Global Information Assurance Certification Paper

GIAC Certification

GCUS Practical Assignment
Version 1.9

Auditing Sun One Web Server

Consultant's Report

Anwar Saadeh
February 2003

Table of Contents

1 Executive Summary:

GIAC Enterprise is an e-business company that deals with online sale of fortune cookie sayings. The company has been growing and successful for the past 2 years. Due to increases of direct and indirect web attacks from Internet connection, top management has necessitated a re-evaluation and audit of how the company conducts its business over the Internet.

The purpose of this audit is to investigate, assess, and provide recommendations to ensure the company's main Web Server, named "sunone", is appropriately protected and secured from internal and external threats. Threats can be natural disasters, equipment failures, or planned attacks on the network and application data.

The scope of this audit is to give a detailed analysis, evaluation, and recommendation of GIAC enterprise e-business Web Server.

Based on our analysis of the Server and its role, we found that the server has numerous security issues:

- The Web Server operating system was built using the entire distribution of Solaris 9 software application. This distribution includes many unneeded software packages and services that are not relevant to the role of this server. We recommend either eliminate all unnecessary packages and services or re-install the system with the core installation cluster.

- System patches are not up to date. The system has not been patched since it was built. We recommend GIAC keep the operating system and iPlanet application up-to-date with the latest patches and security enhancements. New security patches are released frequently so GIAC should check for new security updates on a regular basis.

- File System Issues. GIAC File system is not protected from being modified by malicious codes. Therefore additional steps should be taken to ensure better file system security.

- Unsecured Network Parameters. Some Network parameters need to be modified to help stop attacks that can break into the server and other corporate servers.

- Open ports and buffer overflow vulnerabilities. There were many open ports and buffer overflow vulnerabilities found on the Web Server. It is recommended to allow only a minimum number of open ports to reduce the number of vulnerabilities on the system.

- Incomplete logging capabilities. The Web Server is not capturing all necessary loggings. The more information that is logged about the server, the more information that can be gained about attackers and type of attack.

- Incomplete security policies. GIAC's only complete security policies include offsite storage of backup tapes and administrative practices. Other security policies such as system backup, patch management, or access control are non-existent, incomplete or inadequate.

- No backup or disaster recovery plans. It is recommended that GIAC prepare a disaster recovery plan to ensure business continuity following any disaster or serious incident.

- Web Server is not in DMZ area. Currently, the Web Server straddles the firewall. We recommend the Web Server be re-located within the DMZ area.

Overall, the state of the system security is very poor. The system is at imminent risk of being broken into and should be taken offline and protected immediately to minimize the company's risk exposure. Given the current poor status of the server, it is recommended that GIAC enterprise do one of the following:

- Eliminate all unnecessary packages and services from the server and apply latest patches. The company might also want to consider bringing a forensics team because it is likely that the Web Server vulnerabilities have already been exploited.

- Re-building the server with the core system support.

Its known that there is no system is truly 100% secure. However, by solving the issues outlined above, the Web Server security risks can be greatly reduced.

2 System Description and Audit Methodology

2.1 Hardware platform and specifications

GIAC's e-business Web Server is built on an ultra 10 SPARC machine. The server is configured with a one 440 MHz processor, 1 GB of RAM, and one internal 8 GB hard drive, one IDE CDROM, and 2 100Base-TX network adapters that provides network connection between corporate network and the internet.

Manufacturer	Sun Microsystem
System Type	Ultra-5_10
CPU	UltraSparc-II Processor, 440 MHz
RAM	1000 MB
Hard Disk Drives	8 GB
CD-ROM drives	1 IDE CDROM
Floppy Drive	1 floppy drive
Tape drives	None
Framebuffer	None
Keyboard	None
Console device	Terminal
Network interfaces	2 100Base-TX network adapters.

2.2 Operating System and version

The sunone Web Server is running on a SunOS 5.9 sun4u sparc system. The Operating System installed on this server is the Solaris 9 with Entire Distribution plus OEM support cluster.

2.3 Role of system

The role of the system is to provide online sales of fortune cookie sayings in the most secure way possible. Therefore, GIAC's e-business operations rely heavily on this server.

2.4 Current Situation

Figure 1.1 shows the current location of sunone Web Server on the corporate network.

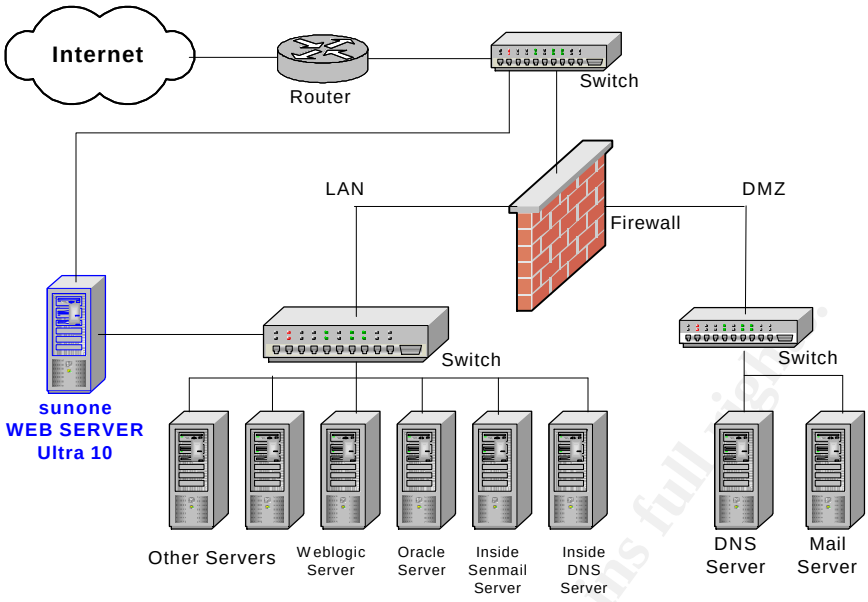

Figure 1.1 GIAC Simplified Network Diagram

From Figure 1.1, we note the followings:

1. The sunone Web Server is located parallel to the outside firewall, thus it is connected to both the Internet and the corporate network. This location poses many risks to the server itself and to the corporate network. Web Server risks can include:

   a. Loss of service by overloading the server with requests (denial of service attacks).
   b. Loss of information such as usernames, configuration or password files.
   c. Loss of control, by not knowing what changes has been made by an intruder.

2. Providing this accessibility to the corporate network leaves the company's confidential information vulnerable to outside attacks. Therefore, if the server was compromised or the system brought down, an attacker can do the following:

   a. Interrupt business operation
   b. Destroy online content
   c. Listen in to or alter transactions
   d. Attack the private network

3. Other risks

   a. Bad publicity especially when an official site is replaced
   b. The system can be used to distribute pirated software

2.5 Additional Tools and Applications

2.5.1 Sun One Web Server

The main software application running on sunone Web Server is the Sun ONE Web Server application (formerly known as iPlanet Web Server) version 6.0 with service pack 2.

The Sun One Web Server provides 2 important security features:

- Administrators can establish encrypted and authenticated transactions between clients and the server through the secure socket layer protocol.

- Access control. The administrator can protect confidential files or directories by implementing access control (viewing, editing, and version control) by user name, password, domain names, or IP address. Access control will be discussed further in detail later on this report.

2.5.2 SSH

SSH encrypts authentication information and data stream. Solaris 9 ships with SSH version 1.0 (protocol support for SSH versions 1.5/2.0), which is based on the BSD-licensed OpenSSH. The "/etc/inetd.conf" file on Solaris 9 sets up many service as listening by default. TCP wrappers 7.6 is also installed with Solaris 9, but needs additional configuring.

2.6 Audit Methodology

OBJECTIVES

Before considering the method of our audit analysis, we first need to clarify our audit objective. Different objectives require different strategies, and hence different methods of system analysis. The objective of the audit is to investigate, assess, and provide recommendations on protecting and securing the sunone Web Server.

METHODOLOGY

The audit performed on GIAC's Web Server includes tests and procedures necessary to accomplish the audit objective. Including:

- Policies and manuals review
- IT staff interview
- Technical Testing using a variety of security tools
- Physical security audit; and
- Disaster Recovery Plans review.

2.6.1 Policy Review

The purpose of the Security Policy Audit is to ensure that GIAC's Web Server security policies are properly aligned with business objective. Policies, in general, define what services should be run, what needs to be protected, who is granted access, what action is allowed and what is not allowed, and which tools or procedures are needed for a specific task. Policies can also help administrators respond effectively and appropriately during security incidents.

GIAC policy review begins with assessing Web Server security procedures and practices. The current policies are analyzed to ensure information security roles and responsibilities, physical security, installations or upgrades, configuration, and administration still represent the current state of the server.

2.6.2 IT Staff Interview

Interviews have been conducted with IT-staff to determine specific information regarding installation and configuration of the Web Server and to determine their understanding and adherence to security policies.

2.6.3 Technical Testing

Technical testing was used to investigate the current system and evaluate its overall security. Testing consisted of using different types of security tools, including: (1) Network Mapping using Nmap utility to check for open ports on the server, (2) Nessus security scanner to audit the Web Server and determine whether bad guys may broken into it, (3) CIS-scan tool to provide easy way to evaluate the Web Server, comparing its configuration settings against the CIS benchmark, and (4) Password Cracking using "John the ripper" password cracker tool.

Two laptops with scanning tools are setup to accomplish the technical testing. As illustrated in Figure 1.2, one laptop with scanning tools is used to scan from outside the corporate network and another laptop from the inside:

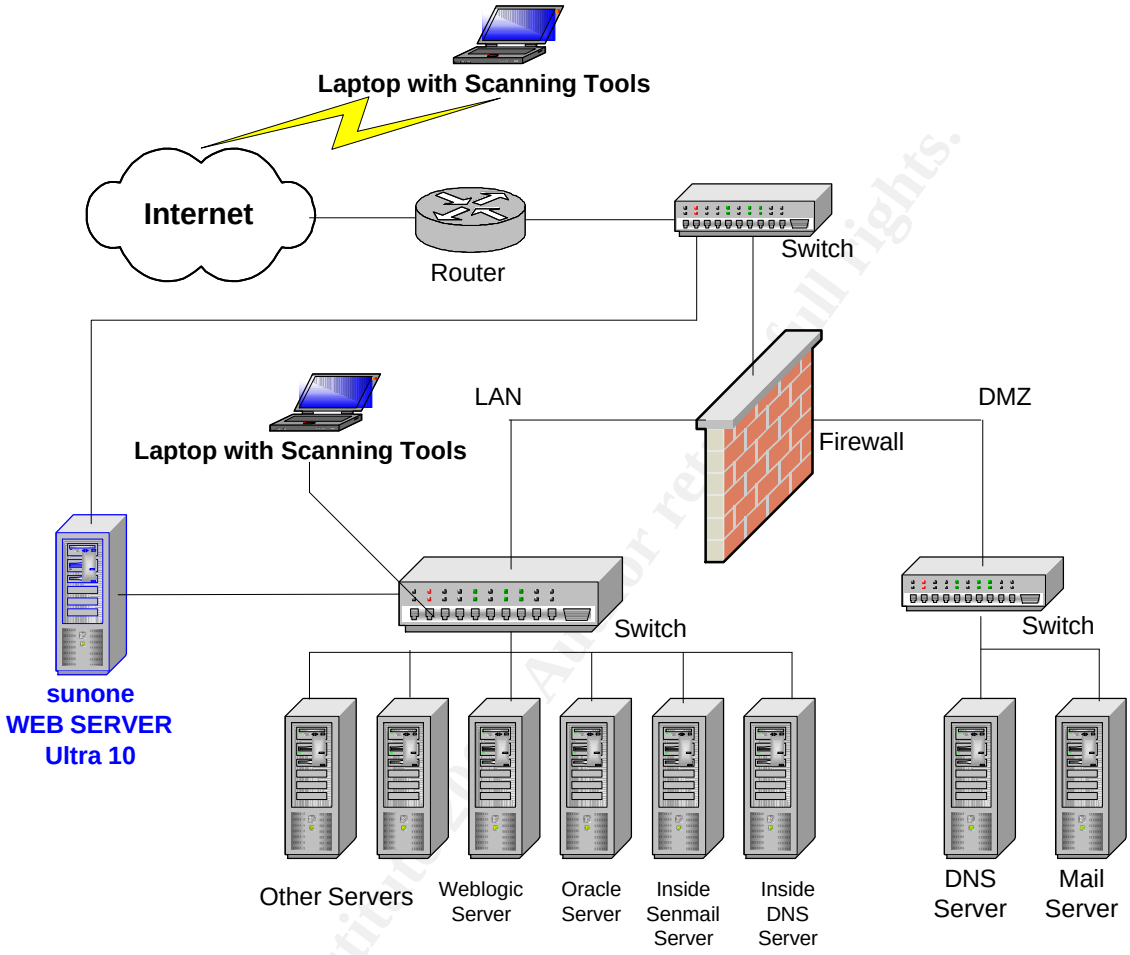

Figure 1.2: Location of laptops with scanning tools.

The results of the technical testing will provide detailed information for most of the existing weaknesses of the system, as well as the depth of the problem.

Nmap version 3.00 was used to scan for active TCP and UDP open ports. Nmap also identifies what RPC service is listening at a given port. Nmap supports many different scan options including TCP (-sT & -sS), UDP, and RPC. Nmap output can be viewed appendix A-5.

In addition, Nessus version 1.2.6 was used to test for various other vulnerabilities. Nessus also has great reporting capabilities with text and graphed HTML output. Not only will it identify vulnerabilities, but it also suggests a solution to those vulnerabilities. For the Nessus scan, the option “Enable all but dangerous plugins” was selected. This option scans the system for known

vulnerabilities and skips others that may damage the system. Nessus output for sunone Web Server is shown in appendix A-6.

2.6.4 Physical Security

As part of the audit, a number of items regarding physical security were inspected, including:

- Is the Web Server located in a secure locked room?
- Is there a proper access given to authorized personnel?
- Is temperature controlled to avoid any equipment damage?
- Is there a UPS on the server?
- Is there a hardware-based or software-based RAID system installed on the system?, and
- Any used modem?

2.6.5 Backup System and Disastor Recovery Plans

Today, it is a standard business practice for organizations to have backup systems that enable data and application recovery for such cases as natural disasters, hardware failure, and deliberate or accidental deletion of data. Without a good backup system and backup policy to set the rules for system backup, an organization might risk losing important data. In addition, no backup solution is reliable unless data is regularly restored to a test location and the backup process is frequently validated and verified.

A verity of issues regarding system backup were looked at, including: backup software used and version, frequency of backup, speed of backups, and off-site storage.

Disaster recovery plan helps ensure business continuity following any disaster or serious incident. The plan should contain:

- Clear, step-by-step instructions needed at the time of recovery,
- Roles and responsibility, and
- Testing and training. Testing should be conducted to ensure critical information is not lost due to a failure.

3 Detail Analysis

3.1 Operating system vulnerabilities

Currently, sunone Web Server runs on a Sun Solaris 9 with Entire Distribution plus OEM support cluster. This distribution is a software group from Sun that contains the entire Solaris 9 release plus additional support for OEMs. The additional components of the Software are not relevant to the role of the server.

The Core System Support cluster is the proper software cluster that should have been initially installed on the server. The Core System Support cluster is a Solaris software group and is the most secure software for the role of the server. This software contains only the minimum software required to boot and run the Solaris operating environment on a system, and hence contains less vulnerabilities.

The current server is built using the Entire Distribution Plus OEM Support instead of only the Core System Support. It is more difficult to identify and remove all unnecessary software packages and operating system vulnerabilities while the system in production. In contrast, it would be easier and more secure to build the Web Server using the core system support, then identify and remove unnecessary packages, eliminate operating system vulnerabilities, re-install all necessary application (such as Sun One Web Server application), and apply patches. Detailed information of installing Solaris Core software is beyond the scope of this audit, however a list of minimum software packages that should be installed is shown at appendix A-1.

3.2 Security patch installation and management

Patches for Solaris exist for most of the flaws identified on the sunone Web Server. Security patches eliminate security vulnerabilities through which attackers can break into the system.

GIAC has no formal policy governing the installation of security patches. GIAC has not been applied any patches since initial installation of the OS. Running the command:

patchadd –p

shows:

“No patches installed”

The recommended security patches for Solaris 9 are available either from Solaris 9 CDs or from http://sunsolve.sun.com site. Sunsolve from Sun Microsystems shows a list of security patches that are required on the system. It is not necessary to install all available patches from Sun. Only that recommended patches and those patches required for specific security problems be installed. Appendix A-2 shows a list of patches that are required on this Web Server.

3.3 Configuration vulnerabilities

The followings show how most of configuration vulnerabilities were found on sunone Web Server:

- "netstat –a" command. The "netstat" command shows network status. The "-a" option is used to show the state of all sockets, all routing table entries, or all interfaces, both physical and logical. Appendix A-3 shows the output of "netstat –a" command.
- CISscan security benchmark. Appendix A-4 shows a list of system vulnerabilities found by CIS-scan tool.
- Information gathering from www.cert.org
- Public white papers and Blueprints

For this audit, configuration vulnerabilities are divided into the following subcategories:

- Unnecessary services and programs,
- File System permissions,
- Kernel Configuration, and
- Logging.

3.3.1 Unnecessary services

Solaris comes with many network services, some of which are not required. There are two main places to configure which services are active: the /etc/inetd.conf file and the /etc/rc.X/ directories.

Attackers can break into the Web Server using ports that are opened by various Unix services, many of which are turned on by default and are not needed for the operation of the Web Server. Any service that listens on a port is a potential security hole, therefore it is necessary to determine what the uses of the Web Server are, turn off any unnecessary services, and monitor connections to necessary services.

- The following services as reported by CIS-scan tool are not needed and should be turned off:

```
telnet not deactivated.
ftp not deactivated.
rsh (shell) should be deactivated.
rlogin (rlogin) should be deactivated.
tftp is deactivated.
network printing should be deactivated.
rquotad is not deactivated.
llc2 not deactivated.
uucp not deactivated.
slpd not deactivated.
PRESERVE not deactivated.
bdconfig not deactivated.
wbem not deactivated.
afbinit not deactivated.
ncalogd not deactivated.
mipagent not deactivated.
sysid.net not deactivated.
sysid.sys not deactivated.
autoinstall not deactivated.
cachefs.daemon not deactivated.
cacheos.finish not deactivated.
power not deactivated.
NFS Server script nfs.server not deactivated.
NFS script nfs.client not deactivated.
NFS script autofs not deactivated.
rpc rc-script (rpcbind) not deactivated.
ldap cache manager not deactivated.
lp not deactivated.
spc not deactivated.
volume manager not deactivated.
Graphical login not deactivated.
snmp daemon should be deactivated.
Coredumps aren't deactivated.
CDE-related daemon rpc.ttdbserverd not deactivated in inetd.conf.
CDE-related daemon fs.auto (port fs) not deactivated in inetd.conf.
CDE-related daemon kcms_server not deactivated in inetd.conf.
kerberos net daemon ktkt_warnd not deactivated in inetd.conf.
kerberos net daemon gssd not deactivated in inetd.conf.
```

- **Other unnecessary services**

Nessus reveals other unnecessary services that are vulnerable to buffer overflow attacks. An attacker can gain root privileges through exploitation of these services. The most severe buffer overflow threats on sunone Web Server can be caused by the following services:

  - dtspcd service,
  - cmsd RPC service,
  - sadmin RPC service,
  - tooltalk RPC service, and
  - rpc.walld RPC service.

- **Unnecessary “r” remote commands**

In general, the "r" commands present a security exposure to a machine. This is because they use a weak authentication method that can be exploited. If some intruders can look at the network traffic, they can get information like passwords, or just get useful information on logged-in users. The following r-commands are not needed on the server and should be disabled:

```
/usr/bin/rlogin
/usr/bin/rsh
/usr/bin/rcp
/usr/bin/remsh
/usr/bin/rusers
/usr/bin/rwho
/usr/bin/rdate
/usr/bin/rup
/usr/bin/rdist
/usr/bin/rpcinfo
/usr/bin/ruptime
```

Unix Secure Shell (SSH) program provides a more secure method of providing remote login access and file transfer. Once a secure version of SSH has been installed, all “r” remote commands should be removed or renamed so they cannot be invoked by their original name.

- **Unnecessary startup files in /etc/rc2.d and /etc/rc3.d**

As part of the minimization process, it is important to reduce the number of processes and services that might have potential vulnerabilities. There are also services that may allow a system to be compromised due to incorrect configuration. GIAC’s Web Server has the followings unnecessary startup files in /etc/rc2.d and /etc/rc3.d:

Under /etc/rc2.d:

S30sysid.net,
S71ldap.client,
S71sysid.sys,
S71rpc,
S72autoinstall,
S73cachefs.daemon,
S73nfs.client,
S74autofs,
S76nscd,
S80lp,
S88sendmail,

S89PRESERVE,
S99dtlogin,

Under /etc/rc3.d:

S15nfs.server,
S76snmpdx

The “init” process invokes the above startup files during the boot process. Some of these scripts are not needed. To stop a particular script from starting during the boot process, either replace the capital “S” at the beginning of each script name with a small “s” or remove the script totally by using “rm” command.

3.3.2 File System

The file system must be protected from being modified by malicious code from hacking scripts. The file system must also prevent users or hackers from placing unauthorized set-UID binaries on the system. Some file systems should either be mounted as a "nosuid" or "read only".

The “/etc/vfstab” file on the Web Server reveals the following file system information:

#device #to mount options	device to fsck	mount point	FS type	fsck pass	mount at boot	mount
#						
fd	-	/dev/fd	fd	-	no	-
/proc	-	/proc	proc	-	no	-
/dev/dsk/c0t0d0s1	-	-	swap	-	no	-
/dev/dsk/c0t0d0s0	/dev/rdsk/c0t0d0s0	/	ufs	1	no	-
swap	-	/tmp	tmpfs	-	yes	-

The following are problems with the “/etc/vfstab” file:

- There is no separate “/usr” file system. The /usr file system contains all of the critical OS programs. File systems shall either be mounted as “nosuid” or “ro” (read-only). If there were a separate usr filesystem, it needs to be mounted as read-only since usr filesystem contains all of the set-UID programs.

- There is no separate “/var” file system. Hence if the “/var” directory becomes full by logs, the whole “/” root file system will be full and therefore no one will be able to access the system.

- The “logging mount option” is not being used. The “logging” mount option enables faster file system recovery and system boot. After a crash, a filesystem can be restored in a matter of seconds or minutes as compared to possibly minutes or hours with the “fsck” command.

Umask

The default permissions on many files are somewhat insecure. Having incorrect permissions on any file or program that get executed invites their replacement by “trojan horse” programs. A Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage or even try to get passwords from the system and pass it along to an intruder.

The “/etc/default/init” file shows the value of CMASK as 022 which creates group and world readable permissions. This can be a problem because it allows group and world permissions to read the contents of system files. CMASK value of 077 is more secured and does not allow group or world to read/write/execute files.

Fix-modes

Finally, CIS-scan reveals that “fix-modes” has never been run:

```
Negative: 9.4 Fix-modes has not been run here
Negative: 8.7 User adm 's homedir is group writable!
Negative: 8.7 User lp 's homedir is group writable!
```

Fix-modes is a set of scripts that make the filesystem modes more secure.

3.3.3 Kernal Configuration

Solaris kernel has many parameters that can be modified to reduce the number of security vulnerabilities on the system. A list of these parameters can be obtained by typing: “ndd -get driver_name \?”. To protect the system from different type of attacks such as SYN floods, ARP floods, ARP spoofs, etc, we need to check the followings:

IP Parameters

- Since this machine uses IP based networking, it can be used as a router by attackers. Attackers could route packets through this machine to other machines on the network. IP forwarding on this Server is turned off to prevent this occurrence.

  #/usr/sbin/ndd ip_forwarding
  0

- Since this machine has two interfaces, we need to prevent packets coming through one interface that are destined for another interface. This can prevent host spoofing. Spoofing is done when a machine mimics another machines IP address by which it tricks the firewall into believing it is an authorized user.

  #/usr/sbin/ndd /dev/ip ip_strict_dst_multihoming
  0
  We need to set the ip_strict_dst_multimhoming to 1:
  #/usr/sbin/ndd –set /dev/ip ip_strict_dst_multihoming 1

- The forwarding of directed broadcasts is disabled. The directed broadcast can be exploited to generate high amounts of network traffic. The directed broadcasts are the basis for the “smurf” attacks.

  Smurf attack is a network-level attack against hosts. A perpetrator sends a large amount of ICMP echo (ping) traffic at IP broadcast addresses, all of it having a spoofed source address of a victim. If the routing device delivering traffic to those broadcast addresses performs the IP broadcast to layer 2 broadcast function noted below, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply each, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, there could potentially be hundreds of machines to reply to each packet.

  # /usr/sbin/ndd /dev/ip ip_forward_directed_broadcasts
  0

- The following command prevents the system from forwarding any IP datagrams that have the source routing option activated. IP datagrams allow attackers to get around some security rules.

  #/usr/sbin/ndd /dev/ip ip_forward_src_routed
  0

TCP Parameters

- “SYN Flooding” occurs when an attacker initiates hundreds of TCP connections to a machine but fails to complete the standard TCP “three-way-handshake”. This will cause the machine to stop accepting new connections due to the system’s buffer for pending connections.

  One-way of preventing the TCP SYN attack is to shorten the value of the abort timer parameter. The default abort timer interval value of this parameter is 180 seconds:

#/usr/sbin/ndd /dev/tcp tcp_ip_abort_cinterval 180000

The abort time should be set to 60 seconds instead:
#/usr/sbin/ndd –set /dev/tcp tcp_ip_abort_cinterval 60000

- Another way to prevent the TCP SYN attack is to lengthen the TCP connection queue. The TCP connection queue is set to a greater value to prevent the server from refusing connections due to small buffer sizes:

  #/usr/sbin/ndd /dev/tcp tcp_conn_req_max_q0
  1024

ARP Parameters

- The ARP cache lifetime is determined by the kernel parameter "arp_cleanup_interval". This parameter governs the cleanup interval for the IP route cache. The default Solaris value is twenty minutes. Tuning down this value can help prevent some ARP spoofing attacks at the cost of more ARP traffic on the LAN and possible reduced performance. This will slow down attackers however will not stop them.

  #/usr/sbin/ndd –set /dev/arp arp_cleanup_interval 60000

ICMP Parameters

- ICMP broadcast query allows an attacker to probe the network and set a range for further probes. Broadcast ICMP mask requests need to be checked.

  #/usr/sbin/ndd /dev/ip ip_respond_to_address_mask_broadcast
  0

- The ICMP timestamp broadcast also allows for more probes.

  #/usr/sbin/ndd /dev/ip ip_respond_to_timestamp
  1

  The ICMP timestamp requests should be disabled:

  #/usr/sbin/ndd –set /dev/ip ip_respond_to_timestamp 0

Other Kernel Configurations

- Other kernel configurations that require modifications include:

```
Negative: 4.4 ip_send_redirects isn't set to 0.
Negative: 4.4 ip_ignore_redirect isn't set to 1.
```

```
Negative: 4.4 ARP timer (ip_ire_arp_interval) should be at most
60000
Negative: 4.5 TCP sequence numbers not strong enough.
```

3.3.4 Logging

The more information logged about the systems, the more information can be detected about an attacker. The following issues are related to logging capabilities at sunone Web Server:

- By default, Solaris doesn't capture file messages from auth.info. The CIS-scan reports the following about the auth.info:

  Negative: 5.1 syslog does not permanently capture auth messages.

- "loginlog", as reported by CIS-scan, doesn't exist to track failed logins. The "/var/adm/loginlog" logs consecutive failed login attempts.

- "Sulog" is also not found on the Web Server. The "/var/adm/sulog" logs all "su" attempts, both successful and failed.

- By isolating the "/var" partition during system installation, GIAC can protect the root partition from overcapacity.

Two logging options are beyond the standard logging services are important but have not been installed on the server. SUNWaccr and SUNWaccu are two packages needed to run process accounting. Running the command "pkginfo" with the package name shows if the package is installed on the system:

#pkginfo SUNWaccr
information for "SUNWaccr" was not found

pkginfo SUNWaccu
information for "SUNWaccu" was not found

Both system accounting and process accounting keep track of extra information on the system but this might generate huge audit logs and also can cause performance issues.

3.4 Access Control

GIAC enterprise does not want every external or internal user to have access to their Web Server and data. To limit access to authorized users, the Web Server needs to have assigned access permissions. In general, access controls refer to the level of grant or deny permissions within an organization. It is important for

GIAC enterprise to restrict their customers, vendors, suppliers, and employees to only those services for which they should have access. Access control can be applied in two areas: (1) Network access control; and (2) User access control.

3.4.1 Network Access Control

The first line of defense for GIAC enterprise access control is the Firewall. Currently, GIAC enterprise sunone Web Server straddles a PIX firewall. The sunone Web Server could have been more protected if it was setup behind the firewall. The firewall can provide secure access and allow only valid users to the required network resources needed. It can also be setup to block packets for all services for sunone except HTTP and HTTPs

The current PIX firewall at GIAC enterprise can provide different types of access control includeing tracking access, advanced logging, reporting and alerting, connection accounting, security alerting, and protection against common attacks such as IP spoofing and denial of service.

Network access control involves using encryption mechanism to allow access to the Web server. Access to the sunone Web Server should be done through a secure logon process.

SSH

OpenSSH has not been installed on this server. However, the current type of "ssh" on this machine is "Sun_SSH_1.0" protocol versions 1.5/2.0. No security alert has been issued regarding this version of SSH. However, the Solaris 9 SSH is based on a really old version of OpenSSH. It is also noted that GIAC administrator is not familiar and frustrated with the lack of information about Sun SSH. The OpenSSH package from Sun can be found at Sun freeware site, http://www.sunfreeware.com.

3.4.2 User Access Control

By default, Solaris installations come with potential security problems. The most basic and important step in securing the system is to set a hard-to-guess password. Unfortunately, this Web Server was found to have a weak root password. Running the "John the Ripper" version 1.6 password cracker utility detected the root password within seconds.

Ran "John the Ripper" with:

```
# ./unshadow /etc/password /etc/shadow > TESTFILE
# ./john TESTFILE
Loaded 1 password (Standard DES [32/32 BS])
```

```
password          (root)
guesses: 1  time: 0:00:00:00 100% (2)  c/s: 32769  trying: cedic3 -
guitar3
```

Currently, the Web Server does not have “sudo” installed. System administrators should always login as a user other than root, then either use “su” or “sudo” to become root. “Sudo” command allows a system administrator to give certain user(s) or group of user(s) the ability to run some commands as root while logging all information related to commands and arguments executed.

Another potential security problem found on this Web Server is that there are several unneeded users -uucp, adm, nuucp, lp, smtp, listen - that get created during the installation. System accounts -adm, daemon, bin - should have their shell be set to /dev/null to block access.

CIS-scan revealed that eeprom isn’t password protected. Setting “eeprom security-mode=full” will prompt for a password before boot commands are executed. This means this setting will prevent the machine from rebooting without a human present however it will prevent attackers who have physical access to the system from booting from a CD and compromising system security. Setting “eeprom security-mode=command” on the other hand forces the boot process to prompt the administrator for a password whenever any EEPROM command is issued other than a normal reboot (including “boot –r” and “boot –s”).

Finally, strict access controls should also be placed on the sunone Web Server application system source code, compilers, and scripting facilities. This will ensure that the system's access control mechanisms cannot be bypassed through code subversion.

3.5 Security Tools

Optimizing the security of the sunone Web Server cannot be completely achieved without the use of all necessary security tools. The system lacks important security tools, all of which are freely available on the Internet, that accomplish different security checks. These security tools include:

- fix-modes that sets appropriate permissions on various OS files and directories,
- Open-SSH and TCP Wrappers which are critical for network security,
- NTP (Network Time Protocol), which is not a security tool by itself but might be used in an investigation by proving time accuracy and providing time synchronization among systems.
- Tripwire or AIDE, which are tools that will inform the administrator if certain files on the system have been modified.

- Logsentry (formerly known as Logcheck) and Swatch tools that automatically monitor system log files and report "interesting" events to the administrator.

3.6 System Security Monitoring

Hardening sunone Web Server with all security measures is also not enough to ensure system security. It is important to monitor this system continuously for signs of intrusion or possible attacks.

Along with Firewall logging information and automatic notification, GIAC uses a monitoring tool “intermapper” that informs the system administrator of the status of all servers and services. This monitoring utility provides capabilities such as e-mail notification and paging notification.

3.7 Risks from installed third-party software

Third party software application installed on this Web server includes Legato Networker.

3.7.1 Legato Networker

Legato Networker Backup Software currently running outdated version 5.5.1 Build.115 Networker client for Solaris. This release causes a reverse domain name system lookup to fail and thus can cause un-authorized access and may allow non-administrators to view the administrator list for a network server.

3.8 Administrative practices

The system administration staff at GIAC consists of four administrators and four computer operators. Two of the administrators specialize in UNIX technologies and are responsible for installing, monitoring, and maintaining the Sunone Web Server and other servers. Computer operators provide 24-hour support for users and help notify administrators of problems with servers during non-working hours.

GIAC has clear roles and responsibilities as well as good written policies of who, when, and what should be done in terms of managing the network and other systems. GIAC ensures each system administrator and computer operator understand these policies.

3.9 Identification and protection of sensitive data on the host

GIAC's human resources department conducts training and provides awareness programs to ensure personnel who interact with IT systems are well aware of the importance of corporate data. Sensitive data are not stored locally on sunone Web Server. GIAC uses this Web Server to process data only.

GIAC's sensitive data is stored and transferred through an encryption mechanism to a more secured database system. To allow secure inquiries from the web server to other servers on the network, only specific ports should be open.

3.10 Protection of sensitive data in transit over the network and Internet

Web Servers are attractive targets for attackers because of their public exposure. To protect GIAC sensitive data from unauthorized users, this web server uses the HTTPS protocol (Hypertext Transfer Protocol over Secure Socket Layer) to encrypt the communication of passwords and other data between users' web browsers and GIAC's Web Server. This level of encryption ensures that sensitive data is not intercepted.

3.11 Backup policies and disaster preparedness

Currently, GIAC does not have a complete system backup policy, only a policy for Archive backup and Storage procedure. The archive and Storage procedure covers the routines that responsible individuals should take to ensure safe transfer and retrieval of backup media.

GIAC also lacks a complete documented disaster recovery plan. However, the system administrator keeps an informal log of critical information to be used to recover the Web Server in case a disaster occurs. A script is used to collect this critical information by using some commands - showrev, df –kl, vfstab, ifconfig –a, prtdiag –v, etc. The script is run every 4 months and the print out is saved in the same server room as the Web Server.

The problems with the disaster recovery plan at GIAC enterprise are as follows:

- Upper management did not make the disaster plan a requirement and formal,
- The information gathered by this script is not complete,

- The printout made from the script is kept in the same room where the Web Server is located and there is no offsite backup copy.

GIAC enterprise has adequate physical security and computer system controls in place to ensure that the data center is adequately safeguarded. The server room includes:

- Adequate UPS to conditions the power and allows time for proper shutdown, and
- A redundant air condition system.

Physical security at the data center is above standard. In addition, detailed system downtime reports are maintained allowing IT staff to correct systemic problems.

3.12 Other issues

3.12.1 iPlanet Sun One Web Server (iWS)

The detailed discussion of securing iPlanet Sun One Web Server application is beyond the scope of this audit. However, the following brief security issues are important to the Sun One Web Server:

- GIAC's Sun One Web Server is currently at version 6.0 with service pack 2b. The current version SP2 contains security vulnerabilities that allow intruders to cause buffer overflow. It is important that the Web Server Application stays at the latest patch level. The latest service pack for Sun One Web Server 6.0 is Service Pack 5 containing updated security vulnerability fixes. The patch needs to be applied before any configuration change is made to the application, otherwise the changes made by the security patch might be lost and the system could be at risk.

- Sun One Web Server can also be customized to log information regarding application access. By default, the application does not include all necessary logs. By going to the "log Preferences" tab, we can select "Record IP Addresses" option instead of the default "Domain Names". Also, the "Use Common Logfile Format" should be changed to "Only log" and then select "HTTP header" and the "HTTP header," checkboxes.

- Certain default files that come with the application are not needed and they might allow an attacker to learn more about the system. The following files are placed in the DocumentRoot directory and need to be removed:

  index.html,

banner.html, and
launch.html.

- The web server directory access should be limited by “chroot”. As the iPlanet documentation reads, a full directory structure is required by iPlanet Web Server under the alternative root directory. “chroot” is a UNIX utility that redefines a program root directory. Therefore, if an attacker breaks into the Web Server, he won’t be able to see all the files on the system thus limiting him with only to the “chroot”-ed area with fewer commands to execute. “chroot installation is beyond the scope of this audit.

- Finally, Sun One Web Server allow us to control who can access files or directories by creating a hierarchy of rules called Access Control Entries (ACEs). The Sun One Web Server has one ACL file that contains multiple ACLs by default. Using ACLs, we can allow or deny access based on who is making the request, where the request is coming from, when the request is happening, and what type of connection is being used.

4 Critical Issues and Recommendations

4.1 System built with Solaris 9 with Entire Distribution

It is sometimes difficult to determine the minimal set of operating system components to install. Therefore, some system administrators end up installing a system with the Entire Distribution Cluster. This makes it easier for them to get the system up and running, on the other hand, it makes it almost impossible to secure the system.

The majority of system vulnerabilities are caused by exploitations of security holes found within the operating system itself. One way to reduce system vulnerabilities is to minimize operating system components.

Currently, the sunone Web Server runs on a Sun Solaris 9 with Entire Distribution plus OEM support cluster. The “Entire Distribution Plus OEM Support” cluster is a software group that contains the entire Solaris 9 release. The additional components of this Software are not relevant to the role of this server; therefore only serve to increase the likelihood of exploitation. We recommend GIAC enterprise to do one of the following:

- Identify and eliminate all unnecessary packages that are currently installed on the server however this process is difficult and requires lots of caution. The company might want also to bring-in a forensics team because it is likely that the Web Server vulnerabilities have already been exploited.
  or

- Re-installing the server with only the core system support. This option installs the minimum amount of packages necessary to run Solaris. The list of packages needed to install the core system support are listed in appendix A-1.

GIAC can also use YASSP to help harden sunone Web server. YASSP, found at http://www.yassp.org, is a Solaris Security package that installs a version of Solaris with good host security without having to spend a great deal of time hardening the system by hand. The package establishes several security settings:

- Network services are disabled,
- File ownership and protection weakness are resolved,
- System logging is enabled,
- The network stack is tuned and several system parameters are set, and
- Runs the fix-modes script.

4.2 Running Unnecessary Services

The sunone Web Server by default has numerous services than required for its role. GIAC enterprise needs to disable all unnecessary services to prevent exploitation of their vulnerabilities. GIAC should either uninstall unnecessary services or disable the services and remove the corresponding files from the server.

- "Inet" services are not required for GIAC enterprise Web Server. Removing the "/etc/inet/inetd.conf" or disabling inetd will eliminate these network services.

  To Disable "Inetd":

  In the /etc/init.d/inetsvc, comment out the line that starts the inetd:

  /usr/sbin/inetd –s

  to

  #/usr/sbin/inetd –s

  Disabling "inetd" will eliminate many unnecessary services that were reported by the CIS-scan.

- Other important issues include eliminate any unnecessary open network ports. Running "netstat –a" will show processes that are listening on the network, and thus subject to exploit by anyone on the Internet. Open network ports are also shown by nmap output at appendix A-5.

- "r"-commands present a security exposure to a machine because because of their weak authentication method. SSH is more secure at accessing remote system than "r" commands. The following "r"-commands are listed under "/usr/bin" and should be disabled: rlogin, rsh, rcp, remsh, rusers, rwho, rdate, rup, rdist, rpcinfo, and ruptime.

- There are also services that may allow a system to be compromised due to incorrect configuration. GIAC's Web Server has the followings unnecessary startup files in /etc/rc2.d and /etc/rc3.d: S30sysid.net, S71ldap.client, S71sysid.sys, S71rpc, S72autoinstall, S73cachefs.daemon, S73nfs.client, S74autofs, S76nscd, S80lp, S88sendmail, S89PRESERVE, S99dtlogin, S15nfs.server, and S76snmpdx.

4.3 System Patches are not up to date

New security vulnerabilities are being discovered all the time. In response, upgrades and "hotfixes' are provided in the form of a patch or "hotfix" by vendors. A patch is a change to a software product that corrects a deficiency or adds an enhancement.

The first step in implementing security at GIAC starts with updating sunone Web Server with the latest recommended and security patches. These patches can be obtained through the World Wide Web or anonymous ftp at sunsolve.sun.com. It is also necessary for GIAC to stay up-to-date with security alerts and fixes. Two sources for security alerts can be found at: Security Focus (http://www.securityfocus.com) and SAN's Security Alert Consensus service (http://www.sans.org/newsletters/sac/).

Running "patchadd –p" command on sunone Web Server reveals that the operating system has no patches installed.

- **Recommended patch cluster**

First step in ensuring security of sunone Web Server is to install the Recommended patch cluster. All security patches will be listed in both the security patch section and recommended patch section. Any security patches not included in the recommended section are denoted in the security section with an asterisk. Solaris 9 Recommended patch cluster can be installed as follow:

1. Obtain Solaris 9 recommended patch cluster from http://sunsolve.sun.com. The recommended patch cluster name for Solaris 9 release is: 9_Reommended.zip
2. Once downloaded, the cluster can be extracted by issuing the following:
   # unzip 9_Recommended.zip
3. Bring the system into single user mode if possible.
4. Check that there is enough disk space. If the patch script is run and there was not enough disk space while patching, the system might end up in a non-bootable state. The script will check to make sure that there is a reasonable disk space but it is always safer to manually check for disk space.
5. cd to the directory where the patch package was unpacked and run:
   # ./install_cluster (to install and make backups of changes)
   or
   # ./install_cluster –nosave (to install and not backup changes)

   If the system is low on disk space, using "-nosave" option is a better way. If there is enough space, it is better to save a backup just in case something unexpected occurs.

6. During patch cluster installation, some errors might show up as “Failure code some_number”, however this is almost always ok. Failure code “8 indicates the application to which the patch relates is not installed. Failure code “2” indicates the patch has already been installed. Only when the Failure code indicates the patch was not successfully installed should be a concern.
7. Check the logfile if more detail is needed. More details about the causes of failure can be found in the detail logfile: more /var/sadm/install_data/install_log
8. Reboot the system

- **Security Patches**

All security-related patches are not always included in the recommended patch cluster. Therefore it is necessary to be aware of the security-related issues. As indicated above, any security patches not included in the recommended section are denoted in the security section with an asterisk. PatchReport, for different release clusters, available from sunsolve.sun.com has a section entitled “Patches Containing Security Fixes.” This section should be reviewed to see if security patches that are not included in the recommended section should be installed on the system. Appendix A-2 shows a list of both recommended and security related patches.

Finally, any additional software on the system should be kept up to date. The current version of iPlanet Sun One Web Server SP2 contains security vulnerabilities that allow intruders to cause buffer overflow. GIAC is recommended to update this software to the latest release.

4.4 File System and Access Control

The followings are the sunone Web Server File system issues and recommendations:

- Looking at the “/etc/vfstab”, it is apparent that the system has not been configured or planned to operate as a Web Server. A separate “/usr” or “/var” file systems were not created. It is recommended the Web Server have a separate partition for “/usr” and “/var”. The ‘/var” should be large enough to handle logging information.

- The “logging” mount option settings in the “/etc/vfstab” is not used. It is recommended this mount option be used to enable faster system boot and file system recovery.

- The CIS-scan tool shows that “fix-modes” has not been run on the server. We recommend GIAC install and use this tool to correct file and directory protections. “Fix-modes” is a set of scripts that makes the filesystem modes

more secure. This is accomplish by removing group and world write permissions of all files, devices, and directories listed in "/var/sadm/install/contents". "Fix-modes" changes can be undone using the audit trails.

- The system root password has a very weak password. The system root password was cracked within seconds of running the "John the Ripper" tool. We recommend that GIAC's system administrator to strengthen root password by using long, complex password including caps, numeral and unprintable characters. GIAC should run the "John the Ripper" tool and change the root password regularly to verify that the password is not weak.

4.5 Network Parameters

Some network parameters need to be updated to provide a more secure network operations. Doing so will help prevent attacks such as SYN Floods, Mapping and Smurfing, ARP spoofings, etc. Creating the following script is the best way to change sunone Web Server default kernel parameters:

```
# vi /etc/init.d/nddconfig

/usr/sbin/ndd -set /dev/tcp tcp_conn_req_max_q0 8129
/usr/sbin/ndd -set /dev/tcp tcp_conn_req_max_q 1024
/usr/sbin/ndd -set /dev/tcp tcp_ip_abort_cinterval 60000
/usr/sbin/ndd -set /dev/tcp tcp_strong_iss 2
/usr/sbin/ndd -set /dev/tcp tcp_rev_src_routes 0
/usr/sbin/ndd -set /dev/arp arp_cleanup_interval 60000
/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp 0
/usr/sbin/ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
/usr/sbin/ndd -set /dev/ip ip_respond_to_address_mask_broadcast 0
/usr/sbin/ndd -set /dev/ip ip_forward_directed_broadcasts 0
/usr/sbin/ndd -set /dev/arp arp_cleanup_interval 60000
/usr/sbin/ndd -set /dev/ip ip_ire_flush_interval 60000
/usr/sbin/ndd -set /dev/ip ip_ire_arp_interval 60000
/usr/sbin/ndd -set /dev/ip ip_ignore_redirect 1
/usr/sbin/ndd -set /dev/ip ip_send_redirects 0
/usr/sbin/ndd -set /dev/ip ip_forward_src_routed 0
/usr/sbin/ndd -set /dev/ip ip_forwarding 0
/usr/sbin/ndd -set /dev/ip ip_strict_dst_multihoming 1
:wq!

#
#
# chown root:root /etc/init.d/nddconfig
# chmod 744 /etc/init.d/nddconfig
# ln -s /etc/init.d/nddconfig /etc/rc2.d/S69nddconfig
```

Also, creating "/etc/notrouter" file prevents the system from starting "in.routed" or "in.rdiscd" daemons that enable dynamic routing.

4.6 Open Ports & Buffer Overflow Threats

A number of serious security issues have been found on sunone Web Server. The most dangerous of these issues include un-necessary open ports and buffer overflows threats on some services. Appendix A-5 shows a list of open ports on sunone Web Server. Unused open ports should be disabled. Routers or firewall configurations should allow incoming connections to only the required ports.

Nessus output, appendix A-6, shows a list of security holes that may cause buffer overflows. All vulnerabilities should be fixed/updated, and then rescanned to verify that al vulnerabilities were taken care of. Once all vulnerabilities are eliminated, the rescanned results can be used for future reference.

Finally, adding the following two lines to the "/etc/system" file will help some buffer overrun attacks:

set noexec_user_stack = 1
set noexec_user_stack_log = 1

4.7 Logging & Monitoring Mechanisms not Optimized

By default, Solaris doesn't capture file messages from "auth.info". Therefore, it is recommended to update the syslog.conf to allow this feature.

Two important logging features -sulog and loginlog - were not found on the Web Server. The "/var/adm/sulog" logs all "su" both successful and failed attempts. This feature monitors attempts that try to gain root access on the system. The "/var/adm/loginlog" logs consecutive failed login attempts. The "loginlog" logs a user with more than 5 consecutive failed logging attempts. To enable "sulog" and "loginlog", we only touch " /var/adm/loginlog" and "/var/adm/sulog". Both files must be chmod 640 as they contain sensitive information.

While the Web Server operating system and the Sun One Web Server application have some mechanisms for logging, these mechanisms do not provide sufficient information such as attacks intended to probe the Web Server for specific vulnerabilities. Other programs such as "Tripwire" and "Logsentry" provide additional important information for analyzing and detecting signs of intrusion. "Tripwire" and "Logsentry" automatically monitor systems and logs and report problems to the administrator via e-mail. "Logsentry", formerly known as LogsCheck, is designed to scan the huge volume of logging for unusual activity. "Tripwire" allows the administrator to take a snapshot of the critical files on the system and alerts him when those files have been changed.

4.8 Incomplete or lack of Security Policies

The purpose of the security plan should provide an overview of the security requirement of the Web Server. This plan should also define responsibilities and expected roles of all individuals who access the system. In order for this plan to reflect the protection of the server, top management acceptance is also required.

During the audit, it was noticed many security policies do not exist. The absence of these security policies may result in a compromise of GIAC's level of security. It is recommended that GIAC prepare a security policy for each critical area of the Web Server.

4.9 No Backup or Disaster Recovery Plans

GIAC does not have a complete system backup or disaster recovery plans. The archive and storage policy by itself is not enough. GIAC should have policy that cover other important information regarding system backups such as, responsible individuals, platforms involved, scheduling, restoration, testing of backup system, on-site backup, offsite backup, etc.

The primary objective of disaster recovery plan is to enable GIAC to survive a disaster and reestablish normal business operations. In order to survive, GIAC must ensure that critical operations can resume normal processing within a reasonable time frame. The disaster recovery should contain contingencies for replacement for hardware, re-installation of software, and the recovery of data.

4.10 Web server not in DMZ

The Web Server should be placed within a Demilitarized Zone (DMZ). DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. The DMZ outer and inner firewall should be set to allow http access on ports 80 and 443. Any configuration changes to the Web server from the local network will have to be done through SSH.

4.11 Other Issues and Recommendations

- GIAC enterprise has upgraded their server to Solaris 9 release not so long ago. Major operating system upgrade such as Solaris 9 should not be accomplished in less than a year period of the release date. This is because most the new major releases that introduce new features also have the tendency to introduce new bugs. Within a year timeframe, most of bugs that

comes with the new release should have been mostly eliminated. At that time, the upgrade can be accomplished on a non-critical machine and evaluated.

- Increase level of security awareness among users. Security should be considered a responsibility of all company employees. Educated users are less likely to cause security breaches or take down the server.

- Add a Development Server on the interior network.

    - Users update the Development Server first.
    - The Development Server replicates the changes to the external Web Server.
    - The Development Server decreases the impact of hacks on the Web Server (but does not prevent them).

References

Pomerantz, Hal Solaris Security Step by Step v. 2.0, SANS Institute, July, 2002 San Diego, California.

Paul A. Watters and Paul Watters, Solaris 9: The Complete Reference, Aprill 2002.

Gregory, Peter Solaris Security: For System Administrators Prentice Hall August 1999

Noordergraaf, Alex and Watson, Keith Solaris Operating Environment Security: Sun BluePrints Online December 2002 Sun Microsystems. Retrieved from Web dated December 2002.

Noordergraaf, Alex Minimizing the Solaris™ Operating Environment for Security. Sun BluePrints Online November 2002 Sun Microsystems. Retrieved from Web dated December 2002.

Noordergraaf, Alex and Watson, Keith Solaris Operating Environment Network Settings for Security Sun BluePrints Online December 2000 Sun Microsystems: Retrieved from Web dated December 2002.

Weise, Joel and Martin, Charles Data Security Policy - Structure and Guidelines Solaris Operating Environment Network Settings for Security Sun BluePrints Online December 2001 Sun Microsystems: Retrieved from Web dated December 2002.

Spitzner, Lance Armoring Solaris Preparing Solaris for a firewall, Preparing Solaris 8 64-bit for CheckPoint FireWall-1 NG Online July, 2002 Retrieved from Web dated December 2002.

Noordergraaf, Alex and Watson, Keith Solaris™ Operating Environment Minimization for Security: A Simple, Reproducible and Secure Application Installation Methodology December 1999 Sun Microsystems. Retrieved from Web dated December 2002.

Farinas, Edmundo Security Consideration for the iPlanet Enterprise Web Server on Solaris. February 03, 2002. SANS SECG. Retrieved from web dated December 2002.

Electronic Reference. Security Bulletin Archive. Sun Security Bulletins Retrieved from Web dated December 2002.

Electronic Reference. Sun Essentials Guide: Security Sun Microsystems Retrieved from Web dated December 2002.

Electronic Reference. Configuring Sun Solaris as a Web server CERT Coordination Center. Retrieved from Web dated December 2002.

Landrum, Darrell Web Application and Databases Security SANS Institute April 2001, Retrieved from Web dated December 2002.

Electronic Reference http://www.nessus.org Retrieved from Web dated December 2002.

Electronic Reference http://www.insecure.org/nmap Retrieved from Web dated December 2002.

Electronic Reference Disaster Recovery: Best Practices White Paper Cisco April 2002. Retrieved from Web dated December 2002.

Electronic Reference Sunsolve Online Sun Microsystems: December 2002. Retrieved from Web dated December 2002.

Electronic Reference Signed Patches Administration Guide Sunsolve September 2002. Retreived from Web dated December 2002.

Electronic Reference Network Security Policy: Best Practices White Paper Cisco December 2002. Retrieved from Web dated December 2002.

Electronic Reference Release Notes for iPlanet Web Server, Enterprise Edition docs.sun Sun Microsystems. April 2002. Retrieved from Web dated December 2002.

Electronic Reference Release Notes for Sun Open Net Environment Sun One Web Server at docs.sun Sun Microsystems. April 2002. Retrieved from Web dated December 2002.

Electronic Reference The Study on the Vulnerabilities of Operating Systems Security Writers Guild 2002. Retrieved from Web dated December 2002.

CERT Advisory CA-2001-31 Buffer Overflow in CDE Subprocess Control Service November 12, 2001Carnegie Mellon Software Engineering Institute: December 2002.

CERT Advisory CA-2001-27 Format String Vulnerability in CDE ToolTalk October 5, 2001Carnegie Mellon Software Engineering Institute: December 2002.

Electronic Reference THE LATEST IN DENIAL OF SERVICE ATTACKS February 2000. Retrieved from Web dated February 2003.

Electronic Reference TechTarget Network May 2001. Retrieved from Web dated February 2003.

Appendix A

A-1 Solaris 9 OE

The following section was retrieved from the Web dated December 2002 at http://www.sun.com/solutions/blueprints/1102/816-5241.pdf by Alex Noordergraaf:

This section presents the minimum packages required to successfully install and run a 64-bit Solaris 9 OE environment. In addition, the packages specifically required for Sun ONE Web Server are listed. The package listing is presented with explanations of why the packages are recommended or required.

Note – This section was written for Solaris 9 OE (5/02), which was the first version released. Subsequent updates of Solaris 9 OE may introduce additional packages that may require modification of the minimization scripts. Use the information provided as a template and customize it to the specific OS and patch version you are minimizing.

Solaris 9 OE—64 Bit

The following packages must be available to run Solaris 9 OE in 64-bit mode based on a Sun4U system:

Package Type	Description
SUNWcar	Core Architecture, (Root)
SUNWcarx	Core Architecture, (Root) (64-bit)
SUNWcsd	Core Solaris Devices
SUNWcsl	Core Solaris, (Shared Libs)
SUNWcslx	Core Solaris Libraries (64-bit)
SUNWcsr	Core Solaris, (Root)
SUNWcsu	Core Solaris, (Usr)
SUNWcsxu	Core Solaris (Usr) (64-bit)
SUNWhmd	SunSwift Adapter Drivers
SUNWhmdx	SunSwift Adapter Drivers (64-bit)
SUNWkvm	Core Architecture, (Kvm)
SUNWkvmx	Core Architecture (Kvm) (64-bit)
SUNWloc	System Localization
SUNWlocx	System Localization (64-bit)
SUNWnamos	Northern America OS Support

Altogether, minimums of 15 packages are required to boot a Solaris 9 OE system running in a 64-bit mode.

The following packages are recommended to simplify administration and support because they contain required utilities such as “awk” and “patchadd”:

Package Type	Description
SUNWesu	Extended System Utilities
SUNWswmt	Install and Patch Utilities

Solaris 9 OE—Sun ONE Web Server

To successfully install and run the Sun ONE Web Server software on a minimized system, the following additional packages are required:

Package Type	Description
SUNWlibms	Forte Developer Bundled shared libm
SUNWlmsx	Forte Developer Bundled 64-bit shared libm
SUNWlibC	Sun Workshop Compilers Bundled libC
SUNWlibCx	Sun WorkShop Bundled 64-bit libC

Solaris 9 OE—Infrastructure Services

The previous list of Solaris 9 OE packages required for Sun ONE Web Server does not include support for some services and protocols that may be required in a data center environment. We recommend that you add the following packages:

Package Type	Description
SUNWsshcu	SSH Common, (Usr)
SUNWsshdr	SSH Server, (Root)
SUNWsshdu	SSH Server, (Usr)
SUNWsshr	SSH Client and utilities, (Root)
SUNWsshu	SSH Client and utilities, (Usr)
SUNWzlib	The Zip compression library
SUNWzlibx	The Zip compression library (64-bit)

To provide support for SSH X Tunneling, add the following packages:

Package Type	Description
SUNWdtbax	CDE application basic runtime environment (64-bit)
SUNWmfrun	Motif RunTime Kit
SUNWxwplt	X Window System platform software
SUNWxwplx	X Window System library software (64-bit)
SUNWxwrtl	X Window System & Graphics Runtime Library Links in /usr/lib

SUNWxwrtx	X Window System Runtime Compatibility Package (64-bit)
SUNWxwice	X Window System Inter-Client Exchange (ICE) Components
SUNWxwicx	X Window System ICE library (64-bit)

To provide support for ping, add the following packages:

Package Type	**Description**
SUNWbip	Basic IP commands (Usr)

To provide FTP support, modify the minimize-iPlanetWS.fin script so that the following packages are not removed:

Package Type	**Description**
SUNWftpr	FTP Server, (Root)
SUNWftpu	FTP Server, (Usr)

To provide Telnet support, modify the minimize-iPlanetWS.fin script so that the following packages are not removed:

Package Type	**Description**
SUNWtnetc	Telnet Command (client)
SUNWtnetd	Telnet Server Daemon (Usr)
SUNWtnetr	Telnet Server Daemon (Root)

To provide Network Time Protocol (NTP) support, add the following packages:

Package Type	**Description**
SUNWntpr	NTP, (Root)
SUNWntpu	NTP, (Usr)

To provide Simple Mail Transport Protocol (SMTP) capabilities, modify the minimize-iPlanetWS.fin script so that the following packages are not removed:

Package Type	**Description**
SUNWsndmu	Sendmail user
SUNWsndmr	Sendmail root

To provide support for truss, add the following packages:

Package Type	**Description**
SUNWtoo	Programming Tools

SUNWtoox	Programming Tools (64-bit)

To provide support for gzip, add the following package:
To support snoop, modify the minimize-iPlanetWS.fin script so that the following packages are not removed:

Package Type	**Description**
SUNWgzip	GNU Zip (gzip) compression utility

To support snoop, modify the minimize-iPlanetWS.fin script so that the following packages are not removed:

Package Type	**Description**
SUNWrcmdc	Remote Network Client Commands

A-2 Solaris 9 Recommended Patches

Solaris 9 Recommended Patches:

112233-04 SunOS 5.9: Kernel Patch
112601-04 SunOS 5.9: PGX32 Graphics
112764-04 SunOS 5.9: Sun Quad FastEthernet qfe driver
112785-12 X11 6.6.1: Xsun patch
112808-03 OpenWindows 3.6.3: Tooltalk patch
112817-06 SunOS 5.9: Sun GigaSwift Ethernet 1.0 driver patch
112875-01 SunOS 5.9: patch /usr/lib/netsvc/rwall/rpc.rwalld
112902-08 SunOS 5.9: kernel/drv/ip Patch
112908-07 SunOS 5.9: gl_kmech_krb5 Patch
112951-04 SunOS 5.9: patchadd and patchrm Patch
112963-05 SunOS 5.9: linker patch
112964-02 SunOS 5.9: ksh using control Z under ksh does not work well with vi
112970-02 SunOS 5.9: patch libresolv.so.2
112975-01 SunOS 5.9: patch /kernel/sys/kaio
112998-02 SunOS 5.9: patch /usr/sbin/syslogd
113023-01 SunOS 5.9: Broken preremove scripts in S9 ALC packages
113033-03 SunOS 5.9: patch /kernel/drv/isp and /kernel/drv/sparcv9/isp
113068-01 SunOS 5.9: hpc3130 patch
113146-01 SunOS 5.9: Apache Security Patch
113273-01 SunOS 5.9: /usr/lib/ssh/sshd Patch
113277-04 SunOS 5.9: sd and ssd Patch
113278-01 SunOS 5.9: NFS Daemon Patch
113279-01 SunOS 5.9: klmmod Patch
113319-05 SunOS 5.9: patch /usr/lib/libnsl.so.1
113333-02 SunOS 5.9: libmeta Patch
113492-01 SunOS 5.9: fsck Patch
113579-01 SunOS 5.9: ypserv/ypxfrd Patch
113718-01 SunOS 5.9: usr/lib/utmp_update Patch

113923-02 X11 6.6.1: security font server patch
114133-01 SunOS 5.9: mail Patch
114135-01 SunOS 5.9: at utility Patch
114153-01 SunOS 5.9: Japanese SunOS 4.x Binary Compatibility(BCP) patch

Solaris 9 Patches Containing Security Fixes:

```
112233-04   SunOS 5.9: Kernel Patch
112617-02 * CDE 1.5: rpc.cmsd patch
112808-03   OpenWindows 3.6.3: Tooltalk patch
112874-12 * SunOS 5.9: patch libc
112875-01   SunOS 5.9: patch /usr/lib/netsvc/rwall/rpc.rwalld
112902-08   SunOS 5.9: kernel/drv/ip Patch
112908-07   SunOS 5.9: gl_kmech_krb5 Patch
112926-03 * SunOS 5.9: smartcard Patch
112945-05 * SunOS 5.9: wbem Patch
112970-02   SunOS 5.9: patch libresolv.so.2
113030-02 * SunOS 5.9: /kernel/sys/doorfs Patch
113146-01   SunOS 5.9: Apache Security Patch
113273-01   SunOS 5.9: /usr/lib/ssh/sshd Patch
113278-01   SunOS 5.9: NFS Daemon Patch
113279-01   SunOS 5.9: klmmod Patch
113319-05   SunOS 5.9: patch /usr/lib/libnsl.so.1
113454-04 * SunOS 5.9: ufs Patch
113575-01 * SunOS 5.9: sendmail Patch
113579-01   SunOS 5.9: ypserv/ypxfrd Patch
113718-01   SunOS 5.9: usr/lib/utmp_update Patch
114133-01   SunOS 5.9: mail Patch
114135-01   SunOS 5.9: at utility Patch
```

generally relevant.

A-3 Output of netstat –a

UDP: IPv4

Local Address	Remote Address	State
*.sunrpc		Idle
.		Unbound
*.32771		Idle
*.32774		Idle
*.time		Idle
*.echo		Idle
*.discard		Idle
*.daytime		Idle
*.chargen		Idle
*.32778		Idle
*.32780		Idle
*.32786		Idle
*.biff		Idle
*.talk		Idle
*.32791		Idle
*.32794		Idle

*.32800	Idle
*.32803	Idle
*.name	Idle
*.32809	Idle
.	Unbound
*.32811	Idle
*.32812	Idle
*.lockd	Idle
*.syslog	Idle
*.32814	Idle
*.32816	Idle
*.32817	Idle
*.32818	Idle
.	Unbound
.	Unbound
*.32820	Idle
*.161	Idle
*.32822	Idle
*.32823	Idle
*.xdm	Idle
*.32824	Idle
*.32825	Idle
*.32826	Idle
*.32831	Idle
*.32838	Idle
*.32839	Idle
.	Unbound
*.1023	Idle
*.32846	Idle
*.1022	Idle
*.1021	Idle
.	Unbound

TCP: IPv4

Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	State
.	*.*	0	0	49152	0	IDLE
*.sunrpc	*.*	0	0	49152	0	LISTEN
.	*.*	0	0	49152	0	IDLE
*.32771	*.*	0	0	49152	0	LISTEN
*.time	*.*	0	0	49152	0	LISTEN
*.echo	*.*	0	0	49152	0	LISTEN
*.discard	*.*	0	0	49152	0	LISTEN
*.daytime	*.*	0	0	49152	0	LISTEN
*.chargen	*.*	0	0	49152	0	LISTEN
*.32774	*.*	0	0	49152	0	LISTEN
*.32776	*.*	0	0	49152	0	LISTEN
*.fs	*.*	0	0	49152	0	LISTEN
*.dtspc	*.*	0	0	49152	0	LISTEN
*.32781	*.*	0	0	49152	0	LISTEN
*.32783	*.*	0	0	49152	0	LISTEN
*.32785	*.*	0	0	49152	0	LISTEN
*.printer	*.*	0	0	49152	0	LISTEN
*.shell	*.*	0	0	49152	0	LISTEN

*.shell	*.*	0	0	49152	0	LISTEN
*.login	*.*	0	0	49152	0	LISTEN
*.exec	*.*	0	0	49152	0	LISTEN
*.exec	*.*	0	0	49152	0	LISTEN
*.finger	*.*	0	0	49152	0	LISTEN
*.32791	*.*	0	0	49152	0	LISTEN
*.telnet	*.*		0	49152	0	LISTEN
*.ftp	*.*	0	0	49152	0	LISTEN
*.uucp	*.*	0	0	49152	0	LISTEN
*.32803	*.*	0	0	49152	0	LISTEN
*.lockd	*.*	0	0	49152	0	LISTEN
*.5987	*.*	0	0	49152	0	LISTEN
*.898	*.*	0	0	49152	0	LISTEN
*.32804	*.*	0	0	49152	0	LISTEN
*.5988	*.*	0	0	49152	0	LISTEN
*.32805	*.*	0	0	49152	0	LISTEN
*.smtp	*.*	0	0	49152	0	LISTEN
*.smtp	*.*	0	0	49152	0	LISTEN
*.submission	*.*	0	0	49152	0	LISTEN
*.9010	*.*	0	0	49152	0	LISTEN
*.32806	*.*	0	0	49152	0	LISTEN
*.32807	*.*	0	0	49152	0	LISTEN
*.32808	*.*	0	0	49152	0	LISTEN
*.ssh	*.*	0	0	49152	0	LISTEN
*.6000	*.*	0	0	49152	0	LISTEN
*.32810	*.*	0	0	49152	0	LISTEN
localhost.32812	localhost.32774	49152	0	49152	0	ESTABLISHED
localhost.32774	localhost.32812	49152	0	49152	0	ESTABLISHED
localhost.32815	localhost.32810	49152	0	49152	0	ESTABLISHED
localhost.32810	localhost.32815	49152	0	49152	0	ESTABLISHED
localhost.32818	localhost.32817	49152	0	49152	0	ESTABLISHED
localhost.32817	localhost.32818	49152	0	49152	0	ESTABLISHED
localhost.32821	localhost.32810	49152	0	49152	0	ESTABLISHED
localhost.32810	localhost.32821	49152	0	49152	0	ESTABLISHED
localhost.32824	localhost.32823	49152	0	49152	0	ESTABLISHED
localhost.32823	localhost.32824	49152	0	49152	0	ESTABLISHED
sunone.32840	merlin.dtspc	8760	0	49485	0	ESTABLISHED
sunone.6000	merlin.40410	8760	0	48564	0	ESTABLISHED
sunone.login	doc.1023	8760	1	49640	0	ESTABLISHED
.	*.*	0	0	49152	0	IDLE

Active UNIX domain sockets

Address	Type	Vnode	Conn	Local Addr	Remote Addr
70d73cf0	stream-ord	70c3e028	00000000	tmp/.X11-unix/X0	
70d73e18	stream-ord	00000000	00000000		

A-4 Output of CISscan

*** CIS Ruler Run ***
Starting at time 20021014-11:22:32

```
Negative: 1.1 System appears not to have been patched within the last
month.
```

```
Negative: 2.2 telnet not deactivated.
Negative: 2.3 ftp not deactivated.
Negative: 2.4 rsh (shell) should be deactivated.
Negative: 2.4 rlogin (rlogin) should be deactivated.
Positive: 2.5 tftp is deactivated.
Negative: 2.6 network printing should be deactivated.
Negative: 2.7 rquotad is not deactivated.
Negative: 2.8 CDE-related daemon rpc.ttdbserverd not deactivated in
inetd.conf.
Negative: 2.8 CDE-related daemon fs.auto (port fs) not deactivated in
inetd.conf.
Negative: 2.8 CDE-related daemon kcms_server not deactivated in
inetd.conf.
Negative: 2.9 kerberos net daemon ktkt_warnd not deactivated in
inetd.conf.
Negative: 2.9 kerberos net daemon gssd not deactivated in inetd.conf.
Negative: 3.1 llc2 not deactivated.
Negative: 3.1 uucp not deactivated.
Negative: 3.1 slpd not deactivated.
Negative: 3.1 PRESERVE not deactivated.
Negative: 3.1 bdconfig not deactivated.
Negative: 3.1 wbem not deactivated.
Negative: 3.1 afbinit not deactivated.
Negative: 3.1 ncalogd not deactivated.
Negative: 3.1 mipagent not deactivated.
Negative: 3.1 sysid.net not deactivated.
Negative: 3.1 sysid.sys not deactivated.
Negative: 3.1 autoinstall not deactivated.
Negative: 3.1 cachefs.daemon not deactivated.
Negative: 3.1 cacheos.finish not deactivated.
Negative: 3.1 power not deactivated.
Negative: 3.1 dmi not deactivated.
Negative: 3.2 NFS Server script nfs.server not deactivated.
Negative: 3.3 NFS script nfs.client not deactivated.
Negative: 3.3 NFS script autofs not deactivated.
Negative: 3.4 rpc rc-script (rpcbind) not deactivated.
Negative: 3.5 ldap cache manager not deactivated.
Negative: 3.6 lp not deactivated.
Negative: 3.6 spc not deactivated.
Negative: 3.7 volume manager not deactivated.
Negative: 3.8 Graphical login not deactivated.
Negative: 3.9 Mail daemon is on and collecting mail from the network.
Negative: 3.11 snmp daemon should be deactivated.
Negative: 3.13 Serial login prompt not disabled.
Negative: 3.12 inetd is still active.
Positive: 3.14 Found a good daemon umask.
Negative: 4.1 Coredumps aren't deactivated.
Negative: 4.2 Stack is not yet set non-executable.
Negative: 4.3 NFS clients aren't restricted to privileged ports.
Negative: 4.4 ip_strict_dst_multihoming isn't activated.
Negative: 4.4 ip_send_redirects isn't set to 0.
Negative: 4.4 ip_ignore_redirect isn't set to 1.
Negative: 4.4 tcp_conn_req_max_q0 should be at least 4096 to avoid TCP
flood problems.
Negative: 4.4 tcp_ip_abort_cinterval should be at most 60,000 to avoid
TCP flood problems.
Negative: 4.4 ip_respond_to_timestamp isn't 0.
```

```
Negative: 4.4 ARP timer (arp_cleanup_interval) should be at most
60,000.
Negative: 4.4 ARP timer (ip_ire_arp_interval) should be at most 60,000
Negative: 4.5 TCP sequence numbers not strong enough.
Negative: 5.1 syslog does not permanently capture auth messages.
Negative: 5.2 /var/adm/loginlog doesn't exist to track failed logins.
Positive: 5.3 cron usage is being logged.
Negative: 5.4 Couldn't find an active sadc line in /etc/rc2.d/S21perf
to verify system acctg.
Negative: 5.4 No sa1 line in /var/spool/cron/crontabs/sys -- no system
accounting.
Negative: 5.4 No sa2 line in /var/spool/cron/crontabs/sys -- no system
accounting.
Negative: 5.5 kernel-level auditing isn't enabled.
Negative: 6.1 Never found separate /usr partition, so it couldn't be
mounted read-only.
Negative: 6.2 logging option isn't set on root file system
Positive: 6.3 /etc/rmmount.conf mounts all file systems nosuid.
Positive: 6.4 password and group files have right permissions and
owners.
Positive: 6.5 all temporary directories have sticky bits set.
Negative: 7.1 /etc/pam.conf appears to support rhost auth.
Positive: 7.2 /etc/hosts.equiv file not present or has size zero.
Negative: 7.3 /etc/ftpusers doesn't exist
Negative: 7.4 Couldn't open cron.allow
Negative: 7.4 Couldn't open at.allow
Positive: 7.5 crontabs all have good ownerships and modes
Positive: 7.7 Root is only allowed to login on console
Negative: 7.8 EEPROM isn't password-protected.
Negative: 8.1 uucp has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 listen has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 nobody4 has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 adm has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 daemon has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 bin has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 lp has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 nobody has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.1 noaccess has a valid shell of /bin/sh.  Remember, an
empty shell field in /etc/passwd signifies /bin/sh.
Positive: 8.2 There were no +: entries in passwd, shadow or group maps.
Positive: 8.3 All users have passwords
Positive: 8.4 Only one UID 0 account AND it is named root.
Positive: 8.5 root's PATH is clean of group/world writable directories
or the current-directory link.
Positive: 8.6 root account has no dangerous rhosts, shosts, or netrc
files.
Negative: 8.7 User adm 's homedir is group writable!
Negative: 8.7 User lp 's homedir is group writable!
Positive: 8.8 No group or world-writable dotfiles!
```

```
Positive: 8.9 No user has a .netrc or .rhosts file.
Negative: 8.10 Default umask may not block world-writable.  Check
/etc/default/login.
Negative: 8.10 Default umask may not block group-writable.  Check
/etc/default/login.
Negative: 8.10 Default umask may not block world-writable.  Check
/etc/.login.
Negative: 8.10 Default umask may not block group-writable.  Check
/etc/.login.
Negative: 9.1 tcp-protocol service fs in inetd.conf is not wrapped.
Negative: 9.1 tcp-protocol service dtspc in inetd.conf is not wrapped.
Negative: 9.1 tcp-protocol service shell in inetd.conf is not wrapped.
Negative: 9.1 tcp-protocol service exec in inetd.conf is not wrapped.
Negative: 9.1 udp-protocol service comsat in inetd.conf is not wrapped.
Negative: 9.1 udp-protocol service talk in inetd.conf is not wrapped.
Negative: 9.1 udp-protocol service name in inetd.conf is not wrapped.
Negative: 9.1 tcp-protocol service uucp in inetd.conf is not wrapped.
Positive: 9.2 System is running sshd.
Negative: 9.3 This machine isn't synced with ntp.
Negative: 9.4 Fix-modes has not been run here.
Preliminary rating given at time: Mon Oct 14 11:22:32 2002

        Preliminary rating = 2.83 / 10.00

Negative: 6.6 Non-standard SUID program /usr/bin/sparcv7/newtask
Negative: 6.6 Non-standard SUID program /usr/bin/mailq
Negative: 6.6 Non-standard SUID program /usr/bin/cdrw
Negative: 6.6 Non-standard SGID program /usr/lib/sendmail
Negative: 6.6 Non-standard SGID program /usr/SUNWale/bin/mailx
Ending run at time: Mon Oct 14 11:23:15 2002
```

Final rating = 2.83 / 10.00

A-5 Results of Nmap port scan

The following command tells Nmap to perform a TCP connect scan that performs the three-way handshake on the sunone Web Server.

 # nmap -sT sunone

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on sunone (10.xxx.x.xx):
(The 1574 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
22/tcp     open        ssh
23/tcp     open        telnet
25/tcp     open        smtp
37/tcp     open        time
79/tcp     open        finger
```

```
80/tcp     open        http
111/tcp    open        sunrpc
512/tcp    open        exec
513/tcp    open        login
514/tcp    open        shell
515/tcp    open        printer
540/tcp    open        uucp
587/tcp    open        submission
898/tcp    open        unknown
4045/tcp   open        lockd
6000/tcp   open        X11
6112/tcp   open        dtspc
7100/tcp   open        font-service
8888/tcp   open        sun-answerbook
32771/tcp  open        sometimes-rpc5
32774/tcp  open        sometimes-rpc11
32776/tcp  open        sometimes-rpc15

Nmap run completed -- 1 IP address (1 host up) scanned in 50 seconds
```

The following command tells Nmap to perform a TCP SYN scan with verbose on and with ports range from 1 to 65535 on the sunone Web Server. Nmap normally scan all of the ports between 1 and 1024 plus any additional ports listed in the services file. We use "–p 1-65535" option to scan all possible ports on the Web Server:

 # nmap -v -sS -p 1-65535 sunone

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Host sunone (10.xxx.x.x) appears to be up ... good.
Initiating SYN Stealth Scan against sunone (10.xxx.x.x)
Adding open port 7100/tcp
Adding open port 32806/tcp
Adding open port 32774/tcp
Adding open port 22/tcp
Adding open port 6000/tcp
Adding open port 587/tcp
Adding open port 32803/tcp
Adding open port 32805/tcp
Adding open port 32807/tcp
Adding open port 13/tcp
Adding open port 32776/tcp
Adding open port 32783/tcp
Adding open port 32785/tcp
Adding open port 32771/tcp
Adding open port 6112/tcp
Adding open port 9010/tcp
Adding open port 32893/tcp
Adding open port 32808/tcp
Adding open port 515/tcp
Adding open port 32804/tcp
Adding open port 5988/tcp
Adding open port 37/tcp
Adding open port 32791/tcp
Adding open port 32781/tcp
```

```
Adding open port 540/tcp
Adding open port 19/tcp
Adding open port 513/tcp
Adding open port 512/tcp
Adding open port 21/tcp
Adding open port 25/tcp
Adding open port 898/tcp
Adding open port 111/tcp
Adding open port 79/tcp
Adding open port 9/tcp
Adding open port 5987/tcp
Adding open port 4045/tcp
Adding open port 7/tcp
Adding open port 80/tcp
Adding open port 23/tcp
Adding open port 8888/tcp
Adding open port 514/tcp
The SYN Stealth Scan took 4305 seconds to scan 65535 ports.
Interesting ports on sunone (10.xxx.x.xx):
(The 65494 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
22/tcp     open        ssh
23/tcp     open        telnet
25/tcp     open        smtp
37/tcp     open        time
79/tcp     open        finger
80/tcp     open        http
111/tcp    open        sunrpc
512/tcp    open        exec
513/tcp    open        login
514/tcp    open        shell
515/tcp    open        printer
540/tcp    open        uucp
587/tcp    open        submission
898/tcp    open        unknown
4045/tcp   open        lockd
5987/tcp   open        unknown
5988/tcp   open        unknown
6000/tcp   open        X11
6112/tcp   open        dtspc
7100/tcp   open        font-service
8888/tcp   open        sun-answerbook
9010/tcp   open        unknown
32771/tcp  open        sometimes-rpc5
32774/tcp  open        sometimes-rpc11
32776/tcp  open        sometimes-rpc15
32781/tcp  open        unknown
32783/tcp  open        unknown
32785/tcp  open        unknown
32791/tcp  open        unknown
32803/tcp  open        unknown
32804/tcp  open        unknown
```

```
32805/tcp  open        unknown
32806/tcp  open        unknown
32807/tcp  open        unknown
32808/tcp  open        unknown
32893/tcp  open        unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 4306 seconds
```

The following command tells Nmap to perform a UDP SYN scan with ports range from 1 to 1024 on the sunone server.

 # nmap -v -sU -p 1-1024 sunone

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Host sunone (10.xxx.x.x) appears to be up ... good.
Initiating UDP Scan against sunone (10.xxx.x.x)
Too many drops ... increasing senddelay to 50000
The UDP Scan took 227 seconds to scan 1024 ports.
Adding open port 161/udp
Adding open port 9/udp
Adding open port 19/udp
Adding open port 42/udp
Adding open port 7/udp
Adding open port 514/udp
Adding open port 37/udp
Adding open port 13/udp
Adding open port 1021/udp
Adding open port 512/udp
Adding open port 1020/udp
Adding open port 517/udp
Adding open port 1023/udp
Adding open port 111/udp
Adding open port 708/udp
Adding open port 1022/udp
Adding open port 177/udp
Adding open port 1019/udp
Adding open port 1018/udp
Interesting ports on sunone (10.xxx.x.xx):
(The 1005 ports scanned but not shown below are in state: closed)
Port       State       Service
7/udp      open        echo
9/udp      open        discard
13/udp     open        daytime
19/udp     open        chargen
37/udp     open        time
42/udp     open        nameserver
111/udp    open        sunrpc
161/udp    open        snmp
177/udp    open        xdmcp
512/udp    open        biff
514/udp    open        syslog
517/udp    open        talk
708/udp    open        unknown
1018/udp   open        unknown
1019/udp   open        unknown
```

```
1020/udp    open         unknown
1021/udp    open         unknown
1022/udp    open         unknown
1023/udp    open         unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 227 seconds
```

A-6 Result of Nessus vulnerabilities scan

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

Nessus Scan Report
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details	
Hosts which where alive and responding during test	1
Number of security holes found	9
Number of security warnings found	29

Host List	
Host(s)	**Possible Issue**
sunone	Security hole(s) found

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
sunone	echo (7/tcp)	Security warning(s) found
sunone	discard (9/tcp)	No Information
sunone	daytime (13/tcp)	Security warning(s) found
sunone	chargen (19/tcp)	Security warning(s) found
sunone	ftp (21/tcp)	Security notes found
sunone	ssh (22/tcp)	Security warning(s) found
sunone	telnet (23/tcp)	Security warning(s) found
sunone	smtp (25/tcp)	Security warning(s) found
sunone	time (37/tcp)	Security notes found
sunone	finger (79/tcp)	Security warning(s) found
sunone	http (80/tcp)	Security notes found
sunone	sunrpc (111/tcp)	Security notes found

sunone	exec (512/tcp)	Security warning(s) found
sunone	login (513/tcp)	Security warning(s) found
sunone	shell (514/tcp)	Security warning(s) found
sunone	printer (515/tcp)	No Information
sunone	uucp (540/tcp)	No Information
sunone	submission (587/tcp)	Security warning(s) found
sunone	unknown (898/tcp)	No Information
sunone	lockd (4045/tcp)	Security notes found
sunone	unknown (5987/tcp)	No Information
sunone	unknown (5988/tcp)	Security notes found
sunone	x11 (6000/tcp)	Security warning(s) found
sunone	dtspc (6112/tcp)	Security hole found
sunone	xfs (7100/tcp)	No Information
sunone	unknown (8888/tcp)	Security notes found
sunone	unknown (9010/tcp)	No Information
sunone	general/tcp	Security notes found
sunone	daytime (13/udp)	Security warning(s) found
sunone	echo (7/udp)	Security warning(s) found
sunone	general/icmp	Security warning(s) found
sunone	unknown (32786/udp)	Security hole found
sunone	sunrpc (111/udp)	Security notes found
sunone	unknown (32774/udp)	Security warning(s) found
sunone	unknown (32771/tcp)	Security notes found
sunone	unknown (32780/udp)	Security hole found
sunone	unknown (32774/tcp)	Security hole found
sunone	unknown (32776/tcp)	Security hole found
sunone	unknown (32781/tcp)	Security notes found
sunone	unknown (32783/tcp)	Security notes found
sunone	unknown (32785/tcp)	Security notes found
sunone	unknown (32791/udp)	Security warning(s) found
sunone	unknown (32794/udp)	Security warning(s) found
sunone	unknown (32791/tcp)	Security notes found
sunone	unknown (32800/udp)	Security hole found
sunone	unknown (32803/udp)	Security warning(s) found
sunone	unknown (32809/udp)	Security warning(s) found
sunone	unknown (32812/udp)	Security hole found
sunone	unknown (32803/tcp)	Security notes found
sunone	lockd (4045/udp)	Security warning(s) found
sunone	unknown (32824/udp)	Security notes found
sunone	unknown (32806/tcp)	Security notes found
sunone	unknown (32825/udp)	Security notes found
sunone	unknown (32808/tcp)	Security hole found
sunone	unknown (32893/tcp)	Security notes found

sunone	unknown (32794/tcp)	Security notes found
sunone	general/udp	Security notes found
sunone	xdmcp (177/udp)	Security warning(s) found

Security Issues and Fixes: sunone

(13/tcp)	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

		There is a vulnerability in this release that may, under some circumstances, allow users to authenticate using a password whereas it is not explicitly listed as a valid authentication mechanism. An attacker may use this flaw to attempt to brute force a password using a dictionary attack (if the passwords used are weak). Solution : Upgrade to version 3.1.2 of SSH which solves this problem. Risk factor : Low
Warning	ssh (22/tcp)	You are running a version of SSH which is older than (or as old as) version 1.2.27. If you compiled ssh with kerberos support, then an attacker may eavesdrop your users kerberos tickets, as sshd will set the environment variable KRB5CCNAME to 'none', so kerberos tickets will be stored in the current working directory of the user, as 'none'. If you have nfs/smb shared disks, then an attacker may eavesdrop the kerberos tickets of your users using this flaw. *** If you are not using kerberos, then *** ignore this warning. Risk factor : Serious Solution : use ssh 1.2.28 or newer CVE : CVE-2000-0575
Warning	ssh (22/tcp)	You are running a version of SSH which is older than (or as old as) version 1.2.27. If this version was compiled against the RSAREF library, then it is very likely to be vulnerable to a buffer overflow which may be exploited by an attacker to gain root on your system. To determine if you compiled ssh against the RSAREF library, type 'ssh -V' on the remote host. Risk factor : High Solution : Use ssh 2.x, or do not compile ssh against the RSAREF library CVE : CVE-1999-0834
Informational	ssh (22/tcp)	An ssh server is running on this port
Informational	ssh (22/tcp)	Remote SSH version : SSH-2.0-Sun_SSH_1.0
Informational	ssh (22/tcp)	The remote SSH daemon supports the following versions of the SSH protocol : . 1.99 . 2.0
Warning	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
Informational	telnet (23/tcp)	A telnet server seems to be running on this port
Warning	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. Solution : if you are using Sendmail, add the option O PrivacyOptions=goaway in /etc/sendmail.cf. Risk factor : Low CVE : CAN-1999-0531
Warning	smtp (25/tcp)	The remote SMTP server allows the relaying. This means that it allows spammers to use your mail server to send their mails to the world, thus wasting your network bandwidth. Risk factor : Low/Medium Solution : configure your SMTP server so that it can't be used as a relay any more. CVE : CAN-1999-0512
Informational	smtp (25/tcp)	An SMTP server is running on this port Here is its banner : 220 sunone.company.com ESMTP Sendmail 8.12.2+Sun/8.12.2; Tue, 21 Jan 2003 10:42:45 -0800 (PST)
Informational	smtp (25/tcp)	Remote SMTP server banner : sunone.company.com ESMTP Sendmail 8.12.2+Sun/8.12.2; Tue, 21 Jan 2003 10:45:20 - 0800 (PST) 214-2.0.0 This is sendmail version 8.12.2+Sun214-2.0.0 Topics: 214-2.0.0 HELO EHLO MAIL RCPT DATA 214-2.0.0 RSET NOOP QUIT HELP VRFY 214-2.0.0 EXPN VERB ETRN DSN 214-2.0.0 For more info use "HELP <topic>". 214-2.0.0 To report bugs in the implementation contact Sun Microsystems 214-2.0.0 Technical Support. 214-2.0.0 For local information send email to Postmaster at your site. 214 2.0.0 End of HELP info
Informational	time (37/tcp)	A time server seems to be running on this port

Warning	finger (79/tcp)	The 'finger' service provides useful information to attackers, 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	finger (79/tcp)	The remote finger daemon accepts to redirect requests. That is, users can perform requests like : finger user@host@victim This allows an attacker 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. Risk factor : Low CVE : CAN-1999-0105
Informational	finger (79/tcp)	An unknown service is running on this port. It is usually reserved for Finger
Informational	http (80/tcp)	A web server is running on this port
Informational	sunrpc (111/tcp)	RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port
Informational	sunrpc (111/tcp)	RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port
Informational	sunrpc (111/tcp)	RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port
Warning	exec (512/tcp)	The rexecd service is open. Because rexecd does not provide any good means of authentication, it can be used by an attacker 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	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	shell	The rsh service is running.

	(514/tcp)	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
Informational	shell (514/tcp)	The service closed the connection after 0 seconds without sending any data It might be protected by some TCP wrapper
Warning	submission (587/tcp)	The remote SMTP server allows the relaying. This means that it allows spammers to use your mail server to send their mails to the world, thus wasting your network bandwidth. Risk factor : Low/Medium Solution : configure your SMTP server so that it can't be used as a relay any more. CVE : CAN-1999-0512
Informational	submission (587/tcp)	An SMTP server is running on this port Here is its banner : 220 sunone.company.com ESMTP Sendmail 8.12.2+Sun/8.12.2; Tue, 21 Jan 2003 10:43:26 -0800 (PST)
Informational	submission (587/tcp)	Remote SMTP server banner : sunone.company.com ESMTP Sendmail 8.12.2+Sun/8.12.2; Tue, 21 Jan 2003 10:45:22 - 0800 (PST) 214-2.0.0 This is sendmail version 8.12.2+Sun214-2.0.0 Topics: 214-2.0.0 HELO EHLO MAIL RCPT DATA 214-2.0.0 RSET NOOP QUIT HELP VRFY 214-2.0.0 EXPN VERB ETRN DSN 214-2.0.0 For more info use "HELP <topic>". 214-2.0.0 To report bugs in the implementation contact Sun Microsystems 214-2.0.0 Technical Support. 214-2.0.0 For local information send email to Postmaster at your site. 214 2.0.0 End of HELP info
Informational	lockd (4045/tcp)	RPC program #100021 version 1 'nlockmgr' is running on this port
Informational	lockd (4045/tcp)	RPC program #100021 version 2 'nlockmgr' is running on this port
Informational	lockd (4045/tcp)	RPC program #100021 version 3 'nlockmgr' is running on this port
Informational	lockd (4045/tcp)	RPC program #100021 version 4 'nlockmgr' is running on this port
Informational	unknown (5988/tcp)	This port was detected as being open by a port scanner but is now closed. This service might have been crashed by a port scanner or by some information gathering plugin
Warning	x11 (6000/tcp)	This X server does *not* allow any client to connect to it however it is recommended that you filter incoming connections to this port as attacker may send garbage data and slow down your X session or even kill the server. Here is the server version : 11.0 Here is the message we received : Client is not authorized to connect to Server Solution : filter incoming connections to ports 6000-6009 Risk factor : Low CVE : CVE-1999-0526

Vulnerability	dtspc (6112/tcp)	The 'dtspcd' service is running. Some versions of this daemon are vulnerable to a buffer overflow attack which allows an attacker to gain root privileges *** This warning might be a false positive, *** as no real overflow was performed Solution : See http://www.cert.org/advisories/CA-2001-31.html to determine if you are vulnerable or deactivate this service (comment out the line 'dtspc' in /etc/inetd.conf) Risk factor : High CVE : CVE-2001-0803
Informational	unknown (8888/tcp)	A web server is running on this port
Informational	general/tcp	HTTP NIDS evasion functions are enabled. You may get some false negative results
Warning	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	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. Risk factor : Low Solution : comment out 'echo' in /etc/inetd.conf CVE : CVE-1999-0103
Warning	general/icmp	The remote host answered to an ICMP_MASKREQ query and sent us its netmask (255.255.0.0) An attacker can use this information to understand how your network is set up and how the routing is done. This may help him to bypass your filters. Solution : reconfigure the remote host so that it does not answer to those requests. Set up filters that deny ICMP packets of type 17. Risk factor : Low CVE : CAN-1999-0524
Warning	general/icmp	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 authentication protocols. Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). Risk factor : Low CVE : CAN-1999-0524
Vulnerability	unknown (32786/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
Informational	unknown (32786/udp)	RPC program #100068 version 2 is running on this port
Informational	unknown (32786/udp)	RPC program #100068 version 3 is running on this port
Informational	unknown (32786/udp)	RPC program #100068 version 4 is running on this port
Informational	unknown (32786/udp)	RPC program #100068 version 5 is running on this port
Informational	sunrpc (111/udp)	RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port
Informational	sunrpc (111/udp)	RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port
Informational	sunrpc (111/udp)	RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port
Warning	unknown (32774/udp)	The ypbind 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 : CVE-1999-0312
Informational	unknown (32774/udp)	RPC program #100007 version 3 'ypbind' is running on this port
Informational	unknown (32774/udp)	RPC program #100007 version 2 'ypbind' is running on this port
Informational	unknown (32774/udp)	RPC program #100007 version 1 'ypbind' is running on this port
Informational	unknown (32771/tcp)	RPC program #100007 version 3 'ypbind' is running on this port

Informational	unknown (32771/tcp)	RPC program #100007 version 2 'ypbind' is running on this port
Informational	unknown (32771/tcp)	RPC program #100007 version 1 'ypbind' is running on this port
Vulnerability	unknown (32780/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
Informational	unknown (32780/udp)	RPC program #100232 version 10 'sadmind' is running on this port
Vulnerability	unknown (32774/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. In addition to this, several versions of this service allow remote attackers to overwrite abitrary memory locations with a zero and possibly gain privileges via a file descriptor argument in an AUTH_UNIX procedure call which is used as a table index by the _TT_ISCLOSE procedure. *** This warning may be a false positive since the presence *** of the bug was not verified locally. Solution : Disable this service or patch it See also : CERT Advisories CA-2001-27 and CA-2002-20 Risk factor : High CVE : CAN-2002-0677
Vulnerability	unknown (32774/tcp)	The tooltalk RPC service is running. An possible implementation fault in the ToolTalk object database server may allow an attacker to execute arbitrary commands as root. *** This warning may be a false *** positive since the presence *** of this vulnerability is only accurately *** identified with local access. Solution : Disable this service. See also : CERT Advisory CA-98.11 Risk factor : High CVE : CVE-1999-0003
Informational	unknown (32774/tcp)	RPC program #100083 version 1 is running on this port
Vulnerability	unknown (32776/tcp)	The Kodak Color Management System service is running. The KCMS service on Solaris 2.5 could allow a local user to write to arbitrary files and gain root access. *** This warning may be a false

		*** positive since the presence *** of the bug has not been tested. Patches: 107337-02 SunOS 5.7 has been released and the following should be out soon: 111400-01 SunOS 5.8, 111401-01 SunOS 5.8_x86 Solution : Disable suid, side effects are minimal. http://www.eeye.com/html/Research/Advisories/AD20010409.html http://www.securityfocus.com/bid/2605 See also: http://packetstorm.decepticons.org/advisories/ibm-ers/96-09 Risk factor : High CVE : CVE-2001-0595
Informational	unknown (32776/tcp)	RPC program #100221 version 1 is running on this port
Informational	unknown (32781/tcp)	RPC program #100229 version 1 is running on this port
Informational	unknown (32783/tcp)	RPC program #100230 version 1 is running on this port
Informational	unknown (32785/tcp)	RPC program #100242 version 1 is running on this port
Warning	unknown (32791/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 Usually, it is not a good idea to let this service open Risk factor : Low CVE : CAN-1999-0624
Informational	unknown (32791/udp)	RPC program #100001 version 2 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port
Informational	unknown (32791/udp)	RPC program #100001 version 3 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port
Informational	unknown (32791/udp)	RPC program #100001 version 4 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port
Warning	unknown (32794/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 leave this service open. Risk factor : Low CVE : CVE-1999-0626
Informational	unknown (32794/udp)	RPC program #100002 version 2 'rusersd' (rusers) is running on this port

Informational	unknown (32794/udp)	RPC program #100002 version 3 'rusersd' (rusers) is running on this port
Informational	unknown (32791/tcp)	RPC program #100002 version 2 'rusersd' (rusers) is running on this port
Informational	unknown (32791/tcp)	RPC program #100002 version 3 'rusersd' (rusers) is running on this port
Vulnerability	unknown (32800/udp)	The rpc.walld RPC service is running. Some versions of this server allow an attacker to gain root access remotely, by consuming the resources of the remote host then sending a specially formed packet with format strings to this host. Solaris 2.5.1, 2.6, 7 and 8 are vulnerable to this issue. Other operating systems might be affected as well. *** Nessus did not check for this vulnerability, *** so this might be a false positive Solution : Deactivate this service. Risk factor : High CVE : CAN-2002-0573
Warning	unknown (32800/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, an attacker 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
Informational	unknown (32800/udp)	RPC program #100008 version 1 'walld' (rwall shutdown) is running on this port
Warning	unknown (32803/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
Informational	unknown (32803/udp)	RPC program #100012 version 1 'sprayd' (spray) is running on this port
Warning	unknown (32809/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
Informational	unknown (32809/udp)	RPC program #100011 version 1 'rquotad' (rquotaprog quota rquota) is running on this port
Vulnerability	unknown (32812/udp)	The remote statd service may be vulnerable to a format string attack. This means that an attacker may execute arbitrary code thanks to a bug in this daemon. *** Nessus reports this vulnerability using only *** information that was gathered. Use caution *** when testing without safe checks enabled. Solution : upgrade to the latest version of rpc.statd Risk factor : High CVE : CVE-2000-0666
Warning	unknown (32812/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-1999-0493
Informational	unknown (32812/udp)	RPC program #100024 version 1 'status' is running on this port
Informational	unknown (32812/udp)	RPC program #100133 version 1 is running on this port
Informational	unknown (32803/tcp)	RPC program #100024 version 1 'status' is running on this port
Informational	unknown (32803/tcp)	RPC program #100133 version 1 is running on this port
Warning	lockd (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 : CVE-2000-0508
Informational	lockd (4045/udp)	RPC program #100021 version 1 'nlockmgr' is running on this port
Informational	lockd (4045/udp)	RPC program #100021 version 2 'nlockmgr' is running on this port

Informational	lockd (4045/udp)	RPC program #100021 version 3 'nlockmgr' is running on this port
Informational	lockd (4045/udp)	RPC program #100021 version 4 'nlockmgr' is running on this port
Informational	unknown (32824/udp)	RPC program #300598 version 1 is running on this port
Informational	unknown (32824/udp)	RPC program #805306368 version 1 is running on this port
Informational	unknown (32806/tcp)	RPC program #300598 version 1 is running on this port
Informational	unknown (32806/tcp)	RPC program #805306368 version 1 is running on this port
Informational	unknown (32825/udp)	RPC program #100249 version 1 is running on this port
Vulnerability	unknown (32808/tcp)	The remote RPC service 100249 (snmpXdmid) may be vulnerable to a heap overflow which allows any user to obtain a root shell on this host. *** Nessus reports this vulnerability using only *** information that was gathered. Use caution *** when testing without safe checks enabled. 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 : CVE-2001-0236
Informational	unknown (32808/tcp)	RPC program #100249 version 1 is running on this port
Informational	unknown (32893/tcp)	RPC program #1289637086 version 5 is running on this port
Informational	unknown (32893/tcp)	RPC program #1289637086 version 1 is running on this port
Informational	unknown (32794/tcp)	Using rusers, we could determine that the following users are logged in : - root (console) from :0 Solution : disable this service. Risk factor : Low CVE : CVE-1999-0626
Informational	general/udp	For your information, here is the traceroute to 10.221.1.74 : 10.221.1.74
Warning	xdmcp (177/udp)	The remote host is running XDMCP. This protocol is used to provide X display connections for X terminals. XDMCP is completely insecure, since the traffic and passwords are not encrypted. An attacker may use this flaw to capture all the keystrokes of the users using this host through their X terminal, including passwords. Risk factor : Medium Solution : Disable XDMCP

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