Global Information Assurance Certification Paper

GCUX Practical Assignment version 1.9

Security Analysis of GIAC Enterprises' UNIX Systems

Submitted By: Josephine Guinto
Date: March 18, 2003

Abstract/Summary

Sound security policies and standards should always be in place to protect an organization's network and its servers from both external and internal attacks. Although a company may be under the assumption that their servers are securely configured, periodic audits should be performed to determine the true security level of the environment. The following paper discusses the results of the UNIX security audit performed by the security consulting company Golden Security for the GIAC Enterprises organization. Several recommendations have been made to significantly improve the current security level of the audited system. The recommendations range from improving and securing the configuration of the UNIX operating system to creating and implementing strong security procedures and practices.

Table of Contents

Executive Summary

Purpose of Audit

GIAC Enterprises has hired Golden Security, a Security Consulting firm, to perform an audit of the UNIX servers within their network. The purpose of this audit is to identify the current security level of the organization's UNIX environment and to determine what actions they must take to reduce their vulnerability to security exposures.

Scope of Audit

Golden Security has chosen to audit the Neptune server, a Mail Transfer Agent (MTA) located within GIAC Enterprises' internal network. The reason behind this selection is that organizations are known to secure servers that are most vulnerable to attacks, such as those servers in direct contact with the Internet (e.g.: web servers). Servers within the internal network are often overlooked and are loosely secured or not secured at all. Similar to those external servers, these internal systems are also vulnerable to attacks as system compromises often originate from within the internal network. To protect their data and assets, organizations should ensure that all of the servers within their network are securely configured.

Conclusions

The overall state of security of the Neptune server must be significantly improved to reduce the organization's susceptibility to common security exposures. Several high-risk security vulnerabilities were detected that could have been addressed earlier by applying basic security practices to the server in question.

Most Important Recommendations for Fixes

The following are Golden Security's top recommendations to address some of the most critical security exposures present on the Neptune server:

- A Security Patch Management System should be implemented to ensure that the latest operating system security patches are applied to the server.
- The controls surrounding the root account should be strengthened.
- Monitoring software should be installed on the server to detect changes to the system.
- All unnecessary packages should be removed from the server.
- All unnecessary services should be disabled.

1.0 Description of System and Audit Methodology

1.1 Description of System

Hardware Platform and Specifications

GIAC Enterprises has selected IBM's xSeries 225 server (model 3SVE003) as their hardware of choice for the Neptune server. The system has been configured with a 2400 MHz Intel Xeon processor along with 512 MB of RAM and 30 GB of hard drive space.

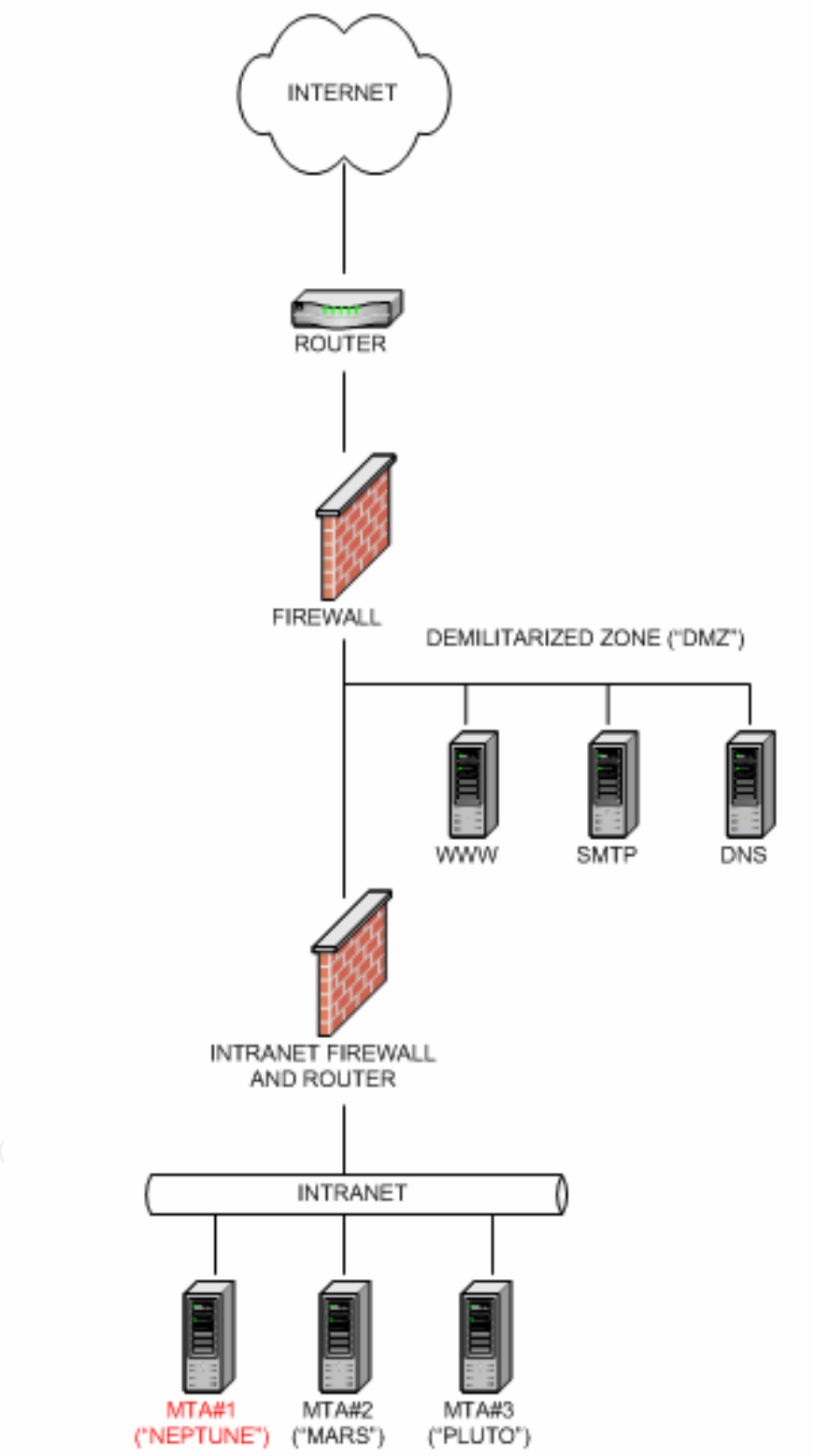
Software Operating System and Version

GIAC Enterprises has chosen to operate their internal MTA using the Red Hat Linux 7.3 operating system (kernel 2.4.18). The organization has commenced testing of the latest Red Hat release, version 8.0. However, an upgrade to this version will not take place until adequate testing has been performed to confirm the stability of this operating system.

Role of the Audited System

The primary role of the audited system is to act as one of the organization's three internal mail servers. As an MTA, the sole purpose of the system is to route mail messages for the organization. Internal mail is routed to its destination machine or to the other MTAs within the Intranet while external bound mail is routed to the organization's primary mail server located within the demilitarized zone (DMZ). The primary mail server within the DMZ has direct access to the Internet while the internal MTAs have no direct Internet connection as they are only located within the organization's Intranet (see figure 1.0).

Figure 1.0: Network Diagram of GIAC Enterprises



Applications and Tools

As the role of the audited server is to transfer mail for the organization, GIAC Enterprises has chosen to use the Sendmail application to carry out this function. The current Sendmail version applied to the server is Sendmail 8.11.6.

Specific Risks and Concerns

Given the role of the server within the environment, the major concern is determining whether or not the system has been sufficiently secured. Although the server is located within the internal network, a minimal amount of hardening to the organization's security standards or to the industry's recommended best practices should have taken place to address commonly known security vulnerabilities. In addition, a process should exist to ensure that the system remains in a secured state. With the Sendmail application installed, security risks pertaining specifically to this application are also of a concern.

1.2 Audit Methodology

Golden Security employed a 4-step process to perform the audit of the internal mail server "Neptune".

Step 1: Review of Corporate Standards & Administrative Procedures.

Golden Security reviewed GIAC Enterprises' standards and security policies relevant to the audited server. In addition, interviews were performed with several GIAC employees to discuss both the standards and the administrative practices currently in place. The main objective was to determine the type of standards and security policies that have been defined by GIAC Enterprises and how the company ensures that these standards and policies are being met.

Step 2: Use of the Center For Internet Security's (CIS) Linux Benchmark Tool (version 1.0.0) to determine operating system vulnerabilities.

Golden Security executed a host based vulnerability scan using the CIS Linux benchmarking tool. The purpose of the scan was to determine the security level of the Neptune server by analyzing the type of vulnerabilities identified by the benchmarking tool. The results of the scan can be viewed in Appendix A.

Step 3: Use of the scanning tools Nmap & Nessus to identify network vulnerabilities.

Golden Security executed a network vulnerability scan against Neptune using both the Nmap and the Nessus scanning tool. The purpose of the scan was to

identify the network vulnerabilities present on the system. The results of these scans can be viewed in Appendices B & C.

Step 4: *Manual execution of security checklist*.

Golden Security verified the configuration of the Neptune server using their own in-house checklist. This checklist is based on several widely known Linux security publications. Many of the items are simple verifications of permission settings of sensitive files while some of the checklist items involve manually executing commands. The results of this manual verification can be viewed in Appendix D.

2.0 Detailed Analysis

2.1 Operating System Vulnerabilities

At this present time, the latest Red Hat Linux Operating System release available is version 8.0. Although GIAC Enterprises is one release behind, the 7.3 version is considered stable and is still supported by Red Hat.

In regards to Security Patch vulnerabilities, the CIS Linux Benchmarking tool has indicated that the server has been patched within the last month. However, Golden Security consulted the Red Hat Errata Alerts website (**https://rhn.redhat.com/errata/rh73-errata.html**) and discovered that the following packages for this server have been updated and are available for installation.

bind-utils-9.2.1-1.7x.2	openldap-2.0.27-2.7.3
cpp-2.96-113	openldap-clients-2.0.27-2.7.3
evolution-1.0.3-6	openssh-3.1p1-6
fileutils-4.1-10.1	openssh-askpass-3.1p1-6
gaim-0.59.1-0.7.3	openssh-askpass-gnome-3.1p1-6
galleon-1.2.6-0.7.3	openssh-clients-3.1p1-6
gcc-2.96-113	openssl-0.9.6b-28
gdb-5.2-2	pam-0.75-46.7.3
ghostscript-6.52-9.4	perl-Digest-MD5-2.20-1
glibc-2.2.5-42	pine-4.44-7.73.0
glibc-common-2.2.5-42	psmisc-20.2-3.73
glibc-devel-2.2.5-42	python-1.5.2-43.73
glibc-kernheaders-2.4-7.16	python2-2.2.2-11.7.3
hwdata-0.14.1-1	qt-3.0.5-7.14
krb5-libs-1.2.4-4	rhn_register-2.8.27-1.7.3
libpng-1.0.14-0.7x.4	rhn_register-gnome-2.8.27-1.7.3

libstdc++-2.96-113	scrollkeeper-0.3.4-5
losetup-2.11n-12.7.3	tar-1.13.25-4.7.1
modutils-2.4.18-3.7x	tkinter-1.5.2-43.73
mount-2.11n-12.7.3	ucd-snmp-4.2.5-7.73.0
mozilla-1.0.1-2.7.3	up2date-2.8.39-1.7.3
mozilla-chat-1.0.1-2.7.3	up2date-gnome-2.8.39-1.7.3
mozilla-mail-1.0.1-2.7.3	util-linux-2.11n-12.7.3
mozilla-nspr-1.0.1-2.7.3	vim-common-6.1-18.7x.2
mozilla-nss-1.0.1-2.7.3	vim-minimal-6.1-18.7x.2
mozilla-psm-1.0.1-2.7.3	wget-1.8.2-4.73
nautilus-1.0.6-16	xchat-1.8.9-1.73.0
nscd-2.2.5-42	xinetd-2.3.7-4.7x

Although a variety of packages are available for updating, several of these packages are not required to support the activities of the server. Rather than updating these packages, they should be removed altogether. Golden Security suggests that GIAC Enterprises closely examine the installed packages on the Neptune server and retain only those that are absolutely required. For instance, development packages such as compilers should be removed to reduce the ability of attackers to compile exploits against the system. In addition, the X Windows system should be removed. This application has many security vulnerabilities associated with it. Since the administrators have confirmed that X Windows has not even been configured for use, it should be removed.

By removing unnecessary packages, GIAC Enterprises will reduce the number of patches that need to be applied to the server. At the same time, they will also decrease their susceptibility to security exposures associated with these removed packages.

2.2 Security Patch Installation/Management

Golden Security could find no evidence of a defined security patch installation/management process to ensure that the latest & most relevant security patches are applied to the server. Through the interviews conducted, it was confirmed that security patches are implemented only when the system administrators have been notified that a new patch is available. The source of this notification is via email from BugTraq. Once notification has been received, the patch may be downloaded and applied directly to the server.

Golden Security has several major concerns with the current security patch implementation process:

- **Testing Not Performed** - the administrators are not adequately testing the patches on a test environment prior to the production installation of the

patch. Without proper testing, there is the risk that the patch could have an adverse impact on the server.

- **Notification Method** - within the system administrators group, two individuals are currently receiving BugTraq email notifications. However, neither of the two has been given the responsibility for ensuring patches have been applied. As a result, email notifications can be received but there is no guarantee that the required patches will be installed.

- **Lack of Records** - records are not maintained to track what patches have been applied to the server. Some form of record keeping (e.g.: database records) should be implemented to allow the organization to quickly determine the current patch level of their servers.

2.3 Configuration vulnerabilities

2.3.1 Unnecessary Services

The following services have been reported as enabled (refer to Appendix D.1 to see the full list of active services). Golden Security recommends that these services be disabled as they are not required for the server to carry out its mail transfer activities:

- **apmd** – used to monitor battery power on laptops. This service is not required as the server is not installed on a laptop. As such, it should be disabled.

- **atd** – this is a scheduling utility to perform one-time execution of jobs. Although scheduling jobs is a necessary function, the cron daemon can be used to perform this function. Consequently, the atd service should be disabled.

- **gpm** – this provides cut and paste functions for command line sessions. This service is not essential so it should be disabled.

- **kudzu** – the hardware detection program. The system administrators have confirmed that the hardware configuration of Neptune is stable and does not change on a frequent basis. As a best practice, this service should be disabled and only activated when hardware changes are made.

- **netfs** – this service mounts exported file systems. Since network-based filesystems are not in use, this service should be disabled.

- **anacron** – this scheduling utility is not used by the administrators. As such, this service should be disabled.

- **xfs** – this is the X font server and is used for font support. Due to the security risks it presents, X Windows should be removed from the server altogether. Consequently, the xfs service should be disabled.

- **lpd** – since the server is not connected to a printer, the line printer daemon should be deactivated.

- **xinetd** – the services defined within the /etc/xinted.d directory have all been disabled thus the xinetd service itself is not required and should be deactivated.

- **rhnsd** – this is the Red Hat Network Service daemon used to connect to the Red Hat Network. Since the administrators use their own workstations to download security patches, this daemon is not required and should be disabled.

- **autofs** & **nfslock** – NFS client processes are not required as Neptune does not access files from remote servers. These NFS-related services should be disabled.

- **portmapper** – NFS and NIS are not in use so the portmapper service should be deactivated (Golden Security has confirmed that no additional RPC-based services are in use).

- **rpc.statd** – this is a service used in conjunction with NFS to notify client machines if an NFS server is rebooting. Since the Neptune server does not make use of NFS, this service should be disabled.

2.3.2 Banners

The CIS benchmark tool has indicated that suitable banners have not been created for the Neptune server. Some form of legal text should be created warning users that only authorized access to the server is permitted. As a form of legal protection, Golden Security strongly recommends that a banner be placed in all locations where users can gain access to the server.

2.3.3 Removable Media Configuration

In regards to removable media, some additional configuration should be made to restrict the ability of users to import unauthorized programs onto the Neptune server.

- **"nosuid" option** - the current configuration within the /etc/fstab file permits floppies to be mounted with setuid programs. Golden Security strongly recommends that floppies be configured with the "nosuid" option within /etc/fstab to prevent users from bringing unauthorized setuid programs onto the server.

- **Users are permitted to mount CD-ROMS and floppies** – the Neptune server has been configured to permit all users to freely mount CD-ROMS and floppy disks. The system administrators have confirmed that unprivileged users do not require this type of access. Consequently, the /etc/security/console.perms file should be reconfigured to disable this feature (all lines with "floppy" or "cdrom" should be commented out or removed).

2.3.4 Boot-Level Access Control

As the Neptune server is not located in a physically secure environment, the server should be configured to prevent individuals from gaining unauthorized access via the following boot processes:

- **boot password** – the installed boot loader, GRUB, is not password protected. As the Neptune server is not physically protected from unauthorized access, a password should be created for the boot loader to prevent users from booting the system using external media (i.e.: CD-ROM, floppy).

- **single-user mode password** – the Neptune server is not password protected for single-user mode. Should a user reboot the server into single-user mode, they will automatically gain root access to the server without needing the root password. The server should be reconfigured to prompt the user for the root password prior to entering single-user mode.

- **<ctrl>-<alt>-<del> shutdown** – the Neptune server is susceptible to anonymous shutdowns via the <ctrl>-<alt>-<del> keyboard sequence. Golden Security recommends that this feature be disabled if it is not required.

2.3.5 System Access Control

The principle of least access privilege should be followed whenever server access is configured. Users should only be provided with the necessary privileges in order to carry out their job functions. Based on the audit, Golden Security has identified several issues regarding system access control. The

following items should be addressed by GIAC Enterprises to improve the system access control levels currently in place:

- **.rhosts** – although .rhosts files were not detected on the Neptune server, support for .rhosts authentication has not been disabled. .rhosts authentication permits users to allow other users on remote systems to log in to their account without providing a password. Although the resident applications do not use .rhosts authentication, as a recommended best practice, this authentication method should be disabled by deleting "rhosts_auth" lines from all files within the /etc/pam.d directory.

- **/etc/ftpusers** – the /etc/ftpusers file should be modified to deny ftp access for the following system accounts: nscd, ident, gopher, rpc, rpcuser, xfs, mailnull. Although these user accounts do not have valid login shells and the ftp service is de-activated, this is a recommended best practice should these accounts and the ftp service be re-enabled in the future.

- **cron usage –** the cron.allow & at.allow files have not been created and configured. As a result, all users are permitted to execute the "crontab" and "at" commands to submit scheduled jobs. The administrators have confirmed that only the root account is used to schedule jobs. As a result, the cron.allow and at.allow files should be created and configured to restrict cron usage to root. In addition, all cron related files (/etc/crontab, /var/spool/cron, /etc/cron.*) should be protected so that only root has read and write access to these files.

- **root logins** – Golden Security recommends that all entries within the /etc/securetty file be removed to prevent direct root logins. This will force users to login and "su" to the root account or to use sudo (if this has been configured). By preventing direct root logins, the root account will be better protected and a more suitable audit trail will be created to allow the administrators or the security group to monitor root's activities.

- **locking system accounts** – the default system accounts on the Neptune server should be locked to prevent users from logging into these accounts. System ids are not accounts that should be logged into. Rather, their privileges are used whenever users execute setuid/setgid programs owned by these accounts. To prevent direct logins, Golden Security recommends that the shell for these accounts be set to /dev/null (an invalid shell). In addition, an asterisk should be placed in the password field within /etc/passwd to create an invalid password for these ids.

- **umask** – an examination of the default umask on the system revealed that the umask value of 022 has been set. However, the CIS benchmarking tool has determined that the umask setting within the files /etc/profile, /etc/csh.login, and /etc/csh.login may have been configured to permit

group and world writable files. As only the owner should be permitted write access to their files, Golden Security recommends that the umask of 022 be set in the /etc/profile, /etc/csh.login, and /etc/csh.login files. If possible, a more secure umask of 027 should be used as this provides additional security by removing read, write, and execute access for the world.

- **password configuration** – GIAC Enterprises has not enforced strong password controls for the Neptune server. As passwords are often the first target for attackers, Golden Security strongly recommends that the password controls be re-configured to include the following:

  Max. Days Password is Valid = 30 days
  Min. Days Password Must be Used Before it is Changed = 1 day
  Min. Password Length = 8 characters
  No. of Previous Passwords Remembered = 5
  Min. Uppercase Letters = 1
  Min. Other Characters = 1
  Min. Digits = 1
  Min. Characters Not Present in Previous Password = 5

- **world writable files** – the "find" command was used to determine if world writable files were present on the server. Several world writable files were detected, most notably in the /tmp and /dev directories (refer to Appendix D.3 for a list of these files). GIAC Enterprises should carefully examine this list to determine if world write access is required as all users on the system have the ability to write to these files.

- **permissions for sensitive files** – Golden Security performed a verification of the permission settings for several critical system files. It was discovered that the majority of the files were not in compliance with the recommended settings and were configured with insecure permissions. To ensure that these files are protected from unauthorized changes, the file permissions should be changed to the recommended settings. Refer to Appendix D.4 for a listing of these files.

- **automatic timeout** – the Neptune server should be configured to automatically log users out after a defined period of time. Golden Security recommends that the timeout parameter within /etc/profile file be set to 600 seconds to ensure that users are logged out after 10 minutes of inactivity. This timeout function is important as the Neptune system administrators often log in using the root account. The lack of physical security is another reason why a timeout parameter should be configured as the server is not suitably protected from unauthorized physical access.

2.4 Risks From Installed Third-Party Software

Since the Neptune server acts as an internal mail server for GIAC Enterprises, Golden Security examined the configurations surrounding Sendmail to determine if security vulnerabilities could be identified. The following are Golden Security*'s* recommendations to improve the security surrounding Sendmail's configuration:

- the current Sendmail version installed on the server (8.11.6) should be upgraded to the latest Sendmail release, version 8.12.8. The main purpose of upgrading is to reduce the server's vulnerability to Sendmail security exposures. This is especially important as a new Sendmail buffer overflow vulnerability was recently detected (http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21950). To protect themselves against this vulnerability, organizations using Sendmail have been encouraged to upgrade their Sendmail application to version 8.12.8. Another benefit of upgrading is that the Sendmail binary is by default no longer setuid to root (as of version 8.12). In addition, the Sendmail daemon no longer needs to run as root. These new security enhancements will reduce Neptune's susceptibility to local root exploits.

- the "EXPN" and "VRFY" commands can be used by attackers to determine what user accounts exist on the system. The "noexpn" and "novrfy" options should be added to the sendmail configuration file to prevent these commands from being executed.

- when a user telnets to port 25 on Neptune, the Sendmail greeting message displays the version of Sendmail currently in use. The greeting string should be changed to remove this information as it lets attackers know which Sendmail exploits you are vulnerable to.

- the current permission setting for the /var/spool/mqueue directory is 755 root mail. These permissions should be changed to 700 as only root should have access to this mail directory and its corresponding files.

2.5 Administrative Practices

Although GIAC Enterprises has standards and policies in place to address how their Red Hat Linux servers should be configured, procedures have not been created to address administrative practices. Currently administrators perform various administrative duties as necessary and in whatever manner they wish. Golden Security strongly suggests that the role of the system administrators group be clearly defined so that they may be held accountable for their actions. In addition, these administrative procedures should contain detailed instructions on how the various administrative tasks should be performed. This will ensure that administrative activities are carried out in a consistent manner. In addition

the procedures can serve as a reference for day-to-day activities and during the training of any new hires.

2.6 Identification and Protection of Sensitive Data on the Host

2.6.1 Sensitive Files

GIAC Enterprises does not employ any type of monitoring software on the Neptune server. As a result, sensitive data files on the system can be modified without GIAC Enterprises' knowledge. Golden Security strongly recommends that a host-based monitoring tool, such as Tripwire, be installed on the server to monitor these critical system files on a periodic basis for changes. In addition, to ensure that the administrators do not make unauthorized changes to these files, a separate group should be given the responsibility for performing the monitoring reviews.

2.6.2 Core Files

Golden Security has detected that coredumps were not deactivated on the Neptune server. Although coredumps can aid in troubleshooting and debugging situations, the Neptune system administrators have confirmed that core files have never been consulted during past production problems. Although a script has been written by the administrators to remove core files on the system on a weekly basis, the /etc/security/limits.conf file has not been reconfigured to disable coredumps entirely. As core files have the potential of containing sensitive information, Golden Security recommends that coredumps be deactivated by setting the hard core limit to a size of zero within the /etc/security/limits.conf file. This would prevent core files from being created, thus removing the need to execute the weekly core file cleanup script.

2.5.1 System Logging

There are some concerns in regards to the logging process taking place on the audited server. The default /etc/syslog.conf file is being used to log various system activities, however, the concern is that the administrators are not monitoring these logs on a frequent basis. Logs are only consulted during troubleshooting or debugging situations. A second concern is that the logs are not shipped to a central logging server. Consequently, attackers could manipulate the logs on the Neptune system to hide their malicious activity. To address these two issues, Golden Security strongly recommends that the logs be transferred to a remote logging server to prevent them from being altered. In addition, a periodic review of these logs should be implemented to verify the activity taking place on the Neptune server.

2.7 Protection of Sensitive Data in Transit Over the Network or Internet

The sole purpose of the Neptune server is to transfer mail for the organization. As such, sensitive data, other than mail messages, are not transmitted over the network on a frequent basis. However, should this change in the future, Golden Security recommends that some form of encryption be used to secure this data in transit.

In regards to remote server access, both telnet and ftp have been disabled thus protecting account passwords and unencrypted data from being exposed. The administrators had installed SSH during the initial operating system set-up, however, this has yet to be configured and implemented as the users who have been granted access to the system log on directly at the server to perform their job functions.

2.8 Access Controls

2.8.1 Password Policy

GIAC Enterprises needs to strengthen their current password policies. Based on the audit, Golden Security did not find suitable password controls in place to protect the accounts on the Neptune server. The standards have indicated that strong password controls are required on all systems, however, no definition of these controls could be identified. The standards should be translated into specific hardening procedures that clearly outline the password controls that should be in place (refer to section 2.3.5 to view Golden Security's recommended password settings).

2.8.1 Administrator Access

As a means of attempting to follow the policy of least access privilege, GIAC Enterprises did not create user accounts for the members of the Neptune administrators group. These individuals access the server through direct root logons. Although the intent was to reduce the number of accounts on the server, the current log in process raises some concerns as the root id is used in such a way that individual accountability cannot be maintained. Should unauthorized activity take place using the root account, it would be difficult to determine which system administrator was responsible for the activity. A more suitable method would be for separate administrator accounts to be created. Should the use of root be required, "sudo" or "su to root" should be employed as opposed to direct root logins. This method would maintain individual accountability and provide a much better audit trail than the current login process in place.

2.8.2 Control of the Root Account

Based on the interviews conducted, it was discovered that the Neptune administrators group controls the root account. Each of the administrators is aware of the root password and as mentioned in the previous section, they directly log on to the root account when needed. This practice should be changed to allow for separation of duties. A separate department with GIAC Enterprises, such as the Information Security group, should take control of the root account (as they currently do for mission critical servers). When root access is required, the Neptune system administrators should request the root password from the Information Security group. This recommended process addresses the issue of separation of duties as the administrators can only obtain root access through valid authorized requests to the Information Security department.

2.8.3 Security Auditing

In regards to the security auditing that is taking place on the Neptune server, the issue of separation of duties is again a concern. The system administrators are responsible for configuring the server to ensure that it meets GIAC Enterprises' security standards. They are also responsible for verifying the security of the server on a periodic basis. Again, the Information Security department within GIAC Enterprises should be assigned this role as the administrators group is in essence auditing themselves.

2.9 Backup Policies & Disaster Preparedness

Every organization should ensure that their systems are adequately backed up and that disaster recovery processes are in place to allow their business to function in the event of a disaster (e.g. fire, flood, power shortage, etc). Should these procedures not exist, a company can quickly find itself out of business.

Within GIAC Enterprises, all servers are backed up to tape on a daily basis, regardless of server classification. As part of the backup process, the tapes are stored on-site for a one-week period and are then shipped to an off-site storage location for a two year retention period (at which point the tapes are then recycled back to GIAC Enterprises). Transmittal forms containing information about each tape, are filed at both GIAC Enterprises and at the off-site location to ensure that the correct tapes can be recalled from storage when required.

Although the current backup process is sound, GIAC Enterprises does not perform any type of restore testing. Golden Security strongly recommends that on a periodic basis, a tape be recalled from storage and a test server be used to

confirm that the Neptune server can be restored. Detailed procedures outlining the restore process should also be created.

In regards to disaster preparedness, GIAC Enterprises has an internal department, Disaster Recovery, that is responsible for ensuring that disaster recovery procedures are in place. As part of their involvement in this process, the administrators have provided all Neptune related standards to Disaster Recovery. In addition, each of the system administrators has been informed of what process they must follow should a disaster situation occur (i.e.: alternate location information, contract information, etc.). To ensure that the administrators can be held accountable during disaster situations, all GIAC Enterprises employees are required to sign a disaster recovery form on a yearly basis acknowledging that they have been informed of the disaster recovery process.

2.10 Other Issues

2.10.1 Change Control Process

Golden Security interviewed the Neptune system administrators to determine how changes are implemented on the server and how problems are resolved. From these interviews, it has been discovered that when changes must be implemented on the server (e.g. Sendmail configuration changes), the administrators log on as root and perform the required modifications. The same process is followed when problems arise in that the administrators log on to the system and perform the necessary troubleshooting activities.

Golden Security has several concerns in the way that system changes and problem resolutions are performed:

- **Testing** – adequate testing is not performed to determine if the configuration changes will adversely affect the server

- **Documentation** – detailed documentation describing what changes will be performed and what steps must be followed to reverse the change (if required) is lacking.

- **Authorization** – authorization from management and other departments that will be affected by these changes is lacking.

- **Verification** – a verification process performed by a separate group to ensure that only the required changes were made is not in place.

Although the current change control method allows the administrators to quickly troubleshoot problems and implement changes, it provides the administrators with the opportunity to impact the applications and processes running on the

server. GIAC Enterprises should re-evaluate their current change control process and modify it in such a way that the above items are addressed.

2.10.2 Anti-Virus Application

It was discovered that the Neptune server has not been configured with anti-virus scanning software. Although virus scanning of emails occurs at the primary mail server within the DMZ, viruses can be transmitted through alternate channels. Golden Security strongly recommends that an anti-virus application be installed on all servers located within GIAC Enterprises' network. Scheduled virus scanning of the Neptune system should take place on a frequent basis to ensure that the server does not contain any viruses.

3.0 Critical Issues and Recommendations

3.1 Top Ten Recommendations

Although several recommendations have been provided in regards to how the Neptune server can be configured to reduce its risk to common security vulnerabilities, the following are the top ten issues uncovered by the audit that should first be addressed.

3.1.1 Implement a Security Patch Management System

A security patch management system should be developed to ensure that the latest security patches and fixes are applied to the Neptune server in a timely fashion. This is a critical item as common security exploits can often be addressed through the application of security patches. Golden Security suggests that the following be performed:

- **Accountability** – an individual within the system administrators group should be made responsible for ensuring that security patch notifications are addressed in a timely fashion.

- **Method of Notification** – although two individuals have been set-up to receive email notifications from BugTraq, a group account should also be created to receive these notifications. This will allow patch notifications to still be sent to GIAC Enterprises should either of the two administrators terminate their employment with the organization.

- **Testing** – upon receiving notification of a new security patch or fix, the individual responsible for patch management must adequately test the

patch on a test server to ensure that it will not adversely affect the system.

- **Adequate Record Keeping** – records should be kept whenever security patches and fixes are applied. This will allow the system administrators to easily determine the current patch level of the Neptune server.

3.1.2 Improve the Controls Surrounding the Root Account

The controls surrounding the root account on the Neptune server must be addressed as the current process gives the administrators the opportunity to use root whenever they see fit. To enhance the current control process, Golden Security suggests that the following practices be applied:

- **su to Root** – the Neptune server should be configured such that the root account can only be accessed via the "su" to root command. To implement this configuration, all entries within the /etc/securetty file must be removed.

- **Information Security Group** – as they do for the mission critical servers, access to the root account should be under the control of an independent group such as the Information Security Group.

- **Authorization** – when the system administrators require access to the root account, a request form should be submitted to the Information Security Group. Via the request form, the administrators will provide justification for their request along with their management's authorization.

- **24-Hour Access Period** – the root password should only be given out for a maximum of 24 hours unless special permission has been granted. Once the 24-hour time period has expired, the Information Security group should terminate any root logins in place and immediately change the root password.

- **Adequate Record Keeping** – the request forms should be filed to keep a history of root access on the Neptune server. These forms can be used as a reference during internal audits or investigations.

3.1.3 Install Monitoring Software

GIAC Enterprises does not employ any type of monitoring software on the Neptune server to monitor sensitive files such as system files or Sendmail configuration files for changes. This must be addressed as unauthorized changes

to critical system files can more easily take place. The following are Golden Security's recommendations on how to address this issue:

- As a first step in this process, GIAC Enterprises should identify and document the permission settings and any specific configuration settings for all of the sensitive files that must be monitored.

- A monitoring tool, such as the open source software Tripwire (see www.tripwire.org/downloads/index.php), should be used to create a baseline of these sensitive files.

- Using this file baseline, a periodic review process should be created to determine if changes to the sensitive files have been made. Investigations can then take place when necessary to determine if the changes were authorized.

- A separate group such as the Information Security group should be responsible for monitoring these sensitive files. This will allow GIAC Enterprises to monitor the system administrators to ensure they have made only authorized modifications to these files.

3.1.4 Strengthen Password Controls

Within their standards, GIAC Enterprises has indicated that strong password controls must be implemented across all of the servers within their network. However, specific password controls have not been defined. This issue should be immediately addressed as attackers attempting to break into a server often target weak passwords. Golden Security recommends that the following password settings be implemented on the Neptune server:

- Max. Days Password is Valid = 30 days
- Min. Days Password Must be Used Before it is Changed = 1 day
- Min. Password Length = 8 characters
- No. of Previously Remembered Passwords = 5
- Minimum Uppercase Letters Required = 1
- Minimum Other Characters Required = 1
- Minimum Digits Required = 1
- Minimum Characters Not Present in Previous Password = 5

To implement the above settings, the following configurations must be made:

a) */etc/login.defs* – the following parameters must be set to the following:

PASS_MAX_DAYS = 30
PASS_MIN_DAYS = 1

PASS_MIN_LEN = 8

b) */etc/pam.d/system-auth* – the following (in bold) must be added to the below lines:

- password sufficient /lib/security/pam_unix.so nullok use_authtok md5 shadow **remember=5**

- password required /lib/security/pam_cracklib.so retry=3 **dcredit=-1 ucredit=-1 ocredit=-1 lcredit=0 minlen=8 difok=5**

c) "touch /etc/opasswd" – this command must be executed as the /etc/opasswd file is required for password history (i.e.: tracks previously used passwords)

3.1.5 Remove Unnecessary Packages

It appears that during the initial operating system installation process, several packages, such as development tools, were installed. For security purposes, packages that are not specifically required for the Neptune server to carry out its mail transfer activities should be removed from the system. This will reduce the server's susceptibility to security vulnerabilities associated with the removed packages. In addition, by removing packages such as the development tools, attackers who have gained access to the system will be unable to compile local root exploits. Should any of the packages be required in the future, they may be reinstalled at a later date. In regards to the compilation tools, these can be installed when required to allow the administrators to compile various source code and then removed once they are no longer needed.

To remove a package from the Neptune server, the command "rpm –e *package name*" should be run. In addition, GIAC Enterprises should document what packages are required for the Neptune server and a review should be performed on a periodic basis to confirm that only these packages remain installed.

3.1.6 Remove Unnecessary Services

Several unnecessary services have been detected as enabled on the Neptune server. Similar to installed packages, only required services should be enabled. The remaining services should be deactivated to reduce the server's vulnerability to service specific exploits (refer to section 2.3.1 for a list of recommended services that should be disabled). To disable a service, the following command should be executed:

chkconfig - -level 2345 <*service name*> off

3.1.7 Address Sendmail Issues

As the Neptune server acts as one of the organization's three internal mail servers, the detected Sendmail issues should be addressed:

- Upgrade the Sendmail package to the latest version (8.12.8) to reduce the server's vulnerability to current Sendmail exploits – the latest version can be downloaded from www.sendmail.org

- To protect user account information, the "noexpn" and "novrfy" options should be added to the sendmail configuration file (this will prevent these commands from being executed). To implement this configuration, the following line should be modified within the /etc/sendmail.mc file (in addition, the following command will be needed to update the sendmail.cf file)

  \/etc/mail/sendmail.mc:
  define(`confPRIVACY_FLAGS', 'authwarnings, **novrfy**, **noexpn**, restrictqrun')dnl

  command to update sendmail.cf file:
  m4 /etc/mail/sendmail.mc > /etc/sendmail.cf\

- When a user telnets to port 25 on Neptune, the Sendmail greeting message displays the version of Sendmail currently in use. The greeting string should be changed to remove this information as it lets attackers know which Sendmail exploits you are vulnerable to. This can be done by modifying the "SMTP initial login message" parameter within the /etc/sendmail.cf file and changing it to a suitable warning banner.

- the current permission setting for the /var/spool/mqueue directory is 755 root mail. These permissions should be changed to 700 as only root should have access to this mail directory and its corresponding files. To change the permissions, the following command should be executed:

  chmod 700 /var/spool/mqueue

3.1.8 Strengthen Boot Level Access Controls

As the Neptune server is not physically isolated and protected, the boot level access controls should be strengthened to prevent unauthorized access to the server. Both the boot loader and single-user mode are not password protected. The server is also susceptible to anonymous shutdowns via the <ctrl>-<alt>-<del> keyboard sequence. To ensure that unauthorized users do not access the

server by compromising the current boot level access controls, the following configurations should be implemented:

- **boot password** – A password can be configured for the boot loader (GRUB) by adding the following line to the /etc/grub.conf file:

  password <*bootloader_password*>

- **single-user mode password** – A password can be configured for single-user mode by adding the following line to the /etc/inittab file:

  sum : S : wait : /sbin/sulogin

- **<ctrl>-<alt>-<del> shutdown** –Anonymous shutdowns should be disabled by adding the following line to the /etc/inittab file:

  ca : : ctrlaltdel : /sbin/shutdown -t3 -r now

3.1.9 Implement a Change Control Process

Section 2.10.1 has identified Golden Security*'s* concerns in regards to the way changes are implemented on the Neptune server. A change control process has not been clearly defined. As such, controls surrounding the changes implemented by the system administrators do not exist. To ensure that only authorized modifications are performed on the Neptune server and to reduce the possibility of a change negatively impacting the system, Golden Security strongly recommends that a change control process be created to encompass the following:

- **Request Form** – change control request forms should be created. These forms should be filled out whenever an administrator must implement any change to the server. Detailed instructions regarding the changes that will be made should be documented on the request form in addition to the steps that must be taken to reverse the change (in the event that the change adversely affects the server).

- **Authorization** – all groups that will be affected by the change should be required to provide their authorization prior to its implementation. It is a common practice for organizations to arrange weekly meetings as a means to discuss and approve/reject any proposed changes.

- **Verification** – a verification process performed by a separate group should be created to ensure that only the required changes were made. GIAC Enterprises' Information Security Group would be a suitable department to perform this function. They should be required to signoff on

the change request form to confirm that the change has been implemented correctly.

3.1.10 Banners

As a form of legal protection, Golden Security recommends that banners be incorporated into the Neptune system to warn users that only authorized access to the Neptune server is permitted. GIAC Enterprises should consult their legal counsel when determining what banner message should be displayed.

The following files should be edited and the appropriate banner message should be added:

- /etc/issue (operating system version information should be removed)
- /etc/issue.net (operating system version information should be removed)
- /etc/motd

3.2 Further Recommendations Outside of the Top Ten Threats

Although this is not a server-related security exposure, Golden Security strongly recommends that GIAC Enterprises re-evaluate their current documentation process to ensure that company standards have been implemented across the organization. Standards have been defined to provide a high-level overview of the security principles that GIAC Enterprises adheres to, however, Golden Security could not see a direct translation of these standards into administrative procedures and hardening practices. Based on the audit of the Neptune server, it appears that the standards were often misinterpreted or overlooked by the system administrators during the initial configuration of the system.

It is highly recommended that GIAC Enterprises translates their standards into detailed hardening procedures/checklists that identify specific server configuration settings that must be implemented during server hardening. These checklists will provide the organization with the following:

- A consistent process that can be followed by the administrators to ensure that the servers within the organization are in compliance with the company's security policies and standards.
- A reduction in the possibility of the standards being misinterpreted or overlooked during server hardening.
- A reference that can be used to re-configure a server should it ever crash or be compromised.

In addition to creating hardening checklists, the standards should be used to create administrative procedures that clearly identify the responsibilities of this group. Currently administrative procedures do not exist. Although the administrators for the Neptune server are well informed of their duties, procedures that detail these responsibilities should be created. This type of documentation will provide GIAC Enterprises with the following:

- Documentation for training newly hired system administrators.
- A method to hold the administrators accountable for their activities.
- A decrease in the possibility of administrative mistakes occurring on the server.
- Documentation that can be used during disaster recovery situations.

REFERENCES

Acheson, Steve, Green, John, and Hal Pomeranz. 6.3 Topics in UNIX Security. The SANS Institute, 2002.

Mann, Scott, and Ellen L. Mitchell. Linux System Security. New Jersey: Prentice Hall PTR, 2000.

Morgan, Andrew G. The Linux-PAM System Administrators' Guide. 26 June 2002 <http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam.html>.

Mourani , Gerhard. "How to Build, Install, Secure & Optimize Xinetd". 22 Oct 2002. OpenNA Linux. 4 February 2003 <http://www.openna.com/documentations/articles/xinetd/>

Nessus. 28 Feb 2003 <http://www.nessus.com/>

Pomeranz, Hal. 6.1 Common Issues and Vulnerabilities in UNIX Security. The SANS Institute, 2002.

---. 6.2 UNIX Security Tools. The SANS Institute, 2002.

---. 6.4 Running UNIX Applications Securely. The SANS Institute, 2002.

---. 6.5 UNIX Practicum. The SANS Institute, 2002.

"Red Hat Linux 7.3 General Advisories". March 12, 2003. Red Hat. 3 February 2003 <https://rhn.redhat.com/errata/rh73-errata.html>

"Red Hat Linux 7.3: The Official Red Hat Linux Reference Guide". 2002. Red Hat. 3 February 2003 <http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/ref-guide>

"Remote Sendmail Header Processing Vulnerability". 3 March 2003. Internet Security Systems. 5 March 2003 <http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21950>

Sendmail.org. 10 Feb 2003 <http://www.sendmail.org/>

The Center for Internet Security. 3 February 2003 <http://www.cisecurity.org/>

Tripwire.org. 5 February 2003 <www.tripwire.org/downloads/index.php>

"UNIX Security Checklist v2.0". 8 Oct. 2001. AusCERT. February 4, 2003 <http://www.auscert.org.au/render.html?it=1935&cid=1920>

APPENDIX A: Results of CIS Linux Benchmark Scan

*** CIS Ruler Run ***
Starting at time 20030206-19:49:41

Positive: 1.1 System appears to have been patched within the last month.
Negative: 2.2 No Authorized Only banner for telnet in file /etc/xinetd.d/telnet.
Negative: 2.2 No Authorized Only banner for ftp in file /etc/xinetd.d/wu-ftpd.
Negative: 2.2 No Authorized Only banner for login in file /etc/xinetd.d/rlogin.
Positive: 2.3 telnet is deactivated.
Positive: 2.4 ftp is deactivated.
Positive: 2.5 rsh, rcp and rlogin are deactivated.
Positive: 2.6 tftp is deactivated.
Negative: 2.7 xinetd either requires global 'only-from' statement or one for each service.
Negative: 3.1 apmd not deactivated.
Negative: 3.1 gpm not deactivated.
Positive: 3.2 NFS Server script nfs is deactivated.
Negative: 3.3 NFS script nfslock not deactivated.
Negative: 3.3 NFS script autofs not deactivated.
Positive: 3.4 NIS Client processes are deactivated.
Positive: 3.5 NIS Server processes are deactivated.
Negative: 3.6 portmapper not deactivated.
Positive: 3.7 samba windows filesharing daemons are deactivated.
Negative: 3.8 netfs rc script not deactivated.
Negative: 3.9 lpd (line printer daemon) not deactivated.
Positive: 3.10 Graphical login is deactivated.
Negative: 3.11 Mail daemon is on and collecting mail from the network.
Positive: 3.12 Web server is deactivated.
Positive: 3.13 snmp daemon is deactivated.
Positive: 3.14 DNS server is deactivated.
Positive: 3.15 postgresql (SQL) database server is deactivated.
Positive: 3.16 routing daemons are deactivated.
Positive: 3.17 Webmin GUI-based system administration daemon deactivated.
Positive: 3.18 Squid web cache daemon deactivated.
Negative: 3.19 xinetd is still active.
Positive: 3.20 Found a good daemon umask.
Negative: 4.1 Coredumps aren't deactivated.
Positive: 4.2 /etc/exports is empty or doesn't exist, so it doesn't need to be tuned for privports.
Negative: 4.3 /proc/sys/net/ipv4/tcp_max_syn_backlog should be at least 4096 to handle SYN floods.
Positive: 4.4 All 'additional' network parameters set correctly.
Positive: 5.1 syslog captures auth and authpriv messages.
Negative: 6.1 Removable filesystem /mnt/floppy is not mounted nosuid.

Negative: 6.2 PAM allows users to mount CD-ROMS. (/etc/security/console.perms)
Negative: 6.2 PAM allows users to mount floppies. (/etc/security/console.perms)
Positive: 6.3 password and group files have right permissions and owners.
Positive: 6.4 all temporary directories have sticky bits set.
Negative: 7.1 rhosts authentication not deactivated in /etc/pam.d/rlogin.
Negative: 7.1 rhosts authentication not deactivated in /etc/pam.d/rsh.
Positive: 7.2 /etc/hosts.equiv file not present or has size zero.
Negative: 7.3 User nscd is not present in /etc/ftpusers
Negative: 7.3 User ident is not present in /etc/ftpusers
Negative: 7.3 User gopher is not present in /etc/ftpusers
Negative: 7.3 User rpc is not present in /etc/ftpusers
Negative: 7.3 User rpcuser is not present in /etc/ftpusers
Negative: 7.3 User xfs is not present in /etc/ftpusers
Negative: 7.3 User mailnull is not present in /etc/ftpusers
Negative: 7.4 Couldn't open cron.allow
Negative: 7.4 Couldn't open at.allow
Negative: 7.5 The permissions on /etc/crontab are not sufficiently restrictive.
Negative: 7.6 No Authorized Only message in /etc/motd.
Negative: 7.6 No Authorized Only message in /etc/issue.
Negative: 7.7 /etc/securetty has a non tty1-12 line: tty10.
Negative: 7.8 GRUB isn't password-protected.
Negative: 8.1 uucp has a valid shell of /sbin/nologin.
Negative: 8.1 operator has a valid shell of /sbin/nologin.
Negative: 8.1 adm has a valid shell of /sbin/nologin.
Negative: 8.1 bin has a valid shell of /sbin/nologin.
Negative: 8.1 daemon has a valid shell of /sbin/nologin.
Negative: 8.1 ftp has a valid shell of /sbin/nologin.
Negative: 8.1 games has a valid shell of /sbin/nologin.
Negative: 8.1 gopher has a valid shell of /sbin/nologin.
Negative: 8.1 ident has a valid shell of /sbin/nologin.
Negative: 8.1 lp has a valid shell of /sbin/nologin.
Negative: 8.1 mail has a valid shell of /sbin/nologin.
Negative: 8.1 news has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 nobody has a valid shell of /sbin/nologin.
Negative: 8.1 rpc has a valid shell of /sbin/nologin.
Negative: 8.1 rpcuser has a valid shell of /sbin/nologin.
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 dangerous rhosts, shosts, or netrc files.
Positive: 8.8 No group or world-writable dotfiles!
Positive: 8.9 No user has a .netrc or .rhosts file.

Negative: 8.10 Default umask may not block world-writable. Check /etc/profile.
Negative: 8.10 Default umask may not block group-writable. Check /etc/profile.
Negative: 8.10 Default umask may not block world-writable. Check /etc/csh.login.
Negative: 8.10 Default umask may not block group-writable. Check /etc/csh.login.
Negative: 8.10 Default umask may not block group-writable. Check /etc/csh.cshrc.
Positive: 9.1 System is running sshd.
Preliminary rating given at time: Thu Feb 6 19:49:45 2003

Preliminary rating = 5.71 / 10.00

Positive: 6.5 No non-standard SUID/SGID programs found.
Ending run at time: Thu Feb 6 19:52:15 2003
Final rating = 5.89 / 10.00

APPENDIX B: Results of Nessus Scan

Nessus Scan Report

SUMMARY

- Number of hosts which were alive during the test : 1
- Number of security holes found : 1
- Number of security warnings found : 7
- Number of security notes found : 8

TESTED HOSTS

localhost (Security holes found)

DETAILS

+ localhost :
. List of open ports :

- smtp (25/tcp) (Security warnings found)
- sunrpc (111/tcp) (Security notes found)
- unknown (1241/tcp) (Security warnings found)
- x11 (6000/tcp) (Security warnings found)
- general/tcp (Security notes found)
- unknown (32769/tcp) (Security warnings found)
- sunrpc (111/udp) (Security notes found)
- unknown (32768/udp) (Security hole found)
- unknown (32768/tcp) (Security notes found)

. Warning found on port smtp (25/tcp)

The remote SMTP server allows anyone to
use it as a mail relay, provided that the source address
is set to '<>'.
This problem allows any spammer to use your mail server
to spam the world, thus blacklisting your mailserver, and
using your network resources.

Risk factor : Medium

Solution : reconfigure this server properly
CVE : CVE-1999-0819

. Warning found on port smtp (25/tcp)

According to the version number of the remote mail server,
a local user may be able to obtain the complete mail configuration
and other interesting information about the mail queue even if
he is not allowed to access those information directly, by running
 sendmail -q -d0-nnnn.xxx
where nnnn & xxx are debugging levels.

If users are not allowed to process the queue (which is the default)
then you are not vulnerable.

Solution : upgrade to the latest version of Sendmail or
do not allow users to process the queue (RestrictQRun option)
Risk factor : Very low / none
Note : This vulnerability is _local_ only
CVE : CAN-2001-0715

. Warning found on port smtp (25/tcp)

The remote SMTP server is vulnerable to a redirection
attack. That is, if a mail is sent to :

  user@hostname1@victim

Then the remote SMTP server (victim) will happily send the
mail to :
  user@hostname1

Using this flaw, an attacker may route a message
through your firewall, in order to exploit other
SMTP servers that can not be reached from the
outside.

*** THIS WARNING MAY BE A FALSE POSITIVE, SINCE
    SOME SMTP SERVERS LIKE POSTFIX WILL NOT
    COMPLAIN BUT DROP THIS MESSAGE ***

Solution : if you are using sendmail, then at the top
of ruleset 98, in /etc/sendmail.cf, insert :
R$*@$*@$* $#error $@ 5.7.1 $: '551 Sorry, no redirections.'

Risk factor :
 Low

. Information found on port smtp (25/tcp)

An SMTP server is running on this port
Here is its banner :
220 localhost.localdomain ESMTP Sendmail 8.11.6/8.11.6; Sat, 8 Feb 2003
09:52:52 -0500

. Information found on port smtp (25/tcp)

Nessus sent several emails containing the EICAR
test strings in them to the postmaster of
the remote SMTP server.

The EICAR test string is a fake virus which
triggers anti-viruses, in order to make sure
they run.

Nessus attempted to e-mail this string five times,
with different codings each time, in order to attempt
to fool the remote anti-virus (if any).

If there is an antivirus filter, these messages should
all be blocked.

*** To determine if the remote host is vulnerable, see
*** if any mail arrived to the postmaster of this host

Solution: Install an antivirus / upgrade it

Risk factor :
Low

. Information found on port sunrpc (111/tcp)

RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is
running on this
port

. Warning found on port unknown (1241/tcp)

A Nessus Daemon listens on this port.
supported versions: < NTP/1.0 >< NTP/1.1 >< NTP/1.2

>

. Warning found on port x11 (6000/tcp)

This X server does *not* allow any client to connect to it
however it is recommended that you filter incoming connections
to this port as attacker may send garbage data and slow down
your X session or even kill the server.

Here is the server version : 11.0
Here is the message we received : No protocol specified

Solution : filter incoming connections to ports 6000-6009
Risk factor : Low
CVE : CVE-1999-0526

. Information found on port general/tcp

Nmap found that this host is running Linux Kernel 2.4.0 - 2.4.17 (X86)

. Warning found on port unknown (32769/tcp)

The fam RPC service is running.
Several versions of this service have
a well-known buffer overflow condition
that allows intruders to execute
arbitrary commands as root on this system.

Solution : disable this service in /etc/inetd.conf
More information :
http://www.nai.com/nai_labs/asp_set/advisory/16_fam_adv.asp
Risk factor : High
CVE : CVE-1999-0059

. Information found on port unknown (32769/tcp)

RPC program #391002 version 2 'sgi_fam' (fam) is running on this
port

. Information found on port sunrpc (111/udp)

RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is
running on this
port

. Vulnerability found on port unknown (32768/udp) :

The remote statd service may be vulnerable
to a format string attack.

This means that an attacker may execute arbitrary
code thanks to a bug in this daemon.

*** Nessus reports this vulnerability using only
*** information that was gathered. Use caution
*** when testing without safe checks enabled.

Solution : upgrade to the latest version of rpc.statd
Risk factor : High
CVE : CVE-2000-0666

. Warning found on port unknown (32768/udp)

The statd RPC service is running.
This service has a long history of
security holes, so you should really
know what you are doing if you decide
to let it run.

* NO SECURITY HOLES REGARDING THIS
PROGRAM HAVE BEEN TESTED, SO
THIS MIGHT BE A FALSE POSITIVE *

We suggest that you disable this
service.

Risk factor : High
CVE : CVE-1999-0493

. Information found on port unknown (32768/udp)

RPC program #100024 version 1 'status' is running on this
port

. Information found on port unknown (32768/tcp)

RPC program #100024 version 1 'status' is running on this port

---

This file was generated by the Nessus Security Scanner

APPENDIX C: Results of nmap Scan

```
# nmap –sS –O localhost
Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1551 ports scanned but not shown below are in state: closed)
Port       State       Service
25/tcp     open        smtp
111/tcp    open        sunrpc
6000/tcp   open        X11

Remote operating system guess: Linux Kernel 2.4.0 - 2.4.17 (X86)
Uptime 0.022 days (since Sat Mar  1 10:35:39 2003)

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

APPENDIX D: Results of Manual Command Execution (part of Golden Security*'s* security checklist verification process).

Appendix D.1: Results of chkconfig - - list

Recommended services that should be turned off have been bolded.

keytable	0:off	1:on	2:on	3:on	4:on	5:on	6:off
atd	0:off	1:off	2:off	3:on	4:on	5:on	6:off
syslog	0:off	1:off	2:on	3:on	4:on	5:on	6:off
gpm	0:off	1:off	2:on	3:on	4:on	5:on	6:off
sendmail	0:off	1:off	2:on	3:on	4:on	5:on	6:off
kudzu	0:off	1:off	2:off	3:on	4:on	5:on	6:off
netfs	0:off	1:off	2:off	3:on	4:on	5:on	6:off
network	0:off	1:off	2:on	3:on	4:on	5:on	6:off
random	0:off	1:off	2:on	3:on	4:on	5:on	6:off
rawdevices	0:off	1:off	2:off	3:on	4:on	5:on	6:off
apmd	0:off	1:off	2:on	3:on	4:on	5:on	6:off
ipchains	0:off	1:off	2:on	3:on	4:on	5:on	6:off
iptables	0:off	1:off	2:on	3:on	4:on	5:on	6:off
crond	0:off	1:off	2:on	3:on	4:on	5:on	6:off
anacron	0:off	1:off	2:on	3:on	4:on	5:on	6:off
lpd	0:off	1:off	2:on	3:on	4:on	5:on	6:off
ntpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
portmap	0:off	1:off	2:off	3:on	4:on	5:on	6:off
xfs	0:off	1:off	2:on	3:on	4:on	5:on	6:off
xinetd	0:off	1:off	2:off	3:on	4:on	5:on	6:off
rhnsd	0:off	1:off	2:off	3:on	4:on	5:on	6:off
autofs	0:off	1:off	2:off	3:on	4:on	5:on	6:off
nfs	0:off	1:off	2:off	3:off	4:off	5:off	6:off
nfslock	0:off	1:off	2:off	3:on	4:on	5:on	6:off
identd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
radvd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
snmpd	0:off	1:off	2:off	3:off	4:off	5:off	6:off
snmptrapd	0:off	1:off	2:off	3:off	4:off	5:off	6:off

xinetd based services:

chargen-udp:	off
chargen:	off
daytime-udp:	off
daytime:	off
echo-udp:	off
echo:	off
services:	off
servers:	off
time-udp:	off

time: off

Appendix D.2: Results of Setuid & Setgid find Command

find / -perm +4000 –type f -print

/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/crontab
/usr/bin/lppasswd
/usr/bin/ssh
/usr/bin/rcp
/usr/bin/rlogin
/usr/bin/rsh
/usr/bin/sudo
/usr/lib/mc/bin/cons.saver
/usr/sbin/ping6
/usr/sbin/traceroute6
/usr/sbin/sendmail.sendmail
/usr/sbin/userhelper
/usr/sbin/usernetctl
/usr/sbin/userisdnctl
/usr/sbin/traceroute
/usr/X11R6/bin/XFree86
/bin/ping
/bin/mount
/bin/umount
/bin/su
/sbin/pwdb_chkpwd
/sbin/unix_chkpwd

find / -perm +2000 –type f –print

/usr/bin/lockfile
/usr/bin/slocate
/usr/bin/wall
/usr/bin/write
/usr/sbin/utempter
/usr/sbin/lockdev
/sbin/netreport

Appendix D.3: Results of World Writable find Command

find / -perm –2 ! –type l ! –type –c -print

/dev/log
/dev/shm
/var/spool/vbox
/var/tmp
/tmp
/tmp/.font-unix
/tmp/.font-unix/fs7100
/tmp/.X11-unix
/tmp/.X11-unix/X0
/tmp/.ICE-unix
/tmp/.ICE-unix/1191
/tmp/.ICE-unix/1143
/tmp/.ICE-unix/1144
/tmp/.ICE-unix/1145
/tmp/.ICE-unix/1146
/tmp/.ICE-unix/1147
/tmp/.ICE-unix/1155
/tmp/.ICE-unix/1164
/tmp/.ICE-unix/1148
/tmp/.ICE-unix/1208
/tmp/.ICE-unix/1207
/tmp/.ICE-unix/1206

Appendix D.4: File Permission Verification Results

File/Directory	Recommended Setting	Current Setting
/etc/inetd.conf or /etc/xinetd.conf	permissions = 600 owner = root	permissions = 664 owner = root
/etc/hosts.equiv	permissions = 600 owner = root	permissions = 664 owner = root
.rhosts (if required)	permissions = 600 owner = owner of account	permissions = 664 owner = root
/etc/netgroup	permissions = 600 owner = root	permissions = 664 owner = root
/etc/services	permissions = 644 owner = root	permissions = 664 owner = root
/etc/hosts.lpd	permissions = 600 owner = root	permissions = 664 owner = root
/etc/login.defs	permissions = 600 owner = root	permissions = 664 owner = root

File/Directory	Recommended Setting	Current Setting
/etc/securetty	permissions = 600 owner = root	permissions = 664 owner = root
/etc/utmp	permissions = 644	permissions = 644
/etc/wtmp	permissions = 644	permissions = 664
/etc/motd	permissions = 644	permissions = 666
/etc/mtab	permissions = 644	permissions = 644
/etc/syslog.pid	permissions = 644	permissions = 644
/etc/aliases	permissions = 755 owner = root	permissions = 664 owner = root
/etc/crontab	permissions = 400 owner = root group = root	permissions = 664 owner = root
/var/spool/cron & its subdirectories and files	permissions = 600 owner = root group = root	permissions = 664 owner = root
/etc/cron/*	permissions = 600 owner = root group = root	permissions = 664 owner = root
Log files within /var/log	Should only be writable by root.	Only writable by root
etc, /usr/etc, /bin, /usr/bin, /sbin, /usr/sbin, /tmp and /var/tmp	owner = root	owner = bin
/tmp, /var/tmp	Sticky bit should be set	Sticky bit set

Last Updated: July 24th, 2017

Upcoming Training

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