



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

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

Sans Network Security 2000

---

# **GIAC SECURING UNIX PRACTICAL ASSIGNMENT**

---

November 22, 2000

Wolfgang Wamsler

<b>1</b>	<b>Introduction .....</b>	<b>1-3</b>
<b>2</b>	<b>Executive Summary .....</b>	<b>2-4</b>
2.1	Policies and Plans .....	2-4
2.2	Administrative Practices .....	2-4
2.3	Backup, Availability, Disaster Recovery .....	2-5
2.4	OS and Application -Software .....	2-5
2.5	System Configuration .....	2-6
2.6	Users, Groups and Login .....	2-6
2.7	Filesystem Integrity .....	2-6
2.8	Logging and Intrusion Detection .....	2-6
<b>3</b>	<b>Hardware .....</b>	<b>3-7</b>
<b>4</b>	<b>OS and Application -Software .....</b>	<b>4-8</b>
4.1	OS Version, Software Cluster .....	4-8
4.2	Optional System Software .....	4-8
4.3	Third Party Software .....	4-8
<b>5</b>	<b>Filesystem Integrity .....</b>	<b>5-9</b>
<b>6</b>	<b>System Configuration .....</b>	<b>6-10</b>
6.1	Processes - what is running? .....	6-10
6.1.1	<i>filtered output of the ps command</i> .....	6-10
6.1.2	<i>Processes and TCP/IP Ports</i> .....	6-11
6.2	Init-Scripts - why is it running? .....	6-12
6.3	Other Configuration Files .....	6-13
6.4	Networking Configuration .....	6-13
6.4.1	<i>Network interfaces</i> .....	6-13
6.4.2	<i>Name Resolution</i> .....	6-14
6.4.3	<i>Routing</i> .....	6-14
6.4.4	<i>Networking - finetuning</i> .....	6-14
<b>7</b>	<b>Users, Groups and Login .....</b>	<b>7-16</b>
7.1	Users .....	7-16
7.2	Groups .....	7-16
7.3	Login Access Restrictions .....	7-17
<b>8</b>	<b>Network: View from the outside .....</b>	<b>8-18</b>
8.1	nmap -scan of 222.222.222.10 .....	8-18
8.2	telnet connect to open ports on 222.222.222.10 .....	8-19
8.3	snmp query at 222.222.222.10 (Port 161) .....	8-21
8.4	nmap scan of address range 222.222.222.20 - .54.....	8-22
<b>9</b>	<b>Appendix, Security Tools .....</b>	<b>9-24</b>

# 1 Introduction

The owner of this host is a big internationally well-known company.

The host is a production system dedicated to web servers. At present there are 35 Netscape Enterprise HTTP-Servers and one streaming Audio-/Video-Server running on it. This is quite a bit of the company's Internet-presence.

The host is located at a big ISP's site for historical reasons. It was installed in May 1999, partly to replace an older system.

Names and other data revealing information about the company have been changed. This host will be called "se250" throughout this document.

## ***Subject of this report***

Security and availability at the system and network level

tools used: nmap  
SATAN  
lsof  
snmpwalk  
TIGER

## ***What the report is not about***

Although security and availability at the web application level is a very vital part in the overall picture, it's simply a too complex matter for this report. It should be investigated separately.

## 2 Executive Summary

### 2.1 Policies and Plans

No policies are in place for the company's hosts located at the ISP. This is a serious problem that does influence all aspects of availability and security. Many essential settings show strong signs of randomness.

Much time is wasted for debugging, searching for information, changing settings and getting simple things done. There are repeated discussions about why, what, how and by whom things have to be done. The employees work under constant pressure. This is not only frustrating for them, but can also have other serious side-effects.

Some important tasks are not done because they are forgotten or nobody feels responsible for it. As for se250, it is unlikely that the system and everything that runs on it can ever be completely recovered in case of a disaster.

#### **Create plans for all critical areas**

All plans should clearly define:

- The area of responsibility, a priority estimation
- The responsible team, a list of its members and how they can be contacted
- All related tasks that have to be done on a regular basis
- How monitoring is done and who is alerted in case of problems or disaster
- The tasks that have to be performed in case of problems or disaster, including who has to be notified
- Where required material and tools are stored

These plans must be handed out to all team members and updated when changes occur. They must also be accessible to other employees, for example on the company's Intranet.

### 2.2 Administrative Practices

se250 is in a special situation. For historical reasons it is located at a large ISP's site instead of the company's DMZ. It can only be accessed remotely over the Internet, what prevents the use of the standard administration and monitoring tools used by the "Internet Operators department". In fact that puts se250 into administrative no man's land.

#### **ISP support Level agreement**

Neither side was able to find a service contract, except for a very general agreement. It is not clear what services are being paid for. The ISP's support-services have virtually ceased to exist.

For more than two months the company has been trying to get a fresh install for another machine at the same location. No success so far. After a minor incident that happened at a Friday night, one host has been offline for 18 hours due to a network configuration mistake.

Here are some of the highlights: The terminal had been removed from the machine, there was no trained staff at the location. A technician called back after six hours. Six more hours later the technician had bought an adapter to attach a terminal. He tried to set the network default route for two hours, but was not successful. Then he was pissed off and went shopping, leaving the host offline.

Administrative tasks are performed on demand by two different departments. At least 10 persons have the root password. There are tendencies of rivalry between the departments, cooperation is sometimes a problem.

- create a policy for administration and monitoring of all hosts at the ISP's location.

## **2.3 Backup, Availability, Disaster Recovery**

se250 is not clustered. When it's off, it's off. Given the role of se250 in contrast to its administrative and security state state, the ability to quickly recover the system is the single most important security issue.

There seems to be no written backup policy or disaster recovery plan. No tape drive is attached. In the past, backups have been made by ufsdump remotely. It is unknown what has been backed up and at what intervals backups were made. It is unknown where the backups are stored and how many copies exist. Integrity of backups has never been tested through restoration attempts. At present there are no signs that backups are made at all.

### ***Immediate action required!***

- contact the ISP immediately to make sure that backups are made, get hold of copies of some backups and try to restore them on a different host
- create a backup schedule and a disaster recovery plan
- create a document that points out the importance of the backups, as well as the (legal) consequences of not doing backups or not having them accessible
- hand the documents to the ISP's responsible person, let him/her sign it and keep at least one copy

An incident has just occurred with a development server in the company's DMZ. Although the hard disks were mirrored (with the same software), it has had an unrecoverable file system error, and no functioning backups were available.

## **2.4 OS and Application-Software**

The amount of software on se250 is a security threat to the server. The more software, the more potential exploits. Nevertheless, no recommendation can be made at this point. See chapter 4 for more.

## 2.5 System Configuration

Attempts have been made to reduce the number of running processes, but unneeded processes are still started from the init-scripts, probably because their use was not clear. rpc services have a history of authentication problems, snmp provides abundant system and network configuration details to anyone who asks for it.

### **Immediate action required!**

- Stop at least rpcbind and snmp services immediately
- Put the machine behind a firewall!

## 2.6 Users, Groups and Login

### **Immediate action required!**

More than half of all successful break -ins have to do with passwords. FTP and telnet send password in clear -text over the net, root's password has never been changed. FTP and telnet are enabled, root can log in by telnet from any location.

- change the root password, limit access to the root account
- modify /etc/default/login to allow root login only at the system console
- lock unused accounts

## 2.7 Filesystem Integrity

This host is not protected by a firewall. It is not very secure and has been on the Internet for quite a while. All filesystems are mounted read/write/setuid. It should be taken into account that there could be trojanized files on it. The Web server directories are a jungle, the permissions a security administrator's nightmare. Many developers from different companies have accounts on se250.

### **Immediate action required!**

- Do thorough filesystem checks, run tripwire on a regular basis

## 2.8 Logging and Intrusion Detection

Logging is almost as out -of-the-box, minor modifications. There is no remote loghost. Logs are hardly ever checked, network scans or break -in attempts go unnoticed.

### **Immediate action required!**

- Set up logging for ssh, ftp, telnet to separate logfiles.
- Use a logchecker program, define alarm events, consider attaching honeypots

### 3 Hardware

Manufacturer	Sun Microsystems
System Type	Ultra Enterprise 250
CPU	UltraSparc-II Processor, 300 MHz
RAM	1000 MB
Hard Disk Drives	5 x 9 GB intern, all of the same type 4 drives in use, 1 not in use (spare)
CD-ROM drives	1 internal
Tape drives	none
Framebuffer	none
Keyboard	none
Console device	Terminal
Network interfaces	1 Fast Ethernet 100 Mbit, up and running 1 Quad Fast Ethernet 100 Mbit, not configured

#### **Potential problems**

- Only one CPU. A runaway process could consume all CPU time, bringing the machine to a virtual halt. (this has already happened). Adding a second CPU would be a benefit to performance and availability
- All disks are attached to the same SCSI controller. The controller is a single point of failure and a potential performance bottleneck



## 4 OS and Application -Software

### 4.1 OS Version, Software Cluster

The Operating System was installed on May 14, 1999.

OS is Solaris 2.6, installed cluster is "all plus OEM" - everything off the CD. This is not a good idea for a machine in an untrusted environment - the more software, the more potential vulnerabilities!

145 patches have been applied. Last patch install date is January 20, 2000.

- install the latest recommended patch -cluster
- check for the latest security -related patches at Sunsolve
- remove all software related to printing

### 4.2 Optional System Software

Solstice DiskSuite is used for disk mirroring (Software RAID Level 0). Solstice DiskSuite needs to be patched to function properly.

```
> showrev -p
...
Patch: 104172-12 Obsoletes: Requires: Incompatibles: Packages: SUNWmd, SUNWmdg
Patch: 104172-14 Obsoletes: Requires: Incompatibles: Packages: SUNWmd, SUNWmdg
Patch: 104172-16 Obsoletes: Requires: Incompatibles: Packages: SUNWmd, SUNWmdg
```

- Three patches have already been installed. Check the latest reports at Sunsolve

### 4.3 Third Party Software

Third-party software is scattered under /opt, /u01/app and /usr/local.

```
bash
emacs
gcc 2.8.1
gzip
ldapsdk-3.0
mysql 2.0.11
several mysql-modules
Netscape Enterprise Server 3.5.1
perl
perl-addons
realserver basic
rsync
ssh 1.2.21
top
traceroute
wu-ftpd 2.4.2
```

I have doubts whether all of it is still (or has ever been) required. Much has been compiled locally, the origin of the source files is sometimes not known. Some of the sources were supplied by Web -developers from other companies.

- Remove gcc. Don't make it easy for an intruder (compiling a rootkit locally)
- consider updating sendmail, wu -ftpd and Netscape Enterprise Server

## 5 Filesystem Integrity

This host is not protected by a firewall. It is not especially secure and has been on the Internet for quite a while.

Filesystem	Mount options	Mount Date/Time	Mounted on
/dev/md/dsk/d1	read/write/setuid/largefiles	Wed Sep 20 00:17:11 2000	/
/dev/md/dsk/d4	read/write/setuid/largefiles	Wed Sep 20 00:17:11 2000	/usr
/proc	read/write/setuid	Wed Sep 20 00:17:11 2000	/proc
fd	read/write/setuid	Wed Sep 20 00:17:11 2000	/dev/fd
/dev/md/dsk/d3	read/write/setuid/largefiles	Wed Sep 20 00:17:11 2000	/var
/dev/md/dsk/d5	read/write/setuid/largefiles	Wed Sep 20 00:21:52 2000	/opt
/dev/md/dsk/d6	read/write/setuid/largefiles	Wed Sep 20 00:21:52 2000	/u01/app
swap	read/write	Wed Sep 20 00:21:52 2000	/tmp

All filesystems are mounted read/write/setuid. It should be taken into account that there could be trojanized files on it.

Parts of the filesystem, namely the Webserver directories, are a jungle, the permissions a security administrator's nightmare. Some CGI -scripts do not parse input, HTTP PUT is partly enabled and the servers are not chrooted. Developers from different companies do develop content updates on se250, automated data transfers come in every few minutes.

### ***Check filesystem integrity immediately!***

Some of the most common standard tools to perform integrity checks are the commands ls, find, ps, netstat, grep. We have to make sure that these commands are exactly the ones we want. This is also true for system daemons, login - and authentication-related commands and shared libraries.

Sun Microsystems has a database of MD5 -hashes of all Solaris files. With the md5 utility you can create hashes of the files you want to check and compare it to the results from Sun's database at <http://sunsolve.sun.com>. The md5 utility can be downloaded from <http://sunsolve.Sun.COM/md5/md5.tar.Z>.

- Create MD5 hashes of all system binaries and feed it into Sunsolve's integrity checker
- Look for SUID and SGID files and directories, especially SUID root!
- Look for unusual filenames like ' . . ', ' . . . '
- The /dev and /devices and webserver -directories are good places to hide trojans
- Look for unusual processes with ps and lsof
- Check all logfiles
- Move all user-homedirs out of /usr
- Install the latest Solaris patch cluster and security -related patches
- use fix-modes (with caution) to fix file and directory permissions
- change /etc/vfstab to mount /usr read -only
- install tripwire, create a tripwire database, store the twdb on a read-only device (CD-ROM) and run tripwire on a regular basis against the stored twdb

## 6 System Configuration

In this chapter we look at what processes are running, why they are running and how they are configured. The running configuration is largely made up by the init-scripts in rc?.d, but there are several other files that affect system and network behaviour.

### 6.1 Processes - what is running?

ps, netstat, rpcinfo and lsof are used to examine what processes are running and what services they do provide.

#### 6.1.1 filtered output of the ps command

```
> ps -eo args | fgrep -v https- | fgrep -v realserver7
COMMAND
sched
/etc/init -
pageout
fsflush
/usr/lib/saf/ttymon
/usr/sbin/rpcbind
/usr/lib/saf/sac -t 300
/usr/lib/power/powerd
/usr/sbin/keyserv
/usr/sbin/inetd -s
/usr/sbin/nscd
/opt/HOLAxntp/bin/xntpd -c /opt/HOLAxntp/etc/ntp.conf
/usr/sbin/vold
/usr/lib/utmpd
/opt/COMPANYssh/sbin/sshd
/usr/lib/dmi/dmispd
/usr/lib/saf/ttymon -g -h -p se250.this.company.ez console login: -T sun -d /
/usr/lib/snmp/snmpdx -y -c /etc/snmp/conf
mibiisa -p 32810
/usr/dt/bin/dtlogin -daemon
/opt/msql/bin/msql2d
rpc.metamhd
ksh
-ksh
rpc.metad
ps -eo args
/usr/lib/sendmail -bd -q15m
/opt/COMPANYssh/sbin/sshd
./ns-admin -d /opt/netscape/suitespot/admin-serv/config
ssh-agent
-ksh
/opt/msql/bin/msql2d
-bash
/usr/sbin/cron
/usr/lib/sendmail -bd -q15m
/usr/sbin/syslogd -n -z 17
/opt/COMPANYssh/sbin/sshd
```

- Too many daemons running
- Stop rpcbind, powerd, keyserv, vold, dmispd, mibiisa, snmpdx, rpc.metamhd, rpc.metad
- syslogd runs with really weird parameters! (-n -z 17)
- Solaris 2.6 has a ntp-package, why not use this one?
- sendmail should not run in daemon mode
- inetd should be started (in /etc/init.d/inetsvc) with -t to enable TCP-logging

## 6.1.2 Processes and TCP/IP Ports

Shows to what TCP/IP ports the processes bind to.  
Can be contacted from the (Inter-) net.

### *rpcinfo*

Shows running RPC-Services. Standard RPC auth is based only on UID, often UID 0.  
May allow unwanted remote "administration".

```
> rpcinfo -p
  program vers proto  port  service
  100000    4  tcp    111   rpcbind
  100000    3  tcp    111   rpcbind
  100000    2  tcp    111   rpcbind
  100000    4  udp    111   rpcbind
  100000    3  udp    111   rpcbind
  100000    2  udp    111   rpcbind
  100229    1  tcp   32771  metad
  100230    1  tcp   32772  metamhd
  300598    1  udp   32805
  300598    1  tcp   32773
  805306368 1  udp   32805
  805306368 1  tcp   32773
  100249    1  udp   32806
  100249    1  tcp   32775
```

- Disable rpcbind, metad and metamhd

### *netstat*

netstat can be used to see what ports are open and to which IP address a listening service is bound. The output is filtered, lines we do not need are omitted.

```
# netstat -af inet -P udp | fgrep -v '.ntp '
*.sunrpc      Idle
*.*           Unbound
*.32771       Idle
*.32805       Idle
*.177         Idle
*.161         Idle
*.32811       Idle
*.32812       Idle
*.32810       Idle
*.*           Unbound
*.9875        Idle
*.32817       Idle
*.6770        Idle
*.syslog      Idle
*.64285       Idle
*.64762       Idle
*.64288       Idle
*.*           Unbound

# netstat -af inet -P tcp | fgrep -v '.80 ' | fgrep LISTEN
*.sunrpc      *.*      0        0        0        0 LISTEN
*.ftp         *.*      0        0        0        0 LISTEN
*.telnet      *.*      0        0        0        0 LISTEN
*.32771       *.*      0        0        0        0 LISTEN
*.32772       *.*      0        0        0        0 LISTEN
*.32773       *.*      0        0        0        0 LISTEN
*.32774       *.*      0        0        0        0 LISTEN
video.company.ez.7070 *.*      0        0        0        0 LISTEN
video.company.ez.554  *.*      0        0        0        0 LISTEN
video.company.ez.8080 *.*      0        0        0        0 LISTEN
video.company.ez.4040 *.*      0        0        0        0 LISTEN
video.company.ez.5050 *.*      0        0        0        0 LISTEN
video.company.ez.7878 *.*      0        0        0        0 LISTEN
video.company.ez.9090 *.*      0        0        0        0 LISTEN
video.company.ez.3030 *.*      0        0        0        0 LISTEN
video.company.ez.7802 *.*      0        0        0        0 LISTEN
```

*.8081	* *	0	0	0	0 LISTEN
*.22	* *	0	0	0	0 LISTEN
www.company.ez.ftp	pC19F67B0.dip.dialin.net.37232	0	0	8855	0 LISTEN
se250.ftp	rsx9315.57491	0	0	8855	0 LISTEN
se250.ftp	rsx9315.52692	0	0	8855	0 LISTEN

## lsof

Can be used for the same tasks as netstat, but has many more powerful features.

# /usr/local/bin/lsof -i   grep 327						
rpcbind	249	root	5u	inet	0x6102fe50	0t0 UDP *:32771 (Idle)
inetd	276	root	6u	inet	0x6102f2d0	0t0 TCP *:32771 (LISTEN)
inetd	276	root	7u	inet	0x6102f150	0t0 TCP *:32772 (LISTEN)
dmispd	673	root	4u	inet	0x61c214f0	0t0 TCP *:32773 (LISTEN)
dtlogin	676	root	7u	inet	0x61c206f0	0t0 TCP *:32774 (LISTEN)
snmpXdmid	677	root	1u	inet	0x61c20b70	0t0 TCP *:32775 (LISTEN)
rpc.metam	17557	root	0u	inet	0x6102f150	0t0 TCP *:32772 (LISTEN)
rpc.metam	17557	root	1u	inet	0x6102f150	0t0 TCP *:32772 (LISTEN)
rpc.metam	17557	root	2u	inet	0x6102f150	0t0 TCP *:32772 (LISTEN)
rpc.metad	17558	root	0u	inet	0x6102f2d0	0t0 TCP *:32771 (LISTEN)
rpc.metad	17558	root	1u	inet	0x6102f2d0	0t0 TCP *:32771 (LISTEN)
rpc.metad	17558	root	2u	inet	0x6102f2d0	0t0 TCP *:32771 (LISTEN)
# /usr/local/bin/lsof -i   grep 328						
snmpdx	662	root	5u	inet	0x613c43e0	0t0 UDP *:32811 (Idle)
snmpdx	662	root	6u	inet	0x613c4ce0	0t0 UDP *:32812 (Idle)
dmispd	673	root	3u	inet	0x61c21870	0t0 UDP *:32805 (Idle)
snmpXdmid	677	root	0u	inet	0x61c210f0	0t0 UDP *:32806 (Idle)
snmpXdmid	677	root	6u	inet	0x61c21970	0t0 UDP *:32807 (Idle)
mibiisa	691	root	0u	inet	0x61c20c70	0t0 UDP *:32810 (Idle)
rmserver	751	root	11u	inet	0x61c21070	0t0 UDP *:32817 (Idle)
# /usr/local/bin/lsof -i   grep 6500						
snmpXdmid	677	root	7u	inet	0x613c4ee0	0t0 UDP *:6500 (Idle)
# /usr/local/bin/lsof -i   grep 6770						
rmserver	751	root	20u	inet	0x61fcebfb8	0t0 UDP *:6770 (Idle)
# /usr/local/bin/lsof -i   grep 9875						
rmserver	688	root	8u	inet	0x61c21270	0t0 UDP *:9875 (Idle)
...						
rmserver	751	root	8u	inet	0x61c21270	0t0 UDP *:9875 (Idle)

## 6.2 Init-Scripts - why is it running?

### /etc/rcS.d

K65pcmcia	S33keymap.sh	S41cachefs.root	S70buildmnttab.sh
README	S35SUNWmd.init	S50drvconfig	
S10initpcmcia	S35cacheos.sh	S60devlinks	
S30rootusr.sh	S40standardmounts.sh	S65pcmcia	

- Disable S10initpcmcia, S65pcmcia

### /etc/rc0.d

K00ANNOUNCE	K42audit	K55syslog	K69autofs	K73volmgt	K85rpc
K10dtlogin	K47asppp	K57sendmail	K69xntpd	K75nfs.client	
K20lp	K50utmpd	K66nfs.server	K70cron	K76nsd	

### /etc/rc1.d

K00ANNOUNCE	K42audit	K55syslog	K67rpc	K70cron	K85power
K10dtlogin	K47asppp	K57sendmail	K68autofs	K76nsd	S01MOUNTFSYS
K20lp	K50utmpd	K65nfs.server	K69xntpd	K80nfs.client	

## ***/etc/rc2.d***

-S21perf	K76snmpdx	S71sysid.sys	S80spc	S92volmgt
-S47asppp	K77dmi	S72autoinstall	S85power	93cacheos.finish
-S70uucp	README	S72inetsvc	S88sendmail	S95SUNWmd.sync
-S73nfs.client	S01MOUNTFSYS	S73cacheofs.daemon	S88utmpd	S98msqld
-S74autofs	S05RMTMPFILES	S74HOLAxntp	S89bdconfig	S99Netscape
-S74xntpd	S20syssetup	S74syslog	S91afbinit	S99audit
-S80lp	S30sysid.net	S75cron	S91agaconfig	S99dtlogin
K20spc	S69inet	S76nsd	S91leoconfig	S99ssh
K60nfs.server	S71rpc	S80PRESERVE	S92rtvc-config	S99video

- Disable S71rpc, S72autoinstall, S74HOLAxntp, S85power, S92volmgt, S99dtlogin
- Probably disable S71sysid.sys, S91afbinit, S91agaconfig, S91leoconfig, S92rtvc - config, S89bdconfig

## ***/etc/rc3.d***

README	S76snmpdx	S77dmi	_S15nfs.server	_S99percol
--------	-----------	--------	----------------	------------

- Disable everything

## **6.3 Other Configuration Files**

### ***Disable command execution from the stack***

Buffer overflows can insert malicious code into the stack and execute it. Add this line to /etc/system to disallow command execution from the stack.

set noexec_user_stack=1
-------------------------

### ***Files that are not used***

- Remove /etc/auto\_\*
- Remove /etc/dfs/dfstab
- Remove adm lp sys crontab files (sys crontab needed for accounting)

## **6.4 Networking Configuration**

### **6.4.1 Network interfaces**

lo0: flags=849<UP,LOOPBACK,RUNNING,MULTICAST> mtu 8232
inet 127.0.0.1 netmask ffffffff00
hme0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
inet 222.222.222.10 netmask ffffffff00 broadcast 222.222.222.255
hme0:20: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
inet 222.222.222.20 netmask ffffffff00 broadcast 222.222.222.255
...
hme0:54: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
inet 222.222.222.54 netmask ffffffff00 broadcast 222.222.222.255
qfe0: flags=842<BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 0.0.0.0 netmask 0

- Netmask is wrong - the host has the lower half of C -class subnet 222.222.222.0
- Multicasting is enabled. If not needed, disable it in /etc/init.d/inetsvc

- qfe0 not configured, why is it there?

## 6.4.2 Name Resolution

```
# cat /etc/resolv.conf
domain this.company.ez
domain company.ez
nameserver 111.1.1.1
nameserver 222.222.111.111

# grep hosts /etc/nsswitch.conf
hosts:      files dns
```

Looks good.

## 6.4.3 Routing

netstat can be used to show routing information. At the same time we get an unordered list of all configured network interfaces and the traffic that flows through.

```
> netstat -rn

Routing Table:
  Destination          Gateway            Flags    Ref    Use  Interface
-----
222.222.222.0         222.222.222.44    U        38    1680  hme0:44
222.222.222.0         222.222.222.38    U        38     1   hme0:38
222.222.222.0         222.222.222.31    U        38     1   hme0:31
222.222.222.0         222.222.222.30    U        38     1   hme0:30
222.222.222.0         222.222.222.29    U        38     0   hme0:29
222.222.222.0         222.222.222.28    U        38     1   hme0:28
222.222.222.0         222.222.222.27    U        38     0   hme0:27
...
222.222.222.0         222.222.222.51    U        38    1668  hme0:51
222.222.222.0         222.222.222.54    U        38     28   hme0:54
...
222.222.222.0         222.222.222.10    U        38     0   hme0
224.0.0.0             222.222.222.10    U        38     0   hme0
default               222.222.222.1     UG       0 1493604
127.0.0.1             127.0.0.1         UH       0 191240  lo0
```

- Odd: all the network traffic should pass through the physical networking device

## 6.4.4 Networking - finetuning

### TCP/IP kernel parameters

By adjusting these parameters the host is prevented from falling prey to or being used for networked Denial-of-Service and spoofing attacks.

```
result
nnd /dev/tcp tcp_conn_req_max_q0 1024
nnd /dev/ip ip_ignore_redirect 0
nnd /dev/ip ip_send_redirects 1
nnd /dev/ip ip_ire_flush_interval 1200000
nnd /dev/arp arp_cleanup_interval 300000
nnd /dev/ip ip_forward_src_routed 1
nnd /dev/ip ip_forward_directed_broadcasts 1
nnd /dev/ip ip_forwarding 0
nnd /dev/ip ip_strict_dst_multihoming 0
```

- Accepts and sends ICMP redirects
- arp-cache update interval should be shorter
- Forwards source routed packets

- Forwards directed broadcasts (can be used in smurf attacks)
- Can act as a router between local interfaces

The parameter's values can be changed on the commandline, but will jump back to their old values at the next reboot. Add this to the end of /etc/init.d/inetinit to make the new settings permanent:

```

nnd -set /dev/tcp tcp_conn_req_max_q0      1024
nnd -set /dev/ip  ip_ignore_redirect        1
nnd -set /dev/ip  ip_send_redirects         0
nnd -set /dev/ip  ip_ire_flush_interval     60000
nnd -set /dev/arp arp_cleanup_interval      60000
nnd -set /dev/ip  ip_forward_src_routed     0
nnd -set /dev/ip  ip_forward_directed_broadcasts 0
nnd -set /dev/ip  ip_forwarding             0
nnd -set /dev/ip  ip_strict_dst_multihoming 1

```

### ***TCP sequence numbering***

```

# cat /etc/default/inetinit
...
# TCP_STRONG_ISS sets the TCP initial sequence number generation parameters.
# Set TCP_STRONG_ISS to be:
#     0 = Old-fashioned sequential initial sequence number generation.
#     1 = Improved sequential generation, with random variance in increment.
#     2 = RFC 1948 sequence number generation, unique-per-connection-ID.
#
TCP_STRONG_ISS=1

```

- Set TCP initial sequence number generation to 2 to prevent session hijacking



# 7 Users, Groups and Login

## 7.1 Users

### */etc/passwd and /etc/shadow*

Contains ~ 80 accounts.

- Inconsistent passwd and shadow files due to manual edits
- Owners of many accounts unknown, many GECOS fields empty
- At least one account shared by users from different companies
- Unused accounts not locked or removed
- The complete set of default system accounts is there

### *root*

- Password has never been changed
- At least 10 persons have the root password

### *useradd default settings*

There are no site-specific defaults.

- No password expiration
- No locking of inactive accounts
- /etc/skel contains only out-of-the-box skeleton files

### *home directories*

- ssh-private keys found in several home directories
- Homedirs scattered over different partitions and directories, many in /usr/home

## 7.2 Groups

### */etc/group*

- Inconsistent due to manual edits
- group memberships look really wild

## 7.3 Login Access Restrictions

### **inetd**

- No tcp-wrapper installed, telnet login from any location allowed

### **wu-ftpd's /opt/wu-ftpd/etc/ftphosts**

- Allows login for ~50 users from hundreds of locations - this includes entire C-class subnets as well as domainnames

### **sshd**

```
# cat /opt/TCssh/etc/sshd_config
...
AllowHosts *.dialin.net *.wooden.ez *.ronf-ip.net *.wcom.net *.company.ez *.compuserve.com
*.compuserve.ez *.jomei.ez *.sowas.net 194.127.67.* 194.127.69.* proxy.company-dingi.ez
62.52.62.* 62.52.63.* 62.52.64.* 62.52.65.* 62.52.66.* 145.228.252.141 193.171.101.*
222.222.222.* 192.168.108.* 194.221.99.* 195.238.226.194 africa.gulu.net
...
```

- Wide open

### **root login restrictions in /etc/default/login**

```
# cat /etc/default/login
...
# If CONSOLE is set, root can only login on that device.
# Comment this line out to allow remote login by root.
#
# CONSOLE=/dev/console
...
```

- No restrictions, root can login over the net

### **root's ~/.ssh/authorized\_keys**

- root has a large ~/.ssh/authorized\_keys that's believed to originate from the ISP's tech staff

## 8 Network: View from the outside

Finally we try to find out what information a potential attacker could gain about this host. The tools used are the popular port-scanner nmap, a standard telnet -client and snmpwalk from the ucd -snmp toolbox.

### 8.1 nmap-scan of 222.222.222.10

A real attacker might probably start with a less intrusive scan. He might also send packets with spoofed source addresses to hide his real IP address in lots of "noise".

I did not need to take any precautions against this scan being logged. Therefore I did full connect scans, which saved me a lot of time compared with a more cautious approach.

#### TCP connect

21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
111/tcp	open	sunrpc
8081/tcp	open	unknown
32771/tcp	open	sometimes-rpc5
32772/tcp	open	sometimes-rpc7
32773/tcp	open	sometimes-rpc9
32774/tcp	open	sometimes-rpc11
32775/tcp	open	sometimes-rpc13

#### UDP connect

111/udp	open	sunrpc
123/udp	open	ntp
161/udp	open	snmp
177/udp	open	xdmcp
514/udp	open	syslog
6500/udp	open	unknown
6770/udp	open	unknown
9875/udp	open	unknown
32771/udp	open	sometimes-rpc6
32805/udp	open	unknown
32806/udp	open	unknown
32807/udp	open	unknown
32810/udp	open	unknown
32811/udp	open	unknown
32812/udp	open	unknown
32817/udp	open	unknown

#### RPC connect

21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
111/tcp	open	sunrpc (rpcbind V2-4)
8081/tcp	open	unknown
32771/tcp	open	sometimes-rpc5 (metad V1)
32772/tcp	open	sometimes-rpc7 (metamhd V1)
32773/tcp	open	sometimes-rpc9 (dmispd V1)
32774/tcp	open	sometimes-rpc11
32775/tcp	open	sometimes-rpc13 (snmpXdmid V1)

- Lots of open ports.

On a properly administered host, some of the open ports could be "honeypots" which are sometimes used as part of an intrusion detection system. There is no real service behind an open honeypot-port. Therefore, no legitimate user would try to connect to it. But a potential attacker, unaware of that fact, is invited to peek in and the source IP address will be logged.

### **Remote OS fingerprint**

Remote fingerprinting makes use of the fact that real-world implementations of the TCP/IP protocol suite do vary, depending on manufacturer, OS, and OS version. Differences are found in the reply behaviour to unexpected packets and in the header flag patterns of the returned packets.

```
Remote OS guesses: Solaris 2.6 - 2.7, Solaris 7
```

## **8.2 telnet connect to open ports on 222.222.222.10**

By telnetting to some of the discovered ports it is possible to find out what service is actually listening. At a properly administered site the obtained information could be forged to mislead an intruder, but this is rarely done.

### **Port 21**

```
$ telnet 222.222.222.10 21
...
(big banner showing the company's name)
220-
220 se250 FTP server (Version wu-2.4.2-academ (1) Mon Aug 29 11:17:10 PAC DST 1999) ready.
```

- Hostname is se250
- FTP-Server wu-ftpd 2.4.2. Old version, possibly vulnerable

### **Port 22**

```
$ telnet 222.222.222.10 22
...
SSH-1.5-1.2.21
```

- ssh 1.2.21. Old version, possibly vulnerable

### **Port 23**

```
$ telnet 222.222.222.10 23
...
SunOS 5.6
login:
```

- Telnet is enabled. OS is Sun OS 5.6/Solaris 2.6

### **Port 8081**

```
$ telnet 222.222.222.10 8081
...
HTTP/1.0 400 Bad Request
Server: Netscape-Administrator/3.5
```

- Netscape Administration Server 3.5. This is a browser -based administration tool, therefore it is likely that we find more Netsc ape server-software on this machine

### Port 25

```
$ telnet 222.222.222.10 25
...
220 se250.this.company.ez ESMTP Sendmail 8.8.8+Sun/8.8.8; Sat, 11 Nov 2000 00:41:32 +0100
(MET)
...
vrfy root
250 Super-User <root@se250.this.company.ez>
...
expn nobody
050 nobody... aliased to /dev/null
250 </dev/null@se250.this.company.ez>
...
```

- FQDN is se250.this.company.ez
- Sendmail Version 8.8.8+Sun
- VRFY and EXPN are enabled

### Port 25 (cont.)

```
root      Super-User
daemon
bin
sys
adm        Admin
lp         Line Printer Admin
smtp       Mail Daemon User
uucp       uucp Admin
nuucp      uucp Admin
listen     Network Admin
nobody
noaccess    No Access User
nobody4    SunOS 4.x Nobody
msql       DB User msql
oracle     pseudo user for Oracle
```

- The above accounts have been verified by guessing commonly used names.

### Port 25 (cont.)

```
nobody... aliased to /dev/null
</dev/null@se250.this.company.ez>

postmaster... aliased to root
Super-User <root@se250.this.company.ez>

MAILER-DAEMON... aliased to postmaster
postmaster... aliased to root
Super-User <root@se250.this.company.ez>
```

- The above aliases have been found by guessing commonly used names.

### Port 25 (cont.)

```
...
mail from: YAS@company.ez
250 YAS@company.ez... Sender ok
rcpt to: someone@company.ez
250 wwcom@company.ez... Recipient ok
data
354 Enter mail, end with "." on a line by itself
```

Subject: Urgent! Change your passwords

Due to a system failure we need to recover server data.  
In order to accomplish this, you need to set all your passwords to "restore".

THANK YOU FOR YOUR COOPERATION

Your Admin Staff

.  
250 OAA18914 Message accepted for delivery  
...

- Host can be used as a mail relay. It is possible to send mail with forged sender address.

### ***How this message was received***

Most mail-client software is by default set to show only a standard header.

Subject: Urgent! Change your passwords  
Date: Sat, 11 Nov 2000 14:27:07 +0100 (MET)  
From: YAS@company.ez

Due to a system failure we need to recover server data.  
In order to accomplish this, you need to set all your passwords to "restore".

THANK YOU FOR YOUR COOPERATION

Your Admin Staff

If a mailclient is set to show the full header, a user can see that there is something wrong with this mail. If he or she can figure out what it all means, of course ...

## **8.3 snmp query at 222.222.222.10 (Port 161)**

Port 161 is the standard port for the Simple Network Management Protocol. If we can guess the community names (default names are "public" and "private") it is possible to read and probably write/change snmp parameters.

The snmp queries were done with `snmpwalk` from the `ucd-snmp` toolkit. I refrained from trying to change parameters, since this is a production server. The snmp service seems to accept commands from any host.

```
system.sysDescr.0 = Sun SNMP Agent, Ultra-250
system.sysObjectID.0 = OID: enterprises.42.2.1.1
system.sysUpTime.0 = Timeticks: (466309781) 53 days, 23:18:17.81
system.sysContact.0 = System administrator
system.sysName.0 = se250.this.company.ez
system.sysLocation.0 = System administrators office
...
interfaces.ifTable.ifEntry.ifDescr.1 = lo0
interfaces.ifTable.ifEntry.ifDescr.2 = hme0
interfaces.ifTable.ifEntry.ifDescr.3 = hme0:20
...
interfaces.ifTable.ifEntry.ifDescr.37 = hme0:54
interfaces.ifTable.ifEntry.ifDescr.38 = qfe0
..
interfaces.ifTable.ifEntry.ifType.2 = ethernetCsmacd(6)
...
interfaces.ifTable.ifEntry.ifSpeed.2 = Gauge: 10000000
...
interfaces.ifTable.ifEntry.ifPhysAddress.2 = 8:0:20:a9:99:aa
...
interfaces.ifTable.ifEntry.ifPhysAddress.38 = 0:0:0:0:0:0
interfaces.ifTable.ifEntry.ifAdminStatus.1 = up(1)
...
interfaces.ifTable.ifEntry.ifAdminStatus.38 = down(2)
...
```

```

ip.ipDefaultTTL.0 = 255
...
ip.ipAddrTable.ipAddrEntry.ipAdEntAddr.127.0.0.1 = IPAddress: 127.0.0.1
ip.ipAddrTable.ipAddrEntry.ipAdEntAddr.222.222.222.10 = IPAddress: 222.222.222.10
ip.ipAddrTable.ipAddrEntry.ipAdEntAddr.222.222.222.20 = IPAddress: 222.222.222.20
...
ip.ipAddrTable.ipAddrEntry.ipAdEntNetMask.222.222.222.10 = IPAddress: 255.255.255.0
...
tcp.tcpConnTable.tcpConnEntry.tcpConnState.0.0.0.0.21.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.0.0.0.0.22.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.0.0.0.0.23.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.0.0.0.0.25.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.0.0.0.0.111.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.0.0.0.0.8081.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.0.0.0.0.32771.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.0.0.0.0.32772.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.0.0.0.0.32773.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.0.0.0.0.32774.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.0.0.0.0.32775.0.0.0.0.0 = listen(2)
...
tcp.tcpConnTable.tcpConnEntry.tcpConnState.222.222.222.23.80.0.0.0.0.0 = listen(2)
...
tcp.tcpConnTable.tcpConnEntry.tcpConnState.222.222.222.52.80.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.222.222.222.52.554.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.222.222.222.52.3030.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.222.222.222.52.4040.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.222.222.222.52.5050.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.222.222.222.52.7070.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.222.222.222.52.7802.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.222.222.222.52.7878.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.222.222.222.52.8080.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.222.222.222.52.9090.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.222.222.222.53.80.0.0.0.0.0 = listen(2)
tcp.tcpConnTable.tcpConnEntry.tcpConnState.222.222.222.54.80.0.0.0.0.0 = listen(2)
...

```

- Guessed default communities public and private
- Got the whole MIB-II tree (3958 lines)
- SNMP agent is Sun SNMP Agent, seems to run with default configuration
- Machine is a SUN ULTRA 250, has been up for 53 days
- FQDN is se250.this.company.ez, domain is Company.ez
- One 100 MBit Quad fast Ethernet interface, not configured
- One 100 Mbit fast Ethernet interface, configured, IP Address 222.222.222.10
- Netmask 255.255.255.0
- MAC address of hme0 is 8:0:20:a9:99:aa
- 35 logical interfaces; hme0:20 (222.222.222.20) to hme0:54 (222.222.222.54)
- There are services listening on port 80 of most logical interfaces
- The pattern of open ports on 222.222.222.52 looks like there could be a streaming Video/Audio Server

## 8.4 nmap scan of address range 222.222.222.20 – .54

The scan results of the address range from 222.222.222.20 to 222.222.222.54 matches the results of the snmp queries. Some ports on 222.222.222.10 (ftp, ssh, telnet, smtp, ...) are also available on other IP-Addresses. Most addresses have also port 80 open, which does not show up on the primary interface. 222.222.222.52 shows a different pattern.

## Port 80

```
$ telnet 222.222.222.23 80
...
get
HTTP/1.1 400 Bad Request
Server: Netscape-Enterprise/3.5.1I
```

- HTTP-Server, Netscape Enterprise 3.5.1I, old version, possibly vulnerable

## RPC-Scan of 222.222.222.52

Port	State	Service (RPC)
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
80/tcp	open	http
111/tcp	open	sunrpc (rpcbind V2-4)
554/tcp	open	rtsp
3030/tcp	open	unknown
4040/tcp	open	unknown
5050/tcp	open	mmcc
7070/tcp	open	unknown
7802/tcp	open	unknown
7878/tcp	open	unknown
8080/tcp	open	http-proxy
8081/tcp	open	unknown
9090/tcp	open	zeus-admin
32771/tcp	open	sometimes-rpc5 (metad V1)
32772/tcp	open	sometimes-rpc7 (metamhd V1)
32773/tcp	open	sometimes-rpc9 (dmispd V1)
32774/tcp	open	sometimes-rpc11
32775/tcp	open	sometimes-rpc13 (snmpXdmid V1)

- There are extra ports on 222.222.222.52, could be a streaming audio/video server



## 9 Appendix, Security Tools

tripwire, file integrity checking

<ftp://ftp.cerias.purdue.edu/pub/tools/unix/ids/tripwire/>

fix-modes, adjusts file and directory permissions

<ftp://ftp.fwi.uva.nl/pub/solaris/fix-modes.tar.gz>

tiger, local Security checks

<ftp://net.tamu.edu/ftp/security/TAMU/tiger-2.2.4pl.tar.gz>

satan, port- & vulnerability scanner

<ftp://ftp.porcupine.org/pub/security/satan-1.1.1.tar.Z>

nessus, port- & vulnerability scanner

<http://www.nessus.org>

nmap, portscanner

<http://www.insecure.org/nmap/>

tcp\_wrappers, network access restriction and logging

[ftp://ftp.porcupine.org/pub/security/tcp\\_wrappers\\_7.6.tar.gz](ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.tar.gz)

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