Global Information Assurance Certification Paper

GIAC Industries

Unix Vulnerability Assessment

February 14, 2001

Review by

Scott Cogan

MYSECCO inc.

Executive Summary

The information presented in this section represents a summary of entire vulnerability assessment. Network and Server security in GIAC Industries can be classified as poor. Immediate action should be taken to remedy the severe security risks discovered during this evaluation of three Unix servers on your network. The primary finding is that no standards, procedures, and policies exist to provide a structured approach to developing a secure technical infrastructure.

Systems Configuration

Systems configuration defines the system services that are initialized and enabled, as well as how they interoperate with the core operating system. Secure systems configuration is required to ensure that authorized and unauthorized users have the necessary restrictions in place to prevent them from accessing unauthorized systems resources. Default configurations of most operating systems are not secure.

A basic concept to remember when configuring "high-value" systems is that less is more, meaning less services equals more security. Fewer services means better security because there are fewer services available to attackers and common users to compromise your security. For example, if you do not require sharing files between servers, do not have NFS running.

The Unix Mail server had numerous recommended Sun Patches that had not been applied. A detailed list of the recommended patches are located in the Technical Vulnerability Analysis portion of this report. These patches should be applied immediately.

Network Design

Secure network design includes developing layers of security that prevent, detect, and trap unauthorized external users from gaining access to internal networks. Typical secure designs implementations separate bastion hosts (Web servers, mail servers, extranet sites, intranet site, external dns, etc.) from the production network in areas known as De-Militarized-Zones (DMZ's). This additional layer between the Internet and your internal networks allow you to provide a necessary level of security. The development/FTP Red Hat 6.2 server was configured to accept traffic from internal networks and the public Internet. This means that only the security measures taken on those machines will prevent external users from accessing internal networks. This violates the fundamental security concept of defense in depth. Based on the current configuration of these dual-homed servers, security could likely be compromised. It is recommended that a more secure architecture be developed to decrease the reliance on current host based security mechanisms.

Advanced network interface configuration (source routing, deny/allow rules, icmp settings) should be done to ensure the appropriate rules are enforced when packets are received or sent from networking interfaces. IP-Forwarding was disabled on most of the

Unix servers. This prevents users from using the server to forward packets on another interface in most cases.

Password Policies

Password policies, in particular, tend to be one of the easiest vulnerabilities to exploit. These policies can define requirements regarding the length, expiration period, and base character set used for individual passwords. Password policies can be developed for network access, remote access, client applications, online applications, and other systems. The following were the predominant password problems on your Unix Servers:

- Minimum password length insufficient – GIACs' passwords were set to 6 character minimums. Passwords should have 8 character minimum length requirements to increase the difficulty of brute force password cracking.
- Password expiration not set – GIACs' passwords did not have specific expiration timeframes set. This means that the same account could be present, with the same password, for the lifetime of the server.
- No automated mechanism to clean out old accounts – GIAC had old accounts that were no longer in use. After an account hasn't been used for several months, it should be deleted. This will prevent accounts that are no longer active from presenting extra security threats to your systems.

Remote Access Authentication

To access machines from remote locations, both telnet and SSH are in use. It is recommended to eliminate the use of telnet since all communications (including passwords) are passed in cleartext from the client, through the network, to the server. Telnet relies on the standard Unix login program for a remote user to access a machine. The login program was not configured to restrict the root account from accessing telnet directly, which means root passwords will be transmitted in the clear. Using su or sudo after logging in through telnet or SSH, is the only way to access the superuser account remotely. A combination of a secure remote access protocol (like SSH), restricting to access to the system with only the "su" command, and implementing TCP Wrappers to require host based (IP address) authentication. SSH has been designed as a secure protocol, however, it is new and has had it's share of recent vulnerabilities. It is imperative that if SSH is used, that security alerts should be carefully monitored.

Auditing

Auditing was enabled inconsistently, or not at all on your Unix servers. Auditing is necessary to ensure that all activities and events that occur on your system are authorized and acceptable. Without proper auditing there is no historical reference material to review important events that take place on your system.
Auditing should be performed to accomplish the following tasks:

- Monitor security-relevant system events
- Record the events in an audit trail
- Detect misuse or unauthorized activity

- Basis for response procedures

Syslog is running, however without regularly scheduled reviews of those logs, the information is useless. Further, many log files are not created, so syslog is unable to write historical events to those files.

File System Security

Many SUID/SGID (set user id, set group id) were discovered on most of your systems. Sinnce these programs are often executed in a root environment, it is paramount that these files never include write permissions for the world (other) and rarely for a group, otherwise, any user could insert foreign code into one of these programs and wait for it to be executed. A list of the SUID/SGID programs that were discovered at the time of our tests can be found in appendix A. For more proactive auditing of SUID/SGID files it is recommended that a file integrity tool (Tripwire, other host-based IDS, etc.) be used to keep track of changes made and alert the superuser when changes occur. All SUID/SGID programs on a system should be kept track of by running regular searches (finds, etc.) to identify all of the SUID/SGID files currently on the system.

Files that can be modified by everyone should be identified and verified on a regular basis to ensure that they do not allow an unauthorized user the opportunity to extend his rights on the system. Decisions should be made regarding the accessibility of these files permissions to all users on your Unix servers. Especially sensitive are program files that can be modified by unprivileged users and are executed by users with greater privileges, such as root. Directories with excessive privileges allow users to copy, and modify files that exist in a directory. If execute permissions are enabled on a directory then users with those permissions can copy, add, overwrite, or delete files that exist in that directory.

Approach

Goals and Objectives

Securing the network and computing resources of any organization is essential. Companies like GAIC Industries hold valuable information and provide essential services to their clients that require them to gather personal information, at the same time providing personal anonymity. The confidentiality and controlled release of this information and the continued and uninterrupted delivery of these services is necessary to preserve credibility and profitability of GAIC Industries. MYSECCO will provide a detailed report regarding the current security posture of your network and its susceptibility to compromise. This information can then be utilized to mitigate vulnerabilities and remedy existing deficiencies in your current infrastructure.

Methodology

MYSECCO developed a tailored security test and evaluation plan in order to identify the vulnerability of GAIC Industries' network infrastructure to internal and external attacks. MYSECCOs' approach to evaluating GAIC Industries' business-operating environment includes reviewing your Unix environment and the host-based security measures implemented. MYSECCO will identify basic network design, server configuration, and internetworking device vulnerabilities. MYSECCO methodology includes analysis of the following areas.

- Network Security Scan and Network Design Evaluation
- Server Review

Network Security Scan

After gaining a detailed understanding of the logical design of the network through a network discovery activity, network-based scans will be used to detect common vulnerabilities. These scans provide a better understanding of the security of your network, systems, and applications. The scans will include a Red Hat 6.2 server, Solaris 2.7 Mail Server, and FreeBSD firewall. The results of the scans will assist us in addressing the major security issues in your environment.

Server Review

The server level assessment includes operating systems-level tests on the three machines identified in the scope section of this document. Our tests are designed to identify vulnerabilities present in the specific operating system. Detailed host system reviews are performed using agent-based scans and/or proprietary manual checks to provide analysis of vulnerabilities found on system hosts. Vulnerabilities at this level will include identification of improper permissions/rights on systems' objects, services allowing unnecessary functionality to unauthorized users, unnecessary services, basic hardness tests, old versions of patches, and other potential anomalies. After the testing has been performed, we will carefully analyze the results and develop recommendations to improve your security infrastructure for both the short and long term protection of your network.

Scope

GAIC Industries has requested that the following network and system assets, located in the be included in this Vulnerability Assessment:

- 1 FreeBSD Server (acting as a firewall)
- 1 Solaris 7 Mail Server
- 1 Red Hat 6.2 FTP Server

The scope of this vulnerability assessment will cover administrative, operating system configuration, file system security, remote access, network service, network design, auditing, and password related vulnerabilities.

Administrative Vulnerability Analysis

Standards

Detailed standards for configuring servers did not exist. It is important to develop a standard build of an operating system (FreeBSD, Solaris, Red Hat, etc.), configured to perform a specific purpose (ipfiltering, routing, Mail, FTP, DNS, etc.). That standard should have accompanying documentation, and an image of the OS. The documentation should describe the hardware, software, and services that are installed, running, and how they are configured. The standards documentation should discuss the security controls that have been implemented to protect this server. The image of the OS should be saved as a baseline build of the specific server configuration.

Policies

Only one security-related policy existed, and the entire systems administration staff did not know about it. Not only did most policies not exist, but GIAC employees did not know about them. This indicates the need for creation of new, more relevant policies, and a security awareness strategy. A Policy is a high-level statement of objectives, beliefs, and goals within a specific subject area. A high-level security policy should be defined to capture your corporations approach to security (kind of like a security mission statement). Lower level security policies should include: Internet Usage Policy, Employee Hiring Policy, Firewall Policy, and Separation of Responsibilities Policy.

Procedures

Documented procedures did not exist in any shape or form. This is a bad idea, since it means that if the individuals currently tasked with these operation left the company, you would be without any and all procedures that individual was responsible for. Procedure define the specific steps of how the policy and supporting standards and how guidelines will be implemented. A procedure is a description of tasks that must be executed in a specific order. Basic procedures that should be developed for GIAC Industries include: Account Creation/Deletion, employee assimilation, backup and recovery, and adding devices/servers to networking environment.

Technical Vulnerabilities

The findings contained in this section include information gathered from running commercial and freeware network-based vulnerability scanners as well as manual checks. Implementing these recommendations that go along with these findings will go along way to improving the security infrastructure of your organization.

Boot Password Missing - If the server gets rebooted this password prevents the machine from finishing the boot process before the firmware password is entered. Set eeprom value to full for the Sun Solaris Machine. For the FreeBSD machine, set console value to "insecure" in the /etc/ttys file.

Development Server in Public Address Space (Red Hat) – The Red Hat 6.2 server is being used for both FTP and developing internal applications. Exposing a machine built to support development and exposing it to external traffic. Immediate weak link in your security perimeter. Since the configuration of the machine is ever changing, it is difficult to secure the machine at any point in time. This can pose a risk to the integrity of the client applications that you are developing for future use, as well as the file-sharing capabilities you are already providing your client. Move all development boxes to a private address space, protected from external traffic. Dedicate a "hardened" machine for client file-transfer.

Patch-levels – The Solaris mail server was missing the following patches:

Patches Missing from Solaris Mail Server
106793-05 SunOS 5.7: ufsdump and ufsrestore patch
106934-03 CDE 1.3: libDtSvc Patch
106938-04 SunOS 5.7: libresolv patch
107018-02 SunOS 5.7: /usr/sbin/in.named patch
107259-01 SunOS 5.7: /usr/sbin/vold patch
107451-05 SunOS 5.7: /usr/sbin/cron patch
107454-05 SunOS 5.7: /usr/bin/ftp patch
107456-01 SunOS 5.7: /etc/nsswitch.dns patch
107477-03 SunOS 5.7: /usr/lib/nfs/mountd patch
107587-01 SunOS 5.7: /usr/lib/acct/lastlogin patch
107684-01 SunOS 5.7: Sendmail patch
107709-07 SunOS 5.7: libssasnmp/libssagent/snmpdx/mibiisa patch
107972-01 SunOS 5.7: /usr/sbin/static/rcp patch
108301-02 SunOS 5.7: /usr/sbin/in.tftpd patch
108327-01 SunOS 5.7: /usr/bin/cu patch
108662-01 SunOS 5.7: Patch for sadmind
108721-02 SunOS 5.7: admintool patch
108748-01 SunOS 5.7: /usr/lib/nfs/statd patch
108760-01 SunOS 5.7: /usr/sbin/rpcbind patch
108762-01 SunOS 5.7: /usr/sbin/rpc.nisd_resolv patch

109253-01 SunOS 5.7: /usr/bin/mail patch
109404-01 SunOS 5.7: /usr/vmsys/bin/chkperm patch
109709-01 SunOS 5.7: /usr/sbin/arp patch
109744-01 SunOS 5.7: /usr/lib/nfs/nfsd patch
109949-01 SunOS 5.7: jserver buffer overflow

This finding indicates that the regular application of patches to this server is not a procedure that is followed by your current systems administrator. Consistently applying the recommended patches recommended by your vendor allows you to keep your production operating systems free of most known vulnerabilities (except for configuration vulnerabilities). Stay up to date with patches as they come out.

Multi-Homed Machine (external/internal) – The Red Hat server had two network interface cards, connecting itself directly to the internal network from the Being exposed to the Internet makes it vulnerable to many different attacks, introducing another risk to your internal network. The only barrier between your internal network and the Internet is security implemented on the host. Provide more separation between your Internet presence and your local area network.

Excess Boot Scripts Enabled - If the server gets rebooted, then the boot scripts in these directories will spawn these services even if they are not currently active. This can provide a window of opportunity to a lurking hacker. Rename or Remove all startup scripts that are not necessary for operations in your production. This vulnerability was present in all three Unix machines.

Sendmail Enabled - Sendmail has had numerous security vulnerabilities that have allowed dangerous compromises for years. Race conditions, buffer-overflows, and poor spam resistance are common problems. Disable and remove sendmail if it is not required (on FreeBSD firewall, and Red Hat ftp server). If it is required (for your Solaris Mail Server), make sure the most recent version is running, and all necessary patches have been applied.

SMTP supports EHLO - Extended HELO (EHLO) provides extra information to attackers about sendmail configurations on your Solaris Mail Server. If this feature is not being used, disable it.

Identd Exists - An identd response was detected, indicating that this exploit was attempted and the identd daemon was detected. Upgrade sendmail version on the Solaris Mail Server.

NFS Enabled - NFS is an RPC based service that typically uses weak authentication to communicate between client and server. The NFS server running on the Solaris mail server is currently using only weak authentication based on the UID of the requestor (AUTH_UNIX). Poor configuration problems can lead to many security vulnerabilities. Disable NFS if it is not necessary for operations. Where it is necessary, verify configuration.

Mountable Network File System (NFS) - NFS was found to be mountable. The security of NFS relies heavily upon who is allowed to mount the files that a server exports, and whether or not they are exported read-only. The /etc/vfstab file in the Solaris server had an entry that was exporting the root directory (eg., /) to everybody, with read write permissions.

NFS Writeable - An NFS export on the Solaris Mail Server was found to be writable by anyone. An attacker could modify any files located in exported directories. If this feature is not being used, disable it. If you require NFS ensure that it is configured properly. If this being used for backup purposes, make sure that only those machines that are backing up have write access.

NFS exports outside domain – The Solaris Mail Server is exporting file systems to a domain not within the GIAC Industries. Exported file systems pose a serious security concern and should be considered carefully. Do not allow machines to export file systems outside of their own domain. This vulnerability should be addressed immediately.

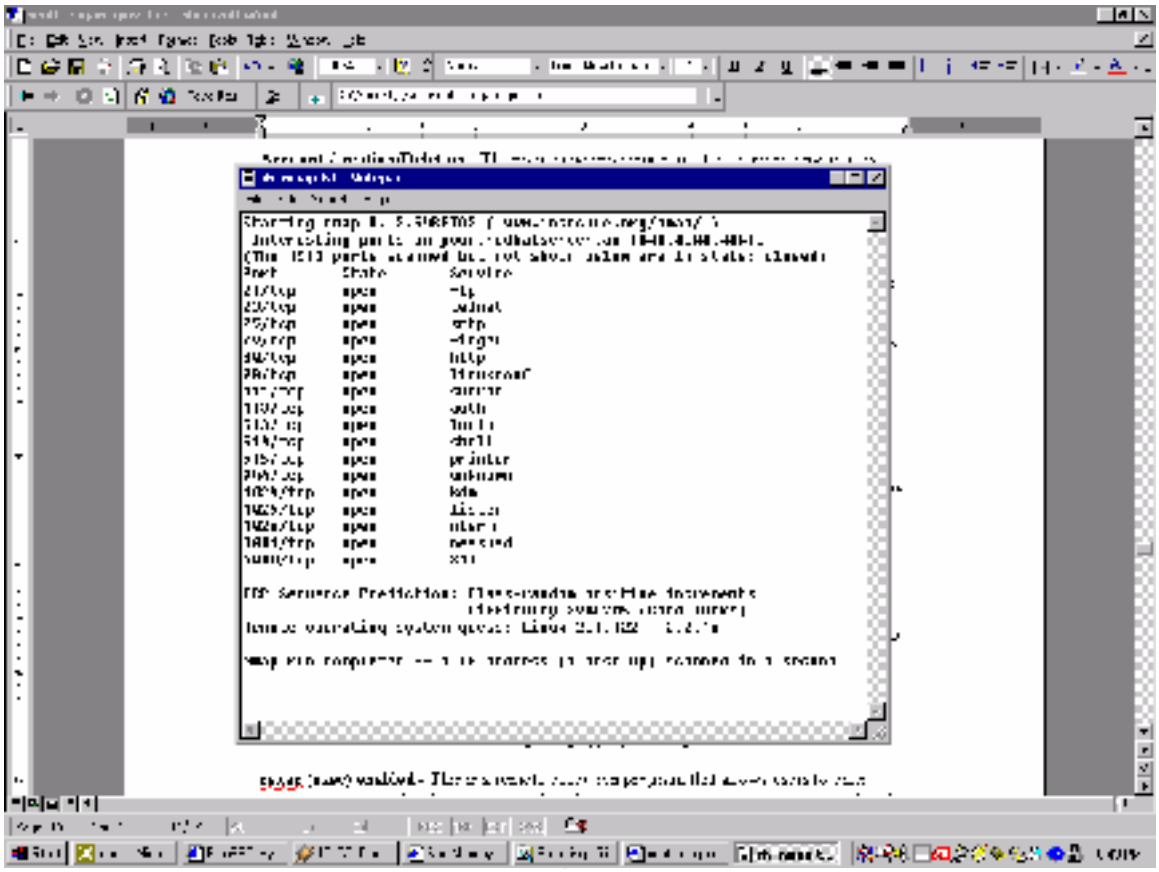
NFS Mountd, File exists (information gathering) - This exploit can be used to determine what files exist on the Solaris Mail Server running a vulnerable version of the RPC mountd service. Upgrade your system's rpc.mountd daemon to a newer version.

NFS mount daemon operating on an unreserved port - The mountd daemon is running over a non-reserved port on the Solaris Mail Server. This daemon may vulnerable to port hijacking and should be moved to a reserved port. Move mount daemon to a reserved port number

Network Interface Configuration – The FreeBSD server has does not make all of the appropriate NIC configurations. Any interface that is connected to the Internet, network interfaces should be configured to properly deny/permit, and route packets to and from internal addresses. It is important to include the right declarations and assign the proper networking parameters in this script to each interface to ensure that that icmp redirecting is disabled, ipforwarding is disabled, source routing is not permitted, and arp cache flushing occurs frequently enough to protect against spoofing attempts. If the Red Hat machine continues to have both internally and externally facing NIC's, then detailed filtering rules should be developed to ensure unwanted traffic is not handled in manner that could compromise your organizations security.

IP-Forwarding enabled - IP-Forwarding allows traffic inbound from one interface, be forwarded to traffic from another interface. Can be used to relay traffic into internal private networks. IP forwarding should be disabled

Excess Processes Active (External discovery) - Many processes were discovered active on the Red Hat 6.2 server during a port scan using Nmap. Here is the output:



Regularly verify the need for every active process on your servers.

Excess Services enabled under Super Server (inetd) - Too many services were found enabled in /etc/inetd.conf file on both the Red Hat and the Solaris Server. The super-server starts too many unnecessary services when it is started. It is recommended that all services be evaluated to determine whether they provide a necessary function for the server. If they are not absolutely required, they should be disabled by including a pound sign (#) in front those lines in the /etc/inetd.conf file. Each service can potentially provide a unique entrance into your server.

rsh (shell) enabled – This service allows a user to remotely execute a command to the rshd server, after weak host authentication. Disable this program. Deny users from remotely execution of commands without completing appropriate login. This service was enabled on both the Solaris Mail server and the Red Hat ftp server.

rexec (exec) enabled - This is a remote execution program that allows users to enter username, password and command without logging in. rexec passwords are passed in the clear in the same manner as telnet. Disable this program. Deny users from remotely execution of commands without completing appropriate login. This service was enabled on both the Solaris Mail server and the Red Hat ftp server.

rexec default account - An accessible default account was detected through rexec on the Red Hat server. Default accounts allow attackers easy access to remote systems. Disable the rexec account or change the password to something difficult to guess. Disable login access to this Unix account in the /etc/passwd file if it is not needed.

rsh default account accessible - Examine the .rhosts file, which contains configuration information for trusted hosts. Any entries containing a + (plus sign) should be removed or commented out. This account was enumerated on both the Solaris Mail server and the Red Hat ftp server.

rhosts Still Enabled - rhosts allow weak authentiction across the network. Removing the appropriate lines in /etc/pam.conf file on your Solaris server can keep users from using the r-utilities for remote access. SSH can fully replace the functionality of these tools and is the recommended substitute, based on the enhanced security that it provides through stronger authentication and encryption.

rstat service enabled - The rstat daemon gives an attacker information about the host, including when the machine was last booted, how much CPU it is using, how many disks it has, and how many packets have reached it. rusers also provides information about some of the users on the system. Unnecessary service unless NIS is being used. Disable it in /etc/inetd.conf. This service was enabled on both the Solaris Mail server and the Red Hat ftp server.

Telnet enabled - All data traffic in telnet transmission passes in cleartext across the network, including passwords. Disable telnet, and use more secure terminal applications such as SSH.

Telnet default account accessible - An accessible default account was detected through Telnet. Default accounts through Telnet allow attackers easy access to remote systems. Disable login access to this Unix account if it is not needed.

Wu-ftpd message file allows attackers to execute code as root - Wu-ftpd macro variables in the message file allow local or remote attackers to overwrite the stack in the FTP daemon and execute code as root. This is caused by improper bounds checking during the expansion of macro variables in the message file. Upgrade to the latest wu-ftpd version. This vulnerability was discovered on the Red Hat FTP server.

FTP Default Account(s) - Accessible default accounts were detected on your Red Hat FTP server. Default accounts through FTP allow attackers easy access to remote systems. Disable the open account or change the password to something difficult to guess. Disable login access to this Unix account if it is not needed.

Wu-ftpd "SITE NEWER" denial of service - Wu-ftpd "SITE NEWER" command consumes excessive amounts of memory that could lead to a denial of service attack. The "SITE NEWER" command is a feature specific to wu-ftpd designed to allow mirroring

software to identify all files newer than a supplied date. Upgrade to wu-ftpd version on the Red Hat server.

FTP bounce attack, proxy connections – The Port command vulnerability exists in the FTP implementation running on your Red Hat FTP server. An attacker could potentially use this command to connect to sites through the vulnerable host, effectively "bouncing" such connections. Upgrade ftp version.

Finger service running - The finger service or daemon was detected as running. Finger gives an attacker login account and trusted host information on the server it is running on. Disable finger or set a shell script to run in its place that will print contact information for the site. This service was enabled on both the Solaris Mail server and the Red Hat FTP server.

RIP tables modified - The Solaris Mail server is vulnerable to false routing table information. RIP is a commonly used method for a local network to share routing information. Since these are development machines, set a default route to the gateway and disable routed.

Routed service active - This service provides an attacker your routing information. Routed accepts routing information from anyone, so it increases the possibility that an attacker can send false RIP packets, causing your data to be routed to the attacker's machine. Disable routed on the Solaris Mail server and the Red Hat ftp server.

UUCP Active - UUCP was found active on the Solaris Mail server and the Red Hat ftp server. This may pose a security risk due to well-known vulnerabilities, and should only be run if required at your site. Disable uucp by commenting out the uucp line in inetd.conf. Kill the inetd process and then restart it.

FTP home directory bug - The FTP daemon running on the Solaris Mail server revealed the true path to the FTP user's home directory by issuing a quote CWD command. This information-gathering probe may give an attacker clues as to the basic structure of the victim's file system. Refer to the Wu-FTP documentation to determine how to disable the CWD command.

BIND Query Feature enabled - BIND servers support the ability to be remotely queried for their version numbers. This feature could be used by an attacker to remotely query computers for vulnerable versions of BIND. Based on recent vulnerabilities discovered in BIND, this is a significant finding. Disable remote query feature, after you have installed the latest version of BIND on your Solaris Mail server. Give careful consideration to implementing split-horizon DNS, to improve your organizations resilience to DNS-based attacks.

SNMP Enabled - The SNMP default Public community name is specified on the Solaris and Red Hat server, allowing anyone the ability to receive responses to queries from the system if they use this default value. An attacker can use SNMP to obtain valuable

information about the machine, such as information on network devices and current open connections. Disable SNMP if you are not using it for network management. Ensure that SNMP public and private community strings are protected properly if it is necessary.

Excess Packages installed - Core System Support was not chosen as the base installation package for the Solaris Mail server. Using other standard installation packages will add packages for developers, Xwindows, and other functions are unnecessary for bastion hosts. Start with the base installation (Choose "Core System Support"), then only install specific packages that you will require for your production machine.

Password Length - The minimum password length for accounts set on all Unix servers were 4 characters. Change password lengths to at least 8 characters

Password Expiration - Password expiration is not set, or enforced on any Unix server. Passwords should expire at least every three months.

Excess Accounts - A large number of accounts were discovered on the Red Hat server. These accounts are difficult to manage and maintain, making it difficult to control the level of access for each user, expiration timeframes, and other account attributes. Limit the number of accounts on your servers.

Shells - Users are provided default shells in the /etc/passwd file without any restrictions. Provide users a restricted shell that does not include as much operating system functionality and/or usage conditions (time, day, etc). This vulnerability was discovered on all servers.

File System Permissions - Incorrect file permissions for /var/adm/vold.log, /var/adm/spellhist, /var/saf/_log, /var/dmi/db/1l.comp, /var/dmi/db/1l.tbl, /var/snmp/snmpdx.st, /var/snmp/snmpdx.st.old were Discovered on the Solaris Mail server. Change the mode of these files to prevent execution.

Syslog not Running - Syslog is the basic logging daemon used for auditing. Syslog was not running on the Red Hat ftp server.

Root owned executable files with improper permissions – During our tests, several files owned by root were discovered with group and other write permissions. There should never be files listed indicating that there are world/group writeable root owned files. Change the mode of these files to prevent group and other write access (chmod 711 or 700 or 755).

Su - Does not log users to the console or to a log file when they "su" to root. Change the su configuration file to log all uses of su to a console and to a log file.

Admintool Permissions - The admintool permissions allow everybody to make changes to it, making it easy to replace it with a Trojan program. This is an administrative tool that was only found (for good reason) on the Solaris mail server.

Root Logins allowed - Using the standard login program, root can remotely log in exposing their password in clear-text over the network. Restrict root from logging on from a remote location by uncommenting the CONSOLE=/dev/console line in login. Use su or sudo to switch to the root account after you have logged into the box as a regular user. This was permitted on all Unix servers.

Root umask too permissive - Umask restricts the permissions applied to a file by the user that creates it. The default umask for root should not grant permissions to "other." In the shell startup scripts, the umask value was set to "002" on all servers. By default this affords too many privileges to users of the same group.

Modem discovered – A modem was discovered connected to the Solaris machine. The presence of this modem allows anyone to circumvent the perimeter access controls of the FreeBSD firewall. This modem should be disconnected immediately.

High Priority Vulnerability List

The following represents the top ten vulnerabilities that should be fixed as soon as the resources become available.

1. **Development Server in Public Address Space** (Red Hat) – The Red Hat 6.2 server is being used for both FTP and developing internal applications should be immediately disconnected from the network. The recommendation is to use this machine as an internal development server after you have reconstructed it. Build a new, "hardened" machine with a chrooted FTP directory to support your client file transfer requirements.

2. **Patch-levels** – The Solaris mail server should be immediately updated with the patches identified in the Technical Security Vulnerability section of the document.

3. **Modem discovered –** The modem connected to your Solaris mail server should be disconnected immediately.

4. **Root owned executable files with improper permissions –** During our tests, several files owned by root were discovered with group and other write permissions. There should never be files listed indicating that there are world/group writeable root owned files. Change the mode of these files to prevent group and other write access (chmod 711 or 700 or 755).

5. **FTP –** The current version of WU-FTP (2.6.1) has many known vulnerabilities and needs to be updated. Update to the current stable version of WU-FTP. On servers where FTP is not required, disable it.

6. **Telnet –** If you require the continued use of Telnet, ensure TCP wrappers are integrated, and configured properly. Otherwise, it is highly recommended that SSH is implemented and used as the only mechanism for remote access and administration.

7. **Excess Services –** Disable services on all servers that are not being used.

8. **Sendmail –** Upgrade your version of Sendmail to 8.11.2. The current version of Senmail you are using has many known vulnerabilities.

9. **NFS Configuration –** Configure NFS to include UNIX_DES authentication, and restrict access to a narrow subset of servers that require access to these file servers.

10. **Standards, Policies, and Procedures** – Need to be developed to ensure that a controlled and organized approach is taken to support your enterprise security infrastructure.

References

Practical Unix and Internet Security, by Simson Garfinkel & Gene Spafford, Oreilly and Associates.
Unix Power Tools, by Jerry Peek, Tim O'Reilly & Mike Loukides, Oreilly and Associates.
The FreeBSD Handbook, Greg Lehey, Walnut Creek.
www.sans.org
www.sun.com
www.securityfocus.com
And many, many more links that I have forgotten over time ; ^)