

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

1.0 EXECUTIVE SUMMARY

The purpose of this audit is to give GIAC Enterprises a detailed analysis of their security, system administration, user policies, and operating procedures of their UNIX servers. This report will give GIAC Enterprises a consensus of what is known as good industry security practices.

1.1 SCOPE

The scope of this audit will be conducted on two departmental UNIX servers. Each server's operating system, third party software, configuration, and administrative practices will be examined for current best known security flaws because most attackers look for the easiest route to compromise a system.

1.2 CONCLUSIONS

GIAC Enterprises has several items to address to improve the security of the systems audited. The first item is the default installation of operating systems. Many compromises come from default installations. Second, there is no documentation for a secure standard configuration policy for GIAC Enterprises' UNIX operating systems. Third, there is no system administration policy. Finally, none of the audited systems had a backup and recovery policy. All of the above items can be addressed with a good company security policy.

1.3 MOST IMPORTANT RECOMMENDATIONS

There are several important recommendations that are high risk vulnerabilities that can result in a compromise of a system. Below is a list of these vulnerable areas:

- Default installation of both servers' operating systems includes extraneous services and numerous open ports. Attackers break into systems through these ports.
- Poor user account management. One of the systems audited had two default user accounts enabled. This could have lead to a compromise of the system. Also, no security or configuration policy is in place to force user to choose strong passwords
- No backup management plan. When a security incident or hardware failure occurs, a backup management plan will enable a speedy recovery.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.0 DESCRIPTION OF SYSTEM AND AUDIT METHODOLOGY

A detailed description of the audited systems' hardware and operating system follows below:

System Name	Platform	Processor(s)	Memory	Operating System	Operating version
Panther	SGI Indigo2	R4400 200 MHZ SC	256mb	IRIX	6.5.14
Sunsup1	Sun Ultra 10	2 400Mhz	1Gb	Solaris	2.7

2.1 THE ROLE OF THE AUDITED SYSTEMS IN GIAC ENTERPRISES NETWORK

The audit was conducted on two non-mission essential UNIX servers. The first server is an IRIX 6.5.14 SGI Indigo. Its primary role in GIAC Enterprises infrastructure is as a temporary file server. The second system, a Sun Ultra 10, primary role is an intranet FTP server.

2.2 OVERVIEW OF HOW THE AUDIT WAS CONDUCTED

The methodology of the audit was conducted by using both remote and host based audit tools that would reveal potential vulnerabilities. Remote testing would reveal what services each system offers over the Local Area Network. Host based testing confirms what the remote testing shows. In addition, it will show system and third application misconfiguration. By using both methods this would give GIAC Enterprises an overall view of possible ways the audited systems could be compromised.

2.2.1 What Tools Were Used

There were several tools and commands that were used in auditing the systems. The tool that was used for remote auditing was Nessus. This tool will probe a remote system for vulnerabilities that can be exploited over the network. It gives a rating ranging from high to low on vulnerabilities found. Nmap was another tool that was used. It probes a remote system for open ports. These ports are the gateways that are used to compromise a system. TARA was the host based scanner used. It scans a system's file system and provides information on possible system misconfiguration. The output report will give details on system's user accounts, file permissions, remote access, and executable files.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3.0 DETAILED ANALYSIS

The following analysis is a detailed description of operating system vulnerabilities, security patch management, configuration vulnerabilities, risks from third party software, and backup/disaster policies of each audited system. Each item identified will have information about what was discovered and how it was found. The output of the data that was used to evaluate what was found is in the appendix at the end of the report.

3.1 OPERATING SYSTEM VULNERABILITIES

The two audit systems Panther and Sunsup1 were audited both locally and remotely for operating system vulnerabilities. The remote audit was conducted by the Nessus scanning tool. It scanned each system over the network from a remote host for open ports. When a port was found open, it was evaluated for its security.

3.1.1 Telnet Vulnerability

The telnetd (23/tcp) daemon was found running on Panther and Sunsup1. This service has a serious buffer overflow vulnerability that was announced in **C**ERT Advisory CA-2001-21. It is remotely exploited during the processing of the Telnet protocol. If it exploited, an intruder can execute arbitrary code with root privileges (CERT CA-2001-21). The telnet service is also dangerous because the data that passes between the telnet client and the telnet server is clear text. This would enable a remote attacker to sniff the data that passes between the client and server.

3.1.2 LPD Vulnerability

The line printer daemon service (port 515/tcp) was found running on Sunsup1. This service has a serious buffer overflow vulnerability that was announced in CERT Advisory CA-2001-15 Buffer Overflow In Sun Solaris in.lpd Print Daemon (CERT CA-2001-15). According to the article, the daemon could be compromised by a remote attacker who executes malicious code as the root user.

3.1.3 Tooltalk Vulnerability

The tooltalk service was found on Panther (port 817/udp) and Sunsup1 (port 32773/tcp). ToolTalk is part of the Common Desktop Environment (CDE) package distributed with various commercial implementations of the Unix Operating System. This service has a serious buffer overflow vulnerability that was announced in CERT Advisory CA-2001-27 Format String Vulnerability in CDE Tooltalk

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

(CERT CA-2001-27). The article states that it contains a serious remote buffer overflow vulnerability that allows arbitrary code to be run with superuser privileges on a remote computer over the network.

3.1.4 SnmpXdmid Vulnerability

The snmpXdmid service was found running on Sunsup1 (port 32777/tcp). This service translates Simple Network Management Protocol (SNMP) events to Desktop Management Interface (DMI) indications and vice-versa. This service has serious remote buffer overflow vulnerability announced in CERT Advisory CA-2001-05 exploitation of snmpXdmid (CERT CA-2001-05). The article states that it can be exploited by local or remote user that is able to send packets to snmpXdmid daemon to gain root privileges.

3.1.5 Cmsd Vulnerability

The cmsd RPC service was found running on Sunsup1 (port 32781/tcp). This service is used by Calendar Manager Service daemon, rpc.cmsd. This daemon is frequently distributed with the Common Desktop Environment (CDE) and Open Windows. It has buffer overflow vulnerability that was announced in CERT Advisory CA-1999-08 Buffer Overflow Vulnerability in Calendar Manager Service Daemon, rpc.cmsd (CERT CA-1999-08). The article says it can be exploited by remote and local users, who can execute arbitrary code with the privileges of the rpc.cmsd daemon, typically root.

3.1.6 Sadmind Vulnerability

The sadmind RPC service was found running on Sunsup1 (port 32775/tcp). This service is installed with Sun Solistice Adminsuite package. It is used to coordinate distributed system administration operations remotely. It has remote buffer overflow vulnerability that was announced in CERT Advisory CA-1999-16 Buffer Overflow in Sun Solstice Adminsuite Daemon sadmind (CERT CA-1999-16). The article discusses how it can be exploited by a remote user who may be able to execute arbitrary code with root privileges.

3.1.7 Walld Vulnerability

The walld RPC service was found running on Sunsup1 (port 32779/tcp). This service allows users to broadcast messages to all users connected to a network. It has a vulnerability that was announced in CVE-1999-0181. The article states how the wall daemon

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

can be used for denial of service, social engineering attacks, or to execute remote commands (CVE-1999-0181).

3.1.8 Login Vulnerability

The telnetd (23/tcp) and rlogind (513/tcp) daemons running on Sunsup1 and Panther use /bin/login command to authenticate remote users as they initiate clear-text terminal connections over a network. The login command has a remote buffer overflow vulnerability that was announced in CERT Advisory CA-2001-34. This vulnerability can be remotely exploited to gain privileges of the invoker of login. In the case of programs such as telnetd and rlogind root access is gained (CERT CA-2001-34).

3.1.9 File Alteration Monitor Vulnerability

The file alteration monitor (1027/tcp) service was found running on Panther. It is used to track changes to the file system. This RPC service has vulnerability that was announced in Network Associates, Inc. Security Advisory #16 Silicon Graphics IRIX fam service (Network Associates #16). The alert says that it could be exploited by a remote attacker to learn the name of files and directories on a system.

3.2 SECURITY PATCH INSTALLATION/MANAGEMENT

The installation of operating system patches is crucial in preventing vulnerabilities. Without it, systems can be compromised because new attacks are being discovered everyday. Each of the audited systems was inspected for the latest patches from each vendor. The tools that were used for auditing each system were a combination of local commands and vendor supplied scripts. The tool that was used for Sunsup1 is called patchcheck v.1.0.4 from Sun Microsystems. It uses the perl command language to format the patchchk and patchdiag commands into a detailed report. Panther's patch management was evaluated by using the versions command. Its output was used to review installed software and patches.

3.2.1 Patch Installation/Management Evaluation

The report from the patchcheck v.1.0.4 was used to evaluate Sunsup1 patch management. The report results reveled that no patches have been installed. The output from the versions command was used to evaluate Panther. It had the latest maintenance and features release for IRIX 6.5.14. However, it did not have any of the latest patches released from the vendor. Inappropriate patch maintenance is the leading cause for system to become compromised.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3.3 CONFIGURATION VULNERABILITIES

Configuration vulnerabilities are one of the leading causes of security breaches. This area of security can not be overlooked by the system administrators of GIAC Enterprises. Default installations of operating systems have extraneous services and corresponding open ports. These are the gateways attackers use to break into systems. Each of the audited servers was reviewed for these substantial risks. The Nessus scanning tool was used along with native system commands to evaluate each system.

3.3.1 Unnecessary Services

Both Panther and Sunsup1 were examined for what services were currently running. Inetd is the process that handles standard internet services. Its default configuration file, /etc/inetd.conf, was used to ascertain what services are enabled. Each server's role in GIAC Enterprises was used to determine what services are not needed. Panther's role as a file server only requires that minimal number of services should be running. The only recommended service for a file server is Secure Shell. It is a secure replacement for telnet, rsh, and rlogin. Unlike the previous commands mentioned, it encrypts data and provides better authentication using RSA technology. Secure Shell suite also provides secure file transfer protocol. It provides a secure means to transfer files over the network. Sunsup1 role as an FTP server was reviewed for unnecessary services. By having default installation, the Nessus scan reported a number of unnecessary services were that were running. With the primary role of a FTP server, the audit team recommends only having Secure Shell and FTP services enabled.

3.3.2 Unnecessary Startup/Shutdown Scripts

At boot time the init command invokes the system run control scripts. These scripts determine what run level the system. The scripts start processes that make the server accessible for users. These scripts can start services that are dangerous or not useful. Each of the audited systems was reviewed for any unnecessary services started during the boot process. The role of Sunsup1 as a FTP server was used to determine what startup/shutdown scripts were necessary. The following scripts were not necessary for Sunsup1 function.

- Sendmail in /etc/rc2.d/S88sendmail.
- Remote Procedure Call (RPC) /etc/rc2.d/S71rpc.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- SNMP (Simple Network Management Protocol) in /etc/rc2.d/S76snpdx.
- NFS (Network File Server) server in /etc/rc3.d/S15nfs.server
- NFS (Network File Server) client in /etc/rc3.d/S15nfs.client

The role of Panther as a file server was used to determine what startup/shutdown scripts were necessary. The following scripts were not necessary for file server function.

- Autofs in /etc/rc2.d/S74autofs
- Autoconfig in /etc/rc2.d/S23autoconfig
- Sendmail in /etc/rc2.d/S50mail.

3.3.3 Cron and At Vulnerabilities

Cron is a job scheduling system that executes commands and/or scripts reputedly at a predetermined time. The at service is also a job scheduling system that executes commands and/or scripts once at a specific time. Both Panther and Sunsup1 both use the default cron jobs that are defined in the /etc/crontab file. Each system had several vulnerabilities that were a result of misconfiguration of the commands or scripts used in the cron jobs. The TARA host scanning tool revealed these warnings. Sunsup1 had a cron job that did not use the full path name for the executable. For example, PATH in a cron launched shell script for the user root is set to /tmp:/usr/bin. An attacker who knew this could create scripts in the /tmp directory that were the same name as the scripts in the cron launched shell script. Then, when the shell script is executed, the attacker's copy in /tmp would be executed instead of the correct version in /usr/bin. Both systems did not have user access control for the cron and at systems. It is recommended that the file /etc/cron.d/cron.deny include system accounts bin, daemon, smtp, nobody, noaccess so they are not allowed to use the cron system. These system accounts should also be included in /etc/cron.d/at.deny.

3.3.4 TCP Sequence Number Vulnerability

Upon connection via TCP/IP to a host, the host generates an Initial Sequence Number. This sequence number is used in the conversation between itself and the host to help keep track of each packet and to ensure that the conversation continues properly. Both the host and the client generate and use these sequence numbers in TCP connections. Both Panther and Sunsup1 are vulnerable to CERT Advisory CA-2001-09, Statistical Weaknesses in TCP/IP Initial Sequence Numbers (CERT CA-2001-09). The nmap tool

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

revealed that each server's TCP sequence number was trivial to guess what the next sequence number. It has long been known that an attacker who can guess the initial sequence number which a system will use for the next incoming TCP connection can spoof a TCP connection handshake coming from a machine to which he does not have access, and then send arbitrary data into the resulting TCP connection which will be accepted by the server as coming from the spoofed machine.

3.3.5 Remote Root Login Vulnerability

The Panther server was found to have configuration vulnerability that allows root to login remotely. It was discovered by the TARA host scanner. This is a serious misconfiguration because an attacker would only have to guess what the root password to gain unlimited privileges. It would allow him/her to read, write, and access all the data on the system.

3.4 RISKS FROM INSTALLED THIRD-PARTY SOFTWARE

Email is used practically everywhere in GIAC Enterprises. Sendmail is a third party application that is used to send, receive, and forward email on UNIX servers. Both Panther and Sunsup1 both use it. Sendmail presents GIAC Enterprises with multiple vulnerabilities because it has some of the most common exploits attackers use. One common exploit that both servers are vulnerable to is using Sendmail to forge email. This ability to relay mail is use send spam to unsolicited users. They were both vulnerable to EXPN and VRFY commands. The EXPN command can be used to find the delivery address 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. Sendmail should not allow remote users to use any of these commands, because it gives them too much information.

3.5 IDENTIFICATON AND PROTECTION OF SENSTIVE DATA ON HOSTS

The need to provide confidentiality, integrity, and availability of sensitive data is a challenge for GIAC Enterprises' system administrators. Both of the audited systems roles in GIAC Enterprises was considered in evaluating data access and how and data was protected. After conducting a risk assessment with the TARA security tool, the following insecurities were noted. Panther had several user accounts that had user identification of 0. The user root should only be the only user account that has a UID of 0. This presents a serious security problem because any account with a UID of 0 has access to all sensitive data on the system.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Panther also had multiple default user accounts that had no password. By not having passwords for each account, enables an attacker access to the system if they know the default account. This could lead to a serious compromise of the data and/or other systems. The environment of the systems is another area that could cause problems protecting the data for a couple of reason. The room that both of the servers were located in did not have air conditioning. The extreme temperature could cause corruption of sensitive data. Also, the each of the audited systems was not in a secure room. This could result in the data being stolen, vandalized, or destroyed by a fired employee.

3.6 PROTECTION OF SENSTIVE DATA IN TRASIT OVER THE NETWORK

The ability use of rsh, rlogin, rcp on GIAC Enterprises' represents one of its biggest security holes. Both Panther and Sunsup1 are running remote login services (ports 512/tcp through 514/tcp). The "r" commands should not used to data transfer over the network for several reasons. First, any password that that is typed is done in the clear. That means an attacker could use a tool like snoop to view the password over the network. Also, any data that is transferred during the session with a remote host is in the clear. That means every character of the session, including passwords could easily be recorded.

3.7 ACCESS CONTROLS

Each of the audited systems at GIAC Enterprises was reviewed for user and system access controls. Currently, there are no company policies for determine how to divide access controls for normal users and UNIX system administrators. This leaves both Panther and Sunsup1 vulnerable to security breaches. Access controls policies are important for several reasons. First, it can be used to protect sensitive data. For example, denying read access helps to protect confidentiality of information, and denying unnecessary write access can help maintain the integrity of information. Secondly, by limiting the execution privilege of most system related tools to authorized system administrators can prevent most users from making configuration changes that could reduce security. It also can restrict the ability of intruders to use those tools to attack the system or other systems on the network. Finally, remote host access controls are important because it limits what inbound network services are available. By limiting what remote systems can access services on both systems, the integrity, confidentiality, and control of the data can be trusted.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3.8 BACKUP POLICIES AND DISASTER PREPAREDNESS

System backups and disaster recover policies are vital procedures that are needed to minimize the impact system failures. At GIAC Enterprises, there are no system recovery policies in place. This places the audited systems Panther and Sunsup1 in a vulnerable situation for several reasons. First, natural disasters like, earthquakes, tornadoes, hurricanes, floods, wind, ice storms, snow, and rain can damage the company's computer systems. Without a backup and disaster recovery policy, the company would be unable to operate. Second, hardware failures are probably the leading cause of destroying data. If a backup has been created, the data could be restored on another system. Third, UNIX system administrator could make a mistake by entering the wrong command. This could cause a catastrophic failure like removing all of the files from the system. Finally, user error though the lack of training, poor documentation, or lack of attention to detail could destroy or corrupt sensitive company data.

3.9 OTHER ISSUES AND VULNERABILITES

Without a security policy, GIAC Enterprises has several vulnerable areas that were not discussed in the items above.

3.9.1 Default Installation of Operating Systems and Applications

The lack of a standard configuration policy for GIAC Enterprises left both audited systems with default an installation. The reason for this is most vendor operating system installation programs are designed for ease of use. This also caused several security holes that were discovered in the above sections. In addition, there are several other items that need to be reviewed. First, Panther has several accounts that did not have passwords. They were discovered by both the Nessus network scanner and TARA host based scan. These accounts create a serious security situation because any attacker who knows these default account names could gain access. Second, both systems by default allow remote root access. The TARA host based scanner uncovered this setting in /etc/default/login. It is highly advisable that root should be limited to login console. This increased accountability forces remote users to login first with a normal account then switch to the super user account. Finally, both systems have numerous set group and set user identification files (SUID, SGID). These files can present a possible security problem because allow a normal user to execute them with elevated privileges. This could potentially allow a user unnecessary access.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3.9.2 System Logging

Each of the audited systems needed to have additional logging configured. Both Panther and Sunsup1 /etc/syslog.conf was inadequately configured. System logging provides a listing of what was done on a system and by whom. This is vital for the system administrators because it with information about system performance, processes, and users activity. Also, there was no system log review policy. This is very important because usual system activity could go unnoticed.

3.9.3 Warning Banners

By offering remote access, each user who accesses the audited system should have a warning banner for several reasons. By not having a warning banner, could result in failure to prosecute a hacker or user for improper use of the system. It also warns users that any thing they do on the system is subject to monitoring. Finally, the Nessus scanning tool determined that default telnet banner on Sunsup1 for ftp offer information about what version of the operating system is running. This provides vital information because an attacker would know what vulnerabilities to attack for that version of the operating system.

4.0 CRITICAL ISSUES AND RECOMMENDATIONS

The conclusion of this audit is to give GIAC Enterprises recommendations on what are it critical vulnerabilities and how to resolve them. The following recommendations are a general consensus of top internet security vulnerabilities. Many of these solutions come from the Sans Institute and Computer Emergency Response Team (CERT). Both of these organizations are leaders in computer security awareness.

4.1 TOP TEN VULNERABILITIES AND ISSUES

The top ten vulnerabilities were areas that an attacker would use to compromise a system. Most attackers use the easiest way to gain access. By implementing the recommendations, GIAC Enterprises computer security will be greatly improved.

4.1.1 Default Operating System Installation

Many of the vulnerabilities listed throughout this document are a result of default operating system installation and poor patch management. Many of these items can be eliminated by having a standard configuration policy. The policy would give GIAC

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Enterprises Unix system administrators a guideline for them to follow in securing the company's UNIX servers. The following is a brief list of ideas that will help writing a standard configuration document:

Before any system is connect to the network:

- Check the vendor for any last minute updates.
- Retrieve security patches before installing.
- Check for the availability of a hardening script for your particular system.

After installation:

- Apply security patches.
- Identify what network services are needed and comment out unnecessary ones by commenting out their individual lines in /etc/inetd.conf with "#".
- Disable "r" commands (rsh, rlogin, and rsh). If they are required, a secure replacement alternative like Secure Shell should be used.
- Install and configure tcp_wrappers in /etc/inetd.conf. It provides greater access and logging features.
- Disable any unnecessary startup scripts in /etc, /etc/rc.d, or /etc/init.d.

4.1.2 User Accounts Without or Weak Passwords

Passwords are the first line of security of a system. Currently, GIAC Enterprises has no security policy governing user passwords. This audit revealed that Panther has two default accounts that were enabled without a password. In addition, there were system accounts that had valid shell. This also could lead to a system compromise because of a default password assigned to the account. The following sections will describe how to address this situation.

4.1.2.1 Locking Accounts Without Passwords

The audited system Panther had several accounts that did not have passwords assigned. The following script will search the /etc/passwd file for accounts that do not have a password and lock the account.

```
#!/bin/sh
for account in `/bin/passwd -sa | /sur/bin/awk '$2 == "NP" {print
$1}'`
do
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
        /bin/echo Locked the $account account
        /bin/passwd -l $account
done
```

4.1.2.2 User Password Auditing

In addition to securing default accounts, auditing user passwords is another important area. Below are several steps that will help password security.

1. Create a master list of user accounts.
2. Validate the list to ensure that no new accounts have been added/
3. Run a password cracking tool like John the Ripper (http://www.openwall.com/john).
4. Remove accounts when employees or contractors leave.

4.1.3 Unnecessary Services

There were numerous services that were enabled on both Panther and Sunsup1. Many of these services are unnecessary because of the roles of each system. Sections 3.3.1 and 3.3.2 discuss this issue. Both Panther and Sunsup1 roles were reviewed to determine what services should be enabled. The following will detail how to limit what services are running.

4.1.3.1 Services In Inetd.conf

Below is a list of services that are enabled on Sunsup1 and Panther. Inetd is the process that handles standard internet services. Its default configuration file, /etc/inetd.conf should be configured to limit what services are enabled. These services should be stopped and disabled. This can be accomplished by typing the following commands as root:

1. Open /etc/inetd.conf in any text editor.
2. Search for the line beginning with the "disabled service" (ie finger).
3. Insert "#" character at the beginning of this line.
4. Restart inetd process by typing, *kill –HUP 'inetd process ID'*. The process ID can be found by typing ps *–ef | grep inetd.*
Here is what the desired result of the edited line should look like.

Before:
finger stream tcp nowait nobody /usr/sbin/in.fingerd in.fingerd

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

After:
#finger stream tcp nowait nobody /usr/sbin/in.fingerd in.fingerd

Services enabled in /etc/inetd.conf

- fingerd
- rshd
- rexecd
- rlogin
- bootp
- dhcp_bootp
- tftpd
- talkd
- uucp
- ruserd
- name
- shell
- rlogin
- shell
- talk
- uucp
- systat
- netstat
- 100232/10
- rusersd/2-3
- sprayd/1
- walld/1
- rstatd/2-4
- rexd/1
- 100083/1
- ufsd/1
- fs

© SANS Institute 2000 - 2002, Author retains full rights.

4.1.3.2 Standalone Daemons

Below is a list of services that are started by run control scripts. The following are details on how to stop these unnecessary daemons from starting up.

On Sunsup1 execute the following commands and reboot the system.

- mv /etc/rc2.d/S88sendmail /etc/rc2.d/NOS88sendmail.
- mv /etc/rc2.d/S71rpc /etc/rc2.d/NOS71rpc.
- mv /etc/rc2.d/S76snpdx/etc/rc2.d/S76NOsnpdx.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- mv /etc/rc3.d/S15nfs.server /etc/rc3.d/NOS15nfs.server
- mv /etc/rc3.d/S15nfs.client /etc/rc3.d/NOS15nfs.client

On Panther, the chkconfig command can be used be used to stop startup scripts. The following are details on how to stop these unnecessary daemons from starting up.

- /sbin/chkconfig sendmail off
- /sbin/chkconfig sendmail_cf off
- /sbin/chkconfig autofs off
- /sbin/chkconfig lp off
- /sbin/chkconfig nfs off
- /sbin/chkconfig ntp off
- /sbin/chkconfig samba off
- /sbin/chkconfig nsd off

4.1.4 Filtering Incoming Hosts Access

By default, a UNIX system offers its network services to any host that tries to access them. This creates an insecure situation because an attacker could compromise vulnerable network services. This is why filtering network services are vital for securing GIAC Enterprises' UNIX systems. Both Panther and Sunsup1 do not use host access filtering. A solution for this is tcp_wrappers. It operates as a filter to intercept incoming network requests by acting as a "wrapper" around the service. This enables the host to filter access by network service, host IP address, or both. Tcp_wrappers is free and can be down loaded from http://www.sunfreeware.com and http://freeware.sgi.com. The package from SGI's freeware site can be installed by the inst program. An example of how to inst to install tcp_wrappers can be found in section 4.1.8.6.1. The package from Sun freeware site can be installed by the pkgadd program. Please note that the downloaded software must be uncompressed by the gunzip command. After installation, there are several steps that need to be completed before network services are filtered. First, there are two configuration files, host.allow and host.deny, for tcp_wrappers that need to be edited. In a text editor open the /etc/host.allow file. Insert the following line:

```
in.telnetd : 192.67.
```

The example above filters the telnet daemon to only allow a host from the 192.67 subnet to access the service.
Note: For every service in /etc/inetd.conf that you want to wrap, put an entry for each of the service(s).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Next, in a text editor open the /etc/host.deny file. Insert the following line:

```
ALL:ALL
```

Finally, in a text editor open the /etc/inetd.conf file. An example of how to what needs to modified for telnet is listed below.

Change:
```
telnet stream tcp nowait root /usr/etc/in.telnetd in.telnetd
```

To:
```
telnet stream tcp nowait root  /usr/bin/tcpd   in.telnetd
```

Restart inetd process by typing, *kill –HUP 'inetd process ID'*. The process ID can be found by typing ps *–ef | grep inetd.*

4.1.5 Incomplete System Logging

System logging is an important security area for a system. Both Panther and Sunsup1 system logging was discussed in section 3.9.2. The following is several steps to help GIAC Enterprises system logging.

4.1.5.1 Modify Syslogd.conf

Reviewing UNIX system logs are very important aspect of system administration. The syslogd sends and receives log events from process running on the system. It sorts these events by priority and writes these messages into log files. The priorities and where the log file are written are determined by syslogd's configuration file /etc/syslogd.conf. This syslogd.conf should be configured to gather and separate information. An example of a syslog.conf file is listed below.

```
*.emerg
*.err;kern.warning;auth.err;daemon.err          /dev/console
*.alert;kern.err;daemon.err                     operator
*.alert                                         root
kern.info               /var/adm/kern.log
user.info               /var/adm/user.log
mail.info               /var/adm/mail.log
daemon.info             /var/adm/daemon.log
auth.info               /var/adm/auth.log
lpr.info                /var/adm/lpr.log
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
cron.info                /var/adm/cron.log
```

Note: Each field is separate by tabs not spaces. Also, the file names listed must be created (ex. touch /var/adm/kern.log). Also, ensure proper file owner and file permissions are assigned (ex. chown root /var/adm/kern.log & chmod 600 /var/adm/kern.log). Complete the reconfiguration by restarting the syslogd daemon.

4.1.5.2 Rotate Logs

Messages that are created by the syslog daemon are appended to existing log files. After a period of time, they become so large that they use all available disk space. GIAC Enterprises System administrators only need to review the most current logs. It is recommended that CERT article, "Using newsyslog to rotate files containing logging messages on systems running Solaris 2.x" (http://www.cert.org/security-improvement/implementations/i041.09.html) be used as a guideline. The newsyslog script rotates and moves logs to a new location.

4.1.6 Securing FTP

With Sunsup1 acting as a FTP server, the proper configuration of it is necessary for having reliable data on it. Although, no vulnerabilities were found, there are a couple of areas that can be security can be improved.

4.1.6.1 Limiting FTP Access

Sunsup1 requires a valid user account for access the FTP daemon. However, the server also allows system accounts to FTP to it. There is no legitimate reason why any system account need to FTP files. The /etc/ftpusers file limits what user accounts can access the FTP server. The following is an example of what accounts should be in it.

```
root
daemon
bin
sys
adm
lp
uucp
nuucp
listen
nobody
noaccess
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

4.1.6.1 Replacing FTP With Secure FTP

The FTP protocol sends data and password in clear text over the network. Anyone who logins in and transfers data is vulnerable to an attacker who could monitor the network with a sniffer package. They could compromise data and/or user accounts. A secure replacement for FTP is Secure Shell's Secure FTP. It creates a tunnel using the SSH protocol. This provides secure means of transferring data across the network.

4.1.7 LPD Vulnerability

The Line Print Daemon service has a serious buffer overflow vulnerability that was discussed in section 3.1.2. Sun Microsystems have provided a patch for this vulnerability. The patch can be downloaded from http://sunsolve.sun.com. Go to the Patch Finder section and look for search for patch number 107115. Preferably, the Line Print Daemon running on Sunsup1 should be stopped and disabled. This can be accomplished by typing the following commands as root:

1. Open /etc/inetd.conf in any text editor.
2. Search for the line beginning with "printer".
3. Insert "#" character at the beginning of this line.
4. Restart inetd process by typing, *kill -HUP 'inetd process ID'*. The process ID can be found by typing ps *-ef | grep inetd.*

4.1.7.1 LPD Patch Installation Procedures

The following procedures are step by step instructions on how to install the LPD patch on both Panther and Sunsup1.

Sun Microsystems Patch Installation Process:

1. Create a directory in which you will work. For example, type *mkdir /tmp/newpatch*
2. Download the patch as a ".tar" file into the work directory.
3. Un-tar the tarfile in place. Type *tar xf 107475.tar* One or more files will be created.
4. Tell patchadd to perform the installation. Type, patchadd */tmp/newpatch/107115.*

4.1.8 Buffer Overflow Vulnerabilities

There were several buffer overflow vulnerabilities that were discovered. A buffer overflow occurs when a memory buffer is

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

filled with more information than it can accommodate. The excess characters can be used to run executable code. When used by an attacker, this could give them root privileges. The following sections will discuss how to address audited systems vulnerabilities.

4.1.8.1 Tooltalk Vulnerability Solution

This service has a serious buffer overflow vulnerability that was discussed in section 3.1.3. Both Silicon Graphics and Sun Microsystems have provided patches for this vulnerability. The patch can be downloaded from SGI at ftp://patches.sgi.com/support/free/security/patches/6.5/patch4416.tar. It can be downloaded from Sun Microsystems at http://sunsolve.sun.com. Go to the Patch Finder section and look for search for patch number 107893. Preferably, the tooltalk daemon running on Sunsup1 should be stopped and disabled. This can be accomplished by typing the following commands as root:

1. Open /etc/inetd.conf in any text editor.
2. Search for the line beginning with "rpc.ttdbserverd".
3. Insert "#" character at the beginning of this line.
4. Restart inetd process by typing, *kill –HUP 'inetd process ID'*. The process ID can be found by typing ps *–ef | grep Inetd.*

4.1.8.1.1 Tooltalk Patch Installation

Sun Microsystems Patch Installation Process:

1. Create a directory in which you will work. For example, type *mkdir /tmp/newpatch*
2. Download the patch as a ".tar" file into the work directory.
3. Un-tar the tarfile in place. Type *tar xf 107893.tar* One or more files will be created.
4. Tell patchadd to perform the installation. Type, patchadd */tmp/newpatch/107893.*

4.1.8.2 SnmpXdmid Vulnerability Solution

This service has a serious buffer overflow vulnerability that was discussed in section 3.1.4. Sun Microsystems have provided a patch for this vulnerability. The patch can be downloaded from http://sunsolve.sun.com. Go to the Patch Finder section and look for search for patch number 107709. Preferably, the SNMP and DMI daemons running on Sunsup1 should be stopped and disabled. This can be accomplished by typing the following commands as root:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- /etc/init.d/snmpdx stop and /etc/init.d/dmi stop; This will stop the daemons that are currently running
- mv /etc/rc3.d/S76snmpdx /etc/rc3.d/NOS76snmpdx and mv /etc/rc3.d/S77dmi /etc/rc3.d/NOS77dmi; This will prevent the daemons from starting after a reboot.
- ps –ef | grep dmi and ps –ef | grep snmp will give you the process IDs (PID). Kill each of the daemons by typing kill -9 PID for each one.
- ps –ef | grep dmi and ps –ef | grep snmp will verify that the daemons are not running.

4.1.8.2.1 SnmpXdmid Patch Installation

Sun Microsystems Patch Installation Process:

1. Create a directory in which you will work. For example, type *mkdir /tmp/newpatch*
2. Download the patch as a ".tar" file into the work directory.
3. Un-tar the tarfile in place. Type *tar xf 107709.tar* One or more files will be created.
4. Tell patchadd to perform the installation. Type, patchadd */tmp/newpatch/107709.*

4.1.8.3 Cmsd Vulnerability Solution

This service has a serious buffer overflow vulnerability that was discussed in section 3.1.5. Sun Microsystems have provided a patch for this vulnerability. The patch can be downloaded from http://sunsolve.sun.com. Go to the Patch Finder section and look for search for patch number 107022. Preferably, the Cmsd service running on Sunsup1 should be stopped and disabled. This can be accomplished by typing the following commands as root:

1. Open /etc/inetd.conf in any text editor.
2. Search for the line beginning with "rpc.cmsd".
3. Insert "#" character at the beginning of this line.
4. Restart inetd process by typing, *kill –HUP 'inetd process ID'*.

The process ID can be found by typing ps *–ef | grep Inetd.*

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

4.1.8.3.1 Cmsd Patch Installation

Sun Microsystems Patch Installation Process:

1. Create a directory in which you will work. For example, type *mkdir /tmp/newpatch*
2. Download the patch as a ".tar" file into the work directory.
3. Un-tar the tarfile in place. Type *tar xf 107022.tar* One or more files will be created.
4. Tell patchadd to perform the installation. Type, patchadd */tmp/newpatch/107022.*

4.1.8.4 Sadmind Vulnerability Solution

This service has a serious buffer overflow vulnerability that was discussed in section 3.1.6. Sun Microsystems have provided a patch for this vulnerability. The patch can be downloaded from http://sunsolve.sun.com. Go to the Patch Finder section and look for search for patch number 108662. Preferably, the sadmind daemon running on Sunsup1 should be stopped and disabled. This can be accomplished by typing the following commands as root:

1. Open /etc/inetd.conf in any text editor.
2. Search for the line beginning with "sadmind".
3. Insert "#" character at the beginning of this line.
4. Restart inetd process by typing, *kill –HUP 'inetd process ID'*.

The process ID can be found by typing ps *–ef | grep Inetd.*

4.1.8.4.1 Sadmind Patch Installation

Sun Microsystems Patch Installation Process:

1. Create a directory in which you will work. For example, type *mkdir /tmp/newpatch*
2. Download the patch as a ".tar" file into the work directory.
3. Un-tar the tarfile in place. Type *tar xf 108662.tar* One or more files will be created.
4. Tell patchadd to perform the installation. Type, patchadd */tmp/newpatch/108662.*

4.1.8.5 Walld Vulnerability Solution

This service has a serious buffer overflow vulnerability that was discussed in section 3.1.7. Sun Microsystems have provided a patch for this vulnerability. The patch can be downloaded from

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

http://sunsolve.sun.com. Go to the Patch Finder section and look for search for patch number 108662. Preferably, the Walld service running on Sunsup1 should be stopped and disabled. This can be accomplished by typing the following commands as root:

1. Open /etc/inetd.conf in any text editor.
2. Search for the line beginning with "walld".
3. Insert "#" character at the beginning of this line.
4. Restart inetd process by typing, *kill –HUP 'inetd process ID'*. The process ID can be found by typing ps *–ef | grep Inetd.*

4.1.8.6 Telnet Vulnerability Solution

This service has a serious buffer overflow vulnerability that was discussed in section 3.1.1. Both Silicon Graphics and Sun Microsystems have provided patches for this vulnerability. The patch can be downloaded from SGI at ftp://patches.sgi.com/support/free/security/patches/6.5/patch4354.tar. Sun Microsystems have provided a patch for this vulnerability. It can be downloaded from Sun Microsystems at http://sunsolve.sun.com. Go to the Patch Finder section and look for search for patch number 107475.

4.1.8.6.1 Telnet Patch Installation Procedures

The following procedures are step by step instructions on how to install the telnetd patches on both Panther and Sunsup1.

SGI Patch Installation Process:

1. Create a directory in which you will work. For example, type *mkdir /tmp/newpatch*
2. Download the patch as a ".tar" file into the work directory.
3. Un-tar the tarfile in place. Type *tar xf patch4354.tar.* One or more files will be created.
4. Run the software installer, "Inst." *inst*
5. Tell Inst to open the patch file. Type, *Inst> open patchSG0004060*
6. Tell Inst to perform the installation. Type, *Inst> go*
7. When the installation finishes, exit Inst. Type, *Inst> exit*

Sun Microsystems Patch Installation Process:

1. Create a directory in which you will work. For example, type *mkdir /tmp/newpatch*
2. Download the patch as a ".tar" file into the work directory.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3. Un-tar the tarfile in place. Type *tar xf 107475.tar* One or more files will be created.
4. Tell patchadd to perform the installation. Type, patchadd */tmp/newpatch/107475*

4.1.9 Sendmail Vulnerabilities Solution

Sendmail presents GIAC Enterprises with unnecessary vulnerabilities. The identified problems with EXPN and VRFY commands were discussed in section 3.4. There are a couple of ways to eliminate these vulnerabilities. First, Sendmail does not need to run as a daemon. The following is steps to stop Sendmail's daemon from running on both systems.

On Panther, as root type */sbin/chkconfig sendmail off* and */sbin/chkconfig sendmail_cf off*

On Sunsup1, as root type mv */etc/rc2.d/S88sendmail /etc/rc2.d/NOS88sendmail*

The daemon on both systems can be stopped by typing, ps *–ef | grep sendmail.* This will give the process ID (PID). Then kill the daemon by typing *kill – "sendmail PID".*

Finally, if either system needs to send email, Sendmail can be configured to run as a cron job. The procedure to do this is below:

Edit the crontab file by typing, as root, *crontab –e*. Then add the line *0 * * * * /usr/lib/sendmail –q*. This will flush the mail queue once every hour.

4.1.10 Non Existent Backups

System backups and recovery policies are an essential part of any company. It provides a method of restoring data after a security incident, hardware failure, or natural disaster. Many of the reasons for having backups and recovery policy are discussed in section 3.8. The following is recommendation for implementing a backup and recovery policy.

4.1.10.1 Determining What to Backup

It is recommended that a full backup of the entire system be done for a couple of reason. First, it is much easer to restore an entire system than try and recover bits and pieces of the system. Also, this will ensure that the availability and integrity of the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

data restored. Second, decide what tools are going to be used for backing systems up. It is recommended that GIAC Enterprises purchase a network based backup system like Legato Networker or Veritas Backup Exec. Finally, backups should be made daily. A general practice is a full backup is done at the beginning of each month and incremental backups every day.

4.1.10.2 Procedures to Recover Data

In addition to having a backup policy, procedures are needed for recovering and storing the data. There's couple of reasons why this is important. First, the ability to recover data off of tapes is not known until it has been tested. Magnetic media and the tape drives that write to them are susceptible to failure. An example of this is a misaligned tape drive. The tape drive could work perfect but it writes tapes that can only be recovered by the same drive. This could cause the data backup by it to be lost if the tape drive is replaced. Also, GIAC Enterprises needs to verify their written implemented recovery policy. Since data recovery is not an everyday occurrence, system administrators need to have procedures that have been tested. This will reduce system downtime.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

REFERENCES.

1) http://www.nessus.org/ Nessus remote security scanner

2) http://www-arc.com/tara/index.shtml TARA Tiger Analytical Research Assistant (TARA)

3) http://www.insecure.org Nmap Security Scanner

4) http://www-arc.com/sara/index.shtml Security Auditor's Research Assistant (SARA)

5) http://www.cert.org/advisories/CA-2001-21.html CERT Advisory CA-2001-21 Buffer Overflow in telnetd

6) http://www.cert.org/advisories/CA-2001-15.html CERT Advisory CA-2001-15 Buffer Overflow In Sun Solaris in.lpd Print Daemon

7) http://www.cert.org/advisories/CA-2001-27.html CERT Advisory CA-2001-27 Format String Vulnerability in CDE ToolTalk

8) http://www.cert.org/adisories/CA-2001-05.html CERT Advisory CA-2001-05 Exploitation of snmpXdmid

9) http://www.cert.org/advisories/CA-1999-08.html CERT Advisory CA-1999-08 Buffer Overflow Vulnerability in Calendar Manager Service Daemon, rpc.cmsd

10) http://www.cert.org/advisories/CA-1999-16.html CERT Advisory CA-1999-16 Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind

11) http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0181 The wall daemon can be used for denial of service, social engineering attacks, or to execute remote commands.

12) http://www.cert.org/advisories/CA-2001-34.html CERT Advisory CA-2001-34 Buffer Overflow in System V Derived Login

13) http://www.pgp.com/research/covert/advisories/016.asp Network Associates, Inc. Security Advisory #16

14) Cole, Eric.. *HACKERS BEWARE*. Copyright 2002 New Riders Publishing.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

15) Gregory, Peter H.. *Solaris Security*. Copyright 2000 Prentice-Hall Inc.

16) Garfinkel, Simson , Spafford Gene. Practical *UNIX & Internet Security* Copyright April 1996 O'Reilly & Associates Inc.

17) http://www.cert.org/security-improvement/practices/p032.html Configure computers for file backups

18) http://www.cert.org/security-improvement/implementations/i041.08.html Configuring and using syslogd to collect logging messages on systems running Solaris 2.x

19) http://www.mcc.ac.uk/cos/unix/Irix/security.shtml How to make an Out-of-the-Box SGI Machine Secure

20) http://www.sans.org/top20.htm The Twenty Most Critical Internet Security Vulnerabilities (Updated) The Experts' Consensus Version 2.501 November 15, 2001

21) http://www.cert.org/security-improvement/implementations/i041.09.html "Using newsyslog to rotate files containing logging messages on systems running Solaris 2.x"

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix A

NESSUS SCAN

```
Nessus Scan Report
------------------

SUMMARY
 - Number of hosts which were alive during the test: 1
 - Number of security holes found: 6
 - Number of security warnings found: 25
 - Number of security notes found: 5

TESTED HOSTS
192.168.0.32 (Security holes found)

DETAILS
+ 192.168.0.32:
 . List of open ports:
   o echo (7/tcp) (Security warnings found)
   o discard (9/tcp)
   o daytime (13/tcp) (Security warnings found)
   o chargen (19/tcp) (Security warnings found)
   o ftp (21/tcp) (Security hole found)
   o telnet (23/tcp) (Security hole found)
   o smtp (25/tcp) (Security warnings found)
   o time (37/tcp)
   o finger (79/tcp) (Security warnings found)
   o sunrpc (111/tcp)
   o exec (512/tcp) (Security warnings found)
   o login (513/tcp) (Security warnings found)
   o shell (514/tcp) (Security warnings found)
   o printer (515/tcp)
   o uucp (540/tcp)
   o x11 (6000/tcp) (Security warnings found)
   o unknown (6112/tcp)
   o xfs (7100/tcp)
   o general/tcp (Security notes found)
   o general/udp (Security notes found)
   o unknown (32779/udp) (Security warnings found)
   o unknown (32773/tcp) (Security warnings found)
   o unknown (32774/udp) (Security warnings found)
   o unknown (32778/udp) (Security warnings found)
   o unknown (32775/udp) (Security hole found)
   o unknown (32777/udp) (Security warnings found)
   o unknown (32780/udp) (Security warnings found)
   o unknown (32776/udp) (Security warnings found)
   o unknown (4045/udp) (Security warnings found)
   o unknown (32781/udp) (Security hole found)
   o echo (7/udp) (Security warnings found)
   o daytime (13/udp) (Security warnings found)
   o chargen (19/udp) (Security warnings found)
   o unknown (32777/tcp) (Security hole found)

. Warning found on port echo (7/tcp)
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
The 'echo' port is open. This port is not of any use nowadays, and may be a
source of problems, since it can be used along with other ports to perform a
denial of service. You should really disable this service.

Risk factor: Low.

Solution: comment out 'echo' in /etc/inetd.conf
CVE: CVE-1999-0103

. Warning found on port daytime (13/tcp)

The daytime service is running. The date format issued by this service may
sometimes help an attacker to guess the operating system type. In addition to
that, when the UDP version of daytime is running, an attacker may link it to
the echo port using spoofing, thus creating a possible denial of service.

Solution: disable this service in /etc/inetd.conf.

Risk factor: Low
CVE: CVE-1999-0103

. Warning found on port chargen (19/tcp)

The chargen service is running. The 'chargen' service should only be enabled
when testing the machine. hen contacted, chargen responds with some random
(something like all the characters in the alphabet in row). When contacted via
UDP, it will respond with a single UDP packet. When contacted via TCP, it will
continue spewing characters until the client closes the connection. An easy
attack is 'pingpong' which IP spoofs a packet between two machines running
chargen. They will commence spewing characters at each other, slowing the
machines down and saturating the network.

Solution: disable this service in /etc/inetd.conf.

Risk factor: Low
CVE: CVE-1999-0103

. Vulnerability found on port ftp (21/tcp):

We weren't able to login into the ftp server but the banner indicates that
you might be running a vulnerable version:

220 rtdsssun1 FTP server (SunOS 5.7) ready.


. Warning found on port ftp (21/tcp)

It is possible to determine the existence of a user on the remote system by
issuing the command

CWD ~<username>, even before logging in.

Ie:
telnet target 21
CWD ~root
530 Please login with USER and PASS.
CWD ~nonexistinguser
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
530 Please login with USER and PASS.
550 Unknown user name after ~

A cracker may use this to determine the existence of known to be vulnerable
accounts (like guest) or to determine which system you are running.

Solution: inform your vendor, and ask for a patch, or change your FTP server

Risk factor:  Low

. Information found on port ftp (21/tcp)

Remote FTP server banner:
rtdsssun1 ftp server (sunos 5.7) ready.


. Vulnerability found on port telnet (23/tcp):

The remote /bin/login seems to crash when it receives too many environment
variables. An attacker may use this flaw to gain a root shell on this system.
See also: http://www.cert.org/advisories/CA-2001-34.html

Solution: Contact your vendor for a patch (or read the CERT advisory)

Risk factor: High

. Vulnerability found on port telnet (23/tcp):

The Telnet server does not return an expected number of replies when it
receives a long sequence of 'Are You There' commands. This probably means it
overflows one of its internal buffers and crashes. It is likely an attacker
could abuse this bug to gain control over the remote host's superuser.

For more information, see: http://www.team-teso.net/advisories/teso-advisory-
011.tar.gz

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

Risk factor: High

 . 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)

Remote telnet banner:

. Warning found on port smtp (25/tcp)
```

© SANS Institute 2001 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
The remote SMTP server answers to the EXPN and/or VRFY commands. The EXPN
command can be used to find the delivery address 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 information.

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

Risk factor: Low
CVE: CAN-1999-0531

. Information found on port smtp (25/tcp)

Remote SMTP server banner:
rtdsssun1. ESMTP Sendmail 8.9.1b+Sun/8.9.1
Mon, 31 Dec 2001 14:08:11 -0500 (EST)
214-This is Sendmail version 8.9.1b+Sun214-Topics:
214-  HELO  EHLO  MAIL  RCPT  DATA
214-  RSET  NOOP  QUIT  HELP  VRFY
214-  EXPN  VERB  ETRN  DSN
214-For more info use "HELP <topic>".
214-To report bugs in the implementation contact Sun Microsystems
214-Technical Support.
214-For local information send email to Postmaster at your site.
214 End of HELP info




 . Warning found on port finger (79/tcp)

There is a bug in the finger service which will make it display the list of the
accounts that have never been used, when anyone issues the request:

finger 'a b c d e f g h'@target

This list will help an attacker to guess the operating system type. It will
also tell him which accounts have never been used, which will often make him
focus his attacks on these accounts.

Solution: disable the finger service in /etc/inetd.conf, or apply the patches
from Sun.

Risk factor: Medium

. Warning found on port finger (79/tcp)

The remote finger daemon accepts to redirect requests. That is, users can
perform requests like: finger user@host@victim This allows crackers to use your
computer as a relay to gather information on another network, making the other
network think you are making the requests.

Solution: disable your finger daemon (comment out the finger line in
/etc/inetd.conf) or install a more secure one.
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
Risk factor: Low
CVE: CAN-1999-0105

. Warning found on port finger (79/tcp)

The 'finger' service provides useful information 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

. Warning found on port exec (512/tcp)

The rexecd service is open. Because rexecd does not provide any good means of
authentication, it can be used by crackers to scan a third party host, giving
you troubles or bypassing your firewall.

Solution: comment out the 'exec' line in /etc/inetd.conf.

Risk factor: Medium
CVE: CAN-1999-0618

 . 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.
ou 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


. 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

. Warning found on port x11 (6000/tcp)

This X server does *not* accept clients to connect to it however it is
recommended that you filter incoming connections to this port as cracker may
send garbage data and slow down your X session or even kill the server Here is
the message we received:
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
      Client is not authorized to connect to Server

Solution: filter incoming connections to ports 6000-6009

Risk factor: Low
CVE: CVE-1999-0526

. Information found on port general/tcp

Nmap found that this host is running Solaris 2.6 - 2.7

. Information found on port general/udp

For your information, here is the traceroute to 192.168.0.32: 192.168.0.32

. Warning found on port unknown (32779/udp)

The walld RPC service is running. It is usually used by the administrator to
tell something to the users of a network by making a message appear on their
screen.

Since this service lacks any kind of authentication, a cracker may use it to
trick users into doing something (change their password, leave the console, or
worse), by sending a message which would appear to be written by the
administrator. It can also be used as a denial of service attack, by
continually sending garbage to the users' screens, preventing them from working
properly.

Solution: Deactivate this service.

Risk factor: Medium
CVE: CVE-1999-0181


. Warning found on port unknown (32773/tcp)

The tooltalk RPC service is running. An possible implementation fault in the
ToolTalk object database server may allow a cracker to execute arbitrary
commands as root.

** This warning may be a false positive since the presence of the bug was not
tested **

Solution: Disable this service.
See also: CERT Advisory CA-98.11

Risk factor: High
CVE: CVE-1999-0003


. Warning found on port unknown (32773/tcp)

The tooltalk RPC service is running. There is a format string bug in many
versions of this service, which allow an attacker to gain root remotely.

** This warning may be a false positive since the presence of the bug was not
tested **
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
Solution: Disable this service or patch it
See also: CERT Advisory CA-2001-27

Risk factor: High

. Warning found on port unknown (32774/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 (32778/udp)

The sprayd 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-1999-0613

. Vulnerability found on port unknown (32775/udp):

The sadmin RPC service is running. There is a bug in Solaris versions of this
service that allow an intruder to execute arbitrary commands on your system.

Solution: disable this service

Risk factor: High
CVE: CVE-1999-0977

. Warning found on port unknown (32777/udp)

The rusersd RPC service is running. It provides attacker interesting
information such as how often the system is being used, the names of the users,
and so on. It usually not a good idea to let this service open.

Risk factor: Low
CVE: CVE-1999-0626

. Warning found on port unknown (32780/udp)

The rstatd RPC service is running. It provides an attacker interesting
information such as:

- the CPU usage
- the system uptime
- its network usage
- and more
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
It usually not a good idea to let this service open

Risk factor: Low
CVE: CAN-1999-0624

. Warning found on port unknown (32776/udp)

The rquotad 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-1999-0625

. Warning found on port unknown (4045/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

. Vulnerability found on port unknown (32781/udp)

The cmsd 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 HAS BEEN TESTED, SO THIS MIGHT BE A
FALSE POSITIVE *

We suggest you to disable this service.


Risk factor: High
CVE: CVE-1999-0320

. Warning found on port echo (7/udp)

The 'echo' port is open. This port is not of any use nowadays, and may be a
source of problems, since it can be used along with other ports to perform a
denial of service. You should really disable this service.

Solution: comment out 'echo' in /etc/inetd.conf

Risk factor: Low.
CVE: CVE-1999-0103

. Warning found on port daytime (13/udp)

The daytime service is running. The date format issued by this service may
sometimes help an attacker to guess the operating system type. In addition to
that, when the UDP version of daytime is running, an attacker may link it to
the echo port using spoofing, thus creating a possible denial of service.
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
Solution: disable this service in /etc/inetd.conf.

Risk factor: Low
CVE: CVE-1999-0103

. Warning found on port chargen (19/udp)

The chargen service is running. The 'chargen' service should only be enabled
when testing the machine. When contacted, chargen responds with some random
(something like all the characters in the alphabet in row). When contacted via
UDP, it will respond with a single UDP packet. When contacted via TCP, it will
continue spewing characters until the client closes the connection. An easy
attack is 'pingpong' which IP spoofs a packet between two machines  running
chargen. They will commence spewing characters at each other, slowing the
machines down and saturating the network.

Solution: disable this service in /etc/inetd.conf.

Risk factor: Low
CVE: CVE-1999-0103

. Vulnerability found on port unknown (32777/tcp)

The remote RPC service 100249 (snmpXdmid) is vulnerable to a heap overflow
which allows any user to obtain a root shell on this host.

Solution: disable this service (/etc/init.d/init.dmi stop) if you don't use it,
or contact Sun for a patch

Risk factor: High
CVE: CAN-2001-0236


------------------------------------------------------
This file was generated by the Nessus Security Scanner


Nessus Scan Report
------------------

SUMMARY

 - Number of hosts which were alive during the test: 1
 - Number of security holes found: 1
 - Number of security warnings found: 26
 - Number of security notes found: 5

TESTED HOSTS

192.168.0.44 (Security holes found)

DETAILS

+ 192.168.0.44:
  . List of open ports:
    o tcpmux (1/tcp)
    o echo (7/tcp) (Security warnings found)
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
   o discard (9/tcp)
   o daytime (13/tcp) (Security warnings found)
   o chargen (19/tcp) (Security warnings found)
   o ftp (21/tcp) (Security notes found)
   o telnet (23/tcp) (Security hole found)
   o smtp (25/tcp) (Security warnings found)
   o time (37/tcp)
   o finger (79/tcp)
   o sunrpc (111/tcp)
   o exec (512/tcp) (Security warnings found)
   o login (513/tcp) (Security warnings found)
   o shell (514/tcp) (Security warnings found)
   o printer (515/tcp)
   o unknown (789/tcp)
   o unknown (1024/tcp)
   o unknown (1025/tcp)
   o unknown (1026/tcp)
   o unknown (1027/tcp) (Security warnings found)
   o unknown (1028/tcp)
   o unknown (1029/tcp)
   o unknown (1030/tcp)
   o nfs (2049/tcp) (Security warnings found)
   o sgi-dgl (5232/tcp)
   o unknown (5600/tcp)
   o general/tcp (Security warnings found)
   o general/udp (Security notes found)
   o unknown (1028/udp) (Security warnings found)
   o unknown (817/udp) (Security warnings found)
   o unknown (787/udp) (Security warnings found)
   o unknown (1031/udp) (Security warnings found)
   o unknown (1029/udp) (Security warnings found)
   o unknown (1027/udp) (Security warnings found)
   o unknown (1030/udp) (Security warnings found)
   o nfs (2049/udp) (Security warnings found)
   o unknown (2048/udp) (Security warnings found)
   o general/icmp (Security warnings found)
   o echo (7/udp) (Security warnings found)
   o daytime (13/udp) (Security warnings found)
   o chargen (19/udp) (Security warnings found)


  . Warning found on port echo (7/tcp)

The 'echo' port is open. This port is not of any use nowadays, and may be a
source of problems, since it can be used along with other ports to perform a
denial of service. You should really disable this service.

Solution: comment out 'echo' in /etc/inetd.conf
Risk factor: Low.
CVE: CVE-1999-0103

. Warning found on port daytime (13/tcp)

The daytime service is running. The date format issued by this service may
sometimes help an attacker to guess the operating system type. In addition to
that, when the UDP version of daytime is running, an attacker may link it to
the echo port using spoofing, thus creating a possible denial of service.
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
Solution: disable this service in /etc/inetd.conf.

Risk factor: Low
CVE: CVE-1999-0103

. Warning found on port chargen (19/tcp)

The chargen service is running. The 'chargen' service should only be enabled
when testing the machine. When contacted, chargen responds with some random
(something like all the characters in the alphabet in row). When contacted via
UDP, it will respond with a single UDP packet. When contacted via TCP, it will
continue spewing characters until the client closes the connection. An easy
attack is 'pingpong' which IP spoofs a packet between two machines running
chargen. They will commence spewing characters at each other, slowing the
machines down and saturating the network.

Solution: disable this service in /etc/inetd.conf.

Risk factor: Low
CVE: CVE-1999-0103

. Information found on port ftp (21/tcp)

Remote FTP server banner: rtdsspan.epa.gov ftp server ready.

. Vulnerability found on port telnet (23/tcp):

The account guest/guest seems to be valid. Change or disable it

CVE: CAN-1999-0502

. 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)

Remote telnet banner:

. 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 address 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 information.
```

© SANS Institute 2000 -2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

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

Risk factor: Low
CVE: CAN-1999-0531

. Information found on port smtp (25/tcp)

Remote SMTP server banner:
rtdsspan.epa.gov ESMTP Sendmail SGI-8.9.3/8.9.3
Sun, 6 Jan 2002 17:51:40 -0800 (PST)
214-This is Sendmail version SGI-8.9.3214-Topics:
214-  HELO  EHLO  MAIL  RCPT  DATA
214-  RSET  NOOP  QUIT  HELP  VRFY
214-  EXPN  VERB  ETRN  DSN
214-  For more info use "HELP <topic>".
214-  To report bugs in the implementation send email to
214-  sendmail-bugs@sendmail.org.
214-  For local information send email to Postmaster at your site.
214 End of HELP info

. Warning found on port exec (512/tcp)

The rexecd service is open. Because rexecd does not provide any good means of
authentication, it can be used by crackers to scan a third party host, giving
you troubles or bypassing your firewall.

Solution: comment out the 'exec' line in /etc/inetd.conf.

Risk factor: Medium
CVE: CAN-1999-0618

. 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

. 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

. Warning found on port unknown (1027/tcp)
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

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

Solution: disable this service in /etc/inetd.conf

More information: http://www.nai.com/nai_labs/asp_set/advisory/16_fam_adv.asp

Risk factor: High
CVE: CVE-1999-0059

. Warning found on port nfs (2049/tcp)

You are running a superfluous NFS daemon. You should consider removing it

CVE: CAN-1999-0554

. Warning found on port general/tcp

The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host. An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for port scanning and other things.

Solution: Contact your vendor for a patch

Risk factor: Low

. Information found on port general/tcp

Nmap found that this host is running IRIX 6.5.7f-6.5.8f

. Information found on port general/udp

For your information, here is the traceroute to 192.168.0.44: 192.168.0.44

. Warning found on port unknown (1028/udp)

The walld RPC service is running. It is usually used by the administrator to tell something to the users of a network by making a message appear on their screen. Since this service lacks any kind of authentication, a cracker may use it to trick users into doing something (change their password, leave the console, or worse), by sending a message which would appear to be written by the administrator.

It can also be used as a denial of service attack, by continually sending garbage to the users' screens, preventing them from working properly.

Solution: Deactivate this service.

Risk factor: Medium
CVE: CVE-1999-0181

. Warning found on port unknown (817/udp)

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
The tooltalk RPC service is running. An possible implementation fault in the
ToolTalk object database server may allow a cracker to execute arbitrary
commands as root.

** This warning may be a false positive since the presence of the bug was not
tested **

Solution: Disable this service.
See also: CERT Advisory CA-98.11

Risk factor: High
CVE: CVE-1999-0003

. Warning found on port unknown (817/udp)

The tooltalk RPC service is running. There is a format string bug in many
versions of this service, which allow an attacker to gain root remotely.

** This warning may be a false positive since the presence of the bug was not
tested **

Solution: Disable this service or patch it
See also: CERT Advisory CA-2001-27

Risk factor: High

. Warning found on port unknown (787/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 (1031/udp)

The sprayd 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-1999-0613

. Warning found on port unknown (1029/udp)

The rusersd RPC service is running. It provides an attacker interesting
information such as how often the system is being used, the names of the users,
and so on. It usually not a good idea to let this service open.

Risk factor: Low
CVE: CVE-1999-0626
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
. Warning found on port unknown (1027/udp)

The rstatd RPC service is running. It provides an attacker interesting
information such as:

- the CPU usage
- the system uptime
- its network usage
- and more

It usually not a good idea to let this service open

Risk factor: Low
CVE: CAN-1999-0624

. Warning found on port unknown (1030/udp)

The rquotad 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-1999-0625

. Warning found on port nfs (2049/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


. Warning found on port nfs (2049/udp)

The nfsd RPC service is running. There is a bug in older versions of this
service that allow an intruder to execute arbitrary commands on your system.
Make sure that you have the latest version of nfsd

Risk factor: High
CVE: CAN-1999-0832

. Warning found on port unknown (2048/udp)

The automountd service is running. There is a bug in the Solaris rpc.statd
and automountd which allow an attacker to execute any command remotely as root.

** THIS VULNERABILITY WAS NOT TESTED AND MAY BE A FALSE POSITIVE **

Solution: Disable your automountd and ask your vendor if you are vulnerable.

Risk factor: High
CVE: CVE-1999-0704

. Warning found on port general/icmp
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
The remote host answers to an ICMP timestamp request. This allows an attacker
to know the date which is set on your machine. This may help him to defeat all
your time based authentications protocols.

Solution: filter out the icmp timestamp requests (13), and the outgoing icmp
timestamp replies (14).

Risk factor: Low
CVE: CAN-1999-0524

. Warning found on port echo (7/udp)

The 'echo' port is open. This port is not of any use nowadays, and may be a
source of problems, since it can be used along with other ports to perform a
denial of service. You should really disable this service.

Solution: comment out 'echo' in /etc/inetd.conf

Risk factor: Low.
CVE: CVE-1999-0103

. Warning found on port daytime (13/udp)

The daytime service is running. The date format issued by this service may
sometimes help an attacker to guess the operating system type. In addition to
that, when the UDP version of daytime is running, an attacker may link it to
the echo port using spoofing, thus creating a possible denial of service.

Solution: disable this service in /etc/inetd.conf.

Risk factor: Low
CVE: CVE-1999-0103


. Warning found on port chargen (19/udp)

The chargen service is running. The 'chargen' service should only be enabled
when testing the machine.

When contacted, chargen responds with some random (something like all the
characters in the alphabet in row). When contacted via UDP, it will respond
with a single UDP packet. When contacted via TCP, it will continue spewing
characters until the client closes the connection.

An easy attack is 'pingpong' which IP spoofs a packet between two machines
running chargen. They will commence spewing characters at each other, slowing
the machines down and saturating the network.

Solution: disable this service in /etc/inetd.conf.

Risk factor: Low
CVE: CVE-1999-0103

------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

© SANS Institute 2000 - 2002, Author retains full rights

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Nmap Scan

```
Starting nmap V. 2.54BETA30 (www.insecure.org/nmap/)

Interesting ports on (192.168.0.32):
(The 1522 ports scanned but not shown below are in state: closed)
Port       State       Service
7/tcp      open        echo
9/tcp      open        discard
13/tcp     open        daytime
19/tcp     open        chargen
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
37/tcp     open        time
79/tcp     open        finger
111/tcp    open        sunrpc
512/tcp    open        exec
513/tcp    open        login
514/tcp    open        shell
515/tcp    open        printer
540/tcp    open        uucp
6000/tcp   open        X11
6112/tcp   open        dtspc
7100/tcp   open        font-service
32771/tcp  open        sometimes-rpc5
32772/tcp  open        sometimes-rpc7
32773/tcp  open        sometimes-rpc9
32774/tcp  open        sometimes-rpc11
32775/tcp  open        sometimes-rpc13
32776/tcp  open        sometimes-rpc15
32777/tcp  open        sometimes-rpc17
32778/tcp  open        sometimes-rpc19
32779/tcp  open        sometimes-rpc21

Remote operating system guess: Solaris 2.6 - 2.7
Uptime 29.685 days (since Wed Dec 26 15:27:14 2001)


Interesting ports on (192.168.0.44):
(The 1545 ports scanned but not shown below are in state: closed)
Port       State       Service
1/tcp      open        tcpmux
7/tcp      open        echo
9/tcp      open        discard
13/tcp     open        daytime
19/tcp     open        chargen
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
37/tcp     open        time
79/tcp     open        finger
111/tcp    open        sunrpc
139/tcp    open        netbios-ssn
512/tcp    open        exec
513/tcp    open        login
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
514/tcp    open        shell
515/tcp    open        printer
789/tcp    open        unknown
819/tcp    open        unknown
1007/tcp   open        unknown
1024/tcp   open        kdm
1025/tcp   open        listen
1026/tcp   open        nterm
1030/tcp   open        iad1
1455/tcp   open        esl-lm
2049/tcp   open        nfs
4321/tcp   open        rwhois
5232/tcp   open        sgi-dgl
6000/tcp   open        X11

Remote operating system guess: IRIX 6.5.7f-6.5.8f
Uptime 17.578 days (since Mon Jan 7 18:02:19 2002)
```

TARA OUPUT

```
Security scripts *** 2.0.9 ARC, 1999.0907.2100 ***
Fri Jan 18 14:01:55 EST 2002
14:01> Beginning security report for rtdsssun1 (sun4u SunOS 5.7).

# Performing check of passwd files...

# Performing check of group files...

# Performing check of user accounts...
# Checking accounts from /etc/passwd.
--WARN-- [acc001w] Login ID adm is disabled, but still has a valid shell.
--WARN-- [acc005w] Login ID adm is disabled, but has a 'cron' file or cron
         entries.
--WARN-- [acc001w] Login ID bin is disabled, but still has a valid shell.
--WARN-- [acc001w] Login ID daemon is disabled, but still has a valid shell.
--WARN-- [acc001w] Login ID listen is disabled, but still has a valid shell.
--WARN-- [acc001w] Login ID lp is disabled, but still has a valid shell.
--WARN-- [acc005w] Login ID lp is disabled, but has a 'cron' file or cron
         entries.
--WARN-- [acc001w] Login ID noaccess is disabled, but still has a valid shell.
--WARN-- [acc001w] Login ID nobody4 is disabled, but still has a valid shell.
--WARN-- [acc001w] Login ID sys is disabled, but still has a valid shell.
--WARN-- [acc005w] Login ID sys is disabled, but has a 'cron' file or cron
         entries.
--WARN-- [acc001w] Login ID uucp is disabled, but still has a valid shell.
--WARN-- [acc005w] Login ID uucp is disabled, but has a 'cron' file or cron
         entries.
--WARN-- [acc006w] Login ID adm's home directory (/var/adm) has group `sys'
         write access.
--WARN-- [acc006w] Login ID bin's home directory (/usr/bin) has group `bin'
         write access.
--WARN-- [acc006w] Login ID lp's home directory (/usr/spool/lp) has group `lp'
         write access.
--WARN-- [acc006w] Login ID nuucp's home directory (/var/spool/uucppublic) has
         group `uucp' and world write access.
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
# Performing check of /etc/hosts.equiv and .rhosts files...

# Checking accounts from /etc/passwd...

# Performing check of .netrc files...

# Checking accounts from /etc/passwd...

# Performing check of /etc/default/login, /securetty, and /etc/ttytab...

# Performing check of PATH components...
# Only checking user 'root'

--WARN-- [path002w] /usr/sbin/accept in root's PATH from default is not owned
         by root (owned by lp).
--WARN-- [path001w] /usr/sbin/install.d in root's PATH from default is group
         `bin' writable.
--WARN-- [path002w] /usr/sbin/lpadmin in root's PATH from default is not owned
         by root (owned by lp).
--WARN-- [path002w] /usr/sbin/lpfilter in root's PATH from default is not
         owned by root (owned by lp).
--WARN-- [path002w] /usr/sbin/lpforms in root's PATH from default is not owned
         by root (owned by lp).
--WARN-- [path002w] /usr/sbin/lpshut in root's PATH from default is not owned
         by root (owned by lp).
--WARN-- [path002w] /usr/sbin/lpsystem in root's PATH from default is not
         owned by root (owned by lp).
--WARN-- [path002w] /usr/sbin/lpusers in root's PATH from default is not owned
         by root (owned by lp).
--WARN-- [path002w] /usr/sbin/reject in root's PATH from default is not owned
         by root (owned by lp).
--WARN-- [path001w] /usr/sbin/static in root's PATH from default is group
         `bin' writable.


--WARN-- [path002w] /usr/bin/disable in root's PATH from default is not owned
         by root (owned by lp).
--WARN-- [path002w] /usr/bin/enable in root's PATH from default is not owned
         by root (owned by lp).

# Performing check of anonymous FTP...

# Performing checks of mail aliases...
# Checking aliases from /etc/mail/aliases.

# Performing check of `cron' entries...
--WARN-- [cron001w] cron entry for lp does not use full pathname:
--WARN-- [cron003] cron entry for lp uses `/bin/mv' which contains `/usr'
         which is group `sys' writable.

--WARN-- [cron003] cron entry for lp uses `/bin/mv' which contains `/usr/bin'
         which is group `bin' writable.

--WARN-- [cron003] cron entry for lp uses `/usr/bin/cp' which contains `/usr'
         which is group `sys' writable.
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
--WARN-- [cron003] cron entry for lp uses `/usr/bin/cp' which contains
         `/usr/bin' which is group `bin' writable.

--WARN-- [cron001w] cron entry for lp does not use full pathname:
--WARN-- [cron003] cron entry for lp uses `/bin/mv' which contains `/usr'
         which is group `sys' writable.

--WARN-- [cron003] cron entry for lp uses `/bin/mv' which contains `/usr/bin'
         which is group `bin' writable.

--WARN-- [cron003] cron entry for lp uses `/usr/bin/cp' which contains `/usr'
         which is group `sys' writable.

--WARN-- [cron003] cron entry for lp uses `/usr/bin/cp' which contains
         `/usr/bin' which is group `bin' writable.

--WARN-- [cron002] cron entry for root uses `/etc/cron.d/logchecker' which is
         not owned by root (owned by bin).

--WARN-- [cron003] cron entry for root uses `/usr/lib/newsyslog' which
         contains `/usr' which is group `sys' writable.

--WARN-- [cron003] cron entry for root uses `/usr/lib/newsyslog' which
         contains `/usr/lib' which is group `bin' writable.

--WARN-- [cron003] cron entry for root uses `/usr/lib/fs/nfs/nfsfind' which
         contains `/usr' which is group `sys' writable.

--WARN-- [cron003] cron entry for root uses `/usr/lib/fs/nfs/nfsfind' which
         contains `/usr/lib' which is group `bin' writable.

--WARN-- [cron003] cron entry for root uses `/usr/lib/fs/nfs/nfsfind' which
         contains `/usr/lib/fs' which is group `sys' writable.

--WARN-- [cron001w] cron entry for root does not use full pathname:




--WARN-- [cron001w] cron entry for root does not use full pathname:
--WARN-- [cron003] cron entry for root uses `/usr/lib/gss/gsscred_clean' which
         contains `/usr' which is group `sys' writable.

--WARN-- [cron003] cron entry for root uses `/usr/lib/gss/gsscred_clean' which
         contains `/usr/lib' which is group `bin' writable.

--WARN-- [cron002] cron entry for root uses `/usr/lib/gss/gsscred_clean' which
         contains `/usr/lib/gss' which is not owned by root (owned by bin).

--WARN-- [cron003] cron entry for root uses `/usr/lib/gss/gsscred_clean' which
         contains `/usr' which is group `sys' writable.

--WARN-- [cron003] cron entry for root uses `/usr/lib/gss/gsscred_clean' which
         contains `/usr/lib' which is group `bin' writable.

--WARN-- [cron002] cron entry for root uses `/usr/lib/gss/gsscred_clean' which
         contains `/usr/lib/gss' which is not owned by root (owned by bin).
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
# Performing check of 'services' and 'inetd'...
# Checking services from /etc/services.
--FAIL-- [inet003f] The port for service pop2 is assigned to service pop-2.
# Checking inetd entries from /etc/inet/inetd.conf
--WARN-- [inet005w] Service 100083/1 is using /usr/dt/bin/rpc.ttdbserverd
         instead of /usr/openwin/bin/rpc.ttdbserverd.

# Performing NFS exports check...

# Performing check of system file permissions...
--WARN-- [perm001w] /export should not have group write.
--WARN-- [perm001w] /sbin should not have group write.
--WARN-- [perm001w] /usr should not have group write.
--WARN-- [perm001w] /usr/4lib should not have group write.
--WARN-- [perm001w] /usr/openwin should not have group write.
--WARN-- [perm001w] /usr/demo should not have group write.
--WARN-- [perm001w] /usr/games should not have group write.
--WARN-- [perm001w] /usr/bin should not have group write.
--WARN-- [perm001w] /usr/lib should not have group write.
--WARN-- [perm001w] /usr/ucb should not have group write.
--WARN-- [perm001w] /dev should not have group write.
--WARN-- [perm001w] /etc/dfs should not have group write.
--WARN-- [perm001w] /etc/vfstab should not have group write.
--WARN-- [perm001w] The owner of /etc/uucp/Permissions should be root (owned
         by uucp).
--WARN-- [perm001w] The owner of /usr/bin/uulog should be root (owned by
         uucp).
--WARN-- [perm001w] The owner of /usr/bin/uuto should be root (owned by uucp).
--WARN-- [perm001w] The owner of /usr/bin/uupick should be root (owned by
         uucp).
--WARN-- [perm001w] /usr/bin/tip should not have owner write.
--ALERT-- [perm024a] /usr/sbin/arp is setgid to `bin'.
--WARN-- [perm021w] Disk device /dev/dsk/c0t3d0s0 has read access for group
         sys.
--WARN-- [perm021w] Disk device /dev/rdsk/c0t3d0s0 has read access for group
         sys.
--WARN-- [perm021w] Disk device /dev/dsk/c0t3d0s7 has read access for group
         sys.
--WARN-- [perm021w] Disk device /dev/rdsk/c0t3d0s7 has read access for group
         sys.
--WARN-- [perm021w] Disk device /dev/dsk/c0t3d0s5 has read access for group
         sys.
--WARN-- [perm021w] Disk device /dev/rdsk/c0t3d0s5 has read access for group
         sys.
--WARN-- [perm021w] Disk device /dev/dsk/c0t3d0s6 has read access for group
         sys.
--WARN-- [perm021w] Disk device /dev/rdsk/c0t3d0s6 has read access for group
         sys.
--WARN-- [perm021w] Disk device /dev/dsk/c0t3d0s1 has read access for group
         sys.
--WARN-- [perm021w] Disk device /dev/rdsk/c0t3d0s1 has read access for group
         sys.

# Checking for known intrusion signs...
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
# Performing check of files in system mail spool...

# Performing system specific checks...
# Performing checks for SunOS/5...
--WARN-- [no-id] The PROM monitor is not in secure mode.
--WARN-- [misc008w] NFS port checking disabled in kernel.
# Running './scripts/check_sendmail'...

# Checking sendmail...

# Checking setuid executables...
--FAIL-- [fsys001f] File /etc/lp/alerts/printer is a setuid script:
-r-sr-xr-x   1 lp       lp           203 Sep 10  1998 /etc/lp/alerts/printer
--WARN-- [fsys002w] setuid program /usr/bin/nispasswd has relative pathnames.
--WARN-- [fsys002w] setuid program /usr/bin/passwd has relative pathnames.
--WARN-- [fsys002w] setuid program /usr/bin/yppasswd has relative pathnames.
--WARN-- [fsys002w] setuid program /usr/lib/fs/ufs/ufsrestore has relative
         pathnames.
--WARN-- [fsys002w] setuid program /usr/openwin/bin/kcms_calibrate has
         relative pathnames.
--WARN-- [fsys002w] setuid program /usr/openwin/bin/kcms_configure has
         relative pathnames.
--WARN-- [fsys002w] setuid program /usr/openwin/bin/sys-suspend has relative
         pathnames.
--WARN-- [suidxxx] Setuid file `/usr/openwin/bin/sys-suspend' which is group
         `bin' writable.

--WARN-- [suidxxx] Setuid file `/usr/openwin/bin/xlock' which is group `bin'
         writable.

--WARN-- [fsys002w] setuid program /usr/sbin/static/rcp has relative
         pathnames.

-r-sr-xr-x root     bin      /usr/bin/sparcv9/uptime
-r-sr-xr-x root     bin      /usr/bin/sparcv9/w
-r-sr-xr-x root     bin      /usr/sbin/ffbconfig
-r-sr-xr-x root     bin      /usr/sbin/sparcv9/whodo
-r-sr-xr-x root     sys      /usr/bin/sparcv9/ps
-r-sr-xr-x root     sys      /usr/ucb/sparcv9/ps


# Checking setgid executables...

--CONFIG-- [fsys003c] No setgid list... listing all setgid files

# Checking unusual file names...

# Looking for unusual device files...

# Checking symbolic links...

Security scripts *** 2.0.9 ARC, 1999.0907.2100 ***
Thu Jan 17 14:42:19 PST 2002
14:42> Beginning security report for rtdsspan.epa.gov (IP22 IRIX 6.5).

# Performing check of passwd files...
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
--WARN-- [pass001w] Username `nobody' exists multiple times in /etc/passwd.
--WARN-- [pass002w] UID 0 exists multiple times in /etc/passwd.
--WARN-- [pass002w] UID 60001 exists multiple times in /etc/passwd.

# Performing check of group files...
--WARN-- [grp002w] GID 0 exists multiple times in /etc/group.

# Performing check of user accounts...
# Checking accounts from /etc/passwd.
--WARN-- [acc012w] Login ID sysadm has uid == 0.
--WARN-- [acc012w] Login ID diag has uid == 0.
--WARN-- [acc011w] Login ID nuucp does not have a password.
--WARN-- [acc011w] Login ID EZsetup does not have a password.
--WARN-- [acc011w] Login ID guest does not have a password.
--WARN-- [acc011w] Login ID 4Dgifts does not have a password.
--WARN-- [acc001w] Login ID sysadm is disabled, but still has a valid shell.

--WARN-- [acc001w] Login ID uucp is disabled, but still has a valid shell.

# Performing check of /etc/hosts.equiv and .rhosts files...
 localhost

# Checking accounts from /etc/passwd...

# Performing check of .netrc files...

# Checking accounts from /etc/passwd...

# Performing check of /etc/default/login, /securetty, and /etc/ttytab...

--WARN-- [root001w] Remote root login allowed in /etc/default/login.

# Performing check of PATH components...
# Only checking user 'root'

# Performing check of anonymous FTP...

# Performing checks of mail aliases...
# Checking aliases from /usr/lib/aliases.

# Performing check of `cron' entries...
--WARN-- CRON file `' is owned by sys.
--WARN-- CRON file `' is owned by sys.

# Performing check of 'services' and 'inetd'...
# Checking services from /etc/services.
# Checking inetd entries from /usr/etc/inetd.conf
--WARN-- [inet005w] Service bootp is using /usr/etc/dhcp_bootp instead of
         /usr/etc/bootp.

# Performing NFS exports check...

# Performing check of system file permissions...
--WARN-- [perm001w] /unix should not have group execute.
--WARN-- [perm001w] /unix should not have world execute.
--WARN-- [perm001w] The owner of /var/tmp should be root (owned by sys).
--WARN-- [perm001w] /dev/vme should not have owner search.
```

SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
--WARN-- [perm001w] /dev/vme should not have group read.
--WARN-- [perm001w] /dev/vme should not have group search.
--WARN-- [perm001w] /dev/vme should not have world read.
--WARN-- [perm001w] /dev/vme should not have world search.
--WARN-- [perm001w] /etc/exports should not have group read.
--WARN-- [perm001w] /etc/exports should not have world read.
--WARN-- [perm001w] /etc/fstab should not have group read.
--WARN-- [perm001w] /etc/fstab should not have world read.
--WARN-- [perm001w] /etc/hosts.equiv should not have group read.
--WARN-- [perm001w] /etc/hosts.equiv should not have world read.
--FAIL-- [perm001w] /etc/netgroup should not have group read.
--FAIL-- [perm001w] /etc/netgroup should not have world read.
--FAIL-- [perm001w] /etc/rc0 should not have owner execute.
--FAIL-- [perm001w] /etc/rc0 should not have group execute.
--FAIL-- [perm001w] /etc/rc0 should not have world execute.
--FAIL-- [perm001w] /etc/rc0.d should not have owner search.
--FAIL-- [perm001w] /etc/rc0.d should not have group search.
--FAIL-- [perm001w] /etc/rc0.d should not have world search.
--FAIL-- [perm001w] /etc/init.d should not have owner search.
--FAIL-- [perm001w] /etc/init.d should not have group search.
--FAIL-- [perm001w] /etc/init.d should not have world search.

# Checking for known intrusion signs...

# Performing check of files in system mail spool...

# Performing system specific checks...
# Running './scripts/check_sendmail'...

# Checking sendmail...
--WARN-- [misc010w] /usr/lib/sendmail appears to be older than November 1993
         (apparent date 10/09/1901), and may contain a security vulnerability.

# Checking setuid executables...
--WARN-- [misc013w] /usr/bin/X11/xterm: see CERT Advisory CA-93:17 about a
         security hole in xterm.
--WARN-- [fsys002w] setuid program /usr/lib/InPerson/inpview has relative
         pathnames.

---s--x--x sys      86152    /usr/freeware/bin/sudo
-r-Sr--r-- sys      2808     /usr/lib/SoftWindows2/sys.swin2config
-r-s--x--x bin      237840   /usr/freeware/bin/cda
-r-s--x--x bin      352924   /usr/freeware/bin/xmcd
-r-sr-sr-x mail     30260    /usr/freeware/libexec/emacs/19.34/mips-sgi-
irix6.x/movemail
-r-sr-xr-x sys      10024    /usr/lib/tour/bin/RemoveSystemTour
-r-sr-xr-x sys      10040    /usr/lib/tour/bin/KillHigh
-r-sr-xr-x sys      223276   /usr/lib/tour/bin/PlayHigh
-r-sr-xr-x sys      31432    /usr/etc/appletalk/print2lpr
-r-sr-xr-x sys      728120   /usr/etc/appletalk/jgui
-rws--x--x sys      39568    /usr/freeware/lib/mh/popwrd
-rwsr-s--- adm      21920    /usr/etc/ts/tsstop
-rwsr-s--- adm      22156    /usr/etc/ts/tsset
-rwsr-s--- adm      65572    /usr/etc/ts/tsdaemon
-rwsr-sr-x sys      22236    /usr/sysadm/bin/runpriv
-rwsr-xr-x mail     39336    /usr/bin/mail.local
-rwsr-xr-x sys      129940   /usr/sbin/scanners
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
-rwsr-xr-x sys      13808    /usr/sysadm/bin/checkpriv
-rwsr-xr-x sys      13836    /usr/sysadm/bin/adddefpriv
-rwsr-xr-x sys      13836    /usr/sysadm/bin/rmdefpriv
-rwsr-xr-x sys      13908    /usr/sysadm/bin/rmprivuser
-rwsr-xr-x sys      181600   /usr/freeware/bin/seyon
-rwsr-xr-x sys      2025392  /usr/lib/SoftWindows2/bin/SoftWindows2
-rwsr-xr-x sys      22000    /usr/sysadm/bin/addprivuser
-rwsr-xr-x sys      22064    /usr/sysadm/bin/rmpriv
-rwsr-xr-x sys      22260    /usr/sysadm/bin/addpriv
-rwsr-xr-x sys      39396    /sbin/df
-rwsr-xr-x sys      44120    /sbin/su
-rwsr-xr-x sys      75096    /usr/freeware/etc/nfswatch
-rwsr-xr-x sys      930428   /usr/samba/bin/swat


# Checking setgid executables...

--CONFIG-- [fsys003c] No setgid list... listing all setgid files

# Checking unusual file names...

# Looking for unusual device files...

# Checking symbolic links...
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.