Global Information Assurance Certification Paper

Consultant's Auditing Report for a Unix Business-to-Business Server

Securing UNIX
GCUX Practical Assignment
Version 1.8

Jack Stinson

May 24, 2002

Table of Contents

1.0 Executive Summary

GIAC Enterprises is a small company that utilizes web-based business transactions as part of its business. This report provides the results of an audit of the GIAC test and development business server, DEV.GIAC.ORG, a Sun Blade 100 system running the Solaris 8 operating system with the default Sun installation. The main application running on the server is a business-to-business server; two other applications, sudo and SSH, provide developer and system administrator access.

The audit evaluated a large number of parameters and operating conditions, including hardware, operating system, application software, physical security, network operation and firewall operation. The auditor performed two external scans on the development server from adjacent hosts, and also executed two internal scans. In addition, the auditor conducted interviews with management, developers and system administrators, and performed specific reviews of operational characteristics and configuration files. The analysis provided a very complete picture of the security state of the computer and network, and the business operation environment.

The server is a test and development server that is used by software developers to test software operation and data interchange with business partners. Because of the development nature of the server, public access is blocked by the firewall. Access from the Internet to the server is limited to either SSH connection or SSL connection. Because of the firewall and encrypted connection protocols, the server security is good but could be improved. Table 1, provides a list of key security issues and their impacts.

Table 1: Summary of Critical Issues and Their Impact

Issue – Impact
CVS system - Software is exposed on a public web server.
Sudo restrictions - Users shell out of sudo because they have access to all commands.
No cron, lpr, uucp and news entries in syslog - There is no logging in syslog to trace key events or provide archiving.
Sa1 and Sa2 are not running - System activity reports are not created.
Default cron.deny with no cron.allow – Users can create jobs to run using cron without system admin approval.
Patches are not current - System is vulnerable to known security issues.
No record of failed logins - Automated attempts to break-in would not be detected.
Stack is executable - Buffer overflows may allow dangerous code to be executed.
Processes running that are not needed - A number of processes not required by the system are running. They use computer resources and some have known security issues.
Non-Standard SUID programs - These run as root when any user runs them, but it is not needed.

A description of the server and its supporting components and the audit methods used in the audit are described in section 2, Description of System and Audit Methodology. The issues discovered and the analysis of these issues are described in section 3, Detailed Analysis. The summary of the most critical issues, their impacts and recommendations for risk mitigation are described in section 4, Critical Issues and Recommendations.

2.0 Description of System and Audit Methodology

This audit was conducted for GIAC Enterprises is a small company that utilizes web-based business transactions as part of its business. It addressed the business transaction test and development server and its associated network infrastructure as well as the business operational environment. The purpose of the audit was to examine, individually and collectively, the security of the test and development server's hardware, operating system parameters, application software parameters, physical access conditions, network operating conditions, firewall operation and to evaluate them in terms of GIAC's business and operational environment. The audit provided information on the characteristics of the examined components, how they impact security and operation of the server, and how they can be adjusted to improve security and continuity of operation.

2.1 Business Mission of GIAC Enterprises

GIAC has two business-to-business (B2B) servers. One is the operational server and the other is the testing and development server. The operational server system supports business-to-business purchasing transactions between several large businesses and a group of selected vendors. The business submits a request-for-quote for a product to the operational server where it is parsed and posted to the web server to be downloaded by an offsite system. The offsite system is accessed by vendor's to determine if they have or can make the product. Vendor's reply to the offsite system which uploads bid/no bid responses to GIAC's operational server. These responses are downloaded to the business. The operational server supplies the interface between business electronic commerce systems and vendor electronic commerce systems. Because of the nature of the businesses, RFQs are submitted no more than once an hour with a vendor response time of two hours. All uploads and downloads use SSH or SSL.

The test and development server provides a means of testing the connectivity from various partners as well as the parsing of various electronic forms. All uploads and downloads are tested using SSH or SSL just like the operational server. The software that provides the parsing and initiates the connections between systems is debugged on the development server. When new businesses or vendor are added, connectivity is established and software is written to parse the incoming and outgoing data. When testing has been completed, the new software is moved to the operational server. Since the operational server is a production machine, it is important that all the software and connections work properly the first time.

2.2 System Description

2.2.1 System Overview

An overview of the system infrastructure is shown in Figure 1. The test and development server path to the Internet goes from the server, to a switch, to the firewall, to a gateway router and to the Internet. This pathway will be our area of focus. The paths to the system administrators' computers and developers' computers vary somewhat after leaving the firewall, but involve other firewalls and switches.

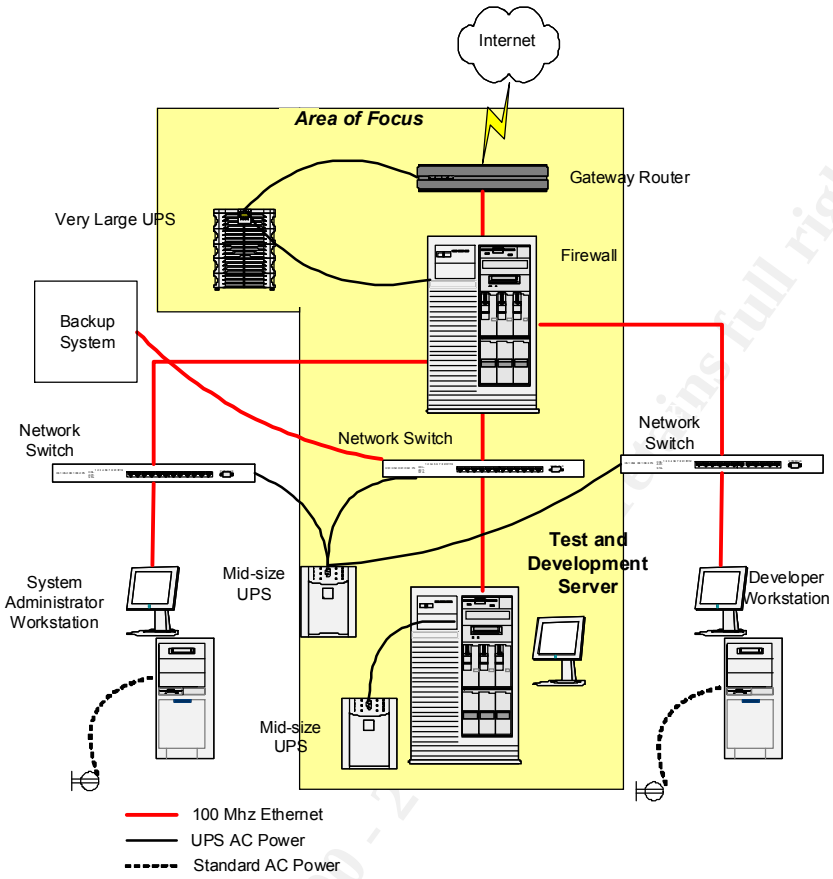

Figure 1- System Infrastructure

2.2.2 Operational Usage of System

The audited computer system is used in the testing and development of a business-to-business (B2B) transaction environment. It has two host names and IP Addresses, dev.giac.org and dev-test.giac.org. While these two names and addresses are for the same computer, this configuration allows developers to develop software and test it internally before testing it with outside clients. Developers use the computer to create software that parses and analyzes dummy electronic B2B purchase request forms from a business customer, and then outputs a dummy electronic request for bid forms to compatible suppliers. Communication between the system, customer and potential suppliers is via the Internet using either SSH or SSL connections. When the software is determined to be stable, it is installed on a different server and actual B2B transactions occur.

2.2.3 System Hardware Description

The DEV.GIAC.ORG computer system was purchased specifically for the B2B application and is used strictly for B2B testing and development. A physical examination of the system and its operational characteristics produced the following hardware configuration data:

SUN Blade 100 computer	DVD/CD-ROM drive
1 Gigabyte of memory	SCSI ports
20 Gigabytes of internal disk storage	USB ports
18 Gigabytes of external disk storage	Smartcard reader
Keyboard, mouse, monitor	100/10 Megabit per second Ethernet interface

Impact of Findings/Improvements – The system is a recent model, capable of running the most current version of the operating system and is dedicated to the B2B application and its supporting software. These factors lessen the potential for security problems.

2.2.4 Major Software Applications

The main software application running on the server is the commercial B2B webserver that provides B2B data exchange. The software running is the current version. Two other applications provide support to the developers: OPENSSH, a user supported version of secure shell (SSH); and sudo, a free restricted command application. These applications are also the current version and were downloaded from a well known site. They are more fully described in section 3.

Impact of Findings/Improvements – The vendor software is well known and used extensively in the computer industry. The two non-commercial applications are well known in the industry and are stable. They were obtained from a trusted site. The security of these applications depends on: keeping the most current version; and installing patches installed and on their configuration.

2.3 Audit Methodology

The audit consisted of a series of evaluations. For the test and development server, the auditor examined the following key items: system and application configuration files, log files, system services, and active applications. Next external scans of the server were performed using Nmap and ISS. [2,3] Internal scans were performed on the server with the lsof tool and CIS Solaris Benchmark tool. [10,13] In addition, evaluations of the physical environment for the area of focus were performed and an overall network evaluation was performed. Also, interviews with management, developers and system administrators were conducted and reviews of operational characteristics and configuration files were performed.

Impact of Findings/Improvements – No audit can be absolutely complete. However, by using different methods to gather and review the information a reasonable coverage of the complete system can be obtained.

3.0 Detailed Analysis

3.1 Server Physical Environment

Security addresses not only Internet hacking attacks, but anything that causes a denial of service (unavailability) or a loss or corruption of data. Therefore the physical environment of the test and development server is important. An audit of the physical environment by physical examination and meetings with management produced the following observations:

Observation	Impact
Computer is located in a lab with other systems. It is in a separate area, but the area is not enclosed. Access to the lab at night is controlled by security card. Access to the building is controlled by security card and guard.	While the system is protected from most external access risks, there is little protection for internal access risks.
Lab has sprinkler system and a fire extinguisher.	A fire in the lab posses the risk of water or smoke damage to the system. If this occurs, it could take several weeks to restore full operation.
Computer, monitor and external drive are connected to a 1250 VA UPS. There are no control connections between the UPS and computer for loss of power shutdown and restart.	UPS The UPS rating is sufficient for short term (5-10 minutes) power interruptions. If longer operation is needed, a larger UPS can provide 30 minutes to several hours of service. Also, longer periods of operation are meaningless if other equipment in the network shutdown because of a power outage.
HVAC is sufficient for computer lab operation, but HVAC will not function with loss of power nor is there any redundancy in the HVAC system.	The loss of HVAC during the summer will make long term operation of all lab computers impractical. A few systems (servers) can continue operating if needed without being immediately impacted by the heat.

Impact of Findings/Improvements – Based on meetings with management and developers, they felt that UPS ride-through was sufficient to allow continuous operation. Interruptions long enough to outlast the UPS systems occurs only three or four times a year. Since the server is a development machine and long term outages occur infrequently, management does not feel that the additional cost for generators or large UPS systems is justified. A control connection should be established between the UPS and computer to allow for automated controlled shutdowns. Software for this is available from the UPS manufacturer. Management felt that expenditures for redundant

HVAC systems or for generators to power HVAC systems to ensure continuity of operation could not be justified given the long payback period due to infrequent usage.

Physical access to the server is fair and could be improved by putting the test and development server and all other servers into an enclosed area that could be controlled by badge access privileges. Business operational policy is that badges are provided to only to employees and contractors. Management feels that the current operational environment in the lab is sufficient to protect equipment.

The enclosed area would also provide additional fire protection. A worst case fire in the lab could disrupt some operations for several weeks. In this case rapid replacement of the hardware and restoration from back up tape would need to occur. Management and system administrators felt that the current fire suppression system is sufficient. They feel that the cost of additional efforts is not cost effective.

3.2 Network Infrastructure

The key components of the GIAC network infrastructure are shown in Figure 2. The key components not only include the test and development server but also the firewall, network switch, Internet gateway, and network backup system.

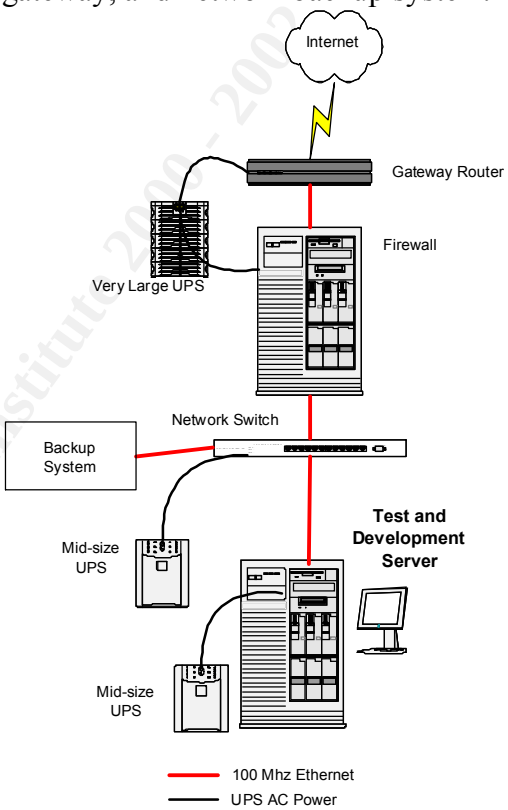

Figure 2- Key Network Infrastructure

3.2.1 Firewall

The Firewall is a major component of the defense in layers security scheme by ensuring that the trust between the server and all other systems is limited to the appropriate level. An audit of the Firewall by physical examination, rule review and discussions with the firewall administrator determined the following:

Network access to the development server is open to all computers on the system administrator network.	Firewall is physically located in a locked computer room with access limited only to network support personnel.
Access to the development server from the developer's network is limited to SSH, http, https, and B2B server port.	Firewall and associated equipment are protected by an automated fire suppression system.
Access to the development server from the Internet is limited to SSH, https, and B2B server port.	Backup power is supplied by a large UPS system that will provide 24 hours of operation.
Outgoing access to the Internet is not limited.	All network interfaces to the firewall are 100 Megabit per second (Mb/s)
Review of the logs for a three month period show 22 cases where the development server was scanned for SSH.	Firewall supports two subnets. One with three web servers and the other with eight Unix workstations including the development server.
Heavy scanning of all company IP Addresses was noted in the firewall log.	No throughput issues were noted.
The Firewall connects to the Internet gateway.	

Impact of Findings/Improvements – The Firewall is configured using "deny-all" methodology. All IP addresses, protocols, and ports not specifically allowed are denied. The number of rules in the Firewall is balanced so that throughput is not impacted. Internal networks have more access than external networks. Outgoing access should be limited on machines (e.g. servers), which are more likely to be at risk, to limit damage if they are compromised. Incoming scans may be looking for system vulnerabilities which can led to possible system compromise.

3.2.2 Network Switches

The switches provide a concentration point for network traffic. The development server, system administrator computers and developer computers are connected to different switches. An audit of a typical switch by physical examination and discussions with the network administrator indicated the following:

Configured for 100Mb/s full duplex network.	Switches are physically located in locked closets with access limited only to network support.

Switch has 1450 VA UPS which shared by several switches. This provides sufficient protection for short term power interruptions.	Switch closets are constructed with firewalls (floor-to-floor walls).

Impact of Findings/Improvements – Switches are generally secure, but will only provide short term (5-10 minutes) operation during a power failure. If longer operation is required, larger UPS systems must be installed here and in conjunction with an UPS upgrade at the development server.

3.2.3 Internet Gateway

The Internet Gateway provides a demarcation between the local network and the Internet. An audit of the Internet Gateway by physical examination and rule review is as follows:

Physically located in same room as the firewall.	T1 connection shared by all building tenants. Usage run 50-85% on a typical day.
Connected to multiple Firewall via a switch.	Incoming and outgoing filtering of the major Trojan programs and Windows authentication ports. Address spoofing filters are in place.

Impact of Findings/Improvements – T1 is reaching the limits of its service. Configuration provides maximum throughput. Filtering, even though limited, provides an excellent way to minimize unwanted traffic on firewalls, as well as providing protection against harmful outgoing traffic.

3.2.4 Backups

Continuity of operations demand that appropriate protection be given to data and software. Backups provide this protection if they are properly implemented. An audit of the development backup system by physical examination, configuration review and discussions with the system administrator determined the following:

Backup logs are created on the local machine and emailed to system administrators. Emailed logs showed disk failure on one drive of the development server.	Monthly backup tapes are kept for two years and then used again.
System administrators review emailed backup logs daily to make sure that backups were properly performed.	Backup tapes are not regularly tested by restoring selected files.
Backup is performed over the network to a central location.	Weekly tapes are kept in an unlocked cabinet.

All the lab computers are backed-up on the same tape.	Monthly tapes are kept in a fireproof vault.
Full backups of system and data are created monthly and require two tapes. This operation is executed on select machines over two nights.	No offsite tape storage occurs.
Incremental backups are performed daily.	Same type of tape hardware and software is used to backup other systems.
Weekly backups require one tape. Incremental backups are performed daily, except for Friday when a level 4 backup is performed. Tapes are changed weekly.	

Impact of Findings/Improvements – Multiple logging provides maximum opportunity to detect system failure as indicated by the detection of a server disk failure through emailed logs. Weekly backups should be kept in a locked cabinet to minimize the chance of loss and system compromise. When full monthly backups occur over the two day period, no incremental backup is made; this approach means that one day of operation is not backed up. Offsite storage is needed to ensure continuity of operation should the building be damaged or access become unavailable. Multiple tape hardware and software systems provide redundancy in case of a backup system failure.

3.3 Server Application Software

3.3.1 B2B Webserver

The B2B webserver software used at GIAC is commercial software that provides B2B data exchange. The webserver can support http, https, email, and ftp inputs. Two instances run on the server, one for internal development and the other for external testing. An audit of the B2B webserver operation conducted by review of the configuration, operational characteristics, operational procedures and interviews with the developers determined the following:

Dev.giac.org runs at 10.10.10.99.	Web based B2B transactions occur on a non-standard port.
Dev-test.giac.org runs at 10.10.10.100.	The B2B webserver runs only https sessions. No http, ftp or email inputs are allowed. Outgoing email used only for error messages.
Access to administrator functions is protected by user id and password using https.	Test and development software cgi scripts are under configuration and control, but on the operational webserver.
Web based B2B transactions occur only using SSL.	Builds are currently performed manually, but there are plans to automate the builds.

SSL software is internal to the server.	Java is used extensively for cgi scripts.
All files and directories have permissions of 775. Owned by b2badmin:e2e	Server is not based on Apache or other similar models.

Impact of Findings/Improvements – Using SSL for all operations provides a great deal of security. The SSL software is internal to the server and is not linked to the OPENSSL software used by SSH. CVS software is installed on the test and development server, but is not being utilized. The developers check in and out software on a CVS server running on a publicly accessible webserver. This is reversed of the way it should be. The software should be stored on the test and development server because it is less likely to be compromised by an attacker. The operational webserver software should then be checked out from the test and development server CVS system. The permissions on the server are too open. The world has permission to read and execute any server file. The permissions should be changed to 770 ("chmod –R 770 /usr/local/b2bserver_root"). The group permissions need to be "rwx" because multiple developers need control of the server.

3.3.2 SSH

Some of the B2B transactions also occur using SSH via SCP or SFTP. All the developer and system administrator interactions with the system use SSH. OpenSSH version 3.0.2.p2 is used. [8,9] The full version of the sshd_config with comments is in Appendix E. This configuration file is based on Sandor W. Sklar file which includes the sshd_config manpages and comments. [12] An audit of the SSHD configuration file (sshd_config) by review and discussions with the system administrator produced the following observations:

Sshd_config Entry	**Explanation**	**Security Impact**
SyslogFacility AUTH LogLevel DEBUG	Authentication is logged using syslog at the debug level.	Allows auditing of operations for regular use and problems.
Protocol 2 Port 22	Only Protocol 2 and port 22 are allowed.	• Protocol 1 with its security problems are not allowed. • Only the well-known port is active. Since no IP address was specified, SSH listens on all IP addresses.
MaxStartups 10 LoginGraceTime 120	Places limits on sessions and time to login.	These limit the chance of automated attempts to break into the system.
UseLogin no PrintLastLog yes	• Restrictions on type of login.	• Disabling the login option prevents

Sshd_config Entry	Explanation	Security Impact
PrintMotd yes	• Print last time you logged in. • Print the banner.	possible security holes. • The printing of the last login provides a quick check of any compromise of the users account. • Banner is printed on SSH connection before login.
StrictModes yes ReverseMappingCheck no	• Strict Modes provides for proper checking of permissions and ownership of the user's files and home directory before login is allowed. • Reverse DNS lookup is not required to establish a connection.	• SSH stores encryption key information in user files. If these are not protected from world access, the user's account could be compromised. Rather than turn this important feature off, the system administrator used ACL's to establish permissions on a shared directory. • Reverse DNS lookup helps prevent spoofing, but because many of the computers that access the server do not have reverse DNS entries it cannot be turned on.
KeyRegenerationInterval 3600 Ciphers aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour MACs hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96	These are default encryption options.	These provide maximum flexibility for the user and SSH. These should not be changed unless operational requirements necessitate the change.
KeepAlive yes ClientAliveInterval 0 ClientAliveCountMax 3 PidFile /var/tmp/sshd.pid	• KeepAlive enables TCP messages. ("Are you still there?" messages)	• Keep alive information is needed to prevent dropping the client. • Client keep alive

Sshd_config Entry	Explanation	Security Impact
	• ClientAlive options use an encrypted channel for keep alive traffic. • Location of SSH process ID.	provides additional security over TCP since the traffic is encrypted. • Provides a quick way to determine the SSH process id. The file needs to be owned by root and be non-world writeable.
## rsa1 key for SSH1 HostKey /usr/local/etc/ssh_host_key ## rsa key for SSH2 HostKey /usr/local/etc/ssh_host_rsa_key ## dsa key for SSH2 HostKey /usr/local/etc/ssh_host_dsa_key	Location of host key for different encryption algorithms.	These are the default locations and should not be changed unless required.
AuthorizedKeysFile .ssh/authorized_keys XAuthLocation /usr/bin/X11/xauth Banner /etc/motd	• AuthorizedKeysFile and XAuthLocation provide the location of files needed for certain applications. • Banner file is displayed when a SSH connection is made.	• AuthorizedKeysFile and XAuthLocation are the default locations and should not be changed unless required. • This option is enabled and provides a banner on SSH connection before user authentication.
AllowUsers dev1@10.10.*.* dev2@10.10.*.* dev3@10.10.*.* dev4@10.10.*.* dev5@10.10.*.* AllowUsers adm1 adm2 AllowUsers customer1@yyyyyy customer2@xxxxxx	Only these users can establish an SSH connection. Developers authenticate using password or public key. Administrators authenticate using password. Remote customers authenticate using host based authentication.	Very good security. This provides an extra layer of security. This is especially true for the hostbased authentication users. All but the adm accounts are restricted certain to IP addresses for SSH access.
DenyUsers root daemon bin sys adm lp uucp nuucp listen	Block these users.	Prevents system process accounts from being

Sshd_config Entry	Explanation	Security Impact
nobody noaccess nobody4 badmin		attacked and denies SSH access to specified users.
PermitRootLogin no PasswordAuthentication yes PermitEmptyPasswords no	• No login as root permitted via SSH. • Permit password authentication. • Empty passwords are not allowed.	These are good options and provide extra layers of protection to the system.
PubkeyAuthentication yes RSAAuthentication yes RhostsAuthentication no RhostsRSAAuthentication yes HostbasedAuthentication yes	• User authenticates with a public key (Protocol 2 only). • User authenticates with an RSA key (Protocol 1 only). • Authentication using only rhost is not allowed. • Authentication using rhost or host.equiv and RSA host key is allowed (Protocol 1 only). • Authentication using rhost or hosts.equiv and public host key is allowed (Protocol 2 only).	• Public Key and RSA Key authentication provide access without passwords, but require the private part of the key. This provides a good alternative to password authentication, especially when combined with user restrictions in AllowUsers. • Rhost only authentication should never be used. • Trusted host authentication used in conjunction with host key authentication provides stronger authentication than trusted host only, but is weaker than password or public key authentication. Additional protection can be provided by the AllowUsers entry. The host.equiv file is owned by root and is write protected so that no other user can add hosts to the file.

Sshd_config Entry	Explanation	Security Impact
IgnoreRhosts yes IgnoreUserKnownHosts no	• Ignore the .rhosts file in the users account even if it is present. • Allows SSH to validate a host from user's .ssh/known_host file.	• These are good options. The .rhost file can be easily compromised and should not be used. • Allowing user known hosts provides host authentication if the key is already present.
PAMAuthenticationViaKbdInt no AllowTcpForwarding no X11Forwarding no X11DisplayOffset 10 GatewayPorts no	No PAM keyboard challenge is allowed. (User receives a character string, performs a calculation based on the string and returns the results.) The other options concern SSH's tunneling features which are disabled. (X11 and other protocols can be layered on SSH).	PAM challenge is not used, but can be enabled if calculating software or hardware present. No tunneling is allowed. This option is not needed by the users, so it is turned off.
Subsystem sftp /usr/local/libexec/sftp-server	Enables a secure replacement for ftp.	SFTP provides encrypted file transfer without requiring that the tunneling feature be enabled.

Impact of Findings/Improvements – SSH is an excellent replacement for telnet, ftp and rcp. Only the system administrators, developers and customers with a need to have access are allowed. This is enforced by restricting SSH access at the firewall and by restricting users in SSH using the "Allowed Users" option. Outside user accounts (customers) are restricted to certain IP Addresses in the "Allowed Users" option. Developers are restricted to internal networks in the "Allowed Users" option. System administrators, are allowed access from any IP Address. No access is allowed for root or other administrative accounts. The test and development server is running with two IP addresses and one instance of SSH. This means that SSH listens on all IP addresses. If a separate instance of SSH is required, it could run on each IP address with different configurations. Host.equiv is used for hostbased host authentication of the outside users. host.equiv entries are made only by the system administrator and these entries are provided to the firewall administrator to enable SSH access for only these hosts through the firewall. Host.equiv could still be used by r-commands if they were enabled. Increased security could be provided if host authentication was performed using shost.equiv. Allowing HostbasedAuthentication, by itself, is a weak authentication method, but by restricting certain users to the trusted hosts authentication is made

stronger. Public key authentication could be used instead of hostbased authentication. To implement a public key authentication, a key (public and private components) needs to be generated and placed into that accounts "home/.ssh" directory. The public key needs to be sent to the test and development server and placed into that accounts "/home/.ssh/authorized_keys" file.

Since "StrictModes" is enabled checking of permissions and ownership of the user's files and home directory is performed before login is allowed. This protects the user's keys from being stolen or from foreign keys being placed in user key files. Kerberose options are disabled because Kerberose is not used. Since only Protocol 2 is allowed, the following Protocol 1 options can be disabled:

RSAAuthentication no *RhostsRSAAuthentication no* *KerberosAuthentication no*

Passwords are allowed for all users. Public key is allowed for developers and system administrators. Outside users are really batch jobs that perform data transfers using sftp. Authentication is hostbased with restrictions on user id and IP address. Since "restrict access" is enabled, access to the user's account is limited to 755 permissions at the most. Host.equiv is owned by root with 644 permissions. Only the system administrator can add hosts to hosts.equiv and user local".rhosts" and ".shosts" are ignored (IgnoreRhosts yes").

The motd file is also used for the banner file which is displayed after a successful SSH connection is established and before a user logins. The motd provides a legal notice to all users logging in or connecting.

3.3.3 Sudo

Sudo is freeware software that allows certain system administrator actions to be performed by users without the user having root access. [1] This is important to have on the test and development server because developers must be able to start and stop the B2B server and perform other operations that require root access. Full logging of user actions when using sudo permits auditing of each user's activities. The complete configuration file for sudo (/usr/local/etc/sudoers) is shown in Appendix F. An audit of the sudo configuration file and log files by review and discussions with the system administrator determined the following:

Only system admin and developers are allowed to sudo.	Design characteristic of sudo allows su and indirect shell to root (vi, etc).
System admin can execute any command.	Logging is in /var/log/sudo.log.
Developers can execute any command.	Log is archived with other syslog files.
Comparison of su log and sudo log show that on two occasions a developer shelled to root instead of using sudo.	A review of the sudo logs shows that most developers use sudo to start/stop the web server and cp, mv, chmod, chown or rm files that are generated by the web server or uploaded to the web server.

Impact of Findings/Improvements – Sudo is an excellent tool for improving security. Only those users with a need for access have sudo privileges and only the system administrator has the root password. Based on discussion with the system administrator sudo privileges were granted to allow the developers to troubleshoot their interface with the web server. On occasions some developers have over stepped their bounds by executing the "su" command from sudo. Security can be improved by instituting a policy that users are not to escape from the sudo program and by restricting the commands that can be run by sudo. This can be accomplished by changing the following as a minimum:

Current Line	**B2B ALL = NOPASSWD: ALL**
Replacement Line	**Cmnd_Alias KILL = /usr/bin/kill** **Cmnd_Alias SHUTDOWN = /usr/sbin/shutdown** **Cmnd_Alias HALT = /usr/sbin/halt** **Cmnd_Alias REBOOT = /usr/sbin/reboot** **Cmnd_Alias SHELLS = /usr/bin/sh, /usr/bin/ksh, /usr/bin/rsh, /usr/bin/remsh, /usr/bin/jsh, /usr/bin/rksh,\ /usr/xpg4/bin/sh** **Cmnd_Alias SU = /usr/bin/su** **Cmnd_Alias SNOOP = /usr/sbin/snoop** **B2B ALL = NOPASSWD: ALL, !KILL, !SHUTDOWN, !HALT, \!REBOOT, !SHELLS, !SU, !SNOOP**

Since a review of the logs showed only a limited set of commands being executed, a better solution would be rather than specifying what commands they cannot execute specify the commands that they can execute. This method provides more security and can be accomplished by changing the following:

Current Line	`B2B ALL = NOPASSWD: ALL`
Replacement Lines	`Cmnd_Alias RMSU = /bin/rm /usr/local/B2Bserver/*` `Cmnd_Alias MVSU = /bin/mv /usr/local/B2Bserver/* \` `/usr/local/B2Bserver/*` `Cmnd_Alias CPSU = /bin/cp /usr/local/B2Bserver/* \` `/usr/local/B2Bserver/*` `Cmnd_Alias CHMODSU = /bin/chmod * /usr/local/B2Bserver/*` `Cmnd_Alias CHOWNSU = /bin/chown * /usr/local/B2Bserver/*` `Cmnd_Alias LS = /bin/ls` `Cmnd_Aias SERVERBIN = /usr/local/B2Bserver/bin/*` `B2B ALL=NOPASSWD: RMSU, MVSU, CPSU, CHMODSU, CHOWNSU,\` `LS, SERVERBIN`

Commands can be added and deleted as required by the system administrator. User accounts are limited only to customer, developer, web server and system administrator,

Since the number of developers is limited and only developers and sytem administrators have sudo privileges all were granted NOPASSWORD sudo execution by the system administrator. No customers have sudo privileges.

3.4 Operating System Software Configuration

The configuration of the operating system software has a major impact on protecting the system and providing auditability of system and user actions.

3.4.1 User Accounts

The user and system accounts are defined in three files. The password file (/etc/passwd) provides the definition of user name, user id, group id, comments, home directory location, and default shell. The shadow file (/etc/shadow) contains the user name, user id, encrypted password, expiration date, expiration warning period, and idle lock time period. The group file (/etc/group) contains group names, group id, and additional user members of the group. These files were audited by review and the following was found:

Two system administrator accounts.	Two user accounts for B2B data transfer.
Six developer accounts.	All accounts except for system administrator's expire at the end of the year.
One web server account.	Six developer accounts have 60 day "lack of activity" expiration.
Comment field contains user name, company, and project.	Only groups associated with active users are present in the group file.
Default accounts are locked.	No password cracking is used by the system administrator.

Impact of Findings/Improvements – Only those with a need to access the computer have accounts. Expiration and "lack of activity" provide guards against lingering accounts. Commenting the user accounts with contact information helps reduce administrative overhead in contacting users. Password crackers should be used on a regular basis to ensure that passwords are not easily broken.

3.4.2 Analysis of Services

Services are network enabled portals that provide data and/or control information to/from other enabled services. Typical services include echo, chargen, telnet, ftp, http, ssh, etc. These services can provide unanticipated opportunities for someone to compromise a computer system. Which services are started by inetd is determined by the /etc/inet/inetd.conf and /etc/inet/services files. The configuration of the firewall helps determine the impact of these services on the system. The audit is derived from the "netstat -a" command, the "lsof -i" (discussed in section 3.11.1), the NMAP scan (discussed in section 3.10.1), the inetd.conf file and a review of the firewall rules. It shows the following services:

Open Ports	Service	Firewall to Internet
22/tcp	Ssh	Selected IP addresses Allowed
111/tcp/udp	Sunrpc	Blocked
177/udp	Xdmcp	Blocked
514/udp	Syslog	Blocked
844/udp,	Cs00	Blocked
859/tpc	Calserver	Blocked
861/tcp	Keyserver	Blocked
898/tcp	Java	Blocked
2201/tcp	Kkcv	Blocked
5555/tcp	B2B server	Select IP addresses Allowed
5987/tcp	Java	Blocked
6000/tcp	X11	Blocked
7100/tcp	Font-service	Blocked
8888/tcp	Sun-answer	Blocked
9010/tcp	Htt_serve	Blocked
33691/tcp	Java	Blocked
32771/tcp	Rpc5	Blocked
32771/udp	Rpc6	Blocked
32772/tcp	Rpc7	Blocked
32772/udp	Rpc8	Blocked
32774/udp	Rpc12	Blocked
32775/tcp	Rpc13	Blocked
32776/tcp	Rpc15	Blocked

Impact of Findings/Improvements – The initd.conf file should be cleared of all commented services so that only active services remain. This prevents services from accidentally being activated. It also makes detection of unauthorized additions easier. The services file should be cleared of all commented services so that only active services remain. Based on the usage of the computer, some of these services are not needed: the Japanese character interface (cs00: port 844, kkcv: port 2201) and the Caldera CAMELEO software (calserver:port 859). The rc startup file for each of these should be changed so that they will not start. See section 3.4.3 for details on disabling these. The firewall configuration blocks all but the two services that need to communicate over the Internet. This greatly increases security and can minimize the effect of poorly secured computers.

3.4.3 Analysis of Active Processes

The ps command provides information on all the processes that are active. This command is very useful in helping to determine if unnecessary programs are running. The columns are as follows: first column is the command list by ps; the second column is derived from other files (e.g., init.d files); the third column is a description from SUN's Answer Book and manpages; the fourth column are the ports are from losf and Nmap; and the last column provides a sort statement of need for the process and how to disable it if it is not needed. The audit of the active processes is as follows:

Services from PS Command	Start-up Script Start-up Path	Description [4,5]	Port [1]	Need Disable Information
/usr/lib/sysevent/ syseventd	/etc/init.d/devfsadm /usr/lib/sysevent/syseventd >/dev/msglog 2>&1	syseventd starts devfsadmd and rcm_daemon on-demand.		This process is needed by system.
/usr/lib/sysevent/ syseventconfd	/etc/init.d/devfsadm /usr/lib/sysevent/syseventconfd >/dev/msglog 2>&1			This process is needed by system.
Devfsadmd		devfsadmd(1M) is the daemon version of devfsadm(1M) . The daemon is started by the /etc/rc* scripts during system startup and is responsible for handling both reconfiguration boot processing and updating /dev and /devices in response to dynamic reconfiguration event notifications from the kernel.		This process is needed by system.
/usr/lib/picl/picld	/etc/init.d/plicd /usr/lib/picl/picld	The Platform Information and Control Library (PICL) provides a mechanism to publish platform-specific information for clients to access in a platform-independent way. picld maintains and controls access to the PICL information from clients and plug-in modules.		This process is needed by system.
/usr/lib/lpsched	/etc/init.d/lp usr/lib/lpsched	The lpsched command starts or restarts the LP print service.		No printer is connected to the server. This process can be disabled.

[1]The F**irewall blocks all incoming Internet access to all ports except these with "*" .**

Services from PS Command	Start-up Script Start-up Path	Description [4,5]	Port [1]	Need Disable Information
				Disable by: **mv /etc/rc2.d/S80lp /etc/rc2.d/.NOS80lp**
/usr/lib/power/powerd	/etc/init.d/power usr/sbin/pmconfig -a -r /etc/power.conf	The powerd daemon is started by pmconfig to monitor system activity and perform an automatic shutdown using the suspend-resume feature. When the system is suspended, complete current state is saved on the disk before power is removed. On reboot, the system automatically starts a resume operation and the system is restored to the same state it was in immediately prior to suspend.		Since this server needs to be active all the time, this process can be disabled. **Disable by:** **mv /etc/rc2.d/S85power /etc/rc2.d/.NOS85power**
/usr/bin/fgd		fg brings the current or specified *job_id* into the foreground.		This process is needed by system.
/opt/cameleo/bin/ calserver /opt/cameleo/lib/calserver.cfg	/etc/init.d/caldera /opt/cameleo/bin/calserver /opt/cameleo/lib/calserver.cfg < /dev/null > /dev/null 2>&1	CameleoLIGHT is the professional software package dedicated to graphic peripheral devices driving on Unix workstations. [6]	859	This is not needed and can be disabled. **Disable by:** **mv /etc/rc2.d/S91caldera /etc/rc2.d/.NOS91caldera**
/opt/cameleo/bin/ keyserver /opt/cameleo/lib/ Caldera.licenses	/etc/init.d/caldera /opt/cameleo/bin/keyserver /opt/cameleo/lib/Caldera.licenses < /dev/null > /dev/null 2>&1	CameleoLIGHT is the professional software package dedicated to graphic peripheral devices driving on Unix workstations. [6]	861	Part of Caldera process and is disabled with when Caldera is disabled (see above).

Services from PS Command	Start-up Script Start-up Path	Description [4,5]	Port [1]	Need Disable Information
/usr/sbin/ ifbdaemon /dev/fbs/ifb0		The ifb driver is the device driver for the Sun Elite3D graphics accelerators. The ifbdaemon process loads the ifb microcode at system startup time and during the resume sequence of a suspend-resume cycle.		This process is needed by system.
/usr/lib/ab2/dweb/ sunos5/bin/ dwhttpd /usr/lib/ab2/dweb/data	/etc/init.d/ab2mgr /usr/lib/ab2/dweb/sunos5/bin /dwhttpd /usr/lib/ab2/dweb/data	Sun Answer Book webserver.	8888	Based on developer and system administrator comments, the Answer Book is used extensively so this process is needed.
/usr/local/sbin/sshd	/etc/init.d/sshdaemon /usr/local/sbin/sshd	sshd version OpenSSH_3.0.2p1.	22 *	Version is most current at this time. See section 3.3.2 for details and information on making SSH more secure.
/usr/local/bin/prngd /var/spool/prngd/pool	/etc/init.d/prngd '/usr/local/bin/prngd /var/spool/prngd/pool	This daemon creates a random number pool for ssh and should start first.		Version is most current at this time. Required for SSH.
/usr/lib/dmi/dmispd	/etc/init.d/init.dmi '/usr/lib/dmi/dmispd	dmispd is the DMI Service Provider. The Service Provider coordinates and arbitrates requests from the management application to the specified component instrumentations. The Service Provider handles runtime management of the Component Interface (CI) and the Management Interface (MI).	32774 32775	This is not needed and can be disabled. **Disable by:** **mv /etc/rc3.d/S77dmi /etc/rc3.d/.NOS77dmi**
/bin/sh -xv /usr/local/B2Bserver/dev/bin/server.sh	/etc/init.d/B2Bserver	Business-to-Business server	5555	The B2B server is needed. See section 3.3.1 for details and information on increasing security.

Services from PS Command	Start-up Script Start-up Path	Description [4,5]	Port [1]	Need Disable Information
/usr/dt/bin/dtlogin -daemon	/usr/dt/bin/dtlogin -daemon /etc/rc2.d/S99dtlogin	Desk top login server is usually started when the system is booted.	177 32776	Based on conversations with the developers and system administrators, the local console is use by both on a regular basis. This is needed for the GUI display.
/usr/sbin/nsr/nsrexecd -s bkuphost bkuphost		Tape backup daemon.	7937 7938	Required for backups.
dtgreet -display :0	/usr/dt/bin/dtgreet	Displays a login screen for the Desk Top display.	32776	Part of dtlogin which is needed.
/usr/j2sdk1_3_1_02/jre/bin/../bin/sparc/native_threads/java -ms64M -mx128M –cla		Java Developers Kit. Used by the B2B server.	898 5987 33691	Java version is recent. Java is need for normal operation of the B2B server.
/usr/sbin/vold	/usr/sbin/vold	Volume Manager automatically mounts CD-ROMs and floppy disks for users whenever a disk is inserted in the local system's drive. Normally the command mount is used and requires superuser privileges.		Since users do not need access to the CD-ROM or floppy drives, this daemon can be disabled. **Disable by:** `mv /etc/rc2.d/S92volmgt /etc/rc2.d/.NOS92volmgt`
/usr/sbin/rpcbind		rpcbind is a server that converts RPC program numbers into universal addresses. It must be running on the host to be able to make RPC calls on a server on that machine. Normally, standard RPC servers are started by port monitors, so rpcbind must be started before port monitors are invoked.		Since the server is a standalone machine, the process can be disabled. **Disable by:** `mv /etc/rc2.d/S71rpc /etc/rc2.d/.NOS71rpc`

Services from PS Command	Start-up Script Start-up Path	Description [4,5]	Port [1]	Need Disable Information
/usr/sbin/syslogd	/etc/init.d/syslogd	syslogd reads and forwards system messages to the appropriate log files and/or users, depending upon the priority of a message and the system facility from which it originates. The configuration file /etc/syslog.conf controls where messages are forwarded.	514/udp	This server is not acting as a syslog server so the upd port can be disabled. Edit /etc/init.d/syslogd. Change: **/usr/sbin/syslogd -m30** to **/usr/sbin/syslogd -m30 -t**
/usr/sbin/cron	/etc/init.d/cron /usr/sbin/cron	The cron command starts a process that executes commands at specified dates and times. Regularly scheduled commands can be specified according to instructions found in crontab files in the directory /var/spool/cron/crontabs. Users can submit their own crontab file using the crontab(1) command. Commands which are to be executed only once may be submitted using the at command.		Needed for normal operation. See section 3.8 for a detail discussion and information on making cron related files more secure.
/usr/sbin/nscd	/etc/init.d/nscd	nscd is a process that provides a cache for the most common name service requests. nscd provides caching for the passwd, group, hosts, ipnodes, exec_attr, prof_attr, and user_attr databases through standard libc interfaces. The default configuration-fileis in /etc/nscd.conf.		This daemon is needed by system.

Services from PS Command	Start-up Script Start-up Path	Description [4,5]	Port [1]	Need Disable Information
cachefsd	/etc/init.d/cachefs.daemon usr/lib/fs/cachefs/cachefsd	The Cache File System (CacheFS) is a general purpose file system caching mechanism that improves NFS server performance.		Since NFS is not running, this daemon is not needed. **Disable by:** **`mv /etc/rc2.d/S72cachefs.daemon /etc/rc2.d/.NO S72cachefs.daemon`**
/usr/sbin/cssd	/etc/init.d/loc.ja.cssd /usr/sbin/cssd	cssd is the command which invokes and watches CS available in MLE (Multi Language Environment).		Since the MLE is not running, this daemon is not needed. **Disable by:** **`mv /etc/rc2.d/S90loc.ja.cssd /etc/rc2.d/.NOS90loc.ja.cssd`**
/usr/lib/im/htt -port 9010 -syslog -message_locale C	/etc/init.d/Iiim	htt server help provide Japanese character conversion in conjuction with the cs00 daemon.	9010	This processs is not needed so it can be disabled. **Disable by:** **`mv /etc/rc2.d/S95Iiim /etc/rc2.d/.NOS95Iiim`**
/usr/lib/locale/ja/atokserver/atokmngdaemon	/etc/init.d/atsv /usr/lib/locale/ja/atokserver/atokmngdaemon	Part of the Japanese Input System ATOKserver for Japanese Solaris.		This processs is not needed and is disabled when the S95Iiim daemon is disabled.
/usr/sbin/ccv -f		Part of the Japanese Input System ATOKserver for Japanese Solaris.	2200	This processs is not needed and is disabled when the S95Iiim daemon is disabled.
/usr/sbin/kkcv -f		Part of the Japanese Input System ATOKserver for Japanese Solaris.	2201	This processs is not needed and is disabled when the S95Iiim daemon is disabled.
/usr/sbin/cs00		Four Japanese input systems, ATOK12, ATOK8, Wnn6, and cs00 support thelJapanese character set.	844	This processs is not needed and is disabled when the S95Iiim daemon is disabled.

Services from PS Command	Start-up Script Start-up Path	Description [4,5]	Port [1]	Need Disable Information
/usr/sadm/lib/smc/bin/smcboot		The Web-Based Enterprise Management (WBEM) and Solaris WBEM Services software makes it easier for software developers to create management applications that run on Solaris and make the Solaris operating environment easier to manage.		This processs is not needed so it can be disabled. **Disable by:** `mv /etc/rc2.d/S90wbem /etc/rc2.d/.NOS90wbem`

Impact of Findings/Improvements – A large number of processes are running that are not needed. This is because the server was setup with the default Sun configuration. Instructions for disabling the daemons are provided in the "Need/Disable Information" column. If, at a later date, a process needs to be re-enabled, remove the ".NO" from the desired file by renaming it (mv .NOSXXyyy SXXyyy). In order for the daemons to be disabled or enabled, the server must be rebooted. If it is not possible to reboot the machine after the filenames have been changed, the daemons can be started or stopped manually by executing the desired command in the /etc/init.d directory (i.e. "/etc/init.d/S90wbem start" or " /etc/init.d/S90wbem stop").

3.5 Operational Environment

The operational environment of the test and development server was determined by reviewing the services running on the machine. The review produced the following observations:

The server is standalone. That is, it does not support the sharing of users accounts or disk space across multiple computers.	The server is not running Network File System (NFS) which allows disk space to be shared across multiple machines. The disk space on the server is only available to the server and no other disk space is available to the server.
Network Information Service (NIS) which allows user accounts across multiple machines is not running. Only users defined in the password file have accounts on the server.	

Impact of Findings/Improvements –Not running NIS and NFS greatly improves the security of the server, since it limits access to the computer and avoids the security problems associated with this software.

3.6 Analysis of System Log Configuration file

The system log configuration file (/etc/syslog.conf) determines what events will be logged by the system and applications, and where they will be logged. These logs can provide evidence of system problems and security breaches. Attackers are also aware of this and attempt to modify the logs to cover their tracks. The audit of the system log configuration file by review determined the following:

The following facilities are logged at some level: daemon, kern, mail, auth, user, local2 (sudo), local10 (backup).	All syslog log files are archived nightly by cron. They have 700 permissions and are owned by root.
The following facilities are not logged in syslog at any level: cron, lpr, uucp, news.	Permission on log files is 644.
No logs are written to console.	Logging occurs only on the local machine.
No mark entry is written to make sure syslog is working correctly. Many logs are zero size.	Logs are manually reviewed on a daily basis.

Impact of Findings/Improvements – The configuration provides good level of protection, but enhancements can be made that will increase system security and the usefulness of the log files. All facilities should be logged. They may be sent to the message log if a separate log is not needed. Emergency level messages should also be sent to the console

to increase the chances of detection. Enable mark entries on all logs to ensure that the logging function is working properly and to make any modification made by an attacker easier to detect. Although, the nightly archiving is excellent, centralized logging would provide an excellent way to overcome attacker modifications of log files since the attacker would need access to the loghost as well as the compromised machine. Manual review of logs is time consuming; automating the analysis will help to reduce the time required. By using automated log analysis in conjunction with a centralized loghost, patterns across multiple machines can be detected.

3.7 Analysis of System Log Archives

The system log files are archived daily using the Syslog Archive script run by cron. See Appendix G for a complete listing of the archive script and section 3.8.1 for additional detail. The audit of the system log configuration file by review and by discussion with the system administrator determined the following:

The script is executed by the root crontab at 8:30am every day.	The archive directory and its subdirectories are owned by root and have 700 permissions.
The script copies the log files in /var/log into the syslog archive directory.	Backups of the archive directory occur as part of the normal daily and monthly backups.
To ensure that each file has a unique name the host name and the current date are appended to the file name (i.e. daemon.log.b2b.051702).	Files in the archive directory are manually deleted every two to three months.
The log files in /var/log are then over written using /usr/bin/cat /dev/null > daemon.log	The syslog archive script is located in /var/adm/scripts which is owned by root and has 700 permissions. The script also has permissions of 700.

Impact of Findings/Improvements – The configuration provides good level of protection. Having all the logs in one directory simplifies the analysis of events that occur over long time periods.

3.8 Analysis of crontabs

Crontabs are used to run system and user programs on a scheduled basis. There are four different crontabs: root, sys, lp and uucp.

3.8.1 Root crontab

The root crontab is run with suid root. The audit of the root crontab by review is as follows:

Crontab Entry	Functional Description
10 3 * * 0,4 /etc/cron.d/logchecker	Rotates CRON log in /var/cron.

10 3 * * 0 /usr/lib/newsyslog	SUN script for rotating syslogs. Also, restarts syslog.
15 3 * * 0 /usr/lib/fs/nfs/nfsfind	Check shared NFS filesystems for .nfs* files that are more than a week old.
1 2 * * * [-x /usr/sbin/rtc] && /usr/sbin/rtc –c > /dev/null 2>&1	Check for daylight saving time.
30 3 * * * [-x /usr/lib/gss/gsscred_clean] && /usr/lib/gss/gsscred_clean	Check for and remove duplicate entries in the Generic Security Service table, /etc/gss/gsscred_db.
#30 20 * * * /usr/local/bin/virus_scan /host-d1 /host-dev2 /host-dev3 /usr/local /station /depot 2>&1 | mailx –s "HOST Virus Scan Results" sysadmin@lab.giac.org	Commented out script to run a virus scan on another machine.
30 8 * * * /var/adm/scripts/archive_syslogs.sh	Archive syslogs. See section 3.7 and Appendix G – Syslog Archive Script for more details.
5 * * * * /usr/lib/sendmail –q > /dev/null 2>&1	Flush out the mail queue.

Impact of Findings/Improvements – The root crontab has many entries that are not needed. The SUN script rotating syslogs is not need since a system administrator written script handles the archiving of the logs. The NFS script is not needed since NFS is not running. The daylight savings time script could be run manually, but does not present a problem. The virus entry should be deleted if it is not used. While the chance of this server getting a virus is small, it would be prudent to install the virus software if it is available. The log archiving entry is good, but precautions must be taken to ensure that the archive script cannot be modified by users because it runs at root. Since the sendmail daemon does not run on the development server, any email that cannot be delivered will be queued. The sendmail entry runs sendmail in order to deliver unsent mail. The crontab files should document the purpose of each entry to assist in troubleshooting. To edit the root crontab use: "crontab –e root".

3.8.2 Sys crontab

The sys crontab is run with suid sys. The audit of the sys crontab by review determined the following:

Crontab Entry	Functional Description
# 0 * * * 0-6 /usr/lib/sa/sa1 # 20,40 8-17 * * 1-5 /usr/lib/sa/sa1 # 5 18 * * 1-5 /usr/lib/sa/sa2 -s 8:00 –e 18:01 -i 1200 –A	Commented out system accounting functions.

Impact of Findings/Improvements – sa1 and sa2 are system activity reporting programs. These are commented out, and, therefore, no system activity is being captured and reported. These entries should be uncomment so that they will run. Useful additions to the entries would be a script that emails the reports to the system admin account. To edit the sys crontab use: "crontab –e sys".

3.8.3 lp crontabs

The lp crontab is run with suid lp. The audit of the lp crontab by review determined the following:

Crontab Entry	Functional Description
13 3 * * 0 cd /var/lp/logs; if [-f requests]; then if [-f requests.1]; then /bin/mv requests.1 requests.2; fi; /usr/bin/cp requests requests.1; >requests; fi	Rotate printer logs.
15 3 * * 0 cd /var/lp/logs; if [-f lpsched]; then if [-f lpsched.1]; then /bin/mv lpsched.1 lpsched.2; fi; /usr/bin/cp lpsched lpsched.1; >lpsched; fi	Rotate printer scheduler logs.

Impact of Findings/Improvements – Since there is no printer on the development server, the file can be deleted using "crontab –r lp". The lp daemon account is locked so that it cannot run. See section 3.4.1.

3.8.4 uucp crontabs

The uucp crontab is run with suid uucp. The audit of the uucp crontab by review determined the following:

Crontab Entry	Functional Description
#48 8,12,16 * * * /usr/lib/uucp/uudemon.admin #20 3 * * * /usr/lib/uucp/uudemon.cleanup #0 * * * * /usr/lib/uucp/uudemon.poll #11,41 * * * * /usr/lib/uucp/uudemon.hour	These entries perform the administration and maintenance of the uucp daemon which run the Unix-to-Unix Copy Protocol.

Impact of Findings/Improvements – Since uucp is not used on the development server, the file can be deleted using "crontab –r uucp". The uucp daemon account is locked so that it cannot run. See section 3.4.1.

3.8.5 Miscellaneous Crontab Information

Several other files relate to the cron daemon. An audit of these files by review determined the following:

File	Functional Description
Cron log is in /var/cron 600 root:root.	Files are protected from users. Users

	cannot read or write.
/var/spool/cron/crontabs - The sys, lp, uucp crontabs are world readable. The root crontab is not readable by world.	User can read sys, lp and uucp crontabs, but cannot modify them.
No Atjobs.	There are no user jobs that are run on a scheduled basis.
No /etc/cron.d/cron.allow file is present /etc/cron.d/cron.deny file is present	Since no cron.allow is present, any user not listed in cron.deny can create crontabs. The default SUN cron.deny files is present and has entries of: daemon, bin, smtp, nuucp, listen, nobody and noaccess.
No /etc/cron.d/at.allow file is present /etc/cron.d/at.deny file is present	Since no at.allow is present, any user not listed in at.deny can create "at jobs." The default SUN cron.deny files is present and has entries of: daemon, bin, smtp, nuucp, listen, nobody and noaccess.

Impact of Findings/Improvements – Enable cron logging in the syslog.conf to provide better logging of events. Change permissions on the crontabs so that only the owner can read them. A cron.deny file without a cron.allow file permits any user not listed in the cron.deny file to create a crontab. Users should be prevented from creating crontabs unless allowed by the system administrator. This can be accomplished by listing only the users that are permitted to create crontabs (root) in the cron.allow file. Cron.allow and cron.deny should be owned by root and have 750 permissions. An at.deny file without an at.allow file permits any user not listed in the at.deny file to create an at job. Users should be prevented from creating at jobs unless allowed by the system administrator. This can be accomplished by listing only the users that are permitted to create at job in the at.allow file. at.allow and at.deny should be owned by root and have 750 permissions.

3.9 Analysis of Patches

Having the most current operating system patches installed in a system is not a goal, it is a process. Since vendors continually release patches, system administrators must check vendor websites or be on vendor mailing lists to ensure that the patch levels of their machines are current. Sun provides a patch diagnostic tool to examine a profile of the patches installed on the system against the most current profiles available from Sun Microsystems [7]. The Sun patch diagnostic tool provided the following audit information:

```
INSTALLED PATCHES  < Sample of 408 installed patches found by the
tool>
Patch  Installed Latest   Synopsis
```

```
  ID   Revision  Revision
------ --------- -------- ------------------------------------------
---------------
108127    05     CURRENT  ShowMe TV 1.3: ShowMe TV application patch
108528    09        13    SunOS 5.8: kernel update patch
108569    05        06    X11 6.4.1: platform support for new hardware
108576    14        26    SunOS 5.8: Expert3D IFB Graphics Patch
108604    16        24    SunOS 5.8: Elite3D AFB Graphics Patch
108605    15        24    SunOS 5.8: Creator 8 FFB Graphics Patch
108606    10        20    SunOS 5.8:  M64 Graphics Patch
108609    01     CURRENT  SunOS 5.8: Buttons/Dials Patch
108623    02        03    SunOS 5.8: Thai Wordbreak Iterator module
108652    34        47    X11 6.4.1: Xsun patch
108711    04     CURRENT  SunOS 5.8: Missing Catalan Locale Support
108714    05     CURRENT  CDE 1.4: libDtWidget patch
108723    01     CURRENT  SunOS 5.8: /kernel/fs/lofs and
/kernel/fs/sparcv9/lofs patch
108725    05        08    SunOS 5.8: st driver patch
108727    06        14    SunOS 5.8: /kernel/fs/nfs and
/kernel/fs/sparcv9/nfs patch
```

```
UNINSTALLED RECOMMENDED PATCHES

Patch  Ins Lat Age  Require    Incomp  Synopsis
  ID   Rev Rev        ID         ID
------ --- --- --- --------- --------- ------------------------------
----------
109041 N/A  04 302 108528-08           Obsoleted by: 108528-09 SunOS
5.8: sockfs patch
109137 N/A  01 713                     Obsoleted by: 110934-03 SunOS
5.8: /usr/sadm/install/bin/pkginstal
109221 N/A  06 417 108993-01           Obsoleted by: 109318-12 SunOS
5.8: Patch for sysidnet
109587 N/A  03 278                     Obsoleted by: 109318-18 SunOS
5.8: libspmistore patch
110700 N/A  01 435                     SunOS 5.8: automount patch
111504 N/A  01 277                     SunOS 5.8: /usr/bin/tip patch
111570 N/A  01 265                     SunOS 5.8: uucp patch
111596 N/A  02 203 111659-01           SunOS 5.8:
/usr/lib/netsvc/yp/rpc.yppasswdd patch
111606 N/A  02 183                     SunOS 5.8: /usr/sbin/in.ftpd
patch
111626 N/A  01 239                     OpenWindows 3.6.2: Xview Patch
111659 N/A  06  15                     SunOS 5.8: passwd and
pam_unix.so.1 patch
111826 N/A  01 216                     SunOS 5.8:
/usr/sbin/sparcv7/whodo & /usr/sbin/sparcv9/whodo patch
111874 N/A  04  60                     SunOS 5.8: usr/bin/mail patch
111881 N/A  01 202                     SunOS 5.8:
/usr/kernel/strmod/telmod patch
112138 N/A  01 134 108991-18           SunOS 5.8:: usr/bin/domainname
patch
```

```
                    108827-15
112218 N/A  01 126                      SunOS 5.8:: pam_ldap.so.1 patch
112325 N/A  01  56                      SunOS 5.8: /kernel/fs/udfs and
/kernel/fs/sparcv9/udfs patch
112334 N/A  02  14                      SunOS 5.8:
/usr/include/sys/archsystm.h patch
112396 N/A  01  43                      SunOS 5.8:` /usr/bin/fgrep
patch
```

```
UNINSTALLED Y2K PATCHES

NOTE: This list includes the Y2K patches that are also Recommended

Patch  Ins Lat Age  Require    Incomp  Synopsis
  ID   Rev Rev        ID         ID
------ --- --- --- --------- --------- --------------------------------
------
All Y2K patches installed!
```

```
UNINSTALLED SECURITY PATCHES

NOTE: This list includes the Security patches that are also
Recommended

Patch  Ins Lat Age  Require    Incomp  Synopsis
  ID   Rev Rev        ID         ID
------ --- --- --- --------- --------- --------------------------------
----------
108979 N/A  10 489 108528-03           Obsoleted by: 108528-04 SunOS
5.8: platform nexus, I2C, Netra ct a
109041 N/A  04 302 108528-08           Obsoleted by: 108528-09 SunOS
5.8: sockfs patch
109965 N/A  03 417                     Obsoleted by: 109887-02 SunOS
5.8: pam_smartcard.so.1 patch
111332 N/A  04 140                     SunOS 5.8: /usr/lib/dcs patch
111504 N/A  01 277                     SunOS 5.8: /usr/bin/tip patch
111570 N/A  01 265                     SunOS 5.8: uucp patch
111596 N/A  02 203 111659-01           SunOS 5.8:
/usr/lib/netsvc/yp/rpc.yppasswdd patch
111606 N/A  02 183                     SunOS 5.8: /usr/sbin/in.ftpd
patch
111626 N/A  01 239                     OpenWindows 3.6.2: Xview Patch
111647 N/A  01 225                     BCP libmle buffer overflow
111659 N/A  06  15                     SunOS 5.8: passwd and
pam_unix.so.1 patch
111826 N/A  01 216                     SunOS 5.8:
/usr/sbin/sparcv7/whodo & /usr/sbin/sparcv9/whodo patch
111874 N/A  04  60                     SunOS 5.8: usr/bin/mail patch
111881 N/A  01 202                     SunOS 5.8:
/usr/kernel/strmod/telmod patch
112039 N/A  01 183                     SunOS 5.8: usr/bin/ckitem patch
```

```
112218 N/A  01 126                          SunOS 5.8:: pam_ldap.so.1 patch
112459 N/A  01  12                          SunOS 5.8: /usr/lib/pt_chmod
patch
```

Impact of Findings/Improvements – The large number of patches to be installed indicate that this machine has not been patched for several months. One way to reduce the number of patches required is to remove packages that are not needed (such as the language packages). A regular schedule of patching should be started so that it is not possible to exploit known vulnerabilities.

3.10 Analysis of Logging

The development server has a number of log files. These files should be protected from user access to prevent modification is an attack should occur. Logs should be archived so that application, system, or security problems may be examined over a long period of time. An audit of the log files by review determined the following:

Log File	Archive
Syslogs are in /var/log. `Daemon /var/log/daemon.log` `Kern /var/log/kern.log` `Mail /var/log/mail.log` `Auth /var/log/auth.log` `User /var/log/user.log` `Syslog /var/log/syslog.log` `local2 /var/log/sudo.log` `local0 /var/log/nsr.log` `*.alert root` `*.emerg *` See Section 3.6 for more information on Syslog.	Archived to a protected archive directory by cron.
Cron log is /var/cron. Owned by root:root 600 permission.	Log file is rotated daily by cron, but only two days worth are kept.
Sulog is in /var/adm/sulog. Owned by root:other 755 permission.	Log file is not rotated or archived.
Message log is in /var/adm/message. Owned by root:other 644 permission.	Log file is rotated weekly by cron, but is not archived.
NSR backup log is in /var/log/nsr. Owned by root:other 644 permission.	Log file is archived. A duplicate log is on the backup host and is emailed to the system administrators.
No /etc/adm/loginlog.	File does not exist so it cannot be archived.
SYSLOG_FAILED_LOGINS=5 commented out in /etc/default.	

Impact of Findings/Improvements – Archiving of syslogs is very good. Archiving log files prevents the files from growing too large and provides a single place where log files are kept. Permissions on all log files should be 600, and they should be owned by root. The sulog, cron log and message log need to be archived by the same cron script that archives the syslogs. SYSLOG_FAILED_LOGINS=5 is commented out in the /etc/default file. This should be uncommented and set to 0 to log all login failures in the syslog files. The /etc/adm/loginlog file needs to exist (create via "`touch /etc/adm/loginlog`") so that failed login attempts can be logged. It should also be added to the archive script so that it is stored in the archive.

3.11 Analysis of External Scans

An external scan is a scan that is conducted between two computers, a scanning computer and a target computer. The scanning computer probes the target computer's ports to determine what services or programs are listening. In order to obtain the true results for the scanned computer, the scanning computer and target computer should not be separated by firewalls or routers the perform filtering. If they are separated, then the result is a combination of firewall/router filtering and target response. While scanning programs can be configured to scan all possible protocols and ports, however, this can take a very long time. Most scanners have a default set of protocols and ports to be scanned that are typical targets of exploitation. Information gathered from the scan can be very simple (e.g., a port is open or closed) to very detailed (e.g., network mounting files, network user passwords, etc).

3.11.1 Analysis of Nmap Scan

Nmap is a freeware scanning tool that can be downloaded from the web [2]. In this case, the development server and the scanning computer were on the same network and were connected by a switch so no filtering occurred. The full scan results are in Appendix B. An audit of the scan is as follows:

Nmap Finding	Explanation of Finding
A total of 1569 TCP ports were scanned and 1569 UDP ports were scanned for a total of 3138 ports.	Nmap has a default range of ports that it scans if no other range is specified. The selection of ports is based on the mostly likely ports to be active.
3117 scanned ports were in a closed state.	A closed port is one that does not have a service running.
21 ports were in an open state. `Port State Service` `22/tcp open ssh` `111/tcp open sunrpc` `111/udp open sunrpc` `177/udp open xdmcp` `514/udp open syslog` `844/udp open unknown`	An open port is one that has a service running. More description of the function of these services is found in Sections 3.4.2, 3.4.3, & 3.11.1. As shown in Section 3.4.2 only port 22, ssh and port 5555, B2B webserver

859/tcp open unknown 861/tcp open unknown 898/tcp open unknown 2201/tcp open ats 5555/tcp open unknown 6000/tcp open X11 7100/tcp open font-service 8888/tcp open sun-answerbook 32771/tcp open sometimes-rpc5 32771/udp open sometimes-rpc6 32772/tcp open sometimes-rpc7 32772/udp open sometimes-rpc8 32774/udp open sometimes-rpc12 32775/tcp open sometimes-rpc13 32776/tcp open sometimes-rpc15	are allowed through the firewall to the Internet.
Operating system guess is Sun Solaris 8	This is correct.
Determined system uptime to be 15.761 days	Determined the time since the last boot.
TCP sequence prediction was random positive increments and was rated difficult.	If the increment is too predictable packets may be spoofed.

Impact of Findings/Improvements - The advantage of using Nmap is that the information is gathered externally and directly shows what is visible to other systems. Since it takes a minimal time to run, large numbers of hosts can be probed efficiently without having to log into each machine.

3.11.2 Analysis of ISS Scan

ISS is a commercial scanning tool. [3] The development server and the scanning computer are again on the same network and are connected by a switch so no filtering occurred. When ISS determines that there is a problem, it provides a severity ranking, a detailed explanation of the problem, and a possible solution to the problem. The full scan results are provided in Appendix C. An audit of the scan is results determined the following:

ISS Finding	Explanation of Finding
The TCP sequence was found to be predictable. 10.10.10.99: Minimum guess (SYN/ACK received order): 1 out of 24 (4.167%) 10.10.10.99: Most frequent guess (SYN/ACK received order): 1 out of 24 (4.167%)	ISS found that there was a 1 in 24 chance of guessing the correct TCP sequence. This may allow packets to be spoofed.

Impact of Findings/Improvements – The external ISS scan found little in terms of security vulnerabilities. It found the open ports, but did not consider them to be a security issue.

3.12 Internal Scans

An internal scan is run on the computer being examined. These scans are usually run as root and look at multiple parameters including: configuration files, file privileges, system processes and network status.

3.12.1 Analysis of lsof Scan

lsof is not a scanner in the typical sense, but provides extensive information in analyzing the state of the computer. lsof stands for **Li**s**t** **O**pen **F**iles and provides information on commands that have open files including : owner, process id, port, status of port, and protocol. An audit of the "lsof –i" output determined the following:

COMMAND	NODE	IP ADDRESS	PORT	STATUS
sshd	TCP	*	22	(LISTEN)
sshd	TCP	*	22	(LISTEN)
dtlogin	UDP	*	177	(Idle)
cs00	UDP	*	844	(Idle)
calserver	TCP	*	859	(LISTEN)
keyserver	TCP	*	861	(LISTEN)
java	TCP	*	898	(LISTEN)
ccv	TCP	*	2200	(LISTEN)
kkcv	TCP	*	2201	(LISTEN)
java	TCP	dev.giac.org	5555	(LISTEN)
java	TCP	*	5555	(LISTEN)
java	TCP	*	5987	(LISTEN)
Xsun	TCP	*	6000	(LISTEN)
nsrexecd	TCP	*	7937	(LISTEN)
nsrexecd	UDP	*	7938	(Idle)
nsrexecd	TCP	*	7938	(LISTEN)
dwhttpd	TCP	*	8888	(LISTEN)
dwhttpd	TCP	*	8888	(LISTEN)
htt_serve	TCP	*	9010	(LISTEN)
rpcbind	UDP	*	32771	(Idle)
inetd	TCP	*	32771	(LISTEN)
cachefsd	TCP	*	32771	(LISTEN)
cachefsd	TCP	*	32771	(LISTEN)
cachefsd	TCP	*	32771	(LISTEN)
inetd	UDP	*	32772	(Idle)
sadmind	UDP	*	32772	(Idle)
sadmind	UDP	*	32772	(Idle)
sadmind	UDP	*	32772	(Idle)
dmispd	UDP	*	32774	(Idle)
dmispd	TCP	*	32775	(LISTEN)
dtlogin	TCP	*	32776	(LISTEN)
Xsun	TCP	*	32776	(LISTEN)
dtlogin	TCP	*	32776	(LISTEN)
fbconsole	TCP	*	32776	(LISTEN)
dtgreet	TCP	*	32776	(LISTEN)
java	TCP	*	33691	(LISTEN)
rpcbind	UDP	*	*	(Unbound)
rpcbind	TCP	*	*	(IDLE)
sshd	TCP	dev.giac.org	22->10.10.10.12	(ESTABLISHED)
java	TCP	localhost	32778->localhost	(BOUND)
java	TCP	localhost	33690->localhost	(BOUND)
java	TCP	localhost	34487->localhost	(BOUND)
java	TCP	dev-test.giac.org	5555->user.giac.org	(ESTABLISHED)
java	TCP	dev-test.giac.org	5555->user.giac.org	(ESTABLISHED)
inetd	TCP	*	fs	(LISTEN)
xfs	TCP	*	fs	(LISTEN)
xfs	TCP	*	fs	(LISTEN)
rpcbind	UDP	*	sunrpc	(Idle)
rpcbind	TCP	*	sunrpc	(LISTEN)
syslogd	UDP	*	syslog	(Idle)

Impact of Findings/Improvements – lsof provides a large amount of information that must be analyzed in terms of the function of the computer. Used with the ps command, as shown in section 3.4.3, processes that are not needed can be determined and disabled. Also, if Trojan processes are running, lsof will list them and they should be recognized as unknown processes by the system administrator.

3.12.2 Analysis of the SANS Top Twenty Vulnerabilities Scan

The SANS Top Twenty Vulnerabilities is a consensus of the most severe security vulnerabilities found on the Internet. [10] Written by Bob Todd, of Advanced Research Corporation (http://www-arc.com), it is an adaptation of the SARA (Security Auditor's Research Assistant) network scanner made to audit against the Top 20 vulnerabilities list. [11] The complete scan is found in Appendix D. A synopsis of the scan results is as follows:

Scan Finding	Explanation/Security Impact
`Negative: 1.1 System appears not to have been patched within the last month.`	Explanation - System has not been patched since it was configured. *Impact – System is vulnerable to known security holes. See section 3.8.*
`Negative: 2.8 CDE-related daemon fs not deactivated in inetd.conf.` `Negative: 3.1 sysid.net not deactivated` `Negative: 3.1 sysid.sys not deactivated` `Negative: 3.1 autoinstall not deactivated` `Negative: 3.1 cachefs.daemon not deactivated.` `Negative: 3.1 cacheos.finish not deactivated.` `Negative: 3.1 power not deactivated.` `Negative: 3.1 dmi rc script not deactivated.` `Negative: 3.1 llc2 not deactivated.` `Negative: 3.1 slpd not deactivated.` `Negative: 3.1 PRESERVE not deactivated.` `Negative: 3.1 bdconfig not deactivated.` `Negative: 3.1 wbem not deactivated.` `Negative: 3.1 afbinit not deactivated.` `Negative: 3.1 ifbinit not deactivated.` `Negative: 3.1 ncalogd not deactivated.` `Negative: 3.1 ncad not deactivated.` `Negative: 3.1 mipagent not deactivated.` `Negative: 3.4 rpc miscellaneous services not deactivated.` `Negative: 3.5 ldap cache manager not deactivated.` `Negative: 3.6 lp not deactivated.`	Explanation – These are the processes that scanner found active. Many of these are not needed. The user must determine which of these is not required to perform the function of the system. Blindly turning off everything will lead to problems. *Impact – Each of these should be examined to determine whether the system needs the provided functionality in order to perform its tasks. Many of these services are described in sections 3.4.2, 3.4.3, 3.10.1, & 3.11.1.*

Scan Finding	Explanation/Security Impact
Negative: 3.6 spc not deactivated. Negative: 3.7 volume manager not deactivated. Negative: 3.8 Graphical dtlogin not deactivated. Negative: 3.10 Apache web server not deactivated. Negative: 3.12 inetd is still active. Negative: 3.13 Serial login prompt not disabled.	
Negative: 4.1 Coredumps aren't deactivated. Negative: 4.2 Stack is not yet set non-executable. Negative: 4.3 NFS clients aren't restricted to privileged ports.	Explanation – These are operating system level configurations. *Impact – Implementing these changes will improve security without negatively impacting the system operation.*
Negative: 4.4 ip_strict_dst_multihoming isn't activated. Negative: 4.4 ip6_strict_dst_multihoming isn't activated. Negative: 4.4 ip_send_redirects isn't set to 0. Negative: 4.4 ip_ignore_redirect isn't set to 1. Negative: 4.4 ip6_ignore_redirect isn't set to 1. Negative: 4.4 Source routing (ip_forward_src_routed) should be deactivated Negative: 4.4 ip6 source routing (ip6_forward_src_routed) should be deactivated Negative: 4.4 Forwarding of directed broadcasts (ip_forward_directed_broadcasts) isn't disabled. Negative: 4.4 tcp_conn_req_max_q0 should be at least 4096 to avoid TCP flood problems. Negative: 4.4 ip_respond_to_timestamp isn't 0. Negative: 4.4 ip_respond_to_timestamp_broadcast should be 0. Negative: 4.4 ARP timer (arp_cleanup_interval) isn't less than 60,000. Negative: 4.5 TCP sequence numbers not	Explanation – These are operating system level network configurations. *Impact – Implementing these changes will improve security without negatively impacting the system operation.*

Scan Finding	Explanation/Security Impact
strong enough.	
Negative: 5.2 /var/adm/loginlog doesn't exist to track failed logins. Negative: 5.4 Couldn't find an active sadc line in /etc/rc2.d/S21perf to verify system acctg. Negative: 5.4 No sa1 line in /var/spool/cron/crontabs/sys -- no system accounting. Negative: 5.4 No sa2 line in /var/spool/cron/crontabs/sys -- no system accounting. Negative: 5.5 kernel-level auditing isn't enabled.	Explanation – These deal with system and process logging. *Impact – Implementing these changes will improve security without negatively impacting the system operation.*
Negative: 6.1 Never found separate /usr partition, so it couldn't be mounted read-only. Negative: 6.1 /dev3 is not mounted nosuid. Negative: 6.1 /dev1 is not mounted nosuid. Negative: 6.1 /dev2 is not mounted nosuid. Negative: 6.2 logging option isn't set on root file system	Explanation – These deal with the mounting options of the disk drives. *Impact – To implement the /usr recommendation the disk would have to be repartitioned which would impact operations. The nosuid recommendation may cause problems with the way the B2B webserver is implemented. The logging option could be implemented without negatively impacting system operations.*
Negative: 7.1 /etc/pam.conf appears to support rhost auth. Negative: 7.2 /etc/hosts.equiv file is present and not size zero. Negative: 7.4 Couldn't open cron.allow Negative: 7.4 Couldn't open at.allow Negative: 7.6 EEPROM banner isn't on. Negative: 7.6 /etc/issue doesn't have a authorized-use banner. Negative: 7.8 EEPROM isn't password-protected. Negative: 9.3 This machine isn't synced with ntp. Negative: 9.4 Fix-modes has not been run here. Negative: 6.6 Non-standard SUID program /usr/bin/pppd. Negative: 6.6 Non-standard SUID program	Explanation – These deal with authentication, SUID and misc issues. *Impact – The pam.conf could be changed without impacting system operation. The hosts.equiv file is needed for customer authentication using SSH hostbased authentication (see section 3.3.2). The file could be changed to shosts.equiv so that "r-commanrd" could not use the file if they were enabled. Banners could be implemented without negatively impacting the system*

Scan Finding	Explanation/Security Impact
/usr/bin/cdrw. Negative: 6.6 Non-standard SGID program /usr/SUNWale/bin/mailx.	*operation. EEPROM password protect will protect against direct attacks, but if the password is lost the operation of the system could be very negatively impacted. The SUID and SGID programs can be changed without negatively impacting the system operation.*

Impact of Findings/Improvements – The output of the tool is very easy to understand, giving either a "positive" or "negative" statement. The numbers associated with the statement refer to sections in the associated manual that provide information on how to correct the problem. The system administrator will need to discern which of the actions need to be taken and which cannot be taken because of the functionality required. Many of the items found were also found through analysis of other means, but the tool did find a number of items that were unique, to include: executable stack, a number of ipv4 and ipv6 issues, pam.conf settings, and non-standard SUID settings. Many of the negative findings relate to the unnecessary daemons that are running and were discussed in sections 3.4.2, 3.4.3, 3.10.1 & 3.11.1. In addition, the state of the ip parameters was examined which was not performed by any previous audit. The final score was 5.25/10.0 with 66 negative findings and 32 positive findings.

4.0 Critical Issues and Recommendations

This audit examined hardware, operating system, application software, physical security, network configuration, and network security within the context of the GIAC business and operational environment. In almost every analysis performed, there is at least one item that could be changed to improve the security or continuity of operation. While many of the negative impacts found were identified in multiple analyses, the findings were not identical, this indicates that no single tool finds everything and that it is necessary to use multiple approaches. Solving some of the issues is as simple as changing one line in a configuration file. There are solutions such as building walls and installing doors that may take an entire day, and others, like installing patches, that may take hours to perform but must be performed periodically. Mitigating the issues that impact security or continuity of operation must performed with care, because resolving some of the issues may also affect a required functionality.

The following table provides the ten most significant problems identified during the audit each with a statement of its impact on the organization and a proposed method for resolving it:

Table 2 – Critical Issues, Impacts and Solutions

Issue	Impact	Solution
CVS system	Software is exposed on a public web server.	Move software to CVS on development server which is not accessible to the public.
Sudo restrictions	Users shell out of sudo because they have the ability to execute all commands.	Restrict escape to shell by policy or reduction in granted commands. Edit the /usr/local/etc/sudoers file for the B2B group. The B2B line should be: **B2B ALL = NOPASSWD: ALL, !KILL, !SHUTDOWN, !HALT, !REBOOT, !SHELLS, !SU, !SNOOP** See section 3.3.3 for a stronger policy.
Absence of cron, lpr, uucp and news logging in syslog	If these are activated (accidentally or as part of an attack), syslog will not log any information so the activation may go unnoticed for a long period of time.	Enable logging to message log. **touch /var/log/messages.log** Then add the following line to /etc/syslog.conf : **cron.debug, lpr.debug, uucp.debug, news.debug /var/log/messages.log** Then restart the syslog daemon using kill – HUP pid.

Issue	Impact	Solution
Sa1 and Sa2 not running	No system activity reports are created.	Uncomment these command lines in sys crontab. (Note that crontab cannot be edited directly.) Use "crontab –e sys" to uncomment the lines.
No limitation on the use of cron.	Users can create jobs to run using cron without system admin approval.	Create a "/etc/cron.d/cron.allow" file with the entry "root". Add other users to the file only if there is a need and the system administrator approves.
Patches not current	System is vulnerable to known security issues.	Install security patches from Sun. Download the Solaris 8 cluster patch and any other security patches from http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access. To apply the patches, first read the directions, plan for downtime, and notify users. Boot system into single user and copy patches to /tmp. Run cluster install "./install_cluster". Install individual patches using "pkgadd –d patch-name". Reboot the system when finished. Make sure main applications are working properly.
No record of failed logins	Automated attempts to break-in are not detected.	Create the loginlog file: `touch /etc/adm/loginlog` and then edit "/etc/default" and set `SYSLOG_FAILED_LOGINS=0`
Executable Stack	Buffer overflows may allow dangerous code to be executed.	Follow directions in Solaris Benchmark Manual from CIS, e.g., `cat <<END_CFG >>/etc/system` `* Attempt to prevent and log stack-smashing attacks` `set noexec_user_stack = 1` `set noexec_user_stack_log = 1` `END_CFG`
Non-Standard SUID programs	These programs run as root when any user runs them, but it is not needed.	Unset SUID bit on programs with non-standard SUID as follows: `cd /usr/bin` `ls –la pppd` `-r-sr-xr-x 1 root bin … pppd`

Issue	Impact	Solution
		chmod u-s pppd **ls -la pppd** **-r-xr-xr-x 1 root bin … pppd** **ls -la cdrw** **-rwsr-xr-x 1 root bin … cdrw** **chmod u-s cdrw** **ls -la cdrw** **-rwxr-xr-x 1 root bin … cdrw**
Unneeded processes are running	The unneeded processes use computer resources, and some have known security issues.	Follow directions in Solaris Benchmark Manual from CIS, e.g., *Turn off services which are not commonly used* **cd /etc/rc2.d** **for file in S30sysid.net S71sysid.sys S72autoinstall ** **S73cachefs.daemon S93cacheos.finish S40llc2 ** **S47asppp S70uucp S72slpd S75flashprom S80PRESERVE ** **S85power S89bdconfig S90wbem S91afbinit S91ifbinit ** **S94ncalogd S95ncad** **Do** **[-s $file] && mv $file .NO$file** **done** **cd /etc/rc3.d** **for file in S77dmi S80mipagent** **do** **[-s $file] && mv $file .NO$file** **done** *Disable NFS server processes* **mv /etc/rc3.d/S15nfs.server ** **/etc/rc3.d/.NOS15nfs.server** *Disable LDAP cache manager* **mv /etc/rc2.d/S71ldap.client ** **/etc/rc2.d/.NOS71ldap.client** *Disable printer daemons* **mv /etc/rc2.d/S80lp /etc/rc2.d/.NOS80lp** **mv /etc/rc2.d/S80spc /etc/rc2.d/.NOS80spc** *Disable volume manager* **mv /etc/rc2.d/S92volmgt **

Issue	Impact	Solution
		`/etc/rc2.d/.NOS92volmgt` *Disable SNMP* `mv /etc/rc3.d/S76snmpdx \` `/etc/rc3.d/.NOS76snmpdx`

In summary, this report analyzed a particular server by examining system settings and processes, log files, and external and internal scans within the context of GIAC's business and operational environment. Each method of examination identified a number of security issues: some were reported by multiple tools, but others were unique, indicating that there is no single tool or method that an analyst can or should depend upon.

Analysis of results identified the ten issues listed in the table above as the most significant insecurities and realistic mitigation plans were defined for them. While these are only a portion of the issues that were found, they represent the major risks for security and continuity of operation of the test and development server. It should take three days or less to apply the fixes listed in the table above. When this has been done, the system administrator should initiate a series of follow-on projects, each beginning with selecting the next set of issues that need to be resolved.

Appendix A - Bibliography

1. *Sudo*: Sudo is free software and is distributed under a BSD-style license. **http://www.courtesan.com/sudo/sudo.html**

2. *Nmap*: "Network Mapper is an open source utility for network exploration or security auditing, **http://www.insecure.org/**

3. ISS: The **Internet Scanner™** application provides comprehensive network vulnerability assessment for measuring online security risks, Internet Security Systems (ISS), **http://www.iss.net/index.php**.

4. Sun Solaris 8 Answer Book, V1.4.2, Sun Microsystems, Inc., 2000, **http://www.sun.com/**.

5. Sun Solaris 8 manpages, Sun Microsystems, Inc., 1999, **http://www.sun.com/**.

6. CAMELEO®: An image processing software package, Caldera, **http://www.caldera.fr/products/products.html**.

7. PatchDiag Tool, version 1.0.4, is a Year 2000 compliant diagnostic tool that enables system administrators to examine a profile of the patches installed on their Solaris system against the most current profiles available from Sun Microsystems. **http://sunsolve.sun.com/**

8. OPENSSH: OpenSSH is a free version of the SSH protocol suite of network connectivity tools that replaces telnet, rlogin, ftp, and other such programs. **http://www.openssh.com/**

9. SSH, The Secure Shell, Barrett, D., Silverman, R., February, 2001, O'Reilly & Associates, Inc.

10. CIS: Center for Internet Security Solaris Benchmark, **http://www.cisecurity.org/**

11. SANS Top Twenty List - The SANS Top Twenty Vulnerabilities is a consensus of the most severe security vulnerabilities found on the Internet. **http://www.sans.org/top20.htm**

12. Sklar, S., SSHD_Config Annotated File, December 2001, **http://whippet.stanford.edu/~ssklar/misc/openssh/sshd_config.txt**

13. *Lsof* – List of Open Files – is a freeware program that provides information on commands that have open files including : owner, process id, port, status of port, and protocol. **http://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/lsof/**

Appendix B –NMAP Scan

```
Script started on Sat Mar 16 10:52:59 2002
/usr/local/bin/nmap -O -I -sT -sU -vv 10.10.10.99


Starting nmap V. 2.54BETA28 ( www.insecure.org/nmap/ )
Host DEV (10.10.10.99) appears to be up ... good.
Initiating Connect() Scan against DEV (10.10.10.99)

The Connect() Scan took 3 seconds to scan 1569 ports.
Initiating UDP Scan against DEV (10.10.10.99)
Too many drops ... increasing senddelay to 50000
The UDP Scan took 968 seconds to scan 1569 ports.

For OSScan assuming that port 22 is open and port 1 is closed and
neither are firewalled

Interesting ports on DEV (10.10.10.99):
(The 3117 ports scanned but not shown below are in state: closed)


Port       State       Service                  Owner
22/tcp     open        ssh
111/tcp    open        sunrpc
111/udp    open        sunrpc
177/udp    open        xdmcp
514/udp    open        syslog
844/udp    open        unknown
859/tcp    open        unknown
861/tcp    open        unknown
898/tcp    open        unknown
2201/tcp   open        ats
5555/tcp   open        unknown
6000/tcp   open        X11
7100/tcp   open        font-service
8888/tcp   open        sun-answerbook
32771/tcp  open        sometimes-rpc5
32771/udp  open        sometimes-rpc6
32772/tcp  open        sometimes-rpc7
32772/udp  open        sometimes-rpc8
32774/udp  open        sometimes-rpc12
32775/tcp  open        sometimes-rpc13
32776/tcp  open        sometimes-rpc15


Remote operating system guess: Sun Solaris 8 early acces beta through
actual release

OS Fingerprint:
```

```
TSeq(Class=RI%gcd=1%SI=13DC9%IPID=I%TS=100HZ)
T1(Resp=Y%DF=Y%W=60DA%ACK=S++%Flags=AS%Ops=NNTNWM)
T2(Resp=N)
T3(Resp=N)
T4(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=Y%W=0%ACK=S%Flags=AR%Ops=)
PU(Resp=Y%DF=Y%TOS=0%IPLEN=70%RIPTL=148%RIPCK=E%UCK=E%ULEN=134%DAT=E)


Uptime 15.761 days (since Thu Feb 28 16:54:29 2002)

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=81353 (Worthy challenge)
TCP ISN Seq. Numbers: B11D04FB B123B7FF B1280D8E B12BB0C8 B131BE39
IPID Sequence Generation: Incremental


Nmap run completed -- 1 IP address (1 host up) scanned in 990 seconds
```

Appendix C – ISS Scan

Network Vulnerability Assessment Report
This report lists the vulnerabilities detected by Internet Scanner after scanning the network.

Intended audience: This report is intended for security technicians (Security Administrators, Network Administrators, Workstation Support Engineers, or Helpdesk Support Engineers).

Purpose: For each host, the report provides the IP address, the DNS name, the operating system type, and remedy information for vulnerabilities detected by Internet Scanner.

Related reports: For a brief list of the types of vulnerabilities detected on each host, see the Line
Management/Vulnerability Assessment reports.

Vulnerability Severity: High Medium Low

IP Address {DNS Name}	Operating System
10.10.10.99 {dev.giac.org}	Unix

Medium tcppred: TCP sequence prediction (CAN-2001-0751)

Additional Information *More Information*
Operating System
10.10.10.99: Minimum guess (SYN/ACK received order):
1 out of 24 (4.167%)
10.10.10.99: Most frequent guess (SYN/ACK received order): 1 out of 24 (4.167%)

The TCP sequence was found to be predictable. When the TCP sequence is predictable, an attacker can send packets that are forged to appear to come from a trusted computer. These forged packets can compromise services, such as rsh and rlogin, because their authentication is based on IP addresses. Attackers can also perform session hijacking to gain access to unauthorized information.

Some Microsoft patches for this did not completely resolve the sequence predicability. The following information explains the varying levels of TCP sequence predictability in Windows operating systems:
- Windows NT 4.0 pre-SP3 systems are highly predictable.

- Windows NT 4.0 SP4 through SP6 use a different algorithm to reduce sequence predictability, but the systems remain predictable.
- Microsoft released patch MS99-046, which uses the same algorithm as Windows 2000, to fully fix the problem.
- Windows 2000 is not TCP predictable.

Internet Scanner users: Please note that this check can potentially be time consuming, and may greatly increase the time required to perform a scan.

Remedy:

Ask your vendor for patches to correct TCP sequence prediction. Note that some patches make sequence prediction more difficult, but still possible. As a result, the host may continue to report this vulnerability.

For Windows NT 4.0:
Apply the latest Windows NT 4.0 Service Pack (SP6a or later), available from the Windows NT Service Packs Web page. Note that Windows NT system may continue to report this vulnerability. After you successfully apply the Service Pack, apply the patch listed in Microsoft Security Bulletin MS99-046. See References.

For HP-UX 9.0:
Apply the appropriate patch for your system, as listed in CERT advisory CA-2001-09. See References.

For FreeBSD 3.x:
Upgrade to the latest version of FreeBSD (3.5.1-STABLE dated after 2000-09-28 or later), as listed in FreeBSD, Inc. Security Advisory FreeBSD-SA-00:52. See References.

For FreeBSD 4.x:
Upgrade to the latest version of FreeBSD (4.1.1-STABLE dated after 2000-09-28 or later), as listed in FreeBSD, Inc. Security Advisory FreeBSD-SA-00:52. See References.

For FreeBSD 5.x:
Upgrade to the latest version of FreeBSD (5.0-CURRENT dated 2000-09-28 or later), as listed in FreeBSD, Inc. Security Advisory FreeBSD-SA-00:52. See References.

For Cisco IOS 11.x and 12.x:
Apply the latest patch for this vulnerability, as listed in Cisco Security Advisory: Cisco IOS Software TCP Initial Sequence Number Randomization Improvements. See References.

For Cisco CBOS 2.0.1, 2.1.0, 2.1.0a, 2.2.0, 2.2.1, 2.2.1a, 2.3, 2.3.2, 2.3.5, 2.3.7 and 2.3.8:

Upgrade to the latest version of CBOS (2.42 or later), as listed in Cisco Systems Field Notice, May 22, 2001. See References.

For other distributions:
Contact your vendor for upgrade or patch information.

Appendix D – SANS Top Twenty Scan

```
*** CIS Ruler Run ***
Starting at time 20020321-15:13:22

Negative: 1.1 System appears not to have been patched within the last
month.
Positive: 2.2 telnet is deactivated.
Positive: 2.3 ftp is deactivated.
Positive: 2.4 rsh, rcp and rlogin are deactivated.
Positive: 2.5 tftp is deactivated.
Positive: 2.6 network printing is deactivated.
Positive: 2.7 rquotad is deactivated.
Negative: 2.8 CDE-related daemon fs not deactivated in inetd.conf.
Positive: 2.9 kerberos net daemons are deactivated.
Negative: 3.1 sysid.net not deactivated
Negative: 3.1 sysid.sys not deactivated
Negative: 3.1 autoinstall not deactivated
Negative: 3.1 cachefs.daemon not deactivated.
Negative: 3.1 cacheos.finish not deactivated.
Negative: 3.1 power not deactivated.
Negative: 3.1 dmi rc script not deactivated.
Negative: 3.1 llc2 not deactivated.
Negative: 3.1 slpd not deactivated.
Negative: 3.1 PRESERVE not deactivated.
Negative: 3.1 bdconfig not deactivated.
Negative: 3.1 wbem not deactivated.
Negative: 3.1 afbinit not deactivated.
Negative: 3.1 ifbinit not deactivated.
Negative: 3.1 ncalogd not deactivated.
Negative: 3.1 ncad not deactivated.
Negative: 3.1 mipagent not deactivated.
Positive: 3.2 nfs.server is deactivated.
Positive: 3.3 This machine isn't being used as an NFS client.
Negative: 3.4 rpc miscellaneous services not deactivated.
Negative: 3.5 ldap cache manager not deactivated.
Negative: 3.6 lp not deactivated.
Negative: 3.6 spc not deactivated.
Negative: 3.7 volume manager not deactivated.
Negative: 3.8 Graphical dtlogin not deactivated.
Positive: 3.9 Mail daemon is not listening on TCP 25.
Negative: 3.10 Apache web server not deactivated.
Positive: 3.11 snmp daemon is deactivated.
Negative: 3.12 inetd is still active.
Negative: 3.13 Serial login prompt not disabled.
Positive: 3.14 Found a good daemon umask.
Negative: 4.1 Coredumps aren't deactivated.
Negative: 4.2 Stack is not yet set non-executable.
Negative: 4.3 NFS clients aren't restricted to privileged ports.
Negative: 4.4 ip_strict_dst_multihoming isn't activated.
Negative: 4.4 ip6_strict_dst_multihoming isn't activated.
Negative: 4.4 ip_send_redirects isn't set to 0.
Negative: 4.4 ip_ignore_redirect isn't set to 1.
```

```
Negative: 4.4 ip6_ignore_redirect isn't set to 1.
Negative: 4.4 Source routing (ip_forward_src_routed) should be
deactivated
Negative: 4.4 ip6 source routing (ip6_forward_src_routed) should be
deactivated
Negative: 4.4 Forwarding of directed broadcasts
(ip_forward_directed_broadcasts) isn't disabled.
Negative: 4.4 tcp_conn_req_max_q0 should be at least 4096 to avoid TCP
flood problems.
Negative: 4.4 ip_respond_to_timestamp isn't 0.
Negative: 4.4 ip_respond_to_timestamp_broadcast should be 0.
Negative: 4.4 ARP timer (arp_cleanup_interval) isn't less than 60,000.
Negative: 4.5 TCP sequence numbers not strong enough.
Positive: 5.1 syslog captures AUTH messages.
Negative: 5.2 /var/adm/loginlog doesn't exist to track failed logins.
Positive: 5.3 cron usage is being logged.
Negative: 5.4 Couldn't find an active sadc line in /etc/rc2.d/S21perf to
verify system acctg.
Negative: 5.4 No sa1 line in /var/spool/cron/crontabs/sys -- no system
accounting.
Negative: 5.4 No sa2 line in /var/spool/cron/crontabs/sys -- no system
accounting.
Negative: 5.5 kernel-level auditing isn't enabled.
Negative: 6.1 Never found separate /usr partition, so it couldn't be
mounted read-only.
Negative: 6.1 /dev3 is not mounted nosuid.
Negative: 6.1 /dev1 is not mounted nosuid.
Negative: 6.1 /dev2 is not mounted nosuid.
Negative: 6.2 logging option isn't set on root file system
Positive: 6.3 /etc/rmmount.conf mounts all file systems nosuid.
Positive: 6.4 passwd, shadow and group files have right permissions and
owners.
Positive: 6.5 /tmp and /var/tmp have sticky bits set.
Negative: 7.1 /etc/pam.conf appears to support rhost auth.
Negative: 7.2 /etc/hosts.equiv file is present and not size zero.
Positive: 7.3 All users necessary are present in /etc/ftpusers
Negative: 7.4 Couldn't open cron.allow
Negative: 7.4 Couldn't open at.allow
Positive: 7.5 crontabs all have good ownerships and modes
Negative: 7.6 EEPROM banner isn't on.
Negative: 7.6 /etc/issue doesn't have a authorized-use banner.
Positive: 7.7 Root is only allowed to login on console
Negative: 7.8 EEPROM isn't password-protected.
Positive: 8.1 All system accounts are locked/deleted
Positive: 8.2 There were no +: entries in passwd, shadow or group maps.
Positive: 8.3 All users have passwords
Positive: 8.4 Only one UID 0 account AND it is named root.
Positive: 8.5 root's PATH is clean of group/world writable directories
or the current-directory link.
Positive: 8.6 root account has no rhosts, shosts, or netrc files.
Positive: 8.7 No user's home directory is world or group writable.
Positive: 8.8 No group or world-writable dotfiles!
Positive: 8.9 No user has a .netrc file.
Positive: 8.10 Umask appears to be good.
```

```
Positive: 9.2 System is running sshd.
Negative: 9.3 This machine isn't synced with ntp.
Negative: 9.4 Fix-modes has not been run here.
Preliminary rating given at time: Thu Mar 21 15:13:23 2002

      Preliminary rating = 5.25 / 10.00

Negative: 6.6 Non-standard SUID program /usr/bin/pppd.
Negative: 6.6 Non-standard SUID program /usr/bin/cdrw.
Negative: 6.6 Non-standard SGID program /usr/SUNWale/bin/mailx.
Ending run at time: Thu Mar 21 15:14:13 2002
```

Final rating = 5.25 / 10.00

Appendix E – Complete SSHD_Config File

```
#############################################################################
## /etc/ssh/sshd_config
##
=============================================================================
===========
## configuration file for OpenSSH sshd server, version 3.0.2/3.0.2p1
##
=============================================================================
===========
## $Id: sshd_config,v 1.2 2001/12/01 05:21:54 ssklar Exp ssklar $
#############################################################################

#############################################################################
##          **** Original ****
##List:      openssh-unix-dev
##Subject: ssh/sshd_config option confusion ...
##From:    "Sandor W. Sklar" <ssklar@stanford.edu>
##Date:    2001-12-01 3:33:35
##           http://whippet.stanford.edu/~ssklar/misc/openssh/sshd_config.txt
##           SSHD configuration file with manpage entries and comments.
##
##          **** Changes ****
## Jack Stinson 01/04/02
##  Made some changes to comments and change were made to obtain
##  the desired  results.
## Jack Stinson 01/09/02
## Added users under Allow and Deny.
## Decided to have just one daemon that listens on all IP Addresses.

#############################################################################

#############################################################################
## logging configuration
#############################################################################

## SyslogFacility [1,2]
## ----------------------------------------------------------------------
## Gives the facility code that is used when logging messages from sshd.
## The possible values are: DAEMON, USER, AUTH, LOCAL0, LOCAL1, LOCAL2,
## LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7.  The default is AUTH.
```

```
SyslogFacility AUTH

## LogLevel [1,2]
## ----------------------------------------------------------------------
## Gives the verbosity level that is used when logging messages from sshd.
## The possible values are: QUIET, FATAL, ERROR, INFO, VERBOSE and DEBUG.
## The default is INFO.  Logging with level DEBUG provides a large amount of data and
## is not recommended.

#LogLevel INFO
LogLevel DEBUG


##########################################################################
## general configuration
##########################################################################


## Protocol [1,2]
## ----------------------------------------------------------------------
## Specifies the protocol versions sshd should support. The possible
## values are "1" and "2". Multiple versions must be comma-separated.  The
## default is "2,1".

Protocol 2

## Port [1,2]
## ----------------------------------------------------------------------
## Specifies the port number that sshd listens on.  The default is 22.
## Multiple options of this type are permitted.  See also ListenAddress.

Port 22

## ListenAddress [1,2]
## ----------------------------------------------------------------------
## Specifies the local addresses sshd should listen on.  The following
## forms may be used:
##
##   ListenAddress host|IPv4_addr|IPv6_addr
##   ListenAddress host|IPv4_addr:port
##   ListenAddress [host|IPv6_addr]:port
##
## If port is not specified, sshd will listen on the address and all prior
## Port options specified. The default is to listen on all local addresses.
```

```
## Multiple ListenAddress options are permitted. Additionally, any Port
## options must precede this option for non-port qualified addresses.

#ListenAddress 0.0.0.0
#ListenAddress ::


## MaxStartups [1,2]
## ---------------------------------------------------------------------
## Specifies the maximum number of concurrent unauthenticated connections
## to the sshd daemon.  Additional connections will be dropped until
## authentication succeeds or the LoginGraceTime expires for a connection.
## The default is 10.
##
## Alternatively, random early drop can be enabled by specifying the three
## colon separated values: "start:rate:full" (e.g., "10:30:60").  sshd will
## refuse connection attempts with a probability of "rate/100" (30%) if there
## are currently "start" (10) unauthenticated connections.  The probability
## increases linearly and all connection attempts are refused if thenumber of
## unauthenticated connections reaches "full" (60).

MaxStartups 10

## LoginGraceTime [1,2]
## ---------------------------------------------------------------------
## The server disconnects after this time if the user has not successfully
## logged in.  If the value is 0, there is no time limit. The default is 600
## seconds.

#LoginGraceTime 600
LoginGraceTime 120

## UseLogin [1,2]
## ---------------------------------------------------------------------
## Specifies whether login(1) is used for interactive login sessions.
## Note that login(1) is never used for remote command execution.  The
## default is "no".

UseLogin no

## PrintLastLog [1,2]
## ---------------------------------------------------------------------
## Specifies whether sshd should print the date and time when the user
## last logged in.  The default is "yes".
```

```
PrintLastLog yes

## PrintMotd [1,2]
## ---------------------------------------------------------------------------
## Specifies whether sshd should print /etc/motd when a  user logs in
## interactively.  (On some systems it is also printed by the shell,
## /etc/profile, or equivalent.)  The default is "yes".

PrintMotd yes

## StrictModes [1,2]
## ---------------------------------------------------------------------------
## Specifies whether sshd should check file modes and ownership of the
## user's files and home directory before accepting login.  This is normally
## desirable because  novices sometimes accidentally leave their directory or
## files world-writable.  The default is "yes".

StrictModes yes

## ReverseMappingCheck [1,2]
## ---------------------------------------------------------------------------
## Specifies whether sshd should try to verify the remote host name and
## check that the resolved host name for the remote IP address maps back to
## the very same IP address.  The default is "no".

ReverseMappingCheck no

## ServerKeyBits [1]
## ---------------------------------------------------------------------------
## Defines the number of bits in the ephemeral protocol version 1 server
## key.  The minimum value is 512, and the default is 768.

ServerKeyBits 768

## KeyRegenerationInterval [1]
## ---------------------------------------------------------------------------
## In protocol version 1, the ephemeral server key is automatically
## regenerated after this many seconds (if it has been used).  The purpose of
## regeneration is to prevent decrypting captured sessions by later breaking
## into the machine and stealing the keys. The key is never stored anywhere.
## If the value is 0, the key is never regenerated.  The default is 3600
## seconds.
```

```
KeyRegenerationInterval 3600


## Ciphers [2]
## ------------------------------------------------------------------------
## Specifies the ciphers allowed for protocol version 2.  Multiple ciphers
## must be comma-separated.  The default is:
## "aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour".

Ciphers aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour

## MACs [2]
## ------------------------------------------------------------------------
## Specifies the available MAC (message authentication code) algorithms.
## The MAC algorithm is used in protocol version 2 for data integrity
## protection.  Multiple algorithms must be comma-separated.  The default is:
## "hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,
##  hmac-sha1-96,hmac-md5-96".

MACs hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-
sha1-96,hmac-md5-96

## KeepAlive [1,2]
## ------------------------------------------------------------------------
## Specifies whether the system should send (TCP) keepalive messages to the
## other side.  If they are sent, death of the connection or crash of one of
## the machines will be properly noticed.  However, this means that
## connections will die if the route is down temporarily, and some people
## find it annoying.  On the other hand, if keepalives are not sent, sessions
## may hang indefinitely on the server, leaving "ghost" users and consuming
## server resources. The default is "yes" (to send keepalives), and the server
## will notice if the network goes down or the client host reboots.  This
## avoids infinitely hanging sessions. To disable keepalives, the value
## should be set to "no" in both the server and the client configuration files.

KeepAlive yes

## ClientAliveInterval [2]
## ------------------------------------------------------------------------
## Sets a timeout interval in seconds after which if no data has been
## received from the client, sshd will send a message through the encrypted
## channel to request a response from the client.  The default is 0,
## indicating that these messages will not be sent to the client.  This
```

```
## option applies to protocol version 2 only.

ClientAliveInterval 0

## ClientAliveCountMax [2]
## ---------------------------------------------------------------------
## Sets the number of client alive messages (see above) which may be sent
## without sshd receiving any messages back from the client. If this
## threshold is reached while client alive messages are being sent, sshd will
## disconnect the client, terminating the session. It is important to note
## that the use of client alive messages is very different from Keepalive.
## The client alive messages are sent through the encrypted channel and
## therefore will not be spoofable. The TCP keepalive option enabled by
## Keepalive is spoofable. You want to use the client alive mechanism when
## you are basing something important on clients having an active connection
## to the server.  The default value is 3. If you set ClientAliveInterval
## (above) to 15, and leave this value at the default, unresponsive ssh
## clients will be disconnected after approximately 45 seconds.

ClientAliveCountMax 3



#########################################################################
##  file locations
#########################################################################

## PidFile [1,2]
## ---------------------------------------------------------------------
## Specifies the file that contains the process identifier of the sshd
## daemon.  The default is /var/tmp/sshd.pid.

PidFile /var/tmp/sshd.pid

## HostKey [1,2]
## ---------------------------------------------------------------------
## Specifies the file containing the private host keys (default
## /etc/ssh/ssh_host_key) used by SSH protocol versions 1 and 2.  Note that
## sshd will refuse to use a file if it is group/world-accessible. It is
## possible to have multiple host key files.  ``rsa1'' keys are used for
## version 1 and ``dsa'' or ``rsa'' are used for version 2 of the SSH
## protocol.  These keys are generated using "/usr/local/bin/ssh-keygen" with
## no password (no password is required for host keys).  Note that the key
## is composed of two parts, the private key: "ssh_host_key" and ssh_host_key.pub.
```

```
## rsa1 key for SSH1
HostKey /usr/local/etc/ssh_host_key
## rsa key for SSH2
HostKey /usr/local/etc/ssh_host_rsa_key
## dsa key for SSH2
HostKey /usr/local/etc/ssh_host_dsa_key

## AuthorizedKeysFile [1,2]
## ---------------------------------------------------------------------
## Specifies the file that contains the public keys that can be used for
## user authentication. AuthorizedKeysFile may contain tokens of the form %T
## which are substituted during connection set-up. The following tokens are
## defined: %% is replaced by a literal '%', %h is replaced by the home
## directory of the user being authenticated and %u is replaced by the
## username of that user.  After expansion, AuthorizedKeysFile is taken to be
## an absolute path or one relative to the user's home directory.  The
## default is ".ssh/authorized_keys".

AuthorizedKeysFile .ssh/authorized_keys

## XAuthLocation [1,2]
## ---------------------------------------------------------------------
## Specifies the location of the xauth(1) program.  The default is
## /usr/bin/X11/xauth.

XAuthLocation /usr/bin/X11/xauth

## Banner [2]
## ---------------------------------------------------------------------
## In some jurisdictions, sending a warning message before authentication
## may be relevant for getting legal protection.  The contents of the
## specified file are sent to the remote user before authentication is
## allowed.  This option is only available for protocol version 2.

#Banner
Banner /etc/motd

#########################################################################
## user and group access control
#########################################################################

## AllowUsers  [1,2]
## ---------------------------------------------------------------------
```

```
## This keyword can be followed by a list of user names, separated by
## spaces.  If specified, login is allowed only for users names that match
## one of the patterns. "*" and "?" can be used as wildcards in the patterns.
## Only user names are valid; a numerical user ID is not recognized.  By
## default login is allowed regardless of the user name.  If the pattern
## takes the form USER@HOST then USER and HOST are separately checked,
## restricting logins to particular users from particular hosts.

AllowUsers dev1@10.10.*.* dev2@10.10.*.* dev3@10.10.*.* dev4@10.10.*.*
dev5@10.10.*.*
AllowUsers adm1 adm2
AllowUsers customer1@yyyyyy customer2@xxxxxx


## DenyUsers [1,2]
## ----------------------------------------------------------------------
## This keyword can be followed by a number of user names, separated by
## spaces.  Login is disallowed for user names that match one of the
## patterns.  "*" and "?"  can be used as wildcards in the patterns.  Only
## user names are valid; a numerical user ID is not recognized.  By default
## login is allowed regardless of the user name.

DenyUsers root daemon bin sys adm lp uucp nuucp listen nobody noaccess nobody4
badmin

## AllowGroups [1,2]
## ----------------------------------------------------------------------
## This keyword can be followed by a list of group names, separated by
## spaces.  If specified, login is allowed only for users whose primary group
## or supplementary group list matches one of the patterns. "*"and "?" can be
## used as wildcards in the patterns.  Only group names are valid; a
## numerical group ID is not recognized.  By default login is allowed
## regardless of the group list.

#AllowGroups

## DenyGroups [1,2]
## ----------------------------------------------------------------------
## This keyword can be followed by a number of group names, separated by
## spaces.  Users whose primary group or supplementary group list matches one
## of the patterns aren't allowed to log in.  "*" and "?" can be used as
## wildcards in the patterns.  Only group names are valid; a numerical group
## ID is not recognized.  By default login is allowed regardless of the group
## list.
```

```
#DenyGroups

## PermitRootLogin [1,2]
## ---------------------------------------------------------------------
## Specifies whether root can login using ssh(1).  The argument must be
## "yes", "without-password", "forced-commands-only" or "no".  The default is
## "yes".

## May be changed to YES, if needed.  Use "su" to obtain root access.  This
## may fail, if You are unable to login to a user account due to corrupt
## login scripts.(JS)

PermitRootLogin no


#########################################################################
##  password authentication
#########################################################################

## PasswordAuthentication [1,2]
## ---------------------------------------------------------------------
## Specifies whether password authentication is allowed. The default is "yes".

PasswordAuthentication yes

## PermitEmptyPasswords [1,2]
## ---------------------------------------------------------------------
## When password authentication is allowed, it specifies whether the
## server allows login to accounts with empty password strings.  The default
## is "no".

PermitEmptyPasswords no

#########################################################################
##  public key and RSA authentication
#########################################################################

## PubkeyAuthentication [2]
## ---------------------------------------------------------------------
## Specifies whether public key authentication is allowed. The default is
## "yes".  Note that this option applies to protocol version 2 only.

PubkeyAuthentication yes
```

```
## RSAAuthentication [1]
## ---------------------------------------------------------------------
## Specifies whether pure RSA authentication is allowed. The default is
## "yes". This option applies to protocol version 1 only.

RSAAuthentication yes


#############################################################################
## trusted-host authentication
#############################################################################

## RhostsAuthentication [1]
## ---------------------------------------------------------------------
## Specifies whether authentication using rhosts or /etc/hosts.equiv files
## is sufficient.  Normally, this method should not be permitted because it
## is insecure. RhostsRSAAuthentication should be used instead, because it
## performs RSA-based host authentication in addition to normal rhosts or
## /etc/hosts.equiv authentication. The default is "no". This option applies
## to protocol version 1 only.

RhostsAuthentication no

## RhostsRSAAuthentication [1]
## ---------------------------------------------------------------------
## Specifies whether rhosts or /etc/hosts.equiv authentication together
## with successful RSA host authentication is allowed.  The default is "no".
## This option applies to protocol version 1 only.

## WARNINGS:
## 1) The /etc/hosts file must have the fully qualified host name
##    first so that an exact match is possible.
## 2) The user id of the client user must match the user id on the server.
##    (i.e. user XXX on client cannot ssh "YYY@server" because
##    the server will not authenticate.


RhostsRSAAuthentication yes

## HostbasedAuthentication [2]
## ---------------------------------------------------------------------
## Specifies whether rhosts or /etc/hosts.equiv authentication together
## with successful public key client host authentication is allowed
```

```
## (hostbased authentication).  This option is similar to
## RhostsRSAAuthentication and applies to protocol version 2 only.  The
## default is "no".


HostbasedAuthentication yes

## IgnoreRhosts  [1,2]
## ---------------------------------------------------------------------
## Specifies that .rhosts and .shosts files will not be used in
## RhostsAuthentication, RhostsRSAAuthentication or HostbasedAuthentication.
## /etc/hosts.equiv and /etc/ssh/shosts.equiv are still used.  The default is
## "yes".

IgnoreRhosts yes

## IgnoreUserKnownHosts  [1,2]
## ---------------------------------------------------------------------
## Specifies whether sshd should ignore the user's $HOME/.ssh/known_hosts
## during RhostsRSAAuthentication or HostbasedAuthentication.  The default is
## "no".

IgnoreUserKnownHosts no


#########################################################################
##  Kerberos and AFS options
##  ---------------------------------------------------------------------
##  Note:  OpenSSH must be built with Kerberos and/or AFS for these options
##         to be valid; do not enable them if sshd was not compiled with
##         that additional software.
#########################################################################

## KerberosAuthentication [1]
## ---------------------------------------------------------------------
## Specifies whether Kerberos authentication is allowed.  This can be in
## the form of a Kerberos ticket, or if PasswordAuthentication is yes, the
## password provided by the user will be validated through the Kerberos KDC.
## To use this option, the server needs a Kerberos servtab which allows the
## verification of the KDCs identity.  Default is "yes".

#KerberosAuthentication yes

## KerberosOrLocalPasswd [1]
```

```
## ----------------------------------------------------------------------
## If set then if password authentication through Kerberos fails then the
## password will be validated via any additional local mechanism such as
## /etc/passwd. Default is "yes".

#KerberosOrLocalPasswd yes

## KerberosTicketCleanup [1]
## ----------------------------------------------------------------------
## Specifies whether to automatically destroy the user's ticket cache file
## on logout.  Default is "yes".

#KerberosTicketCleanup yes

## KerberosTgtPassing [1]
## ----------------------------------------------------------------------
## Specifies whether a Kerberos TGT may be forwarded to the server.
## Default is "no", as this only works when the Kerberos KDC is actually an
## AFS kaserver.

#KerberosTgtPassing no

## AFSTokenPassing [1]
## ----------------------------------------------------------------------
## Specifies whether an AFS token may be forwarded to the server. Default
## is "yes".

#AFSTokenPassing yes

######################################################################
## other authentication methods
## ----------------------------------------------------------------------
## Note:  OpenSSH must be compiled with additional software for these
##        options to be of any use.
######################################################################

## ChallengeResponseAuthentication [?]
## ----------------------------------------------------------------------
## Specifies whether challenge response authentication is allowed. All
## authentication styles from login.comf(5) are supported. The default is
## "yes".

ChallengeResponseAuthentication yes
```

```
## PAMAuthenticationViaKbdInt [?]
## ---------------------------------------------------------------------
## Specifies whether PAM challenge response authentication is allowed.  This
## allows the use of most PAM challenge response authentication modules, but
## it will allow password authentication regardless of whether
## PasswordAuthentication is disabled.  The default is "no".

PAMAuthenticationViaKbdInt no

#########################################################################
##  port and X11 forwarding options
#########################################################################

## AllowTcpForwarding  [1,2]
## ---------------------------------------------------------------------
## Specifies whether TCP forwarding is permitted.  The default is "yes".
## Note that disabling TCP forwarding does not improve security unless users
## are also denied shell access, as they can always install their own
## forwarders.

## Not needed for E2E

AllowTcpForwarding no

## X11Forwarding [1,2]
## ---------------------------------------------------------------------
## Specifies whether X11 forwarding is permitted.  The default is "no".
## Note that disabling X11 forwarding does not improve security in any way,
## as users can always install their own forwarders.

X11Forwarding no

## X11DisplayOffset [1,2]
## ---------------------------------------------------------------------
## Specifies the first display number available for sshd's X11 forwarding.
## This prevents sshd from interfering with real X11 servers.  The default
## is 10.

X11DisplayOffset 10

## GatewayPorts [1,2]
## ---------------------------------------------------------------------
## Specifies whether remote hosts are allowed to connect to ports
## forwarded for the client.  The argument must be "yes" or "no". The default
```

```
## is "no".

GatewayPorts no


#########################################################################
##  subsystems
#########################################################################

## Subsystem [2]
## ----------------------------------------------------------------------
## Configures an external subsystem (e.g., file transfer daemon).
## Arguments should be a subsystem name and a command to execute upon
## subsystem request.  The command sftp-server(8) implements the "sftp" file
## transfer subsystem.  By default no subsystems are defined. Note that this
## option applies to protocol version 2 only.


Subsystem      sftp    /usr/local/libexec/sftp-server

#########################################################################
#########################################################################
```

Appendix F – Sudoers Configuration File

```
##########################################################################
##
# IMPORTANT:    Any modification of this file without authorization     #
#             from the GAIC Lab Systems Administrator is a violation    #
#             of GAIC Lab Security Policies and Procedures.             #
##########################################################################
##
# sudoers config for dev.gaic.org
#
# Note:        Only administrators are allowed root priviledges.
# Admins:      adm1, adm2
#
#      **** CHANGES ****
# Created November 01, 2001  by Jack Stinson
#
# sudoers file.
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the sudoers man page for the details on how to write a sudoers file.
#
#

# Host alias specification

# User alias specification
User_Alias      FULLTIMERS = adm1, adm2
User_Alias      B2B = dev1, dev2, dev3, dev4, dev5, dev6

# Cmnd alias specification
Cmnd_Alias      KILL = /usr/bin/kill
Cmnd_Alias      SHUTDOWN = /usr/sbin/shutdown
Cmnd_Alias      HALT = /usr/sbin/halt
Cmnd_Alias      REBOOT = /usr/sbin/reboot
Cmnd_Alias      SHELLS = /usr/bin/sh, /usr/bin/ksh, /usr/bin/rsh, /usr/bin/remsh,
/usr/bin/jsh, /usr/bin/rksh, /usr/xpg4/bin/sh
Cmnd_Alias      SU = /usr/bin/su
Cmnd_Alias      SNOOP = /usr/sbin/snoop

# User privilege specification
root    ALL=(ALL) ALL
```

```
Defaults:B2B    !authenticate
FULLTIMERS      ALL = NOPASSWD: ALL
B2B             ALL = NOPASSWD: ALL
```

Appendix G – Syslog Archive Script

```
#!/bin/sh
# archive_syslogs.sh
# RUN DAILY VIA ROOT CRON JOB
#
#
# Procedure:
# 1. copy all syslog files to archive directory
# 2. "zero" the current syslog files
#
# set up directory paths
#
ARCHIVE_DIR=/b2b/ARCHIVE
SYSLOG_ARCHIVE_DIR=$ARCHIVE_DIR/syslog_archive
#
# set up variables for archived log names
# format: <logname>.log.<hostname>.<date>
#
HOSTNAME=`/usr/bin/hostname`
ARCHIVE_DATE=`/usr/bin/date '+%m%d%y%n'`
#
# "echo" variables (used for debugging)
#echo ${ARCHIVE_DIR}
#echo ${SYSLOG_ARCHIVE_DIR}
#echo ${HOSTNAME}
#echo ${ARCHIVE_DATE}
#
# start script
#
# check the archive directory
if [ ! -d $ARCHIVE_DIR ]; then
      mkdir $ARCHIVE_DIR
fi
if [ ! -d $SYSLOG_ARCHIVE_DIR ]; then
      mkdir $SYSLOG_ARCHIVE_DIR
fi
#
# copy the "syslog" files to the archive directory,
# then "zero" the current logs
cd /var/log
if [ -f auth.log ]; then
      cp -p auth.log
$SYSLOG_ARCHIVE_DIR/auth.log.$HOSTNAME.$ARCHIVE_DATE
```

```
        /usr/bin/cat /dev/null > auth.log
fi
if [ -f auth-debug.log ]; then
        cp -p auth-debug.log $SYSLOG_ARCHIVE_DIR/auth-
debug.log.$HOSTNAME.$ARCHIVE_DATE
        /usr/bin/cat /dev/null > auth-debug.log
fi
if [ -f daemon.log ]; then
        cp -p daemon.log
$SYSLOG_ARCHIVE_DIR/daemon.log.$HOSTNAME.$ARCHIVE_DATE
        /usr/bin/cat /dev/null > daemon.log
fi
if [ -f kern.log ]; then
        cp -p kern.log
$SYSLOG_ARCHIVE_DIR/kern.log.$HOSTNAME.$ARCHIVE_DATE
        /usr/bin/cat /dev/null > kern.log
fi
if [ -f mail.log ]; then
        cp -p mail.log
$SYSLOG_ARCHIVE_DIR/mail.log.$HOSTNAME.$ARCHIVE_DATE
        /usr/bin/cat /dev/null > mail.log
fi
if [ -f message.log ]; then
        cp -p message.log
$SYSLOG_ARCHIVE_DIR/messages.log.$HOSTNAME.$ARCHIVE_DATE
        /usr/bin/cat /dev/null > message.log
fi
if [ -f sudo.log ]; then
        cp -p sudo.log
$SYSLOG_ARCHIVE_DIR/sudo.log.$HOSTNAME.$ARCHIVE_DATE
        /usr/bin/cat /dev/null > sudo.log
fi
if [ -f syslog.log ]; then
        cp -p syslog.log
$SYSLOG_ARCHIVE_DIR/syslog.log.$HOSTNAME.$ARCHIVE_DATE
        /usr/bin/cat /dev/null > syslog.log
fi
if [ -f user.log ]; then
        cp -p user.log
$SYSLOG_ARCHIVE_DIR/user.log.$HOSTNAME.$ARCHIVE_DATE
        /usr/bin/cat /dev/null > user.log
fi
if [ -f messages ]; then
```

```
        cp -p messages
$SYSLOG_ARCHIVE_DIR/messages.$HOSTNAME.$ARCHIVE_DATE
        /usr/bin/cat /dev/null > messages
fi
if [ -f sulog ]; then
        cp -p sulog $SYSLOG_ARCHIVE_DIR/sulog.$HOSTNAME.$ARCHIVE_DATE
        /usr/bin/cat /dev/null > sulog
fi
if [ -f loginlog ]; then
        cp -p loginlog
$SYSLOG_ARCHIVE_DIR/loginlog.$HOSTNAME.$ARCHIVE_DATE
        /usr/bin/cat /dev/null > loginlog
fi
if [ -f vold.log ]; then
        cp -p vold.log
$SYSLOG_ARCHIVE_DIR/vold.log.$HOSTNAME.$ARCHIVE_DATE
        /usr/bin/cat /dev/null > vold.log
fi

# end script
```