# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

# GIAC Enterprises
# Solaris Corporate Information Database Server Security Evaluation

**Prepared by**

**Stephen T. Kelly**
**Security Consultant**
**20 November 2001**

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

# Executive Overview

We applaud the selection of the Sun Microsystems Ultra10 server as the hardware selection for your corporate "Fortune Database" server. We further find the selection of the Solaris 7 operating systems adequate and appropriate. The use of the Oracle Database for the Server is again a fine choice. Further, the use of Sun Microsystem's SKIP for site-to-site communication almost assures that the data you transmit remains proprietary.

Unfortunately, this fine selection of both hardware and software broke down in execution. The installation of the operating system was not done with security issues in mind. Corrections to the operating system to rectify these errors have not been made. Further, no apparent administrative, maintenance, or backup plan or policy has been developed. This leads to an even larger number of security risks.

The following paper outlines the major issues in more detail by section, but briefly they are as follows:

- Operating System Problems that must be corrected
- Operating System Configuration Vulnerabilities that must be corrected
- Oracle Server System/Configuration Vulnerabilities that must be corrected
- Administrative Practices that should be followed
- Patches that must be applied
- Storage of Sensitive Data
- Access Control configuration and policies
- Backup & Data Recovery policies and practices that must be implemented
- Auditing mechanisms that must be put in place
- Self Evaluation software that must be used

Detailed in conclusion of this report is a prioritized list of vulnerabilities that must be addressed as well as a prioritized list of recommended fixes.

Recommendations can be found for multiple solutions to the same problem. This follows the policy of a multi-layers approach to security.

Without a doubt, the system in its current state poses a security risk for both the data and the corporate network itself. It is strongly suggested that all the recommendation in this report be implemented immediately.



© SANS Institute 2000 - 2005 Author retains full rights.

# Table of Contents



© SANS Institute 2000 - 2005, Author retains full rights.



© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.



© SANS Institute 2000 - 2005 Author retains full rights.

# 2 Data Collection

The external analysis was performed without any access to the system under test to determine what exploits might be used to compromise the system.

It should be noted that these test were performed from a trusted host on the same subnet. Although this represents a considerable advantage in gaining access, it does not necessarily represent an unreasonable trusted host compromise used to leverage access into the COOKIE[1] platform.

The following were used to capture data about the COOKIE platform:

- Network Analysis Tools
  - nmap 2.53
  - snoop (on the local network)
- Host Based Analysis Tools
  - HATs (Host Analysis Tool; a proprietary tool developed to examine a file system)

## *2.1 Off-Host Network Data Collection*

### 2.1.1 Nmap

We ran a version of Nmap that we had downloaded previously. Initially it yielded the following results from another host.

```
$ ./nmap COOKIE

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0
Nmap run completed -- 1 IP address (0 hosts up) scanned in 60 seconds
$
```

This was from a randomly selected host on the network. It reran the test from another host with the "-P0" switches. It yielded the following:

```
$./nmap COOKIE -P0

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
All 1523 scanned ports on COOKIE (192.168.1.212) are: filtered
Nmap run completed -- 1 IP address (1 host up) scanned in 1727 seconds
$
```

[1] COOKIE is the actual hostname of the system.



© SANS Institute 2000 - 2005 Author retains full rights.

From this information the host appeared to be protected by some router or encryption. We would learn more snooping network traffic. One last step was to run nmap from the host COOKIE against itself. This yielded a very different picture:

```
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on COOKIE.giac-enterprises.com (192.168.1.212):
(The 1509 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
23/tcp     open        telnet
111/tcp    open        sunrpc
512/tcp    open        exec
513/tcp    open        login
514/tcp    open        shell
1521/tcp   open        ncube-lm
4045/tcp   open        lockd
6000/tcp   open        X11
7100/tcp   open        font-service
8080/tcp   open        http-proxy
32771/tcp  open        sometimes-rpc5

Nmap run completed -- 1 IP address (1 host up) scanned in 3 seconds
$
```

This is of some concern. Although there is some access control mechanism in place here, there are clearly also a number of active processes on this host that might be compromised. Actual examination of network traffic to the host would tell more.

### 2.1.2 Snoop

One method of collecting data about services running is to monitor connections on the target between the target and other machines. These active connections will give some perspective as to the possible services ports as well as the possible IPs to spoof to use for future compromise. It also gives some indication as to future trusted hosts to attack once the target is compromised.

Several tools are available to "sniff" traffic. In a Window environment we might have used Sniffer Pro but the environment here was primarily Unix. If the network is switched (it's hubbed) we might have used Ettercap(http://ettercap.sourceforge.net/). Another choice is Ethereal (http://www.ethereal.com). Tcpdump is also freely available for this platform (http://sunfreeware.sun.com/ ). In this case we elected to use the on-board utility "snoop".

#### 2.1.2.1 Encrypted Traffic

We observered that there is a great deal of IP 57 (we subsequently verified that this was SKIP) traffic between this host and other hosts (see section 2.7) and this data is encrypted and considered safe. For the purposes of brevity examples of that traffic are not shown here.



© SANS Institute 2000 - 2005 Author retains full rights.

```
# snoop nvtbox
Using device /dev/hme (promiscuous mode)
NVTBOX.giac-enterprises.com -> COOKIE IP D=192.168.1.212 S=192.168.1.197 LEN=172,ID=16151
COOKIE -> NVTBOX.giac-enterprises.com IP D=192.168.1.197 S=192.168.1.212 LEN=212,ID=2732
NVTBOX.giac-enterprises.com -> COOKIE IP D=192.168.1.212 S=192.168.1.197 LEN=172,ID=16152
COOKIE -> NVTBOX.giac-enterprises.com IP D=192.168.1.197 S=192.168.1.212 LEN=260,ID=2733
NVTBOX.giac-enterprises.com -> COOKIE IP D=192.168.1.212 S=192.168.1.197 LEN=172,ID=16153
COOKIE -> NVTBOX.giac-enterprises.com IP D=192.168.1.197 S=192.168.1.212 LEN=356,ID=2734
NVTBOX.giac-enterprises.com -> COOKIE IP D=192.168.1.212 S=192.168.1.197 LEN=172,ID=16154
COOKIE -> NVTBOX.giac-enterprises.com IP D=192.168.1.197 S=192.168.1.212 LEN=260,ID=2735
NVTBOX.giac-enterprises.com -> COOKIE IP D=192.168.1.212 S=192.168.1.197 LEN=172,ID=16155
^C#
```

There are however, several systems that are allowed to connect in cleartext to the system (COOKIE).

#### 2.1.2.2 DNS Traffic – NSX.adm.giac-enterprises.com

The host appears to use NSX.adm.giac-enterprises.com as a source for DNS information.

```
COOKIE -> FORTUNE.giac-enterprises.com ICMP Echo reply (ID: 256 Sequence number: 17016)
COOKIE -> NSX.adm.giac-enterprises.com DNS C 34.1.168.192.in-addr.arpa. Internet PTR ?
NSX.adm.giac-enterprises.com -> COOKIE        DNS R 34.1.168.192.in-addr.arpa. Internet PTR FORTUNE.unity.giac-
enterprises.com.
COOKIE -> NSX.adm.giac-enterprises.com DNS C FORTUNE.giac-enterprises.com. Internet Addr ?
NSX.adm.giac-enterprises.com -> COOKIE        DNS R FORTUNE.giac-enterprises.com. Internet Addr 192.168.1.34
```

#### 2.1.2.3 Oracle Traffic - D34.west.giac-enterprises.com

This host appears to be using Oracle port 1521 for communication. It is likely some front-end application accessing the oracle database.

```
COOKIE -> D34.west.giac-enterprises.com TCP D=1177 S=1521 Ack=3680218628
 Seq=3890743602 Len=93 Win=24820
D2101RA046167.west.giac-enterprises.com -> COOKIE TCP D=1521 S=1177 Ack=3890743695
 Seq=3680218628 Len=160 Win=17097
      COOKIE -> D34.west.giac-enterprises.com TCP D=1177 S=1521 Ack=3680218788
 Seq=3890743695 Len=123 Win=24820
```

#### 2.1.2.4 Cleartext Traffic - TRITON.west.giac-enterprises.com

This host appears to be allowed at least telnet, HTTP, and FTP access as this was observed. The risk here is clear: these services could be attacked via this host or by spoofing the IP for this host. This will be elaborated in the following sections.

```
COOKIE -> TRITON.west.giac-enterprises.com TELNET R port=1161
TRITON.west.giac-enterprises.com -> COOKIE        TELNET C port=1161
TRITON.west.giac-enterprises.com -> COOKIE        TELNET C port=1161
COOKIE -> TRITON.west.giac-enterprises.com TELNET R port=1161
TRITON.west.giac-enterprises.com -> COOKIE        HTTP C port=1189
TRITON.west.giac-enterprises.com -> COOKIE        HTTP C port=1188
TRITON.west.giac-enterprises.com -> COOKIE        HTTP GET /WebGUI/prioritree.cfm HTTP/1.1
COOKIE -> TRITON.west.giac-enterprises.com HTTP R port=1188
COOKIE -> TRITON.west.giac-enterprises.com HTTP HTTP/1.1 200 OK
```



© SANS Institute 2000 - 2005 Author retains full rights.

```
TRITON.west.giac-enterprises.com -> COOKIE        FTP C port=1037
TRITON.west.giac-enterprises.com -> COOKIE        FTP C port=1037 QUIT\r\n
      COOKIE -> TRITON.west.giac-enterprises.com FTP R port=1037 221 Goodbye.\r\n
      COOKIE -> TRITON.west.giac-enterprises.com FTP R port=1037
TRITON.west.giac-enterprises.com -> COOKIE        FTP C port=1037
TRITON.west.giac-enterprises.com -> COOKIE        FTP C port=1037
```

Interestingly, we observed a password exchange for a user account (another problem here, poor password choice, which will be elaborated in the following sections) while watching…

```
TRITON.west.giac-enterprises.com -> COOKIE        TELNET C port=1182
TRITON.west.giac-enterprises.com -> COOKIE        TELNET C port=1182
      COOKIE -> TRITON.west.giac-enterprises.com TELNET R port=1182
TRITON.west.giac-enterprises.com -> COOKIE        TELNET C port=1182
      COOKIE -> TRITON.west.giac-enterprises.com TELNET R port=1182 Password:\0
TRITON.west.giac-enterprises.com -> COOKIE        TELNET C port=1182
TRITON.west.giac-enterprises.com -> COOKIE        TELNET C port=1182 s
      COOKIE -> TRITON.west.giac-enterprises.com TELNET R port=1182
TRITON.west.giac-enterprises.com -> COOKIE        TELNET C port=1182 t
      COOKIE -> TRITON.west.giac-enterprises.com TELNET R port=1182
TRITON.west.giac-enterprises.com -> COOKIE        TELNET C port=1182 u
      COOKIE -> TRITON.west.giac-enterprises.com TELNET R port=1182
TRITON.west.giac-enterprises.com -> COOKIE        TELNET C port=1182 d
      COOKIE -> TRITON.west.giac-enterprises.com TELNET R port=1182
TRITON.west.giac-enterprises.com -> COOKIE        TELNET C port=1182 p
      COOKIE -> TRITON.west.giac-enterprises.com TELNET R port=1182
TRITON.west.giac-enterprises.com -> COOKIE        TELNET C port=1182 i
      COOKIE -> TRITON.west.giac-enterprises.com TELNET R port=1182
TRITON.west.giac-enterprises.com -> COOKIE        TELNET C port=1182 d
      COOKIE -> TRITON.west.giac-enterprises.com TELNET R port=1182
TRITON.west.giac-enterprises.com -> COOKIE        TELNET C port=1182
```

## *2.2 On-Host Internal Analysis*

Although an external analysis is an interesting study, an internal analysis will yield a better measurement of security and therefore acceptability. Initially the system was examined to determine the running processes and the connections active. The following sections show some of this information as it is primary information that allows examination of specific areas identified in this data. These are basic system commands elaborated below.

### 2.2.1 ifconfig –a

One of the first things we did is examine the interface configuration with the "ifconfig –a" command. This shows the status of the network interfaces. It's going to yield additional information about connections to this host. The following output was gathered:

```
[COOKIE][Jul 16][4:30pm][~]>ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
      inet 127.0.0.1 netmask ff000000
hme0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
      inet 192.168.1.212 netmask ffffff00 broadcast 192.168.1.255
```



© SANS Institute 2000 - 2005 Author retains full rights.

```
hme1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
        inet 10.0.0.7 netmask ff000000 broadcast 10.255.255.255
lo0: flags=2000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1
        inet6 ::1/128
hme0: flags=2000841<UP,RUNNING,MULTICAST,IPv6> mtu 1500 index 2
        inet6 fe80::a00:20ff:feb4:f03a/10
```

This tells us several things:

1. An active interface is up on 192.168.1.212 for COOKIE.
2. It appears to be subnetted to a Class C subnet.
3. Both Ipv4 and Ipv6 are supported on the primary interface.
4. There is a second network interface in operation.

The most interesting thing here is the second network. It was later discovered that the second network is a "backdoor" administration and network security network. We should point out that dual-homed hosts are prized targets for hackers as they allow their investigation to be spread to additional networks. It should be also noted that the second network was attached to numerous machines on yet several other networks and that little monitoring or security was present on this network. Although this second network was not examined in detail we find it important to point out that this represents a high additional security risk to the system. *Should this network be compromised it could lead allow a person to compromise many additional hosts undetected.*

### 2.2.2 netstat –a

With direct access to the host, we can confirm the information from the nmap and determine if there are any additional services. We can also see active connections at the time and gain additional connection information. The following shows the output from the "netstat –na" command:

```
UDP
  Local Address        Remote Address    State
-------------------- -------------------- -------
      *.111                                Idle
      *.*                                  Unbound
      *.32771                              Idle
      *.32776                              Idle
      *.4045                               Idle
      *.514                                Idle
      *.123                                Idle
      *.32780                              Idle
      *.6549                               Idle
      *.177                                Idle
      *.32797                              Idle
      *.32798                              Idle
      *.47763                              Idle
      *.1640                               Idle
      *.37304                              Idle
      *.37305                              Idle
      *.38144                              Idle
      *.39423                              Idle
      *.*                                  Unbound

                                TCP
  Local Address        Remote Address    Swind Send-Q Rwind Recv-Q  State
```



© SANS Institute 2000 - 2005 Author retains full rights.

```
---------------------- ---------------------- ----- ------ ------ ------ --------
      *.*                    *.*                0      0      0      0 IDLE
      *.111                  *.*                0      0      0      0 LISTEN
      *.*                    *.*                0      0      0      0 IDLE
      *.32771                *.*                0      0      0      0 LISTEN
      *.21                   *.*                0      0      0      0 LISTEN
      *.23                   *.*                0      0      0      0 LISTEN
      *.514                  *.*                0      0      0      0 LISTEN
      *.513                  *.*                0      0      0      0 LISTEN
      *.512                  *.*                0      0      0      0 LISTEN
      *.7100                 *.*                0      0      0      0 LISTEN
192.168.1.212.32780  192.168.1.25.734     9282      0  9282      0 CLOSE_WAIT
192.168.1.212.16151        *.*                0      0      0      0 LISTEN
      *.*                    *.*                0      0      0      0 IDLE
      *.8080                 *.*                0      0      0      0 LISTEN
      *.1521                 *.*                0      0      0      0 LISTEN
      *.6000                 *.*                0      0      0      0 LISTEN
192.168.1.212.16152        *.*                0      0      0      0 LISTEN
192.168.1.212.32799  192.168.1.212.16151  32768      0 32768      0 ESTABLISHED
192.168.1.212.16151  192.168.1.212.32799  32768      0 32768      0 ESTABLISHED
192.168.1.212.16153        *.*                0      0      0      0 LISTEN
      *.*                    *.*                0      0      0      0 IDLE
127.0.0.1.32812      127.0.0.1.1521       32768      0 32768      0 ESTABLISHED
127.0.0.1.1521       127.0.0.1.32812      32768      0 32768      0 ESTABLISHED
      *.32817                *.*                0      0      0      0 LISTEN
192.168.1.212.16154        *.*                0      0      0      0 LISTEN
192.168.1.212.32888  192.168.1.212.16152  32768      0 32768      0 ESTABLISHED
192.168.1.212.32889  192.168.1.212.16153  32768      0 32768      0 ESTABLISHED
192.168.1.212.16153  192.168.1.212.32889  32768      0 32768      0 ESTABLISHED
192.168.1.212.16152  192.168.1.212.32888  32768      0 32768      0 ESTABLISHED
      *.32910                *.*                0      0      0      0 LISTEN      *.32817                *.*                0      0      0      0
LISTEN
192.168.1.212.16154        *.*                0      0      0      0 LISTEN
192.168.1.212.32888  192.168.1.212.16152  32768      0 32768      0 ESTABLISHED
192.168.1.212.32889  192.168.1.212.16153  32768      0 32768      0 ESTABLISHED
192.168.1.212.16153  192.168.1.212.32889  32768      0 32768      0 ESTABLISHED
192.168.1.212.16152  192.168.1.212.32888  32768      0 32768      0 ESTABLISHED
      *.32910                *.*                0      0      0      0 LISTEN
127.0.0.1.32912      127.0.0.1.32910      32768      0 32768      0 ESTABLISHED
127.0.0.1.32910      127.0.0.1.32912      32768      0 32768      0 ESTABLISHED
127.0.0.1.32915      127.0.0.1.32914      32768      0 32768      0 ESTABLISHED
127.0.0.1.32914      127.0.0.1.32915      32768      0 32768      0 ESTABLISHED
127.0.0.1.32918      127.0.0.1.32910      32768      0 32768      0 ESTABLISHED
127.0.0.1.32910      127.0.0.1.32918      32768      0 32768      0 ESTABLISHED
127.0.0.1.32921      127.0.0.1.32920      32768      0 32768      0 ESTABLISHED
127.0.0.1.32920      127.0.0.1.32921      32768      0 32768      0 ESTABLISHED
192.168.1.212.40262  192.168.1.212.6000   32768      0 32768      0 ESTABLISHED
192.168.1.212.6000   192.168.1.212.40262  32768      0 32768      0 ESTABLISHED
192.168.1.212.40263  192.168.1.212.16152  32768      0 32768      0 ESTABLISHED
192.168.1.212.40264  192.168.1.212.16153  32768      0 32768      0 ESTABLISHED
192.168.1.212.16152  192.168.1.212.40263  32768      0 32768      0 ESTABLISHED
192.168.1.212.16153  192.168.1.212.40264  32768      0 32768      0 ESTABLISHED
192.168.1.212.16158        *.*                0      0      0      0 LISTEN
192.168.1.212.40267  192.168.1.212.16158  32768      0 32768      0 ESTABLISHED
192.168.1.212.16158  192.168.1.212.40267  32768      0 32768      0 ESTABLISHED
192.168.1.212.40268  192.168.1.212.6000   32768      0 32768      0 ESTABLISHED
192.168.1.212.6000   192.168.1.212.40268  32768      0 32768      0 ESTABLISHED
192.168.1.212.40269  192.168.1.212.16152  32768      0 32768      0 ESTABLISHED
192.168.1.212.16152  192.168.1.212.40269  32768      0 32768      0 ESTABLISHED
192.168.1.212.40270  192.168.1.212.16153  32768      0 32768      0 ESTABLISHED
192.168.1.212.16153  192.168.1.212.40270  32768      0 32768      0 ESTABLISHED
192.168.1.212.16356        *.*                0      0      0      0 LISTEN
192.168.1.212.40271  192.168.1.212.16356  32768      0 32768      0 ESTABLISHED
192.168.1.212.16356  192.168.1.212.40271  32768      0 32768      0 ESTABLISHED
192.168.1.212.40272  192.168.1.212.6000   32768      0 32768      0 ESTABLISHED
192.168.1.212.6000   192.168.1.212.40272  32768      0 32768      0 ESTABLISHED
192.168.1.212.40273  192.168.1.212.16152  32768      0 32768      0 ESTABLISHED
```



© SANS Institute 2000 - 2005 Author retains full rights.

```
192.168.1.212.16152  192.168.1.212.40273  32768      0 32768      0 ESTABLISHED
192.168.1.212.40274  192.168.1.212.16153  32768      0 32768      0 ESTABLISHED
192.168.1.212.16153  192.168.1.212.40274  32768      0 32768      0 ESTABLISHED
192.168.1.212.16556        *.*            0      0     0      0 LISTEN
192.168.1.212.40275  192.168.1.212.16556  32768      0 32768      0 ESTABLISHED
192.168.1.212.16556  192.168.1.212.40275  32768      0 32768      0 ESTABLISHED
127.0.0.1.39133      127.0.0.1.32910      32768      0 32768      0 ESTABLISHED
127.0.0.1.32910      127.0.0.1.39133      32768      0 32768      0 ESTABLISHED
127.0.0.1.39136      127.0.0.1.39135      32768      0 32768      0 ESTABLISHED
192.168.1.212.16357        *.*            0      0     0      0 LISTEN
192.168.1.212.36843  192.168.1.212.16357  32768      0 32768      0 ESTABLISHED
192.168.1.212.16357  192.168.1.212.36843  32768      0 32768      0 ESTABLISHED
     *.25                *.*             0      0     0      0 LISTEN
192.168.1.212.23     192.168.1.197.2350   9240       3  9282      0 ESTABLISHED
192.168.1.212.700    192.168.1.25.2049    9282       0  9282    116 ESTABLISHED
192.168.1.212.57248  192.168.1.25.111     9282       0  9282      0 TIME_WAIT
192.168.1.212.57247  192.168.1.25.735     9282       0  9282      0 TIME_WAIT
     *.*                 *.*             0      0     0      0 IDLE

TCP: IPv6
  Local Address                 Remote Address              Swind Send-Q Rwind Recv-Q   State      If
--------------------------------- --------------------------------- ----- ------ ----- ------ ----------- -----
     *.*                           *.*                        0      0 24576      0 IDLE
     *.111                          *.*                       0      0 24576      0 LISTEN
     *.*                           *.*                        0      0 24576      0 IDLE
     *.21                           *.*                       0      0 24576      0 LISTEN
     *.23                           *.*                       0      0 24576      0 LISTEN

Active UNIX domain sockets
Address  Type         Vnode     Conn  Local Addr      Remote Addr
30001625048 dgram      30001524080 00000000 /tmp/.skip.km.pipe
300016256c8 stream-ord 300001afce8 00000000 /tmp/.X11-unix/X0
30001625868 stream-ord 00000000 00000000
30001625a08 stream-ord 30001add590 00000000 /var/tmp/.oracle/sEXTPROC0

30001625ba8 stream-ord 300016a0110 00000000 /var/tmp/.oracle/s#485.1
```

From the above information we can verify the information gained from the nmap run. Shown in bold, it is clear that is a FTP on 21, a telnet on 23, sunrpc on 111, the exec, login and shell on 512, 513, and 514. These are basic services. There are some additional services such as font service on 7100, a HTTP daemon running on 8080 (not the default port 80), as well as an additional sunrpc on 32771. In should be noted that although misidentified, the 1521 Oracle service was found. Note an active local connection in bold italics.

Although much additional information is shown here including UDP services and the Ipv6 configuration; two additional points are worth noting. First, it is clear from the X service and the large number of local host connections that X-windows (of some version) is running on the server. This opens up possibilities of inappropriate X activity (such as users issuing an "xhost +" command vulnerable to session monitoring) but this is not typical of this server and was a byproduct of the active investigation. Secondly, a large number of connections are for Oracle and it is clear SKIP, X, and Oracle are running from the sockets information.

### 2.2.3 ps –ef

To further verify active servers as well as gain some additional insight into what is running



© SANS Institute 2000 - 2005 Author retains full rights.

on the host we examined the process status. The following is a cut and sorted "ps –ef" command (actually issued "ps -ef | cut -c1-21,47- | sort"):

```
   UID   PID  PPID  CMD

   cookie 16013 16010  -tcsh
   cookie 16031 16028  -tcsh
   cookie 16052 16049  -tcsh

   root     0     0  sched
   root     1     0  /etc/init -r
   root     2     0  pageout
   root     3     0 7 fsflush
   root    58     1  /usr/lib/devfsadm/devfseventd
   root    62     1  /usr/lib/devfsadm/devfsadmd
   root   125     1  /usr/lib/inet/in.ndpd
   root   136     1  /usr/sbin/rpcbind
   root   157     1  /usr/sbin/inetd -s
   root   166     1  /usr/sbin/syslogd
   root   168     1  /usr/sbin/cron
   root   185     1  /usr/sbin/vold
   root   187     1  /usr/lib/utmpd
   root   188     1  /usr/sbin/nscd
   root   251     1  /usr/java1.1/bin/sparc/native_threads/java -mx32m -Dadmin.server.properties=/et
   root   254     1  /usr/lib/saf/sac -t 300
   root   262   254  /usr/lib/saf/ttymon
   root 14500   393  xlock -mode blank
   root 16010   157  in.telnetd
   root 16028   157  in.telnetd
   root 16035 16031  sh
   root 16036 16035  csh
   root 16049   157  in.telnetd
   root 16075 16036  ps -ef
   root 16076 16036  cut -c1-21,47-
   root 16077 16036  sort
oracle8   355     1  -tcsh
oracle8   360   355  /bin/sh /usr/openwin/bin/openwin -nobanner
oracle8   364   360  /usr/openwin/bin/xinit -- /usr/openwin/bin/X :0 –nobanner -auth /cookie/oracle8/.
oracle8   365   364 0 /usr/openwin/bin/X :0 -nobanner -auth /cookie/oracle8/.xsun.COOKIE:0
oracle8   366   364  sh /usr/openwin/lib/Xinitrc
oracle8   371     1  fbconsole
oracle8   378     1  vkbd -nopopup
oracle8   381     1  ttsession -s
oracle8   383     1  /usr/openwin/bin/speckeysd
oracle8   386   366  /usr/local/bin/fvwm2
oracle8   387   366  dsdm
oracle8   389   386  /usr/local/libexec/fvwm/2.2.4/FvwmPager 7 4 .fvwm2rc 0 8 0 3
oracle8   393     1  /usr/local/bin/xautolock -time 10 -locker xlock -mode blank
oracle8   394   386  /usr/local/libexec/fvwm/2.2.4/FvwmAnimate 9 4 .fvwm2rc 0 8
oracle8  1789     1  / /oracle8/product/8.1.6/bin/tnslsnr LISTENER -inherit
oracle8 12549     1  /cookie/oracle8/product/8.1.7/Apache/Apache/bin/httpd -d /cookie/oracle8/product/8.
oracle8 12550 12549  /cookie/oracle8/product/8.1.7/Apache/Apache/bin/httpd -d /cookie/oracle8/product/8.
oracle8 12551 12549  /cookie/oracle8/product/8.1.7/Apache/Apache/bin/httpd -d /cookie/oracle8/product/8.
oracle8 12552 12549  /cookie/oracle8/product/8.1.7/Apache/Apache/bin/httpd -d /cookie/oracle8/product/8.
oracle8 12553 12549  /cookie/oracle8/product/8.1.7/Apache/Apache/bin/httpd -d /cookie/oracle8/product/8.
oracle8 12554 12549  /cookie/oracle8/product/8.1.7/Apache/Apache/bin/httpd -d /cookie/oracle8/product/8.
oracle8 12555 12549  /cookie/oracle8/product/8.1.7/Apache/Apache/bin/httpd -d /cookie/oracle8/product/8.
oracle8 12556 12550  /cookie/oracle8/product/8.1.7/Apache/jdk/bin/../bin/sparc/native_threads/java org
oracle8 12619     1  /usr/openwin/bin/xterm -sb -geometry 120x65 -e /usr/local/bin/tcsh
oracle8 12620 12619  /usr/local/bin/tcsh
oracle8 12647     1  ora_pmon_NAME
oracle8 12649     1  ora_dbw0_NAME
oracle8 12651     1  ora_lgwr_NAME
oracle8 12653     1  ora_ckpt_NAME
oracle8 12655     1  ora_smon_NAME
```



© SANS Institute 2000 - 2005 Author retains full rights.

```
oracle8 12657     1  ora_reco_NAME
oracle8 12659     1  ora_snp0_NAME
oracle8 12661     1  ora_snp1_NAME
oracle8 12663     1  ora_snp2_NAME
oracle8 12665     1  ora_snp3_NAME
oracle8 12667     1  ora_snp4_NAME
oracle8 12669     1  ora_snp5_NAME
oracle8 12671     1  ora_s000_NAME
oracle8 12673     1  ora_d000_NAME
oracle8 13565     1  /usr/openwin/bin/xterm -sb -geometry 120x65 -e /usr/local/bin/tcsh
oracle8 13566 13565  /usr/local/bin/tcsh
oracle8 13880 12620  sqlplus NAME_1/NAME12_1
oracle8 13881 13880  oracleNAME (DESCRIPTION=(LOCAL=YES)(ADDRESS=(PROTOCOL=beq)))
oracle8 13922 13566  sqlplus NAME_1/NAME12_1
oracle8 13923 13922  oracleNAME (DESCRIPTION=(LOCAL=YES)(ADDRESS=(PROTOCOL=beq)))
oracle8 13989     1  dbsnmp
oracle8 13990 13989  dbsnmp
oracle8 13997     1  oracleNAME (DESCRIPTION=(LOCAL=YES)(ADDRESS=(PROTOCOL=beq)))
oracle8 13998     1  oracleNAME (DESCRIPTION=(LOCAL=YES)(ADDRESS=(PROTOCOL=beq)))
oracle8 15323     1  oracleNAME (DESCRIPTION=(LOCAL=no)(ADDRESS=(PROTOCOL=BEQ)))
oracle8 15993     1  oracleNAME (DESCRIPTION=(LOCAL=no)(ADDRESS=(PROTOCOL=BEQ)))
```

This information confirms the Oracle processes (such as the listener) and indicates a full Oracle database server (including SQL support ). It should be noted the previously discovered HTTPd is apparently spawned by Oracle as shown in the bold above. The bold italics show some of the X processes. We can also see several shells and xterms as well as some of the basic SUN process (process Ids lower that 500 near the top). The first underlined line is the inet process that controls the many of the services (some of the active ones are also underlined). Since inet spawns many of the common services this will merit further investigation.

### 2.1.4 File system examination

Aside from previous examination of the active state of the machine, a complete examination or evaluation of the file system was accomplished. This included examination of a large number of files, their permissions, their presence or absence, and their contents. This was done with full permission and access to the system. The specific examinations conducted across the file system are too detailed to list in their entirety here. What is listed in the following sections are the steps used in the discovery of an actual problem with the system as identified by the use of an automated tool.

# 3 Evaluation

The following sections contain the test result from the physical examination, interviews, and testing conducted during the security evaluation. The results of this testing are documented as findings. A finding is a security activity or capability that is not in place and should be required. The findings will be separated into four (4) categories. These categories are:



© SANS Institute 2000 - 2005 Author retains full rights.

**Category I**: A significant security finding, which should be fixed before the system continues to operate.

**Category II**: A security relevant finding which should be fixed within a specified time period. However, the system may still be operated.

**Category III**: A minor security relevant recommendation for which implementation is an option.

**Category IV**: A non-security related recommendation for which implementation is an option.

Again, it should be noted that this examination was made with full access to the system under evaluation. Although the security issues identified in this way were not directly compromised, they represent known security issues that could be leveraged to compromise this system.

Also, it must be noted **the following subsections identify the discovered security issues on the system only**; not all possible security problems or all security issues evaluated. An automated set of scripts were used to check a large number of possible problems; where problems were identified we show the basic procedure the script used (usually in the form of a simple command line output) to identify the problem.

Finally, since so many of the issues uncovered relate to access and permissions of files, We'd like to comment on file system permissions. A number of references in the following sections identify "owner" or "group" and permissions as "0755" or similar notation. Briefly, very file on a Solaris OS has an owner. Typically this is who created the file but it may be assigned to any valid user listed in the password file. This user is assigned a User ID (or UID which is a number). For example the user root is typically UID 1, bin is 2, sys is 3, etc.. There may be files with UIDs not found in the /etc/passwd file. These will appear in the output of an "ls" command as the number and not the user name. Each file will also have a group assigned in a similar fashion from the /etc/group file. File permissions are assigned to each file with permission being given to read, write, and execute. These appear as "rwx" in the "ls" command. Permissions are further given based on owner, group, and other (anybody else) such that each one of these has some combination of read, write, and execute. These are annotated (in the order above for each file) as "rwxrwxrwx" (which would allow full read, write, and execute permission for owner, group and other. "rwxr-x---" would translate to read, write, and execute for the owner, read and execute for the group, and no permission for others. Order is important here. As a shorthand notation, these can be represented by the binary representation of a bit in each of the corresponding rwx positions with each "rwx" being one number. That is . "rwxr-x---" would translate to 7 (111 binary) for owner, 5 (101 binary) for group, and 0 (000 binary) for other or 750. Remember it is important to know the actual owner and group of the file to assess the full impact of a file's permissions. In this numeric



© SANS Institute 2000 - 2005 Author retains full rights.

representation you may also see a number preceding the 3 digit representation. This indicated a SET bit 4 for owner and 2 for group[2]. Additionally a 1 represents the "sticky bit". This provides a brief explanation of the file permission notation identified later in this report. For a more detailed explanation, it is suggested one references the manual pages for "ls" and "chmod" commands.

## *3.1 Operating System Vulnerabilities*

The default Solaris 7 operating system is a fairly secure operating system. It does however require some tuning and configuration.

It should be noted that some of the items reflected in this section could just have easily been listed under the following section. Often the subtleties in configuration vs. inherent vulnerability are very fine.

### 3.1.1 DNS

Finding # 2.1.1 (CAT I): The DNS executable was found to be subject to a commonly exploited buffer overflow.

**Discovery:** Some of the best sources of information are found on the WEB. In this case we examined the version information from the in.named binary. This was done by executing a "strings" command against the binary and "greping" for the string "BIND". This yielded:

```
$ strings /usr/sbin/in.named | grep BIND
;BIND LOG V8
;BIND DUMP V8
VERSION.BIND
BIND
@(#)in.named BIND 8.1.2 Tue Nov 10 18:16:24 PST 1998 Generic 107018-01-5.7-Septe
mber 1998
in.named BIND 8.1.2 Tue Nov 10 18:16:24 PST 1998
BIND 8.1.2
$
```

The system was then checked for patches (the list of appropriate patches was found at **http://sunsolve.sun.com/**) for the binary and none were found. Finally the, CERT was reviewed about BIND vulnerabilities (**http://www.cert.org/advisories/CA-2001-02.html**) and the unpatched version was found to be subject to an exploit.

**Risk:** The system should function so that each user has access to all of the information to which the user is entitled (by virtue of job duty, formal access approval), but to no more.

[2] Only in cases where the SUID/SGID is significant will the 4 number notation be used. The majority of the references will use the 3 number notation indicating a 0 up as the first digit.



© SANS Institute 2000 - 2005 Author retains full rights.

In the case of "need- to-know" for proprietary information, access must be essential for accomplishment of job function. The risk here is an exploit may utilize a known buffer overflow to interrupt proper DNS resolution. This combined with DNS poisoning (getting a DNS server to propagate improper information) can lead to users getting bad information or worse a system compromise.

**Recommendation:** Ensure the DNS service is updated to the latest version such as 9.1.3 (which can be downloaded from ftp://ftp.isc.org/isc/bind9/). Ensure that a process exists to ensure that security updates to applications or system components are identified, tested and applied in an efficient manner.

### 3.1.2 Root Home

Finding # 2.1.2 (CAT IV): The root account is the root directory (/).

**Discovery:** It is known that Solaris by default creates the root user's home at /. The /etc/password file contains as the 6th colon delimited field the home directory of the user account listed in the fist field. A simple examination of the /etc/password file (the command below "cats" the file and cuts the 1st and 6th colon delimited field out for examination) yields the following:

```
$ cat /etc/passwd | cut -f1,6 -d: | egrep :/$
root:/
daemon:/
sys:/
nobody:/
noaccess:/
nobody4:/
$
```

**Risk:** The root home being co-located with the operating system root can allow additional levels of system compromise. Having a home directory were the entire file system lies below the home directory can pose security risks as the entire file system is accessable. The ability to place files that root might execute is increased as / must have some accessability for the system to operate. Solaris by default locates the root account home at /. Although this is not a critical issue, it should be changed to minimize risk.

**Recommendation:** Create a separate home directory, such as "/root" owned by the root user, root group with 0700 permissions and set the root user home directory to that home directory. It is suggested that all the subordinate files have the "other" permission set to "0" (perhaps 0640 permissions).

### 3.1.3 Allowed shells

Finding # 2.1.3 (CAT II): Approved system shells were not listed in the /etc/shells file.



© SANS Institute 2000 - 2005 Author retains full rights.

**Discovery:** In this case simple examination yielded the fact that the file was not present on the system. For example:

```
$ ls –al /etc/shells
/etc/shells not found
$
```

**Risk:** The shells file contains a list of the shells on the system. Applications use this file to determine whether a shell is valid (see the manual pages for getusershell, manual section 3C). There should be in place an access control policy for the system. It should include features and/or procedures to enforce the access control policy of the information within the system. By restricting the shells that a user can run this further supports the other access control mechanisms. By having fully qualified path names to all shells, you can defend those shells you want users to run as well as stop a malicious user from placing his own malicious shell and running it.

**Recommendation:** All authorized shells should be listed in the /etc/shells file to ensure only users with approved shells are allowed to log into the system. The following is an example of an appropriate file:

```
$ cat /etc/shells
/bin/sh
/bin/csh

$
```

### 3.1.4 SetUID files

Finding # 2.1.4 (CAT II): An excessive number of files have the SUID and/or SGID bits set.

**Discovery:** During the system examination the following commands were run:

```
find / -local –type f –perm –4000 –exec ls –ld {} \;
find / -local –type f –perm –2000 –exec ls –ld {} \;
```

This disclosed an abnormally large number of files (a larger and different set than what was expected for a default Solaris 7 installation [as taken from the list of files in our tool]).

**Risk:** It is of particular concern when SUID or SGID files appear on a system. Although a standard installation of a system (as well as the installation of such software as Oracle) will have some SUID/SGID files, identification of this is critical. It should be noted that sizes were not evaluated nor MD5 checksums on the files identified. From this test we only know that the files are NOT part of a standard Operating system installation and should be reviewed.



© SANS Institute 2000 - 2005 Author retains full rights.

Examples of typical files are (these are part of the standard OS):

```
-rwsr-xr-x   1 root     sys        35916 Oct  6  1998 /usr/bin/at
-rwsr-xr-x   1 root     sys        13996 Oct  6  1998 /usr/bin/atq
-rwsr-xr-x   1 root     sys        12704 Oct  6  1998 /usr/bin/atrm
-r-sr-xr-x   1 root     bin        17044 Oct  6  1998 /usr/bin/crontab
-r-sr-xr-x   1 root     bin        14352 Oct  6  1998 /usr/bin/eject
-r-sr-xr-x   1 root     bin        28776 Oct  6  1998 /usr/bin/fdformat
-r-sr-xr-x   1 root     bin        29292 Oct  6  1998 /usr/bin/login
```

Examples of likely OK files are (these are not part of the OS but likely valid application files):

```
-rwsr-s--x   1 root     oinstall 1383248 Nov  3  1999
/oracle/product/server/8.1.5/bin/dbsnmp
-rwsr-s--x   1 oracle   oinstall  499684 Nov  3  1999
/oracle/product/server/8.1.5/bin/lsnrctl
-rwsr-s--x   1 oracle   oinstall  494068 Nov  3  1999
/oracle/product/server/8.1.5/bin/lsnrctl0
-rwsr-s--x   1 oracle   oinstall  457960 Nov  3  1999
/oracle/product/server/8.1.5/bin/oemevent
-rwsr-s--x   1 oracle   oinstall  562688 Nov  3  1999
/oracle/product/server/8.1.5/bin/onrsd
```

However this file found on the system merits a *much* closer examination (its' in a bad place [nothing like this should be in the /dev directory]; the directory is named supiciously; and it's a root owned SUID binary):

```
-rwsr-xr-x   1 root     actd       19920 May 15  1998 /dev/.hold/fping/fping
```

The primary risk here is that a malicious SUID or SGID can allow a user to run with altered permissions potentially allowing access not intended. It can further be used as a Trojan allowing a legitimate user to accidentally execute malicious code as that user.

**Recommendation:** Verify the need for SUID and/or SGID bit set on executables. If not necessary remove SUID and/or SGID capability from the permissions associated with those files. Unfortunately, the horse is out of the barn with this one- this is a task best done when the system is built before the system is put online when the utilities are installed from vendor supplied media and the validity of the SUID/SGID files can be better assessed.

The best solution for problems of this type is the utilization of Tripwire or some similar package which can identify changes in the files on the system.

### 3.1.5 SNMP Issues

Finding # 2.1.5.1 (CAT I): The SNMP community string was set to the default.

**Discovery:** The file /etc/snmp/conf/snmpd.conf was examined. The non-commented



© SANS Institute 2000 - 2005 Author retains full rights.

lines were as follows:

```
sysdescr        ALLDESC
syscontact      ALLCONT
sysLocation     ALLLOC
system-group-read-community     public
read-community  public
trap            localhost
trap-community  SNMP-trap
managers        localhost
```

These are all the default settings. Of particular concern is the read-community remaining public.

**Risk:** There should be in place an access control policy for the system. It should include features and/or procedures to enforce the access control policy of the information within the system. The identity of each user authorized access to the system shall be established positively before authorizing access. With the default string set any person knowing the default value might be able to compromise the SNMP daemon or at a minimum gain SNMP information about the system which can be used to further exploit the system.

**Recommendation:** Set the SNMP community strings to values that complies with the policy for construction of strong passwords.

Finding # 2.1.5.2 (CAT II): SNMP management information base (MIB) files were not properly protected.

**Discovery:** The snmpdx.mib and sun.mib files were found with 744 permissions:

```
# cd /var/snmp/mib
# ls -al
total 258
drwxrwxr-x   2 root     sys          512 Oct  5 18:37 .
drwxrwxr-x   3 root     sys          512 Jan  2  2001 ..
-rwxr--r--   1 root     sys        14346 Sep  1  1998 snmpdx.mib
-rwxr--r--   1 root     sys       100780 Oct  4 02:07 sun.mib
#
```

**Rationale:** With the setting on these files any person with sufficient file system permissions to access these files might be able to compromise the SNMP daemon or at a minimum gain SNMP information about the system.

**Recommendation:** Set all MIB file permissions to 700 or more restrictive.

### 3.1.6 Devices

Finding # 2.1.6 (CAT II): Device files are not properly protected.

**Discovery:** An audio device file was not owned by the root user and in the sys or bin groups. This was uncovered by examination of files in the /dev directory and looking at



© SANS Institute 2000 - 2005 Author retains full rights.

the ownership.

```
# ls -al /dev/audio
lrwxrwxrwx   1 root     root          12 Nov 12  1999 /dev/audio -> /dev/sound/0
# ls -al /dev/sound/0
lrwxrwxrwx   1 root     root          66 Nov 12  1999 /dev/sound/0 ->
../../devices/pci@1f,4000/ebus@1/SUNW,CS4231@14,200000:sound,audio
# ls -al ../../devices/pci@1f,4000/ebus@1/SUNW,CS4231@14,200000:sound,audio
crw-rw-rw-   1 root     other    108,  0 Nov 12  1999
../../devices/pci@1f,4000/ebus@1/SUNW,CS4231@14,200000:sound,audio
#
```

**Risk:** Although the device file noted may seem insignificant (there was no speaker or microphone attached to the system) in some cases it could be used to eavesdrop on the room where the system is located or even to prevent an audible warning from being heard. It should be noted this is the Solaris default and that the lack of group permissions would make this very difficult to leverage.

**Recommendation:** Ensure device files are appropriately owned, preferably by root with bin or sys group. Note that changes to device files must especially be tested prior to implementation and it is likely that more restrictive permissions (such as 0700) can be set.

## *3.2 Configuration Vulnerabilities*

Configuring Solaris involves altering settings and parameters on a variety of files. Many of these files are just different from the default configurations that are set when Solaris 7 is installed. By default there are services running, software installed, and access permissions that are not configured for optimal security

It should be noted that many of the access issues could be termed configuration issues also. The distinction between the two is minimal.

### 3.2.1 Rhosts

Finding # 2.2.1 (CAT II): <u>The RLOGIN service was running and .rhosts files were present.</u>

**Discovery:** The discovery of this problem resulted from the evaluation of the inetd.conf file (and confirmation of the running inetd process in the "ps" shown up front) as well as access testing. The following is a section of the /etc/inetd.conf showing the uncommented services. Although the majority of the services were commented out, the 5 uncommented lines were active services:

```
# Ftp and telnet are standard Internet services.
#
# BELOW MODIFIED FOR TCP WRAPPERS
ftp     stream  tcp     nowait  root    /usr/sbin/tcpd  in.ftpd
# BELOW MODIFIED FOR TCP WRAPPERS
```



© SANS Institute 2000 - 2005 Author retains full rights.

```
telnet  stream  tcp     nowait  root    /usr/sbin/tcpd  in.telnetd
#
# Tnamed serves the obsolete IEN-116 name server protocol.
#
# BELOW COMMENTED OUT
#name   dgram   udp     wait    root    /usr/sbin/in.tnamed     in.tnamed
#
# Shell, login, exec, comsat and talk are BSD protocols.
#
# BELOW MODIFIED FOR TCP WRAPPERS
shell   stream  tcp     nowait  root    /usr/sbin/tcpd  in.rshd
# BELOW MODIFIED FOR TCP WRAPPERS
login   stream  tcp     nowait  root    /usr/sbin/tcpd  in.rlogind
# BELOW MODIFIED FOR TCP WRAPPERS
exec    stream  tcp     nowait  root    /usr/sbin/tcpd  in.rexecd
# BELOW COMMENTED OUT
#comsat dgram   udp     wait    root    /usr/sbin/in.comsat     in.comsat
# BELOW COMMENTED OUT
#talk   dgram   udp     wait    root    /usr/sbin/in.talkd      in.talkd
#
# Must run as root (to read /etc/shadow); "-n" turns off logging in utmp/wtmp.
#
# BELOW COMMENTED OUT
#uucp   stream  tcp     nowait  root    /usr/sbin/in.uucpd      in.uucpd
#
```

**Risk:** The system should function so that each user has authenticated access to the information (normally by virtue of password, but in this case by file presence), but to no more. RLOGIN service does not appear necessary for the intended system use. A malicious user could use the capability (via .rhosts files) to run commands from a remote system or access the system. Any facility that grants authentication without a password should be reviewed.

**Recommendation:** Discontinue the use of the RLOGIN service [the other services will be addressed in section 2.7.1]. Unless this service is specifically required its use should be discontinued. Ensure all users are authenticated by the host.

**There is a general recommendation here:** Stop all unnecessary services. If started by initd.conf they can be commented out. If started in the /etc/rcX.d directories remove the startup scripts.

### 3.2.2 Password Configuration

Finding # 2.2.3.1 (CAT III): Users can change passwords more than once every 24 hours.

**Discovery:** Control over a users capability to alter the password within a minimum time period is controlled by the parameters in the /etc/default/password file. The file on the system (with no MINWEEKS value which allows unlimited changing) is shown:

```
# cat /etc/default/passwd
#ident  "@(#)passwd.dfl 1.3     92/07/14 SMI"
```



© SANS Institute 2000 - 2005 Author retains full rights.

```
MAXWEEKS=
MINWEEKS=
PASSLENGTH=6
#
```

In actuality these fields are added on user creation and can be forced into the /etc/shadow file. This file was also examined (note that the 4th, 5th ,6th ,7th, and 8th colon delimited fields representing min change days, max change days, warn days, inactive days, and expire date are empty indicating no limit):

```
root:6p3nrmcm49i2Q:11523::::::
daemon:*LK*:6445::::::
bin:*LK*:6445::::::
sys:*LK*:6445::::::
adm:*LK*:6445::::::
lp:*LK*:6445::::::
uucp:*LK*:6445::::::
nuucp:*LK*:6445::::::
listen:*LK*:::::::
nobody:*LK*:6445::::::
noaccess:*LK*:6445::::::
nobody4:*LK*:6445::::::
oracle:.BZa9dLnR4k/I:11477::::::
```

**Risk:** This may allow users to bypass security controls over the proper construction of passwords. Although this might seem as discouraging the principle of changing passwords, you need control over the change. One would not want users to immediately reset passwords to their old password after a change. As a minimum, passwords will be a minimum of six characters and changed at least every 180 days or more frequently as warranted. Passwords should be protected from disclosure and handled and marked as "PROPRIATARY".

**Recommendation:** Restrict the ability of users to change passwords by setting a limit of a minimum of 24 hours (/etc/default/passwd). It is further recommended that the PASSLENGTH be set to 8 and the MAXWEEKS be set to some number of weeks (13 is suggested) such that passwords expire. See the following finding.

Finding # 2.2.3.2 (CAT II): Password aging controls are not configured.

**Discovery:** As shown in the preceding finding, the MAXWEEKS variable is not configured nor are the /etc/shadow fields configured for users.

**Risk:** As a minimum, passwords should be a minimum of six characters and changed at least every 180 days or more frequently as warranted. The risk is that current technology allows a brute force attack to be executed in a reasonable amount of time given the encrypted password. This system uses a known algorithm. Should the /etc/shadow file (or some other source of encrypted passwords) be compromised the system is at risk. Passwords should be protected from disclosure and handled and marked as "COMPANY PRIVATE" or something similar.



© SANS Institute 2000 - 2005 Author retains full rights.

**Recommendation:** Enable password aging controls (see above and below) for all interactive users to ensure passwords are changed at a maximum of 180 days (/etc/default/passwd); 90 is recommended.

**There is a general recommendation here:** As part of this and the previous finding, it is suggested that for each user account on the system (replace <*User Name*> with the user account name), the following command be run:

passwd -f -n 7 -w 14 -x 91 <*User Name*>

The "-f" switch forces the password to be changed on next login. The "-n" and "-x" switches force immediately the MINWEEKS (days actually) and MAXWEEKS (days actually) values for the user. The "-w" provides the number of days when a user is warned of password expiration.

### 3.2.3 Startup Scripts

Finding # 2.2.3 (CAT II): System startup files were not properly protected. Files run by system startup scripts were found world writeable.

**Discovery:** In examination of the /etc/rc2.d and /etc/rc3.d directories several startup scripts were discovered with inappropriate permission settings. Most of these were user application startup scripts but several operating system scripts were also set to the inappropriate permissions (like having unnecessary group or world write). This is likely a misconfiguration issue. Although every script in /etc/rc2.d and /etc/rc3.d should be reviewed for permissions, one particular example is of great concern. Shown below is a common problem. A start script is linked to an installed directory however the permissions were assigned inappropriately:

```
# cd /etc/rc2.d
# ls -al ./S99hostcall
lrwxrwxrwx   1 root    other         21 Nov  9 22:04 ./S99hostcall ->
/usr/local/bin/S99hostcall
# ls -al /usr/local/bin/S99hostcall
-rwxrwxrwx   1 root   other         824 Nov 30  2000 /usr/local/bin/S99hostcall
#
```

**Risk:** A startup script was installed to /etc/rc2.d (apparently as root). This was then linked to a file in /usr/local/bin. For some reason the file has world write permission. The risk in the above example is that *any* user can modify this start script (which is run by root at startup) to accomplish any task *as root*!

**Recommendation:** Ensure all system startup files are assigned permissions no more permissive than 750. Ensure that all scripts or executables run by rc scripts are not world



© SANS Institute 2000 - 2005 Author retains full rights.

writeable.

### 3.2.4 System defaults files

Finding # 2.2.4 (CAT II): The system profile file does not contain the command 'mesg n'.

**Discovery:** The /etc/profile (the default profile for a system user) was examined. Although several changes could be made, one of concern was that the message utility was not disabled (default). While reviewing system settings, it was also noted a large number of files in /etc/default files could also be altered and improved.

**Risk:** The example here is the stopping of users from sending messages to each other by default (not the Solaris 7 default) in the /etc/profile file. This could be used mislead a user.

**Recommendation:** Ensure other users can not send messages to the user's terminal by ensuring that 'mesg n' command is included in the system profile (/etc/profile). An additional precaution could be taken by forcing execution in a system wide script forcefully injected into every .cshrc and .profile file on the system.

| **There is a general recommendation here:** Review *all* system default files, especially those in the /etc/default directory. The default configuration of these files can be improved upon to enhance security. |
|---|

### 3.2.5 FTP Configuration

Finding # 2.2.5 (CAT II): System users are not restricted from the use of the FTP protocol

**Discovery:** From the /etc/initd.conf file (shown previously) and the local nmap run (shown previously) show the ftp service is active. Access to the FTP service is partially controlled by the file /etc/ftpusers. This file was not present on the system. On a positive note, not ftp user (allowing anonymous FTP) was found in the /etc/passwd file.

```
# ls -al /etc/ftpusers
/etc/ftpusers: No such file or directory
```

**Risk:** The standard FTP daemon provided by Solaris is likely sufficient if necessary. As with any service, if it is not necessary it should be eliminated. It may be more cumbersome for some other method of transfer (although secure FTP is simple enough for any user) but it should be implemented to be more secure. The risk here is the FTP service could be exploited to place malicious files on the system or the service itself could be subjected to an exploit (buffer overflow) yielding access to the process and/or user



© SANS Institute 2000 - 2005 Author retains full rights.

running the service. Typically it is recommended that the WU (Washington University) FTP daemon be used and configured appropriately. Again, as any other unused service, if it is not needed then it should be shut off.

**Recommendation:** At a minimum, create the /etc/ftpuser file. This file should contain all users of the system without a business need to access the FTP service. Per the ftpd manual page: "…if the user name appears in the file /etc/ftpusers, ftp access is denied." At a minimum, this file should contain the root user, any application user IDs, and any system IDs not requiring interactive logon. Consideration should be given to installing and *properly* configuring the WU FTP daemon.

### 3.2.6 Timeout

Finding # 2.2.6 (CAT IV): The default shell idle is unlimited.

**Discovery:** Examination of the /etc/default/login yielded the following (a section of the file is shown). Note the (shown here and not found elsewhere in the file) TIMEOUT value is not set by virtue of being commented out:

```
# SUPATH sets the initial shell PATH variable for root
#
#SUPATH=/usr/sbin:/usr/bin

# TIMEOUT sets the number of seconds (between 0 and 900) to wait before
# abandoning a login session.
#
#TIMEOUT=300

# UMASK sets the initial shell file creation mode mask.  See umask(1).
#
#UMASK=022
```

**Risk:** All systems that process sensitive information should have a "timeout" protection feature that automatically terminates the user session after a predetermined period has passed without communication between the user and the system. The risk is that a user could leave a open session and anyone accessing the session could continue and do actions as that user. Although policy to assure that sessions are not left unattended should be put in place (see the policy recommendations); enabling this feature can prevent mistakes and help enforce those trying to ignore the policy. The timeout feature may not be required if the system must remain active as a communications device. However, physical security for the system should meet the requirements for storage of data at the highest level that could be received. The time period may vary, depending on the sensitivity of the data, but should not exceed 15 minutes.

**Recommendation:** Set the shell idle time (TIMEOUT in the /etc/default/login to no greater than 15 minutes (5 minutes [300 seconds] is suggested).



© SANS Institute 2000 - 2005 Author retains full rights.

**There is a general recommendation here:** Review *all* parameters in the /etc/default/login file. The default configuration of this file can be improved upon to enhance security; in many cases an improvement is provided but commented out.

## *3.3 Risks from Third-party Software*

The primary third-party application on this host is the Oracle Database. Although it is clear that other software has been installed the security recommendations center on the Oracle Database software.

### 3.3.1 Unowned files

Finding # 2.3.1 (CAT II): Files were found that were not owned by a valid user account on the system.

**Discovery:** This problem is listed here as the installation of improperly prepared software can often result in this adverse side-effect. Using the "-nouser" and "-nogroup" switched on the find command. Note the following looks in /usr/local – a typical installation location.

```
$ cd /usr/local
$ find . -nouser -ls
1980354    1 drwxrwxrwx  3 514      staff         512 Jan 31  2000 ./purify/purify-
4.5.1-solaris2/cache/usr/local/purify
1986564    1 drwxrwxrwx  2 514      staff         512 Jan 31  2000 ./purify/purify-
4.5.1-solaris2/cache/usr/local/purify/purify-4.5.1-solaris2
1986565    0 -rw-rw-rw-  1 514      staff           0 Jan 31  2000 ./purify/purify-
4.5.1-solaris2/cache/usr/local/purify/purify-4.5.1-solaris2/.pure
1986566    6 -rw-rw-rw-  1 514      staff        5856 Jan 31  2000 ./purify/purify-
4.5.1-solaris2/cache/usr/local/purify/purify-
4.5.solaris2/solaris2_threads.so_pure_p3_c0_451_57
1992777   68 -rw-rw-rw-  1 514      staff       69152 Jan 31  2000 ./purify/purify-
4.5.1-solaris2/cache/usr/lib/libsocket.so.1_pure_p3_c0_451_57
1992778 1104 -rw-rw-rw-  1 514      staff     1119944 Jan 31  2000 ./purify/purify-
4.5.1-solaris2/cache/usr/lib/libnsl.so.1_pure_p3_c0_451_57
1992779  168 -rw-rw-rw-  1 514      staff      159060 Jan 31  2000 ./purify/purify-
4.5.1-solaris2/cache/usr/lib/libm.so.1_pure_p3_c0_451_57
1992780   51 -rw-rw-rw-  1 514      staff       51892 Jan 31  2000 ./purify/purify-
4.5.1-solaris2/cache/usr/lib/libgen.so.1_pure_p3_c0_451_57
1992781   53 -rw-rw-rw-  1 514      staff       53776 Jan 31  2000 ./purify/purify-
4.5.1-solaris2/cache/usr/lib/libaio.so.1_pure_p3_c0_451_57
1992782   25 -rw-rw-rw-  1 514      staff       25536 Jan 31  2000 ./purify/purify-
4.5.1-solaris2/cache/usr/lib/libmp.so.2_pure_p3_c0_451_57
$
```

Here files are owned by UID 514. Note this is a very bad situation also shown on file permissions – there are libraries and shared objects that may be linked to dynamically linked executables which are world writeable.

**Risk:** Safeguards used by the system must be able to detect and minimize unauthorized



© SANS Institute 2000 - 2005 Author retains full rights.

modification or destruction of data. Safeguards should ensure that information is protected from the potentially destructive impact of human error (inadvertent actions) as well as malicious logic and unauthorized modification of hardware, software, or data.

This should not happen during the default installation of the operating system or third party utilities. Unfortunately during the installation of third-party software it can be the case that the user or group ids of the developer gets propagated to the local system. This could also happen as the result of passing data from one system to another. In a worst-case scenario, this could be an indication of an already occurred compromise. In this case with world writeable it is a moot point but if the files were only user writeable, one could assume the UID of 514 and have write permissions on the files.

**Recommendation:** All files should be reviewed and associated with a valid uid, or otherwise removed from the system. Installation and security standard operating procedures should be reviewed to ensure that unowned files are detected, investigated, and corrected during normal system operation.

### 3.3.2 Oracle Database Auditing

Finding # 2.3.2 (CAT II): Oracle Auditing is not enabled.

**Discovery:** Many of the Oracle discoveries are through examination of various table values or the lack of a table or value. In this case there was a lack of entries in the DBA_STMT_AUDIT_OPT tables. The Oracle database was found to have auditing disabled. In other cases where it could be implemented it was not. Although this is an auditing issue, it is specific to Oracle.

**Risk:** Just like system audit trails, the data in the database can be altered with no record of when or by whom. Without this traceability, how can anyone be sure of the validity of the data?

**Recommendation:** Enable auditing to ensure that appropriate events are logged. These should include creation, alteration and dropping of database user-IDs, creation, alteration, dropping and managing tablespaces or segments, creation, alteration and dropping of database tables, creation, alteration, and dropping of database indexes, creation, alteration and dropping of procedures, creation, alteration and dropping of profiles, enabling or disabling audit functionality, granting and revocation of database system level privileges, error messages due to attempted access to non-existent objects, renaming of database objects, user-level granting or revoking of object level privileges from a role or user, modifications to the system area, and all session connection requests. Also ensure that the AUDIT_TRAIL parameter is set to DB or TRUE.



© SANS Institute 2000 - 2005 Author retains full rights.

### 3.3.3 Oracle Data Access issues

Finding # 2.3.3.1 (CAT I): The PUBLIC user has access to the database audit trail views.

**Discovery:** This is a data access issue specific to the Oracle database. By examining the allowed views for each user (including the PUBLIC [effectively any] user) via SQL thia access was discovered.

**Risk:** Much like system audit files, a malicious user can cover their actions by rewriting the log file to eliminate their action. The validity of the audit data and the ability to discover inappropriate action are compromised.

**Recommendation:** Remove access privilege for the PUBLIC user to access the views holding the database audit trails.

Finding # 2.3.3.2 (CAT III): Auditing table AUD$ is located in the SYSTEM tablespace.

**Discovery:** This is a data access issue specific to the Oracle database. By examining the SYS tables (again via SQL using the SQL statements "desc <table>" and "select * from <table>") the location of the audit data can be determined.

**Risk:** As above, the data can be compromised. In this case it is by a higher privileged user (SYS) but the problems is the same as SYS has access to the SYSTEM tablespace.

**Recommendation:** Relocate the auditing tables to a separate tablespace or data file.

### 3.3.4 Oracle Database User Roles

Finding # 2.3.4 1 (CAT II): Individual application, user, and administrator roles have Oracle system privileges allowing action on database objects, including administrative roles.

In addition to the individual assignment of unique identifiers, there should be established guidelines for the management of passwords as the primary authenticator.

**Discovery:** In this case there are no views or ownership associated with any of the data tables. All tables, views, and permissions were assigned to NAME_1 with full read, update and drop privilege. Again, via SQL (using the SQL statements "desc <table>" and "select * from <table>") the ownership and permission can be displayed.

**Risk:** The risk here is also tracability. Without defined roles any system user (*they all access and connect to the oracle database via the NAME_1 user via the application!*)



© SANS Institute 2000 - 2005 Author retains full rights.

can not directly be traced to a database action. Further, no limiting to access can be provided. An application user that should have limited access may via the application but if the application is circumvented the users unlimited database privilege could be used to destroy or otherwise compromise data.

**Recommendation:** Evaluate the impact and consider removing the CONNECT capability for the APPDBA, OUTLN, and WEBSYS (default) users. Access to system objects should be granted only through the use of roles. Database object permissions should be set to limit the ability of application users to perform action on database objects. Administrative roles options should be restricted from application roles.

Finding # 2.3.4.2 (CAT I): An unidentified user is assigned DBA role privileges. Individuals may log in as the application object owner.

**Discovery:** As above.

**Risk:** Application or typical users should not have DBA privileges. All the same risks in the above example apply. This goes hand-in-hand with the preceding problem; roles must be assigned for individual users.

**Recommendation:** Remove administrative privilege from the NAME_1 user. Ensure a sufficient change control process is in place to track addition, alteration or removal of privilege, and that the system is periodically checked to ensure that users are assigned to proper roles and that permissions are appropriate.

## *3.4 Administrative Practices*

Administrative practices cover the policy and physical security put in place to protect the system. Unfortunately, a complete lack of policy was found as was physical security. Both of these areas require immediate attention.

### 3.4.1 SOPs

Finding # 2.4.1 (CAT I): Formalized Security Standard Operating Procedures (SOPs) do not exist.

**Discovery:** Owners, Management, operators were all asked to produce SOPs. None could do so. It was determined from interviews that no SOPs exists for aspects of the system as to the manner in which the ownership or responsibility for the system is turned over to site personnel, the secure operation, maintenance, or requirements of the fielded system by site personnel, or testing and hardening system components with respect to security.



© SANS Institute 2000 - 2005 Author retains full rights.

**Risk:** There are many risks here. Procedures can be lost. Basic security policy cannot be followed or referenced if not documented. Documentation should be maintained that describes how security will be managed and will include rules for gaining physical, local, and remote access. Additionally, procedures for providing local and remote access by maintenance personnel, and site-specific rules for managing automated security management systems or access control programs will be documented. Standard security operating procedures should include the development and review of audit trails, management of user identification codes (USERIDs) and passwords, and retention periods of information system security records. There are many actions required to assure proper security that cannot be implemented on the system and require a policy or procedure to be followed; without proper documentation to define and require these, overall security can be compromised.

**Recommendation:** Develop Standard Operating Procedures to formally document the procedures for securely installing, configuring, maintaining, and operating the system. Implement "sudo" and require it's utilization to track root user access.

### 3.4.2 Physical Security

Finding # 2.4.2 (CAT I): Physical Security does not exist. No security exists for the system where it is currently located.

**Discovery:** In the course of this evaluation it was uncovered that anyone in the facility could access the system. Its location was somewhat concealed, such that it would be difficult to know who had used the system; yet the area was accessible by all employees and could even be accessed by visitors. Further, the system was not screen locked and the screen active most times the system was audited. The system root passwords were found under the keyboard.

**Risk:** The risk here should be clear. An unlocked screen allows anyone with physical access to perform any operation as that user. Having the root password written and accessible means anyone who wants to can run any command that machine. As the machine could be accessed by anyone, it must be understood- given direct uncontrolled physical access: the machine *can* be compromised.

**Recommendation:** Incorporate into the Security Standard Operating Procedures to formally document the procedures for maintaining the physical security including having the server behind a locked door and general user security (writing and giving out passwords).

## *3.5 Security Patches*



© SANS Institute 2000 - 2005 Author retains full rights.

Both the operating system and application have errors discovered during use. The vendor typically (this is the case for the operating system and the database) provides "patches" to correct these vulnerabilities. To assure the highest level of security the security patches should be applied.

It should be noted that the plan for the Standard Operating Procedures discussed in the previous section should include provisions to assure that the patches are available and applied to the system.

### 3.5.1 Sun Recommended Patch Cluster

Finding # 2.5.1 (CAT II): Recommended security patches have not been applied.

**Discovery:** It is clear for an examination of the output from the "showrev –p" command that a number of patch revisions are not current (as compared to the patches listed in the latest Recommended Patch Cluster available from Sun Microsystems). It is also clear from the policies and procedures that there has been no recent update of the patches for the operating system.

**Risk:** Exploits on systems are well circulated among hackers. When a vunerability is discovered it can be quickly spread reaching many systems. Although vendors provide patches to rectify these problems, if the patch is not implemented the system remains vunerable. An old hack may be tried and succeed.

**Recommendation:** Properly apply recommended security patches. Ensure that a process exists to ensure that security patches are identified, tested and applied in an efficient manner. For this system the Recommended patch cluster can be downloaded from http://sunsolve.sun.com/.

## *3.6 Sensitive Data Issues*

All data on this system in the database can be said to be proprietary and sensitive. The most sensitive data could be stored encrypted. Limited numbers AES applications are available. As such, a 3DES solution is recommended. Implementation could be done at the application layer or at the data level. An application such as PGP could be installed. This area requires additional investigation.

## *3.7 Network Data Encryption*

The system uses SKIP to protect network access to the systems network services. SKIP is a transparent kernel module that works at the Network (IP) layer of the ISO stack. This level of host-to-host data encryption is very good and can provide sufficient security if implemented correctly.



© SANS Institute 2000 - 2005 Author retains full rights.

However it was apparent during the evaluation that some hosts are allowed access to the system and any network protocols without SKIP's protection (using the "default line" in the access control list (/etc/skip/acl.hme0). The main risk is limited to those hosts that are allowed to bypass SKIP. No hosts should be allowed to connect to the system that are not using SKIP.

A minor issue is that via SKIP all the protocols are tunneled within the IP packets. The down side of this is that it does not allow examination of the individual protocols or restriction by them. New protocols can be applied within the tunnel and are not obvious. To counter this problem, a tool that allows control over the traffic at a lower protocol such as IP filter (available at http://coombs.anu.edu.au/~avalon/ip-filter.html ) should also be considered for use.

The Oracle Advance Security Option also allows transmitted Oracle data to be encrypted. This option should be strongly considered.

### 3.7.1 Vulnerable Protocols

Finding # 2.7.1 (CAT II): Vulnerable network protocols were in use. These include TELNET, FTP, SNMP, REXEC, RLOGIN, and RSH.

**Discovery:** The nmap, netstat –na, and examination of the inetd.conf (all previously shown) identified these protocols/services in use and active. When accessing the system from a remote location (even another system) it was discovered that the most common method was telnet.

**Risk:** For hosts allowed to bypass SKIP (see below) any one of these protocols is subject to attack. Other SNMP hazards and general risks have been previously described. The RLOGIN hazard has been previously described. Similar problems and compromises exist for REXEC and RSH. For a database server it is unlikely that REXEC, RLOGIN, SNMP, AND RSH are required. In fact, it is reasonable to assume that TELNET and FTP may not be required.

**Recommendation:** Verify the need for using any of the vulnerable protocols (disable in the inetd.conf file if they are determined to be unnecessary) and consider using a more secure protocol such as Secure Shell (SSH) version 2 to replace TELNET and FTP if required.

### 3.7.2 SKIP default

Finding # 2.7.2 (CAT I): The default line is enabled in SKIP.



© SANS Institute 2000 - 2005 Author retains full rights.

**Discovery:** When accessing the system from a remote location (even another system) it was discovered that the most common method was telnet. This was encrypted by SKIP. The access control list for SKIP limits the connecting hosts unless the default line is present; then any host may connect cleartext. The access control file is shown:

```
# cd /etc/skip
# cat acl.hme0
skiphost -i hme0 -p
skiphost -i hme0 -a default
skiphost -i hme0 -a 192.168.1.201
skiphost -i hme0 -a 224.0.0.1
skiphost -i hme0 -a 224.0.0.2
skiphost -i hme0 -a 192.168.1.25
skiphost -i hme0 -a 192.168.1.34
skiphost -i hme0 -a 63.17.12.10 -v 2 -k DES-EDE-K3 -t DES-EDE-K3 -m MD5 -r 8 -R
0x9c23331d14071dc23453c1d1c3d90a27 -s 8 -S 0x2365abcdef8348723fdecab36532fade
skiphost -i hme0 -a 13.20.118.17 -v 2 -k DES-EDE-K3 -t DES-EDE-K3 -m MD5 -r 8 -R
0x9144403f56fd35bff3c2d717a545a85e -s 8 -S 0x2365abcdef8348723fdecab36532fade
skiphost -i hme0 -a 128.190.161.26 -v 2 -k DES-EDE-K3 -t DES-EDE-K3 -m MD5-NAT -r
8 -R 0x666ae5f28fffcde8fe1a78d526b69da5 -s 8 -S 0xe61258207f4d488137984e7f58cd
fe98
skiphost -i hme0 -a 189.57.24.30 -v 2 -k DES-EDE-K3 -t DES-EDE-K3 -m MD5 -r 8 -R
0x2f3000746c36fbc5685a1b261d5a3068 -s 8 -S 0x2365abcdef8348723fdecab36532fade
skiphost -i hme0 -a 192.168.1.224 -A 63.117.141.40 -v 2 -k DES-EDE-K3 -t DES-EDE
-K3 -m MD5-NAT -r 8 -R 0x3b3aaaa273af38fcd541f050ac25df1f -s 8 -S 0xe61258207f4d
488137984e7f58cdfe98
skiphost -i hme0 -a 209.22.91.233 -v 2 -k DES-EDE-K3 -t DES-EDE-K3 -m MD5 -r 8 -R
0x5dbddd21d32983456fc66d350def56de6 -s 8 -S 0x2365abcdef8348723fdecab36532fade
skiphost -i hme0 -a 172.16.1.244 -A 128.190.161.26 -v 2 -k DES-EDE-K3 -t DES-EDE
-K3 -m MD5-NAT -r 8 -R 0x41fae5f283e246e827fcccd526b69da5 -s 8 -S 0xe61258207f4d
488137984e7f58cdfe98
skiphost -i hme0 -a 204.37.14.250 -v 2 -k DES-EDE-K3 -t DES-EDE-K3 -m MD5 -r 8 -
R 0xcacedcf2c5df3452a85c7753fff1be24e -s 8 -S 0x2365abcdef8348723fdecab36532fade
skiphost -i hme0 -o
```

**Risk:** If all hosts were encrypted using the 3DES encryption (hosts shown in italics) there would be little direct risk. Again, as noted above, if an encrypted host is compromised it will be impossible to identify problematic traffic from that host because of SKIP. The real risk is in the "cleartext" unencrypted connections show in bold. Although some of these may be required (a nameserver for example) they should be limited and require alternate protection (service filtering, service disabled, or alternate encryption). The biggest risk here is likely a misconfiguration- the presence (underlined) of the default line. This allows any other hosts not listed to connect "cleartext" bypassing the ACL without any encryption.

**Recommendation:** There is no need for using the default line. It should be removed and any hosts needing access added to the access control list; preferable encrypted.

## *3.8 Access Control*

One of the primary methods of securing a system is to implement access control to both the system (services and logins) and files on the system (file system access control via



© SANS Institute 2000 - 2005 Author retains full rights.

users and groups). The following subsections deal with these issues.

### 3.8.1 Warnings and Banners

Finding # 2.8.1 (CAT II): An appropriate warning banner was not present on the system.

**Discovery:** The basic login banner was listed (a similar lack of change from the default was found in the X banner and default for FTP [no banner modification] also):

```
# cat /etc/motd
Sun Microsystems Inc.  SunOS 5.7      Generic October 1998
#
```

**Risk:** There are two risks here. First, anyone should be warned that they are accessing a controlled system and that they may be monitored. This allows proper prosecution if someone is caught. Second, no information that could be used to assist in compromise (such as the operating system version) should be displayed. This can be used to direct the type of attacks used and speed up the hackers progress an limit the chance of being observed.

**Recommendation:** Install an appropriate warning banner on the system and network components. All information systems should display the a warning logon banner immediately upon startup and before the logon request for user ID and password. The banner should remain displayed at least until a suitable user response (e.g., disconnect or start of login) is detected. This is the first step in restricting access: letting a potential hacker know that they are trespassing and in violation of the law.

### 3.8.2 Improper file access permissions

Finding # 2.8.2.1 (CAT II): System log files and files located within the system log partition were not properly protected.

**Discovery:** Log files were found with permissions more greater than 744. Files were found allowing world-readable and world-writeable permissions Examination of files in ./var/adm yielded the following:

```
# ls -al /var/adm
total 43748
drwxrwxr-x   6 root     sys         1024 Nov 18 03:10 .
drwxr-xr-x  26 root     sys          512 Jun 28 18:17 ..
drwxrwxr-x   5 adm      adm          512 Nov 12  1999 acct
-rw-------   1 uucp     bin            0 Nov 12  1999 aculog
-r--r--rwx   1 root     root      220948 Nov 21 18:16 lastlog
-rwxr-xr-x   1 root     other      10836 Sep  8  2000 lastx
-rw-r--r--   1 root     other       5369 Sep  8  2000 lastx.c
```



© SANS Institute 2000 - 2005 Author retains full rights.

```
-rwxr-xr-x   1 root     other       4058 Feb 26  2001 lastx.pl
drwxrwxr-x   2 adm      adm          512 Nov 12  1999 log
-rw-r--r--   1 root     other          0 Jul 19 19:51 login
-rw----rwx   1 root     sys        10875 Jun  7 12:42 loginlog
-rw-r--r--   1 root     other      74652 Nov 21 21:14 messages
-rw-r--r--   1 root     other     139660 Nov 18 03:08 messages.0
-rw-r--r--   1 root     other     139913 Nov 11 03:08 messages.1
-rw-r--r--   1 root     other     139684 Nov  4 03:08 messages.2
-rw-r--r--   1 root     other     139382 Oct 28 03:08 messages.3
-rw-r--r--   1 adm      adm       804320 Aug 22 19:59 pacct
-rw-r--r--   1 adm      adm       485800 Sep 11  2000 pacct1
-rw-r--r--   1 adm      adm       117200 Sep 12  2000 pacct2
-rw-r--r--   1 adm      adm      5111120 Oct  3  2000 pacct3
drwxrwxr-x   2 adm      adm          512 Nov 12  1999 passwd
drwxrwxr-x   2 adm      sys          512 Nov 12  1999 sa
-rw-rw-rw-   1 bin      bin            0 Nov 12  1999 spellhist
-rw----rwx   1 root     root     1086274 Nov 21 21:10 sulog
-rw-r--r--   1 root     bin         1764 Nov 21 18:16 utmp
-rw-r--r--   1 root     bin        18228 Nov 21 18:16 utmpx
-rw-rw-rw-   1 root     root         134 Apr 24  2000 vold.log
-rw-rw-r--   1 adm      adm       362628 Nov 21 18:16 wtmp
-rw-r--r--   1 root     other      28560 Sep  8  2000 wtmp.txt
-rw-rw-r--   1 adm      adm      11505216 Nov 21 18:16 wtmpx
-rw-r--r--   1 root     other    1966791 Sep  8  2000 wtmpx.txt
-rw-r--r--   1 root     other      18288 Sep 11  2000 wtmpx.txt.odc
#
```

**Risk:** The system should function so that each user has access to all of the information to which the user is entitled (by virtue of job duty, formal access approval), but to no more. In the case of "need- to-know" for proprietary information, access must be essential for accomplishment of job function. Modified log files could be used to hide security problems or compromises. The most problematic files are shown in bold. *This is not the default permissions on these files. It must have been altered to allow world write! Any user can easily alter these logs and hide compromises!*

**Recommendation:** Remove world-write permissions on all files located within the system log partition and on all log files. Where possible, remove world-readable permissions on log files. Log files should be protected with a minimum permission of 744.

Finding # 2.8.2.2 (CAT III): Manual files were found not properly protected.

**Discovery:** All the files in /usr/man and /usr/local/man were evaluated for permissions.

**Risk:** Altered manual files could be used to cause a user to take an inappropriate action. See the access requirements in finding 2.8.2.1.

**Recommendation:** Restrict permissions to manual pages to no greater than 744.

Finding # 2.8.2.3 (CAT II): System files were found not properly protected.

**Discovery:** System executables were found with permissions greater than 755 (to permissive), and were not owned by a privileged user. The inetd.conf file was found with



© SANS Institute 2000 - 2005 Author retains full rights.

permissions of 555 (not default and too permissive). The following is a list of files in /etc and /usr/bin:

```
$ pwd
/etc
$ ls -al inetd.conf
lrwxrwxrwx   1 root     root          17 Oct 29  1999 inetd.conf -> ./inet/inetd
.conf
$ ls -al ./inet/inetd.conf
-r-xr-xr-x   1 root     other       6294 Jul 26 17:38 ./inet/inetd.conf
$


$ cd /usr/bin
$ ls -al | grep rwx | grep -v ">"
drwxrwxr-x   4 root     bin         7680 Sep 27 20:06 .
drwxrwxr-x  31 root     sys         1024 Nov  3  1999 ..
-rwxr-xr-x   1 bin      bin        20360 Sep 11  1998 apm
-rwxrwxr-x   1 root     staff     220568 Aug 13  1998 audioconvert
-rwxrwxr-x   1 root     staff     109560 Aug 13  1998 audioplay
-rwxrwxr-x   1 root     staff      27660 Aug 13  1998 audiorecord
-rwxr-xr-x   1 bin      bin        10592 Sep  1  1998 bdiff
-rwxr-xr-x   1 oracle   other       2840 Jul 12 17:53 coraenv
-rwxr-xr-x   1 oracle   other       2428 Jul 12 17:53 dbhome
-rwxr-xr-x   1 bin      bin       317580 Oct  6  1998 fmli
-rwxr-xr-x   1 bin      bin         8540 Sep  1  1998 lastcomm
-rwxr-x---   1 bin      bin        13184 Oct  6  1998 logins
-rwxr-xr-x   1 bin      bin         6456 Sep  1  1998 look
-rwxr-xr-x   1 oracle   oinstall     62 Oct 12  2000 mann
-rwxr-xr-x   1 oracle   other       2559 Jul 12 17:53 oraenv
-rwxrwxr-x   1 root     root         821 Oct 12  1998 prodreg
-rwxr-xr-x   1 root     sys        30552 Sep 11  1998 showrev
-rwxr-xr-x   1 bin      bin         1765 Sep  1  1998 sotruss
drwxr-xr-x   2 root     bin          512 Nov  1  1999 sparcv7
drwxr-xr-x   2 root     bin          512 Nov  1  1999 sparcv9
-rwxr-xr-x   1 bin      bin         5576 Sep  1  1998 vsig
-rwxr-xr-x   1 bin      bin         1083 Sep  1  1998 whocalls
$
```

**Risk:** A malicious user could start an unneeded compromisable process or even malicious process after a reboot by altering the inetd.conf file. See the access requirements in finding 2.8.2.1. The bold lines indicate a file with group write permissions that may not be necessary. There may be a reason for staff write access to the audio tools but this is not the default and should be evaluated for necessity.

**Recommendation:** Restrict permissions to system executables to no greater than 755. Ensure system executables are owned preferably by the root account or alternatively by another privileged user account. The inetd.conf file should be set to 400 permissions.

### 3.8.3 System password file permissions

Finding # 2.8.3.1 (CAT II): The file that defines user account parameters was not properly protected.

**Discovery:** On examinination of the /etc/passwd file it was discovered set to 755 permissions.



© SANS Institute 2000 - 2005 Author retains full rights.

```
$ ls -al /etc/passwd
-rwxr-xr-x   1 root     sys          710 Jul 12 19:38 /etc/passwd
$
```

**Risk:** The permission on this file is not sufficiently restrictive (it has been altered from the default). It is likely they have been altered. This needs to be corrected. It should be noted that the owner and group were correct. Compromise of this data can allow user directed attacks.

**Recommendation:** Set the /etc/passwd file to permissions or 444.

Finding # 2.8.3.2 (CAT II): The file containing the encrypted passwords of users was not properly protected.

**Discovery:** As above, on examination the /etc/shadow file was found with 555 permissions.

```
$ ls -al /etc/shadow
-r-xr-xr-x   1 root     sys          416 Jul 12 19:38 /etc/shadow
$
```

**Risk:** As above, the permission on this file is not sufficiently restrictive (it is not the default). It is likely they have been altered. This needs to be corrected. It should be noted that the owner and group were correct. This is of higher risk than the above in that the encrypted passwords are stored in this file and could be taken and subjected to a brute force attack.

**Recommendation:** Set the permissions of the /etc/shadow file to 400.

### 3.8.4 User home directory access

Finding # 2.8.4.1 (CAT II): User home directories were not properly protected.

**Discovery:** All the home directories were examined for all users in the /etc/passwd file. Shown below is an example:

```
$ grep oracle /etc/passwd
oracle:x:1001:102:Oracle software owner:/opt/oracle:/bin/sh
$ ls -ald /opt/oracle
drwxr-xr-x  12 oracle   oinstall    2048 Oct 29 20:54 /opt/oracle
$
```

**Risk:** The system should function so that each user has access to all of the information to which the user is entitled (by virtue of job duty, formal access approval), but to no more. In the case of "need- to-know" for proprietary information, access must be essential for accomplishment of job function.



© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

It appeared that the /etc/group file was properly configured for allowing group sharing of the file systems. With the home directory in this configuration any user can at least see all the files in a user's home directory and may be able to access the contents of this files. Most importantly, the files should be protected such that "other" users are not allowed to read the data.

**Recommendation:** Ensure all user home accounts are protected with permissions no more permissive than 750.

Finding # 2.8.4.2 (CAT II): User startup files were not properly protected.

**Discovery:** As in the previous example the home for a user was identified and the "dot" files examined:

```
$ cd /opt/oracle
$ ls -al
total 69130
drwxr-xr-x  12 oracle   oinstall    2048 Oct 29 20:54 .
drwxrwxr-x  15 root     other        512 Jul 26 17:38 ..
-rw-------   1 oracle   oinstall     297 Sep  5 17:55 .Xauthority
-rw-r--r--   1 oracle   oinstall       4 Aug 10 15:30 .cshrc
-rw-r--r--   1 oracle   oinstall     477 Jul 13 18:41 .cshrc_old
drwxr-xr-x  14 oracle   oinstall     512 Sep  5 17:55 .dt
-rwxr-xr-x   1 oracle   oinstall    5111 Nov  4  1999 .dtprofile
drwxr-xr-x   2 oracle   oinstall     512 Jul 23 17:54 .hotjava
-rw-r--r--   1 nobody   oinstall       0 Nov  4  1999 .login
drwx------   4 oracle   oinstall     512 Nov  7 19:40 .netscape
-rw-rw-rw-   1 oracle   oinstall    1163 Jul 23 15:56 .profile
-rw-r--r--   1 root     other          72 Sep 14  2000 .razor_login
-rw-r--r--   1 root     other          72 Sep 14  2000 .razor_login.BAK
-rw-------   1 oracle   oinstall       2 Feb  2  2000 .sh_history
drwx------   2 oracle   oinstall     512 Sep  5 17:55 .solregis
```

**Risk:** See the access requirements in finding 2.8.4.1. Many of this files are read or executed (or the files in the subdirectories) on startup. Being able to read and worse write some of the files could allow a user to be compromised. Of particular concern in this case is a world writable .profile file. Any user could read and alter this file to take action when the user runs a shell.

**Recommendation:** Ensure all user startup files, including .Xauthority, .dtprofile, .profile, .login, and .cshrc files, are protected with privileges no more permissive than 740.

Finding # 2.8.4.3 (CAT II): Files within user home directories were not owned by the user.

**Discovery:** See the data shown above. The italicized lines show files not owned by the user. Of particular concern is a file owned by nobody in a users home.

**Risk:** See the access requirements in finding 2.8.4.1 as well as the risks identified above.



© SANS Institute 2000 - 2005 Author retains full rights.

A user running as nobody could read and alter this file to take action when the user runs a shell.

**Recommendation**: Ensure users own all files within their respective home directories. In the case of files within application users' home directories, ensure that ownership of files are properly restricted.

### 3.8.5 Cron/AT Files

Finding # 2.8.5 (CAT II): Cron and AT service files were not properly protected.

**Discovery:** An examination of the various cron and at directories was undertaken. Crontab files had permissions greater than 600 and the cron.deny file was found with 744 permissions. The at.deny file was found with 744 permissions. This data is shown below:

```
$ cd /var/spool/cron/crontabs
$ ls -al
total 14
drwxr-xr-x   2 root     sys          512 Oct 29  1999 .
drwxr-xr-x   4 root     sys          512 Oct 29  1999 ..
-rw-r--r--   1 root     sys          190 Oct 29  1999 adm
-rwxrwxrwx   1 root     root         750 Oct 29  1999 lp
-rw-r--r--   1 root     sys          482 Oct 29  1999 root
-rw-r--r--   1 root     sys          308 Oct 29  1999 sys
-r--r--r--   1 root     sys          404 Oct 29  1999 uucp
$

$ ls -al /etc/cron.d
total 20
drwxr-xr-x   2 root     sys          512 Oct  9 13:52 .
drwxr-xr-x  32 root     other       3072 Oct  9 13:52 ..
-rwxr--r--   1 root     sys           72 Jan  1  1970 .proto
prw-------   1 root     root           0 Oct  9 13:52 FIFO
-rwxr--r--   1 root     sys           45 Oct 29  1999 at.deny
-rwxr--r--   1 root     sys           45 Oct 29  1999 cron.deny
-r-xr-xr-x   1 bin      bin         1626 Nov 24  1998 logchecker
-rw-r--r--   1 root     sys           17 Jan  1  1970 queuedefs
$
```

**Risk:** Inappropriate protection on these files allows user to run commands as other users (perhaps root) by inserting commands in the existing files. At least one user account (lp) had world writable permissions on the crontab file allowing any other user to edit the file and get any command to be run by that user at any time.

**Recommendation:** Set permissions on the crontab files to 600. Set permissions on the at.deny and cron.deny files to 400.

### 3.8.6 General Access Issues



© SANS Institute 2000 - 2005 Author retains full rights.

Finding # 2.8.6 (CAT II): World writeable files were found on the system.

**Discovery:** The following command was run on the system:

```
find / -perm -2 -a \( -type d -o -type f \) -exec ls -ld {} \;
```

This command finds all the world writable files on the file system.

**Risk:** As a general rule on a system such as this there is no need for world writeable files.

**Recommendation:** Verify the need for world writeable permissions on files. Remove the world-writeable permissions as necessary from files on the system.

## *3.9 Backup & Disaster Recovery*

### 3.9.1 Backup Device

Finding # 2.9.1 (CAT IV): Device files used for backup are world writable.

**Discovery:** The primary backup device on the system a 8mm magnetic tape drive located at /dev/rmt/0. The information is as follows:

```
# ls -al /dev/rmt/0
lrwxrwxrwx   1 root     root          42 Nov 12  1999 /dev/rmt/0 -> ../../device
s/pci@1f,4000/scsi@3,1/st@4,0:
# ls -al /devices/pci@1f,4000/scsi@3,1/st@4,0:
crw-rw-rw-   1 root     sys       33,267 Nov  7 17:57 /devices/pci@1f,4000/scsi@
3,1/st@4,0:
#
```

**Risk:** Although this finds its way into the Backup section it might equally be described as a configuration issue. The nature of the system utilization requires backups be performed. If the physical access issues are resolved limiting by user or group id may not be necessary. If tapes are left unattended in place in the device any user could compromise the data.

**Recommendation:** Ensure only users that have a documented business need to backup the system are allowed access to the device files used for backups.

### 3.9.2 Backup Policy

Finding # 2.9.2 (CAT II): There is no formal backup policy.



© SANS Institute 2000 - 2005 Author retains full rights.

**Discovery:** As with SOPs inquiries were made to the backup policy. No formal policy was discovered when operators and system administrators were queried.

**Risk:** Although this finds its way into the Backup section it might equally be described as a administrative issue. The nature of the system utilization requires backups be performed. Backups were found and have been done on an ad-hoc basis. The operators have never tried a restore from the tapes. Should the disk be compromised (or even fail) no data recovery could be made as the backups might be incomplete or bad. At best some quanity of data will be lost.

**Recommendation:** Ensure the SOPs include a backup policy addressing a complete backup strategy including a schedule and backup validation.

### 3.9.3 Off Site Storage

Finding # 2.9.3 (CAT II): The backup tapes were stored with the system.

**Discovery:** During the examination of the backup policy and procedures it was asked as to where the backups were stored. The operators identified a box on top of the drive as the place they had put the ad-hoc backup sets they had generated.

**Risk:** Although this finds its way into the Backup section it might equally be described as a administration issue as the pervious issue. When policy defines backup it should include provisions for off site storage. The physical audit found *all* backup taped to be stored on top of the system. In the event of a fire or water damage it is likely hat all backup would be lost with the system. Further, anyone with physical access to compromise the system could destroy or alter the backup tapes.

**Recommendation:** Ensure the SOPs include a backup policy addressing an off site backup storage strategy including when the tapes will be moved off site, where they will be stored (including security off site), and who will execute the policy.

## *3.10 Logging and Data Collection*

One of the essential steps in securing a system is reviewing the various log information to assure that the system remains secure and has not been compromised. The following subsection address some shortcomings of the current data collection and review.

### 3.10.1 BSM Configuration

Finding # 2.10.1 (CAT II): The BSM was not configured and auditing not running.



© SANS Institute 2000 - 2005 Author retains full rights.

**Discovery:** On physical audit it appeared that the files in /etc/security had not had the Basic Security Module turned on. This means there is not a audit file in /var/audit and that bsmconv was never run. Further the default switches had not been changed (see previous findings).

**Risk:** There is a great deal of audit information to be collected through the configuration of the files in the /etc/security directory. It will impact performance but it should be a requirement for operation as it will provide significant information to monitor security. By reviewing this data system compromises can in some cases be detected and the information can be used to confirm intrusions detected from other sources and assess the damage. Since it was not collected, it is obviously not reviewed.

**Recommendation:** Create the /var/adm/loginlog log file and ensure failed and successful logins are properly audited. This information should be audited as defined in the SOPs.

### 3.10.2 Login Log

Finding # 2.10.2 (CAT II): Successful and unsuccessful logons are not logged.

**Discovery:** The log file /var/adm/loginlog did not exist.

```
# ls -al /var/adm/loginlog
/var/adm/loginlog: No such file or directory
#
```

**Risk:** There should be in place safeguards to ensure each person having access to an system may be held accountable for his or her actions on the system. There should be an audit trail providing a documented history of system use. The audit trail shall be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise should a security violation or malfunction occur. The risk is not having this information (as above). Since it was not collected, it is obviously not reviewed.

**Recommendation:** Create the /var/adm/loginlog log file and ensure failed and successful logins are properly audited. This information should be audited as defined in the SOPs.

### 3.10.3 Auditing Flags

Finding # 2.10.3 (CAT II): Audit flags were not set according to standard.

During the analysis of the /etc/security directory several of the configuration files were examined. The -fw and -ex flags (which can provide useful audit information) were not set. Shown is the audit_control file:

```
# cd /etc/security
# cat audit_control
```



© SANS Institute 2000 - 2005 Author retains full rights.

```
#
# Copyright (c) 1988 by Sun Microsystems, Inc.
#
#ident  @(#)audit_control.txt  1.3     97/06/20 SMI
#
dir:/var/audit
flags:
minfree:20
naflags:lo
#
```

**Risk:** Like the two previous findings, the risk is not having data to evaluate for suspicious activity or to confirm that compromises have taken place. The following table lists the predefined audit classes (from the manual pages for audit_control):

| short name | long name | short description |
|---|---|---|
| no | no_class | null value for turning off event preselection |
| fr | file_read | Read of data, open for reading, etc. |
| fw | file_write | Write of data, open for writing, etc. |
| fa | file_attr_acc | Access of object attributes: stat, pathconf, etc. |
| fm | file_attr_mod | Change of object attributes: chown, flock, etc. |
| fc | file_creation | Creation of object |
| fd | file_deletion | Deletion of object |
| cl | file_close | close(2) system call |
| pc | process | Process operations: fork, exec, exit, etc. |
| nt | network | Network events: bind, connect, accept, etc. |
| ip | ipc | System V IPC operations |
| na | non_attrib | non-attributable events |
| ad | administrative | administrative actions: mount, exportfs, etc. |
| lo | login_logout | Login and logout events |
| ap | application | Application auditing |
| io | ioctl | ioctl(2) system call |
| ex | exec | exec(2) system call |
| ot | other | Everything else |
| all | all | All flags set |

These flags can also be set for a specific user in the audit_user file. For a user like "root" many more flags might be set. Also see the requirements description for finding 2.10.2.

**Recommendation:** Ensure appropriate audit flags are configured. The appropriate flags are a function of the nature of the data, the amount of data that can be stored, the amount of the collected data that will be reviewed, and the activity of the system. At a minimum add the ex flag in the audit_control file and as many of the "f" flags as possible for root in the audit_user file.

### 3.10.4 Sendmail Auditing



© SANS Institute 2000 - 2005 Author retains full rights.

Finding # 2.10.4 (CAT III): Critical sendmail log entries are not sent to the postmaster.

**Discovery:** The sendmail configuration doesn't not have an entry for critical errors to de delivered to the postmaster.

**Risk:** Again this an availability of log data for review issue. Although sendmail has been disabled on this system, to allow proper logging should sendmail be configured to run again

**Recommendation:** Ensure that the system is configured to send all critical sendmail log entries to the postmaster. This should be configured even if sendmail is not running in the case that sendmail should be started at any time in the future. Sendmail itself should not be run if not needed.

### 3.10.5 Service Logging

Finding # 2.10.5 (CAT II): The INETD and FTP services do not appropriately log events.

**Discovery:** While examining the /etc/inetd.conf file (see section 2.2.1) the FTP line was listed:

```
# Ftp and telnet are standard Internet services.
#
# BELOW MODIFIED FOR TCP WRAPPERS
ftp     stream  tcp     nowait  root    /usr/sbin/tcpd  in.ftpd
```

Additionally the /etc/rc2.d startup file was examined and the call to start inetd did not have the "-t" option (this is the SUN default).

Risk: Any service that is started by the inetd.conf file (especially the FTP service as noted above) should have information about its activity logged. The current configuration does not do this for these two services. We applaud the use of wrappers but also suggest the following.

**Recommendation:** Add the -t option to the inetd startup command within the inetsvc service startup file. Insert the -l and -v options into the command that starts the in.ftpd service within the inetd.conf file.

## *3.11 Other Appropriate Actions*

There are several other actions that should be taken that do not fall into the categories above. They are identified below.



© SANS Institute 2000 - 2005 Author retains full rights.

### 3.11.1 ASET

Finding # 2.11.1 (CAT II): The Automated Security Enhancement Tool (ASET) is not configured to run weekly to compare the system against an ASET security baseline.

**Discovery:** Examination of the crontabs had no indication of weekly (or any scheduled running for that matter) of ASET. In addition, ASET files were not properly protected.

**Risk:** One of the most important steps in securing a system is vigilance and auditing the system. The auditing information collected (as specified in the previous section) goes a long way to this end. Additionally some tools that evaluate the current state of the system should be used (tripwire was already suggested); ASET is one such tool. Numerous system evaluation tools are available, without showing favor to any single tool we suggest a web search for "security analysis tools".

**Recommendation:** Configure the ASET tool to run at least weekly to ensure critical system components remain securely configured. Ensure only valid users that have a need to run ASET are specified in the ASET userlist file, which is owned by root with permissions of 600 or more restrictive. Strongly consider using tripwire to monitor changes to the system and performing security analysis periodically with a security analysis tool.

# 4 Conclusion

In conclusion, the system requires many changes to be deemed secure. Additionally numerous policies need to be created, approved, and implemented. It is suggested that the findings be addressed in the order by priority as identified in the following section (Section 3.1). The specific recommended fix is shown in the previous subsection; however a sorted list by expected cost (least to greatest) is shown in the subsequent subsection (Section 3.2).

In Summary:

- **It is without doubt the system is currently at high risk.**
- **The findings should be corrected immediately.**
- **The system is not secure.**

We would appreciate any opportunity to provide a detailed cost estimate to correct the problems identified in this report.



© SANS Institute 2000 - 2005 Author retains full rights.

## 4.1 Prioritized Vulnerabilities

| | FINDINGS SORTED BY PRIORITY | |
|---|---|---|
| **Finding** | **Priority** | **Description** |
| Finding # 2.1.1 | (CAT I) | The DNS executable |
| Finding # 2.1.5.1 | (CAT I) | The SNMP community string was set to the default |
| Finding # 2.3.3.1 | (CAT I) | The PUBLIC user |
| Finding # 2.3.4.3 | (CAT I) | An unidentified user is assigned DBA role |
| Finding # 2.4.1 | (CAT I) | Formalized Security Standard Operating Procedures |
| Finding # 2.4.2 | (CAT I) | Physical Security does not exist |
| Finding # 2.7.2 | (CAT I) | The default line is enabled in SKIP |
| Finding # 2.1.3 | (CAT II) | Approved shells were not listed in the /etc/shells |
| Finding # 2.1.4 | (CAT II) | Files have the SUID and/or SGID |
| Finding # 2.1.5.2 | (CAT II) | SNMP management information base (MIB) files |
| Finding # 2.1.6 | (CAT II) | Device files are not properly protected |
| Finding # 2.2.1 | (CAT II) | The RLOGIN service was running |
| Finding # 2.2.3.2 | (CAT II) | Password aging controls are not configured |
| Finding # 2.2.3 | (CAT II) | System startup files were not properly protected |
| Finding # 2.2.4 | (CAT II) | The system profile file |
| Finding # 2.2.5 | (CAT II) | System users are not restricted from FTP |
| Finding # 2.3.1 | (CAT II) | Files found that were not owned by a valid user |
| Finding # 2.3.2 | (CAT II) | Oracle Auditing is not enabled |
| Finding # 2.3.4 1 | (CAT II) | Individuals may log in as application obj owner |
| Finding # 2.3.4.2 | (CAT II) | Individual application, user, and administrator roles |
| Finding # 2.5.1 | (CAT II) | Recommended security patches not applied |
| Finding # 2.7.1 | (CAT II) | Vulnerable network protocols were in use |
| Finding # 2.8.1 | (CAT II) | An appropriate warning banner |
| Finding # 2.8.2.1 | (CAT II) | System log files |
| Finding # 2.8.2.3 | (CAT II) | System files were found not properly protected |
| Finding # 2.8.3.1 | (CAT II) | The /etc/passwd file |
| Finding # 2.8.3.2 | (CAT II) | The /etc/shadow file |
| Finding # 2.8.4.1 | (CAT II) | User home directories were not properly protected |
| Finding # 2.8.4.2 | (CAT II) | User startup files were not properly protected |
| Finding # 2.8.4.3 | (CAT II) | Files within home directories not owned by user |
| Finding # 2.8.5 | (CAT II) | Cron/AT files not properly protected |
| Finding # 2.8.6 | (CAT II) | World writeable files were found on the system |
| Finding # 2.9.2 | (CAT II) | There is no formal backup policy |
| Finding # 2.9.3 | (CAT II) | The backup tapes were stored with the system |
| Finding # 2.10.1 | (CAT II) | The BSM not configured and auditing not running |
| Finding # 2.10.2 | (CAT II) | Successful and unsuccessful logons are not logged |
| Finding # 2.10.3 | (CAT II) | Audit flags were not set according to standard |
| Finding # 2.10.5 | (CAT II) | The INETD and FTP services do not log |
| Finding # 2.11.1 | (CAT II) | The Automated Security Enhancement Tool (ASET) |
| Finding # 2.2.3.1 | (CAT III) | Users can change passwords within 24 hours |
| Finding # 2.3.3.2 | (CAT III) | Auditing table |
| Finding # 2.8.2.2 | (CAT III) | Manual files were found not properly protected |
| Finding # 2.10.4 | (CAT III) | Critical sendmail log entries not sent to postmaster |
| Finding # 2.1.2 | (CAT IV) | The root account is the root directory |
| Finding # 2.2.6 | (CAT IV) | The default shell idle is unlimited |
| Finding # 2.9.1 | (CAT IV) | Device files used for backup are world writable |
| | | |



© SANS Institute 2000 - 2005 Author retains full rights.

## 4.2 Recommended Fixes Cost

| | FINDINGS SORTED BY COST | | | | |
|---|---|---|---|---|---|
| | | Labor rate used for calculations is $150.00/Hour | | | |
| Finding | Priority | Description | Hours | Material | Total |
| Finding # 2.1.3 | (CAT II) | Approved shells were not listed in the /etc/shells | 0.5 | 0.00 | 75.00 |
| Finding # 2.1.5.1 | (CAT I) | The SNMP community string was set to the default | 0.5 | 0.00 | 75.00 |
| Finding # 2.10.3 | (CAT II) | Audit flags were not set according to standard | 0.5 | 0.00 | 75.00 |
| Finding # 2.10.4 | (CAT III) | Critical sendmail log entries not sent to postmaster | 0.5 | 0.00 | 75.00 |
| Finding # 2.2.1 | (CAT II) | The RLOGIN service was running | 0.5 | 0.00 | 75.00 |
| Finding # 2.2.3.1 | (CAT III) | Users can change passwords within 24 hours | 0.5 | 0.00 | 75.00 |
| Finding # 2.2.3.2 | (CAT II) | Password aging controls are not configured | 0.5 | 0.00 | 75.00 |
| Finding # 2.2.4 | (CAT II) | The system profile file | 0.5 | 0.00 | 75.00 |
| Finding # 2.2.5 | (CAT II) | System users are not restricted from FTP | 0.5 | 0.00 | 75.00 |
| Finding # 2.7.2 | (CAT I) | The default line is enabled in SKIP | 0.5 | 0.00 | 75.00 |
| Finding # 2.8.2.2 | (CAT III) | Manual files were found not properly protected | 0.5 | 0.00 | 75.00 |
| Finding # 2.8.3.1 | (CAT II) | The /etc/passwd file | 0.5 | 0.00 | 75.00 |
| Finding # 2.8.3.2 | (CAT II) | The /etc/shadow file | 0.5 | 0.00 | 75.00 |
| Finding # 2.10.5 | (CAT II) | The INETD and FTP services do not log | 1.0 | 0.00 | 150.00 |
| Finding # 2.2.6 | (CAT IV) | The default shell idle is unlimited | 1.0 | 0.00 | 150.00 |
| Finding # 2.8.1 | (CAT II) | An appropriate warning banner | 1.0 | 0.00 | 150.00 |
| Finding # 2.8.2.3 | (CAT II) | System files were found not properly protected | 1.0 | 0.00 | 150.00 |
| Finding # 2.8.5 | (CAT II) | Cron/AT files not properly protected | 1.0 | 0.00 | 150.00 |
| Finding # 2.8.6 | (CAT II) | World writeable files were found on the system | 1.0 | 0.00 | 150.00 |
| Finding # 2.1.1 | (CAT I) | The DNS executable | 2.0 | 0.00 | 300.00 |
| Finding # 2.1.5.2 | (CAT II) | SNMP management information base (MIB) files | 2.0 | 0.00 | 300.00 |
| Finding # 2.10.2 | (CAT II) | Successful and unsuccessful logons are not bgged | 2.0 | 0.00 | 300.00 |
| Finding # 2.11.1 | (CAT II) | The Automated Security Enhancement Tool(ASET) | 2.0 | 0.00 | 300.00 |
| Finding # 2.2.3 | (CAT II) | System startup files were not properly protected | 2.0 | 0.00 | 300.00 |
| Finding # 2.3.1 | (CAT II) | Files found that were not owned by a valid user | 2.0 | 0.00 | 300.00 |
| Finding # 2.5.1 | (CAT II) | Recommended security patches not applied | 2.0 | 0.00 | 300.00 |
| Finding # 2.8.2.1 | (CAT II) | System log files | 2.0 | 0.00 | 300.00 |
| Finding # 2.8.4.3 | (CAT II) | Files within home directories not owned by user | 2.0 | 0.00 | 300.00 |
| Finding # 2.9.1 | (CAT IV) | Device files used for backup are world writable | 2.0 | 0.00 | 300.00 |
| Finding # 2.1.2 | (CAT IV) | The root account is the root directory | 4.0 | 0.00 | 600.00 |
| Finding # 2.1.4 | (CAT II) | Files have the SUID and/or SGID | 4.0 | 0.00 | 600.00 |
| Finding # 2.1.6 | (CAT II) | Device files are not properly protected | 4.0 | 0.00 | 600.00 |
| Finding # 2.10.1 | (CAT II) | The BSM not configured and auditing not running | 4.0 | 0.00 | 600.00 |
| Finding # 2.3.2 | (CAT II) | Oracle Auditing is not enabled | 4.0 | 0.00 | 600.00 |
| Finding # 2.3.3.1 | (CAT I) | The PUBLIC user | 4.0 | 0.00 | 600.00 |
| Finding # 2.8.4.1 | (CAT II) | User home directories were not properly protected | 4.0 | 0.00 | 600.00 |
| Finding # 2.8.4.2 | (CAT II) | User startup files were not properly protected | 4.0 | 0.00 | 600.00 |
| Finding # 2.9.3 | (CAT II) | The backup tapes were stored with the system | 2.0 | 750.00 | 1,050.00 |
| Finding # 2.9.2 | (CAT II) | There is no formal backup policy | 8.0 | 100.00 | 1,300.00 |
| Finding # 2.7.1 | (CAT II) | Vulnerable network protocols were in use | 12.0 | 500.00 | 2,300.00 |
| Finding # 2.3.3.2 | (CAT III) | Auditing table | 16.0 | 0.00 | 2,400.00 |
| Finding # 2.4.2 | (CAT I) | Physical Security does not exist | 12.0 | 1,000.00 | 2,800.00 |
| Finding # 2.3.4.3 | (CAT I) | An unidentified user is assigned DBA role | 24.0 | 0.00 | 3,600.00 |
| Finding # 2.3.4 1 | (CAT II) | Individuals may log in as application obj owner | 32.0 | 0.00 | 4,800.00 |
| Finding # 2.3.4.2 | (CAT II) | Individual application, user, and administrator roles | 32.0 | 0.00 | 4,800.00 |
| Finding # 2.4.1 | (CAT I) | Formalized Security Standard Operating Procedures | 40.0 | 200.00 | 6,200.00 |
| | | **SUM** | 242.5 | 2,550.00 | 38,925.00 |
| | | | | | |



© SANS Institute 2000 - 2005 Author retains full rights.

# 5 References

Anonymous, Maximum Security: A Hackers Guide to Protecting Your Internet Site and Network Second Edition. Copyright 1998 Sams Publishing.

Ashford Computer Consulting Service. Securing a Solaris Server. URL: http://www.accs.com/p_and_p/SolSec/ .

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

Mcclure, Stuart, and Scambray, Joel, and Kurtz George. Hacking Exposed: Network Security Secrets & Solutions. Copyright 1999 McGraw-Hill.

SANS Institute, Solaris Security step by step Version 2.0. Copyright 2001 The SANS Institute.

Winsor, Janice. Solaris Advanced Systems Administrator's Guide. Copyright 1993 Sun Microsystems Inc..

© SANS Institute 2000 - 2005, Author retains full rights.



© SANS Institute 2000 - 2005 Author retains full rights.