Global Information Assurance Certification Paper

GIAC Enterprises
Internal Report on
Security Audit of Unix Host Security
April 3, 2001

By: Paul Parzen
System Administrator

Table of Contents

I. EXECUTIVE SUMMARY

GIAC Enterprises Ltd. (GIAC), an Internet Startup company specializing the in the sale of online fortune cookie sayings, recently undertook a project to audit the security of a segment of their information technology infrastructure. The project team consisted of Paul Parzen, a junior systems administrator, who had recently been on training at the SANS security conference. Due to the company's investment in the training, management requested a security audit of their key webserver, Maverick.

The field work for the audit took place during the week of March 5th through 9th, 2001. This work consisted of running various automated vulnerability scanning tools as well as review of key configuration files within the operating system on Maverick.

The network architecture surrounding Maverick is depicted in Figure 1 on the following page. It consists of a connection to the Internet through a Cisco router, the webserver in the demilitarized zone (DMZ), an intrusion detection system (IDS) and a database server located in the trusted side of the corporate network. The scope of this audit was focused only on Maverick, the key webserver where the corporate information web pages and online ordering system reside. Although some enquiry and discussion surrounding the other component of GIAC's network was performed, this analysis was conducted only to support the audit of Maverick.

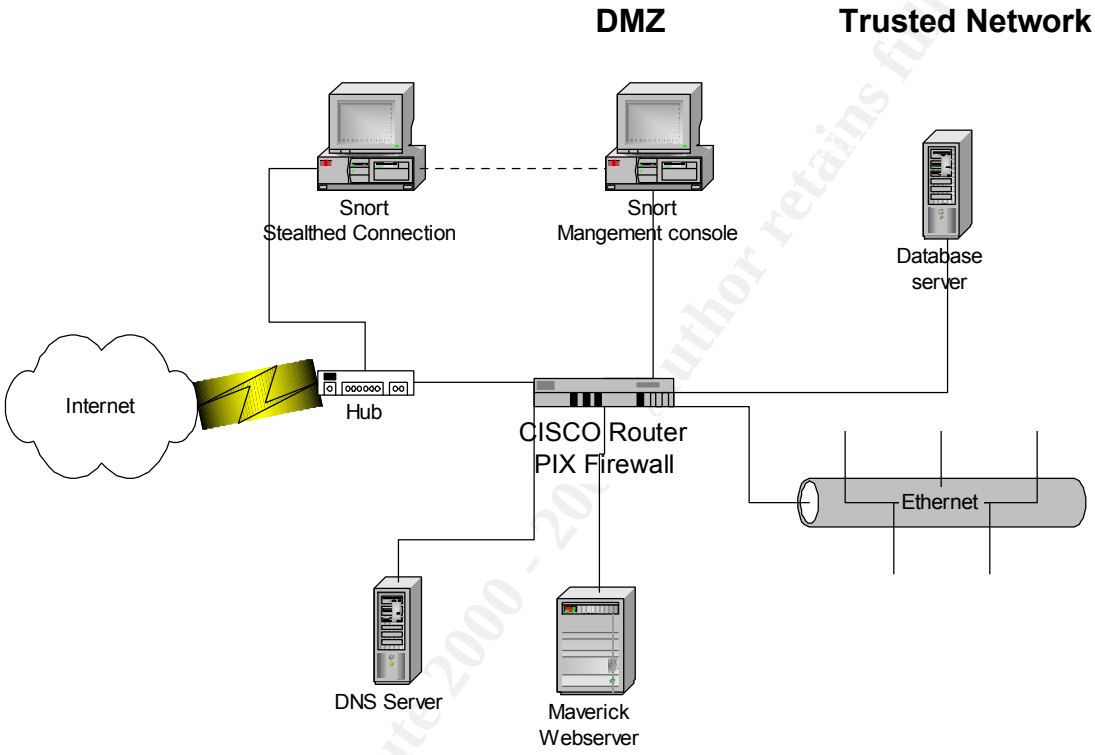
While the results of the audit indicated there were some high risk vulnerabilities in the configuration of the Maverick server that should be immediately addressed, they were not serious enough to recommend taking the server off-line to correct the issues. The criticality of this server to the company's revenue source is too great for any significant down time (see section III, PRIORITIZED SECURITY VULNERABILITIES AND RECOMMENDATIONS). These issues include the application of security patches, turning off unnecessary services, securing the firewall for external RPC traffic and stopping the use of `rlogin` and `rsh` until SSH can be implemented.

There is a back-up and test server which is identical to Maverick in hardware, software and configuration. This back-up server provides the ability for GIAC to recover rapidly from a potential failure of Maverick and provides an environment to test new software and configurations prior to being placed into production. All software implementation and operating system configuration changes recommended in this report should be tested on the back-up server prior to implementation on Maverick.

Although not specifically considered part of the audit, the audit team noted there was a general lack of policies and procedures and strategy for the organization and operation of the information technology (IT) department. This stems largely from the youth of the GIAC organization and many of the issues identified in this report are a direct result of the absence of policies for the IT department to follow. It is recommended that an IT strategy that aligns the IT department with the business strategy be developed in addition to policies and procedures for the organization and operation of the IT department. Included in the security policy should be a data classification model that specifies how

the data is to be protected based on it's criticality and sensitivity. In addition, there should be a description of expectations of employee responsibility for maintaining security. Without a definition of these responsibilities, employees may not be aware of the seriousness of a compromise of the confidentiality of company data.

Figure 1: Simplified Network Diagram:



This diagram provides a simplified view of the architecture within which Maverick operates. It does not show all of the hardware and software which forms the GIAC network.

II. DETAILED FINDINGS

This section of the report provides the detailed analysis of the findings of the audit team. All recommendations are included as part of the analysis. The server reviewed as part of this audit, (Maverick), is a Compaq AlphaServer ES40 running Red Hat Linux 7.0. While version 7.0 is the most recent release of the Red Hat operating system, there have been many published vulnerabilities and related patches to close those vulnerabilities.

1. Operating System Vulnerabilities

A. O/S security patches not applied: As part of the audit, a review of the security patches applied to the operating system was performed (see also section 5, Security Patches Analysis) . Through discussions with the system administrator, it was learned that no patches have been applied since the initial set up of the system. The audit team reviewed the Red Hat Linux Security Advisory (Errata)[1] web site for vulnerabilities in the operating system used.

The results of this review clearly demonstrated several serious vulnerabilities in Red Hat Linux 7.0 that GIAC has not implemented security patches for. These included, but are not limited to, the following:

- Updated VIM packages available (ID RHSA-2001:008-02): "Users could embed malicious VIM control codes in to a file – as soon as any user opened that file in vim-enhanced or vim-X11 with the status line option enabled in .vimrc, the commands would be executed as that user."[2]
- Updated licq packages fixing security problems (ID RHSA-2001:022-03): "licq as shipped with two security problems: An overrrunnable buffer in its logging code, and an unguarded system () call to execute an external browser when receiving an URL."[3]
- New vixie-cron packages available (ID RHSA-2001:0014-03): "A buffer overflow existed in the 'crontab' command; if called by a user with a username longer than 20 characters."[4]

The above list is not intended as a complete list of the security patches that have not been applied to Maverick's operating system. It is intended only to demonstrate three of the forty three (as at March 26, 2001) operating system vulnerabilities that have been identified by the Red Hat Errata team for which patches have been made available at the web site noted in Endnote (i), at the end of this report. Buffer overflow vulnerabilities are serious vulnerability that can provide root access to a successful attacker.[5] These vulnerabilities are high risk and need to be addressed immediately (see also "Security Patch Analysis" below).

All security patches that have not been installed should be reviewed for applicability to services being run on Maverick. If the patches are applicable, they should be installed in a test environment (ideally the mirror image of Maverick) to ensure the patches work and do not cause other applications (i.e. Apache web server) to fail. Once the patches have

been tested, they should be installed on Maverick during off-peak hours to minimize the impact to users (i.e. customers).

2. Configuration Vulnerabilities

In the course of auditing Maverick, several automated vulnerability scanning tools in addition to Unix commands were used to analyze the configuration of the server. These tools included Nmap version 2.53 and Nessus version 1.0.7a. These were installed on a notebook PC and run from unprivileged access to the network segment that contained Maverick. Excerpt from these reports are contained in Appendices A. 2, A. 3 and A. 4 at the end of this report and are specifically referred to from this section. Further, excerpts from key commands and review of files are also contained in the Appendices and are referred to below. Analysis of the operating system was performed in off-peak hours to minimize the impact to the response time from the server.

A. Inittab configuration: At server boot time, the `init` program is responsible for starting all of the normal processes that need to be run. The `inittab` configuration file (see Appendix A.1. for detail) is responsible for determining the process' boot-time and run-time behavior. As currently configured, Maverick allows "Ctrl+Alt+Del" reboots and does not require the root password for single user mode. This means an attacker can cause the server to restart by pressing "Ctrl+Alt+Del" shutting down this critical server (leading to lost revenues) and allows booting up into single user mode without providing a password,[6] giving the attacker root privileges from the console. This risk is mitigated by good physical security over the server (see section 9, Access Restriction, in *E. Physical access* discussed later in this report)

These vulnerabilities are easily fixed by editing the `/etc/inittab` file in the following manner:

- comment out the "`ca`" option to prevent "Ctrl+Alt+Del" shutdowns as follows:
  - `#ca::ctrlaltdel:/sbin/shutdown -t3 -r now`
- add the following command at the end of the "`si`" option:
  - `~~:S:wait:/sbin/sulogin`

B. Unnecessary services running: Through the use of Nmap (see Appendices A. 2 and A. 3), Nessus (see Appendix A. 4) and the `netstat` (see Appendix A.5) command, the audit team determined which services are active on Maverick. Given the function of Maverick as a web server for customers to place orders, the following services are not required:

- ftp (21/tcp): File Transfer Protocol is a standard protocol for transferring files from one system to another as set forth in RFC 0765. This protocol has a long history of security vulnerabilities[7] and new ones are regularly discovered. There is no practical reason for having this service on Maverick as it exposes the server to unnecessary security risks.
- telnet (23/tcp): "Telnet is a service designed to allow you to log onto a remote computer on the Internet… [and provide] a "virtual terminal" on [a] remote

computer."[8] Due to this protocol being a clear text service, there are security exposures with its use. This service provides a convenience to users by allowing them to login to the server remotely. However, given the nature of Maverick, only system administrators should be logging into Maverick to perform their maintenance duties and this can be accomplished through more secure means (see 7. Data Transmission Analysis, *A. Secure Shell (SSH) implementation*).

- smtp (25 & 587/tcp): The Simple Mail Transfer Protocol is used for transferring electronic mail between computers. Maverick has been set up using Sendmail 8.11.0 for which there are known bugs in the software[9]. Further, there has been a long history of vulnerabilities in the Sendmail software which include forging emails, back doors, dangerous aliases, addressing attacks, buffer overflows and set-UID exploits.[10] Maverick is not a mail server and, due to its location in the DMZ, it should never be required to act as a mail relay. Therefore, this service should be turned off with a `cron` job set up daily to flush out any messages that may occur at this machine.

- finger (79/tcp): Finger reports personal information of users making it available to other people. It is an "nonessential [program that] can expose [the] system to unwanted intelligence-gathering".[11]

- auth (identification protocol) (113/tcp): This protocol provides the ability for the server to know the "real" name of a person initiating a TCP/IP connection.[12] There is no practical reason for this program to be running and should be turned off to avoid potential security problems.

- rlogin & rsh (513 & 514/tcp): The remote login (rlogin) and remote shell server (rsh) provide the ability for users to login and execute commands on the Maverick host from other servers and workstations on the network. If the request comes from a "trusted host" or "trusted user", the receiving computer allows the connection without any form of authentication. The "trusted host" verification relies on IP addresses and is susceptible to IP spoofing attacks.[13] In addition to these vulnerabilities, the communication through the "R" services is in clear text and susceptible to packet sniffing for passwords. Although remote administration is a practical necessity for system administrators, there are better, more secure means of providing this ability (see *Secure Shell (SSH) implementation* in "Data Transmission Analysis", section 7A).

- printer (515/tcp): Although the LPRng program resident in Red Hat 7.0 does not have any know vulnerabilities at this time,[14] there is no need for this service to be running on Maverick. There is no requirement for printing from this server.

The services listed above should be turned off to minimize the risk of a security compromise on Maverick. Although services can be turned on and off through editing of the `/etc/rc.d` hierarchy, this is a tedious and lengthy process in which it is too easy to make configuration errors. A simpler interface is provided through the `netsysv`

program which allows for activating and deactivating services managed by `xinetd` and set-up in the `/etc/rc.d` hierarchy. A good "rule-of-thumb" with respect to services running on a Unix server is if you do not need it, turn it off.

C. RPC service running: Remote Procedure Call is a mechanism to simplify the deployment of networked applications. RPC services have had a history of security vulnerabilities due to weak authentication and trusting of the client side authentication. The Maverick server, however, requires this mechanism to be in place as this server must make calls to the database server located in the trusted network for information related to the sales of fortune cookie sayings.

To mitigate the risks with running RPC on Maverick, the following steps must be taken:

- Maintain the most up to date version of Weitse Venema's `rpcbind` program. At the time of the audit, this was the case, however, GIAC system administrators must maintain vigilance over the currency of the program to ensure any new vulnerabilities are patched.
- Rules must be maintained on the firewall that do not permit external connections to ports 111 tcp and udp and to high-order ports.
- Do not permit source routing of packets and do not allow external connections from internal address.
- The intrusion detection systems located in the DMZ and internal networks should be configured to alert for any RPC traffic that is not between Maverick and the database server.

D. Banners: During the Nessus scan of Maverick (see Appendix A. 4.), several banners were detected which reported information about the programs and versions running on the server. Apache, sendmail, ftp and telnet are all reporting information about the program and versions running. This information does not need to be advertised for any practical network administration reasons and only provides information for attackers to concentrate their efforts to break in.

The banners associated with ftp, telnet and sendmail will be removed by turning the services off (see section 2. Configuration Vulnerabilities, component *B, Unnecessary services running*). The Apache banner which provides information about the version of the application itself, SSL and Perl running should be reconfigured to provide false information to any individual that enquires. This will help ensure the efforts of an attacker will be wasted on researching and utilizing exploits that likely do not exist for the Apache webserver.

3. Risks from Installed Third-Party Software

A. Apache webserver version: Currently, the only actively used third party software installed on Maverick is the Apache webserver being utilized for customers to connect to from the Internet. The version being used is 1.3.12 which is several steps out from the most up to date version which is 1.3.19[15] as at March 28, 2001. Although there does not appear to be any serious vulnerabilities associated with 1.3.12, it is good administrative

practice to ensure you are always up to date on the latest version to minimize exposure to potential vulnerabilities.

B. Apache cgi script review: In an effort to determine if there were common gateway interface (cgi) script vulnerabilities, a website scanning tool, Whisker,[16] was used to find vulnerabilities (see Appendix A.6). The audit team reviewed the pages listed by Whisker and did not discover any easily exploitable script vulnerabilities. GIAC should ensure that future additions to cgi scripts in the website should be thoroughly tested for weaknesses prior to implementation into production. There are many resources available for determining cgi script vulnerabilities and the following web site should be regularly consulted for the latest developments: http://www.w3.org/Security/Faq/wwwsf4.html.

C. OpenSSH version: As reported in the Nessus scan (see Appendix A.4) the version of OpenSSH currently deployed is older than 1.2.32. There have been several serious security vulnerabilities reported with versions of OpenSSH older than s 2.3.0. These include design flaws which allow a malicious attacker to insert packets into the encrypted stream and session key vulnerabilities.[17] All current known vulnerabilities are corrected in the latest version of OpenSSH version 2.5.2 released on March 18, 2001,[18] including the man-in-the middle vulnerability that version 1 is susceptible to. GIAC is not currently using OpenSSH for remote connections to the server and this mitigates the risks with the version being out of date. However, as part of the recommendations in this report, OpenSSH will be deployed for remote connections (see 7. Data Transmission Analysis below) and this issue will need to be resolved prior to using OpenSSH.

4. Administrative Practices

A. Audit logging and review procedures: Audit logging on Maverick was set in the default Red Hat Linux 7.0 configuration. While this does provide sufficient logging, procedures for review and escalation of issues must be implemented (see Administrative Practice, Section F, *Incident response and escalation*). Currently, there is no person or group of people assigned the responsibility for reviewing audit logs for anomalous entries. The risks associated with not monitoring operating system logs are mitigated by the intrusion detection systems in place. However, should an attacker evade the IDS, then the system audit logs will be the last line of defense for detection.

As system administrator resources are scarce at GIAC, we recommend automated tools be employed to warn system administrators to key critical events. Psionic Logcheck, from the Abacus Project (http://www.psionic.com/abacus/) is a freely available tool that monitors system logs and mails security violations on a regular basis. This tool comes pre-configured and can be customized as time and experience determine what types of events should be escalated. This will ensure logs are regularly monitored and key events can be reviewed. Ensure that login failures are reported to the system administrator if they exceed three failures. Detecting login failures will minimize the risk of brute force password guessing attacks.

B. System time for logging: The Network Time Protocol (NTP) allows networked machines to keep their system clocks in synch. It requires little bandwidth and will maintain the accuracy of the clocks very precisely based on secondary NTP servers located on the Internet. Currently, this protocol is not deployed on the GIAC network. Its importance is elevated through the "Central audit logging server" issue following. By having operating system clocks that are internally consistent, the ability to review and compare audit logs on the central logging server to detect inconsistencies will be enhanced. Further, should GIAC be successfully attacked and want to prosecute the perpetrator, having system clocks that are accurate and synchronized will improve the reliability of evidence gathered for court proceedings.

At least one machine should be set up as an NTP server to collect time information from secondary NTP servers on the Internet. This could be the edge router, depending on the current load. All other servers should be set up as NTP peers and synchronize to the NTP server(s). The NTP servers should be synchronizing to three Internet NTP servers to avoid timing attacks (where an attacker feeds false time information to the company's server in an effort to skew machine clocks to perpetrate further attacks). Three time sources are needed to be able to discard on false ticker (source with incorrect time information).

C. Central audit logging server: GIAC does not have a central audit logging (syslog) server to gather logging information from all servers in one central location. Having a syslog server provides many benefits for minimal cost.

The syslog server should be a moderately powered machine (needs minimal CPU speed and RAM) with large capacity disk drives and tape back-up for archiving. This machine will provide for redundancy in the audit logs should any of the other servers in the organization be compromised and have their logs deleted or modified by an attacker. A syslog server can increase the likelihood of detecting multiple system attacks by consolidating the log information in one location for cross host comparisons. To affect this change, the "`@<sysloghost>`" command should be appended to the appropriate lines in the `syslog.conf` file (see Appendix A. 7 for review of `syslog.conf`).

To minimize the risk of this server being compromised by a motivated attacker, the only services running on this machine should be the syslog daemon and SSH to provide secure channels between the various servers. Futher, TCP wrappers, authored by Wietse Venema, should be used to restrict the connections to the syslog server. These connections should be limited to the hosts within the network logging to the server and the system administrators. The firewall should also be configured to not permit any external connections. As a final note, the hosts logging to the syslog server should issue periodic messages or "marks" to record the fact they are still "up". If the marks are no longer received, then there is further evidence of a system compromise.

D. Core files: The Maverick webserver is currently configured to allow core dumps – "these files are the remains of a system process that has aborted unexpectedly and contain debugging information which can be useful in figuring out a why the program died"[19]

(see Appendix A. 8). Core files can contain passwords, file contents, directory path and other sensitive information that could be valuable to an attacker. As Maverick is a production server, there should be no need for core dumps, which are often utilized by developers to debug programs. The only down side to preventing core dumps is for gather data in reconstructing an attack that has occurred. However, this loss of potential information is far outweighed by minimizing the information an attacker might get through being able to read core files.

The current setting for core dump files is 1,000,000 (see bold line in Appendix A. 8). This should be set to 0 to prevent core dump files.

E. Password configuration and policies: At a corporate policy level, there are no policies and procedures to govern and standardize passwords. Reusable password policies are critical to the maintenance of security in any networked environment. The current configuration on Maverick is the default configuration from when the server was installed. The only setting was the requirement for 6 character long passwords.

Standard policies and procedures covering the configuration of passwords should be developed at GIAC. These policies should cover the following in order to maximize security of passwords and the access that goes along with those passwords:

- root passwords should be exactly 8 characters long (the limit of the operating system),
- root passwords should be different for each host,
- root passwords should contain upper and lower case alphabetic characters in addition to special and numeric characters
- root passwords should be changed bi-monthly to minimize the risk of discovery
- due to there being a significant number of hosts requiring root passwords, password sheets should be developed with the following parameters:
    - use 6 point font to make the listing as small as possible (i.e. wallet sized),
    - systems should not be specifically identified, a cryptic descriptor in which the system administrators will be able to understand which host is being referred to should be used, and
    - a simple algorithm, not printed on the password sheet, the system administrators can remember (e.g. change vowels to * and add 3 to any number) to minimize exposure should the sheet fall into the wrong hands,
- all other passwords on the system should be a minimum of 6 characters long (as is the current setting) and include the following settings configured in the `linuxconf` program:
    - minimum 2 non-alphabetic characters,
    - must keep the current password for 7 days,
    - must change password after 90 days, and
    - warn the user 7 days before the expiration of the password,
- bulletins should be regularly distributed to employees regarding the importance of maintaining good password practices; these could be emailed monthly as a reminder.

F. Incident response and escalation: Currently there are no incident response and escalation procedures for responding to attacks against GIAC's networks. Although the company is running Snort as an IDS at the perimeter with the Internet, in the DMZ and within the trusted network, there are no procedures in place to determine the action taken in response to those attacks. The general response from the system administrators is to block the IP addresses of suspected attackers and not report the incident to anyone outside of the IT group. While this will generally stop "script kiddies", it will not stop the determined attacker who can change IP addresses easily. Further, there is a chance that customers could be mistaken for attackers and their business my be blocked at the firewall.

Escalation procedures for suspected attacks should be developed and implemented. The senior management of the company must decide if the appropriate response should be simply block all attacks at the firewall or if some types of attacks, e.g. those of an attack that appears to be more sophisticated, should be monitored and evidence gathered for later prosecution. This should be considered in conjunction with the implementation of a "honey pot" or "man trap". This is a server that is designed with some security weaknesses and "dummy" or false data so that an attacker will be lured to that machine. Once inside of the "honey pot", the attacker can be monitored and evidence gathered regarding the actions they take.

Should an attack on GIAC's network be successful, the company needs appropriate response procedures. In order for the company to have an ability to reconstruct the events that led to the successful penetration and the subsequent damage done to systems, there need to be clear procedures for gathering records as evidence. Even if the company decides not to prosecute the perpetrator, they need this data to be able to recover from the security breach.

Data residing on Unix servers can be very volatile and the order of gathering information on the attack is crucial. Checklists need to be developed to ensure all steps are covered and in the right order. Some of the broad procedures that need to be covered are the following:

- the processes that reside in memory are very volatile and must be recorded first
- perform and record the results of the `netstat -a` and `lsof -ef` commands, being sure to use trusted binaries of those programs instead of the ones on the compromised server as these cannot be trusted,
- do a `dd` and then `tar` back-ups of the affected server as well as the logs on the syslog server
- the results of this documentation should be saved to a removable archive (e.g. tape back-up),
- ensure the custody of the evidence is documented and maintained in the strictest manner, and
- never perform analysis on the original archives of the data, only use copied images.

5. Security Patches Analysis

A. Security and bug patch update process: Through discussions with the systems administrators, the audit team discovered there have been no updates to the operating system packages since initial build of the operating system. As noted in the operating system vulnerabilities section of this report, there are many patches which have not been applied due to a lack of process.

Installing the latest bug and security fixes for the operating system can be accomplished through the `up2date` program (`up2date -h` for the command arguments help file and `up2date -l` for a list of packages available for retrieval). This should be run on a weekly basis to ensure the operating system is appropriately patched. Unfortunately, at the time of this report, there was no AutoRPM program available for the Red Hat Linux 7.0 operating system. This is a program that automates the package update process.

B. Security mailing list subscription: There is no one in the IT group currently receiving emails regarding recent security vulnerabilities. There should be at least two system administrators receiving and keeping current on the latest vulnerabilities that concern the operating systems GIAC runs. The following is a list of web sites to which the administrators can subscribe to get the latest information on security vulnerabilities:

- http://www.cert.org/contact_cert/certmaillist.html
- http://www.sans.org/sansnews
- http://www.securityfocus.com/

6. Sensitive Data Storage Analysis

A. Database server: Maverick is only being used as a web server to run the web based applications for GIAC customers to get information about the company and place orders for online fortunes. The database the web based application gets information from, and writes data to, is located in the trusted corporate network. RPC is being used to make calls to the database.

Although the audit team did not specifically look at the database server, the system administrators noted the operating system was configured in much the same way. Many of the recommendations of this report should be implemented at the database server also (e.g. turn off unnecessary services, install security and bug fix patches, improve password standards, connecting through SSH, etc.). Further, the audit team learned that sensitive, personally identifiable information (e.g. credit card numbers, addresses, names, etc.) was not being encrypted. While this machine is on the trusted side of the network, additional security measures, such as storing this data encrypted, should be implemented. This will provide better compliance with national and international privacy legislation the company must comply with given their customers are not only from North America. Legal counsel should be involved in determining the levels of protection that will be required to comply with privacy legislation.

7. Data Transmission Analysis

A. Secure Shell (SSH) implementation: Although an early version of SSH v1 is installed on Maverick, it is not currently being utilized for secure connections. The current practice of using the `rlogin` and `rsh` commands must be stopped immediately. These commands go over the network in clear text, including any passwords that may be used for connection. Until such time as the current loaded version is upgraded, all "`r`" type connections to Maverick should be stopped. Further to this, connections through X11 should also be stopped until SSH version 2.5.2 is installed and X Windows can be run through SSH. X Window vulnerabilities include Trojan logins, transmission over the network in clear text which easily allows other users to see what the authorized user is doing.

Start doing all "`r`" type commands through the SSH program after version 2.5.2 of OpenSSH is implemented. SSH was intended to replace `rlogin` and `rsh` and allow X11 to tunnel through the network encrypted. Combine SSH with TCP Wrappers to limit where the connection can come from to provide even finer control. Ensure the IgnoreRhosts (in the SSH configuration) is set to disable the use of `.rhosts` or `.shosts` for authentication. The only users that should be logging in to Maverick are the system administrators using their own accounts on the system. For all users on Maverick, consideration should be given to the implementation of RSA SecureID to provide strong authentication. This product works very well with SSH and provides an extra layer of security by constantly changing the user's password every 30 or 60 seconds through the use of password tokens.

B. Upgrade to latest version of SSL: GIAC is using OpenSSL to provide strong authentication and end-to-end encryption for customers placing orders. SSL can provide excellent security for GIAC as well as their customers, however, the current version deployed, 0.9.5a, is a few patches out of date. In order to ensure known vulnerabilities have been patched, the version should be upgraded to 0.9.6.

C. Detection of promiscuous network cards: No procedures are in place to detect packet sniffers that might be installed on the network. The audit team used the `ifconfig` command to ensure the network interface card (NIC) was not in promiscuous mode. Sniffers are programs that place the NIC on a computer into promiscuous mode and copy all the packets that travel on the same network segment as the machine with the sniffer. Sniffers can be used to capture such information as passwords and confidential information flowing over the network.

To ensure sniffers are not installed on Maverick (and other servers in the organization) by an attacker, a `cron` job could be created to look for promiscuous NICs. A `cron` job could be executed daily that would execute the `ifconfig` command with the output piped to find the characters `PROMISC` in the output (through the use of `grep`). If the `PROMISC` parameter is found, an email would be sent to all the system administrators on the system. Another defense against sniffers is to break the network up into segments through the use of switches such that only small areas of the network could be "seen" by

a sniffer running on a network segment. The DMZ would be a logical segment of the network with the location of the database server being another segment separate from the "regular" users of the network.

8. Anti-Virus Software Analysis

A. Anti-virus software: Although Maverick is not used as a file server for Windows systems, there are risks associated with viruses and worms infecting Unix platforms. The 'Lion' and 'Ramen' worms are currently in the "wild" and specifically target Red Hat Linux systems. Although there are security patches available to close the vulnerabilities these worms take advantage of, this demonstrates Unix is not immune to worms due to the operating system being different from Windows. Further, late in March 2001, the first cross platform worm, dubbed 'Winux', was released into the "wild". The need for virus protection on Unix servers is rapidly becoming mandatory.

There are virus protection vendors available for the Linux/Alpha operating systems. One such example is Sophos (see http://www.sophos.com/products/antivirus/savunix.html). The audit team recommends virus protection software be tested and then deployed on all Unix servers at GIAC.

9. Access Restrictions

A. User ID and password review: As part of the audit of Maverick, the `/etc/passwd` and `/etc/shadow` files were reviewed (see Appendix A. 9) for unusual users and the John the Ripper password cracking program (available at http://www.openwall.com/john/) was run against the `shadow` password file. The audit team noted two user ID's from Bob Widdowson, a terminated employee, who was a systems administrator until recently. Further, Bob was part of the user group "wheel" which has root privileges and the passwords that were used for these accounts was easily cracked by the John the Ripper program (details of report not included for security reasons). All other passwords used on Maverick were not cracked by John the Ripper using a dictionary based attack.

Although it is most likely that Bob Widdowson was not intending to perpetrate any attacks on GIAC, the accounts should be disabled by changing the password field in the `/etc/shadow` for both bwiddowson and bwiddowson1 user IDs to "`==NP==`". This will ensure the account is no longer accessible. Further, the system administrators should ensure the Psionic Logcheck program specifically warns for attempt to access these user IDs. If someone does try to access these user IDs, it might indicate Bob is trying his old accounts. Lastly, procedures should be put in place to regularly review all user IDs to ensure they are current employees and lock down the accounts of employees that have been terminated. Regular usage of password cracking programs, like John the Ripper, should be performed and easily guessable passwords should be changed.

B. Set UID and Set GID files: The audit team performed a search for files with the SUID or SGID bit set on them and owned by root (see Appendix A. 10). These files allow other users to execute the files as though they were the owner. We noted there are

many files that are SUID and SGID owned by root that are not required for the operation of the system. These were mostly games files.

Unnecessary SUID and SGID files should be deleted and periodic checks of these files, using the command in the appendix, to ensure minimum SUID and SGID files owned by root should be performed.

C. Unowned and world-writable files: A search for unowned and world-writable files was performed (see Appendices A. 11 and A. 12). No unowned files were discovered, however, several world-writable files were discovered. These files are required by the operating system and no compromised world-writable files were discovered. Periodic reviews should be continued by the system administrators for unowned and world-writable files and remove as necessary.

D. Root login: Currently, the system administrators are using the `su` command to login as root to Maverick. While this is better than directly logging in as root, a better solution to control root is the `sudo` program (available from http://www.courtesan.com/sudo). The most current version is 1.6.3p7, released on March 2, 2001.

The `sudo` program provides for more granular control over the abilities of users needing root access. Furthermore, it provides the ability to track the actions of users performing superuser commands. This risk is mitigated by the fact that only system administrators are logging in directly to Maverick to perform system maintenance.

E. Physical access: The physical security of the Maverick webserver and other servers is of critical importance. Due to the design of the Unix operating system, physical access equates to root access. An attacker can crash the machine repeatedly by cycling the power on and off or plugging and unplugging the keyboard repeatedly. Eventually, the root file system will become corrupted and need manual intervention. This is when the system will come up in a root shell. At this time, the attacker has root access.[20]

The audit team found the physical security of the computer operations center at GIAC to be adequate. All servers and consoles are in a separate room with magnetic card swipe (token based) access. Logs are produced and reviewed by IT management for all personnel accessing the computer room. Walls for the room extend from floor to floor to ensure no access through the false ceiling. The floor is raised inside the operations center and temperature and humidity are controlled with warning systems should the environment fall outside the acceptable parameters. Fire suppression system consists of pressurized inert gas with dead-man switch easily accessible on the wall. There is an analog phone beside the dead-man switch for emergency purposes. No network cabling was detected in easily accessible areas.

10. Back-Up and Recovery Procedures

A. Back-up and recovery procedures: Back-up procedures for Maverick and other servers consists of nightly incremental back-ups and weekly full back-ups. A copy of the weekly full back-up is stored off site at a third party vault. Monthly copies are maintained off site and annual back-ups are maintained for 7 years at the vault. Although the back-up procedures are adequate, restoration of data from back-ups has not been tested beyond recovering a few files occasionally. The value of back-ups cannot be verified unless they are tested for recovery.

On a quarterly basis, full recovery from back-up tapes should be performed to ensure they are recoverable.

11. Other

A. Hardware and software inventory: An up-to-date inventory of all computer equipment (including hardware and software) is maintained. This ensures the company knows what hardware they have on any given date, will be able to verify the theft of any equipment and helps the company ensure licenses for software are adequate. These procedures should be continued.

III. PRIORITIZED SECURITY VULNERABILITIES & RECOMMENDATIONS

The following matrix provides a prioritized list of vulnerabilities and issues in the order they should be addressed considering risk and interdependencies. Included in the listing are the summary recommendations to correct the vulnerabilities and issues and an approximation of the hours required by system administrators to correct the deficiencies. Hardware and proprietary software costs were not included as these are specification dependent. The detail for executing the recommendations is included in the detailed findings section of this report with each of the specific vulnerabilities.

Those recommendations with 0 hours in the column are already implemented and need only to be maintained.

#	Vulnerability or Issue	Risk	Recommendation	Approx. hours to correct
1	O/S security patches not applied (1.A.)	High	Apply all security patches which have not been installed. Prior to installing patches, use "test" environment to ensure patches work and will not cause applications to "break".	24
2	Unnecessary services running (2.B.)	High	Deactivate all unnecessary services.	16
3	OpenSSH version (3.C)	Low	Upgrade to version 2.5.2 of OpenSSH. Risk described as low, however, will need to be implemented prior to use.	8
4	Secure Shell (SSH) implementation (7.A)	High	Stop using "`r`" facilities for network logins and use SSH. Consider the use of SecureID for all users connecting to the operating system on Maverick.	24
5	Root login (9.D)	High	Implement `sudo` program for root login and have all system administrators use this for getting root privileges. Ensure only minimum permissions for completing their jobs are granted to each superuser.	32
6	Password configuration and policies (4.E.)	High	Improve configuration of password policies as detailed in report. Develop and implement corporate password policies in accordance with recommendations in body of report.	Policies: 40 Config.: 2
7	User ID and password review (9.A)	High	Lock down accounts for Bob Widdowson and monitor for attempted access. Change password configuration to improve minimum standards. Implement procedures to	8

#	Vulnerability or Issue	Risk	Recommendation	Approx. hours to correct
			regularly review and lock down user ID's that are no longer required by the users.	
8	Security and bug patch update process (5.A.)	High	The up2date program should be run weekly to ensure all security and bug fixes are installed in a timely manner.	8
9	Upgrade to latest version of SSL (7.B)	High	Upgrade to latest version of OpenSSL.	16
10	Back-up and recovery procedures (10.A)	High	Perform quarterly full recovery tests from tape back-up to ensure recoverability.	8
11	RPC service running (2.C)	High	Maintain currency of `rpcbind` program. Ensure firewall blocks external RPC traffic and IDS appropriately configured.	8
12	Anti-virus software (8.A)	Moderate	Test and deploy anti-virus software on all Unix servers.	32
13	Inittab configuration (2.A)	Moderate	Change settings in configuration file to comment out "`ca`" option and add root password requirement for single user mode in "`si`" option.	1
14	Central audit logging server (4.C)	Moderate	Design and implement a central audit logging server and deploy Psionic Logcheck to provide alerting of potential compromises.	56
15	System time for logging (4.B)	Moderate	Deploy NTP to all servers and have two internal servers linked to secondary servers on the Internet.	40
16	Audit logging and review procedures (4.A)	Moderate	Deploy Psionic Logcheck using default rule sets. Adjust rule sets for administrator warnings as experience necessitates.	24
17	Incident response and escalation (4.F)	Moderate	Develop incident response and escalation procedures to be able to adequately respond to attacks. Develop evidence gathering checklists to ensure all appropriate steps are taken in the correct order.	40
18	Database server (6.A)	Moderate	Implement security recommendations from this report on the database server. Consider the need for encryption of personally identifiable customer information contained on the server.	N/A

#	Vulnerability or Issue	Risk	Recommendation	Approx. hours to correct
19	Set UID and Set GID files (9.B)	Moderate	Remove SUID and SGID files owned by root that are unnecessary. Perform regular reviews for these types of files and remove as required.	4
20	Banners (2.D)	Low	Remove the ftp, telnet and smtp/sendmail services from Maverick which will remove the banners. Reconfigure the banner in Apache to provide false information to enquiring users.	16
21	Core files (4.D)	Low	Set `ulimit` parameter for core files to 0.	1
22	Apache webserver version (3.A.)	Low	Update Apache webserver to most current version.	8
23	Detection of promiscuous network cards (7.C.)	Low	Create cron job run daily to detect NICs in promiscuous mode. Segment the network into smaller segments to minimize the traffic on any one segment.	4
24	Apache cgi script review (3.B.)	Low	Ensure all future implementations of cgi scripts to the production environment are first thoroughly tested for vulnerabilities.	0
25	Security mailing list subscription (5.B)	Low	A minimum of two system administrators should subscribe to security mailing lists to ensure they are aware of the latest vulnerabilities to be discovered.	0
26	Unowned and world-writable files (9.C.)	Low	Perform periodic reviews for unowned and world-writable files using the commands in the appendix and remove as necessary.	0
27	Physical access (9.E.)	Low	Maintain current physical security.	0
28	Hardware and software inventory (11.A.)	Low	Maintain current procedures for inventory of hardware and software.	0

IV. APPENDIX A – RESULTS OF ANALYSES AND TOOL EXECUTION

A.1. Results of `inittab` file review:

```
more inittab
#
# inittab       This file describes how the INIT process should set up
#               the system in a certain run-level.
#
# Author:       Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>
#               Modified for RHS Linux by Marc Ewing and Donnie Barnes
#

# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have
networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit

l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6

# Things to run in every runlevel.
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few minutes
# of power left.  Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have powerd installed and your
# UPS connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting
Down"

# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown
Cancelled"


# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
```

```
--More--(84%)
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

A. 2 Results of Nmap TCP port scan:

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Nmap run completed -- 0 IP addresses (0 hosts up) scanned in 0 seconds

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host Maverick appears to be up ... good.
Initiating TCP connect() scan against Maverick
Adding TCP port 113 (state open).
Adding TCP port 515 (state open).
Adding TCP port 21 (state open).
Adding TCP port 1024 (state open).
Adding TCP port 111 (state open).
Adding TCP port 514 (state open).
Adding TCP port 25 (state open).
Adding TCP port 443 (state open).
Adding TCP port 513 (state open).
Adding TCP port 79 (state open).
Adding TCP port 23 (state open).
Adding TCP port 22 (state open).
Adding TCP port 80 (state open).
Adding TCP port 587 (state open).
The TCP connect scan took 5 seconds to scan 65000 ports.
For OSScan assuming that port 21 is open and port 1 is closed and neither are firewalled
Interesting ports on Maverick:
(The 64986 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     open        telnet
25/tcp     open        smtp
79/tcp     open        finger
80/tcp     open        http
111/tcp    open        sunrpc
113/tcp    open        auth
443/tcp    open        https
513/tcp    open        login
```

```
514/tcp    open        shell
515/tcp    open        printer
587/tcp    open        submission
1024/tcp   open        kdm

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=2870162 (Good luck!)

Sequence numbers: 490AB516 490AB516 495CEBE5 495CEBE5 49BCA5C3 49BCA5C3
Remote operating system guess: Linux 2.1.122 - 2.2.14
OS Fingerprint:
TSeq(Class=RI%gcd=1%SI=2BCB92)
T1(Resp=Y%DF=Y%W=7F53%ACK=S++%Flags=AS%Ops=MENNTNW)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=7F53%ACK=S++%Flags=AS%Ops=MENNTNW)
T4(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=C0%IPLEN=164%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)


Nmap run completed -- 1 IP address (1 host up) scanned in 6 seconds
```

A. 3. Results of Nmap UDP port scan:

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Host Maverick appears to be up ... good.
Initiating FIN,NULL, UDP, or Xmas stealth scan against Maverick
The UDP or stealth FIN/NULL/XMAS scan took 12 seconds to scan 65000 ports.
Warning:  No TCP ports found open on this machine, OS detection will be MUCH less reliable
Interesting ports on Maverick:
(The 64996 ports scanned but not shown below are in state: closed)
Port       State       Service
111/udp    open        sunrpc
994/udp    open        unknown
```

```
1024/udp   open        unknown
1025/udp   open        blackjack

Remote OS guesses: Linux 2.0.27 - 2.0.30, Linux 2.0.32-34, Linux 2.0.35-38, Linux 2.1.24 PowerPC, Linux
2.1.76, Linux Kernel 2.1.88, Linux 2.1.91 - 2.1.103, Linux 2.1.122 - 2.2.14, Linux 2.2.12, Linux 2.2.13
SMP, Linux 2.3.12, NetBSD 1.4 / Generic mac68k (Quadra 610)
OS Fingerprint:
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=C0%IPLEN=164%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)


Nmap run completed -- 1 IP address (1 host up) scanned in 12 seconds
```

A. 4. Results of Nessus:

Nessus Scan Report

Number of hosts which were alive during the test : 1
Number of security holes found : 1
Number of security warnings found : 14
Number of security notes found : 24

List of the tested hosts :

- **Maverick (Security holes found)**

Maverick :
List of open ports :

- *ftp (21/tcp) (Security warnings found)*
- *ssh (22/tcp) (Security hole found)*
- *telnet (23/tcp) (Security warnings found)*
- *smtp (25/tcp) (Security warnings found)*
- *finger (79/tcp) (Security warnings found)*
- *www (80/tcp) (Security notes found)*
- *sunrpc (111/tcp) (Security notes found)*
- *auth (113/tcp) (Security warnings found)*
- *https (443/tcp) (Security warnings found)*
- *login (513/tcp) (Security warnings found)*
- *shell (514/tcp) (Security warnings found)*
- *printer (515/tcp) (Security notes found)*
- *unknown (587/tcp) (Security warnings found)*
- *unknown (1024/tcp) (Security notes found)*
- *unknown (1241/tcp) (Security notes found)*
- *X (6000/tcp) (Security notes found)*
- *general/tcp (Security notes found)*
- *general/udp (Security notes found)*
- *unknown (1025/udp) (Security warnings found)*
- *unknown (1024/udp) (Security warnings found)*

[back to the list of ports]

Warning found on port ftp (21/tcp)

The FTP service allows anonymous logins. If you do not want to share data with anyone you do not know, then you should deactivate the anonymous account, since it can only cause troubles. Under most Unix system, doing : echo ftp >>

/etc/ftpusers will correct this.

Risk factor : Low
CVE : CAN-1999-0497

Information found on port ftp (21/tcp)
This service is owned by user root

Information found on port ftp (21/tcp)
Remote FTP server banner : maverick ftp server (version wu-2.6.1(1) wed aug 9 05:54:50 edt 2000) ready.

Vulnerability found on port ssh (22/tcp)

You are running a version of SSH which is older than version 1.2.32, or a version of OpenSSH which is older than 2.3.0.

This version is vulnerable to a flaw which allows an attacker to insert arbitrary commands in a ssh stream.

Solution : Upgrade to version 1.2.32 of SSH which solves this problem, or to version 2.3.0 of OpenSSH

More information: http://www.core-sdi.com/english/ssh/

Risk factor : High

Information found on port ssh (22/tcp)
This service is owned by user root

Information found on port ssh (22/tcp)
Remote SSH version : ssh-1.99-openssh_2.1.1

Warning found on port telnet (23/tcp)
The Telnet service is running. This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the telnet client and the telnet server. This includes logins and passwords.

You should disable this service and use OpenSSH instead. (www.openssh.com)

Solution : Comment out the 'telnet' line in /etc/inetd.conf.

Risk factor : Low
CVE : CAN-1999-0619

Information found on port telnet (23/tcp)

This service is owned by user root

Information found on port telnet (23/tcp)

Remote telnet banner :

Red Hat Linux release 7.0 (Guinness)
Kernel 2.2.16-22 on an alpha

login:

Warning found on port smtp (25/tcp)

The remote SMTP server answers to the EXPN and/or VRFY commands.

The EXPN command can be used to find the delivery adress of mail aliases, or even the full name of the recipients, and the VRFY command may be used to check the validity of an account.

Your mailer should not allow remote users to use any of these commands, because it gives them too much informations.

Solution : if you are using sendmail, add the option
O PrivacyOptions=goaway
in /etc/sendmail.cf.

Risk factor : Low
CVE : CAN-1999-0531

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

Warning found on port smtp (25/tcp)

There is a problem in NTMail3, which allows anyone to use it as a mail relay, provided that the source adress 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 : There are no solution provided by the author of NTMail, so you might want to change mail servers
CVE : CAN-1999-0819

Information found on port smtp (25/tcp)

This service is owned by user root

Information found on port smtp (25/tcp)

Remote SMTP server banner :
localhost.localdomain ESMTP Sendmail 8.11.0/8.11.0
Fri, 9 Mar 2001 16:39:47 -0500
214-2.0.0 This is sendmail version 8.11.0214-2.0.0 Topics:
214-2.0.0 HELO EHLO MAIL RCPT DATA
214-2.0.0 RSET NOOP QUIT HELP VRFY
214-2.0.0 EXPN VERB ETRN DSN AUTH
214-2.0.0 STARTTLS
214-2.0.0 For more info use "HELP <topic>".
214-2.0.0 To report bugs in the implementation send email to
214-2.0.0 sendmail-bugs@sendmail.org.
214-2.0.0 For local information send email to Postmaster at your site.
214 2.0.0 End of HELP info

Warning found on port finger (79/tcp)

The 'finger' service provides useful informations to crackers, since it allow them to gain usernames, check if a machine is being used, and so on...

Risk factor : Low.

Solution : comment out the 'finger' line in /etc/inetd.conf
CVE : CVE-1999-0612

Information found on port finger (79/tcp)

This service is owned by user root

Appendix A
Results of Analyses and Tool Execution

Information found on port www (80/tcp)

This service is owned by user apache

Information found on port www (80/tcp)

The remote web server type is :
Apache/1.3.12 (Unix) (Red Hat/Linux) mod_ssl/2.6.6 OpenSSL/0.9.5a mod_perl/1.24

We recommend that you configure your web server to return bogus versions, so that it makes the cracker job more difficult

Information found on port sunrpc (111/tcp)

This service is owned by user rpc

Warning found on port auth (113/tcp)

The 'ident' service provides sensitives informations to the intruders : it mainly says which accounts are running which services. This helps attackers to focus on valuable services [those owned by root]. If you don't use this service, disable it.

Risk factor : Low.

Solution : comment out the 'auth' line in /etc/inetd.conf
CVE : CAN-1999-0629

Information found on port auth (113/tcp)

This service is owned by user nobody

Warning found on port https (443/tcp)

a web server is running on this port

Information found on port https (443/tcp)

This service is owned by user apache

Information found on port https (443/tcp)

The remote web server type is :
Apache/1.3.12 (Unix) (Red Hat/Linux) mod_ssl/2.6.6 OpenSSL/0.9.5a mod_perl/1.24

We recommend that you configure your web server to return bogus versions, so that it makes the cracker job more difficult

Warning found on port login (513/tcp)

The rlogin service is running. This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the rlogin client

and the rlogin server. This includes logins and passwords.

You should disable this service and use openssh instead (www.openssh.com)

Solution : Comment out the 'rlogin' line in /etc/inetd.conf.

Risk factor : Low
CVE : CAN-1999-0651

Information found on port login (513/tcp)
This service is owned by user root

Warning found on port shell (514/tcp)
The rsh service is running. This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the rsh client and the rsh server. This includes logins and passwords.

You should disable this service and use ssh instead.

Solution : Comment out the 'rsh' line in /etc/inetd.conf.

Risk factor : Low
CVE : CAN-1999-0651

Information found on port shell (514/tcp)
This service is owned by user root

Information found on port printer (515/tcp)
This service is owned by user lp

Warning found on port unknown (587/tcp)
a SMTP server is running on this port. Here is its banner :
220 localhost.localdomain esmtp sendmail 8.11.0/8.11.0 fri, 9 mar 2001 16:37:52 -0500

Warning found on port unknown (587/tcp)
There is a problem in NTMail3, which allows anyone to use it as a mail relay, provided that the source adress 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 : There are no solution provided by the author of NTMail, so you might want to change mail servers
CVE : CAN-1999-0819

Appendix A
Results of Analyses and Tool Execution

Information found on port unknown (587/tcp)

This service is owned by user root

Information found on port unknown (587/tcp)

Remote SMTP server banner :
localhost.localdomain ESMTP Sendmail 8.11.0/8.11.0 Fri, 9 Mar 2001 16:39:48 -0500
214-2.0.0 This is sendmail version 8.11.0214-2.0.0 Topics:
214-2.0.0 HELO EHLO MAIL RCPT DATA
214-2.0.0 RSET NOOP QUIT HELP VRFY
214-2.0.0 EXPN VERB ETRN DSN AUTH
214-2.0.0 STARTTLS
214-2.0.0 For more info use "HELP <topic>".
214-2.0.0 To report bugs in the implementation send email to
214-2.0.0 sendmail-bugs@sendmail.org.
214-2.0.0 For local information send email to Postmaster at your site.
214 2.0.0 End of HELP info

Information found on port unknown (1024/tcp)

This service is owned by user rpcuser

Information found on port unknown (1241/tcp)

This service is owned by user root

Information found on port X (6000/tcp)

This service is owned by user root

Information found on port general/tcp

Nmap found that this host is running Linux 2.1.122 - 2.2.14

Warning found on port unknown (1025/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 HOLE REGARDING THIS PROGRAM HAVE BEEN TESTED, SO THIS MIGHT BE A FALSE POSITIVE *

We suggest you to disable this service.

Risk factor : High
CVE : CVE-1999-0018

Warning found on port unknown (1024/udp)

The nlockmgr RPC service is running. If you do not use this service, then disable it as it may become a security threat in the future, if a vulnerability is discovered.

Risk factor : Low
CVE : CAN-2000-0508

This file was generated by Nessus, the open-sourced security scanner.

A. 5. Result of `netstat` command:

```
netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        1      0 Maverick:1089          xxxx.xxx.net:www        CLOSE_WAIT
tcp        1      0 Maverick:1088          xxxx.xxx.net:www        CLOSE_WAIT
tcp        1      0 Maverick:1087          xxxx.xxx.net:www        CLOSE_WAIT
tcp        0      0 *:X                    *:*                     LISTEN
tcp        0      0 *:www                  *:*                     LISTEN
tcp        0      0 *:https                *:*                     LISTEN
tcp        0      0 *:587                  *:*                     LISTEN
tcp        0      0 *:smtp                 *:*                     LISTEN
tcp        0      0 *:printer              *:*                     LISTEN
tcp        0      0 *:ssh                  *:*                     LISTEN
tcp        0      0 *:login                *:*                     LISTEN
tcp        0      0 *:shell                *:*                     LISTEN
tcp        0      0 *:telnet               *:*                     LISTEN
tcp        0      0 *:ftp                  *:*                     LISTEN
tcp        0      0 *:finger               *:*                     LISTEN
tcp        0      0 *:auth                 *:*                     LISTEN
tcp        0      0 *:1024                 *:*                     LISTEN
tcp        0      0 *:sunrpc               *:*                     LISTEN
udp        0      0 *:1025                 *:*
udp        0      0 *:996                  *:*
udp        0      0 *:1024                 *:*
udp        0      0 *:sunrpc               *:*
raw        0      0 *:icmp                 *:*                     7
raw        0      0 *:tcp                  *:*                     7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  1      [ ]         STREAM     CONNECTED     1468   @000000bb
unix  1      [ ]         STREAM     CONNECTED     1088   @00000091
unix  1      [ ]         STREAM     CONNECTED     1466   @000000ba
unix  1      [ ]         STREAM     CONNECTED     1091   @00000092
unix  1      [ ]         STREAM     CONNECTED     1402   @000000aa
unix  0      [ ACC ]     STREAM     LISTENING     1360   /tmp/orbit-root/orb-1182732604924858302
```

Appendix A
Results of Analyses and Tool Execution

```
unix  0      [ ACC ]     STREAM     LISTENING     1086   /tmp/.X11-unix/X0
unix  1      [ ]         STREAM     CONNECTED     1406   @000000ab
unix  0      [ ACC ]     STREAM     LISTENING     882    /dev/gpmctl
unix  1      [ ]         STREAM     CONNECTED     1645   @000000bf
unix  0      [ ACC ]     STREAM     LISTENING     1450   /tmp/orbit-root/orb-434888901778089632
unix  1      [ ]         STREAM     CONNECTED     1408   @000000ac
unix  0      [ ACC ]     STREAM     LISTENING     1018   /tmp/.font-unix/fs7100
unix  1      [ ]         STREAM     CONNECTED     1463   @000000b8
unix  1      [ ]         STREAM     CONNECTED     1415   @000000ad
unix  0      [ ACC ]     STREAM     LISTENING     1400   /tmp/orbit-root/orb-15468947551857399547
unix  1      [ ]         STREAM     CONNECTED     1115   @00000096
unix  0      [ ACC ]     STREAM     LISTENING     1111   /tmp/.ICE-unix/892
unix  1      [ ]         STREAM     CONNECTED     1465   @000000b9
unix  1      [ ]         STREAM     CONNECTED     1427   @000000ae
unix  0      [ ACC ]     STREAM     LISTENING     1413   /tmp/orbit-root/orb-991366279618433778
unix  1      [ ]         STREAM     CONNECTED     1391   @000000a8
unix  1      [ ]         STREAM     CONNECTED     1488   @000000bc
unix  0      [ ACC ]     STREAM     LISTENING     1433   /tmp/orbit-root/orb-17544345601986543838
unix  1      [ ]         STREAM     CONNECTED     1429   @000000af
unix  0      [ ACC ]     STREAM     LISTENING     1453   /tmp/orbit-root/orb-16673200901793118383
unix  1      [ ]         STREAM     CONNECTED     1334   @0000009d
unix  0      [ ]         STREAM     CONNECTED     553    @0000008c
unix  0      [ ACC ]     STREAM     LISTENING     1650   /tmp/orbit-root/orb-18019542041910621575
unix  1      [ ]         STREAM     CONNECTED     1455   @000000b4
unix  1      [ ]         STREAM     CONNECTED     1326   @0000009c
unix  0      [ ACC ]     STREAM     LISTENING     1144   /tmp/.sawmill-root/localhost.localdomain:0.0
unix  1      [ ]         STREAM     CONNECTED     1120   @00000097
unix  1      [ ]         STREAM     CONNECTED     1459   @000000b6
unix  1      [ ]         STREAM     CONNECTED     1122   @00000098
unix  10     [ ]         DGRAM                    599    /dev/log
unix  1      [ ]         STREAM     CONNECTED     1647   @000000c0
unix  1      [ ]         STREAM     CONNECTED     1435   @000000b0
unix  1      [ ]         STREAM     CONNECTED     1350   @000000a1
unix  0      [ ACC ]     STREAM     LISTENING     373    /var/run/pump.sock
unix  0      [ ]         STREAM     CONNECTED     232    @00000023
unix  1      [ ]         STREAM     CONNECTED     1442   @000000b1
unix  1      [ ]         STREAM     CONNECTED     1140   @0000009b
unix  1      [ ]         STREAM     CONNECTED     1652   @000000c1
```

```
unix  1      [ ]         STREAM     CONNECTED     1445   @000000b2
unix  1      [ ]         STREAM     CONNECTED     1659
unix  1      [ ]         STREAM     CONNECTED     1658
unix  1      [ W ]       STREAM     CONNECTED     1657
unix  1      [ ]         STREAM     CONNECTED     1656
unix  1      [ ]         STREAM     CONNECTED     1653   /tmp/orbit-root/orb-1546894755185739954 7
unix  1      [ ]         STREAM     CONNECTED     1648   /tmp/.ICE-unix/892
unix  1      [ ]         STREAM     CONNECTED     1646   /tmp/.X11-unix/X0
unix  1      [ ]         STREAM     CONNECTED     1489   /tmp/.X11-unix/X0
unix  1      [ ]         STREAM     CONNECTED     1470   /tmp/orbit-root/orb-434888901778089632
unix  1      [ ]         STREAM     CONNECTED     1467   /tmp/orbit-root/orb-991366279618433778
unix  1      [ ]         STREAM     CONNECTED     1472   /tmp/orbit-root/orb-16673200901793118383
unix  1      [ ]         STREAM     CONNECTED     1464   /tmp/orbit-root/orb-991366279618433778
unix  1      [ ]         STREAM     CONNECTED     1460   /tmp/orbit-root/orb-1546894755185739954 7
unix  1      [ ]         STREAM     CONNECTED     1456   /tmp/orbit-root/orb-1546894755185739954 7
unix  1      [ ]         STREAM     CONNECTED     1446   /tmp/.X11-unix/X0
unix  1      [ ]         STREAM     CONNECTED     1443   /tmp/.X11-unix/X0
unix  1      [ ]         STREAM     CONNECTED     1436   /tmp/orbit-root/orb-1546894755185739954 7
unix  1      [ ]         STREAM     CONNECTED     1430   /tmp/.ICE-unix/892
unix  1      [ ]         STREAM     CONNECTED     1428   /tmp/.X11-unix/X0
unix  1      [ ]         STREAM     CONNECTED     1416   /tmp/orbit-root/orb-1546894755185739954 7
unix  1      [ ]         STREAM     CONNECTED     1409   /tmp/.ICE-unix/892
unix  1      [ ]         STREAM     CONNECTED     1407   /tmp/.X11-unix/X0
unix  1      [ ]         STREAM     CONNECTED     1404   /tmp/orbit-root/orb-1546894755185739954 7
unix  1      [ ]         STREAM     CONNECTED     1392   /tmp/.X11-unix/X0
unix  0      [ ]         DGRAM                    1390
unix  1      [ ]         STREAM     CONNECTED     1355   /tmp/.ICE-unix/892
unix  1      [ ]         STREAM     CONNECTED     1335   /tmp/.X11-unix/X0
unix  1      [ ]         STREAM     CONNECTED     1327   /tmp/.ICE-unix/892
unix  1      [ ]         STREAM     CONNECTED     1141   /tmp/.X11-unix/X0
unix  1      [ ]         STREAM     CONNECTED     1123   /tmp/.ICE-unix/892
unix  1      [ ]         STREAM     CONNECTED     1121   /tmp/.X11-unix/X0
unix  1      [ ]         STREAM     CONNECTED     1116   /tmp/.X11-unix/X0
unix  1      [ ]         STREAM     CONNECTED     1092   /tmp/.font-unix/fs7100
unix  1      [ ]         STREAM     CONNECTED     1094   /tmp/.X11-unix/X0
unix  0      [ ]         DGRAM                    1061
unix  0      [ ]         DGRAM                    1045
unix  0      [ ]         DGRAM                    993
```

```
unix  0      [ ]         DGRAM                    866
unix  0      [ ]         DGRAM                    766
unix  0      [ ]         DGRAM                    718
unix  0      [ ]         DGRAM                    679
unix  0      [ ]         DGRAM                    655
unix  0      [ ]         DGRAM                    614
```

A. 6. Results of Whisker scan of webserver:

```
E:\downloads\scanners\whisker\v1.4>perl whisker.pl -I1 -i -v -h XXX.XXX.XXX.XXX -S  "Apache/1.3.12"
-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net --
- Using IDS spoofing mode(s) 1
- Loaded script database of 1968 lines

= - = - = - = - = - =
= Host: XXX.XXX.XXX.XXX
+ 302 Found: HEAD /
= Server: Apache/1.3.12

-  www.apache.org
+ 302 Found: GET /cfdocs/
+ 302 Found: GET /scripts/
+ 302 Found: GET /cgi-bin/
+ 302 Found: HEAD /_vti_pvt/
+ 302 Found: HEAD /PDG_Cart/
+ 302 Found: HEAD /orders/
+ 302 Found: HEAD /WebShop/
+ 302 Found: HEAD /icat
+ 302 Found: HEAD /cgi-local/
+ 302 Found: HEAD /htbin/
+ 302 Found: HEAD /cgibin/
+ 302 Found: HEAD /cgis/
+ 302 Found: HEAD /cgi/
+ 302 Found: HEAD /cgi-win/
+ 302 Found: HEAD /wwwboard/
+ 302 Found: HEAD /.htaccess
```

```
+ 302 Found: HEAD /bb-dnbd/
+ 302 Found: HEAD /wwwthreads/
+ 302 Found: HEAD /php/
+ 302 Found: HEAD /mlog.phtml
+ 302 Found: HEAD /mylog.phtml
+ 302 Found: HEAD /bin/
+ 302 Found: HEAD /admin/
+ 302 Found: HEAD /passwd
+ 302 Found: HEAD /passwd.txt
+ 302 Found: HEAD /password
+ 302 Found: HEAD /password.txt
```

A. 7. Results of display of `/etc/syslog.conf`:

```
more /etc/syslog.conf

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                         /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none                        /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                  /var/log/secure

# Log all the mail messages in one place.
mail.*                                          /var/log/maillog


# Log cron stuff
cron.*                                          /var/log/cron

# Everybody gets emergency messages, plus log them on another
# machine.
```

```
*.emerg                                                 *

# Save mail and news errors of level err and higher in a
# special file.
uucp,news.crit                                          /var/log/spooler

# Save boot messages also to boot.log
local7.*                                        /var/log/boot.log
```

A. 8. Results of `/etc/profile` file review:

```
more /etc/profile
# /etc/profile

# System wide environment and startup programs
# Functions and aliases go in /etc/bashrc

PATH="$PATH:/usr/X11R6/bin"

ulimit -S -c 1000000 > /dev/null 2>&1
if [ `id -gn` = `id -un` -a `id -u` -gt 14 ]; then
      umask 002
else
      umask 022
fi

USER=`id -un`
LOGNAME=$USER
MAIL="/var/spool/mail/$USER"

HOSTNAME=`/bin/hostname`
HISTSIZE=1000

if [ -z "$INPUTRC" -a ! -f "$HOME/.inputrc" ]; then
      INPUTRC=/etc/inputrc
fi
```

```
export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE INPUTRC

for i in /etc/profile.d/*.sh ; do
      if [ -x $i ]; then
            . $i
      fi
done

unset i
```

A. 9. Results of display of `/etc/passwd`:

```
more /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:
operator:x:11:0:operator:/root:
games:x:12:100:games:/usr/games:
gopher:x:13:30:gopher:/usr/lib/gopher-data:
ftp:x:14:50:FTP User:/var/ftp:
nobody:x:99:99:Nobody:/:
apache:x:48:48:Apache:/var/www:/bin/false
named:x:25:25:Named:/var/named:/bin/false
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
gdm:x:42:42::/home/gdm:/bin/bash
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/bin/false
rpc:x:32:32:Portmapper RPC user:/:/bin/false
```

```
mailnull:x:47:47::/var/spool/mqueue:/dev/null
pparzen:x:500:500:Paul Parzen:/home/pparzen:/bin/bash
cwilson:x:501:501:Chris Wilson:/home/cwilson:/bin/bash
bsapiro:x:502:502:Ben Sapiro:/home/bsapiro:/bin/bash
bwiddowson:x:503:10:Bob Widdowson:/home/bwiddowson:/bin/bash
bwiddowson1:x:504:10:Bob Widdowson:/home/bwiddowson1:/bin/ash
```

A. 10. Results of search for SUID and SGID files with `root` user:

```
find / -user root \( -perm -4000 -o -perm -2000 \) -ls
151101    8 -rws--x--x   1 root     root         6024 Aug 30  2000 /usr/X11R6/bin/Xwrapper
 64815   36 -rwsr-xr-x   1 root     root        34220 Aug  8  2000 /usr/bin/chage
 64817   36 -rwsr-xr-x   1 root     root        36344 Aug  8  2000 /usr/bin/gpasswd
 65013   24 -rwsr-xr-x   1 root     root        21248 Aug 24  2000 /usr/bin/crontab
 65019   36 -rwsr-xr-x   1 root     root        35964 Aug 23  2000 /usr/bin/at
 65088  780 -rws--x--x   2 root     root       793603 Aug  7  2000 /usr/bin/suidperl
 65088  780 -rws--x--x   2 root     root       793603 Aug  7  2000 /usr/bin/sperl5.6.0
 65606    8 -r-xr-sr-x   1 root     tty          6524 Aug  8  2000 /usr/bin/wall
 72067   40 -r-xr-s--x   1 root     games       40300 Aug 21  2000 /usr/bin/gataxx
 72068   24 -r-xr-s--x   1 root     games       20636 Aug 21  2000 /usr/bin/glines
 72069   72 -r-xr-s--x   1 root     games       69292 Aug 21  2000 /usr/bin/gnibbles
 72070   80 -r-xr-s--x   1 root     games       75900 Aug 21  2000 /usr/bin/gnobots2
 72071   56 -r-xr-s--x   1 root     games       52608 Aug 21  2000 /usr/bin/gnome-stones
 72072   76 -r-xr-s--x   1 root     games       71860 Aug 21  2000 /usr/bin/gnomine
 72073   28 -r-xr-s--x   1 root     games       25580 Aug 21  2000 /usr/bin/gnotravex
 72074   24 -r-xr-s--x   1 root     games       23132 Aug 21  2000 /usr/bin/gnotski
 72075  236 -r-xr-s--x   1 root     games      234044 Aug 21  2000 /usr/bin/gtali
 72076   48 -r-xr-s--x   1 root     games       47932 Aug 21  2000 /usr/bin/iagno
 72077   48 -r-xr-s--x   1 root     games       45452 Aug 21  2000 /usr/bin/mahjongg
 72078   24 -r-xr-s--x   1 root     games       21052 Aug 21  2000 /usr/bin/same-gnome
 72214    8 -rwsr-xr-x   1 root     root         6964 Aug 25  2000 /usr/bin/kcheckpass
 72452   36 -rwxr-sr-x   1 root     man         35260 Aug 23  2000 /usr/bin/man
 72776  156 -rwsr-xr-x   1 root     root       155436 Jul 17  2000 /usr/bin/ssh
 72786   16 -r-s--x--x   1 root     root        13536 Jul 12  2000 /usr/bin/passwd
 72841   12 -rwxr-sr-x   1 root     mail        10932 Aug 11  2000 /usr/bin/lockfile
 72843   68 -rwsr-sr-x   1 root     mail        63772 Aug 11  2000 /usr/bin/procmail
```

```
 72872   16 -rwsr-xr-x   1 root     root        14492 Jul 21  2000 /usr/bin/rcp
 72874   12 -rwsr-xr-x   1 root     root        10876 Jul 21  2000 /usr/bin/rlogin
 72875    8 -rwsr-xr-x   1 root     root         7828 Jul 21  2000 /usr/bin/rsh
 72928   24 -rwxr-sr-x   1 root     slocate     23964 Aug 23  2000 /usr/bin/slocate
 73195   16 -rws--x--x   1 root     root        13184 Aug 30  2000 /usr/bin/chfn
 73196   16 -rws--x--x   1 root     root        12640 Aug 30  2000 /usr/bin/chsh
 73213    8 -rws--x--x   1 root     root         5464 Aug 30  2000 /usr/bin/newgrp
 73224   12 -rwxr-sr-x   1 root     tty          8500 Aug 30  2000 /usr/bin/write
 48908    8 -rwsr-xr-x   1 root     root         6288 Aug 23  2000 /usr/sbin/usernetctl
 51125   12 -rwxr-sr-x   1 root     utmp         9212 Aug 23  2000 /usr/sbin/gnome-pty-helper
 54128  400 -r-sr-xr-x   1 root     root       401748 Aug 22  2000 /usr/sbin/sendmail
 54290   20 -rwsr-xr-x   1 root     root        16992 Jul 19  2000 /usr/sbin/traceroute
 54301   24 -rwsr-xr-x   1 root     root        20880 Oct  6 10:32 /usr/sbin/userhelper
 54302    8 -rwxr-sr-x   1 root     utmp         6584 Jul 13  2000 /usr/sbin/utempter
 63241    1 drwxr-sr-x   2 root     ftp          1024 Aug 17  2000 /var/ftp/pub
 48952   16 -rwsr-xr-x   1 root     root        14184 Jul 12  2000 /bin/su
 51510   24 -rwsr-xr-x   1 root     root        20604 Aug  8  2000 /bin/ping
 52861   60 -rwsr-xr-x   1 root     root        55356 Aug  5  2000 /bin/mount
 52862   28 -rwsr-xr-x   1 root     root        25404 Aug  5  2000 /bin/umount
113354    8 -rwxr-sr-x   1 root     root         4116 Aug 23  2000 /sbin/netreport
113359   16 -r-sr-xr-x   1 root     root        14732 Aug 22  2000 /sbin/pwdb_chkpwd
113360   16 -r-sr-xr-x   1 root     root        15340 Aug 22  2000 /sbin/unix_chkpwd
```

A. 11. Results of search for files which are unowned:

```
find / -nouser -o -nogroup -print / -ls
```

No unowned files on the server.

A. 12. Results of search for world-writable files:

```
find / -perm -2 ! typel -ls | grep -v dev
     2    2 drwxrwxrwt  21 root     root         2048 Mar  9 14:58 /tmp
```

Appendix A
Results of Analyses and Tool Execution

```
 32339    1 drwxrwxrwt   2 xfs      xfs          1024 Mar  9 14:40 /tmp/.font-unix
 32340    0 srwxrwxrwx   1 xfs      xfs             0 Mar  9 14:40 /tmp/.font-unix/fs7100
 20081    1 drwxrwxrwt   2 root     root         1024 Mar  9 14:41 /tmp/.X11-unix
 20082    0 srwxrwxrwx   1 root     root            0 Mar  9 14:41 /tmp/.X11-unix/X0
 22089    1 drwxrwxrwt   2 root     root         1024 Mar  9 14:41 /tmp/.ICE-unix
 22090    0 srwxrwxrwx   1 root     root            0 Dec 18 14:10 /tmp/.ICE-unix/671
 22221    0 srwxrwxrwx   1 root     root            0 Mar  5 15:30 /tmp/.ICE-unix/566
 22222    0 srwxrwxrwx   1 root     root            0 Mar  7 09:45 /tmp/.ICE-unix/559
 22223    0 srwxrwxrwx   1 root     root            0 Mar  7 16:09 /tmp/.ICE-unix/3902
 22261    0 srwxrwxrwx   1 root     root            0 Mar  9 14:41 /tmp/.ICE-unix/892
 87722    1 drwxrwxrwt   2 root     root         1024 Aug  4  2000 /var/lib/cddb
104042    1 drwxrwxrwt   2 root     root         1024 Aug 14  2000 /var/spool/samba
 46921    1 drwxrwxrwt   2 root     root         1024 Mar  5 15:36 /var/tmp
```

Bibliography

Track 6 – Common Issues and Vulnerabilities in UNIX Security, 6.1; Hal Pomeranz; The SANS Institute, Monday, January 29, 2001

Track 6 – UNIX Security Tools and Their Uses, 6.2; Matt Bishop; The SANS Institute, Tuesday, January 30, 2001

Track 6 – Topics in UNIX Security, 6.3; Steve Acheson & Hal Pomeranz; The SANS Institute, Wednesday, January 31, 2001

Track 6 – Running UNIX Applications Securely, 6.4; Lee Brotzman & Hal Pomeranz; The SANS Institute, Thursday, February 1, 2001

Track 6 – UNIX Practicum, 6.5; Lee Brotzman & Hal Pomeranz; The SANS Institute, Friday, February 2, 2001

Securing Linux Step-By-Step, Version 1.0; Lee Brotzman et al.; The SANS Institute, 2000

Red Hat Linux 7 Unleashed; Bill Ball, David Pitts, et al.; Sams Publishing, October 2000

Maximum Linux Security; Sams Publishing, September 1999

Practical Unix & Internet Security, Second Edition; O'Reilly & Associates, Inc., April 1996

Hacking Exposed: Network Security Secrets & Solutions, Second Edition; Joel Scrambray, Stuart McClure, George Kurtz; Osborne/McGraw-Hill, 2001

Endnotes

[1] Red Hat Errata; located online at http://www.redhat.com/support/errata/rh7-errata-security.htm

[2] http://www.redhat.com/support/errata/RHSA-2001-008.html

[3] http://www.redhat.com/support/errata/RHSA-2001-022.html

[4] http://www.redhat.com/support/errata/RHSA-2001-014.html

[5] Anonymous, Maximum Linux Security: A Hacker's Guide to Protecting Your Linux Server and Workstation; Sams Publishing, 2000; page 448

[6] Hal Pomeranz, "Track 6 – Securing Unix Systems, Unix Practicum 6.5"; The SANS Institute; Friday, February 2, 2001; page 17

[7] Anonymous, Maximum Linux Security: A Hacker's Guide to Protecting Your Linux Server and Workstation; Sams Publishing, 2000; page 320

[8] Simson Garfinkel and Gene Spafford, Practical Unix & Internet Security; O'Reilly & Associates, Inc., 1996; page 495

[9] Sendmail website: http://www.sendmail.org/

[10] Hal Pomeranz, "Track 6 – Securing Unix Systems, Running Unix Applications Securely 6.4"; The SANS Institute; Thursday, February 1, 2001; page 141

[11] Anonymous, Maximum Linux Security: A Hacker's Guide to Protecting Your Linux Server and Workstation; Sams Publishing, 2000; page 377

[12] Simson Garfinkel and Gene Spafford, Practical Unix & Internet Security; O'Reilly & Associates, Inc., 1996; pages 511-512

[13] Simson Garfinkel and Gene Spafford, Practical Unix & Internet Security; O'Reilly & Associates, Inc., 1996; pages 515-516

[14] Hal Pomeranz, "Track 6 – Securing Unix Systems, Unix Practicum 6.5"; The SANS Institute; Friday, February 2, 2001; page 74

[15] http://httpd.apache.org/dist/

[16] authored by rainforest puppy; http://www.wiretrip.net; obtained through http://packetstorm.securify.com

[17] http://www.core-sdi.com/english/index.html

[18] http://www.openssh.com/

[19] Hal Pomeranz, "Track 6 – Securing Unix Systems, Common Issues and Vulnerabilities in Unix Security, 6.1"; The SANS Institute; Monday, January 29, 2001; page 48

[20] Ibid, page 146

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**