Global Information Assurance Certification Paper

Securing UNIX
GCUX Practical Assignment
Securing UNIX Step By Step
Apache Webserver

GCUX Practical Assignment version 2.1

Rudy Pereda
September 2004

Table of Contents

Abstract

The goal of this document is to provide an easy to follow method for installing and configuring Apache Web Server on Sun Microsystems' Solaris 5.9 platform. The web server is one of many servers being utilized for an ERP project. This document walks the reader through the installation of Sun Microsystems Operating Environment, Solaris version 5.9 and other third party applications. The environment will go through a hardening process where unneeded services will be disabled, file and group permissions will be modified, etc…to ensure the integrity of the server. An on-going maintenance plan will be established to ensure the hardening process is not weakened by the addition of new applications and/or patches. A backup process will be established to ensure the environment is recoverable in the event of a compromise or disaster. Finally, tests will be performed on the web server to ensure the hardening process does work and nothing has been overlooked. Once completed, the web server should only be listening to two ports, http (80), and ssh (22).

1. Server Specification and Risk Mitigation Plan

1.1. Introduction

Corporate Headquarters has initiated the replacement of the company's accounting system. Management has asked the System Administrators Team (SAT) to establish a secure web server for the dissemination of project data. Access to project data will be limited to upper management and project staff. Although, this server is not considered "critical", it is, nevertheless, an important part of the overall project.

Due to the critical nature of the project, management has asked both the Sun Group and Network Group to devise a plan to ensure the following:

- Secure web server running Sun Microsystems Solaris OS 5.9 [1] and Apache 1.3.31[2]
- Ensure integrity of data transmitted to and from server
- Secure server authentication for certain project employees
- Limit access to Web Server to only parties involved
- Project servers must be isolated by firewall appliance

1.2. Server Specification

In keeping with management requests, the network team has made modifications to the network environment to ensure project servers are secured and only accessible to project staff. Switches have been used to provide a degree of security[3]. Although, switches are more secure than hubs, they are vulnerable to "Arp Spoofing" [4]

Virtual Local Area Networks or VLANS have been established exclusively for project environments (e.g. Production (Prod), Development (Dev)…) separated from the corporate network by an appliance firewall (see figure 1).

On the corporate network, VLANS have been established for Project staff. Access Control Lists or ALCs have been defined on the Project Firewall providing access to only those VLANS established exclusively for the project.

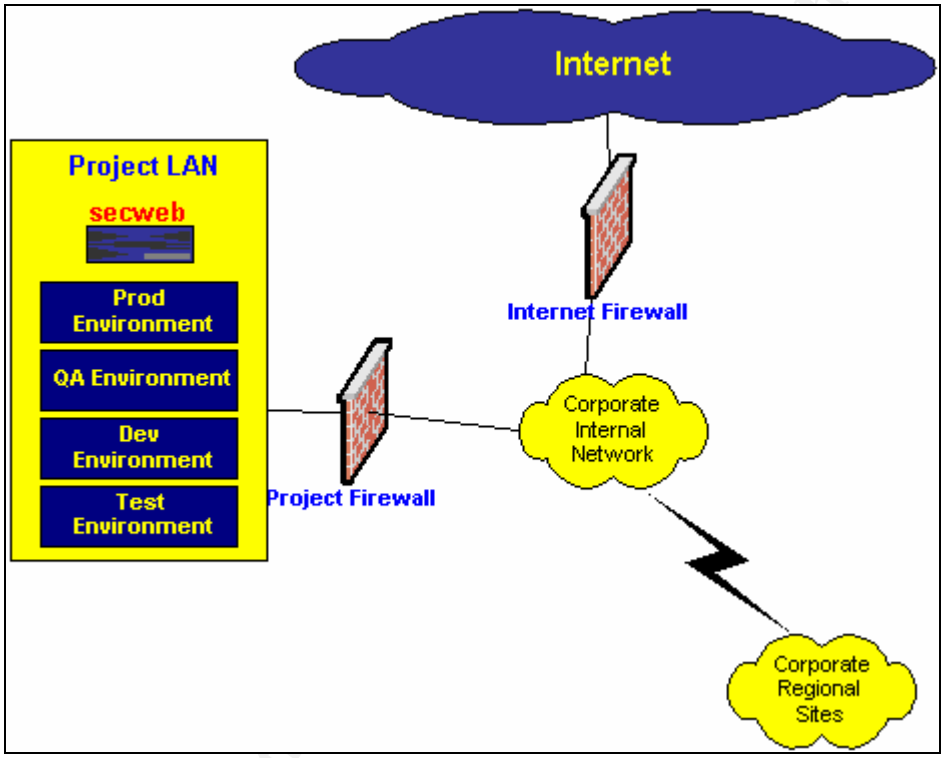

Figure 1

Why separate the project environment from the internal corporate network and establish VLANs for project staff?

The answer to this question is quite simple. A couple of points:

- Limited number of employees
  - Filter everyone that does not need access to the environment; VLANs provide a medium for grouping project staff ; using the VLANs subnet address, they are easily filtered at the firewall appliance for specific services, thereby separating the project environment from the corporate network.
- Possibility of internal attacks
  - All attacks are not equal. This being the case, you need to protect your

systems from employees that might have an ulterior motive;

- With the firewall, access to the project servers is minimized; for this document, only the the following ports will be open at the firewall:
  - Ssh (port 22)
  - http (port 80)

1.2.1. Hardware & Software

1.2.1.1. Hardware

Hardware requirements recommended provide a degree of fault tolerance ensuring the environment is up at all times and keeping it within the bounds of the corporate "Server Policy". All systems adhering to the "Server Policy" must be fault tolerant. Fault tolerance as defined by the policy means dual CPUs, mirrored drives, etc…

System Hardware	
Server	Sun Fire 240V
CPU	Dual 1 GHZ SUNW,UltraSPARC-IIIi
Memory size	2 Gigabytes
Storage	Two Mirrored 72GB Drives

1.2.1.2. Software

The secure web server will utilize Sun's Solaris 5.9 operating system along with ApacheSSL providing web services and data integrity. TCPwrappers will be used to provide access control to certain services such as SSH. This product allows system administrators the flexibility to deny services to users not needing it while allowing the project staff.

System Software	
Operating System	Sun Solaris version 5.9
Web Server	ApacheSSL 1.3.31
Data encryption/integrity	OpenSSL
Access Control	TCPwrappers
File Integrity	TripWire

1.2.2. Services Provided by SYSWEB

SYSWEB will provide web services to the project team and secure shell to those project members updating the server regularly. It will be used by the project team to disseminate project data via html and pdf formats. The server will listen on ports 443 and 22.

1.2.3. Additional Processes

Once the server has been hardened and all third party software has been installed the only additional processes that will be running are ntpd, httpd, and sshd.

1.2.4. Security Tools

Security tools are the systems administrator's best friend. These tools allow administrators to perform an assessment of their systems. Reports generated from the assessment provide them with a wealth of information regarding services, ports, and potential vulnerabilities. From this they can begin the task of hardening their systems. Nessus will be used to audit the web server before and after installation and configuration. Two reports will be generated from the audit. The first report will detail services, ports, and potential vulnerabilities found prior to the hardening phase. The second report will provide a snapshot of the server after the hardening phase. We expect ports 22, 80 and 443 to be listening.

System Security Tool	
Assessment tool	Nessus
Auditing tool	NMAP
Tool written by Casper Dik of Sun Microsystems that checks for SUID/SGID	Fix-Modes

1.2.5. Access to Web Environment

Access to the Project web server will be limited to only upper management and project staff. Staff working on the project will be located across the global enterprise. Specific network requirements, as stated above, have been asked of the Network infrastructure group, which they have satisfied.

1.3. Risk Analysis

Management considers the project web server, SYSWEB, to be a critical part of the project. SYSWEB's primary function is to provide upper management and project staff a vehicle for accessing project data. Although the web server will not be exposed to the internet, it is nonetheless, susceptible to attacks from within. Anyone that believes otherwise shouldn't be in this line of work. System Administrators should always be concerned about their systems. This is not to say that they should worry about whether or not one or all of their systems are going to be compromised. As a system administrator, there should always be some level of concern. When there isn't that means that you have fallen into a state of complacency. You either don't care anymore, maybe because your job doesn't challenge you anymore; or maybe it's because you consider yourself a top notch system administrator and your blinders don't let you see that all your systems are

now in a vulnerable state. I believe the complacent administrator to be the most dangerous adversary in any systems environment. Although attacks are a primary concern, other concerns of mine are:

- Password Guessing
- Logs or the lack there of
- Vulnerable services that should have been disabled
- Proper patch management
- Buffer overflows
- Denial of service
- And. Of course, the complacent administrator

1.3.1. Concerns

I begin addressing these concerns by restating our network infrastructure. First, the project LAN has been physically separated from the corporate network by an appliance firewall. The corporate network is separated from the internet by another appliance firewall.

1.3.1.1. Outside Attacker:

The likelihood of an outsider breaking in and accessing the project web server is extremely slim. First, the attacker would have to manage to get through the outside firewall. By this time, if the network team has been doing there job, they would have encountered a few flags in there logs. Considering that an IDS monitors the outside interface and inside interface of the internet firewall. The IDS has been setup via two taps that allow it to monitor the traffic without the attacker detecting the presence of the IDS. If, for some small chance, the attacker got through, they would still have to get through the second firewall. Then considering that the firewall only has a couple of ports open (ssh http) and has been configured to accept connections only from specific subnets, the chances are very slim.

1.3.1.2. Inside Attacker:

The inside attacker is a different animal. They are already on the inside. All they have to do is gather information and plan their attack. They would have to do some social engineering for their information gathering. But luckily, in this scenario, the odds are also against the insider. First, as stated above, only specific subnets are allowed access across the project firewall. Only certain ports are open at the firewall. Even if the insider managed d to get to a machine that is on the right subnet, he or she would still have to break into the web server.

1.3.1.3. The Complacent Administrator:

If anything is worse than the two types of attackers, is the complacent administrator. In the IT world today you cannot have complacent administrators. Administrators that do not stay abreast of vulnerabilities and exploits and do not maintain their servers up-to-date with the latest patches for the latest vulnerabilities are doing a disservice. If they are not vigilant as to the state of their systems, sooner or later they will be in a world of trouble.

Sometimes it's the believe that, oh well we've never been compromised or we've never been hit by a worm. That attitude sooner or later comes face to face with the reality of a compromised environment. The most damaging part of this scenario is that by the time the system administrator is aware of it, it is somewhat difficult to trust your servers and for that matter your backups. Then the question that floats quickly to the surface is, "Where do we start?"
Fortunately, in this organization our system administrators are just the opposite. They stay abreast of the latest vulnerabilities and update our servers accordingly. Our network team has implemented Intrusion Detection Systems(IDS) at the perimeter as well as internally with the use of TAPs, which is a device that make s them virtually invisible.

1.3.1.4. Hardware failure:

Component failure could render the web server non-functional. Precautions have been taken to ensure the server's uptime. In the event of an unforeseen failure at a component level, a secondary server has been set aside that can be used to bring up the system in a minimal amount of time with minimal or no data loss.

1.3.2. Corrective Action

The actions stated below will greatly minimize the possibility of attackers, whether insiders or outsiders, gaining access to our web server. It will ensure that new servers are setup correctly and follow a policy.

1.3.2.1. Server Policy

All Information Technology Centers should have policies in place that dictate how systems are setup and configured. It should state what groups are responsible for adhering to the policy. The policy at a minimum should have a checklist (one created by a competent administrator) that everyone can follow. We have already implemented a server policy that will, hopefully, change the "Complacent administrator". The following is an example of a checklist:

- Server is physically secure
- All appropriate packages installed

- All appropriated patches have been applied
- Patch management has been instituted
- All unused services have been disabled
- telnet, rlogin, have been disabled
- SSH has been installed and configured
- Logging has been configured
- Log rotation has been instituted
- Userids not in use have been deleted
- /dev/null has been added to all accounts without a defined shell
- Network kernel parameters have been set to protect against DoS, IP Spoofing, etc…
- Appropriate file permissions have been set
- An integrity checker installed, such as Tripwire or AIDE
- Vulnerability scans performed to ensure we haven't overlooked a service
- Mount partitions as read-only and/or nosuid
- Mount options for Volume Management modified

1.3.2.2. Disabling of Boot Services

The Solaris installation of Solaris 9, even when choosing the smallest install option, "Core System Support-64 bit" installs a number of services that are not needed. These services can open up a whole new world for attacks. The more services that are enabled the higher the risk of someone exploiting a vulnerability. To minimize the possibility of vulnerabilities or holes, all services not needed will be removed from their location. These services, instead of being deleted, will be moved to another location preventing them from being executed during the boot process. If the need arises for any one of these services, they can be easily copied back to its appropriate location.

Under Solaris 9, all scripts reside in the run-level directories. These are rc?.d where ? = 0,1,2,3,5,S – 4 is not used. For a listing of all services turned off, see ***table 5***. The rule of thumb for services is, if the service is not needed, do not start it.

1.3.2.3. Implement Encryption

The principal impetus for using encryption is to prevent attackers from snooping, eavesdropping, or sniffing. OpenSSH will be used to provide project staff a secure channel to communicate with the server. All communications will go through an encrypted channel ensuring data security and integrity. The use of OpenSSH helps to augment the overall security of the server. OpenSSH is widely and used and available at www.openssh.org.

1.3.2.4. Patch Management

Sun Microsystems periodically releases a number of patches that are meant to correct programming bugs or security flaws. These patches are bundled into a package called, "os_version_recommended". These are required to mitigate any possible problems the operating environment may have.
The recommended patches will be applied to our web server only have they have been tested on our demo system.

Caveat:

Sun support requires that your server be up-to-date on its recommended patches in order to receive support.

1.3.2.5. Fix-modes

Fix-modes is a script written by Casper Dik that scans the file systems and makes modification to file and group permissions. It will be used to further harden our web server by changing the permissions on those files that have excessive rights by default. Addition of applications and patches can introduce files with excessive rights as well as undo changes committed by Fix-modes. As a result, Fix-Modes will be used periodically to make this does not happen.

1.3.2.6. Modification of Network Parameters

Most attackers when first looking for a victim will scan networks in search of information. Based on the information gathered, they choose their victim(s). Under the Solaris operating system, the information a server provides can be either minimized or turned off completely. Solaris has a number of modifiable network parameters that can be changed for specifically this reason. Some actions negated to attackers once implemented are:

- Mapping and Smurfing
- SYN floods
- ICMP redirects
- IP forwarding

1.3.2.7. Physical Security

Physical security is one of the most important aspects of the overall security policy. Our web server will be located in the DTC or Data Technology Center. Entrance to the center requires key card access at three different locations. Access to one does not automatically give you access to the others. The server's location negates the possibility

of anyone walking up to it and maliciously bringing it down or rebooting it with a CDROM and installing a backdoor of some kind.

1.3.2.8. Periodic Testing

There is only one method of determining that our web server has not contracted, either by the installation of new programs or the application of patches, new bugs or vulnerabilities. And that is by testing. The server will be tested for vulnerabilities and open ports with the use of assessment tools such as Nessus and Nmap.

2. Operating System Installation

2.1. Physical Location

The web services server will be located at the Data Technology Center (DTC) at Corporate Headquarters. Entrance to the building is secured by security guards; all non-employees are required to sign-in and are escorted to their destination. Access into the Data Technology Center requires keycard access at three locations. This type of access has been limited to system administrators, print operators, and the Information Technology Office's upper management. Individuals requiring access to the DTC are given an extensive background check and are required to be finger printed by local law enforcement.

Note
In the event your server cannot be physically secured, you should at least lock it down where no-one can come up to it, insert a bootable cdrom and reboot your system. Once the system boots up, they can very easily do anything with it.

The OpenBoot Prom has two security modes that can help. These are:

- "command" security mode
- "FULL" security mode

"Command" security mode prevents anyone from modifying the EEPROM and executing any OBP commands while at the OBP prompt. The "FULL" security mode is comprised of all the "command" security mode offers, plus the system will not boot unless the correct OpenBoot Prom password is provided. The only downside to this setup is that whenever the server reboots someone has to be there to enter the password. But, nevertheless, is better than having your server exposed.

Setting the EEPROM to full:

```
#eeprom security-mode=full
```

Changing Prom password:
New Password: *********
Retype new password: ********

Once the security-mode is set, you can use the following command to change the EEPROM password periodically.

#eeprom security-password=
Changing Prom password:
New password: ******
Retype new password: ******

Another effective command to use is "security-#badlogins". This command allows you to monitor OBP password guessing. Simply executing the following command will give a count of bad login attempts.

#eeprom security-#badlogins
security-#badlogins=9

To reset, simply execute:

#eeprom security-#badlogins=0

A word of CAUTION, if you forget your eeprom password, you will have to contact SUN and have your eeprom replaced.

2.2. Pre-installation

At the DTC, an isolated network has been established for the sole purpose of setting up servers. The new web server will be connected to this network and the installation begun. This ensures that servers can be setup without the possibility of them being compromised.

Another system will be used to connect to the production network and download patches for Solaris 5.9 as well as any third party software. Verification of all downloads will be performed to ensure downloads have not been tampered.

To being the installation, a PC running terminal emulation was used along with a Null modem cable for communication via the serial port. Two adapters and a cat 5 patch cable were used to create a Null modem cable. The pinout for the Null terminal adapter is listed below.

Table 1

Null terminal pinout DB9 to DB9: [Top of Page] [Pin ID]
Used in connecting 2 computers without modem signalling capability. You usually have to build this cable

```
yourself.
```

```
DB9       DB9
----      ---
3 TD   -- 2 RD
2 RD   -- 3 TD
5 GND  -- 5 GND
```

Connect the serial cable to the Sun Server and bring up the terminal emulation window. There are a number of terminal emulators that can be downloaded off of the internet, or you can use HyperTerminal that comes packaged with any Windows operating system.

2.2.1. Solaris Initial Phase

To begin the installation process, insert the "Solaris9 CD 1 of 2" into the cdrom and turn your system on.

Note: Do not attach your system to the network unless it is an isolated network and has been setup strictly for configuring systems. Ensuring the integrity of your system is of utmost importance.

The system will go through a post phase and stop at the Open Boot Parameter (OBP) prompt also known as the "ok" prompt. The OBP is used extensively by system administrators when configuring Sun Systems. This low-level interface provides direct access to system resources and devices attached to the system [10].

The following table lists some of the commands available in OpenBoot version 4.*x*.

Table 2 – Open Boot Prompt Parameters

pci-probe-list	*7,c,3,8,d,5,13*	*7,c,3,8,d,5,13*
local-mac-address?	*false*	*False*
fcode-debug?	*false*	*False*
ttyb-rts-dtr-off	*false*	*False*
ttyb-ignore-cd	*true*	*True*
ttya-rts-dtr-off	*false*	*False*
ttya-ignore-cd	*true*	*True*

At the "ok" prompt, now with Solaris9 CD 1 of 2 in the tray, enter "boot cdrom". This will launch the installation process.
The following is a summary of the various prompts the administrator will encounter. I consider this part the initial phase of the installation. At this point you are basically providing the installation process with information regarding language, location, whether the server is networked or not, etc … They are basic and you shouldn't have any trouble.

Table 3 - Solaris Installation - Initial Phase

Prompt	Answer
Ok prompt	ok boot cdrom
Language	0)English
Locale	0)English (C - 7-bit ASCII)
Terminal type	1) ANSI Standard CRT
Network Connectivity – this server is attached to an isolated network. Therefore, we choose "yes". **Security Note** If you do not have an isolated network and the server is disconnected, select Networked as well.	Networked Yes X
DHCP Yes/No	No
Host Name	Hostname: secweb
IP Address	address:10.100.10.10
Part of a subnet	Yes
Netmask **Note: *make sure this is correct or else you'll experience connectivity issues*	255.255.255.0
IPv6	No
Default Route – server is isolated - choose None	None
Confirm the following information.	Networked: Yes Use DHCP: No Host name: sysweb IP address: 10.100.10.10 System part of a subnet: Yes Netmask: 255.255.255.0 Enable IPv6: No Default Route: None
Kerberos security	No
Name Service	None
Time Zone	United States - Eastern Time
Accept the default date and time or enter new values **Security Note: Ensure the date and time are correct. This is extremely important for	Date and time: 2004-08-16 15:51 Year (4 digits): 2004 Month (1-12): 08 Day (1-31): 16

time sensitive files such as logs. We'll ensure date and time are properly maintained by installing NTP later in this document.	Hour (0-23): 15 Minute (0-59): 51
System identification complete. Generating software table of contents [this may take a few minutes...] Table of contents complete. Starting Solaris installation program...	
Solaris Interactive Installation If the server you are configuring previously had an OS, you will be prompted with a message stating, "This system is upgradable, so there are two ways to install the Solaris software. The Upgrade option updates the Solaris software to the new release,… The Initial option overwrites the system disks with the new version of Solaris software.	Choose "Initial"

2.2.2. Solaris Interactive Installation

At this point we are ready to choose where to install from and select the software group that best meets our needs. For our distribution we are going to choose "Core System Support 64-bit". This provides the smallest set of core files needed for our server. We will later examine the installation to ensure we haven't missed anything.

There are two ways to install your Solaris software: - "Standard" installs your system from a standard Solaris Distribution. - "Flash" installs your system from one or more Flash Archives.	Select "Standard"

Select the geographic regions for which support should be installed.	North America -U.S.A. (en_US.ISO8859-1)

Select the Solaris software to install on the system. NOTE: After selecting a software group, you can add or remove software by customizing it. However, this requires understanding of software dependencies and how Solaris software is packaged. The software groups displaying 64-bit contain 64-bit support	Entire Distribution plus OEM support 64-bit 2426.00 MB [ ] Entire Distribution 64-bit ..... 2386.00 MB [ ] Developer System Support 64-bit ..... 1881.00 MB [ ] End User System Support 64-bit ..... 1406.00 MB [X] Core System Support 64-bit ..... 684.00 MB

On this screen you must select the disk for installing the Solaris software. We'll choose c0t0d0 at this point and later mirror it with c0t2d0.	Disk Device (Size)[39GAvailable Space [X] c0t0d0 (38162 MB) boot disk 38162 MB [ ] c0t2d0 (38162 MB) 38162 MB

Automatically Layout File Systems?	Choose "Manual Layout"

Reboot After Installation?	Yes

2.2.3. Disk Partitioning

When it comes to disk partitioning, system administrators have their own preference. At a minimum, you must create root /, and swap. It is not the best partitioning scheme, but it works. But just because it works doesn't mean you should use it.
A better scheme is to at least create /, /usr, /opt, and /var. This scheme provides the flexibility to lock down some of your file systems, easier for backups.
Typically, when an attacker is successful, the first thing they will do is cover up their tracks by installing some form of rootkit, typically under /usr, and then creating a backdoor for him or herself to get back in.
With /usr as its own partition, access controls can be enabled. For instance, the /usr partition can be setup under the vfstab file to "ro", read only, hampering the attackers predisposed actions.

For our installation we have chosen the scheme shown in the table below.

Table 4 Disk Partioning Scheme

File System/Mount point	Disk	Slice Size
/	c0t0d0s0	10000 MB
Swap	c0t0d0s1	2000 MB
Overlap	c0t0d0s2	38162 MB
/usr	c0t0d0s3	10000 MB
/opt	c0t0d0s4	10000 MB
/var	c0t0d0s5	5000 MB
(to be used for metadb mirroring information)	c0t0d0s7	256 MB

Once the installation completes, the system will automatically reboot.

2.2.4. Network Configuration

During the installation process we deferred configuration of the router and name server.

- Under /etc, create a file "defaultrouter" and add your gateway address, which is also your default router.

```
#cd /etc
#vi defaultrouter
10.100.10.10
~
~
~
~
:wq                    ------- save and quit
```

Next, disable IP forwarding by creating a file under /etc called "notrouter". This will also prevent in.routed and in.rdiscd from loading at boot time.

- During the installation the Name Sever/Search Domain were deferred. To define the name server and search domain perform the following:

```
#cd /etc
#vi resolv.conf
search    nebulus.org
nameserver   10.100.10.20
:wq                          ---------- save and quit
```

2.2.5. Patch Update

Vulnerabilities are found daily all across the spectrum. They are not specific to any one product, although, at times it seems like it is, but we will not mention Microsoft. But nevertheless, system administrators must stay vigilant and maintain their systems up-to-date on all patches. All it takes is one small vulnerability and your system is someone else's. Remember to perform the "Patch Update" only after all additional needed packages have been determined and applied. Installing packages after the patch update will render the system with un-patched packages that could possibly have vulnerabilities or bugs. To ensure our system is up to date, download the latest "Recommended" patch bundle from Sun Microsystems.

Go to: ftp://sunsolve.sun.com/pub/patches/9_Recommended.zip

Copy or move the patch bundle to /tmp and unzip it.

```
#unzip 9_Recommended.zip
#ls
9_Recommended       9_Recommended.zip
#cd  9_Recommended
#./install_bundle          ---------- This executes the script and installs all patches
```

The bundle comes with an installation script to automate the install process. Once completed, reboot your system. On reboot all contents found under /tmp are removed. If you choose to use a temporary location other then /tmp follow the instructions below to perform a "rm –R" to remove 9_Recommended.zip and the extracted contents found under 9_Recommended.

Use the following syntax to remove all:

Note: Ensure you're in the correct directory before performing "rm –R". Or else the results could be devastating. You might just have to reinstall your operating system.

#cd /*your_temp_directory*
#ls
9_Recommended 9_Recommended.zip
#rm –R *
The above syntax removes all files under /your_temp_directory including subdirectories.

Always test patches on a non-production system before pushing them out. Although patches are written to correct bugs, sometimes they are not very friendly with other applications.

2.3. Hardening the Operating Environment

2.3.1. System Accounts

System accounts is the subject that sometimes goes unnoticed unless there is an established policy. This policy should dictate what accounts, if any, will be removed. It should also state those accounts that will remain, but will be disabled.
By default, solaris sets up a number of accounts for various services. The system administrator should look at these and determine which accounts will not be used, and either remove them or disable them. Of course, if there is a set policy for user accounts, then the policy should be followed.
Some user accounts that were created during installation are [12]:

- uucp
- nuucp
- listen
- lp
- nobody
- smmsp

Once these files are removed, "/dev/null" should be included for all non-authorized and all non-root users as their default shell.[1]

2.3.2. Superfluous Services

You might ask, "Why disable services?" The reason is simple. If you don't need them, turn them off. A good rule of thumb is, the fewer the services, the lesser the chance of having a vulnerability. Many attacks are successful because of services left enabled by the administrator that had no place in the environment in the first place. Sometimes administrators become complacent and disconnected from their environments, which lead to the OS not being properly patched and secured.

Lets begin by examining the various run-level scripts. From this we can determine which services we don't need based on the server's role. Keep in mind, this server will be providing web services and secure shell and not much more. A couple of excellent

[1] Nortel Networks, Solaris 8 and 9 Operating System Hardening Guideline

quotes to keep in mind are, "Patches protect you from problems we already know about" and "Disabling a service protects you from undiscovered exploits" [11]. You just can't explain it any clearer. Patch management and disabling un-needed services is a very important part of system administration. This alone will add a degree of difficulty for anyone trying to break into your system.

2.3.3. Boot Services

Unlike other operating systems, services running under Unix have to be manually executed. The operating system does not automatically bring them up. To automate process, there are a number of scripts written for each specific service that are executed during the boot process. Based on the run-level initiated by the administrator, the OS executes a number of scripts found under /etc/rc0.d, /etc/rc1.d, /etc/rc2.d, /etc/rc3.d, or /etc/rcS.d.
Disabling of services can be accomplished in one of two ways:

- The script for the specific service can be renamed
- Or you can create a directory such as ".asSupplied" and copy all unnecessary scripts to it.

For this document we'll create a folder called ".asSupplied" under rc?.d. The question mark refers to the run-level and the dot in front of "asSupplied" makes the directory hidden. These directories will be used as our repository for all unneeded scripts.

The services that are not needed are as follows:

Table 5 - Unneeded Services

Service	Description
S71ldap.client	Starts ldap cache manager
S71rpc	Starts rpc
S73nfs.client	Starts lockd and statd; mounts remote file systems
S88sendmail	Starts sendmail; if mail is not needed, this service can be disabled; if it is, configure sendmail for outbound only; stop it from listening
S30sysid.net	Automatically configures basic network functions; if this disabled, the functions have to be performed manually
S71sysid.sys	Automatically configures basic network functions; if this disabled, the functions have to be performed manually
S72autoinstall	Automatically configures basic network functions; if this disabled, the functions have to be performed manually

S15nfs.server	Starts up remote file sharing daemons
S74autofs	Start automounter daemon
S76nscd	Starts up the name service cache daemon
S89PRESERVE	Recovers data from unsaved vi sessions

The following represents the syntax for moving all unneeded services over to te .asSupplied directory. In the event a service is needed in the future, all that need to be done is copy the script out of .asSupplied.

```
First, cd over to /etc/rc2.d:

#cd /rc2.d
#mkdir asSupplied
#mv S71ldap.client S71rpc S73nfs.client S88sendmail  S30sysid.net S71sysid.sys
S72autoinstall ./asSupplied

Next, remove the CacheFS script as well as the NFS script found in /etc/rc3.d. If there
isn't a need to perform NFS mounts, then remove it. If the need arises, the system
administrator can always re-enable it.

#cd /etc/rc3.d
#mv S15nfs.server  S73cachefs.daemon ./asSupplied

Next, move all unneeded scripts from under /etc/rcS.d to ./.asSupplied

#cd /etc/rcS.d
#mv S35cacheos.sh S41cachefs.root ./.asSupplied
```

2.3.4. Tightening down the System Default Umask

The Solaris Operating Environment installs with a default system file mode creation of 000. This basically means that any files created by any of the services running are by default readable and writable by everyone. In order to correct this problem a script has to be created that sets the default mask to 022. Create the script under the /etc/init.d directory, then create hard links from each of the rc?.d directories to the newly created script. This script must be one of the first to execute out of the rc?.d directories, so give it a name such as S00umask022.sh. See below.

Table 6 - Script for umask 022

```
touch /etc/init.d/umask022.sh
chmod 744 /etc/init.d/umask022.sh
chgrp sys /etc/init.d/umask022.sh
```

```
for i in /etc/rc?.d; do ln /etc/init.d/umask022.sh $i/S00umask022.sh; done
```

2.3.5. Network Parameters

There are a number of tunable network parameters that can be set under Solaris to harden your system against certain network attacks. These attacks if directed at your system can cause your system to become non-responsive.

As your system is booting up, one of the boot up processes is to initialize all network interfaces. This process is performed by the initinet script found under /etc/init. When this script runs, it sets all tunable network parameters to their system defaults. This means that if you wish to set the parameters to something other then their defaults you will need to run a script after the all network interfaces have been initialized. Preferably, you will want to perform this immediately after "initinet" runs to ensure that no-one can affect your system before the parameters have changed.

In order to accomplish what has been stated above, we will need to create a script called "nddconfig". This script will reside under /etc/init and will execute the commands that will provide the new settings.

Create the script:

touch /etc/init.d/nddconfig

Next, create a soft link:

ln –s /etc/init.d/nddconfig /etc/rc2.d/S80nddconfig

Once the file has been created and appropriate permissions set, add the following lines to it.

Contents of nddconfig:

- ndd –set /dev/tcp tcp_conn_req_max_q0 8192
- ndd –set /dev/tcp tcp_ip_abort_cinterval 60000
- ndd –set /dev/ip ip_respond_to_timestamp 0
- ndd –set /dev/ip ip_respond_to_timestamp_broadcast 0
- ndd –set /dev/ip ip_respond_to_address_mask_broadcast 0
- ndd –set /dev/ip ip_forward_directed_broadcasts 0
- ndd –set /dev/arp arp_cleanup_interval 60000
- ndd –set /dev/ip ip_ire_arp_interval 60000
- ndd –set /dev/ip ip_ignore_redirect 1
- ndd –set /dev/ip ip_send_redirects 0
- ndd –set /dev/ip ip_forward_src_routed 0
- ndd –set /dev/ip ip_forwarding 0

- ndd –set /dev/ip ip_strict_dst_multihoming 1

The nddconfig script should look as follows:

Table 7 - nddconfig script

```
#!/sbin/sh
#
#
#
#
ndd -set /dev/tcp tcp_conn_req_max_q0 8192
ndd -set /dev/tcp tcp_ip_abort_cinterval 60000
ndd -set /dev/ip ip_respond_to_timestamp 0
ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
ndd -set /dev/ip ip_respond_to_address_mask_broadcast 0
ndd -set /dev/ip ip_forward_directed_broadcasts 0
ndd -set /dev/arp arp_cleanup_interval 60000
ndd -set /dev/ip ip_ire_arp_interval 60000
ndd -set /dev/ip ip_ignore_redirect 1
ndd -set /dev/ip ip_send_redirects 0
ndd -set /dev/ip ip_forward_src_routed 0
ndd -set /dev/ip ip_forwarding 0
ndd -set /dev/ip ip_strict_dst_multihoming 1
```

2.3.6. Stop the Attack on the Stack

There is a feature that was introduced into Solaris 6 and later that allows a system administrator to make the system stack non-executable. This feature came about because of programs that would try to overwrite parts of the program stack of a privileged program in an attempt to control it. All 64 bit processes on Solaris 7 and later use non-executable stacks by default.

To set make the stack non-executable you would add the following lines in /etc/system.

```
set noexec_user_stack = 1
set noexec_user_stack_log = 1
```

2.3.7. Sequencing

The TCP initial sequence number generation parameters should be set to 2 to enable RFC 1948 sequence number generation. This makes it more difficult to hijack a session by predicting TCP sequencing. The file to modify is found under /etc/default and it's called inetinit. Edit the file and search for the following parameter and set it to a value of 2.

- **TCP_STRONG_ISS=2**

2.3.8. Modify Inetsvc

The script inetsvc is responsible for starting a number of services that are unnecessary. Looking carefully at the script, there is only one line that applies to our server. Unless, of course, you are utilizing DHCP and/or DNS, in which case the modifications would be minimal. For this script, delete all lines except the following line:

/usr/sbin/ifconfig -auD4 netmask + broadcast +
The highlighted portion of the following script is the only line left after the modification. All other lines are comments.

```
#!/sbin/sh
#
# Copyright 2004 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
#ident  "@(#)inetsvc    1.31    04/03/16 SMI"

#
# This is third phase of TCP/IP startup/configuration.  This script
# runs after the NIS/NIS+ startup script.  We run things here that may
# depend on NIS/NIS+ maps.
#
# Re-set the netmask and broadcast addr for all IP interfaces.  This ifconfig
# is run here, after waiting for name services, so that "netmask +" will find
# the netmask if it lives in a NIS map. The 'D' in -auD tells ifconfig NOT to
# mess with the interface if it is under DHCP control
#
/usr/sbin/ifconfig -auD4 netmask + broadcast +
```

2.4. Password Aging

Password aging, a process that is not popular among users, but, nevertheless, an important part of any system. To change the setting for password aging, edit the File passwd found under /etc/default. The variable to change is:

- MAXWEEKS=6

2.5. Console Logins

To ensure that no-one logs on remotely using the root account, change the setting in the file *login* found under /etc/default to reflect the following:

- CONSOLE=/dev/console
- If you don't want root login in from anywhere use:
  CONSOLE=/etc/default/login

2.5.1. Mount Options

Another important feature of file system partitions is "Mount Options". Mount options provide the system administrator with a level of flexibility that allows him or her to further secure file systems. Attackers look for ways of escalating their privileges. A method by which they escalate their privileges is by the use of set-user-id (SUID) executables. These executables are attractive to them because when executed they run with the owners or groups privileges – not the person who executes them.

The mount options for file systems are:

- read only (ro)
- read – write (rw)
- no set-user-id (nosuid)
- logging

Table 8 - vfstab with no options

VFSTAB before applying options						
#device #to mount #	device to fsck	mount point	FS type	fsck pass	mount at boot	mount ptions
fd	-	/dev/fd	fd	-	no	-
/proc	-	/proc	proc	-	no	-
/dev/dsk/c0t0d0s1	-	-	swap	-	no	-
/dev/dsk/c0t0d0s0	/dev/rdsk/c0t0d0s0	/	ufs	1	no	-
/dev/dsk/c0t0d0s3	/dev/rdsk/c0t0d0s3	/usr	ufs	1	no	-
/dev/dsk/c0t0d0s5	/dev/rdsk/c0t0d0s5	/var	ufs	1	no	-

/dev/dsk/c0t0d0s4	/dev/rdsk/c0t0d0s4	/opt	ufs	2	yes	-
swap	-	/tmp	tmpfs	-	yes	-

As mentioned above, attackers like to use SUID executables to escalate their privileges. File systems mounted with the "nosuid" option ignore the SUID bit, thereby negating the attacker the ability to execute these types of files. Below is the vfstab showing the various mount options for the different partitions.

Table 9 - vfstab with options

VFSTAB before applying options						
#device	device	mount	FS	fsck	mount	mount
#to mount	to fsck	point	type	pass	at boot	ptions
#						
fd	-	/dev/fd	fd	-	no	-
/proc	-	/proc	proc	-	no	-
/dev/dsk/c0t0d0s1	-	-	swap	-	no	-
/dev/dsk/c0t0d0s0	/dev/rdsk/c0t0d0s0	/	ufs	1	no	-
/dev/dsk/c0t0d0s3	/dev/rdsk/c0t0d0s3	/usr	ufs	1	no	ro
/dev/dsk/c0t0d0s5	/dev/rdsk/c0t0d0s5	/var	ufs	1	no	nosuid
/dev/dsk/c0t0d0s4	/dev/rdsk/c0t0d0s4	/opt	ufs	2	yes	nosuid,ro
swap	-	/tmp	tmpfs	-	yes	-

Note:

Although these file systems can be mounted as shown above, the options can be changed. For example, a file system mounted as read-only (ro) can be easily remounted as a read-write partition. The same is true of file systems mounted as no-set-user-id (nosuid). The only caveat to this is that to bring them back to their original, for instance as shown above, state requires a reboot. Keep a watch on log files for any unscheduled reboots.

SUID & SGID

Let's talk about Set-User-ID (SUID) and Set-Group-ID (SGID) bits. These are two bits that when not used properly or used with security in mind, can leave your system wide open or allow an individual to escalate his or her privileges. There are a number of files under Solaris that are marked SUID or SGID for the purpose of allowing an ordinary user to perform certain functions that require higher privileges. The problem with these bits stems from the fact that some executables have flaws and some of these flaws can allow an attacker to escalate their privileges or allow them to hide a backdoor, say a SUID executable of their choice, for later use.

- *Some examples of SUID root programs are:*[11]
  - *logging in*
  - *changing passwords*
  - *low level networking routines*
  - *control of graphical display functions*
  - *su*

- *Thomas Akin's Seven Rules for Safe SUID Programming*[2]

  - *Do not use SUID shell scripts.*
  - *Never use SUID C-shell scripts.*
  - *Always manually set your internal field separator (IFS).*
  - *Always manually set your PATH and use absolute path names.*
  - *Understand how programs you call work, and how they handle arguments.*
  - *Do not use temporary files. If you must, don't put them in a publicly writeable area.*
  - *Distrust and check all user input and eliminate dangers such as meta-characters.*

Change your mount options on those file systems that do not have any SUID or SGID files. This will negate the possibility of an attacker wanting to execute a SUID file in other file system partitions.

To find out what files are marked as SUID or SGID, run the following command:

```
Find / -type f \( -perm –u+s –o –perm –g+s \) –ls
```

.

2.5.2. Solaris Volume Management

Volume management is a method of mounting and un-mounting floppy disks and CDROMs without user intervention. The daemon "vold" automatically mounts the floppy or CDROM whenever it is inserted. Obviously, this would make a user's life much easier. But it also makes it easier for attackers. The Volume Management system supports SUID file systems for any removable media that supports it. If this system is needed, then mount options should be specified for the media.
The daemon "vold" uses the rmmount command to mount the removable media device. It uses a configuration file, located under /etc/, to determine how to mount the media. This configuration file should reflect the lines below:

```
mount hsfs –o nosuid
mount ufs –o nosuid
```

[2] Tom Akins' "Dangers of SUID Shell Scripts"
http://www.samag.com/documents/s=1149/sam0106a/0106a.htm

2.5.3. Syslog Logs

Logging is a process by which systems and applications document information regarding system processes, abnormal terminations, warnings, and errors. Logs are extremely important with respect to computer forensics. Without logs, administrators would be incapable of tracing a compromise. The syslog daemon is the process responsible, within the Solaris Operating Environment, for logging. Syslog reads a file found under /etc that defines what types of messages it will record and to where. The configuration file is, syslog.conf. By default, syslog is configured to send log messages to:

/var/adm/messages - majority of system messages come here
and
/var/log/syslog - mail messages come here

Another log defined in syslog.conf collect messages regarding authentication. Although, this log is defined, it is not enabled. To enable, simply edit the syslog.conf file located under /etc, search for "auth" (without the quotes), and uncomment it.

```
cd /etc
vi syslog.conf

The highlighted line is the line that should be uncommented.

#ident  "@(#)syslog.conf        1.5     98/12/14 SMI"   /* SunOS 5.0 */
#
# Copyright (c) 1991-1998 by Sun Microsystems, Inc.
# All rights reserved.
#
# syslog configuration file.
#
# This file is processed by m4 so be careful to quote (`') names
# that match m4 reserved words.  Also, within ifdef's, arguments
# containing commas must be quoted.
#
*.err;kern.notice;auth.notice                   /dev/sysmsg
*.err;kern.debug;daemon.notice;mail.crit        /var/adm/messages

*.alert;kern.err;daemon.err                     operator
*.alert                                 root

*.emerg                                 *

# if a non-loghost machine chooses to have authentication messages
# sent to the loghost machine, un-comment out the following line:
```

```
auth.notice             ifdef(`LOGHOST', /var/log/authlog, @loghost)

mail.debug              ifdef(`LOGHOST', /var/log/syslog, @loghost)

#
# non-loghost machines will use the following lines to cause "user"
# log messages to be logged locally.
#
ifdef(`LOGHOST', ,
user.err                        /dev/sysmsg
user.err                        /var/adm/messages
user.alert                      `root, operator'
user.emerg                      *
```

This will provide us with added valuable information. All logs become important building blocks in reconstructing a compromise.

2.5.4. System Banners

System banners should be the first text on the screen a user sees after he or she logs in. Law enforcement believes they stand a better chance at prosecuting an attacker if banners are displayed. An example of banner follows:

```
#
# The system you are accessing is for authorized use only. Anyone using this computer
# is subject to being monitoring. Any illegal activity generated as a result of login into this
# system will be provided to law enforcement in response to criminal prosecution.
#
# All users login into this system consent to monitoring.
```

Adding a system banner is rather simple. Go to /etc and modify ***motd*** and ***issue*** adding the verbiage approved by your legal counsel. These two files provide banners at login.

2.5.5. Sendmail

Although mail systems always seem to be a part of any server, for our web environment we will not be using one. All our logs will be sent to a central log server filtering the logs based on pre-defined rules. The central log server will then email, and page the administrators if any logs match the rules.

2.6. Apache Web Server – Installation and Configuration

Apache web server is one of the most widely used web servers out there. Although it's popularity is high, it has seen its share of vulnerabilities. Its imperative that administrators stay abreast of new vulnerabilities by subscribing to some of the security lists such as bugtrac, CERT, SANS, etc….

To download go to www.apache.org:

First, download apache-1.3.31.tar.gz into /tmp.

"cd" into /tmp and untar your apache tar ball.
#tar -xvf apache-1.3.31.tar.gz

create a symbolic link :
#ln –s apache-1.3.31 httpd ----this is optional

"cd" into httpd and perform the following:

#./configure -- prefix=/www/httpd -- sysconfdir=/www/conf -- enable-module=rewrite – enable-module=so -- enable-module=status

Compile

#make

Install apache

#make install

Modify Configuration File

```
 ###Section 1: Global Environment
#
ServerType standalone
#
ServerRoot "/www/httpd"
#
ExtendedStatus On
#
###Section 2: 'Main' server configuration
#
Port 80
#
ServerAdmin yourusername@yourservername
#
ServerName sysweb ( you servers`s name )
#
```

```
DocumentRoot "/www/wwwdocs"
#
<Directory "/www/wwwdocs">
#
      AllowOverride All
#
HostnameLookups   On
#
ErrorLog /usr/local/etc/httpd/logs/error_log
#
<Location /server-status>
      SetHandler server-status
      Order deny,allow
      Deny from all
      Allow from sysweb ( your server's name )
</Location>


###Section 3: Vitual Hosts
I set up a virtual host for my netx3 server. I leave the example
<VirtualHost> </VirtualHost> as is and place my <VirtualHost>
information below it.
NameVirtualHost 127.0.0.1:80
#
<VirtualHost 127.0.0.1:80>
      ServerAdmin root@netx3
      DocumentRoot      /www/wwwdocs/project
      Servername  sysweb
      ErrorLog    /www/logs/localhost
      CustomLog   /www/logs/sysweb/access-log combined
</VirtualHost>
```

2.7. OS Hardening with Third Party Software

Now that we have a minimized version of Solaris installed and have hardened the OS as much as we can, it is time to augment the installation by adding third party software.

2.7.1. Fix-Modes

Fix-Modes is a set of scripts written by Casper Dik of Sun Microsystems. His intention in writing these scripts was to have a tool that could easily scan all files, devices and directories, based on those listed under /var/sadm/install/contents, and be able to remove all "group and world writable" permissions and change ownership to root. Although this tool has had an acceptance in the Sun community, Sun has not officially accepted it.

To install and apply Fix-Modes perform the following steps.

First of all, you need to get your hands on a copy of Fix-Modes.

Go to:
http://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/fix-modes/
and download fix-modes.tar.gz

move the file to /tmp or your temporary location of choice.
#mv fix-modes.tar.gz /tmp
#gunzip fix-modes.tar.gz
#tar –xvf fix-modes.tar

#cd fix-modes
#make (include CC=gcc if using gcc)

To execute:
#./fix-modes ---------- (launches fix-modes)

2.7.2. TCPWrappers

TCP Wrappers is a program written by Weitse Venema as a method of logging and filtering requests by various network services. For our installation we'll be using TCPWrappers to augment the security of SSH. The program can be downloaded from Weitse Venema's site at:

- ftp.porcupine.org/pub/security/index.html

Installing TCPWrappers:

The installation of TCPWrappers is rather simple. Go to the above site and download **`tcp_wrappers_7.6-ipv6.4.tar.gz`**

Once downloaded. Move the file to a temporary directory such as /tmp.
#mv tcp_wrappers_7.6-ipv6.4.tar.gz /tmp

Next, unzip and untar it;

#gunzip tcp_wrappers_7.6-ipv6.4.tar.gz
#tar –xvf tcp_wrappers_7.6-ipv6.4.tar
cd tcp_wrappers_7.6-ipv6.4

Next, we need to make some changes to the make file:
vi Makefile

Search for the following lines and uncomment the second line.
# SysV.4 Solaris 2.x OSF AIX
REAL_DAEMON_DIR=/usr/sbin

Search for the next set of lines:

```
# SunOS 5.x is another SYSV4 variant.
sunos5:
	@make REAL_DAEMON_DIR=$(REAL_DAEMON_DIR) STYLE=$(STYLE) \
	LIBS="-lsocket -lnsl" RANLIB=echo ARFLAGS=rv VSYSLOG= \
	NETGROUP=-DNETGROUP AUX_OBJ=setenv.o TLI=-DTLI \
	BUGS="$(BUGS) -DSOLARIS_24_GETHOSTBYNAME_BUG" all
```

Once found, change the fourth line (start couting with SunOS 5.x) to read:
LIBS="-lsocket -lnsl" RANLIB=echo ARFLAGS=rv CC=gcc VSYSLOG= \
The highlighted portion marks the change.

Search for the string "IPV6 = -DHAVE_IPV6". When you find it, uncomment it. The line should look as follows (Failure to do this will result in 0.0.0.0 as the log address.):

IPV6 = -DHAVE_IPV6

The default setting for LOG LEVEL and LOG FACILITY are LOG_MAIL and LOG_INFO. If you need to change do so at this time. If you are not sure about the possible values, look at /usr/include/sys/syslog.h.

Next, compile the source based on your OS version and revision. The OS version and revision can be easily determined with the next command:

#uname –sr

make sunos5

Configuring inetd.conf to include tcpd (tcpwrappers daemon)
First, we need to copy the tcpd binary to /usr/sbin:
cp -p /var/tmp/tcpd/tcpd /usr/sbin;

Lets now create a backup copy of inetd.conf:

cp -p /etc/inetd.conf /etc/inetd.conf.orig

Now we'll cd into /etc and edit inetd.conf:

#cd /etc
vi inetd.conf
.
.
telnet stream tcp6 nowait root /usr/sbin/in.telnetd in.telnetd
should now read:
The example above with the telnet daemon should read as follows:
telnet stream tcp6 nowait root /usr/sbin/tcpd in.telnetd

Similarly, make changes to all the services you want. Save your changes and exit out of vi.
Send a HUP to inetd to re-read the configuration file.
pkill -HUP inetd

Modify Syslog:
Since the facility and log level were never modified when TCP wrappers was compiled, we don't need to make any changes to syslog. Next, we'll test our installation and make sure it is working.

Testing TCPWrappers:

From another machine, telnet into the system running tcpwrappers. Then check out the tail end of syslog. Their should be a line as follows:

Aug 10 10:12:02 sysweb in.telnetd[294]: connect from systest

Tightening Down with TCPWrappers:

To further take advantage of what TCPwrappers offers, create two hosts files under /etc. The files to be created are *hosts.allow* and *hosts.deny*. The syntax to use within these files is as follows:

- service-list:host-list

These files will be used to identify those systems that will be able to access our system based on service and ip address, sebnet, or domain.

Make sure the hosts.deny file contains the ALL:ALL statement. This will deny everyone else that does not meet the hosts.allow test.

Next we'll install and configure OpenSSH, but before we do, we need to install a few dependencies. OpenSSH requires zlib and OpenSSL to function. First, download zlib from:

http://www.zlib.net/zlib-1.2.1.tar.gz.

OpenSSL can be downloaded from:

http://www.openssl.org/source/openssl-0.9.7d.tar.gz

OpenSSH can be downloaded from:

http://www.openssh.org

2.7.3. Installation and Configuration of OpenSSH

As we have mentioned, OpenSSH is dependent on zlib and openssl. Now that we have downloaded the dependencies, move them to a temporary directory such as /tmp.

ZLIB Installation:

```
cd /tmp
gunzip zlib-1.2.1.tar.gz
tar –xvf zlib-1.2.1.tar
Next,

cd zlib-1.2.1
./configure
make
make install
```

ZLIB should now be installed.

Next, install OpenSSL:

OpenSSL Installation:

Note: The auto configuration script that is part of the OpenSSL package requires Perl version 5. Ensure you have the correct version of Perl. If not, go to the following url and download it.

http://www.perl.com/CPAN/src/perl5.005_03.tar.gz

The procedure for installing it is basically the same as that for ZLIB above.

```
cd /tmp
gunzip openssl-0.9.7d.tar.gz
tar –xvf openssl-0.9.7d.tar
cd openssl-0.9.7d
./config
make
make install
```

Now that we have both ZLIB and OpenSSL installed, we can proceed with the installation of OpenSSH.

OpenSSH Installation

Move the OpenSSH download to your temporary directory.

```
cd /tmp
gunzip  openssh-3.9p1.tar.gz
tar –xvf  openssh-3.9p1.tar
cd openssh-3.9p1

setenv CFLAGS –I /usr/local/include
setenv LDFLAGS –I /usr/local/lib

./configure –prefix=/usr/local –with-tcp-wrappers –without-rsh –disable-suid-ssh
make
```

Once the above has completed, copy the binaries, sshd and ssh-keygen to /usr/bin. Also copy ssh_prng_cmds to /usr/local/etc.

Next, modify the sshd.config file found under /etc/ssh. Your changes should look as follows:

```
Port 22
ListenAddress 0.0.0.0
SyslogFacility AUTH
LogLevel INFO
HostKey /etc/ssh/ssh_host_key
ServerKeyBits 1024
KeyRegenerationInterval 900
CheckMail no
UseLogin no
PrintMotd no
KeepAlive no
PermitRootLogin no
IgnoreRhosts yes
RhostsAuthentication no
RhostsRSAAuthentication no
RSAAuthentication yes
PasswordAuthentication yes
PermitEmptyPasswords no
StrictModes yes
UseLogin no
LoginGraceTime 180
```

2.8. **Backups**

The web server although important is not considered to be critical. But regardless, it is imperative we perform nightly backups to ensure that in the event of a compromise or failure, the server can easily restored.
This sever will be used as a repository for documents - it needs be backed up nightly.

For the web server environment, the following schedule will be followed:

Daily	-	differential
Weekly	-	full
Monthly	-	full

The daily tapes will go offsite every day with a copy remaining on site. The weekly tapes will go offsite and remain off site for a duration of two months. At the end of those two months the older of the weekly tapes will come back and go into the scratch pool. The monthly tapes will remain offsite for the duration of six months. At the end of the six month period, the oldest of the monthly tapes will go back into the scratch pool.

All backups will be performed via a backup server running Tivoli Storage Manager (TSM). A client running on sysweb will talk to the TSM server based on its backup schedule.
The client installation for sysweb follows:

Client Installation

Unix Client

The following packages represent the TSM client for Unix. To add simply use the following command:

Pkgadd –d . *package_name*

- TIVguid.pkg
- TIVsmCapi.pkg
- TIVsmCba.pkg

Next, modify the following files as follows:

- Dsm.opt – make the following changes for DSM.opt

```
************************************************************************
* IBM Tivoli Storage Manager                                           *
*                                                                      *
* Sample Client User Options file for UNIX (dsm.opt.smp)               *
************************************************************************

*  This file contains an option you can use to specify the TSM
*  server to contact if more than one is defined in your client
*  system options file (dsm.sys).  Copy dsm.opt.smp to dsm.opt.
```

```
*  If you enter a server name for the option below, remove the
*  leading asterisk (*).

************************************************************************
**** This is the server defined in DMS.SYS ****
SERVERNAME TSM
**** DOMAIN refers to mount points to backup ****
DOMAIN  "/"
DOMAIN "/usr"
DOMAIN "/var"
DOMAIN "/opt"
```

- Dsm.sys – make the following changes for DSM.sys

```
************************************************************************
* IBM Tivoli Storage Manager                                  *
*                                                             *
* Sample Client System Options file for UNIX (dsm.sys.smp)    *
************************************************************************

*  This file contains the minimum options required to get started
*  using TSM.  Copy dsm.sys.smp to dsm.sys.  In the dsm.sys file,
*  enter the appropriate values for each option listed below and
*  remove the leading asterisk (*) for each one.

*  If your client node communicates with multiple TSM servers, be
*  sure to add a stanza, beginning with the SERVERNAME option, for
*  each additional server.

************************************************************************
SERVERNAME TSM
**** These are directories within mount points****
VIRTUALMOUNTPOINT /test
VIRTUALMOUNTPOINT /files
  COMMmethod                TCPip
  TCPPort                   1500
  TCPServeraddress          10.100.10.80
  PASSWORDACCESS            GENERATE
  schedlogname /var/tsm/dsmsched.log
  errorlogname /var/tsm/dsmerror.log
  schedlogret  7
  errorlogret  7
INCLEXCL /var/tsm/inclexcl.txt
  txnb       25600
  tcpw       32
  tcpnodelay   yes
```

DSM.OPT and DSM.SYS can both be modified using vi .

3. On-going Maintenance and Backups

At this point, our system should be pretty tight. All bases have been covered to effectively lock down all possible scenarios that could be used by an attacker. But as I mentioned in **Section 1.3** ***Risk Analysis***, under *The Complacent Administrator*, if the newly hardened server is not kept up-to-date, it will eventually become vulnerable again. I'd like to compare a new car to a hardened server. You might be asking yourself, "What's a new car have to do with a hardened server anyways? Well, let's think about it. Lets say you purchase some brand new hot wheels (and I don't mean the ones you buy at Toys-r-us) and you take it everywhere with you. The first year you put 30,000 miles on it. The second year you put another 30k, and third year 40k. But at the end of the third year, your car starts having some major problems. You sit back and start to think about all the times you changed the oil, sparkplugs, etc…. But you realize this wasn't on your list of exciting things to do. In much the same way, administrators shun from the idea of on-going maintenance because it's not that exciting or they've become too complacent. There should be a policy in place detailing backups and on-going maintenance for servers.

3.1. Patch Management

Patch management is critical to a server's health. Patches are written by software developers because, either someone using their product came across a bug, or they in their research uncovered bugs or holes in their systems.
Although patches are critical, you should always have a demo system to download the patches to. The system would have an installation of the OS and any third party software that are used on the production server. This system should be the first one that patches are applied to. If the OS and third party software continue to function without any problems, then at that point the patches should be applied to the servers.

For our patch management, there will be no automatic download and application of patches to any server. A server in our demo environment has been setup to mirror the production web server. Whenever new patches come out, they will be downloaded to the demo environment and applied. Depending on the outcome, the patches will or will not be applied.
Any issues experienced with the Sun recommended patches will be looked into and rectified. Then and only then will the patches be applied.

3.2. Fix-Modes

Whenever new applications are installed or patches applied , settings that were changed by fix-modes get reversed. It is important to always run fix-modes after the application of any patches and/or installation of new packages. See section 2.7.1

3.3. Vulnerability Testing

As with fix-modes above, whenever new applications are installed and/or patches applied, there are always changes that occur to the server. When this happens there has to be a method of testing the server to determine if any holes or bugs have come up. Vulnerability testing provides a picture of the server pointing out any weaknesses, or potential vulnerabilities. This function that should be performed periodically to ensure services have not been overlooked or applications installed with possible vulnerabilities.

Our vulnerability testing will performed with two applications:

- Nessus
- NMAP

3.3.1. Nessus

Nessus is a popular vulnerability assessment tool that is used to remotely audit systems to determine whether someone could break into it or misuse it in any way. Nessus is a client server environment which means that the server portion can be installed on one system and the client portion on administrators' workstations. This provides an administrator with the flexibility to setup the server, and give access to others running the client the ability to perform assessments. Nessus is open source and can be downloaded from the following site:

http://www.nessus.org/download.html

3.3.2. NMAP

Another popular assessment tool is called NMAP or Network Mapper. It is a program that was designed to quickly scan and explore local area networks, both large and small. NMAP is a popular tool because of its ability to stealthily scan systems for open ports and determine what operating system is on the other end.

NMAP will be used to scan the web server to get a picture of what may be open. It will provide additional information to ensure proper steps are being taken in the maintenance of the web server.

NMAP can be downloaded from the following site:

http://www.insecure.org/nmap/nmap_download.html

3.4. Backups

Fault tolerance is great, but sometimes there are forces beyond our control that make fault tolerance useless. These could be in the form of an attacker compromising a system or systems. It could be in the form a natural disaster, such as a hurricane, wiping out all systems. In these forms fault tolerance provides absolutely no help.

This is where backups come in to play. Without proper backups, anyone in one of the scenarios mentioned above would have to start from scratch. Backups in any environment are crucial and necessary. Part of the on-going process will be to, on a quarterly basis, restore sysweb off of tape. This practice will tell us two things: that the tapes and data being backed up are good, and that the full restore process is doable. See section 2.8 for more on backups.

4. Testing the Server

4.1. Vulnerability Testing

For our vulnerability testing, two very popular tools were used, Nessus and NMAP. Nessus is a freeware tool that utilizes NMAP along with number of signatures to perform an assessment of your systems. The pre-hardening report is found in Appendix B. The post hardening report can be found in Appendix C.
The reports for NMAP our also found in the same locations.

4.2. Telnet/rlogin/ftp Test

Table 10 - telnet

```
bash-2.05# telnet sysweb
Trying sysweb...
telnet: Unable to connect to remote host: Connection refused
bash-2.05#
```

Table 11 - rlogin

```
bash-2.05# rlogin sysweb
::ffff:sysweb: Connection refused
bash-2.05#
```

Table 12 - ftp

```
bash-2.05# ftp 172.17.111.99
ftp: connect: Connection refused
ftp>
```

4.3. SSH Test

Table 13 - ssh

```
bash-2.05# ssh sysweb
root@sysweb's password:
Permission denied, please try again.
root@sysweb's password:
Permission denied, please try again.
root@sysweb's password:
Unable to find an authentication method
```

4.4. auhtlog test

authlog test

Oct 4 22:15:36 rudy login: [ID 644210 auth.notice] ROOT LOGIN /dev/console

4.5. MOTD Test

```
#
# The system you are accessing is for authorized use only. Anyone using this
computer is subject to being monitoring. Any illegal activity generated as a
result of login into this # system will be provided to law enforcement in
response to criminal prosecution.
#
# All users login into this system consent to monitoring.

Sourcing //.profile-local.....

Display set to: SUNW-UNIX-AUTHTOK-DATA term: xterm
```

Appendix A

TCP Wrapper: Configuration files

hosts.allow configuration file
vi /etc/hosts.allow
#
Only allow access from the project VLANS. Explicit
deny policy in /etc/hosts.deny
#
The IP addresses allocated from the management network
/usr/local/bin/sshd: 10.200.10.20/255.255.255.0
/usr/local/bin/sshd: 10.200.10.30/255.255.255.0
/usr/local/bin/sshd: 10.200.10.40/255.255.255.0

hosts.deny configuration file
vi /etc/hosts.deny
#
Explicitly deny access from all stations except those
that match the allow rule in /etc/hosts.allow
#
ALL : ALL

Appendix B

Assessment Reports: Pre-Hardening Phase

Nessus

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 were alive and responding during test	1
Number of security holes found	7
Number of security warnings found	17

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

[return to top]

Analysis of Host 10.100.10.10		
Address of Host	**Port/Service**	**Issue regarding Port**
10.100.10.10	smtp (25/tcp)	Security hole found
10.100.10.10	telnet (23/tcp)	Security notes found
10.100.10.10	ftp (21/tcp)	Security notes found
10.100.10.10	chargen (19/tcp)	Security notes found
10.100.10.10	daytime (13/tcp)	Security notes found
10.100.10.10	discard (9/tcp)	Security warning(s) found
10.100.10.10	echo (7/tcp)	Security warning(s) found
10.100.10.10	time (37/tcp)	Security notes found
10.100.10.10	finger (79/tcp)	Security hole found
10.100.10.10	http (80/tcp)	Security warning(s) found
10.100.10.10	sunrpc (111/tcp)	Security notes found
10.100.10.10	shell (514/tcp)	Security warning(s) found
10.100.10.10	login (513/tcp)	Security warning(s) found
10.100.10.10	exec (512/tcp)	No Information
10.100.10.10	submission (587/tcp)	Security hole found
10.100.10.10	lockd (4045/tcp)	Security notes found
10.100.10.10	font-service (7100/tcp)	Security hole found
10.100.10.10	sometimes-rpc11 (32774/tcp)	Security notes found

10.100.10.10	sometimes-rpc9 (32773/tcp)	Security notes found
10.100.10.10	sometimes-rpc7 (32772/tcp)	Security notes found
10.100.10.10	sometimes-rpc5 (32771/tcp)	Security hole found
10.100.10.10	general/tcp	Security warning(s) found
10.100.10.10	sunrpc (111/udp)	Security notes found
10.100.10.10	lockd (4045/udp)	Security warning(s) found
10.100.10.10	sometimes-rpc8 (32772/udp)	Security hole found
10.100.10.10	sometimes-rpc10 (32773/udp)	Security hole found
10.100.10.10	sometimes-rpc12 (32774/udp)	Security warning(s) found
10.100.10.10	sometimes-rpc14 (32775/udp)	Security warning(s) found
10.100.10.10	sometimes-rpc16 (32776/udp)	Security warning(s) found
10.100.10.10	sometimes-rpc18 (32777/udp)	Security warning(s) found
10.100.10.10	sometimes-rpc20 (32778/udp)	Security warning(s) found
10.100.10.10	sometimes-rpc22 (32779/udp)	Security warning(s) found
10.100.10.10	general/icmp	Security warning(s) found
10.100.10.10	general/udp	Security notes found

Security Issues and Fixes: 10.100.10.10

Type	Port	Issue and Fix
Vulnerability	smtp (25/tcp)	The remote sendmail server, according to its version number, may be vulnerable to a remote buffer overflow allowing remote users to gain root privileges. Sendmail versions from 5.79 to 8.12.9 are vulnerable. Solution : Upgrade to Sendmail ver 8.12.10. See also : http://lists.netsys.com/pipermail/full-disclosure/2003-September/010287.html NOTE: manual patches do not change the version numbers. Vendors who have released patched versions of sendmail may still falsely show vulnerability. *** Nessus reports this vulnerability using only *** the banner of the remote SMTP server. Therefore, *** this might be a false positive. Risk factor : High CVE : CAN-2003-0681, CAN-2003-0694 BID : 8641 Other references : RHSA:RHSA-2003:283-01, SuSE:SUSE-SA:2003:040 Nessus ID : 11838
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 Nessus ID : 10249
Informational	smtp (25/tcp)	An SMTP server is running on this port Here is its banner : 220 rudy ESMTP Sendmail 8.12.9+Sun/8.12.9; Fri, 17 Sep 2004 15:24:50 -0400 (EDT) Nessus ID : 10330
Informational	smtp (25/tcp)	Remote SMTP server banner : 220 rudy ESMTP Sendmail 8.12.9+Sun/8.12.9; Fri, 17 Sep 2004 15:26:09 -0400 (EDT) This is probably: Sendmail version 8.12.9+Sun Nessus ID : 10263
Informational	smtp (25/tcp)	smtpscan was not able to reliably identify this server. It might be: Sendmail 8.11.6 (EXPN, VRFY) Sendmail 8.12.2 Sendmail 8.10.1 Sendmail 8.11.6p2/8.11.6 -36- Sendmail 8.11.6p2/8.11.6 -134- The fingerprint differs from these known signatures on 1 point(s) Nessus ID : 11421
Informational	telnet (23/tcp)	An unknown service is running on this port. It is usually reserved for Telnet Nessus ID : 10330
Informational	telnet (23/tcp)	Remote telnet banner : SunOS 5.9 Nessus ID : 10281
Informational	ftp (21/tcp)	An unknown service is running on this port. It is usually reserved for FTP Nessus ID : 10330
Informational	ftp (21/tcp)	Remote FTP server banner : 220 rudy FTP server ready. Nessus ID : 10092
Informational	ftp (21/tcp)	An unknown service runs on this port. It is sometimes opened by this/these Trojan horse(s): Back Construction Blade Runner Cattivik FTP Server

CC Invader
Dark FTP
Doly Trojan
Fore
FreddyK
Invisible FTP
Juggernaut 42
Larva
MotIv FTP
Net Administrator
Ramen
RTB 666
Senna Spy FTP server
The Flu
Traitor 21
WebEx
WinCrash

Unless you know for sure what is behind it, you'd better
check your system

*** Anyway, don't panic, Nessus only found an open port. It may
*** have been dynamically allocated to some service (RPC...)

Solution: if a trojan horse is running, run a good antivirus scanner
Risk factor : Low
Nessus ID : 11157

Informational	chargen (19/tcp)	An unknown service is running on this port. It is usually reserved for Chargen Nessus ID : 10330
Informational	daytime (13/tcp)	An unknown server is running on this port. If you know what it is, please send this banner to the Nessus team: 00: 46 72 69 20 53 65 70 20 31 37 20 31 35 3a 32 35 Fri Sep 17 15:25 10: 3a 30 32 20 32 30 30 34 0a 0d :02 2004.. Nessus ID : 11154
Warning	discard (9/tcp)	The remote host is running a 'discard' service. This service typically sets up a listening socket and will ignore all the data which it receives. This service is unused these days, so it is advised that you disable it. Solution : - Under Unix systems, comment out the 'discard' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the following registry key to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDiscard Then launch cmd.exe and type : net stop simptcp net start simptcp To restart the service. Risk factor : Low CVE : CAN-1999-0636 Nessus ID : 11367

Warning	echo (7/tcp)	The remote host is running the 'echo' service. This service echoes any data which is sent to it. This service is unused these days, so it is strongly advised that you disable it, as it may be used by attackers to set up denial of services attacks against this host. Solution : - Under Unix systems, comment out the 'echo' line in /etc/inetd.conf and restart the inetd process - Under Windows systems, set the following registry key to 0 : HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpEcho HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpEcho Then launch cmd.exe and type : net stop simptcp net start simptcp To restart the service. Risk factor : Low CVE : CVE-1999-0103, CAN-1999-0635 Nessus ID : 10061
Informational	time (37/tcp)	An unknown service is running on this port. It is usually reserved for Time Nessus ID : 10330
Vulnerability	finger (79/tcp)	The remote finger daemon seems to be a backdoor, as it seems to react to the request : cmd_rootsh@target If a root shell has been installed as /tmp/.sh, then this finger daemon is definitely a trojan, and this system has been compromised. Solution: audit the integrity of this system, since it seems to have been compromised. Risk factor : High CVE : CAN-1999-0660 Nessus ID : 10070
Warning	finger (79/tcp)	The 'finger' service provides useful information to attackers, since it allows them to gain usernames, check if a machine is being used, and so on... Here is the output we obtained for 'root' : Login Name TTY Idle When Where root Super-User console Fri 14:11 Solution : comment out the 'finger' line in /etc/inetd.conf Risk factor : Low CVE : CVE-1999-0612 Nessus ID : 10068
Informational	finger (79/tcp)	A finger server seems to be running on this port Nessus ID : 10330
Warning	http (80/tcp)	Your webserver supports the TRACE and/or TRACK methods. TRACE and TRACK

		are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials. Solution: Disable these methods. If you are using Apache, add the following lines for each virtual host in your configuration file : RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F] If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. If you are using Sun ONE Web Server releases 6.0 SP2 and later, add the following to the default object section in obj.conf: <Client method="TRACE"> AuthTrans fn="set-variable" remove-headers="transfer-encoding" set-headers="content-length: -1" error="501" </Client> If you are using Sun ONE Web Server releases 6.0 SP2 or below, compile the NSAPI plugin located at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603 See http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603 http://www.kb.cert.org/vuls/id/867593 Risk factor : Medium Nessus ID : 11213
Informational	sunrpc (111/tcp)	The RPC portmapper is running on this port. An attacker may use it to enumerate your list of RPC services. We recommend you filter traffic going to this port. Risk factor : Low CVE : CAN-1999-0632, CVE-1999-0189 BID : 205 Nessus ID : 10223
Informational	sunrpc (111/tcp)	RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port Nessus ID : 11111

Warning	shell (514/tcp)	The rsh service is running. This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the rsh client and the rsh server. This includes logins and passwords. You should disable this service and use ssh instead. Solution : Comment out the 'rsh' line in /etc/inetd.conf. Risk factor : Low CVE : CAN-1999-0651 Nessus ID : 10245
Warning	login (513/tcp)	The remote host is running the 'rlogin' service, a remote login daemon which allows people to log in this host and obtain an interactive shell. This service is dangerous in the sense thatit is not ciphered - that is, everyone can sniff the data that passes between the rlogin client and the rlogin server, which includes logins and passwords as well as the commands executed by the remote host. You should disable this service and use openssh instead (www.openssh.com) Solution : Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Risk factor : Low CVE : CAN-1999-0651 Nessus ID : 10205
Vulnerability	submission (587/tcp)	The remote sendmail server, according to its version number, may be vulnerable to a remote buffer overflow allowing remote users to gain root privileges. Sendmail versions from 5.79 to 8.12.9 are vulnerable. Solution : Upgrade to Sendmail ver 8.12.10. See also : http://lists.netsys.com/pipermail/full-disclosure/2003-September/010287.html NOTE: manual patches do not change the version numbers. Vendors who have released patched versions of sendmail may still falsely show vulnerability. *** Nessus reports this vulnerability using only *** the banner of the remote SMTP server. Therefore, *** this might be a false positive. Risk factor : High CVE : CAN-2003-0681, CAN-2003-0694 BID : 8641 Other references : RHSA:RHSA-2003:283-01, SuSE:SUSE-SA:2003:040 Nessus ID : 11838
Informational	submission (587/tcp)	An SMTP server is running on this port Here is its banner : 220 rudy ESMTP Sendmail 8.12.9+Sun/8.12.9; Fri, 17 Sep 2004 15:25:04 -0400 (EDT) Nessus ID : 10330
Informational	submission (587/tcp)	Remote SMTP server banner : 220 rudy ESMTP Sendmail 8.12.9+Sun/8.12.9; Fri, 17 Sep 2004 15:26:09 -0400 (EDT)

		This is probably: Sendmail version 8.12.9+Sun Nessus ID : 10263
Informational	submission (587/tcp)	smtpscan was not able to reliably identify this server. It might be: Sendmail 8.11.6 (EXPN, VRFY) Sendmail 8.12.2 Sendmail 8.10.1 Sendmail 8.11.6p2/8.11.6 -36- Sendmail 8.11.6p2/8.11.6 -134- The fingerprint differs from these known signatures on 1 point(s) Nessus ID : 11421
Informational	lockd (4045/tcp)	RPC program #100021 version 1 'nlockmgr' is running on this port RPC program #100021 version 2 'nlockmgr' is running on this port RPC program #100021 version 3 'nlockmgr' is running on this port RPC program #100021 version 4 'nlockmgr' is running on this port Nessus ID : 11111
Vulnerability	font-service (7100/tcp)	The remote X Font Service (xfs) might be vulnerable to a buffer overflow. An attacker may use this flaw to gain root on this host remotely. *** Note that Nessus did not actually check for the flaw *** as details about this vulnerability are still unknown Solution : See CERT Advisory CA-2002-34 Risk factor : High CVE : CAN-2002-1317 Nessus ID : 11188
Informational	sometimes-rpc11 (32774/tcp)	RPC program #100024 version 1 'status' is running on this port RPC program #100133 version 1 is running on this port Nessus ID : 11111
Informational	sometimes-rpc9 (32773/tcp)	RPC program #100002 version 2 'rusersd' (rusers) is running on this port RPC program #100002 version 3 'rusersd' (rusers) is running on this port Nessus ID : 11111
Informational	sometimes-rpc7 (32772/tcp)	RPC program #100221 version 1 is running on this port Nessus ID : 11111
Vulnerability	sometimes-rpc5 (32771/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, CVE-2001-0717, CVE-2002-0679 BID : 3382 Nessus ID : 10787
Informational	sometimes-rpc5 (32771/tcp)	RPC program #100083 version 1 is running on this port Nessus ID : 11111
Warning	general/tcp	The remote host does not discard TCP SYN packets which have the FIN flag set. Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules. See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html http://www.kb.cert.org/vuls/id/464113 Solution : Contact your vendor for a patch Risk factor : Medium BID : 7487 Nessus ID : 11618
Warning	general/tcp	The remote host accepts loose source routed IP packets. The feature was designed for testing purpose. An attacker may use it to circumvent poorly designed IP filtering and exploit another flaw. However, it is not dangerous by itself. Solution : drop source routed packets on this host or on other ingress routers or firewalls. Risk factor : Low Nessus ID : 11834
Informational	general/tcp	The remote host is running Sun Solaris 9 Nessus ID : 11936
Informational	sunrpc (111/udp)	RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port Nessus ID : 11111
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 BID : 1372 Nessus ID : 10220
Informational	lockd (4045/udp)	RPC program #100021 version 1 'nlockmgr' is running on this port RPC program #100021 version 2 'nlockmgr' is running on this port RPC program #100021 version 3 'nlockmgr' is running on this port RPC program #100021 version 4 'nlockmgr' is running on this port Nessus ID : 11111
Vulnerability	sometimes-rpc8 (32772/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 BID : 866, 8615 Nessus ID : 10229
Informational	sometimes-rpc8 (32772/udp)	RPC program #100232 version 10 'sadmind' is running on this port Nessus ID : 11111
Vulnerability	sometimes-rpc10 (32773/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 Solution : We suggest that you disable this service. Risk factor : High CVE : CVE-1999-0320, CVE-1999-0696, CVE-2002-0391 BID : 428, 5356 Nessus ID : 10213
Informational	sometimes-rpc10 (32773/udp)	RPC program #100068 version 2 is running on this port RPC program #100068 version 3 is running on this port RPC program #100068 version 4 is running on this port RPC program #100068 version 5 is running on this port Nessus ID : 11111
Warning	sometimes-rpc12 (32774/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 Nessus ID : 10226
Informational	sometimes-rpc12 (32774/udp)	RPC program #100011 version 1 'rquotad' (rquotaprog quota rquota) is running on this port Nessus ID : 11111
Warning	sometimes-rpc14 (32775/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 Letting this service run is not recommended. Risk factor : Low CVE : CAN-1999-0624 Nessus ID : 10227
Informational	sometimes-rpc14 (32775/udp)	RPC program #100001 version 2 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port RPC program #100001 version 3 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port RPC program #100001 version 4 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port Nessus ID : 11111

Warning	sometimes-rpc16 (32776/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 more. It usually not a good idea to leave this service open. Risk factor : Low CVE : CVE-1999-0626 Nessus ID : 10228
Informational	sometimes-rpc16 (32776/udp)	RPC program #100002 version 2 'rusersd' (rusers) is running on this port RPC program #100002 version 3 'rusersd' (rusers) is running on this port Nessus ID : 11111
Informational	sometimes-rpc16 (32776/udp)	Using rusers, we could determine that the following users are logged in : - root (console) Solution : disable this service. Risk factor : Low CVE : CVE-1999-0626 Nessus ID : 11058
Warning	sometimes-rpc18 (32777/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 : Disable this service. Risk factor : Medium CVE : CVE-1999-0181 Nessus ID : 10240
Informational	sometimes-rpc18 (32777/udp)	RPC program #100008 version 1 'walld' (rwall shutdown) is running on this port Nessus ID : 11111
Warning	sometimes-rpc20 (32778/udp)	The sprayd RPC service is running. You should disable this service, as it may be used to saturate your network. Furthermore, it might become a security threat in the future, if a RPC vulnerability is discovered. Risk factor : Low CVE : CAN-1999-0613 Nessus ID : 10234
Informational	sometimes-rpc20 (32778/udp)	RPC program #100012 version 1 'sprayd' (spray) is running on this port Nessus ID : 11111
Warning	sometimes-rpc22 (32779/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. Solution : We suggest that you disable this service. Risk factor : High

		CVE : CVE-1999-0018, CVE-1999-0019, CVE-1999-0493 BID : 127, 450 Nessus ID : 10235
Informational	sometimes-rpc22 (32779/udp)	RPC program #100024 version 1 'status' is running on this port RPC program #100133 version 1 is running on this port Nessus ID : 11111
Warning	general/icmp	The remote host answered to an ICMP_MASKREQ query and sent us its netmask (255.255.255.0). 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 Nessus ID : 10113
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 Nessus ID : 10114
Informational	general/udp	For your information, here is the traceroute to 10.100.10.10 : 172.17.111.61 10.100.10.10 Nessus ID : 10287

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

NMAP Pre-Hardening Phase

```
NMAP Report - Pre Hardening Phase

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
 Interesting ports on  (10.100.10.10):
(The 1581 ports scanned but not shown below are in state: closed)
Port       State       Service                 Owner
7/tcp      open        echo
9/tcp      open        discard
13/tcp     open        daytime
19/tcp     open        chargen
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
37/tcp     open        time
79/tcp     open        finger
80/tcp     open        http
111/tcp    open        sunrpc
512/tcp    open        exec
513/tcp    open        login
514/tcp    open        shell
587/tcp    open        submission
4045/tcp   open        lockd
7100/tcp   open        font-service
32771/tcp  open        sometimes-rpc5
32772/tcp  open        sometimes-rpc7
32773/tcp  open        sometimes-rpc9
32774/tcp  open        sometimes-rpc11
Remote operating system guess: Solaris 9 Beta through Release on SPARC
Uptime 1.713 days (since Thu Aug 1 15:47:07 2004)

Nmap run completed -- 1 IP address (1 host up) scanned in 54 seconds
```

Appendix C

Assessment Reports: Post-Hardening Phase

Nessus 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 were alive and responding during test	1
Number of security holes found	0
Number of security warnings found	3

Host List	
Host(s)	**Possible Issue**
172.17.111.99	Security warning(s) found

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
172.17.111.99	ssh (22/tcp)	Security notes found
172.17.111.99	time (37/tcp)	Security notes found
172.17.111.99	general/tcp	Security warning(s) found
172.17.111.99	general/icmp	Security warning(s) found
172.17.111.99	general/udp	Security notes found

Security Issues and Fixes: 172.17.111.99		
Type	**Port**	**Issue and Fix**
Informational	ssh (22/tcp)	An ssh server is running on this port Nessus ID : 10330
Informational	ssh (22/tcp)	Remote SSH version : SSH-2.0-Sun_SSH_1.0.1 Nessus ID : 10267
Informational	ssh (22/tcp)	The remote SSH daemon supports the following versions of the SSH protocol : . 1.99 . 2.0 Nessus ID : 10881

Informational	http (80/tcp)	A web server is running on this port Nessus ID : 10330
Warning	general/tcp	The remote host does not discard TCP SYN packets which have the FIN flag set. Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules. See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html http://www.kb.cert.org/vuls/id/464113 Solution : Contact your vendor for a patch Risk factor : Medium BID : 7487 Nessus ID : 11618
Warning	general/tcp	The remote host accepts loose source routed IP packets. The feature was designed for testing purpose. An attacker may use it to circumvent poorly designed IP filtering and exploit another flaw. However, it is not dangerous by itself. Solution : drop source routed packets on this host or on other ingress routers or firewalls. Risk factor : Low Nessus ID : 11834
Informational	general/tcp	Nessus was not able to reliably identify the remote operating system. It might be: Sun Solaris 9 The fingerprint differs from these known signatures on 1 points. If you know what operating system this host is running, please send this signature to os-signatures@nessus.org : :1:1:1:255:0:255:1:1:255:1:0:255:1:64:255:1:1:1:1:1:1:1:1:1:64:49232:NNTMNWNNS:0:1:1 Nessus ID : 11936
Warning	general/icmp	The remote host answered to an ICMP_MASKREQ query and sent us its netmask (255.255.255.0). 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 Nessus ID : 10113
Informational	general/udp	For your information, here is the traceroute to 172.17.111.99 : 172.17.111.61 172.17.111.99 Nessus ID : 10287

NMAP Report

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
 Interesting ports on  (172.17.111.99):
(The 1599 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
80/tcp     open        http
Remote operating system guess: Solaris 9 Beta through Release on SPARC
Uptime 0.357 days (since Sun Oct  3 10:16:45 2004)

Nmap run completed -- 1 IP address (1 host up) scanned in 55 seconds
```

References

GIAC References

The Enemy Within, Lawrence Dubin, http://www.sans.org/rr/papers/51/530.pdf.

[G1] SANS Institute, GCUX Securing UNIX, Unix Practicum
Hal Pomeranz, Deer Run Associates

Internet References

[1] Sun Microsystems, www.sun.com

[2] Apache.org, www.apache.org

[3] Cisco Systems, Catalyst 3550 series
http://www.cisco.com/en/US/products/hw/switches/ps646/index.html

[4] SecurityPro News,
http://securitypronews.com/securitypronews-24-20030623EtterCapARPSpoofingandBeyond.html

[5] Sun Microsystems, http://www.sun.com/servers/

[6] University of California at Berkeley, Computer Science Division
http://www.cs.berkeley.edu/~nweaver/sapphire/

[7] OpenSSH, www.openssh.org

[8] OpenSSL, www.openssl.org

[9] Defcon, http://www.defcon.org/html/defcon-3.htm

[10] **Hardware Diagnostics for Sun™ Systems:** A Toolkit for System Administrators
http://sunsolve.sun.com/pub-cgi/show.pl?target=content/content9

[11] Lisa Bogar, SUID, SGID and fix-modes,
http://www.homepage.montana.edu/~unixuser/051602/SUID.html

[12] Nortel Networks, Solaris 8 and 9 Operating System
Hardening Guideline Document
http://www.nortelnetworks.com/solutions/securenet/collateral/solaris_hardening_guide_v1.pdf