) `-rw-r--r--  1 root  sys  0 Aug 27 13:46 /tmp/testfile.10863` Output 2a) Output must indicate `022` or more restrictive. Output 2b) `-rw-r--r--  1 reguser  users  0 Aug 27 13:48 /tmp/testfile.14321`
Objective / Subjective	Objective (Stimulus/Response test)
Findings	
Pass / Fail	

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.4.6 Checklist item #28: Global "chown" privileges

Global "chown" privileges	Do all users have privileges to change the group designation of a file?
References	• "Building a Bastion Host Using HP-UX 11", Section 5. • Jones, p.12.
Risk Evaluation	HP provides a capability to assign privileges to groups of users. By default all users are given the privilege of changing ownership of files. This opens up possibilities of many types of devious behavior such as changing or deleting other users' files. Best practices suggest disabling this ability via the "/usr/sbin/setprivgrp" command. **Risk Rating="7".** Leaving "chown" privileges enabled unnecessarily makes several privilege escalation methods possible.
Compliance	Compliance will be measured by logging in as a non-privileged user, listing the global privileges, and then attempting to change ownership of a file.

Testing	Test 1) Type `/usr/bin/getprivgrp`
	
	Test 2) Login as a non-privileged user and attempt to change ownership of a test file. Using "user1" as an example, type the following commands:
	`/usr/bin/touch /home/user1/testfile`
	`/usr/bin/ls -l /home/user1/testfile`
	`/usr/bin/chown user2 /home/user1/testfile`
	`/usr/bin/ls -l /home/user1/testfile`

Expected Output	Output 1) Output should show the following header with no privileges listed:
	`global privileges:`
	
	Output 2) Output of the series of commands in Test2 should show:
	`$ /usr/bin/touch /home/user1/testfile`
	`$ /usr/bin/ls -l /home/user1/testfile`
	`-rw-r--r--  1 user1  users  0 Aug 29 11:45 /home/user1/testfile`
	`$ /usr/bin/chown  user2  /home/user1/testfile`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Global "chown" privileges	Do all users have privileges to change the group designation of a file?

	`/home/user1/testfile: Not owner`
	`$ /usr/bin/ls -l /home/user1/testfile`
	`-rw-r--r--  1 user1  users  0 Aug 29 11:45 /home/ user1/testfile`

Objective / Subjective	Objective (Stimulus/Response test)
Findings	
Pass / Fail	

2.4.7 Checklist item #29: SUID/SGID files

SUID/SGID files	Have the default Set-UID and Set-GID files been secured?
References	• "Building a Bastion Host Using HP-UX 11", section 8. • "Center for Internet Security: Level-1 Benchmark (v1.0.4) for HP-UX", p.25. • Wong, p.96. • Jones, p.29. • Personal experience
Risk Evaluation	By default HP-UX ships with many programs and scripts with the SUID bit or the SGID bit set. These SUID and SGID bits allow the programs or scripts to be run with the privileges of the owner (or group respectively) of the file instead of the privileges of the user or group actually executing the file. Vulnerabilities are frequently discovered in scripts with these bits set and they are a prime target for malicious users intent on raising their privileges on the system. A default installation of 11i can have over 150 files with these SUID and SGID enabled files, many of them do not need have these abilities enabled as they will likely be run only by their owners. **Risk Rating="7".** Each company must decide the acceptable tradeoffs between functionality and security for each server. Most SUID/SGID programs can have that ability removed without adversely affecting the function of the system. Changing the permissions on these files can cause some loss of functionality (they can then only be run by root) and will cause the "/usr/sbin/swverify" program to report errors due to

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

SUID/SGID files	Have the default Set-UID and Set-GID files been secured?
	permission changes.
Compliance	This checklist item simply aims to determine if the company has gone to the effort of reducing the number of SUID/SGID scripts. Due to the large number of SUID/SGID files shipped with HP-UX and the many possible combinations left after a company completes an effort of this type, this checklist item will not examine every SUID/SGID file on the system. Compliance will be measured by examining the permissions on a subset of files most likely to have their SUID/SGID ability removed in any lock-down effort. If more than half of these files no longer have their SUID/SGID status, it will be assumed the company has hardened the system to some extent in this area.

Testing	Logged in as root, type
	`/usr/bin/find / \( -perm -4000 -o -perm -2000 \) -type f \`
	`  -exec /usr/bin/ls -l {} \; > /tmp/suid-sgid-tmp.txt`
	
	`/usr/bin/more /tmp/suid-sgid-tmp.txt`
	
	This will produce a file in the /tmp directory to be reviewed.
	
	The list in “Expected Output” shows *a sample* of the files that may be found. The list shows their permissions corrected (without the SUID/SGID). These files were chosen for the sample as they are not used often or probably would be executed by the superuser in regular production and would likely NOT need SUID/SGID. If an effort to close this vulnerability has been performed in the past, these would likely have been cleaned up.
	
	Note: Any files under the /var/adm/sw/save directory should probably NOT need SUID/SGID. These should be examined.
	
	Example of a file that should retain SUID:
	-r-sr-xr-x 1 root bin 24576 Nov 14 2000 /usr/bin/su

Expected	The CIS benchmark identifies several of the following files as “having a history of significant security risk

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

SUID/SGID files	Have the default Set-UID and Set-GID files been secured?

Output	as a result of shipping set-UID, are not required to be set-UID in most circumstances, and therefore are recommended to [have set-UID ability removed]:"[9]
	
	50% or more of this list must be shown to **not** have the SUID or SGID bit set ("s" in the permissions string):
	`-r-xr-xr-x  1 bin  bin  221184 Nov 14  2000 /opt/audio/bin/Aserver`
	`-r-xr-xr-x  1 root  bin  270336 Nov 14  2000 /sbin/shutdown`
	`-r-xr-xr-x  1 root  bin  20480 Nov 14  2000 /usr/bin/bdf`
	`-r-xr-xr-x  1 root  bin  73728 Nov 14  2000 /usr/bin/df`
	`-r-xr-xr-x  1 bin  mail  507904 Nov 14  2000 /usr/bin/elm`
	`-r-xr-xr-x  1 bin  daemon  1699840 Nov 14  2000 /usr/bin/kermit`
	`-r-xr-xr-x  1 uucp  bin  57344 Nov 14  2000 /usr/bin/uucp`
	`-r-xr-xr-x  1 uucp  bin  20480 Nov 14  2000 /usr/bin/uuls`
	`-r-xr-xr-x  1 root  bin  212992 Nov 14  2000 /usr/contrib/bin/X11/xconsole`
	`-r-xr-xr-x  1 root  bin  16384 Nov 14  2000 /usr/lbin/expreserve`
	`-r-xr-xr-x  1 root  bin  20480 Nov 14  2000 /usr/lbin/exrecover`
	`-r-xr-xr-x  1 uucp  bin  118784 Nov 14  2000 /usr/lbin/uucp/uucico`
	`-r-xr-xr-x  1 uucp  bin  32768 Nov 14  2000 /usr/lbin/uucp/uuclean`
	`-r-xr-xr-x  1 uucp  bin  28672 Nov 14  2000 /usr/lbin/uucp/uusched`
	`-r-xr-xr-x  1 uucp  bin  57344 Nov 14  2000 /usr/lbin/uucp/uuxqt`
	`-r-xr-xr-x  11 root  bin  1925120 Oct 24  2002 /usr/sbin/swinstall`
	`-r-xr-xr-x  26 root  sys  528384 Aug  7  2002 /usr/sbin/vgcreate`
	`-r-xr-xr-x  1 bin  tty  16384 Nov 14  2000 /usr/sbin/wall`

Objective / Subjective	Objective
Findings	
Pass / Fail	

[9] "Center for Internet Security: Level-1 Benchmark (v1.0.4) for HP-UX", p.25.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.4.8 Checklist item #30: File integrity software

File integrity software	Is file integrity software (like Tripwire, *swverify*, or *mkpdf*) used to detect (and alert to) changes in critical system files?
References	• Ellis, p.23. • "Man" page for *swverify(1M)* http://docs.hp.com/cgi-bin/onlinedocs.py?mpn=B2355-90692&service=hpux&path=00/01/173&title=HP-UX%20Reference%20%28Volume%204%20of%209%29 • "Man" page for *pdfck(4)* (Compare Product Description File to contents of file system). http://docs.hp.com/cgi-bin/onlinedocs.py?mpn=B2355-90692&service=hpux&path=00/00/55&title=HP-UX%20Reference%20%28Volume%204%20of%209%29 • Tripwire Academic Source Release (free) http://www.tripwire.com/downloads/tripwire_asr/ • Personal experience
Risk Evaluation	Maintaining control over the integrity of the software that is installed on a machine is critical. One way this is accomplished is to create a baseline when a system is installed of many of the critical files with their signatures. This baseline is stored off line or in a read-only archive and periodic comparisons are made to see if anything has changed that should not have changed. Tripwire has been used for years on many different platforms to accomplish this purpose. Tripwire has a commercial product and an "Academic Source Release" that is free and compiles on most UNIX machines. Although it is no longer updated by Tripwire, it still accomplishes its task very well. The IPD (Installed Products Database) is a database on HP-UX that tracks all installations, products and filesets on the system that were added, changed, or removed by the swinstall, swconfig, or swremove programs. Administrators can use the "swverify" command to determine if binaries have changed. **Warning**: Many measures taken to lock down a system for security will cause swverify to give alerts. Steps should be taken so the "false positives" do not drown out other information and cause the administrators to stop using swverify. HP-UX also has PDFs or Product Description Files. These are packages of files that are processed by the "mkpdf" program to create a list of vital information and signatures. This PDF can then be compared

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

File integrity software	Is file integrity software (like Tripwire, *swverify*, or *mkpdf*) used to detect (and alert to) changes in critical system files?
	using "pdfck" or "pdfdiff". As with the other methods, the PDF should be kept in a read-only location to prevent tampering. HP discourages PDF usage[10] because most of its functionality can be found in Software Distributor, but it is still a useful tool for tracking files that may not be in the IPD. **Risk Rating="7".** Tripwire or one of the other tools *if run regularly against write-protected file signatures* will be one of the most likely ways a system administrator will find out about a compromise.
Compliance	With the number of options and the complexity of the available solutions, compliance for this item will be measured by the examination of any company procedures detailing the process of file integrity checking as well as proof that file signatures are being confirmed regularly.

Testing	Test 1) Auditor must review copies of the company procedures addressing file integrity checking and any associated configuration files and results reports.
	
	Test 2) To determine if one of the identified file integrity methods is being automatically run, type:
	`/usr/bin/grep -e tripwire -e swverify -e pdfdiff -e pdfck \`
	`/var/spool/cron/crontabs/* | /usr/bin/more`

Expected Output	Output 1) Expected output would consist of company documents detailing the process for file integrity checking and a recent Tripwire policy file or PDF description file with the resulting output reports. Output 2) Output should indicate regularly scheduled cron jobs for at least one of the file integrity check programs. An example would be: `0 4 * * 5 /usr/sbin/swverify \*` **Note:** The above line is only an example. The actual output would probably have different arguments (or would be for one of the other tools like Tripwire).
Objective / Subjective	Subjective
Findings	
Pass / Fail	

[10] "Man" page for *pdfck(4)*

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.4.9 Checklist item #31: Log file and configuration file permissions

Log file and configuration file permissions	Are the permissions of system log files and configuration files sufficient to prevent regular users from tampering with the contents?
References	• "Center for Internet Security: Level-1 Benchmark (v1.0.4) for HP-UX", p.27. • Personal experience
Risk Evaluation	Log files can be a vital source of information in the event of a suspected system compromise. The log files must have permissions that prevent regular system users from tampering with them. The system configuration files must also be secured to prevent unauthorized changes from damaging the system. **Risk Rating="7".** Confidence in the log files is critical to the security posture of the system and unauthorized changes to system configuration files could cause significant downtime and troubleshooting time.
Compliance	Listings of files that should be secured can be found on pages 27 and 28 of the CIS Benchmark document referenced above. Compliance will be tested by confirming that any log files specified in the /etc/syslog.conf file are not world writable and examining a subset of the files and directories listed in the CIS benchmark.
Testing	Test 1a) Type `/usr/bin/grep -v "^#" /etc/syslog.conf` Test 1b) For any log files listed in the previous step, type `/usr/bin/ls -l <filename>` Test 2) For each of the following files or directories, type `/usr/bin/ls -ld <filename>` (Some may not exist on some systems). • /var/spool/cron/crontabs/root • /var/X11/Xserver/logs/X0.log • /var/adm/automount.log • /var/adm/snmpd.log • /var/opt/dce/svc/fatal.log • /var/opt/dce/svc/warning.log

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Log file and configuration file permissions	Are the permissions of system log files and configuration files sufficient to prevent regular users from tampering with the contents?
	• /var/opt/ignite/recovery/fstab • /var/sam/hpbottom.iout • /var/sam/`/usr/bin/uname –n`.dion (command inside back-ticks provides hostname) • /var/sam/lock • /var/sam/log/samlog • /var/adm/sw/sav • /var/adm/sw/patch • /stand/dlkm • /stand/dlkm.vmunix.prev • /usr/local • /usr/lbin • /var/stm • /usr/share/man • /var/dt/Xerrors • /var/opt/common • /var/spool/sockets/common

Expected Output	Output 1a)
	`mail.debug /var/adm/syslog/mail.log`
	`*.info;mail.none /var/adm/syslog/syslog.log`
	`*.alert /dev/console`
	`*.alert root`
	`*.emerg *`
	
	Output 1b) Output should be similar to the following:
	`-r--r--r-- 1 root root 9298 Aug 27 14:40 /var/adm/syslog/mail.log`
	`-rw-r--r-- 1 root root 396570 Aug 30 12:22 /var/adm/syslog/syslog.log`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Log file and configuration file permissions	Are the permissions of system log files and configuration files sufficient to prevent regular users from tampering with the contents?

	Output 2)
	`-r--------  1 root  sys  2988 Aug 26 18:26 /var/spool/cron/crontabs/root`
	`-rw-r--r--  1 root  root  2717 Aug 26 15:43 /var/X11/Xserver/logs/X0.log`
	`-rw-r--r--  1 root  root  0 Jan 11  2003 /var/adm/automount.log`
	`-rw-r--r--  1 root  root  4168 Aug 27 18:28 /var/adm/snmpd.log`
	`-rw-r--r--  1 bin  bin  0 Jan 11  2003 /var/opt/dce/svc/fatal.log`
	`-rw-r--r--  1 bin  bin  0 Jan 11  2003 /var/opt/dce/svc/warning.log`
	`/var/opt/ignite/recovery/fstab not found`
	`/var/sam/hpbottom.iout not found`
	`/var/sam/HP-UX.dion not found`
	`drwxr-xr-x  2 bin  bin  8192 Aug 24 14:53 /var/sam/lock`
	`-rw-r--r--  1 root  sys  16806 Aug 26 15:43 /var/sam/log/samlog`
	`dr-x------ 85 root  sys  8192 Jan 11  2003 /var/adm/sw/save`
	`/var/adm/sw/patch not found`
	`drwxr-xr-x  6 root  sys  1024 Jan 11  2003 /stand/dlkm`
	`/stand/dlkm.vmunix.prev not found`
	`drwxr-xr-x  9 bin  bin  8192 Jan 11  2003 /usr/local`
	`dr-xr-xr-x 11 bin  bin  8192 Aug 26 22:50 /usr/lbin`
	`drwxr-xr-x  5 root  other  96 Jan 11  2003 /var/stm`
	`dr-xr-xr-x 36 bin  bin  8192 Jan 11  2003 /usr/share/man`
	`-rw-r--r--  1 root  root  220 Aug 27 18:18 /var/dt/Xerrors`
	`drwxr-xr-x  2 root  sys  96 Jan 11  2003 /var/opt/common`
	`drwxr-xr-x  2 root  sys  96 Jan 11  2003 /var/spool/sockets/common`

Objective / Subjective	Objective
Findings	
Pass / Fail	

2.4.10 Checklist item #32: Use of cron/at

Use of cron/at	Is the use of “cron/at” by regular users restricted?

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Use of cron/at	Is the use of “cron/at” by regular users restricted?
References	• Rehman, p.463. • Personal experience
Risk Evaluation	The ability to schedule jobs is frequently reserved for system administrators and power users such as database administrators. Ability to schedule jobs using the “cron” and “at” commands can be restricted using the “/var/adm/cron/cron.allow” and /var/adm/cron/at.allow” files. **Risk Rating=”5”.** Allowing all regular users access to “cron” and “at” is not a direct avenue for system compromise, but it could be abused to circumvent system security.
Compliance	The best way to restrict use of “cron” and “at” is to have authorized users listed in the /var/adm/cron/cron.allow and /var/adm/cron/at.allow files. The “cron.deny” and “at.deny” companions to these files need not be used. Compliance will be measured by ensuring that some combination of allow and deny files exists that allows only authorized users access to “cron” and “at”. Rehman includes a useful chart on page 463 of his book detailing the rules of precedence for these files, it is reproduced below: ***Role of cron Files to Allow/Deny User of cron*** **cron.allow** **cron.deny** **Effect on user** Not exists Not exists Only the root user can use cron. Not exists Exists

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Use of cron/at	Is the use of “cron/at” by regular users restricted?
	All users except those listed in cron.deny can use cron. Not exists Exists (empty) All users can use cron. Exists Not exists Only those users listed in the cron.allow file can use cron. Exists Exists Only those users listed in the cron.allow file can use cron. Exists (empty) Not exists Only the root user can use cron. Exists (empty) Exists Only the root user can use cron.
Testing	In the /var/adm/cron directory, examine the contents of cron.allow, cron.deny, at.allow, and at.deny.
Expected Output	Best practice would be to have no cron.deny or at.deny files and have only authorized users in cron.allow and at.allow files.
Objective / Subjective	Subjective
Findings	

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Use of cron/at	Is the use of "cron/at" by regular users restricted?
Pass / Fail	

2.4.11 Checklist item #33: Buffer overflow protection mechanism

Buffer overflow protection mechanism	Is the buffer overflow protection currently enabled on this system (provided by the "executable_stack" kernel parameter)?
References	• Wong, p121. • "Center for Internet Security: Level-1 Benchmark (v1.0.4) for HP-UX", p.20. • Personal experience
Risk Evaluation	"Buffer overflow" attacks are attacks in which a vulnerable program is fed incorrect input and consequently executes commands not intended by the program's authors. This is a general, well-known problem affecting programs on many different types of systems. Starting in HP-UX 11i, HP has provided a kernel parameter ("executable_stack") which can be configured to prevent buffer overflow from being executed. **Risk Rating="4".** The risk to the audit target from buffer overflow attacks seems low, as the environment is fairly stable. However, the solution is easy to implement and it should not adversely affect the running of the system. Buffer overflows are so common that it is definitely recommended for the system administrators to implement this feature if they have not already done so.
Compliance	Compliance will be measured by querying the current kernel to determine the setting of the "executable_stack" kernel parameter.
Testing	Type `/usr/sbin/kmtune -q executable_stack`

Expected Output	Output should be:
	`Parameter  Current Dyn Planned  Module  Version`
	`==========`
	`executable_stack  0  -  0`
	
	A "Current" setting of "0" indicates that stacks cannot be executable, a "1" indicates that all program stacks

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Buffer overflow protection mechanism	Is the buffer overflow protection currently enabled on this system (provided by the "executable_stack" kernel parameter)?
	are executable, and a "2" also indicates that the stacks cannot be executable but the process will not terminate and a non-fatal warning will be issued.[11]
Objective / Subjective	Objective
Findings	
Pass / Fail	

2.4.12 Checklist item #34: Retirement of old media

Retirement of old media	Are old hard drives, backup tapes, and disaster recovery tapes sanitized when they are retired or redeployed?
References	• Personal experience
Risk Evaluation	All of the expensive measures taken to secure data and network ports can be circumvented by a janitor pulling an old disaster recovery tape out of the dumpster. Recent news stories of hard drives purchased in online auctions being found to contain a wealth of corporate data have many companies reevaluating their media retirement/redeployment strategies. **Risk Rating="7".** Personal experience of the auditor has shown many companies with a blind spot in this area.
Compliance	Due to the scope and length constraints of this project, discussions of forensic data recovery and details of "how many overwrites is good enough?" will be left for the reader to research. Compliance will be measured by a review of company policies addressing disposition of end-of-life media. Contemporaneous records indicating such media was destroyed or adequately erased will also constitute compliance.

[11] Wong,p121.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Retirement of old media	Are old hard drives, backup tapes, and disaster recovery tapes sanitized when they are retired or redeployed?
Testing	Review any company policies addressing media retirement and any logs of such activities.
Expected Output	Policies should call for secure disposal or erasure of old hard drives, backup tapes, disaster recovery tapes, and any other media containing files from the audit target.
Objective / Subjective	Objective
Findings	
Pass / Fail	

2.5 Control Objective: Verify that the administrators are monitoring the system.

2.5.1 Checklist item #35: Root's mail must be read in a timely manner

Root's mail must be read in a timely manner.	Is root's mail being read and/or forwarded to administrator's work e-mail addresses for review and action?
References	• Personal experience
Risk Evaluation	Many programs try to alert the administrators by sending mail to the root user. If no attention is given to the messages in root's mailbox, system events could go unchecked. **Risk Rating="7".** Lack of attention to root's mail may not directly allow a compromise, but it is critical for early detection of system and security problems.
Compliance	It is difficult to prove that someone is watching the mail. Compliance for this item will be measured by either of the following tests being positive. • There must either be no more than two business days of new e-mail in root's mail file • root's mail must be forwarded to one or more system administrator's business e-mail address (with the assumption that it is read and acted upon).
Testing	Test 1) To get a list of mail message headers, while logged in as root, type `/usr/bin/mailx -H` Test 2a) Type `/usr/bin/cat ~root/.forward`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Root's mail must be read in a timely manner.	Is root's mail being read and/or forwarded to administrator's work e-mail addresses for review and action?
	Test 2b) Type `/usr/bin/grep "^root" /etc/mail/aliases`
Expected Output	Output 1) Output should consist of one mail header per line. There should be no more than two business days worth of new mail (denoted by an "N" in leftmost field). Output 2a) Output should consist of a list of e-mail addresses to which root's mail is currently forwarded. Output 2b) `root : adminname@xyzmfg.com`
Objective / Subjective	Subjective
Findings	
Pass / Fail	

2.5.2 Checklist item #36: System logs must be reviewed on a regular schedule

System logs must be reviewed on a regular schedule.	Are system logs being reviewed on a regular schedule?
References	• Wong, p.336. • Personal experience
Risk Evaluation	On many systems, a system administrator who is performing a routine check of log files will be the first to discover possible intrusions and other system events. **Risk Rating="7".** Although it is one of the more easily overlooked administrative functions, it is vital that knowledgeable administrators routinely evaluate system log files and investigate any unusual entries.
Compliance	As with reading root's mail, it is sometimes difficult to prove that someone is reviewing the system log files. This test is one of the few in the audit that is not purely objective.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

System logs must be reviewed on a regular schedule.	Are system logs being reviewed on a regular schedule?
	Unfortunately, compliance for this item will be measured by interviewing the system administrator to ascertain the frequency with which the log files are reviewed.
Testing	At a minimum, the following log files should be reviewed on a weekly basis: • Examine /var/adm/syslog/syslog.log • Examine /var/adm/sulog • Examine /var/adm/syslog/mail.log • Examine /etc/rc.log Page 336 of Chris Wong's HP-UX Security book lists several good open source tools to assist with log rotation and review.
Expected Output	As this test consists of an interview question, the expected output for compliance would be information to the effect that system administrators consistently review the above mentioned logs at least weekly.
Objective / Subjective	Subjective
Findings	
Pass / Fail	

2.5.3 Checklist item #37: Regular vulnerability assessments

Regular vulnerability assessments	Are vulnerability assessments addressed in company policy and regularly run against this machine?
References	• Personal experience
Risk Evaluation	New vulnerabilities are discovered regularly by security researchers on both sides of the law. A system that is configured securely to one administrator's experience level will face threats months later that didn't exist when the system was originally configured. Company policy should call for the regular assessment of system security by administrators or auditors and by the use of third party

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Regular vulnerability assessments	Are vulnerability assessments addressed in company policy and regularly run against this machine?
	vulnerability assessment tools. These tools are updated regularly, used extensively in the security profession, and can catch issues that manual examination of a system might miss. A survey of the "Top 75 Security Tools" (as reported by users of the popular "nmap" network scanner) can be found at http://www.insecure.org/tools.html. This list contains descriptions and links to many commercial and Open Source security tools including vulnerability assessment tools such as Nessus and SARA. **WARNING:** Any tools to be used in securing a system should be tested on a non-production system *before* being used on a production system. Tools like "nmap" and "Nessus" can cause unpredictable behavior on a system such as causing network services to stop responding or even crashing the target machine. Great care should be taken that a security audit of a machine does not turn into a denial-of-service attack. **Risk Rating="8".** With new vulnerabilities being reported regularly and the security landscape changing constantly, continual vigilance is required.
Compliance	Compliance will be measured by the review of company policies and procedures addressing regular security checks or audits and the use of vulnerability assessment tools. Proof of the regular execution of these checks or audits must also be reviewed. Such proof can consist of output reports from automated tools, reports from internal/external auditors, or logs of checks run by system administrators.
Testing	Review company policies, procedures, log books, and audit reports addressing regular vulnerability assessments.
Expected Output	Documentation must show that periodic assessments are authorized, required, and have been performed periodically (if frequency is not specified in company documentation, evidence should show a review within the past year).
Objective / Subjective	Objective

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Regular vulnerability assessments	Are vulnerability assessments addressed in company policy and regularly run against this machine?
Findings	
Pass / Fail	

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3 Audit Evidence

3.1 Execution of the audit

The audit of XYZ Mfg's rp5470 was completed without complications. The checklist developed for this audit and detailed in Audit Checklist starting on page 12 was successfully followed in the presence of the primary system administrator.

Notes:

- Several of the checklist items begin by calling for a review of company policy or procedure documents relating to a specific topic. The system administrators indicated that XYZ Mfg. had no IT related policies.
- The audit was scheduled by XYZ to occur during business hours. Due to XYZ's concerns about any possible interruption of normal processing, third-party software such as "nmap" for network scans, "nessus" for vulnerability scans, and The Center For Internet Security's Benchmark and Scoring Tool were removed from the audit by request.
- The "script" command was used to track all screen input and output for later review. A copy of the resulting file was given to the system administrators in the event that some process used by the auditor was questioned.
- **Suggestion:** When using "script" to track steps during execution of a checklist, mark the beginning of each checklist item by executing a command line like "/usr/bin/echo Now testing item 01". This makes searching the resulting typescript output file much easier. The auditor can also use this technique to leave notes regarding odd output or suggestions for further research.

A simple chart describing the "Pass/Fail" results of the audit is provided below and is followed by a selection of checklist items for review. Checklist items were selected for inclusion based on their risk rating or their ability to illustrate the auditing process. For ease of reading, entire checklist item tables have not been copied from Assignment #2. A table similar to the original checklist table will be presented with "Actual Output" and appropriate detail added to the "Findings" and "Pass/Fail" sections. Any exceptions to the checklist item are noted.

3.1.1 Audit Results Summary Table

Checklist Item	Risk Rating	Pass	Fail

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Control Objective: Verify the system's network services are configured securely.			
#01 System time synchronization	4		4
#02 Unnecessary services being started	9		9
#03 Internet daemon logging	5		5
#04 Services brokered by inetd	9		9
#05 TCP Wrappers	9		9
#06 Internet daemon security file	7		7
#07 Secure Shell	10		10
#08 Trust relationships	9	9	
#09 Sendmail configuration	7		7
#10 CDE access	8		8
#11 Banners	5		5
#12 Modems	8	8	
Control Objective: Verify that the system is patched regularly according to company policy.			
#13 Security patches	10		10
#14 Operating system patches	9		9
Control Objective: Verify that access to the system is properly controlled.			
#15 Shadow passwords	9		9
#16 Minimum password length	8	8	
#17 Empty passwords	9		9
#18 Weak passwords	9		9
#19 Duplicate superuser accounts	7	7	
#20 Root login restricted	6		6
#21 Unneeded system accounts	5		5
#22 Path variable for root	5	5	
Control Objective: Verify that access and modification are properly controlled for sensitive files			
#23 Change control	3		3
#24 User directory security	6		6
#25 Sticky bit on temporary directories	3		3
#26 Root's home directory	2		2

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

#27 Default umask	5		5
#28 Global “chown” privileges	7		7
#29 SUID/SGID files	7		7
#30 File integrity software	7		7
#31 Log file and configuration file permissions	7		7
#32 Use of cron/at	5		5
#33 Buffer overflow protection mechanism	4		4
#34 Retirement of old media	7		7
Control Objective: Verify that the administrators are monitoring the system.			
#35 Root’s mail must be read in a timely manner	7	7	
#36 System logs must be reviewed on a regular schedule	7		7
#37 Regular vulnerability assessments	8		8
totals	**252**	**49 (19%)**	**203 (81%)**

3.1.2 Audit Results of Checklist item #02: Unnecessary services being started

- Full checklist item with references and risk evaluation on page 14
- Analysis of findings is in section 4.2.1 “Findings for Objective: Verify the system’s network services are configured securely” on page 104

Unnecessary services being started	Are any services being allowed to start from the scripts in /etc/rc.config.d which are not needed by the system and are disallowed by company policy?
Compliance	Compliance will be measured against the company’s documented list of acceptable services. In the absence of such a document, the exception will be noted and a few of the services known to have a history of vulnerability will be examined.
Testing	Test 1) Examine copies of any company policies and procedures detailing acceptable services. Test 2) As root, type `/usr/bin/grep -v “^#” /etc/rc.config.d/* | /usr/bin/grep “=1” | /usr/bin/more`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Unnecessary services being started	Are any services being allowed to start from the scripts in /etc/rc.config.d which are not needed by the system and are disallowed by company policy?
	Test 3) As root, type `/usr/bin/grep -v "^#" /etc/rc.config.d/* | /usr/bin/grep "=0" | /usr/bin/more`

Actual Output	Output 1) No documents were available for review.
	
	Output 2)
	`Dmiconfig:START_DMI=1`
	`Rpcd:START_RPCD=1`
	`SnmpCmdVw:SNMP_CMDVW_START=1  # Start the commandview SNMP subAgent.`
	`SnmpHpunix:SNMP_HPUNIX_START=1  # Start the hp-unix MIB SNMP subAgent by default.`
	`SnmpMaster:SNMP_MASTER_START=1  # Start the master SNMP agent.`
	`SnmpMib2:SNMP_MIB2_START=1  # Start the MIB2 SNMP subAgent.`
	`SnmpTrpDst:SNMP_TRAPDEST_START=1  # Start the master SNMP agent.`
	`apacheconf:APACHE_START=1`
	`auditing:PRI_SWITCH=1000`
	`auditing:SEC_SWITCH=1000`
	`clean:CLEAN_ADM=1`
	`clean:CLEAN_UUCP=1`
	`clean_tmps:LIST_TEMPS=1`
	`clean_uucp:CLEAN_UUCP=1`
	`comsec:TTSYNCD=1`
	`crashconf:CRASHCONF_ENABLED=1`
	`crashconf:CRASHCONF_READ_FSTAB=1`
	`cron:CRON=1`
	`diagnostic:DIAGNOSTICS=1`
	`dial.conf:OPENDIAL_START=1`
	`ems:EMS_ENABLED=1`
	`emsagtconf:AUTOSTART_EMSAGT=1`
	`envd:ENVD=1`
	`fc_td_conf:FC_TD_START=1`
	`ha.conf:HOSTAGENT_START=1`
	`hparamgr:HPARAMGR_START_STOP=1`
	`hparray:HPARRAY_START_STOP=1`
	`hpfcmsconf:FCMS_START=1`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Unnecessary services being started	Are any services being allowed to start from the scripts in /etc/rc.config.d which are not needed by the system and are disallowed by company policy?

	`kminit:KM_INIT=1`
	`list_mode:USE_COLOR=1`
	`lp:LP=1`
	`mailservs:export SENDMAIL_SERVER=1`
	`mwa:MWA_START=1`
	`netconf:LOOPBACK_ADDRESS=127.0.0.1`
	`netconf:IP_ADDRESS[0]=192.64.206.3`
	`netconf:ROUTE_GATEWAY[0]=192.64.206.1`
	`netconf:ROUTE_COUNT[0]=1`
	`netdaemons:START_RBOOTD=1`
	`nettl:NETTL=1`
	`nettl:  NETTL_CONSOLE=1`
	`nfsconf:NFS_CLIENT=1`
	`nfsconf:NFS_SERVER=1`
	`nfsconf:START_MOUNTD=1`
	`pd:PD_CLIENT=1`
	`pdcinfo:PDCINFO=1`
	`ptydaemon:PTYDAEMON_START=1`
	`pwgr:PWGR=1`
	`scrdaemon:SCR_DAEMON=1`
	`syncer:SYNCER=1`
	`vt:VTDAEMON_START=1`
	`wdog.conf:HOSTWATCHDOG_START=1`
	
	Output 3)
	`Dmiconfig:DMI_IGNORECONFIGURECHECK=0`
	`ServCtlMgr:SCM_START_AGENT=0`
	`ServCtlMgr:SCM_START_CMS=0`
	`acct:START_ACCT=0`
	`apacheconf:WEBMIN_START=0`
	`apacheconf:TOMCAT_START=0`
	`audio:AUDIO_SERVER=0`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Unnecessary services being started	Are any services being allowed to start from the scripts in /etc/rc.config.d which are not needed by the system and are disallowed by company policy?
	auditing:AUDITING=0 cifsclient:RUN_CIFSCLIENT=0 clean_tmps:CLEAR_TMP=0 crashconf:CRASHCONF_REPLACE=0 dce:DCED=0 dce:ACTIVATE_SECVAL=0 dce:AUDITD=0 dce:SECD=0 dce:CDSADV=0 dce:CDSD=0 dce:GDAD=0 dce:DTSD=0 dce:DTS_NULL_PROVIDER=0 dce:DTS_NTP_PROVIDER=0 dce:DTS_SPECTRACOM_PROVIDER=0 dce:PWD_STRENGTHD=0 dce:ILOGIND=0 eus:RUN_EUSRV=0 i4lmd:START_I4LMD=0 kl:KL=0 list_mode:LIST_MODE=0 list_mode:LIST_TIMEOUT=0 namesvrs:NAMED=0 namesvrs:NIS_MASTER_SERVER=0 namesvrs:NIS_SLAVE_SERVER=0 namesvrs:NIS_CLIENT=0 namesvrs:NISPLUS_SERVER=0 namesvrs:NISPLUS_CLIENT=0 netconf:DHCP_ENABLE[0]=0 netconf:GATED=0 netconf:RDPD=0 netconf:RARP=0 netdaemons:export XNTPD=0 netdaemons:export MROUTED=0

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Unnecessary services being started	Are any services being allowed to start from the scripts in /etc/rc.config.d which are not needed by the system and are disallowed by company policy?

	`netdaemons:export RWHOD=0`
	`netdaemons:export DDFA=0`
	`nfsconf:PCNFS_SERVER=0`
	`nfsconf:AUTOMOUNT=0`
	`nfsconf:AUTOFS=0`
	`pd.OLD:PD_CLIENT=0`
	`pwgr:PWGRD_WITH_NISPLUS=0`
	`samba:RUN_SAMBA=0`
	`set_date:DATE_TIMEOUT=0`
	`slsd:SLSD_DAEMON=0`
	`webadmin:WEBADMIN=0`
	`xfs:RUN_X_FONT_SERVER=0`

Objective / Subjective	Subjective
Findings	In the absence of company documentation defining what services are allowed and not allowed, this test becomes more subjective. The "Expected Output" section on page 14 will be used to measure compliance. All of the services listed in that section (rpcd, snmp, mailservs, and nfs) were found to be enabled. Discussion with the system administrators revealed that the only service in that list that they knew they were running was nfs. Services that are shown as not enabled but probably should be, are: ntp (addressed in Checklist item #01: System time synchronization) and auditing. Both services greatly aid in troubleshooting and problem resolution, thereby reducing downtime. These results indicate that the services enabled by the files in /etc/rc.config.d have either not been secured or have only been lightly secured. There are no business reasons to have rpc, sendmail, and snmp enabled on this server if they are not being used. NFS is only being used for light file sharing for administrative purposes and could easily be migrated off of this server to a less critical machine.
Pass / Fail	Fail

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3.1.3 Audit Results of Checklist item #04: Services brokered by the Internet daemon

- Full checklist item with references and risk evaluation on page 17
- Analysis of findings is in section 4.2.1 "Findings for Objective: Verify the system's network services are configured securely" on page 104

Services brokered by the Internet daemon	Are any services being started by the inetd daemon that are not necessary to the function of this server and are disallowed by company policy?
Compliance	Compliance will be measured against the company's documented list of acceptable services. In the absence of such a document, the exception will be noted and a few of the services known to have a history of vulnerability will be examined (bootps, chargen, daytime, discard, echo, exec, finger, ident, ntalk, login, rpc, shell, tftp, time, uucp). ftp and telnet may be required by business need, but should be replaced with ssh as soon as possible. Use of ftp and telnet will not constitute non-compliance with this checklist item.
Testing	Test 1) Examine any company policies which address acceptable network services. Test 2) To get a list of services currently being brokered by inetd, type: `/usr/bin/grep -v "^#" /etc/inetd.conf`

Actual Output	Output 1) No documents were available for review.
	
	Output 2)
	`ftp stream tcp nowait root /usr/lbin/ftpd ftpd -l`
	`telnet stream tcp nowait root /usr/lbin/telnetd telnetd`
	
	`bootps dgram udp wait root /usr/lbin/bootpd bootpd`
	`login stream tcp nowait root /usr/lbin/rlogind rlogind`
	`shell stream tcp nowait root /usr/lbin/remshd remshd`
	`exec stream tcp nowait root /usr/lbin/rexecd rexecd`
	`ntalk dgram udp wait root /usr/lbin/ntalkd ntalkd`
	`ident stream tcp wait bin /usr/lbin/identd identd`
	
	`printer stream tcp nowait root /usr/sbin/rlpdaemon rlpdaemon -i`
	
	`daytime stream tcp nowait root internal`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Services brokered by the Internet daemon	Are any services being started by the inetd daemon that are not necessary to the function of this server and are disallowed by company policy?

	`daytime dgram udp nowait root internal`
	`time stream tcp nowait root internal`
	`echo stream tcp nowait root internal`
	`echo dgram udp nowait root internal`
	`discard stream tcp nowait root internal`
	`discard dgram udp nowait root internal`
	`chargen stream tcp nowait root internal`
	`chargen dgram udp nowait root internal`
	
	`kshell stream tcp nowait root /usr/lbin/remshd remshd -K`
	`klogin stream tcp nowait root /usr/lbin/rlogind rlogind -K`
	
	`dtspc stream tcp nowait root /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd`
	`rpc xti tcp swait root /usr/dt/bin/rpc.ttdbserver 100083 1 /usr/dt/bin/rpc.ttdbserver`
	`recserv stream tcp nowait root /usr/lbin/recserv recserv -display :0`
	`rpc dgram udp wait root /usr/dt/bin/rpc.cmsd 100068 2-5 rpc.cmsd`
	`swat stream tcp nowait.400 root /opt/samba/bin/swat swat`
	`registrar stream tcp nowait root /etc/opt/resmon/lbin/registrar`
	`/etc/opt/resmon/lbin/registrar`
	`pop3 stream tcp nowait root /usr/facetwin/sys/fct_pop3d fct_pop3d`
	`netbios_ssn stream tcp nowait root /usr/facetwin/sys/fct_nbsd fct_nbsd`
	`tftp dgram udp wait root /usr/lbin/tftpd tftpd\`
	`/opt/ignite\`
	`/var/opt/ignite`
	`instl_boots dgram udp wait root /opt/ignite/lbin/instl_bootd instl_bootd`

Objective / Subjective	Subjective
Findings	No policies exist to determine which services may be provided. In the absence of a company policy, the fifteen likely unnecessary services listed in the “Compliance” section of this item were examined; all but two were found enabled (finger and uucp). These results seem to indicate that an initial “lock-down” of network services had not yet taken

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Services brokered by the Internet daemon	Are any services being started by the inetd daemon that are not necessary to the function of this server and are disallowed by company policy?
	place. Some of these enabled services have a history of being exploited, while others can be used to cause a denial-of-service attack on the server. Earlier in this report the threat of a determined insider was considered a more likely threat than an outside intruder. An insider would know the most opportune time for a denial-of-service attack to cause maximum disruption to production (month-end, year-end, deadline for large orders, etc.). The assets to be protected are not only the data but also the availability of that data. Given these considerations, effort should be focused on researching and disabling any services the company deems unnecessary.
Pass / Fail	Fail

3.1.4 Audit Results of Checklist item #05: TCP Wrappers

- Full checklist item with references and risk evaluation on page 20
- Analysis of findings is in section 4.2.1 "Findings for Objective: Verify the system's network services are configured securely" on page 104

TCP Wrappers	Is the system making use of TCP Wrappers to secure network services?
Compliance	Compliance will be determined by verifying several component programs are on the system, checking for tcpwrap usage in inetd.conf, examining the allow/deny files, and attempting to connect to a service that the configuration files indicate is protected.
Testing	Test 1) Type **`/usr/bin/ls -l /usr/lbin/tcpd  /usr/bin/tcpdchk /opt/tcpwrap/bin/tcpd`** Test 2) Type **`/usr/bin/grep tcpwrap /etc/inetd.conf`** Test 3) Type **`/usr/bin/more /etc/hosts.allow /etc/hosts.deny`** **Note:** Chris Wong notes on page 266 of her book that TCP Wrapper follows these two rules: • Search the /etc/hosts.allow file. If a match is found, service is allowed. If no match is found, continue to next rule.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

TCP Wrappers	Is the system making use of TCP Wrappers to secure network services?
	• Search the /etc/hosts.deny file. If a match is found, service is denied. If no match is made, *the service is allowed*. **This default "fall through" and the use of wildcard words such as "ALL: ALL" must be considered when building allow/deny files.** Test 4) Given the two rules listed above and the output of Test 3) try to connect to a service that is protected by TCP Wrappers from a host that is not allowed.

Actual Output	Output 1)
	`/usr/lbin/tcpd not found`
	`/usr/bin/tcpdchk not found`
	`/opt/tcpwrap/bin/tcpd not found`
	
	Output 2)
	<no output>
	
	Output 3)
	`/etc/hosts.allow: No such file or directory`
	`/etc/hosts.deny: No such file or directory`
	
	Output 4) No services are protected by TCP Wrappers, so Test 4 is not applicable in this case.

Objective / Subjective	Objective (Stimulus/Response test)
Findings	TCP Wrappers is not installed on this system. The /var/adm/inetd.sec file is also not being used to secure network services (discovered while auditing Checklist item #06: Internet daemon security file, but not included in these audit results). As mentioned earlier, TCP Wrappers allows access control based on IP address and enhanced logging which can be used to find evidence of suspicious activity. Implementation of TCP Wrappers is a highly recommended step in securing this server, especially if telnet and ftp are used regularly as is the case on this system.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

TCP Wrappers	Is the system making use of TCP Wrappers to secure network services?
Pass / Fail	Fail

3.1.5 Audit Results of Checklist item #07: Secure Shell

- Full checklist item with references and risk evaluation on page 23
- Analysis of findings is in section 4.2.1 "Findings for Objective: Verify the system's network services are configured securely" on page 104

Secure Shell	Is ssh used instead of telnet and ftp?
Compliance	Compliance will be measured by confirming that there are no telnetd or ftpd daemons listening, that ssh is installed and accessible from the network.
Testing	Test 1) Type `/usr/bin/netstat -af inet | /usr/bin/grep telnet` Test 2) Type `/usr/bin/netstat -af inet | /usr/bin/grep ftp` Test 3) Type `/usr/bin/ssh -V` (capital V) Test 4) From a different host, try to use ssh to connect to the audit target. Type `ssh username@audittarget.xyzmfg.com`

Expected Output	Output 1) `tcp 0 0 *.telnet *.* LISTEN`
	
	Output 2)
	`tcp 0 0 *.ftp *.* LISTEN`
	`udp 0 0 *.tftp *.*`
	
	Output 3) `sh: /usr/bin/ssh: not found.`
	
	Output 4) `18727: ssh: connect to host audittarget.xyzmfg.com port 22: Connection refused`

Objective / Subjective	Objective (Stimulus/Response test)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Secure Shell	Is ssh used instead of telnet and ftp?
Findings	SSH is not installed on this system, telnet and ftp are still being used for access and file transfer. The advantages of using ssh instead of telnet and ftp for access and file transfer have been stated (no clear text passwords, increased access control, encrypted traffic). While the risk of unauthorized access to the system can never be totally eliminated, use of ssh will go a long way toward achieving that goal.
Pass / Fail	Fail

3.1.6 Audit Results of Checklist item #11: Banners

- Full checklist item with references and risk evaluation on page 30
- Analysis of findings is in section 4.2.1 "Findings for Objective: Verify the system's network services are configured securely" on page 104

Banners	Do system banners provide version numbers or are unnecessarily welcoming?
Compliance	The auditor will examine the /etc/motd, /etc/issue, /etc/ftpd/ftpaccess, and /etc/inetd.conf files as well as attempt connections to the ftp and telnet services. Compliance will be measured by assuring there are no version numbers of the operating system or system services and there is verbiage indicating that access to the system is for authorized users and for official purposes only.
Testing	Test 1) Type **`/usr/bin/cat /etc/motd`** and **`/usr/bin/cat /etc/issue`** Test 2a) If ftp is being used, test that a banner is configured by typing: **`/usr/bin/grep banner /etc/ftpd/ftpaccess`** Test 2b) If ftp is being used, verify the banner by attempting to connect to the machine. Test 3a) If telnet is being used, test that the daemon is configured to not display a banner by typing: **`/usr/bin/grep telnetd /etc/inetd.conf`** Test 3b) If telnet is being used, verify the banner is turned off by attempting to connect to the machine via telnet.
Actual	Output 1)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Banners	Do system banners provide version numbers or are unnecessarily welcoming?

Output	`cat: Cannot open /etc/motd: No such file or directory`
	and
	`GenericSysName [HP Release B.11.11] (see /etc/issue)`
	
	Output 2a) `grep: can't open /etc/ftpd/ftpaccess`
	
	Output 2b)
	`Connected to audittarget.xyzmfg.com.`
	`220 audittarget.xyzmfg.com FTP server (Version 1.1.214.4(PHNE_23950) Tue May 22 05:49:01 GMT 2001) ready.`
	`Name (audittarget:username):`
	`331 Password required for username.`
	`Password:`
	`230 User username logged in.`
	`Remote system type is UNIX.`
	`Using binary mode to transfer files.`
	`ftp> quit`
	`221 Goodbye.`
	
	Output 3a) `telnet stream tcp nowait root /usr/lbin/telnetd telnetd`
	
	Output 3b)
	`Trying...`
	`Connected to audittarget.xyzmfg.com.`
	`Escape character is '^]'.`
	`Local flow control on`
	`Telnet TERMINAL-SPEED option ON`
	
	`HP-UX audittarget B.11.11 U 9000/800 (ta)`
	
	`login:`
	`telnet> quit`
	`Connection closed.`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Banners	Do system banners provide version numbers or are unnecessarily welcoming?
Objective / Subjective	Objective (Stimulus/Response test)
Findings	The /etc/motd does not exist and the /etc/issue banner provides the version of HP-UX being run. The banner for ftp gives the exact version number of the ftp server and telnet gives the version of HP-UX. These banners provide an attacker with information he can use to research possible exploits for attacking this machine. Research and legal counsel should be consulted regarding proper wording for banners. The banners provided by ftp and telnet can be turned off.
Pass / Fail	Fail

3.1.7 Audit Results of Checklist item #13: Security patches

- Full checklist item with references and risk evaluation on page 34
- Analysis of findings is in section 4.2.2 "Findings for Objective: Verify that the system is patched regularly according to the company's patching strategy" on page 105

Security patches	Is HP's Security Patch Checker tool run regularly?
Compliance	Compliance will be measured by the determination that HP's Security Patch Checker is installed on the audit target, configured to run regularly (at least weekly), and configured to mail the results to an administrator.
Testing	Test 1) As root, type `/usr/bin/ls -l /opt/sec_mgmt/spc/bin/security_patch_check` Test 2) As root, type `/usr/bin/grep security_patch_check /var/spool/cron/crontabs/*` Test 3) Examine evidence that the security_patch_check tool successfully sent mail to the administrator(s) regarding available security patches.
Actual Output	Output 1) `/opt/sec_mgmt/spc/bin/security_patch_check not found` Output 2) `<no output>`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Security patches	Is HP's Security Patch Checker tool run regularly?
	Output 3) The Security Patch Check tool is not installed, so Test 3 is not applicable.
Objective / Subjective	Objective
Findings	The Security Patch Checker tool is not installed. With the constant emergence of new threats such as worms, viruses, and new exploits for network services, automatic execution of the Security Patch Checker tool is **highly** recommended. Once configured, this tool will notify the system administrators of new security patches that need to be applied. It should be run at least weekly.
Pass / Fail	Fail

3.1.8 Audit Results of Checklist item #15: Shadow Passwords

- Full checklist item with references and risk evaluation on page 38
- Analysis of findings is in section 4.2.3 "Findings for Objective: Verify that access to the system is properly controlled" on page 106

Shadow Passwords	Are Shadow Passwords used on this machine?
Compliance	Compliance will be measured by the meeting of the following two criteria: • Existence of the /etc/shadow file (with file size larger than 0). • Existence of a single "x" in every user's password field in the /etc/passwd file.
Testing	Test 1) Type `/usr/bin/ls -l /etc/shadow` Test 2) Type `/usr/bin/awk -F: '{print $2}'  /etc/passwd | /usr/bin/sort -u`
Actual Output	Output 1) `/etc/shadow not found` Output 2) Output consisted of one "*" followed by a sorted list of hashed passwords. No "x" passwords were listed. The hashed passwords are not listed here due to the possibility they could be cracked and reveal information about the company.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Shadow Passwords	Are Shadow Passwords used on this machine?
Objective / Subjective	Objective
Findings	The Shadow Password software is not installed and used on this machine. This means that all passwords are stored in a file that can be retrieved by any user on the system. This user could copy the file to a diskette or e-mail it to an external address and run a "password cracker" against it at their leisure. Retrieval and cracking of the password file is one of the most likely steps a malicious user would take to compromise a system. Successful cracking of the password file would allow the malicious user to access the system as any user whose password was discovered. If root's password were discovered (and abused), the malicious user could cause such mischief as reformatting or corrupting system files or drives and modifying the manufacturing or shipping data to cause damage or loss of product.
Pass / Fail	Fail

3.1.9 Audit Results of Checklist item #17: Empty passwords

- Full checklist item with references and risk evaluation on page 41
- Analysis of findings is in section 4.2.3 "Findings for Objective: Verify that access to the system is properly controlled" on page 106

Empty passwords	Are there any users in the password file with empty or null passwords?
Compliance	No accounts on this machine should have empty passwords.
Testing	While logged in as root, type `/usr/sbin/logins -p`

Actual Output	Twenty-three of the fifty-five accounts in the password file were reported to have empty passwords.
	
	Actual output would be included in a report being presented to a customer, but to preserve anonymity only a sample of fictitious names will be presented here.
	
	`qualctrl 141 users 20 Quality Station,,,`
	`finish 150 users 20 Finishing Station,,,`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Empty passwords	Are there any users in the password file with empty or null passwords?
Objective / Subjective	Objective
Findings	Of the twenty-three accounts without passwords, three appear to be employee accounts and twenty appear to be shared accounts with names like “qualctrl” and “finish”. The lack of passwords on 42% of this system’s accounts makes it trivially easy for a determined insider to access the system. One of the principles of good security practice is “defense in depth” (throw enough obstacles in an intruder’s path to slow them down and give yourself time to identify them or make them give up and go away). Use of password-less accounts and group accounts is generally discouraged as it removes accountability and makes it very unlikely that a system intrusion would be able to be traced to a specific individual.
Pass / Fail	Fail

3.1.10 Audit Results of Checklist item #18: Weak passwords

- Full checklist item with references and risk evaluation on page 42
- Analysis of findings is in section 4.2.3 “Findings for Objective: Verify that access to the system is properly controlled” on page 106

Weak passwords	Are the users of this system choosing passwords that are not easy to guess and are not found in any dictionary?
Compliance	Compliance for this test will be measured by the use of the tool “John the Ripper” to attempt to crack passwords in the /etc/passwd file over the course of one hour. To preserve the objectivity of the test, this item will be considered non-compliant (failed) if any passwords are successfully cracked. Although many systems fail this test, full compliance is not impossible. John the Ripper is a well-known tool available at http://www.openwall.com/john/. Configuration and execution of this tool is outside the scope of this document. It could be argued that one hour is not long enough to make a valid test. As we are only looking for the weakest of passwords, we will continue with a one hour test.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Weak passwords	Are the users of this system choosing passwords that are not easy to guess and are not found in any dictionary?

Testing	Type `./john copy-of-passwd-file > /dev/null`
	After one hour, terminate the program with a ^C (CTRL-C) and type the following:
	`./john -show copy-of-passwd-file | /usr/bin/awk '{print $2}' ; \`
	`/usr/bin/rm john.pot restore`

Actual Output	The twenty-three accounts with blank passwords identified in "Audit Results of Checklist item #17: Empty passwords" on page 89 were displayed in this list along with two new additional accounts whose passwords were cracked. As with the "Empty passwords" item, the actual output will not be presented here to preserve anonymity.
Objective / Subjective	Objective
Findings	Almost half of the passwords in the /etc/passwd file were discovered by this checklist item. It was previously determined that this system does not use shadow password files and is not using "Trusted Systems" thus, all users have the ability to read the password file. 45% of the passwords in the /etc/passwd file were found to be vulnerable by this test. The relative openness of the password file makes it practically impossible to ensure that a trespasser on this system could be tracked with any certainty. It is interesting to note that one of the two non-blank passwords which cracked belongs to an IT manager. This illustrates the need for education at all levels of what constitutes a strong password and the need for management to lead by example.
Pass / Fail	Fail

3.1.11 Audit Results of Checklist item #20: Root login restricted

- Full checklist item with references and risk evaluation on page 44
- Analysis of findings is in section 4.2.3 "Findings for Objective: Verify that access to the system is properly controlled" on page 106

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Root login restricted	Is root restricted to logging in on the console only?
Compliance	The /etc/securetty file must exist, contain only the word “console”, and have no write permissions for any user other than root. Root must not be able to log in from another terminal.
Testing	Test 1) As root, type `/usr/bin/ls -l /etc/securetty` Test 2) As root, type `/usr/bin/cat /etc/securetty` Test 3) Attempt to login as root from somewhere other than the console.

Actual Output	Output 1) `/etc/securetty not found`
	
	Output 2) `cat: /etc/securetty: No such file or directory`
	
	Output 3)
	`$ telnet audittarget`
	`Trying...`
	`Connected to audittarget.xyzmfg.com.`
	`Escape character is '^]'.`
	`Local flow control on`
	`Telnet TERMINAL-SPEED option ON`
	
	`HP-UX audittarget B.11.11 U 9000/800 (ta)`
	
	`login: root`
	`Password:`
	`Please wait...checking for disk quotas`
	`(c)Copyright 1983-2000 Hewlett-Packard Co., All Rights Reserved.`
	<snip copyright information>
	`RESTRICTED RIGHTS LEGEND`
	`Use, duplication, or disclosure by the U.S. Government is subject to`
	`restrictions as set forth in sub-paragraph (c)(1)(ii) of the Rights in`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Root login restricted	Is root restricted to logging in on the console only?

	`Technical Data and Computer Software clause in DFARS 252.227-7013.`
	
	`Hewlett-Packard Company`
	`3000 Hanover Street`
	`Palo Alto, CA 94304 U.S.A.`
	
	`Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).`
	`You have mail.`
	`Value of TERM has been set to "dtterm".`
	`WARNING:  YOU ARE SUPERUSER !!`

Objective / Subjective	Objective (Stimulus/Response test)
Findings	The /etc/securetty file does not exist on this system. This means that the root user can log in from any terminal, not just the console. The lack of this restriction on root's logins coupled with the use of telnet instead of ssh means that it is very possible for a determined insider to sniff root's password from network traffic giving them the ability to do whatever they would like to with the system.
Pass / Fail	Fail

3.1.12 Audit Results of Checklist item #27: Default umask

- Full checklist item with references and risk evaluation on page 53
- Analysis of findings is in section 4.2.4 "Findings for Objective: Verify that access and modification are properly controlled" on page 107

Default umask	Is the default file mode creation mask 022 or more restrictive?
Compliance	Compliance will be measured by logging in as root and as a regular user and confirming the umask value is 022 or stricter.
Testing	Test 1a) Login as root and type `/usr/bin/umask`

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Default umask	Is the default file mode creation mask 022 or more restrictive?
	Test 1b) While logged in as root, type `/usr/bin/touch /tmp/testfile.$$; /usr/bin/ls -l /tmp/testfile.$$` Test 2a) Login as regular user and type `/usr/bin/umask` Test 2b) While logged in as a regular user, type `/usr/bin/touch /tmp/testfile.$$; /usr/bin/ls -l /tmp/testfile.$$`
Actual Output	Output 1a) `02` Output 1b) `-rw-rw-r--  1 root  sys  0 Sep  9 15:01 /tmp/testfile.23898` Output 2a) `02` Output 2b) `-rw-rw-r--  1 username  users  0 Sep  9 15:02 /tmp/testfile.24621`
Objective / Subjective	Objective (Stimulus/Response test)
Findings	The umask values for root and the sample user are both "02" (less restrictive than the value of "022" required. This gives other members of the user's group write access to the user's files.
Pass / Fail	Fail

3.1.13 Audit Results of Checklist item #28: Global "chown" privileges

- Full checklist item with references and risk evaluation on page 55
- Analysis of findings is in section 4.2.4 "Findings for Objective: Verify that access and modification are properly controlled" on page 107

Global "chown" privileges	Do all users have privileges to change the group designation of a file?

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Global "chown" privileges	Do all users have privileges to change the group designation of a file?
Compliance	Compliance will be measured by logging in as a non-privileged user, listing the global privileges, and then attempting to change ownership of a file.
Testing	Test 1) Type **/usr/bin/getprivgrp** Test 2) Login as a non-privileged user and attempt to change ownership of a test file. Using "user1" as an example, type the following commands: **/usr/bin/touch /home/user1/testfile** **/usr/bin/ls –l /home/user1/testfile** **/usr/bin/chown user2 /home/user1/testfile** **/usr/bin/ls –l /home/user1/testfile**
Actual Output	Output 1) **global privileges: CHOWN** Output 2) **$ /usr/bin/touch /home/user1/testfile** **$ /usr/bin/ls -l /home/user1/testfile** **-rw-rw-r-- 1 user1 users 0 Sep 9 15:05 /home/user1/testfile** **$ /usr/bin/chown user2 /home/user1/testfile** **$ /usr/bin/ls -ld /home/user1/tdob.testfile** **-rw-rw-r-- 1 user2 users 0 Sep 9 15:05 /home/user1/testfile**
Objective / Subjective	Objective (Stimulus/Response test)
Findings	The global privilege of being able to change file ownership is still enabled on this machine. Best practices and the default configurations of many of the latest Linux and UNIX systems indicate that allowing users to change ownership of files is not recommended. In most cases, root is the only user that should need to change file ownership.
Pass / Fail	Fail

3.1.14 Audit Results of Checklist item #30: File integrity software

- Full checklist item with references and risk evaluation on page 59

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Analysis of findings is in section 4.2.4 “Findings for Objective: Verify that access and modification are properly controlled” on page 107

File integrity software	Is file integrity software (like Tripwire, *swverify*, or *mkpdf*) used to detect (and alert to) changes in critical system files?
Compliance	With the number of options and the complexity of the available solutions, compliance for this item will be measured by the examination of any company procedures detailing the process of file integrity checking as well as proof that file signatures are being confirmed regularly.

Testing	Test 1) Auditor must review copies of the company procedures addressing file integrity checking and any associated configuration files and results reports.
	
	Test 2) To determine if one of the identified file integrity methods is being automatically run, type:
	`/usr/bin/grep -e tripwire -e swverify -e pdfdiff -e pdfck \`
	`/var/spool/cron/crontabs/* | /usr/bin/more`

Actual Output	Output 1) There were no company policy or procedure documents available which address file integrity checking. There are no file integrity checkers in use so there are no reports produced. Output 2) `<no output>`
Objective / Subjective	Subjective
Findings	No file integrity checking software is in use on this machine. This means that changes to system programs as part of a possible intrusion attempt would probably go undetected.
Pass / Fail	Fail

3.1.15 Audit Results of Checklist item #34: Retirement of old media

- Full checklist item with references and risk evaluation on page 67
- Analysis of findings is in section 4.2.4 “Findings for Objective: Verify that access and modification are properly controlled” on page 107

Retirement of old media	Are old hard drives, backup tapes, and disaster recovery tapes sanitized when they are retired or redeployed?
Compliance	Due to the scope and length constraints of this project, discussions of forensic data recovery and details

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Retirement of old media	Are old hard drives, backup tapes, and disaster recovery tapes sanitized when they are retired or redeployed?
	of "how many overwrites is good enough?" will be left for the reader to research. Compliance will be measured by a review of company policies addressing disposition of end-of-life media. Contemporaneous records indicating such media was destroyed or adequately erased will also constitute compliance.
Testing	Review any company policies addressing media retirement and any logs of such activities.
Actual Output	`<no output>`
Objective / Subjective	Objective
Findings	No written company policies were available which address the secure retirement of digital media. **Note:** On the day of the audit, XYZ Mfg. was donating several older PCs to a local high school. The system administrators were running software to securely erase the hard drives multiple times. This illustrates initiative and recognition of the need for secure media retirement.
Pass / Fail	Fail

3.1.16 Audit Results of Checklist item #35: Root's mail must be read in a timely manner

- Full checklist item with references and risk evaluation on page 68
- Analysis of findings is in section 4.2.5 "Findings for Objective: Verify that administrators are monitoring the system" on page 108

Root's mail must be read in a timely manner.	Is root's mail being read and/or forwarded to administrator's work e-mail addresses for review and action?
Compliance	It is difficult to prove that someone is watching the mail. Compliance for this item will be measured by either of the following tests being positive. • There must either be no more than two business days of new e-mail in root's mail file • root's mail must be forwarded to one or more system administrator's business e-mail address (with the assumption that it is read and acted upon).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Root's mail must be read in a timely manner.	Is root's mail being read and/or forwarded to administrator's work e-mail addresses for review and action?
Testing	Test 1) To get a list of mail message headers, while logged in as root, type `/usr/bin/mailx -H` Test 2a) Type `/usr/bin/cat ~root/.forward` Test 2b) Type `/usr/bin/grep "^root" /etc/mail/aliases`

Actual Output	Output 1)
	`N 1 root@audittarget.xyzmfg Mon Sep 8 17:51 50/2703 backup results`
	`N 2 root@audittarget.xyzmfg Tue Sep 9 05:52 52/2889 backup results`
	
	Output 2a) `cat: Cannot open //.forward: No such file or directory`
	
	Output 2b) `<no output>`

Objective / Subjective	Subjective
Findings	Tests 2a and 2b show that root's mail is not being forwarded, but the mail in root's local mailbox indicates that it is being read (and deleted) regularly. The two headers shown are for daily backups and there are only two in the mailbox, one from the day of the audit and one from the day before.
Pass / Fail	Pass

3.1.17 Audit Results of Checklist item #36: System logs must be reviewed on a regular schedule

- Full checklist item with references and risk evaluation on page 69
- Analysis of findings is in section 4.2.5 "Findings for Objective: Verify that administrators are monitoring the system" on page 108

System logs must be reviewed on a regular schedule.	Are system logs being reviewed on a regular schedule?

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

System logs must be reviewed on a regular schedule.	Are system logs being reviewed on a regular schedule?
Compliance	As with reading root's mail, it is sometimes difficult to prove that someone is reviewing the system log files. This test is one of the few in the audit that is not purely objective. Unfortunately, compliance for this item will be measured by interviewing the system administrator to ascertain the frequency with which the log files are reviewed.
Testing	At a minimum, the following log files should be reviewed on a weekly basis: • Examine /var/adm/syslog/syslog.log • Examine /var/adm/sulog • Examine /var/adm/syslog/mail.log • Examine /etc/rc.log Page 336 of Chris Wong's HP-UX Security book lists several good open source tools to assist with log rotation and review.
Actual Output	As this test consists of an interview question, the expected output for compliance would be information to the effect that system administrators consistently review the above mentioned logs at least weekly.
Objective / Subjective	Subjective
Findings	The system administrators indicated that they do not review the specified log files unless they are troubleshooting a problem.
Pass / Fail	Fail

3.2 Measurement of residual risk

3.2.1 Original risk

It has been said by many that the only truly secure system is one that is unplugged and locked in a vault. There will always be some risk of exploit or compromise to a production server. In its pre-audit state, the audit target machine is vulnerable to:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- External attacks through its unprotected network services.
- Internal attacks made possible by weak passwords, relaxed permissions on files, and a lack of operating system level auditing.
- Untrained administrators who are able to keep up with routine system maintenance, but are less likely to perform such tasks as investigating system hardening tools and proactively tightening other security settings.

Fortunately, this audit highlights many opportunities for increasing the security of the audit target system and reducing the accompanying exposure and risk.

3.2.2 First steps toward remediation

As new threats materialize and business needs change the use of the system, the risk profile of the system will continue to change. However, the risk ratings summarized in the Audit Results Summary Table on page 73 can be used to prioritize remediation efforts with the goal of reducing risk and protecting the assets as defined in 1.4.1 “Assets to be protected” (the integrity of the data, operating system, and manufacturing software, and the availability of the operating system and manufacturing software). A few suggested first steps include:

- Attention to security and operating system patches (Checklist item #13: Security patches and Checklist item #14: Operating system patches) will reduce the likelihood of operating system components being compromised by a newly discovered exploit.
- Examination and possible disabling of unneeded network services (Checklist item #02: Unnecessary services being started and Checklist item #04: Services brokered by the Internet daemon) will greatly reduce the number of possible avenues of attack for an external attacker.
- Installation of TCP Wrappers to limit access to the network services that remain enabled (Checklist item #05: TCP Wrappers) will allow finer-grained control of access to the system even with some of the less secure network services (telnet & ftp). TCP Wrappers also provides optional logging mechanisms that would allow the administrators and management to determine exactly how the system is being used.
- Installation and use of ssh (Checklist item #07: Secure Shell) will reduce the likelihood that administrative passwords can be “sniffed” off of the network and used to compromise the system. Like TCP Wrappers, ssh also allows fine control of which hosts and addresses are allowed to connect to the system.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Enforcement of stronger passwords (Checklist item #18: Weak passwords) will greatly reduce the risk of an insider performing malicious activity while masquerading as another user. The strongest network services can still be bypassed by an unauthorized user who determines that certain accounts have weak or non-existent passwords.
- Use of a system-hardening tool like Bastille for HP-UX[12] will have a primary effect of helping to identify additional steps for tightening security of this system to acceptable levels and will have a secondary effect of helping to educate the system administrators on best practices in security.

3.2.3 Risk remaining after remediation

The scope of this audit was limited to an examination of the operating system configuration for one system only. After remediation efforts address the areas of opportunity highlighted in this audit, some risk will remain due to considerations outside of the defined scope of this audit. The areas of risk not covered in this audit and remaining after the audit are presented in the following section.

3.2.3.1 Policies and procedures

The development of policies governing how information technology is to be managed and the procedures to implement those policies is strongly encouraged. Policies addressing Change Management, Acceptable Use, Acceptable Network Services, Password Management, and Security Management if they are implemented with management sponsorship can go a long way in reducing risks due to downtime and system compromise. This will enable XYZ to manage their IT investments more proactively.

3.2.3.2 Network

The network to which the audit target belongs should be audited as part of XYZ's new focus on security. It was discovered during the audit that this XYZ plant shares a network with two other sister plants connected by high-speed persistent connections. This increases the pool of potential attackers and reduces the amount that we can trust the network.

[12] http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6849AA

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3.2.3.3 Security training

As previously mentioned, the system administrators have a need for security training and advanced system administration training. Many items discovered in the audit would be easily remedied by the regular attention of a knowledgeable and trained system administrator.

3.2.4 Were the stated control objectives met?

Given that 81% of the risk rating points were classified in the "Fail" column of the Audit Results Summary Table on page 73, the risk of compromise for this system remains high after the audit. As this system is a critical server for XYZ Manufacturing's production and shipping operations, we will review whether the control objectives identified earlier were met. Several objectives were identified for this audit:

- Objective: Verify the system's network services are configured securely – Many vulnerable network services were found to be configured/running and full advantage is not being taken of available logging mechanisms among other items. This audit was not able to show that the system's network services are configured securely.
- Objective: Verify that the system is patched regularly according to the company's patching strategy – Security patches are not kept current on this system and operating system patches do not seem to have been updated since the system was put into production approximately one year ago. This lack of currency of patches could affect the ability of this system to support the company to its fullest ability.
- Objective: Verify that access to the system is properly controlled – Empty passwords coupled with the ability of all users on the system to access the password file prevent this objective from being met. If one of the identified threats were to be realized (external attacker or determined insider), there is little ability to authoritatively prove who did what.
- Objective: Verify that access and modification are controlled for sensitive files – With the openness of access to this machine, preventing unauthorized modification of sensitive files becomes difficult. The auditing functions provided by HP-UX 11i Trusted System would allow access control and tracking for modifications of sensitive files.
- Objective: Verify that administrators are monitoring the system – The system administrators on this machine are stretched thin. They monitor the things they know to monitor (like root's mail) and they keep up with regular maintenance. Further training is required to bring the administrators to the place where they can effectively manage the security of this machine.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3.2.5 Summary of residual risk

To summarize the residual risk section, the control objectives for the security of this system were not met. Each of the objectives contained several items that were out of compliance. Most of the items could be brought into compliance through the efforts of XYZ's system administrators working with security professionals. Items that would require more time than allowed in the following estimate are: Checklist item #23: Change Control, Checklist item #29: SUID/SGID files, and possibly Checklist item #30: File integrity software. These items would require an investment of time to determine the best form of change control for the company, which SUID/SGID files are not actually required to have those permissions on the audit target machine, and which files and directories relating to XYZ's applications would need to be tracked by file integrity software.

A rough estimate of time and costs required to remediate the items that failed the audit (with the exceptions noted above) and to begin building a base for continuing management of this system's security:

Forty hours of security consultant time not including expenses = $8,000 (estimated at $200/hour)
Eighty hours of system administrator time to work with a security professional = $2,600 (estimated at $32.50/hour)
Total cost for this rough estimate is $10,600.

3.3 Evaluation of the audit

An evaluation of this audit begins with the observation that the best audit is an objective audit. Effort was made to keep this audit as objective as possible. There was no security baseline or existing policy and procedure documents against which the system could be measured, so many of the tests were measured against best practices in the security field. This makes them less tailored to the specific system under review.

The understandable choice by the management of XYZ Mfg. to not allow third party auditing applications (such as nmap, Nessus, and the CIS Benchmarking Tool) to be run on the production server may have reduced the authoritative goal of the report, but the tests performed definitely support the conclusions and recommendations presented.

The scope of this audit was defined as an examination of the security configuration of the operating system only. Considering that scope, this system was definitely auditable.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4 Audit Report

4.1 Executive Summary

The goal of this audit: This audit was requested as part of XYZ Manufacturing's new security initiative. The goal was to verify that the control objectives for the system (as defined in 1.4.4 "Goal of this audit" on page 9) were being met. An analysis of this goal is included in section 3.2.4 "Were the stated control objectives met?" on page 102. The goal of this audit was accomplished. Unfortunately, the tests performed on the system were able to determine that the control objectives are not being met on this system.

The scope of the audit: The scope of the audit was defined in 1.3 "Scope of the audit" on page 5. Briefly, the scope was defined to include an examination of the security configuration of the HP-UX 11i system which hosts XYZ's manufacturing and shop floor control applications. Not included in the scope are the network on which the target machine resides and company policies except where they intersect with security and operating system configuration.

This audit was customized to the specific system under review. The methodology used was that of examining configuration settings and, where possible, testing those settings to achieve objective results on the effectiveness of the settings. As the audit was conducted during production hours, no third-party tools were used that could have impacted system performance. This was by request of XYZ management.

The outcome of the audit: The audit was completed successfully with the valuable assistance of XYZ's system administrators and IT manager. The findings and recommendations are presented in the sections below.

4.2 Audit Findings

As could be expected for any new security initiative, many opportunities for improvement were discovered. The following sections detail what was found when investigating whether control objectives were being met.

4.2.1 Findings for Objective: Verify the system's network services are configured securely

The first control objective this audit seeks to verify is the secure configuration of this system's network services. All network services provided by this server are enabled or disabled by a set of configuration files. Examples of these services include: web server, e-mail, file transfer, and others. Some of these services were developed decades ago and have a history of vulnerability, other services can be used against each other to cause system outages.

A standard security practice is to provide only the services on the machine that are supported by a business need. Services that are allowed to remain should

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

be configured as securely as possible with logging enabled if available. The system should also leak as little information about itself as possible.

Finding: "Audit Results of Checklist item #02: Unnecessary services being started" on page 75 and "Audit Results of Checklist item #04: Services brokered by the Internet daemon" on page 80, show that there are many network services configured and running that have no use to the system and in some cases could be used to cause outages on the system.

Finding: "Audit Results of Checklist item #05: TCP Wrappers" on page 82 shows that an available tool for restricting access to this machine is not being used. In addition to access control, this tool also allows for the logging of connections to monitor usage of certain services.

Finding: "Audit Results of Checklist item #07: Secure Shell" on page 84 indicates another free tool that is not currently installed but could be used to prevent a malicious system on the network from viewing the administrative passwords flowing across the network.

Finding: "Audit Results of Checklist item #11: Banners" on page 85 shows that some information about specific versions of software used on the system are made available to users connecting to the system. This leakage of information does not lead directly to a compromise, but can give a potential attacker more information to use against the machine.

Risk: A curious or malicious user within the company network could use several of the unneeded, but still enabled, legacy network services to retrieve enough information about the system to either gain access immediately or to perform further research on possible exploits for later use. Even if denied access, the attacker could use some of these services to execute a denial-of-service attack on the system, rendering it unusable for some period of time.

In the case of a denial-of-service attack, the results could range from one to many hours of downtime (possibly at a critical period like month-end or year-end). In the case of an attacker actually gaining access to the operating system, the results could range from general mischief like deleting simple files or causing printers to go offline, to more serious sabotage such as corrupting databases, or changing manufacturing data with the intent to ruin batches of product.

In some cases, the impact to the company could be significant in terms of payroll dollars for recovery and lost production time.

4.2.2 Findings for Objective: Verify that the system is patched regularly according to the company's patching strategy

The second control objective to be examined is related to the application of security and operating system patches. Given the frequency with which new

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

vulnerabilities are discovered in most software, proactive research and installation of security patches is critical. Many well-known vulnerabilities are exploited simply because system administrators are not able to keep current with patching their systems.

Finding: "Audit Results of Checklist item #13: Security patches" on page 87 indicates that HP's Security Patch Checker tool is not installed on this machine. This tool can be configured to run nightly, download the latest catalog of security patches from HP, and cross-reference with what is currently installed on the system giving recommendations on patches that should be installed.

Risk: If security patches are not being applied proactively, by definition, they are being applied reactively or not at all. If the company has data-loss insurance or other business-loss insurance, the insurance company may be slow to pay (or not pay at all) if it is discovered that an attacker gained access to the system through an unpatched vulnerability for which security patches exist.

4.2.3 Findings for Objective: Verify that access to the system is properly controlled

The third control objective evaluated is that of access to the system (accounts and passwords). Passwords on user accounts and administrative accounts are the first line of defense against unauthorized users, but all too frequently proper attention is not paid to the strength of the passwords and users are known to go to great lengths to avoid having to remember strong passwords. According to the SANS/FBI Top 20 List, weak or nonexistent passwords are the tenth most common vulnerability on UNIX systems [13]

Another weakness of passwords on some systems is that the file containing all of the passwords (in "hashed" or encrypted format) is readable by all users so they can check and change their own password. The user may not be able to determine other users' passwords from looking, but he can copy the file to a different system and run programs against it to discover the weakest passwords. One way to defeat this "world-readable" password file is through installation of a utility called "Shadow Passwords". It moves the actual passwords to a file not readable by regular users. Shadow Passwords is standard on most current UNIX and UNIX-like operating systems and can be added to the version of HP-UX running on the audit target for free.

Special attention must also be paid to controlling access to the administrative account ("root"). The password for this account must be strong and, given the all-powerful role of this account on a UNIX system, administrators are encouraged to use the account only when necessary. One way to encourage this behavior is to restrict root logins to the system console only.

[13] "SANS/FBI Tops 20 List", http://www.sans.org/top20/#U10

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Finding: "Audit Results of Checklist item #15: Shadow Passwords" on page 88 shows that the Shadow Passwords functionality is not installed on this system.

Finding: "Audit Results of Checklist item #17: Empty passwords" on page 89 and "Audit Results of Checklist item #18: Weak passwords" on page 90 indicate that the passwords on this system are not as strong as they should be. As part of this audit, Checklist item #18 included the use of a password assessment tool to attempt to discover weak or empty passwords. Of the forty-three unlocked users in the password file, twenty-three of them had no password (over half). Of the remaining twenty accounts with passwords, only two of them had weak passwords that were discovered by the assessment tool.

Finding: "Audit Results of Checklist item #20: Root login restricted" on page 91 shows that logins to the root account are not restricted to the console as was suggested. This usually leads to administrators logging into the account all the time instead of logging in as themselves and switching over to the root account. This makes tracking what was done on during a security event more difficult.

Risk: The risk identified in this section is one of the highest identified on the system, but fortunately it is also one of the easiest to fix. With approximately half of the accounts on the system having no password, it would be almost impossible to authoritatively determine who was responsible for some mistake or act of mischief. It was also noted in the audit results that many of the accounts with blank passwords were accounts used by all members of a group. This makes it likely that a person wishing to do something malicious on the system would know the password-less accounts and would be able to remove files, corrupt databases, or redirect manufacturing processes with near-complete anonymity.

Fortunately, the technology already exists on the system to require stronger passwords. The roadblocks to securing this area are in implementation. Employees have to be convinced of the need for security before they will suffer the inconvenience of harder-to-remember passwords without simply writing them on the monitor.

4.2.4 Findings for Objective: Verify that access and modification are properly controlled for sensitive files

The fourth control objective examined attempted to determine if sensitive files were safe from unauthorized access and modification.

Finding: "Audit Results of Checklist item #27: Default umask" on page 93 shows that all files are created with read and write access enabled for users other than the file's owner (users in the same group as the owner). This means that files can be modified or overwritten by people other than their owners.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Finding: "Audit Results of Checklist item #28: Global "chown" privileges" on page 94 proves the ability of all users to change ownership of some files which could lead to deletion of the wrong files by malicious users.

Finding: "Audit Results of Checklist item #30: File integrity software" on page 95 indicates that tools which can warn of changes to system component programs are not configured to run automatically. One common action after compromising a machine is to change certain system programs to hide the compromise. File Integrity software can determine if these programs have changed.

Finding: "Audit Results of Checklist item #34: Retirement of old media" on page 96 shows that there is no clear policy of retirement for old digital media. If old or unused backup tapes or hard drives are just thrown in the dumpster or sold at auction, company data can easily be retrieved from them.

Risk: While there are risks associated with items like "default umask" and "global chown privileges" such as the ability to change or erase files, the problems are relatively easy (if time consuming) to clear up. The issue of file integrity software deserves a little more attention. While the use of file integrity software will only notify the administrators of a change **after** the change has taken place, it is far more desirable to know about it then, than to not find out about it until it is too late. Use of this kind of software also leads to the administrators having a better handle on what is happening on their system as it requires them to be aware of such topics as patching, locations of configuration files, and changes to the applications.

Note: During the time the auditor was on-site, the system administrators were running software to securely erase the hard drives of PCs that were being donated to a local high school. This illustrates initiative and recognition of the need for secure media retirement.

4.2.5 Findings for Objective: Verify that administrators are monitoring the system

The final control objective examined is that of verifying that the administrators are monitoring the system. This objective showed mixed results. On the one hand, system log files are not being reviewed on a regular basis. On the other hand, administrators are doing a very good job of keeping up with reading and responding to system mail in the root account.

Finding: "Audit Results of Checklist item #35: Root's mail must be read in a timely manner" on page 97 shows that the administrators are reading root's mail at least every two days (if not more frequently).

Finding: "Audit Results of Checklist item #36: System logs must be reviewed on a regular schedule" on page 98 indicates that standard system logs which may

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

show evidence of hardware problems or security events are not being reviewed by administrators on a regular basis.

Risk: A system administrator's time is not infinite and must be spent on tasks that are a priority to the company. With the number and variety of responsibilities held by the system administrators at this company, it is not surprising that a time-consuming proactive step like reviewing logs is put aside. Several free programs[14] exist which can assist the system administrator with the task of evaluating and reacting to the information in system log files.

4.3 Audit Recommendations

Although this audit focused on one HP-UX system, the principles and suggestions conveyed in the audit can be applied to many different systems. Section 3.2.2 "First steps toward remediation" on page 100 gives several suggestions on what steps should be taken first as XYZ Manufacturing moves toward a more secure environment. These steps include the following (see the section for more information):

- Attention to security and operating system patches
- Examination and possible disabling of unneeded network services
- Installation of TCP Wrappers to limit access to the network services that remain enabled
- Installation and use of ssh
- Enforcement of stronger passwords
- Use of a system-hardening tool like Bastille for HP-UX[15]

In addition to remediation of the areas identified, further steps that can be implemented are explained in section 3.2.3 "Risk remaining after remediation" on page 101. These steps include the following (see the section for more information):

- Development of policies and procedures to address such Information Technology needs as Change Management, Acceptable Network Services, Password Management, and Security Management.
- A security analysis of the network itself. This analysis should include discovery of what devices are on the network, what their intended uses are, what their actual uses are, and an evaluation of external connections to the Internet.
- Establishment of a plan for security and advanced system administration training. There are many medium and low cost opportunities for security and system administration training. As security becomes a priority at XYZ Manufacturing, training will become more necessary.

[14] Wong, page 336
[15] http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6849AA

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The primary goal of the Information Technology department is to support the business processes of the company. The proactive management of the Information Technology infrastructure (in a secure manner) best accomplishes this goal. The establishment and implementation of process to proactively manage operating system and security patches, authentication of users, and management of the systems will take upfront work, but will end up saving the company money down the road as ongoing maintenance will be less expensive than the possibility of several costly outages.

As with any other large project, XYZ's new security initiative should focus on developing a maintainable process of making and keeping the infrastructure secure, as opposed to reactively fixing symptoms as they arise. Efforts should center on strengthening "preventative controls" such as stronger passwords, access control lists for network services, and the "fixing" of weak file permissions as these preventative controls are geared toward keeping intruders out of the system. The alternatives are "detective and corrective" controls that simply determine what happened and attempt to fix it.

4.4 Cost summary

Section 3.2.5 "Summary of residual risk" on page 103 contains a rough estimate of the cost of correcting the issues identified in this audit. Most of the solutions identified could probably be implemented by a security professional working with XYZ's system administrators for one or two weeks to correct most of the items and to help establish an ongoing plan for managing the remaining items.

Rough estimate for correcting recognized issues:

$8,000	40 hours of consultant time not including expenses (estimated at $200 per hour, an average from various on-line sources)
$2,600	80 hours of system administrator time (estimated at $32.50 per hour, an average from various on-line sources)
$10,600	An estimate of the expense to correct identified security issues

The costs of developing a body of policies would have to be part of an ongoing effort. The development of a "security culture" does not happen overnight and can only happen gradually as a company recognizes the need for it. The costs associated with such a large effort would have to be weighed against the costs of downtime (payroll and overtime costs for system administrators, stalled manufacturing employees, possible outside assistance, lost revenue, product spoilage if any, etc.)

4.5 Compensating controls

Coordination of effort: It was determined that the network at XYZ is shared by two sister plants and managed by network administrators at one of those plants. Network administrators and system administrators at the other two plants can possibly be leveraged to assist with security efforts at this plant. Creation of a

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

formal or informal cross-plant administrative/security team might be a very efficient way to capitalize on existing skill sets.

The costs of correcting identified issues can probably be handled locally, but the effort and costs associated with development of policies and procedures can likely be rolled up to the corporate level. If the corporation determines that the costs to develop these policies are too great, local management can develop a smaller set for local use only. There are many on-line resources containing sample policies that can be customized for use.

Other options: If the cost of bringing in a security consultant to assist local administrators with remediation is determined to be cost prohibitive, there are sufficient on-line resources to guide the administrators though securing the HP-UX system.

Security and System Administration training was suggested as a way to allow the system administrators to operate more proactively and more efficiently. A chart containing a curriculum roadmap for a system administrator (with security courses) can be found at: http://education.hp.com/hp-uxsecurity.htm

Given the variety of training options, their costs will not be listed here. Options include books available for $50 or less and vendor-neutral or vendor-provided security/system administrator training with prices ranging from $500 to several thousand dollars.

4.6 Summary

This audit found a system that has not changed much since it was received with the operating system pre-installed. The system is being well maintained by busy system administrators with varied job responsibilities. This is not unusual for IT departments of similar size.

There are many opportunities for improvement in the security of the system and fortunately, none of these corrections should be difficult to make. All that is required is management support, a few weeks of research, and careful adjustments to the system.

The purpose of an audit is to objectively evaluate the risk to a system. This system is not very complex, and it will not be difficult to bring the system to a more secure state. Although the company must plan for the possibility of a security related incident, this system does not have a high profile outside of the company. Completing the steps outlined in this audit will go a long way toward relieving security concerns and allowing XYZ Manufacturing to focus on the business of manufacturing.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

1. "Administering Your HP-UX Trusted System". 08/1996. Retrieved on 08/10/2003 from http://docs.hp.com/hpux/pdf/B2355-90121.pdf
2. "Building a Bastion Host Using HP-UX 11". 08/2000. http://www.hp.com/products1/unix/operating/infolibrary/whitepapers/building_a_bastion_host.pdf
3. "Center for Internet Security: Level-1 Benchmark (v1.0.4) and Scoring Tool (v1.2.1) for HP-UX". 04/2002. Retrieved on 08/10/2003 from http://www.cisecurity.org/bench_HPUX.html
4. "HP-UX 11i System Security White Paper". 05/2003. Retrieved on 08/20/2003 from http://www.hp.com/products1/unix/operating/infolibrary/whitepapers/hpux11isecuritywp.pdf
5. "HP-UX Audit Program". 03/2000. Retrieved on 08/10/2003 from http://www.auditnet.org/docs/HP-UX%20Audit%20Program.txt
6. "HP-UX Networking Ports Reference Guide". Edition 1. 2003. Retrieved on 08/14/2003 from http://docs.hp.com/hpux/pdf/5187-4242.pdf
7. "Managing Systems and Workgroups: A Guide for HP-UX Systems Administrators". 06/2003. Retrieved on 08/10/2003 from http://docs.hp.com/hpux/pdf/B2355-90742.pdf
8. "Network Security Features of HP-UX 11i: An HP-UX 11i White Paper from Hewlett-Packard". 02/2002. Retrieved on 08/14/2003 from http://docs.hp.com/hpux/onlinedocs/2238/netsecur_final.pdf
9. "Stack Buffer Overflow Protection in HP-UX 11i White Paper". 11/2001. Retrieved on 08/14/2003 from http://docs.hp.com/hpux/onlinedocs/os/11i/59807127en.pdf
10. Bosworth, Seymour and Kabay, M.E eds. Computer Security Handbook: Fourth Edition. John Wiley & Sons. 2002
11. Ellis, Theodore. HP-UX 11.0 Installation and Security Verification Checklist for "Lawson" Application Server. 04/2002. Retrieved on 08/11/2003 from http://www.giac.org/practical/Theodore_Ellis_GCUX.doc
12. Hoelzer, David. Auditing Principles and Concepts. The SANS Institute, 2003
13. Jones, Walt CISSP. "How-to" secure HPUX 11i for use in a DMZ environment. Whitepaper v1.8. 08/2003
14. LeClerc, Rey. "UNIX Operating System Security Review". Retrieved on 08/10/2003 from http://www.auditnet.org/docs/unixos.txt
15. Mookhey, K.K. "The UNIX Auditor's Practical Handbook". Retrieved on 08/10/2003 from http://www.nii.co.in/tuaph1.html
16. Poulsen, Kevin. "Slammer worm crashed Ohio nuke plant network". SecurityFocus.com. 08/2003. Retrieved on 08/20/2003 from http://www.securityfocus.com/news/6767

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

17. Rehman, Rafeeq Ur. HP Certified: HP-UX System Administration. New Jersey: Prentice Hall PTR, 2000.
18. Ryan, Leslie. Securing HP-UX 11i (11.11) For Use as an IDS/9000 Server. 08/2003. Retrieved on 8/23/2003 from http://www.giac.org/practical/GCUX/Leslie_Ryan_GCUX.pdf
19. Schwartau, Winn. Time Based Security. Seminole, FL: Interpact Press, 1999
20. Stoneburner, Gary; Goguen, Alice; Feringa, Alexis. "Risk Management Guide for Information Technology Systems". NIST Special Publication 800-30. Jan. 2002. Retrieved on 08/10/2003 from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
21. Verton, Dan. "Insider threat to security may be harder to detect, experts say". Retrieved on 08/10/2003 from http://www.computerworld.com/securitytopics/security/story/0,10801,70112,00.html
22. Wong, Chris. HP-UX 11i Security. New Jersey: Prentice Hall PTR, 2002

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS IT Audit Training

Community SANS @ CANHEIT	Ottawa, ON	Jun 13, 2013 - Jun 14, 2013	Community SANS
SANSFIRE 2013	Washington, DC	Jun 14, 2013 - Jun 22, 2013	Live Event
Community SANS Chicago	Chicago, IL	Jul 08, 2013 - Jul 12, 2013	Community SANS
SANS vLive - SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth	SEC566 - 201307,	Jul 08, 2013 - Aug 07, 2013	vLive
SANS Rocky Mountain 2013	Denver, CO	Jul 14, 2013 - Jul 20, 2013	Live Event
Critical Security Controls Summit	Washington, DC	Aug 12, 2013 - Aug 18, 2013	Live Event
Community SANS Dallas	Dallas, TX	Aug 19, 2013 - Aug 22, 2013	Community SANS
SANS vLive - AUD507: Auditing Networks, Perimeters, and Systems	AUD507 - 201309,	Sep 02, 2013 - Oct 16, 2013	vLive
SANS CyberCon Fall 2013	Online, VA	Sep 09, 2013 - Sep 14, 2013	CyberCon
Network Security 2013	Las Vegas, NV	Sep 14, 2013 - Sep 23, 2013	Live Event
Community SANS Miami	Miami, FL	Sep 16, 2013 - Sep 19, 2013	Community SANS
Network Security 2013 - SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth	Las Vegas, NV	Sep 16, 2013 - Sep 20, 2013	vLive
Mentor Session - SEC 566	Troy, MI	Oct 01, 2013 - Dec 10, 2013	Mentor
Community SANS Washington @ GWU	Washington, DC	Oct 07, 2013 - Oct 10, 2013	Community SANS
SANS Baltimore 2013	Baltimore, MD	Oct 14, 2013 - Oct 19, 2013	Live Event
SOS SANS October Singapore 2013	Singapore, Singapore	Oct 21, 2013 - Nov 02, 2013	Live Event
SANS Chicago 2013	Chicago, IL	Oct 28, 2013 - Nov 02, 2013	Live Event
Community SANS New York	New York, NY	Nov 04, 2013 - Nov 07, 2013	Community SANS
SANS Sydney 2013	Sydney, Australia	Nov 11, 2013 - Nov 23, 2013	Live Event
SANS London 2013	London, United Kingdom	Nov 16, 2013 - Nov 25, 2013	Live Event
Community SANS Toronto	Toronto, ON	Nov 18, 2013 - Nov 21, 2013	Community SANS
SANS vLive - SEC566: Implementing and Auditing the Twenty Critical Security Controls - In-Depth	SEC566 - 201312,	Dec 02, 2013 - Jan 15, 2014	vLive
Community SANS Vancouver	Burnaby, BC	Dec 09, 2013 - Dec 12, 2013	Community SANS
North America ICS Security Summit & Training 2014	Lake Buena Vista, FL	Mar 11, 2014 - Mar 20, 2014	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced