Global Information Assurance Certification Paper

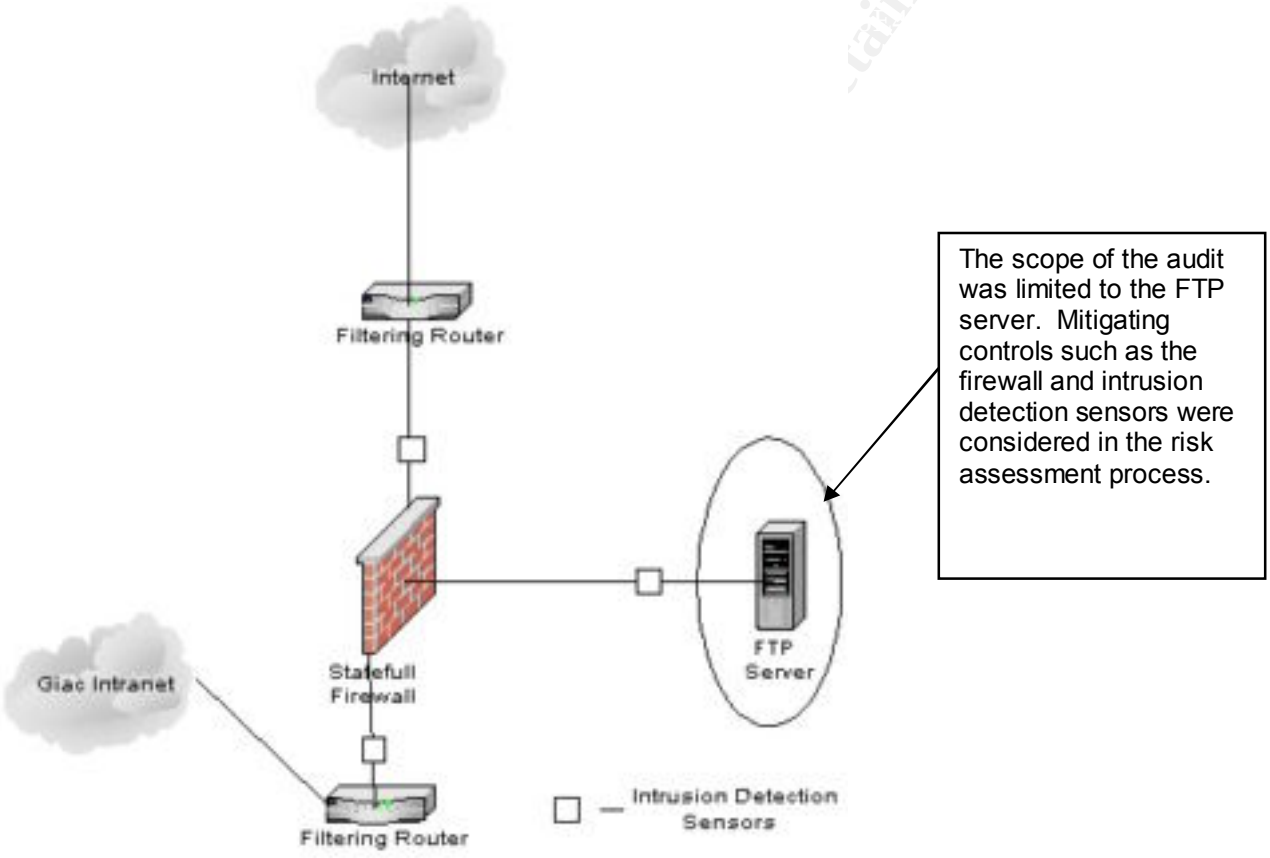
Robert (Bob) Grill
GSEC, GCIA, GCIH, GCFW
Other Certifications and Qualifications: CISA, CISSP, SSCP, CCNA, CRP, CNA, and MBA

Assignment - GCUX Version 1.8 (Option 2)
Consultants Report – Audit of AIX 4.3.3 FTP Server
For Giac Enterprises

Index

Executive Summary

Mustache enterprises has been contracted by Giac Enterprises (Giac), the proprietor of on-line Fortune Cookie Sayings, to perform a security audit of their new AIX version 4.3.3 operating system implementation. This system has been in production for 4 days at the start of our Audit. Fortune cookie sayings are very valuable because no one wants to be responsible for their own future. This server is used as the FTP server for all Giac's customers to download fortune cookie sayings. The server does not allow uploading information. A summary of Giac's configuration is below.



The scope and objectives of our audit were to:

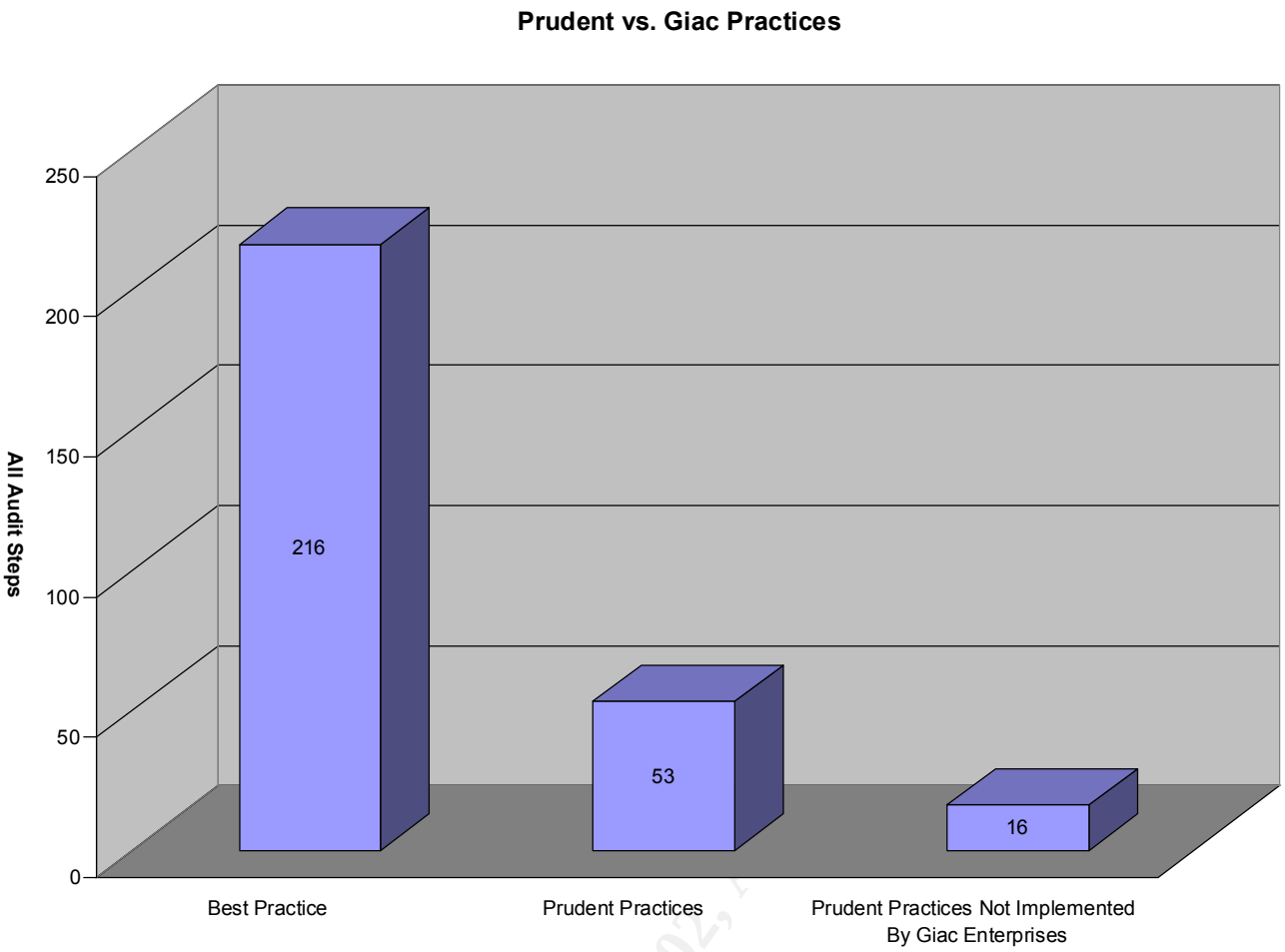
- Compare Giac Enterprises AIX 4.3.3 security practices to best practice, and select among them, the prudent practices that make business sense. Our analysis included;
  - Operating system vulnerabilities
  - Security patch installation and management
  - Configuration vulnerabilities
  - Risks from installed third-party software
  - Administrative practices
  - Identification and protection of sensitive data on the host

    - Protection of sensitive data in transit over the trusted network or the Internet
    - Access Controls (enforcement of general access controls, as well as least privilege and segregation of duties)
    - Backup policies and disaster preparedness
    - Other issues/vulnerabilities as appropriate
- Review processes for maintaining security and verify they are prudent
- Advise Giac Enterprises on prudent security measures for their AIX FTP application
- Determine if the appropriate information is available (audit trail) for user accountability and forensics

Our recommendations included:

1. Implementing the auditing function built into AIX to enable effective security monitoring of the server
2. Implementing change control to provide greater availability and detection of unauthorized changes
3. Disabling the root user account, to avoid administrator mistakes and enforce individual user accountability
4. IP filtering and logging should be implemented to avoid unwanted connection attempts and to aid in the investigation of actual or attempted intrusions
5. Creation of a security incident detection and follow - up procedures (Management oversight control)
6. Setting default umask values to a prudent level
7. Deleting unneeded system created accounts
8. Assignment of an owner to files without an owner or group
9. Enforcing a segregation of duties with the user roles function built into AIX
10. The creation of standards and policy documents to support the server implementation (Management oversight control)

Of the 216 best practice items reviewed, 53 were determined to be prudent practices because they make good business sense to implement. Of the 53, 16 were not implemented. Two of the recommendations are intended to address the root cause (or management oversight issues) of the technical deficiencies noted. The graph that follows illustrates this concept.



Description of System and Audit Methodology

The system audited was an RS/6000 type 7012 with a 200Mhz RISC processor, 64MB Ram, 2.1GB Hard drive, GXT550P video card and includes an integrated Ethernet, Integrated SCSI, SCSI CD, and Floppy. AIX 4.3.3.09 is installed.

This section of the consultant's report was also used to describe how risk was ranked. Risk was ranked based on the likelihood (popularity of an exploit and simplicity) and consequence (cost of the possible loss in monetary value and market reputation loss).

If a high or medium risk was addressed by management controls this was considered prudent practice or a score of 0. Best practice is not considered prudent practice because, often the cost of implementing the control outweighs the risk. Prudent practice includes cost to implement, so recommendations will be ranked by cost as well as risk.

Recommended actions were ranked according to risk and cost to implement. The most cost effective approach was determined with our recommendations. Items with the highest risk and the lowest cost to implement were listed first. Because cost to correct the weakness and implementation is considered in our analysis these may not represent the security concerns with the largest likelihood and consequence.

The most prudent solution that makes **business sense**, rather than best practice were selected. Since the system was only audited against prudent practices, rather than best practices, the highest score that can be reached is a 51 (the number of audit steps). The prudent practices did not include low risk items or items that the cost of implementation exceeds the cost of the consequence. Addressing low risks (over controlling a system) does not make business sense. The chart below illustrates the risk rankings.

Consequence +	Likelihood =	Risk
High	High	High
Medium	High	Med
Low	High	Low = Not Addressed in Audit (due to high cost of implementation)
High	Medium	Medium
Medium	Medium	Medium
Low	Medium	Low - Not Addressed in Audit
High	Low	Low - Not Addressed in Audit
Medium	Low	Low - Not Addressed in Audit
Low	Low	Low - Not Addressed in Audit

The guiding principles of the audit was to fulfill the following objectives:

- **Least Privilege** - Employees only given the access necessary to perform their jobs.
- **Process Control** - Manual or automated processes to support security administration, security will be viewed as a process, not a one-time fix.
- **Unneeded Services** - Services are enabled on devices by default that are not needed, and may enable elevated access. The audit will verify that unneeded services are disabled.
- **Confidentiality / Integrity** - Data is changed to make it unreadable during transit.
- **Monitoring** – Proactive action, reviewing security, error and application logs for anomalies.
- **Compliance Verification** - Management has a process in place to ensure compliance with prudent practice.
- **Accounting and Audit Trail** - User actions are recorded for sensitive transactions to support user accountability and forensics, network events are responded to appropriately.

Operating system vulnerabilities

The objective of this section is to list the vulnerabilities documented at the bugtrack web site that this version AIX is vulnerable to. A search for AIX at http://www.securityfocus.com/search did not note any vulnerabilities that this application of AIX was exposed to that was not already fixed by IBM and patches applied by Giac. As noted in the next section, security patches were up to date.

Security patches installation \ management

As previously noted, Mustache Enterprises was contracted to audit a newly configured system. (the **oslevel** command had returned 4.3.3.09) the output indicated that the system was loaded with Version Release Maintenance Fix (VRMF) 4.3.3.09. According to IBM's web site at http://techsupport.services.ibm.com/rs6k/ml.fixes.html this is the latest VRMF.

Microcode can also be updated but this is for performance reasons and other non – security bug fixes. Accordingly, it is out of the scope of this audit.

A database of Authorized Problem Analysis Reports (APARs) can be found at http://techsupport.services.ibm.com/server/aix.CAPARdb a query for "Security" hit the display limit of 100. Accordingly, an application called FixDist must be loaded to figure out what fixes are needed. http://service.boulder.ibm.com/aix/tools/fixdist/fixdist.html has instructions. This application is loaded on the system and it has downloaded and installed the appropriate fixes. A process for maintaining security was implemented that runs this program and updates the system once a week or more often if a serious security incident arises.

It was noted that management also subscribed to the appropriate AIX listserve advisory services and updates, the maintenance levels and emergency patches were applied as appropriate. Emergency fixes can be found at ftp://aix.software.ibm.com/aix/efixes/security .

Configuration vulnerabilities and Risks from installed third-party software (The following information was read in various pages in Reference 6 p.391-415, nothing was taken verbatim)

The objective of this section is to list risks from third party software such as browsers and applications. The only application being used on this server is FTP. FTP was designed with the minimum security. Because of this, alterations to FTP have been created. However, changes to the protocol must result in the party at the other end of the connection using the same protocol. Giac's customers are resistant to change and installing new software, accordingly this is not an option.

The greatest risk is the disclosure of confidential information. Specifically, in this application, it is the disclosure of Giac Enterprises proprietary fortune cookie sayings. One risk is an FTP Bounce attack see http://www.cert.org/advisories/CA-1997-27.html.

In this attack, a client could issue an FTP **PORT** command to initiate an additional outbound connection from the server to a target at a specified port. This attack could be used to initiate a variety of attacks against other machines. The next risk is inappropriate uploads, these files may be offensive or malicious. Giac allows only downloads for this reason.

Available Risk Mitigating Controls

Policy

Security policies are the foundation of a company's implementation of security. Policies guide the implementation of services, appropriate application use and provide accountability for actions that are not allowed by the company.

Access Controls

Access controls can be used to limit FTP communication between servers. After access is achieved, the term "authorization" is used to describe what a party can do from within the application. Connection filtering cannot be used with FTP because the FTP client that initiates the connection usually uses an ephemeral port and connects to the server on port 21. The client then instructs the server to initiate an additional connection back to the client on a specified port for file transfer. An FTP capable firewall is used to limit the risk to clients from hijacked FTP data sessions. Otherwise Giac's partners can use an option called passive FTP. In this case the server initiates the second connection. Unfortunately, many FTP clients do not support passive FTP. Also, the Giac firewall limits connections based on approved return IP addresses.

Outbound FTP can utilize a proxy that affords access controls to prevent unintended untrusted users from using the application. This could prevent spy's from within Giac from sending out fortune cookie sayings to competitors through this connection.

Account Disclosure

All FTP command information (including user name and password) is sent unencrypted over public networks, this leaves them vulnerable to sniffing. Additionally, an attacker can use brute force to find the user name and password combinations due to the way FTP sends error messages (RFC959). This RFC also provides no means of data encryption. To prevent brute force guessing of passwords, login attempts will be set to 3 before closing the connection.

To protect Giac's internal network, the FTP application will be in a screened subnet in the company's DMZ. The server is built for this specific role and will not share authentication services (NIS for example) with any other machines in the internal network.

Other alternatives suggested to our business partners, such as SSH, SSL over FTP and sneaker net, have been rejected.

Since the culture of Giac's customers cause them to refuse to use a more secure form of internet communication besides active FTP, a separate firewall will be used to restrict outbound access to approved IP addresses on the public network and Fortune Cookie sayings will only be placed in the outbound FTP directory at scheduled times. No other data will reside on the machine and the machine will rely on a separate firewall for connection oriented access control. A firewall conduit is created for each order to a specific IP address and then closed after the order is fulfilled. The firewall in the Giac DMZ tracks the state of the FTP session and prevents most risk from common FTP exploits.

Administrative practices

This section lists the processes in place to support a segregation of duties, accountability, forensics, general access controls, and to generally maintain a secure system.

Process	Interval	Documentation	Results	Audit Step
Change Control	At every change, also check TCB every week and compare to authorized changes.	Evidenced by a change log with authorizations from a person other than who made the change.	See finding #2	5.2
Listserv Monitoring	As needed	Verified by comparing the last listserve advisory to the patch installed.	No Exception Noted	None
Data Backups	Daily	See Audit Program for Steps	No Exception Noted	9.0
Business Resumption Plan Testing	Annually	Test Plan, Test Results	No Exception Noted	9.0
Disaster Recovery Plan Testing	Annually	Test Plan, Test Results	No Exception Noted.	9.0

Process	Interval	Documentation	Results	Audit Step
Log analysis – error, su, login and error	Weekly	Log kept by administrator with management review evidenced by a signature log.	No Exception Noted	4.1
Incident follow-up	As needed	Documented incident response process.	See Finding #5	None
Review of audit logs	Weekly	Audit Logs	See Finding #1	7.0
Housekeeping	Weekly	Compliance Monitoring	No Exception Noted	6.1
Antivirus	Weekly	AIX comes with a virus scanner that looks for PC viruses. It is updated as part of the aforementioned patch update process. The audit noted that a Cron job is run on a daily basis to check the system for viruses and the output sent to a text file. This file is reviewed by the administrator weekly, and the review evidenced by the managers signature in the log evidencing that the manager verified that the administrator performed the task. The manager stated that no viruses have ever been found with the scanner.	No Exception Noted	5.1

Identification and protection of sensitive data on the host

This objective does not apply to this server because of its use.

Protection of sensitive data in transit over the network or Internet

This objective does not apply to this server because of its use. Management has chosen to accept the risk in this area due to customer requirements as described previously in this paper. Data is not encrypted on the internal network because Giac Enterprises is housed in a physically secure building, no satellite offices exist and employees do not work at home.

For the sections of the consultants report that address

- **Access Controls (Note 1)**
- **Backup policies and disaster preparedness (Note 1, See Page 37)**
- **Other issues/vulnerabilities as appropriate (Note 1)**

Note 1: See Appendix A: Comprehensive Audit Program and Results to Support the Audit Report.

Critical Issues and Recommendations

Mustache Enterprises looks forward to the opportunity to review Giac's other computing devices and fix the items noted in this audit. (at an additional fee). Mustache can provide these services without a conflict of interest because Giac is welcome to bid this work to other consultants. However, since we are also your financial auditors, we will have to re-perform the work of the other consultants in order to place reliance on it for our financial audit and have to charge Giac again for it. Accordingly, we do not have a conflict of interest but it will cost double if someone else performs the work.

Below is a prioritized list of our findings and proposed solutions. The list is in order of what should be addressed first. $350 an hour was used as a basis for the estimated cost to implement our recommendations.

#	Recommendation	The Risk to the Overall System	Cost to Implement
1	**Title: Auditing Not Implemented** We used the Command: **auditpr -v < /audit/trail** and observed the output: */audit/trail: A file or directory in this path name does not exist.* This indicated that auditing was not enabled. (Audit Program Step 7.4) "The auditing subsystem of AIX provides the means to record security-related information and to alert system administrators of potential and actual violations of the system security policy. The information collected by auditing includes: the name of the auditable event, the status (success or failure) of the event, and any additional event-specific information related to security auditing." [9p.9] For example, security related events include: • USER_SU - provides information about a user that unsuccessfully tries to su to another user and fails. • Files (called objects by IBM) that are read, written to or executed. We also used the command: **more /etc/rc** and noted that the **/usr/sbin/audit start** command was not in the file. This means that auditing is not started when the machine is started. (Audit Program Step 7.5) **Recommendation:** Configure server to start auditing on the AIX system automatically at startup. Auditing could be started automatically by adding the line **/usr/sbin/audit start** to the **/etc/rc** file. A process should be implemented to define what is considered a security events. (see finding #5) Configure the /etc/security/audit/events and /etc/security/audit/objects files for the items that management has decided to audit by this process and review the auditing logs for these security incidents. **Mitigating Controls in place:** Review of the su, login and error logs.	Without auditing implemented, intrusion attempts, successful or not, may not be monitored and actual intrusion attempts responded to accordingly. For certain activities a segregation of duties is not practical and audit logs are the only means to monitor user activity. 4 Related Prudent Practices Not Implemented	**Cost: Expensive** **Risk: High** Auditing process Development and Implementation. 4 hours (4 * 350 = $1,400) Ongoing log review (4 * 350 = $1,400) Weekly

#	Recommendation	The Risk to the Overall System	Cost to Implement
2	**Title: Trusted Computing Base (TCB) Not implemented** We used the Command: **tcbck –n -tree** And noted the following results : (abbreviated) *3001-101 The Trusted Computing Base is not enabled on this machine.* After further inquiry we also noted that a change control process was also not in place. Change Control is one of the most important controls in a production environment. Change control provides: • Virus Protection – viruses can be detected without a virus scanner by looking for unauthorized changes to the operating system. • Availability – once a system is running it usually only will go down if it is changed, with change control a back out process could be implemented. • Security – change control ensures that only authorized configurations are implemented. A change control process should be implemented to prevent unauthorized changes. Once a change control process is implemented change detection software must be implemented to detect unauthorized changes so they can be corrected.	Change control is the most basic control needed for a production environment. Without change control, availability and security can be compromised. This compromise may ultimately result in the disclosure or destruction of confidential data. Audit Program Step # 5.2 4 Related Prudent Practices Not Implemented	**Cost: Expensive** **Risk: High** Change Control Process Development and Implementation. 120 hours (120 * 350 = $42,000) The change control process will cost money initially but will pay for itself many times over through increased availability and security.

#	Recommendation	The Risk to the Overall System	Cost to Implement
	Recommendation: We recommend that Giac Enterprises implement a change control process. Additionally, the Trusted Computing Base (TCB) tool that is built into the AIX operating system should be implemented to track changes. The changes recorded by the TCB should be compared to authorized changes as part of the change control process to detect and facilitate correction of any unauthorized changes found. **Mitigating Controls in place:** If the server goes down an investigation would be performed and a virus or faulty change may be located. However, the condition is not prevented with this control. Preventative controls are superior because they may prevent a loss of confidentiality or production time.		

#	Recommendation	The Risk to the Overall System	Cost to Implement
3	**Title: Root User Not Disabled** We used the Command: **smit and selected the option for Change / Show Characteristics of a User** and observed the results for the Root User ID: (Abbreviated) *User can LOGIN? true* *User can LOGIN REMOTELY? true* "The command indicated that a user can login directly using the root account rather than using the SU function. There is seldom a good reason for logging in as root. Most system accidents in UNIX are partly caused by routine use of root as a working user." [1.p20] **Recommendation:** Disable the root user using the **smit** utility described above. If the root user is disabled through smit rather than editing the /etc/passwd file, then administrators will still be able to SU to root, but accountability will be enforced because the usage of root will be tied to their user ID in the SU log. **Mitigating Controls in place:** A mistake that caused data loss or a system corruption can be restored from a backup copy. However, this is a very time consuming fix and data may be lost if the backup is not current.	The risk to the overall system falls in the category of accountability. Each user should have a unique user ID to enforce accountability. Availability is also improved by preventing mistakes. Audit Program Step # 3.3 1 Related Prudent Practices Not Implemented	**Cost: Inexpensive** **Risk: High** (.5 * 350 =$175)

#	Recommendation	The Risk to the Overall System	Cost to Implement
4	**Title: IP Filtering and logging not implemented** We used the Command: **smit ips4_advanced** and selected the option: **List Active IP Security Filter Rules** and observed the results *Can not open device /dev/ipsec4_filt.* This result was noted because IP filtering and logging was not implemented (Audit Test # 4.6 and 8.6) IP filtering is used to protect the server from possibly malicious connection attempts. **Recommendation:** Implement IP filtering for all protocols and ports except for TCP port 21 (FTP) **Mitigating Controls in place:** • Server in a DMZ protected by a filtering router and stateful, FTP aware firewall. • Unneeded services on the server are disabled.	Without port connection attempt filtering and logging actual or attempted connection attempts may be carried out with impunity. This activity may lead to a breach of security. Control Objectives: • Least Privilege • Defense in Depth 2 Related Prudent Practices Not Implemented	**Cost: Expensive** **Risk: High** IP Filter Process Development and Implementation. 120 hours (120 * 350 = $42,000) Ongoing Process of log review (4 * 350 = $1,400) Weekly

#	Recommendation	The Risk to the Overall System	Cost to Implement
5	**Title: Security Incident Detection and Follow-Up** During our review, we noted that the criteria for each activity that may indicate a security incident (such as unauthorized network scanning, adding unauthorized network services, etc.) has not been established. We also noted that procedures for detection and follow-up of defined security incidents (or other security-related events, such as unauthorized "Super User" activities) have not been established. A security incident is an activity that results in an attempted or actual compromise of computerized information (whether intentional or unintentional). Security incidents are identified based on an analysis of activity that exceeds pre-defined limits, a comparison of current activity to already known security incident indicators, or other control processes, such as change control. For example, if a user tries to access the FTP application, but cannot succeed within three attempts (a pre-defined limit), the user ID is locked. Such an activity may indicate an unauthorized attempt to access Giac Fortune Cookie Sayings. A security incident may also result from a computer virus or malicious programming code (e.g., Trojan horses, or worms) introduced to the production environment. **Recommendation:** To ensure effective and timely security incident detection and response, types of security incidents are usually defined, and subsequent prepared	Without adequate security incident definitions and documented procedures for their quick resolution, security of information assets may be compromised. Without an effective incident handling processes, interruption to normal processing could result or reduce customer service levels. Due process, accountability, and forensics cannot be implemented without this process. This was not in the prudent practice calculation because it is a management oversight activity, not a finding from audit tests.	**Cost: Expensive** **Risk: High** Incident definition development and response process Implementation. 120 hours (120 * 350 = $42,000) Ongoing Process of incident response. 4 hours (4 * 350 = $1,400) Monthly

#	Recommendation	The Risk to the Overall System	Cost to Implement
	follow-up actions articulated. While it would be unreasonable to assume that all potential security incidents could be known in advance, the goal of security incident management activities is to have well thought out processes in place to anticipate the most common exposures. **Mitigating Controls in place:** If the server stops, a customer will call the help desk causing beepers to go off telling the administrator to fix the problem. This will include designation of a scapegoat to take blame for the problem.		

#	Recommendation	The Risk to the Overall System	Cost to Implement
6	**Title: Default Umask Value was Inappropriate** We reviewed the default settings for Umask in /etc/security/.profile and noted that the umask command was not included. This means that the files created by the user will have a default value of; owner access = all, group access = read, execute and all others = read, execute for all other users (except root, who has access to everything.) "Every file (and directory) has permission bits. The owner can change them with the chmod command. The initial, default permissions set when a file is created are controlled by a parameter named umask. There is no way to enforce a standard value for users." [1p.94] **Recommendation:** The /etc/security/.profile command should include the line **umask 0077**, this will allow the owner full control of the file and no access to anyone else. **Mitigating Controls in place:** Machine is restricted to only a few users.	Default values leave the task up to the user to intervene to change the parameter. See Audit Program Step # 10.2 1 Related Prudent Practice Not Implemented	**Cost: Inexpensive** **Risk: Medium** Change default configuration. 1 hour (1* 350 = $350) Ongoing Process of review of accounts to enforce policy (4 * 350 = $1,400) Annually

#	Recommendation	The Risk to the Overall System	Cost to Implement
7	**Title: Unneeded System Installed Accounts Not Removed.** We used the Command: **more /etc/passwd** And noted the following: (Abstract) *uucp:!:5:5::/usr/lib/uucp:* *guest:!:100:100::/home/guest:* *nobody:!:4294967294:4294967294::/:* All users should be associated with a unique user ID to enforce accountability. Default accounts also supply potential intruders with known user names. **Recommendation:** Edit the /etc/passwd file to read as follows: uucp:*:5:5::/usr/lib/uucp: guest:*:100:100::/home/guest: nobody:*:4294967294:4294967294::/: An asterisk in the second field of a user ID indicates that the user is disabled. **Mitigating Controls:** The special purpose of this machine and place on the network limits remote logins.	Default users offer an attacker a known user name to use to attempt access to the system. Audit Program Step # 1.1 1 Related Prudent Practice Not Implemented	**Cost: Inexpensive** **Risk: Medium** Change default configuration. 1 hour (1* 350 = $350) Ongoing Process of review of accounts to enforce policy (4 * 350 = $1,400) Bi -Annually

#	Recommendation	The Risk to the Overall System	Cost to Implement
8	**Title: Files without owner or group** We used the Command: **/usr/bin/find / -nouser** and observed 32 files with no user listed in /etc/passwd. **Recommendation:** Use the **Chown** command to assign a valid user and group to these files. **Mitigating Controls in place:** Due to the limited login capability on this machine, this vulnerability is only available to users who can log into the machine.	Sensitive operating system files without adequate access control lists may pose a threat to the system if users access the files with malicious intentions. Audit Program Step # 6.9 1 Related Prudent Practice Not Implemented	**Cost: Inexpensive** **Risk: Medium** Clean up initial findings (12 * 350 = $4,200) Ongoing Process of review of files to enforce policy (4 * 350 = $1,400) Annually

#	Recommendation	The Risk to the Overall System	Cost to Implement
9	**Title: Segregation of Duties Not Implemented for Administrative Functions** We reviewed the contents of the /etc/security/user.roles file and noted that no users are assigned to roles. "Roles consist of authorizations that allow a user to execute functions that would normally require root user permission. These roles, allow for non-root users to be assigned portions of root privileges. Roles virtually eliminate the need to log on as root since they provide for almost all the common administration functions." 1p.50 Roles limit the amount of users with administrative functions and thus reduce the risk of impropriety, they also provide a segregation of duties for the system. The principle of Segregation of Duties provides for two people to be involved in every business transaction. This is achieved by a segregation of duties between the record keeping, approval and custody functions. The rationale is that the majority of business fraud involves one person acting alone, not in collusion with others. **Recommendation:** Assign users to roles according to job function. These roles should enforce the least privilege and segregation of duties concepts. **Mitigating Controls in place:** The root user account will be disabled and all SU commands to root will be logged.	Employees should only be given enough access to do their jobs. Also known as the least privilege concept. Job functions should provide for a segregation of duties to prevent fraud. Audit Program Step # 1.3 1 Related Prudent Practice Not Implemented	**Cost: Inexpensive** **Risk: Medium** Assign initial roles using segregation of duties principles. (12* 350 = $4,200)

#	Recommendation	The Risk to the Overall System	Cost to Implement
10	**Title: Create Policy and Standards** We proceeded with the audit by reviewing best practices, determining which ones where prudent by considering cost and risk and then comparing this to the configuration in place. This is a subjective practice that may not reflect the risk acceptance level that management desired for the resource. We were forced to do this because management did not perform a risk assessment for the resource that would let us know what security attributes the machine should employ. **Recommendation:** "Policy helps to define what a company considers to be valuable, and it specified what steps should be taken to safeguard those assets. Policy plays three major roles. It makes clear what is being protected, the responsibility for that protection and grounds in which to interpret later conflicts that might arise regarding the policy." [6 p.35] Giac Enterprises should consider crating a security policy. **Mitigating Controls in place:** Punishment mechanisms after a security events occur.	Without a security policy in place, no users will be formally accountable for security, and the computing assets most important to the organization may not be given priority in protection. Also a security policy for a specific machine, provides a metric for measuring a machine's compliance with policy. Often, system administrators are rewarded for availability and cost control, and maintainability, this sometimes causes a tradeoff with security. Policy and compliance monitoring helps ensure accountability for security and thus forces administrators to implement security although they may not want to. This was not in the prudent practice calculation because it is a management oversight activity, not a finding from audit tests.	**Cost: Inexpensive** **Risk: Medium** Develop Initial Policies (12* 350 = $4,200) Compliance Monitoring (12* 350 = $4,200) Bi-Annually This item was recommended in the top 10 for its minimal cost although the absence of a security policy does not mean that security will not be implemented, it increases the chance that it will be.

Comprehensive Audit Program and Results to Support the Audit Report.

Note1: These audit tests are designed whenever possible to provide independence to the auditor. To achieve independence, the auditor should be able to perform tests without reliance on the system administrator or administrator privileges. Ideally this would be performed with Audit software; unfortunately, none is available at a reasonable cost. As part of this project GIAC enterprises has commissioned Mustache Enterprises to perform the tasks of creating an audit script to be used in a future self audit. Mustache has agreed, provided that the script can be submitted to the ***Security Consensus Operational Readiness Evaluation*** www.sans.org/SCORE/ to assist the audit community. Tests were designed so the auditor can just request the output of files, without having administrator privileges. All of the commands will output to files for evidential matter.

Note 2: This is a risk based audit. Items judged as low risk will not be addressed because of limited resources. Additionally, addressing low risk items may be best practice but it is not prudent (cost effective) practice. The limited use of this machine also eliminated risks and thus audit steps.

Scores

Best Practice = +1 (to much control) - Steps do not appear in audit program because they do not make business sense.

Prudent Practice Implemented = 0

Low = -1 (not enough control) - Low risk steps to not appear in the audit program because they do not make business sense. However, if a prudent practice is not implemented a –1 is given.

Below are hyperlinks to the audit program

KEY - What you type is in **bold**, computer output is in *Italics*. H = High Risk, M= Medium Risk and L= Low Risk.

#	Audit Test Description	Explanation of Risk (why I am doing this)	Audit Tests (How I am doing this) Note 1 Note 2	Results & W/P Ref	Consequence	Likelihood	Score	Ref.
1.0	**Logon Restrictions**							
1.1	User Accountability	Ensure individual user accountability by ensuring that all users have a unique user ID	Use the **usrck** command or perform manually by using the command: **more etc/passwd > etc/wp/1.1** – if the third operand in the UID command is the same than users are sharing a UID. Also, each user should have a unique user ID that they are accountable for.	Finding # 7	M	M	-1	1p.153
1.2	**Login Banner** Change login banner	If login banner is not changed, valuable information such as operating system could be enumerated before login and could assist an intruder.	Type command **more /etc/security/login.cfg > /etc/wp/1.2** The message after the command herald = Should contain a restrictive login banner.	No Exception Noted in Test	M	M	0	1p.36

#	Audit Test Description	Explanation of Risk (why I am doing this)	Audit Tests (How I am doing this) Note 1 Note 2	Results & W/P Ref	Consequence	Likelihood	Score	Ref.
1.3	Segregation of Duties	The principle of Segregation of Duties provides for two people to be involved in every business transaction. This is achieved by a segregation of duties between the record keeping, approval and custody functions. The rationale is that the majority of business fraud involves one person acting alone, not in collusion with others.	Use the Command: **more /etc/security/user.roles > /etc/wp/1.3** verify that roles are defined in the file to specific user ID's.	Finding # 9	H	H	-1	1p.50

#	Audit Test Description	Explanation of Risk (why I am doing this)	Audit Tests (How I am doing this) Note 1 Note 2	Results & W/P Ref	Consequence	Likelihood	Score	Ref.
2.0	**Password Restrictions**							
2.1	Verify that default user stanza password settings are changed with the chsec command or by editing the /etc/security/ : user, limits, login.cfg, mkuser.default and mkuserfile.sys files.	The defaults in /etc/security/user and /etc/security/limits are used for every user every time they log in. It can be used to suggest prudent practice for every user. Unfortunately, users can be customized so sampling must still take place.	Type command **more /etc/security/user > /etc/wp/2.1.4** verify that the password settings agree to corporate policy and best practice. **more /etc/security/limits > /etc/wp/2.1.1** **more /etc/security/login.cfg > /etc/wp/2.1.2** **more /etc/security/mkuser.default >/etc/wp/2.1.3** **more /etc/security/user > /etc/wp/2.1.4** ***Challenge / Response*** – Attempt to create a new account with a password that does not conform to the standards and verify the system does not accept the attempt.	No Exception Noted in Test	M	M	0	1p.30

#	Audit Test Description	Explanation of Risk (why I am doing this)	Audit Tests (How I am doing this) Note 1 Note 2	Results & W/P Ref	Consequence	Likelihood	Score	Ref.
2.2	Verify passwords are defined for all users in the Shadow Password File	Since /etc/passwd is world readable passwords must be linked to the UID strings in the shadow password file not available for cracking or reading, except by root.	Get the contents of the /etc/password file Command: **more /etc/password > /etc/wp/2.2** The second field in the /etc/passwd file (the file is delimited by colons) is the password field. Verify that all password fields have a exclamation mark in the second field. This means that they are using the shadow password file, the ! acts as a pointer to the shadow password file. Audit findings could be: A Null Entry = no password An Asterisk = Disabled user An Encrypted Password – always 13 characters long.	No Exception Noted in Test	M	M	0	1p.42
2.3	Verify only authorized users can use outbound FTP	Users should only be given access enough to perform their job. Also known as the "Least Privilege concept"	Command: **more /etc/ftpusers > /etc/wp/2.3** verify that this file is created and only approved users can use the file.	No Exception Noted in Test	M	M	0	1p.42

#	Audit Test Description	Explanation of Risk (why I am doing this)	Audit Tests (How I am doing this) Note 1 Note 2	Results & W/P Ref	Consequence	Likelihood	Score	Ref.
3.0	**Root User**	Access to files and directories owned by root may gain unauthorized access to files and directories to which root is also a member.	Command: **More lsgroup –n ALL** Verify all files owned by group are appropriate.	No Exception Noted in Test	M	H	0	2p.91
3.1	Limited Superuser Access	Ensure only authorized individuals have administrator privileges.	using **more etc/passwd > etc/wp/3.1** command look for UID of 0, this means that they have administrative (root) privileges. Also use more /etc/security/user for users with a admin = true entry Verify that this level of access is approved and a justification of why the **su** command or roles are not used as an alternative.	No Exception Noted in Test	H	H	0	1p.17
3.2	See Above	See Above	Members of the security group also constructively have root privileges. Verify that members of the security group are authorized.	No Exception Noted in Test	H	H	0	1p.34
3.3	See Above	See Above	Verify that the root user is disabled. Command: **smit chuser** select the root account. Verify that the following two lines in the users characteristics are as follows. User can LOGIN? false User can LOGIN REMOTELY? false	Finding # 3	M	M	-1	1p.20

#	Audit Test Description	Explanation of Risk (why I am doing this)	Audit Tests (How I am doing this) Note 1 Note 2	Results & W/P Ref	Consequence	Likelihood	Score	Ref.
3.4	Suid and Guid Files	See Above	Review a list of all SUID and GUID programs and verify they are prudent. **Find / -type f –perm 4000 – exec ls –aeo {} \; > /etc/wp/suid.files** And for GUID Command : **Find / -type f –perm 2000 – exec ls –aeo {} \; > /etc/wp/guid.files**	No Exception Noted in Test	H	H	0	2p.122
4.0	**Log Review**							
4.1	Security Log Monitoring	Verify that uses of administrative privileges are not abused. Also verify that only users with administrative privileges **su** to root and within their own accounts. If an administrator SU's to a root account from within an account with less privilege than and a Trojan Horse is present, a user may be able to steal the root account password.	All su events are kept in the logs. Use the **more /var/adm/sulog | grep –e' –root' > /etc/wp/4.1** command. Note that + is a success and – is a failure.	No Exception Noted in Test	H	H	0	1p.171 and 2p.55
4.2	See Above	Verify error log is turned on and security related errors are investigated promptly.	Review the error log for security related messages. Command = **errpt | pg > /etc/wp/4.2**	No Exception Noted in Test	H	H	0	1p.106
4.3	See Above	Unusual events are sometimes an indicator of malicious activity.	Look for an unusual amount of failed login attempts use the Command: **who /etc/security/failedlogin > /etc/wp/4.3**	No Exception Noted in Test	H	H	0	4p.230

#	Audit Test Description	Explanation of Risk (why I am doing this)	Audit Tests (How I am doing this) Note 1 Note 2	Results & W/P Ref	Consequence	Likelihood	Score	Ref.
4.4	See Above	See Above	Look for unusual (for example, after hours or unusually long) login activity Command: **last > /etc/wp/4.4**	No Exception Noted in Test	H	H	0	4p.230
4.5	See Above	Look for failed attempts to communicate with the machine. This activity may be a prelude to an attack. Note this procedure is performed in lue of installing IP Filters.	Use Command **netstat –p tcp** to look for failed connection attempts. Use Command: **netstat – p udp** and **netstat –p icmp** and **netstat –p ip** Verify failed connection attempts are followed up upon timely.	No Exception Noted in Test	H	H	0	7p.152
4.6	See Above	IP filtering are based on rules that must match management's intentions.	Used the Command: **smit ips4_advanced** and selected the option: **List Active IP Security Filter Rules** to verify that IP filters are activated an unsuccessful attempts are logged.	See Finding #4	H	H	-1	1p.142
5.0	**Change Control and Virus Protection**							
5.1	Implement Tripwire and a change control process. AIX has a tool similar to tripwire called Trusted Computing Base (TCB)	Since commercial virus scanners are not readily available for Unix systems change control is of importance.	Use the **virscan / > /etc/wp/5.1** command that comes with AIX to search for pc viruses on the entire file system.	No Exception Noted in Test	H	H	0	1p108

#	Audit Test Description	Explanation of Risk (why I am doing this)	Audit Tests (How I am doing this) Note 1 Note 2	Results & W/P Ref	Consequence	Likelihood	Score	Ref.
5.2	See Above	Good change control would prevent viruses and unauthorized changes.	Verify that TCB is installed. Use the Command: **tcbck –n –tree > /etc/wp/5.2** and verify sensitive files are defined to it.	No – see finding #2	H	H	-1	1.p114
5.3	See Above	Good change control would prevent viruses and unauthorized changes.	The parameters and base image for TCB are kept in the sysck.cfg file. Verify that a copy of this file is kept off line.	No – see finding #2	H	H	-1	2p.211
5.4	See Above	Good change control would prevent viruses and unauthorized changes.	Verify the TCB maintains its secure status. Use the command **/bin/tcbck -n ALL > /etc/wp/5.4** (the –n flag causes inconsistencies to be reported but not to update sysck.cfg.) Before this command is run, a trusted version of sysck.cfg should be loaded from an off line storage location, see previous step.	No – see finding #2	H	H	-1	2p.41
5.5	See Above	Good change control would prevent viruses and unauthorized changes.	Review the contents of the sysck.cfg and verify that sensitive files are under TCB change control.	No – see finding #2	H	H	-1	2p41
6.0	**Housekeeping**							
6.1	Verify consistency of related databases.	Housekeeping prevents security weaknesses by making the system easier to maintain and increases the chance that the system will operate as intended.	The **grpck –t ALL** command verifies that all group members are defined as users	No Exception Noted in Test	H	H	0	1p.55

#	Audit Test Description	Explanation of Risk (why I am doing this)	Audit Tests (How I am doing this) Note 1 Note 2	Results & W/P Ref	Consequence	Likelihood	Score	Ref.
6.2	See Above	Determine if all users of the system follow the company standards for security.	The **Usrck –t ALL** This command checks for consistency of the files used for user management.	No Exception Noted in Test	H	H	0	1p. 55
6.3	See Above	Housekeeping prevents security weaknesses by making the system easier to maintain and increases the chance that the system will operate as intended.	The **pwdck –t ALL** compares the password and shadow password files for consistency	No Exception Noted in Test	H	H	0	1p.56
6.4	Password Cracker	Determine if all users of the system follow the company standards for passwords.	Verify the passwords are strong by running the program Crack.	No Exception Noted in Test	H	H	0	N/A
6.4	System Software	Only authorized systems software should be installed	Command: **lslpp –1 > installed.software** Verify only authorized software is installed.	No Exception Noted in Test	H	H	0	1p.127
6.5	System Hardware	Only authorized system hardware should be installed.	Command: **lsdev –C | sort –d –f > installed.hardware** Verify only authorized hardware is installed.	No Exception Noted in Test	H	H	0	1p.128
6.6	Inactive users	If a user is inactive it is a good sign that they are either dead or not working at Giac anymore. Old unused user ID's pose the potential risk of an imposter using the ID or a disgruntled former employee gaining access.	Command: **more /etc/security/lastlog >/etc/wp/6.6** The command lists each user and the time_last_login = stanza shows the time in seconds since Jan 1, 1970 that the user last logged in. Users that have not logged in 45 days should have their user ID removed from the system.	No Exception Noted in Test	H	H	0	1p.40

#	Audit Test Description	Explanation of Risk (why I am doing this)	Audit Tests (How I am doing this) Note 1 Note 2	Results & W/P Ref	Consequence	Likelihood	Score	Ref.
	Physical Controls							
6.7	Place CPU in controlled environment	If physical control can be achieved, logical control is easily obtained.	Verify that physical security is achieved.	No Exception Noted in Test	H	H	0	N/A
6.8	Set User ID (SUID) Audit	The SUID function allows a user to execute a program that adopts the authority of the owner of the file. If the owner is root than the user is acting with root authority within the confines of the program.	Verify that files owned by root with the x bit in the user set to s in the owners permission block are appropriate.	No Exception Noted in Test	H	H	0	1p.90
6.9	All files must have an owner to ensure they are being shared with the intended parties.	Sensitive operating system files without adequate access control lists may pose a threat to the system if users access the files with malicious intentions.	Verify all files are assigned to a specific user. Command: **/usr/bin/find / -nouser > /etc/wp/6.9**	See Finding # 8	H	M	-1	1p.96
7.0	**Auditing**							
7.1	Verify server audit logs are reviewed.	As the computer is the record keeper and has custody of assets the only way to achieve a segregation of duties is to monitor user actions with the auditing function.	Verify auditing is turned on every time the system is started by looking in the initialization file. Command: **more /etc/rc > /etc/wp/wpaudsrt** verify that the line: /usr/sbin/audit start appears in the file.	See Audit Finding #1	M	H	-1	2p.47

#	Audit Test Description	Explanation of Risk (why I am doing this)	Audit Tests (How I am doing this) Note 1 Note 2	Results & W/P Ref	Consequence	Likelihood	Score	Ref.
7.2	See Above	See Above	Review the contents of the events file and verify the following is defined. Command: **more /etc/security/audit/events > /etc/wp/7.2** • Changes to the TCB • Changes made to suer and group profiles. • The creation and deletion of any user and group. • System initializations • Installation of software • Changes made to system configuration (new devices in /dev directory, changes to the rhosts, inetd.conf or profile files in the /etc directory and changes to the /bin directory) • Changes to the /etc/security/ files including; audit, group, limits, login.cfg, passwd and user.	See Audit Finding #1	M	H	-1	2p.47
7.3	See Above	See Above	Use the **auditpr –t2 > /etc/wp/7.3** command to read the audited events. A process should be in place to follow up on any anomalies.	See Audit Finding #1	M	H	-1	2p.47
7.4	See Above	See Above	Verify audit logs are in place. Command: **auditpr -v < /audit/trail**	See Audit Finding #1	M	H	-1	2.p47
7.5	Verify Auditing is started every time the machine is started.	Automated practices are more reliable than manual processes.	Command: **more /etc/rc** verify that the **/usr/sbin/audit start** command is in the file.	See Audit Finding #1	M	H	-1	2.p47

#	Audit Test Description	Explanation of Risk (why I am doing this)	Audit Tests (How I am doing this) Note 1 Note 2	Results & W/P Ref	Consequence	Likelihood	Score	Ref.
8.0	**Network Security**							
8.1	Take an inventory of network interfaces	Know what you are auditing	Command: **ifconfig –a > /etc/wp/8.1**	No Exception Noted in Test	M	M	0	6p.27
8.2	Verify authorized services are running	Only services needed should be running. In the case of this implementation only FTP should be running.	Review the TCP/IP services running. Command: **more /etc/inetd.conf > /etc/wp/8.2** Verify that only authorized services are running.	No Exception Noted in Test	H	H	0	2p.57
8.3	Note this implementation does not require NIS, NFS or UUCP so these services are disabled.	Only authorized remote systems should be able to gain access.	Review the hosts that are trusted. **More /etc/hosts.equiv > /etc/wp/8.3** (note: + means allow) or IP addresses that are trusted **More /etc/hosts > /etc/wp/8.3.1**	No Exception Noted in Test	H	H	0	2p.60
8.4	Review network services running.	Only services needed should be running. In the case of this implementation only FTP should be running.	Review internet services running. Command : **more /etc/rc.tcpip > /etc/wp/8.4** and **more /etc/inittab > /etc/wp/8.4.1** verify that no unneeded network services are running. This machines should only be running FTP.	No Exception Noted in Test	H	H	0	2p.61
8.5	Challenge / Response test to verify	Only services needed should be running. In the case of this implementation only FTP should be running.	Command for TCP: **Nmap –sT –O 10.10.10.55** Note: 10.10.10.55 is the address of the FTP server In the Giac DMZ. Command for UDP: **Nmap –sU –O 10.10.10.55**	No Exception Noted in Test	H	H	0	6p.206

#	Audit Test Description	Explanation of Risk (why I am doing this)	Audit Tests (How I am doing this) Note 1 Note 2	Results & W/P Ref	Consequence	Likelihood	Score	Ref.
8.6	Review IP Filter Ruleset	See Above	We used the Command: **smit ips4_advanced** and selected the option: observed the results Can not open device /dev/ipsec4_filt. This result was noted because IP filtering and logging was not implemented.	See Audit Finding #4	H	H	-1	1p.142
9.0	**Backup policies and disaster preparedness**							
9.0	Business Recovery Plan (BRP)	Without a backup plan for business functions and computing resources, business activity may not be recoverable in the desired period of time.	Verify that management has a documented business recovery plan. A business recovery plan is essential to recover non computer related business functions in the case of a disaster.	No Exception Noted in Test	H	H	0	
9.1	Disaster Recovery Plan (DRP)	See Above. Backups and disaster recovery are a corrective control. Preventative controls are better.	Verify that the company has a documented disaster recovery plan.	No Exception Noted in Test	H	H	0	
9.2	BRP and DRP Testing	Unless a plan is regularly tested, there is no guarantee that it will function as intended.	Verify that the company has a test plan and have they conducted tests of their business recovery and disaster recovery plan.	No Exception Noted in Test	H	H	0	

#	Audit Test Description	Explanation of Risk (why I am doing this)	Audit Tests (How I am doing this) Note 1 Note 2	Results & W/P Ref	Consequence	Likelihood	Score	Ref.
9.3	See Above	Media must be backed up daily and kept off site. To be recovered in the case of an emergency.	Verify data is backed up daily and a copy stored off site.	No Exception Noted in Test	H	H	0	
9.4	See Above	Backup media must be tested periodically for readability to ensure that data can be restored.	Verify data backup media is tested for readability.	No Exception Noted in Test	H	H	0	
9.5	See Above	An accurate inventory verifies the correct data is offsite.	Compare the inventory of data held off site with what is actually there and verify that the inventory is accurate.	No Exception Noted in Test	H	H	0	
10	**Miscellaneous**							
10.1	Common Exploit Prevention	Protect users that use the SU command from Trojan programs.	Verify that the PATH= statement in /.profile, etc/profile and /etc/environment do not contain the "." In the search path.	No Exception Noted in Test	M	M	0	5p.45
10.2	Default file permissions	Default values leave the task up to the user to intervene to change the parameter.	Verify that the Umask value is appropriate. Command: **more /etc/security/.profile > /etc/wp/10.2**	See Finding #6	M	M	-1	1p.32
10.3	Physical Port Security	Users of alternate physical login ports should be given least privilege and follow password login policy.	Type command **more /etc/security/login.cfg.** Verify that default settings in /etc/security/login.cfg to restrict port settings to authorized personnel.	No Exception Noted in Test	M	M	0	1.p.31
10.4	Security scanner	Just checking if I overlooked anything.	Run the security scanner Nessus and verify that the system is not vulnerable to any items in the Nessus database.	No Exception Noted in Test	H	H	0	

If you did not see an audit step it is because the consultant considered the step low risk. For example, Terminal Timeouts, and restricted shells are considered low risk because this system is physically secure. Soft limits such as file size and CPU units were also not restricted because of the machines purpose.

NFS – mounting remote file systems and NIS – Network Information Systems, used for sharing a single userID and password for several machines in a network; and DNS – used for resolving host names to IP addresses, will not be used due to their security implications.

Appendix B: Script for Gathering Audit Information

```
#!/bin/ksh
#This is a korn shell script for gathering your audit information
#Just copy this into vi or your favorite UNIX editor, don't forget to chmod the file
for execution
Mkdir /etc/wp
more etc/passwd > etc/wp/1.1
more /etc/security/login.cfg > /etc/wp/1.2
more /etc/security/user.roles > /etc/wp/1.3
more /etc/security/limits > /etc/wp/2.1.1
more /etc/security/login.cfg > /etc/wp/2.1.2
more /etc/security/mkuser.default >/etc/wp/2.1.3
more /etc/security/user > /etc/wp/2.1.4
more /etc/password > /etc/wp/2.2
more /etc/ftpusers > /etc/wp/2.3
more etc/passwd > etc/wp/3.1
Find / -type f –perm 4000 – exec ls –aeo {} \; > /etc/wp/suid.files
Find / -type f –perm 2000 – exec ls –aeo {} \; > /etc/wp/guid.files
more /var/adm/sulog | grep –e' –root'  > /etc/wp/4.1
errpt | pg > /etc/wp/4.2
who /etc/security/failedlogin > /etc/wp/4.3
last > /etc/wp/4.4
virscan / > /etc/wp/5.1
tcbck –n –tree > /etc/wp/5.2
/bin/tcbck -n ALL > /etc/wp/5.4
grpck –t ALL /etc/wp/6.1
Usrck –t ALL /etc/wp/6.2
pwdck –t ALL /etc/wp/6.3
lslpp –1 > /etc/wp/installed.software
lsdev –C | sort –d –f > /etc/wp/installed.hardware
#All the file numbers coincide with audit steps so the script is self documenting
more /etc/security/lastlog >/etc/wp/6.6
/usr/bin/find / -nouser > /etc/wp/6.9
more /etc/rc > /etc/wp/wpaudsrt
more /etc/security/audit/events > /etc/wp/7.2
auditpr –t2 > /etc/wp/7.3
more /etc/rc > /etc/wp/7.5
ifconfig –a > /etc/wp/8.1
more /etc/inetd.conf > /etc/wp/8.2
more /etc/hosts.equiv > /etc/wp/8.3  (
more /etc/hosts > /etc/wp/8.3.1
more /etc/rc.tcpip > /etc/wp/8.4
more /etc/inittab > /etc/wp/8.4.1
more /dev/ipsec4_filt > /etc/wp/8.6
```

```
more /etc/security/.profile > /etc/wp/10.2
more /etc/security/login.cfg > /etc/wp/10.3
print “I am done”
```

References

1. Kosuge, Yoshimichi; Armingaud, Francois; Chew, Lip-Ping; Horne, Leonie; Witteveen; AIX 4.3 Elements of Security Effective and Efficient Implementation, International Business Machines (IBM), August 2000
2. Unknown, Audit, Control and Security Features of the AIX Operating System, Ernst and Young, 1995
3. UNIX: Its Use, Control and Audit, Information Systems Audit and Control Foundation and the Institute of Internal Auditors Research Foundation, 1995.
4. Cannon, Casey; Trent, Scott; Jones, Carolyn; Simply AIX 4.3, New Jersey; Prentice Hall, 1999
5. Simson, Garfinkel; Spafford, Gene; Practical Unix Security ; New Jersey; O'Reilly and Associates, Inc., 1991
6. Hatch, Brian; Lee, James; Kurtz, George; Hacking Linux Exposed, New York, Osborne / McGraw-Hill, 2002
7. Unknown "AIX Security Checklist", http://www.cop.vt.edu/unix/aix.security.html (December 11, 2001)
8. Pomeranz, Hal; Green; Acheson; Brotzman, Lee; GCUX Course Materials, The SANS Institute, 2002
9. Laurent Vanel, Rosabelle Zapata-Balingit, Gonzalo R. Archondo-Callao, "Auditing and Accounting on AIX", http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg246020.pdf , IBM (January 11, 2002)

Last Updated: July 25th, 2017

Upcoming Training

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