Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?
Check out the list of upcoming events offering "Securing Linux/Unix (Security 506)"
at http://www.giac.org/registration/gcux
“The only reason the castle wall is secure is because of the dedicated people behind it” (Author Unknown)

GCUX Practical Assignment
Version 1.9

Title: Auditing a University Solaris System
Submitted By: Geoffrey Poer
Date: June 10, 2003

Securing UNIX Certification Dec 30, 2002
Abstract:

Security in University environments is often deemed none existent. More and more the universities are striving to better themselves in these areas but the road is long and difficult. As budget are decreasing in University environments more and more pressure is being put on administrators to provide resources but not the resource to maintain the systems in question. This paper expresses the need to move to a more secure infrastructure and change the philosophy of administrators and users alike by providing the requirements to move to a more secure environment and the configuration required to do it.
Table of Contents

Executive Summary ........................................................................................................... 3
Section 1.0: Description of System and Audit Methodology ........................................ 4
  1.1 Hardware Specifications ....................................................................................... 4
  1.2 Operating System ............................................................................................... 4
  1.3 Role of the Audited System ................................................................................. 4
  1.4 Network Configuration ....................................................................................... 5
  1.5 Applications ........................................................................................................ 5
  1.6 Tools .................................................................................................................. 13
  1.7 System Defenses ............................................................................................... 13
  1.8 Audit Methodology .......................................................................................... 17

Section 2.0: Detailed Analysis ..................................................................................... 18
  2.1 Operating System Vulnerabilities ..................................................................... 18
  2.2 Security Patch Installation/Management ........................................................... 18
  2.3 Configuration vulnerabilities ............................................................................. 18
  2.4 Risks from Installed Third-Party Software ....................................................... 25
  2.5 Administrative Practices ................................................................................... 30
  2.6 Identification and Protection of Sensitive Data on the Host ......................... 31
  2.7 Protection of Sensitive Data in Transit over the Network or Internet ........ 32
  2.8 Access Controls ............................................................................................... 32
  2.9 Backup Policies & Disaster Preparedness ......................................................... 32
  2.10 Other Issues .................................................................................................... 33

Section 3.0: Critical Issues and Recommendations .................................................. 34
  3.1 Top Ten Recommendations .............................................................................. 34
  3.2 Further Recommendations Outside of the Top Ten Threats ......................... 38

References .................................................................................................................... 39
Appendix A: Output of “LSOF –I” ........................................................................... 40
Appendix B: Complete Access-list ............................................................................ 42
Appendix C: Hosts.allow & Hosts.Deny ................................................................. 45
Appendix D: Results of “Listit” ................................................................................. 47
Appendix E: Results of TitanReport ......................................................................... 49
Appendix F: Results of Internal Nessus Scan ......................................................... 52
Appendix G: List of Recommended and Security Patches ......................................... 64
Executive Summary

Purpose of Audit

GIAC University has several systems with varying levels of exposure and criticality. This audit will identify the current level of security for the system. We will also be assessing the potential vulnerabilities and making recommendation on changes to reduce the risk of those vulnerabilities.

Scope of Audit

The University has chosen to audit BigDog.dep.univ.edu. This system was chosen for its similarity to other critical systems and its high level of exposure due to the multiple world accessible services that the machine offers.

Conclusions

This system is running in an environment that is not geared toward security. A culture change is going to need to take place in order for this system to be brought to a higher level of security. Infrastructure changes and resources are going to be required in order for the suggested changes to be successful.

Most important recommendations

The following are the minimum requirements suggested for security changes to BigDog and the infrastructure.

1. Develop written policies
2. Put systems behind a proxy firewall on a Service Network and redesign the network defenses
3. Remove unnecessary services
4. Move away from Clear text protocols
5. Develop a service network for network management applications
6. Remove ftp (use scp)
7. Move to SSH as the only network connection method
8. Separate Services on different machines
1.0 Description of System and Audit Methodology

1.1 Hardware Platform and Specifications

BigDog’s hardware is provided by Sun Microsystems.

Sun ultra sparc 60
2 Processor ultra sparc 440
2 internal Sun 36 gig SCSI
2 external Fujitisus 36 gig SCSI

1.2 Software Operating System and Version

> showrev
Hostname: BigDog.Dep.univ.EDU
Hostid: 1234abcd
Release: 5.8
Kernel architecture: sun4u
Application architecture: sparc
Hardware provider: Sun Microsystems
Domain: MyBuilding
Kernel version: SunOS 5.8 Generic 108528-17 September 2002

1.3 Role of the Audited System

From interview with administrator:

This machine serves many roles. The primary web server for the department is running APACHE. It also serves as a MySQL database server, a Samba file server and the departmental server which implies that it runs multiple services. Several of these services are world accessible due to a customer need. Multi-function systems are a side effect of an ever decreasing budget placing more and more services on single machines in order to save on Vendor support costs as well as Hardware costs.

BigDog is user login server where employees look to find everything from web services to compliers. The current mindset for the department is that every box must have the ability to do everything. Running with NFS shared home directory you can connected to any machine in the cluster and receive files in the users home directory.
1.4 Network Configuration

BigDog is connected to a class C subnet with a 100 meg connection. There are no dedicated firewall services to this network. However there is a firewall in place for the campus that is running a limited set of ACL’s as well as an intrusion detection system. The routed interface supports multiple networks some out of the control of the department. The routed interface has a more restricted ACL that will be discussed later when we talk about Defenses. There are redundant gigabit connection from the core network to the Cisco 3524 switches where BigDog is connected.

1.5 Applications

1.5.1 Network Services:

Two commands were run to establish the network services that are being offered. We later compare this output with Nessus to see if we have any inconsistencies.

```
> /usr/local/sbin/lsof -i tcp
> /usr/local/sbin/lsof -i udp
```

As a note it should be mentioned that some services which are IPv6 aware have multiple entries because they have an IPv4 and IPv6 version; SHELL and EXEC are indicated as duplicates because of this. For the complete list of services please see appendix A.

1.5.2 Applications Running on BigDog:

Below is the list of applications installed on BigDog.

```
> ps -e -o "user,comm" | egrep -v 'Bob|Tom|Greg|Ric|NetMons' | sort -u
  USER COMMAND
    root /dfs/nms/rover/bin/InetRoverd
    root /dfs/nms/rover/bin/pingd
    root /etc/init
    root /private/apache/bin/httpd
    root /private/samba/sbin/nmbd
    root /private/samba/sbin/smbd
    root /usr/dt/bin/dtlogin
    root /usr/lib/autofs/automountd
    root /usr/lib/inet/xntpd
    root /usr/lib/lpsched
    root /usr/lib/nfs/lockd
    root /usr/lib/nfs/mountd
```
1.5.3 Description of Applications

Next we will dig a bit deeper into each application collecting version information and pull any network that is offered information from the application. We will use the information later to compare the internal Nessus scan to get a better idea of the potential vulnerabilities running on BigDog. It is important to manually run through the applications and compare the data with tools like Nessus. As you will see when you look at the Nessus output it does provide false positives.

SunRPC

> /bin/pwd
/devfsadmd

> rpcinfo -p
program vers proto port service
100000 4 tcp 111 rpcbind
100000 3 tcp 111 rpcbind
100000 2 tcp 111 rpcbind
100000 4 udp 111 rpcbind
100000 3 udp 111 rpcbind
100000  2  udp  111  rpcbind
100008  1  udp  32772  walld
100024  1  udp  32773  status
100024  1  tcp  32771  status
100133  1  udp  32773
100133  1  tcp  32771
100021  1  udp  4045  nlockmgr
100021  2  udp  4045  nlockmgr
100021  3  udp  4045  nlockmgr
100021  4  udp  4045  nlockmgr
100021  1  tcp  4045  nlockmgr
100021  2  tcp  4045  nlockmgr
100021  3  tcp  4045  nlockmgr
100021  4  tcp  4045  nlockmgr
100008  1  udp  32808  mountd
100008  2  udp  32808  mountd
100008  3  udp  32808  mountd
100008  1  tcp  32785  mountd
100008  2  tcp  32785  mountd
100008  3  tcp  32785  mountd
100003  2  udp  2049  nfs
100003  3  udp  2049  nfs
100227  2  udp  2049  nfs_acl
100227  3  udp  2049  nfs_acl
100003  2  tcp  2049  nfs
100003  3  tcp  2049  nfs
100227  2  tcp  2049  nfs_acl
100227  3  tcp  2049  nfs_acl

Apache
>./httpd -v
Server version: Apache/1.3.27 (Unix)
Server built: Oct 11 2002 10:01:04

> telnet localhost 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 02 Jun 2003 18:18:22 GMT
Server: Apache/1.3.27 (Unix) PHP/4.2.2 mod_ssl/2.8.11 OpenSSL/0.9.6e
Last-Modified: Thu, 26 Dec 2002 02:50:54 GMT
ETag: "30e698-17fe-3e0a6e8e"
Accept-Ranges: bytes
FINGER
A version number would be irrelevant for this service as it is locally written and maintained. This version of finger was developed by the administrator and does not listening for more than one request this alleviates the vulnerability of catching the process in core and bypass TCP wrapper. This version processes one request and drops the connection. The configuration file available for the finger daemon allows the customization of requests and access controls. Such that finger will not allow user lists or produce information on a configurable set of accounts. This version of finger was written in house and was not released open source.
> finger @BigDog
[BigDog.Dep.univ.EDU]

Finger request for *ALL USERS* refused.

FTP (not world accessible... being controlled by wrappers)

The FTP daemon is an extremely old version of the WUFTP daemon. However, it has been heavily modified with in house fixes or back stitched with patches available open source. Most of the newer vulnerabilities do not relate to this version. The administrator feels that FTP is too useful of a tool to get rid of and does not feel that SSH, SCP or SFTP is reliable enough to be used in a production environment.

TELNET (not world accessible... being controlled by TCP Wrappers)
Sun Release

This service is still running because some systems in the infrastructure DO NOT have a working SSH clients. Management has exhibited no interest in solving the problem and the users which are requiring the telnet daemon will need to be pushed by upper management to find a way to upgrade those machines.

RSH (not world accessible... being controlled by TCP Wrappers)
Sun Version
The admin does not feel that SSH is reliable and it IS NOT A DROP IN REPLACEMENT for this service. You can’t copy SSH.exe to RSH.exe and expect it to work. RSH is used heavily in the batch jobs and it would take a great deal of effort to configure SSH reliably to replace RSH’s ability to run a command remotely.
**RLOGIN** (not world accessible... being controlled by TCP Wrappers)
Sun Version
Currently rlogin is used to get an interactive shell without having to provide a password. It is possible to replace this service with SSH. However some work will need to be done to be used in the batch jobs that currently employ its use. Most notably, work would need to be done lock down display variables.

**NTPD**
/usr/sbin/ntpq
ntpq 3-5.93e Mon Sep 20 15:45:42 PDT 1999 (1)

Locked down to localhost in config file. Not doing any authentication.
# server should match /etc/defaultrouter...
server dep.univ.128.1
restrict dep.univ.128.1

# allow localhost so "ntp -p" works
restrict 127.0.0.1 noserver

> /usr/sbin/ntpq -p BigDog
BigDog.Dep.univ.EDU: timed out, nothing received
***Request timed out

**LPD**
Running to enable cancellation of print jobs
Sun Version

**Samba** (using samba acl also being looked down to a few external networks)
> /bin/pwd
/dfs/src/samba-2.2.5
Restricted via its config file

```bash
username map=/private/samba/etc/smbusers
hosts allow = localhost,
dep.univ.47.80/255.255.255.240, \
dep.univ.63.64/255.255.255.192,
dep.univ.128.0/255.255.255.0, \
dep.univ.129.0/255.255.255.0, \
dep.univ.160.0/255.255.255.0, \
dep.univ.176.128/255.255.255.128,
dep.univ.252.0/255.255.255.0, \
dep.univ.100.32/255.255.255.248, \
dep.univ.112.16/255.255.255.240, \
dep.univ.112.32/255.255.255.224, \
dep.univ.248.176/255.255.255.240, \
xxx.xxx.34.144, xxx.xxx.16.144/255.255.255.240
```
### MySQL

Only available via a network connection

```sql
> mysql -h BigDog -V
mysql Ver 11.18 Distrib 3.23.54, for sun-solaris2.8 (sparc)
```

```sql
mysql> select * from user;
```

<table>
<thead>
<tr>
<th>Host</th>
<th>User</th>
<th>Password</th>
<th>Select_priv</th>
<th>Insert_priv</th>
<th>Update_priv</th>
<th>Delete_priv</th>
<th>Create_priv</th>
<th>Drop_priv</th>
<th>Reload_priv</th>
<th>Shutdown_priv</th>
<th>Process_priv</th>
<th>File_priv</th>
<th>Grant_priv</th>
<th>References_priv</th>
<th>Index_priv</th>
<th>Alter_priv</th>
</tr>
</thead>
<tbody>
<tr>
<td>localhost</td>
<td>root</td>
<td>****</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>root</td>
<td>****</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>tick.dep.univ.edu</td>
<td>Tom</td>
<td>****</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>Tom</td>
<td>****</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>Tom</td>
<td>****</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>%</td>
<td>Tom</td>
<td>****</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>%</td>
<td>ric</td>
<td>****</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>ric</td>
<td>****</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>localhost</td>
<td>NetMons</td>
<td>****</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>opie.univ.edu</td>
<td>NetMons</td>
<td>****</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>tick.dep.univ.edu</td>
<td>NetMons</td>
<td>****</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>NetMons</td>
<td>****</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.homer.org">www.homer.org</a></td>
<td>Tom</td>
<td>****</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>bobies.dep.univ.edu</td>
<td>stuff</td>
<td>****</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>%</td>
<td>ghilde</td>
<td>****</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>cartman.sirt.univ.edu</td>
<td>NetMons</td>
<td>****</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td></td>
</tr>
</tbody>
</table>
```

### SendMail

```bash
> telnet localhost 25
trying 127.0.0.1...
Connected to localhost.
Escape character is '^[']'.
```

```bash
quit
```
```
221 2.0.0 BigDog.Dep.univ.EDU closing connection
Connection closed by foreign host.
NFS (world accessible except that we block it at the edge) (NFS Access Control Feature... meaning that Read Write options are restricted by hosts)
SunVersion

More /etc/dfs/dfstab shows the list of directories BigDog shared with other computers.

More /etc/dfs/vfstab shows the list of file systems we mount. We do not use this we use the automounter daemon.

Automounter runs with root privileges. All home directories are defines to by the automounter. A user can cause a mount to occur but only the ones predefined by the admin.

Blocking NFS 2049 at the border of campus and blocked on local router port. We do not allow mounts from networks outside of our control.

/etc/netgroups holds the group files:

SSH
> ssh -V
OpenSSH_3.5p1, SSH protocols 1.5/2.0, OpenSSL 0x0090605f
1.X is disabled in the configuration file.

Cisco Flow Daemon
> /usr/local/sbin/lsof -i tcp:omnisky
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
   cflowd  447 NetMons 5u IPv4 0x300028101b8 0t0 TCP *:omnisky (LISTEN)

This service listens for Netflow data from the routers. It is a historical artifact that could be removed as its use discontinued.

ROVER
Does a ping and optionally probes a static list of hosts. Rover will probe by connecting to the web server and look for the a 200 on the server meaning it has a problem. Rover also understands and can probe nntp, http, smtp, ftp, ldap, and named.

Keep a 90 running log of host problems. To get a summary.
> pwd
/dfs/nms/rover/etc
> ../bin/roversummary

SysLOGD
Sun VERSION

BigDog also accepts syslog entries from other systems.

1.6 TOOLS Available on BigDog

*BigDog is the distribution point for all software so many of the tools that are installed on the system, such as Sudo, are installed but do not perform a function on the machine.

GCC
PERL
AWK
PHP
VI
GREP
SED
MAKE
SUDO

1.7 System Defenses

1.7.1 Network Defenses

*for complete access-lists please see Appendix B

ACL Summary
The access-list for the routed interface is long and convoluted. It will allow established connections to return with the “established” line. It also allows the two other co-located networks into the network unrestricted access as they are sharing a routed interface. Several networks that are considered inside campus are allowed through to the Network management machine. SSH is allowed into the network management machine from anywhere and well as SMTP, DNS, Syslog, SNMP, TFTP and all types of ICMP. Machines that are being used for network authentication are also allowed to be reached from anywhere to their TACACS port. Web access is allowed to BigDog from anywhere as well as a eight other machines with-in BigDog’s local network. No other machine is allowed a web server. RPCBind services are allowed in from select machines with-in control of the administrator while all other port 111 access is blocked. The same machines are permitted NFS and font server access all other port 2049 and 7100 access is blocked. Oracle listener access is blocked. APC access is blocked.
Port 6000 access is allowed from 3 networks within the admin's control. Multicast subscription is permitted.

As it relates to BigDog these are the services that are restricted from the world based on the ACL on the Routed interface:

RPCBIND tcp/udp 111
NFS tcp/udp 2049
FONT tcp 7100
Oracle tcp 1521
Radius tcp 1646
APC Power tcp/udp 5454-5456 & 6666
X11 tcp 6000
SNMPtrap messages

These are the services that are restricted from the world on the order of campus:

Worm udp 58085
Worm udp 17300
MSSQL udp 1434
Worm tcp 7597
UPnP tcp/udp 1900, 5000
TFTP udp tftp
dtspcd tcp 6112
Font tcp 7100
SNMP tcp/udp 161,161,199,391,705,1993
Bugbear trojan tcp 1080

ICMP
permit icmp echo-reply
permit icmp unreachable
permit icmp source-quench
permit icmp time-exceeded
permit icmp parameter-problem
deny icmp any any

Microsoft Ports
deny tcp/udp 135
deny tcp/udp netbios-ns
deny tcp/udp netbios-dgm
deny tcp/udp 139
deny tcp/udp 445

Standard blocks...
deny ip host 0.0.0.0 any
deny ip 10.0.0.0 0.255.255.255 any
deny ip 127.0.0.0 0.255.255.255 any
deny ip xxx.xxx.0.0   0.0.255.255   any
deny ip xxx.xxx.0.0   0.15.255.255   any
deny ip xxx.255.0.0   0.0.255.255   any
deny ip xxx.0.xx.0     0.0.0.255   any
deny ip xxx.xxx.0.0   0.0.2.255.255   any
deny ip xxx.xxx.0.0   0.0.255.255   any
deny ip any xxx.xxx.0.0   0.0.255.255
deny ip xxxx.0.0.0     0.0.0.255   any
deny ip xxx.xxx.xxx.0 0.0.0.255   any
deny ip dep.univ.0.0 0.0.255.255 any
deny ip dep.univ.0.0 0.0.255.255 any
deny ip xxx.xxx.69.0 0.0.0.255 any
deny ip dep.univ.224.0 0.0.31.255 any

1.7.2 Configuration Defenses

* Solaris system do not allow 64 bit applications to execute arbitrary code on the stack.

/etc/system
* Security fix - prevent execution on stack...
set noexec_user_stack=1
set noexec_user_stack_log=1

* Security fix - require remote side to use a privileged port for NFS
* Transactions
set nfssrv:nfs_portmon=1

Cron File Checker
This is a piece of code in /usr/local/sbin/actions which executes on multiple systems, each of which checks all the other systems hourly to make sure that cron is running.

Sysfile watch
This is a perl script that runs 4 times/day (midnight, 6am, noon, 6pm) which checks selected system text files for changes and mails those differences. It was originally designed to catch things like a Cisco install creating a username or group, so we didn't lose that when BigDog pushed the "standard" copy of the file onto the other systems. It has been expanded to watch other files, and be a more of a general audit tool.

Daemon watch
This checks to make sure only one copy of inetd is running. It will restart certain critical daemons if they are missing (sendmail, ssh, apache...).
Findtit (Cron)
This tool does a find for world write, suid, and .rhosts files and saves the modify time. It then compares the modify times to the previous run of the tool and reports back (through email) any changed or new files.

Findit is a home grown utility based on the tool FINDIT written by Andrey Yeatts. Cliff Hathaway added .rhosts support in mid 1990, and our administrator has maintained the open source tool ever since.

TCPWRAPPERS
*Full hosts.allow and Deny files can be found in Appendix C

Summary of hosts.allow
The Hosts.allow file is allowing any connection for the networks in the department and any connection from a select members of the staff.

It is also allowing in connections from the Test Network and the rsh connections from a machine maintained by the system admin on another network.

SSHD is also allowed from any where but mail is generated if any connections are made from a host considered to be external.

RPCBind requests are restricted to specific machines that require that functionality.

Summary of hosts.deny
The Hosts.deny file will spawn an email message with the connection attempt for RPC bind as well as another service controlled by inetd.

COPS
COPS is a 16 bit checksum tool that has been modified by the admin to include MD5 checksum abilities. This tool maintains a md5 checksum file of the system files on BigDog and also checks the permission files in /dev to establish whether these files are world writable (a classic intrusion sign). COPS is run nightly out of cron.

1.7.3 Specific Risks and Concerns

This system is on a network with several other machine providing critical network management functions as well as authentication services for the network devices on campus. BigDog itself is providing several services available to the world, such as HTTP and SSH, and doubles as a departmental server. The admin of the machine; however, is extremely competent and well versed in the Solaris operating system. Of course, everyone can make mistakes and this audit will hopefully empower the admin to make changes to the network infrastructure
as well as the computing policies currently in use by the department to help minimize mistakes when they do happen.

The main concern for this machine is the wealth of information that it has access to. If we are looking for the crown jewels of the department. We have found the treasure chest. BigDog has access to router configs, password files, mail directories and is trusted by almost every machine in the department. BigDog is a main target for an attack. To alleviate some of this the functionality will need to be divided along the lines of internal and externally available services. This will help us invent an entirely NEW infrastructure design that will allow the admin for freedom in implementing security features on BigDog while still offering services to the world on a services network huge from the firewall.

1.8 Audit Methodology

Step 1: Review of Administrative Procedures and system configuration.

To begin we will interview the system administrator to get his assessment of the system. No one knows the system like the individual charged with its care and feeding. Next we will review the record keeping procedures and patching procedures to evaluate their effectiveness. We will also run several command line tools that will enable us to assess the system configuration. Most of these you have already seen in the System Description section.

Step 2: Titan Security Audit Tool.

Titan is an open source host-based security tool. Its primary function is to improve the security of a UNIX operating system. However, it does have the ability to audit the security of a system based on the changes that Titan would have made to the system.

The tool is composed mostly of Bourne Shell scripts and is run out of a master directory which calls to several other scripts. Each module has various flags which can cause the script to change settings or simply log the differences. We are using this tool with the “-v” flag or the “verify’’ option. As an auditing tool it does have some draw backs. The current implementation of TitanReport simply looks for the changes that the Titan script would have made. If the permissions are more restrictive or if certain files are not present it will log the particular module as a FAILURE, when in fact it is not.

Titan does not check for patch level security or look for bug replacements; its focus is on the configurations options available as an OS and the most secure way to implement those options.
Step 3: Use of the scanning tool Nessus to identify network vulnerabilities.
Internal: Nessus will be run from a machine on the Local Network to assess the possible points of intrusion and trust relation exploits that could be taken advantage of.
External: Nessus will be run from machines completely outside of the network and system defenses will be used to ascertain the possible intrusion points in addition to verifying access-lists.

*results of these scan can be seen in the Appendices

Step 4: Analyze collected Data
Taking the System description data, the output from the Titian tool and the results of the Nessus scan we will drill into the application and system configurations to develop a current state of security and suggest changes to better secure the environment in the future.

2.0 Detailed Analysis

2.1 Operating System Vulnerabilities
As of this audit the latest version of Solaris is 9. However in their current environment there is no reason (application or hardware) that requires it. Currently Sun is still fully supporting version 8 and when that support decreases the organization will plan on moving to Solaris 9. Until that time The administrator will continue to test Solaris 9 at his convenience.
The current patch REV is from the Solaris 8 Patch Report Update of Dec/16/2002. We will talk more about the Patching procedure in the next section.
Appendix G has a complete list of the current recommended patches as well as the security patches that are not included in the recommended patch cluster. These should be installed as soon as possible.

2.2 Security Patch Installation/Management
OS Install is covered /dfs/sysadmin/doc/Sun/local_changes_[78].
Patch procedure is to download the recommended patch cluster from sun and run its built-in installer, and then put back our sendmail and rpcbind if needed. The administrator does this over Christmas and late in the summer, unless something extremely critical comes along.

There are basically NO written standards or policies available. The unwritten standards are basic. Be good and you get to keep your account. If you need a service or application installed just let the administrator know and he will get it installed with-in the week and take full responsibility for keeping it up to date.
Testing
To test the patch cluster the admin installs them on his desktop. If all goes well the admin will move the patches to other users desktops. When this proves stable a general rollout is done to all servers and systems. Patches and testing are done when the administrator has the time to accomplish the task. If the patches are necessary to fix a critical vulnerability then the patch will take precedence over all other activities however that decision is at the discretion of the admin.

2.3 Configuration vulnerabilities

2.3.1 Unnecessary Services

SendMail
Version of Program/version of config file:
BigDog currently receives and routes mail. There is a dedicated mail server that is already providing this function. It would be possible to modify the MX records on the dedicated mail server to receive and route mail for BigDog and to set up a sendmail –q procedure on Bigdog to have mail sent from the host. Another problem with removing sendmail is that various applications talk to localhost 25. These application could break if we removed sendmail. It will require a great deal of configuration work to accomplish this however another option is to simply reconfigure sendmail to accept connection only form the localhost.

RSH (TCP Wrapper)
Sun Version
Removing this and using SSH is a recommendation. However, it will not be an easy job. The admin does not feel it is reliable and it IS NOT A DROP IN REPLACEMENT for RSH. We have provided scripts for the admin to review from www.billsterns.org that describes how to do this. Also RSH is used VERY heavily in the batch jobs and these jobs will need to be re-written to allow for SSH syntax.

RLOGIN (TCP Wrapper)
Sun Version
Currently rlogin is used to get an interactive shell without having to provide a password. It is possible to replace this service with SSH. However some work will need to be done to be used in the batch jobs that currently employ its use. Most notably work would need to be done lock down display variables.

TELNET
The Telnet Daemon is not world accessible and is controlled by tcpwrappers. We discovered in our interview with the admin that it is really only being kept accessible for one administrator of other systems. We are recommending that the admin in question upgrade to SSH version 2.0 and that telnet be disabled and removed from the system.
From Nessus output:
> Vulnerability telnet (23/tcp)
> The Telnet server does not return an expected number of replies
> when it receives a long sequence of 'Are You There' commands.
> This probably means it overflows one of its internal buffers and
> crashes. It is likely an attacker could abuse this bug to gain
> control over the remote host's superuser.

With the no_exec_user_stack configured this is not a possibility however we do
not recommend using telnet because as it is a clear text protocol and leaves the
possibility of a vulnerability in the advent of an administrative mistake.

Apache
This is by no means an unnecessary service. However, this application/service
needs to run on a different machine on the service network off a firewall.

>./httpd -v
Server version: Apache/1.3.27 (Unix)
Server built: Oct 11 2002 10:01:04

> telnet localhost 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 02 Jun 2003 18:18:22 GMT
Server: Apache/1.3.27 (Unix) PHP/4.2.2 mod_ssl/2.8.11
OpenSSL/0.9.6e
Last-Modified: Thu, 26 Dec 2002 02:50:54 GMT
ETag: "30e698-17fe-3e0a6e8e"
Accept-Ranges: bytes
Content-Length: 6142
Connection: close
Content-Type: text/html

Network Management System (NMS)
These applications and servers should also be separate from BigDog's network.
The network management applications which house passwords and
configurations for every network device on campus need to be better secured.
The primary function of the department is telecommunications therefore the NMS
tools need to be run from a separate service network. The costs of changing
infrastructure at this level are high however in the event of an intrusion an
attacker would be able to destroy the configurations of every switch and router on
campus. That would be a very bad day. There are 2 network applications that
reside on BigDog;
Cisco Flow Daemon

> /usr/local/sbin/lsof -i tcp:omnisky

```bash
COMMAND PID USER   FD   TYPE        DEVICE SIZE/OFF NODE NAME
   cflowd  447 NetMons 5u IPv4 0x300028101b8 0t0 TCP *:omnisky (LISTEN)
```

Listen from Netflow data. Historical artifact that could be removed as it is no longer used.

ROVER

Rover does a ping and optionally probes a static list of hosts. Rover will probe by connecting to the web server and look for the a 200 on the server meaning it has a problem. Rover also understands and can probe nntp, http, smtp, ftp, Ldap, and named. This tool should be moved to the management network that we will discuss later.

It also keeps a 90 day running log of host problems for network devices on campus.

> pwd

```
/dfs/nms/rover/etc
``` 

> ../bin/roversummary

Ilc2

Titan output:

```
-------begin ../logs/modules/disable-Ilc2.sh.V.rpt-------
Ilc2 Service is enabled in /etc/rc2.d/S40Ilc2 - FAILS CHECK
```

This is a false positive because the service isn’t configured. However, it should be removed if not in use.

Ncad

Titan output:

```
-------begin ../logs/modules/disable-ncad.sh.V.rpt-------
Ncad daemon Service is enabled in /etc/rc2.d/S95ncad - FAILS CHECK
```

False positive as the service has a start up script but is not in use. The package should be removed if not in use.

2.3.2 Banners

Several of the services being offered on BigDog provide banner information that gives away critical information concerning the application. SSH, sendmail, PHP, Apache, Samba, FTP and MySQL applications need to have the banners changed in order to prevent this information leak. One caveat of doing this is that scripts and other utilities that use the banner information to verify connections to
the these services will need to be taken into consideration when changing the
banners.

2.3.3 Removable Media Configuration

Titan output:

Rmount allows mounting of CD filesystems with suid binaries enabled - FAILS CHECK
Rmount allows mounting of Floppy filesystems with suid binaries enabled - FAILS CHECK

The threat on BigDog is minimal, as you need an account and physical access to be able to exploit this. However, it is still an unnecessary risk that is easy to resolve.

2.3.4 Boot-Level Access Control

boot password

Titan output:

The Admin does not like to place eeprom passwords on the servers. We still recommend that this change be made to better secure the boot procedures.

single-user mode password
Solaris boots to single user mode and asks for the root password by default, although that can be disabled.

< L1 -A> shutdown

Titan output:

The administrator is fine with the idea that someone with console access is able to L1-A (halt) a system - it’s less drastic than pulling the power plug.

2.3.5 System Access Control

.rhosts

Titan output:

We do use rsh and rlogin, and there is no way the admin would ever turn those of in PAM, even if I did disable them in inetd.conf.
Titan output:

```
-------begin ../logs/modules/rhosts.sh.V.rpt-------
Found //.rhosts... - FAILS CHECK
Rsh connections are allowed from BigDog to BigDog

Found /home/stuff/..rhosts... - FAILS CHECK
This was being used to rdist files from another system. Currently it is not being
used and should be disabled.

Found /home/bob/..rhosts... - FAILS CHECK
This user will need to update their machine in order to support SSH as this
connection will not be allowed in the future.

Found /private/backup_user/.rhosts... - FAILS CHECK
A new backup system will be implanted and this will need to be removed.
```

```
/etc/ftpusers
Titan output:
-------begin ../logs/modules/ftpusers.sh.V.rpt-------
smtp not in /etc/ftpusers - FAILS CHECK
nuucp not in /etc/ftpusers - FAILS CHECK
ingres not in /etc/ftpusers - FAILS CHECK
audit not in /etc/ftpusers - FAILS CHECK
admin not in /etc/ftpusers - FAILS CHECK
sync not in /etc/ftpusers - FAILS CHECK

The admin does not believe in putting non-existent accounts in /etc/ftpusers.
However it does provide a useful audit function. In either case we are suggesting
that the FTP service be removed.
```

```
cron usage
Titan output:
-------begin ../logs/modules/cronset.sh.V.rpt-------
CRONLOG entry found - PASSES CHECK
/var/cron permissions - FAILS CHECK
/etc/cron.d/logchecker LIMIT - FAILS CHECK

The cron logs are not readable by anyone other than root, although you can get a
directory listing of them.

The "LIMIT - FAILS CHECK" is because the limit script
/etc/cron.d/logchecker has LIMIT=1024 (.5mb) instead of
LIMIT=4096.  We suggest making the limit size larger to allow for more logs in
the event of a problem.
```

```
Titan output:
-------begin ../logs/modules/fix-cronpath.sh.V.rpt-------
/etc is not writable by world - PASSES CHECK.
/etc is not writable by group - PASSES CHECK.
```
/etc/cron.d is not writable by world - PASSES CHECK.
/etc/cron.d is not writable by group - PASSES CHECK.
/usr is not writable by world - PASSES CHECK.
/usr is not writable by group - PASSES CHECK.
/usr/sbin is not writable by world - PASSES CHECK.
/usr/sbin is not writable by group - PASSES CHECK.
/usr/lib is not writable by world - PASSES CHECK.
/usr/lib is not writable by group - PASSES CHECK.
/usr/lib/fs is not writable by world - PASSES CHECK.
/usr/lib/fs is not writable by group - PASSES CHECK.
/usr/lib/fs/nfs is not writable by world - PASSES CHECK.
/usr/lib/fs/nfs is not writable by group - PASSES CHECK.
/usr/bin is not writable by world - PASSES CHECK.
/usr/bin is not writable by group - PASSES CHECK.
/etc/cron.d/logchecker is owned by root - PASSES CHECK.
/usr/lib/newsyslog is owned by root - PASSES CHECK.
/usr/bin/rdate is owned by root - PASSES CHECK.
No cron.allow file - FAILS CHECK.
No at.allow file - FAILS CHECK.
-------end .. /logs/modules/fix-cronpath.sh.V.rpt-------

Any user is allowed to use “cron” and “at” unless they are listed in cron.deny and/or at.deny.

root logins
Root login (except on the console) is prohibited by the setting CONSOLE=/dev/console in 
/etc/default/login
The ability to "su root" is allowed which allows for much better audit control of the root account.

Default Logins
Titan output:
-------begin .. /logs/modules/disable-accounts.sh.V.rpt-------
daemon shell = /usr/local/sbin/nologin - FAILS CHECK
bin shell = /usr/local/sbin/nologin - FAILS CHECK

This is a false positive. The method of blocking certain accounts does not match Titan's. These accounts however are disabled.

daemon:x:1:1::/usr/local/sbin/nologin
bin:x:2:2::/usr/bin:/usr/local/sbin/nologin
IP
Titan output:
------begin ../logs/modules/disable_ip_holes.sh.V.rpt------
System set to not forward source routed packets - PASSES CHECK
System does not Forward IP packets - PASSES CHECK
System does not forward directed broadcast packets - PASSES CHECK
System is not set to ignore redirected packets - FAILS CHECK
System is set to do strict multihoming - PASSES CHECK
System configured as 'notrouter' - PASSES CHECK
------end ../logs/modules/disable_ip_holes.sh.V.rpt------
We suggest that the host set redirected packets to ignore. This can be done by setting /dev/ip ip_ignore_redirect to 1.

umask
Titan output:
------begin ../logs/modules/add-umask.sh.V.rpt------
No umask file /etc/init.d/umask.sh found - FAILS CHECK
Solaris 8 sets the boot up umask via /etc/default/init, using the CMASK= variable. This check is valid for Solaris 7 and below, which should have an umask.sh. In any event this script is checking for the umask to be 022. BigDog has set the umask to be 027 which is MORE restrictive than the Titan script suggests.

World writable files
Findit Shows world writable DIR's
Findit |grep -v drwx
for a complete list please see appendix D

Permissions for sensitive files
Titan output:
------begin ../logs/modules/file-own.sh.V.rpt------
Found 15908 files in /usr that should be root owned - FAILS CHECK
Found 0 files in /sbin that should be root owned - PASSES CHECK
Found 0 files in /usr that should be set group g-w - PASSES CHECK
Found 0 files in /sbin that should be set group g-w - PASSES CHECK
Found 0 files in /etc that should be set group g-w - PASSES CHECK
Found 0 files in /opt that should be set group g-w - PASSES CHECK
-------end ../logs/modules/file-own.sh.V.rpt-------

According to the admin Sun will have to change this. Chowning all these files will cause large problems with patchadd.

**INETD**

Titan output:

begin ../logs/modules/inetd.sh.V.rpt-------
exec Open - FAILS CHECK
comsat Open - FAILS CHECK
talk Open - FAILS CHECK
finger Open - FAILS CHECK
wallld Open - FAILS CHECK
shell Open - FAILS CHECK
login Open - FAILS CHECK
exec Open - FAILS CHECK
comsat Open - FAILS CHECK
time Open - FAILS CHECK
printer Open - FAILS CHECK

**XDMCP**

------begin ../logs/modules/cde.sh.V.rpt------
/usr/dt/config/Xaccess allows XDMCP login connections. - FAILS CHECK 1
/etc/dt/config allows XDMCP login connections. - FAILS CHECK 2
Xdmcp is accepted from selected hosts, and used within the cluster.

2.4 Risks From Installed Third-Party Software

2.4.1 APACHE

As of this audit Apache is up to date with the latest security patches.

2.4.2 FTP

FTP (not world accessible... being controlled by wrappers)

The FTP daemon is an extremely old version of the WUftp daemon. However, it has been heavily modified with in-house fixes or back stitched with patches available open source. Most of the newer vulnerabilities do not relate to this version. This application is widely used in the organization. The administrator
does not feel that SSH, SCP or SFTP is reliable enough to be used in a production environment.

**Vulnerability**  ftp (21/tcp)  You seem to be running an FTP server which is vulnerable to the 'glob heap corruption' flaw.  An attacker may use this problem to execute arbitrary commands on this host.

*** Nessus relied solely on the banner of the server to issue this warning,  *** so this alert might be a false positive

Solution : Upgrade your ftp server software to the latest version.  
Risk factor : High

CVE : [CAN-2001-0249](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0249), [CVE-2001-0550](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0550)  
BID : [2550](https://nvd.nist.gov/vuln/detail/CVE-2001-0550), [3581](https://nvd.nist.gov/vuln/detail/CVE-2001-0550)  
Nessus ID : [10821](https://nmap.org/nessus/10821)

**Informational**  ftp (21/tcp)  An FTP server is running on this port.  
Nessus ID : [10330](https://nmap.org/nessus/10330)

**Informational**  ftp (21/tcp)  Remote FTP server banner :

```
220- All transfers and commands are logged with your host name and email
220- address. If you don’t like this policy, disconnect now!
220- If your FTP client crashes or hangs shortly after login, try using a dash (-) as the first character of your password. This will turn off
220- the informational messages which may be confusing your ftp client.
220- In case of problems, questions, suggestions: send mail to
220- ftp-bugs@ms.Dep.univ.EDU.
220- Anonymous access is not allowed.
```

Nessus ID : [10092](https://nmap.org/nessus/10092)
The report from Nessus says that the FTP server is vulnerable to vulnerabilities that are several years old. From our assessment of the system earlier and the interview with the administrator we believe this to be false. The administrator is maintaining the code patches on the FTP server as well as adding custom application tweaking into the source code. It is suggested that the a expert in application security run the code through a few checks to look for possible exploits that the administrator may have missed. This is a low priority action as the administrator is capable of maintaining such code. However, additional checks are always a good idea.

2.4.3 SAMBA

Vulnerability netbios-ssn (139/tcp)
The remote Samba server, according to its version number, has a bug in the length checking for encrypted password change requests from clients. A client could potentially send an encrypted password, which, when decrypted with the old hashed password could be used as a buffer overrun attack on the stack of smbd.
Solution: upgrade to Samba 2.2.7
Risk factor: High
Nessus ID: 11168
Client password changes are prohibited.

Vulnerability netbios-ssn (139/tcp)
The remote Samba server, according to its version number, may be vulnerable to a remote buffer overflow when receiving specially crafted SMB fragment packets.
An attacker needs to be able to access at least one share to exploit this flaw.
Solution: upgrade to Samba 2.2.8
Risk factor: High
BID: 7106, 7107
Nessus ID: 11398
That would put the attacker on a dep.univ internal net, making the threat less likely. However, it is still recommended that these applications be upgraded.

2.4.4 Sendmail

Sendmail seemed to pass the test as far as Nessus was concerned.
Informational smtp (25/tcp) An SMTP server is running on this port
Here is its banner:
Nessus ID: 10330

Informational smtp (25/tcp) Remote SMTP server banner:
This is probably: Sendmail version 8.12.9

Nessus ID: 10263

Informational smtp (25/tcp) This server could be fingerprinted as being Sendmail
8.12.2-8.12.5
Nessus ID: 11421

Informational smtp (25/tcp) For some reason, we could not send the EICAR test string
to this MTA
Nessus ID: 11034

Informational smtp (25/tcp) For some reason, we could not send the 42.zip file to this
MTA
BID: 3027
Nessus ID: 11036

2.4.5 MySQL

> Vulnerability mysql (3306/tcp)
> You are running a version of MySQL which is older than version
> 3.23.56.
> It is vulnerable to a vulnerability that may allow the mysqld service
> to start with elevated privileges.
> An attacker can exploit this vulnerability by creating a
> DATADIR/my.cnf
> that includes the line 'user=root' under the '[mysqld]' option
> section.
> When the mysqld service is executed, it will run as the root
> user instead of the default user.
> Risk factor: High
> Solution: Upgrade to at least version 3.23.56
> CVE: CAN-2003-0150
> BID: 7052
> Nessus ID: 11378

This exploit requires a login, and access to the MySQL group. The MySQL
application should be upgraded as soon as possible.

2.4.6 PHP

> Warning http (80/tcp)
> The remote host is running a version of PHP which is
> older than 4.3.2
> There is a flaw in this version which may allow
> an attacker who has the ability to inject an arbitrary
> argument to the function socket_iovec_alloc() to crash...
> the remote service and possibly to execute arbitrary code
> For this attack to work, PHP has to be compiled with the option
> --enable-sockets (which is disabled by default), and an attacker
> needs to be able to pass arbitrary values to socket_iovec_alloc().
> Other functions are vulnerable to such flaws: openlog(),
> socket_recv(),
> socket_recvfrom() and emalloc()
> Solution: Upgrade to PHP 4.3.2
> Risk factor: Low
> CVE: CAN-2003-0172
> BID: 7187, 7197, 7198, 7199, 7210, 7256, 7259
> Nessus ID: 11468
--enable-sockets is not enabled on BigDog and no_exec_user_stack stops the rest. Risk of this is low; however, updating the service is still a good idea to prevent opening a hole in the event of an administrative mistake.

2.4.7 SSH

> Nessus output:
> You are running OpenSSH-portable 3.6.1p1 or older.

PAM is not enabled.

> If PAM support is enabled, an attacker may use a flaw in this version
> to determine the existence or a given login name by comparing the
> times the remote SSHD daemon takes to refuse a bad password for a
> non-existent
> login compared to the time it takes to refuse a bad password for an
> existent login.
>
2.4.8 OpenSSL

> Warning http (80/tcp)
> The remote host is using a version of OpenSSL which is
> older than 0.9.6j or 0.9.7b
> This version is vulnerable to a timing based attack which may
> allow an attacker to guess the content of fixed data blocks and
> may eventually be able to guess the value of the private RSA key
> of the server.
> An attacker may use this implementation flaw to sniff the
> data going to this host and decrypt some parts of it, as well
> as impersonate your server and perform man in the middle attacks.
> *** Nessus solely relied on the banner of the remote host
> *** to issue this warning
> See also: http://www.openssl.org/news/secadv_20030219.txt
> http://lasecwww.epfl.ch/memo_ssl.shtml
> http://eprint.iacr.org/2003/052/
> Solution: Upgrade to version 0.9.6j (0.9.7b) or newer
This vulnerability will allow a remote attacker to decrypt the https session. If sensitive data is being passed it is HIGHLY recommended to update this application.

2.5 Administrative Practices

The administrative practices are well documented. A living set of documents reside in /dfs/sysadmin/doc/Sun. The documents cover the creation and deletion of accounts. The procedures needed for installing from scratch and a host of others applications. This is a list of the files in that directory.

Auburn.A1000.Howto backup_info realplayer_g2_setup sunstore
CA_info disable_ip_forwarding serial_and_parallel_printers telalert
Dynamic_reconfig local_changes_7 solaris7_media ultra5_info
RCS local_changes_8
SunSolve_Acct local_changes_8
Sun_PC_Keyboard_Interchange locations_and_serials
Sun_PC_Keyboard_Interchange lpl.patch.server
TT_DB_fixup.ps monitors using_apache_for_answerbook x86_info
Unique_Mac_address paging_performance
User_Accounts patch_error_codes
adding_a_new_window_manager pgx64_pci

Backup procedures are also well documented however we will talk more about those later.

2.6 Identification and Protection of Sensitive Data on the Host

2.6.1 Sensitive Files

COPS
COPS is a 16 bit checksum tool that has been modified by the admin to include MD5 checksum abilities. This tool maintains a md5 checksum file of the system files on BigDog and also checks the permission files in /dev to establish whether these files are world writable (a classic intrusion sign). COPS is run nightly out of cron.

Cron File Checker
This is a piece of code in /usr/local/sbin/actions which executes on multiple systems, each of which checks all the others hourly to make sure a file that should be created every hour is in fact created as it should be.

Sysfile_watch
This is a perl script that runs 4 times/day (midnight,6am,noon,6pm) which checks selected system text files for changes and mails those differences. It was originally designed to catch things like a Cisco install creating a username or a
group, so we didn’t lose that when BigDog pushed the "standard" copy of the file onto the other system. It has been expanded to watch other files, and be more of a general audit tool.

**Daemon watch**
This checks to make sure only one copy of inetd is running, restarts certain critical daemons if they are missing (sendmail, ssh, apache...).

**Findit (Cron)**
This tool does a find for world write, suid, and .rhosts files and saves the modify time. It then compares the modify times to the previous run of the tool and reports back (through email) any changed or new files.
Findit is a home grown utility based on the tool FINDIT written by Andrey Yeatts Cliff Hathaway added .rhosts support in mid 1990, and our administrator has maintained since.

### 2.6.2 Core Files

```bash
-------begin ../logs/modules/disable-core-sol8.sh.V.rpt-------
  per-process core dumps: enabled
One or more core dumps permitted - FAILS CHECK
This is a useful user and sysadmin diagnostic tool.
```

### 2.6.3 System Logging

Several home grown scripts generate email or page the administrator when a threshold of tolerance is breached. BigDog is also acting as a syslog server for other hosts. This is another reason to move BigDog behind a firewall and lock it down a bit tighter.

### 2.7 Protection of Sensitive Data in Transit Over the Network or Internet

No encryption of the data at rest has been instituted
Beyond SSH no encryption of data in transit has been implemented

### 2.8 Access Controls

#### 2.8.1 Password Policy

**password configuration**
The current password policy would be considered weak by any standard. Below is the current policy.

```bash
> cat /etc/default/passwd
#ident "(@(#)passwd.dfl 1.3 92/07/14 SMI"
```
MAXWEEKS=
MINWEEKS=
PASSLENGTH=6

According to the Titan Security Tool this does not pass very many parameters.

-------begin ../logs/modules/defpwparams.sh.V.rpt-------
paswd MINWEEKS - FAILS CHECK
paswd MAXWEEKS - FAILS CHECK
paswd WARNWEEKS - FAILS CHECK
paswd PASSLENGTH - PASSES CHECK
       -------end ../logs/modules/defpwparams.sh.V.rpt-------

The administrator is reluctant to change the password policy with out direction from management. He feels that the users would find changes in the password policy to be less than agreeable. However, the admin does run a passwdchk tool nightly. This tool checks for easily guessable passwords and does a limited dictionary attack. In the even that a password appears that is easily guessable the admin is sent an email with the username. The password it’s self is not sent to the admin. The admin then contacts the users and asks then to choose a stronger password. This practice by the admin helps to secure the passwords of the users however it would save time as well as work to simply implant a stronger policy for passwords. This decision will need to back and enforced by management in this particular environment.

2.8.2 Control of the Root Account and Administrator Access

Several people have the root password. Due to the inability of a user to connect as root they will need to connect as their user and su to root. This makes attributing changes to individuals possible. The many scripts that run also look for changes in system files and email the systems group when selected files are changed. This allows for the quick recognition and correction of configuration errors.

We are recommending that the root password be changed and that system administrative functions be regulated to those responsible for those duties. Arm Chair admins are never a good idea. To provide functionality to those users that require root type privileges we are suggesting that the tools sudo be more widely used. The tool is currently installed but not being used on this server.

2.8.3 Security Auditing

According to the Titan Security Tool auditing is not enabled. However the admin of the system does not feel that this level of auditing is useful in our environment.
We recommend leaving this option disabled until such a time that more resources are made available to the administrator. His current work load will not allow him to monitor logs at this level.

This can be enabled by editing:
/etc/security/audit_control.

This is the Titan output for this check.
-----begin ../logs/modules/bsm.sh.V.rpt------
auditing not configured - FAILS CHECK

2.9 Backup Policies & Disaster Preparedness

Below is the current back up procedure.

“The backup groups are defined in /usr/local/etc/ghosts. The /usr/local/sbin/do_backup script uses that information to spread the load across the two DLT drives in the Sun L-1800 library on BigDog used for backups.

On Monday, the level 0 backups written over the weekend and identified in the "Disaster Recovery" Email are removed from the respective libraries and dropped off at the CCIT Operations I/O window. The previous week's tapes are retrieved on Tuesday so there is one set off site at all times. There is a Solaris 8 2/02 media kit stored at the offsite location

Each tape is assigned a unique barcode. Tapes DJB-484, 485 and 486 round-robin in the slot labeled "1" on the magazine in the L-280. DJB-487, 488, 489, 490, and 491 are permanently assigned to magazine slots 2-6, and 492 is in the fixed slot deep inside the L-280. All other tapes have fixed slot assignments in the L-1800, with tape DJB-396 being in slot 1 DJB-391 in slot2,... up thru DJB-442 in slot 47." (taken from Backup Documentation by the admin)

The backup procedures are adequate and well designed. Improvements could be made by implanting separate back up servers in both local and off site locations that contained the same data. With the advent of Storage Area Networking and the increased bandwidth available to a University environment it becomes much easier to construct this kind of backup procedure both securely and efficiently.

2.10 Analysis of System Defenses

2.10.1 Access-lists and Network Architecture

An analysis of the access-list for this network begs for a complete redesign of the network architecture. Little protection is being provided by this access-list. The permit established line at the top only requires an attacker to set the ACK flag in a tcp packet to be able to subvert this line. The "permit tcp any
any established” ACL needs to be replaced with a firewall or some other stateful filter. The machines running on this network need to be separated into services and placed on different networks. Because the network in question is an entire class C subletting and firewalls that support routing (such as PIX 535) could be used to separate machine. The DNS servers could be moved to outside the Firewall as the primary DNS machines a VMS and the administrator for those machines does not like to filter ANY connection coming to the machines.

The 2 “other” networks that are on the routed interface would not be a problem if we as long as we put their traffic to a different switch port and ran everything for our networks into the firewalls. Using the firewalls for routing OR using the firewalls to separate the traffic into VLANS and using a switch router to separate the traffic 1 hop in from the firewalls. Separating the traffic into Vlans would be considered my many to be less secure but for this situation may allow greater flexibility in the interoperability of the networked machines.

Non Exec Stack configuration takes care of a great many of the script kiddie attacks on a system. Having this configured is extremely important.

NFS connects from ports under1024 is not as secure as it used to be. Now that just about every attack out their runs from an attacker with root privileges restricting access to privileged ports provides little added security. However, it does have the advantage of stopping the attackers with little to no understanding of the systems they are attacking.

3.0 Critical Issues and Recommendations

3.1 Top Ten Recommendations

3.1.1 Infrastructure Redesign

This is our most important recommendation. It also happens to be the most expensive and hardest to implement. The current infrastructure is not designed with security in mind. Users and Servers should be placed behind a stateful firewall that can monitor access and drop packets. Services that are offered to the world should be removed from the internal network and moved to a service network. Network management applications that need to run should not run clear text over world routable address space. A network management network is suggested to help maintain a higher level of security and access control.

3.1.2 Remove World Accessible services

A department web server does not need to be world accessible. If employees need to connect from home they can connect via a VPN or other authenticated server. If there is a business need to have world accessible servers such as a web server then those services should be moved to a separate network and placed on a service network behind the firewall discussed above. It is a basic
security practice to NOT offered services to world if you can help it. Obviously, their will need to be some services, such as HTTP, that will need to be offered.

3.1.3 Separate and define server roles

In today’s ever decreasing budgets managers are asking for consolidation of services and applications to few numbers of machines. This department is running under the same guise. Unfortunately, we dig ourselves into a hole with our systems and sacrifice security by have one machine run EVERYTHING. Recommend separating and defining the servers into roles.

- Syslog Server
- Applications server
  - MySql
  - Various Tools
- Mail Server
- Web Server
- SFTP Server
- Etc.

Because this is budget dependant the management and the administrator need to establish what the costs would be if there were an intrusion and assess the risks involved to adequately make this decision.

3.1.4 Strengthen Password Controls

Password guessing is an easy attack that has been around for decades. Strong passwords are an essential piece of security and often the 1st attack for an attacker. These are the recommendations;

- Max. Days Password is Valid = 182 days
- Min. Days Password Must be Used Before it is Changed = 1 day
- Min. Password Length = 8 characters
- No. of Previously Remembered Passwords = 5
- Minimum Uppercase Letters Required = 1
- Minimum Other Characters Required = 1
- Minimum Digits Required = 1
- Minimum Characters Not Present in Previous Password = 5

3.1.5 Remove Unnecessary Packages

Several packages are installed that are either not configured or not in use. Because this machine is the application depository for the entire machine on the cluster it is impossible to know what is really needed and what is not. An effort needs to be made to audit all of the systems in the cluster and come up with a list of packages that can be removed for all the systems.
3.1.6 Remove Unnecessary Services

Telnet……………. Replace with SSH
Rsh………………..Replace with SSH
Rlogin……………..Replace with SSH
Rexec……………..Comment out in inetd
Sendmail………….Replace with Cron job to flush Qued mail and relay mail to mail server
FTP………………..Replace with SCP or SFTP

3.1.7 Address Application and Patch level

There are several applications that need to be brought up to current patch level. This includes the operating system. While currently the threat to these services is minimized by the configuration it still leaves an attack avenue in the event a password is compromised. Install the recommended patch cluster as well as the security patches. And update these applications to version:

OpenSSH 3.6.1p2 or newer
OpenSSL 0.9.7b or newer
MySql 3.23.56 or newer (4.0 provides a great deal of feature enhancement)
Samba 2.2.8 or newer
PHP 4.3.2 or newer

3.1.8 Strengthen Boot Level Access Controls

BigDog currently sits in a locked room monitored by 24 hours a day by cameras. However, there is a long list of individuals that have access to that area leaving the systems open to an insider threat. Boot level restriction have the price of being annoying in a critically time sensitive environment. While BigDog is a critical server every machine is configured in such a manner that it could double for a downed machine quickly and with little effort. Meaning that the expense of Boot level security is minimized due to the nature of the clusters ability to take on the duties of another system leaving more time to rebuild in the event of catastrophic hardware failure. These changes are recommended

eeprom passwords on servers.
single-user mode password
disable <L1 -A>shutdown

3.1.9 Restrict administrative access

Only allow admins to make changes to the system configuration. Currently, individuals have access to make changes to system configurations that are not filling the role of a system administrator. This can create problems of accountability and duty overlap both of which to not lend them selves to a
productive environment. Users requiring root privileges should be limited to sudo access. The initial setup and maintenance of these environments can be expensive to and already over worked admin. This brings us to our next topic.

3.1.10 Increase administrative resources

Under current load the administrator can only find the time to administer patches to the machine every 6 months. Combined with application maintenance for a variety of vendor tools on a cluster of servers there is simply no way an administrator can accurately maintain the load sufficiently. The current administrator relies greatly on custom scripts and his well versed knowledge to carry the load. If the organization where to lose this administrator the system would fall into disarray fairly quickly. To combat this we suggest a “junior” administrator be brought in and trained by the administrator to learn the systems and help with the maintenance.

3.2 Further Recommendations Outside of the Top Ten Threats

A philosophy change needs to occur in the organization that has a great focus on security. As we have soon the systems are being held together by a competent and diligent admin. The administrator is willing to make any changes dictated to him by management however management needs to make the call. Written policies should have been implemented long ago and the only reason they did not make it into the TOP 10 is due to the inherent lack of management support for change. The administrator's work load will increase immensely in trying to implement these changes. However with defined roles and polices when the changes are complete the admin will find that his job will be easier.
References:


Peter H. Gregory Solaris Security Sun Microsystems Press


---. 6.5 UNIX Practicum. The SANS Institute, 2002.

The Center for Internet Security. 3 February 2003 <http://www.cisecurity.org/>

SunSolve <http://sunsolve.sun.com>

Entellus Technology Group Sun Solaris Audit Guide

Sun Microsystems, Solaris Patch Management Recommended Strategies (whitepaper)

**Lastly, a very special thanks to the Admin (who didn’t want his name mentioned) for all of his help and for letting me audit his system!**

Appendix A

```
> /usr/local/sbin/lsof
COMMAND     PID     USER   FD   TYPE        DEVICE   SIZE/OFF NODE NAME
rpcbind     150     root    6u  IPv4 0x3000216d5a8 0t0  TCP *:sunrpc (LISTEN)
rpcbind     150     root    7u  IPv4 0x30001bae060 0t0  TCP *:* (IDLE)
```
rpcbind 150 root 15u IPv4 0x30009b1d1d8 0:32 TCP BigDog.Dep.univ.EDU:sunrpc -> dep.univ128.20:1017
(ESTABLISHED)
rpcbind 150 root 16u IPv4 0x30009949b0 0:32 TCP BigDog.Dep.univ.EDU:sunrpc -> dep.univ128.20:711
(ESTABLISHED)
inetch 177 root 11u IPv4 0x3000216dde8 0:00 TCP *:ftp (LISTEN)
inetch 177 root 12u IPv4 0x3000216ca668 0:00 TCP *:telnet (LISTEN)
inetch 177 root 13u IPv4 0x3000216c568 0:00 TCP *:shell (LISTEN)
inetch 177 root 14u IPv4 0x3000216e2e8 0:00 TCP *:shell (LISTEN)
inetch 177 root 15u IPv4 0x3000216e668 0:00 TCP *:login (LISTEN)
inetch 177 root 16u IPv4 0x3000216c5d30 0:00 TCP *:exec (LISTEN)
inetch 177 root 17u IPv4 0x3000216c928 0:00 TCP *:exec (LISTEN)
inetch 177 root 20u IPv4 0x3000216c55b0 0:00 TCP *:finger (LISTEN)
inetch 177 root 21u IPv4 0x3000216c53b0 0:00 TCP *:time (LISTEN)
inetch 177 root 25u IPv4 0x3000216c420 0:00 TCP *:printer (LISTEN)
lockd 190 root 5u IPv4 0x30002811478 0:00 TCP *:lockd (LISTEN)
lockd 190 root 6u IPv4 0x30004d62538 0:00 TCP BigDog.Dep.univ.EDU:lockd -> robIn.Dep.univ.EDU:613
(ESTABLISHED)
statd 193 daemon 6u IPv4 0x300027c4570 0:00 TCP *:32771 (LISTEN)
statd 193 daemon 16u IPv4 0x30004d32f68 0:00 TCP BigDog.Dep.univ.EDU:32771->tcp02179639pcs.sabrna01.az.comcast.net:52933
(ESTABLISHED)
mysql 281 mysql 3u IPv4 0x300026e6300 0:00 TCP *:mysql (LISTEN)
smbd 283 root 9u IPv4 0x300031a7c08 0:00 TCP *:netbios-ssn (LISTEN)
dlogin 363 7u IPv4 0x300048c7d58 0:00 TCP *:32783 (LISTEN)
dlogin 363 9u IPv4 0x30004d330a8 0:00 TCP BigDog.Dep.univ.EDU:32783->tcp02179639pcs.sabrna01.az.comcast.net:52765
(ESTABLISHED)
sshd 375 root 3u IPv4 0x3000348ac50 0:00 TCP *:sshd (LISTEN)
mountd 423 root 8u IPv4 0x300048c7358 0:00 TCP *:32785 (LISTEN)
mountd 423 root 15u IPv4 0x300057ee940 0:00 TCP BigDog.Dep.univ.EDU:32785->tcp02179639pcs.sabrna01.az.comcast.net:52821
(ESTABLISHED)
mountd 423 root 16u IPv4 0x30004d75a0 0:00 TCP BigDog.Dep.univ.EDU:32785->tcp02179639pcs.sabrna01.az.comcast.net:52825
(ESTABLISHED)
netfs 425 root 5u IPv4 0x300048c7948 0:00 TCP *:netfs (LISTEN)
nfsd 425 root 6u IPv4 0x300049ca4a48 0:00 TCP BigDog.Dep.univ.EDU:nfsd -> tick.Dep.univ.EDU:933
(ESTABLISHED)
nfsd 425 root 7u IPv4 0x3000493f068 0:00 TCP BigDog.Dep.univ.EDU:nfsd -> quiver.Dep.univ.EDU:1023
(ESTABLISHED)
nfsd 425 root 8u IPv4 0x30004a5e60 0:00 TCP BigDog.Dep.univ.EDU:nfsd -> robIn.Dep.univ.EDU:614
(ESTABLISHED)
nfsd 425 root 9u IPv4 0x30004a11ac0 0:00 TCP BigDog.Dep.univ.EDU:nfsd -> batman.Dep.univ.EDU:760
(ESTABLISHED)
cflowd 447 getstats 5u IPv4 0x30004a10f8 0:00 TCP *:omnisky (LISTEN)
smbd 1038 root 12u IPv4 0x30004d8d978 0:20843 TCP www.dep.univ.EDU:netbios-ssn->tc128-164.dep.univ.EDU:1070
(ESTABLISHED)
smbd 2496 root 5u IPv4 0x30004d75a0 0:11421 TCP BigDog.Dep.univ.EDU:netbios-ssn->Broke.dep.univ.edu:1103
(ESTABLISHED)
sshd 2625 root 5u IPv4 0x30004a051c0 0:250882 TCP BigDog.Dep.univ.EDU:sshd -> sirt-dhcp-230.dep.univ.EDU:1074
(ESTABLISHED)
sshd 2634 gpoer 5u IPv4 0x30004a051c0 0:250882 TCP BigDog.Dep.univ.EDU:sshd -> sirt-dhcp-230.dep.univ.EDU:1074
(ESTABLISHED)
inetrOv 3751 root 5u IPv4 0x30004a051c0 0:14 TCP BigDog.Dep.univ.EDU:* -> dep.univ.EDU:* (IDLE)
inetrOv 3751 root 6u IPv4 0x30004a051c0 0:14 TCP BigDog.Dep.univ.EDU:* -> dep.univ.EDU:* (IDLE)
inetrOv 3751 root 7u IPv4 0x30004a051c0 0:14 TCP BigDog.Dep.univ.EDU:* -> dep.univ.EDU:* (IDLE)
inetrOv 3751 root 8u IPv4 0x30004a051c0 0:14 TCP BigDog.Dep.univ.EDU:* -> dep.univ.EDU:* (IDLE)
smbd 5009 root 5u IPv4 0x30004a051c0 0:1776 TCP BigDog.Dep.univ.EDU:netbios-ssn-> sirt-dhcp-239.dep.univ.EDU:1038
(ESTABLISHED)
smbd 5213 root 5u IPv4 0x30004a051c0 0:22627 TCP BigDog.Dep.univ.EDU:netbios-ssn->tc128-178.dep.univ.EDU:1092
(ESTABLISHED)
smbd 7148 root 12u IPv4 0x30004a051c0 0:2761 TCP BigDog.Dep.univ.EDU:netbios-ssn-> sirt-dhcp-242.dep.univ.EDU:2862
(ESTABLISHED)
smbd 7457 root 12u IPv4 0x30004a051c0 0:9494 TCP BigDog.Dep.univ.EDU:netbios-ssn->shovel.dep.univ.EDU:4670
(ESTABLISHED)
sshd 7915 root 5u IPv4 0x30004a051c0 0:2718916 TCP BigDog.Dep.univ.EDU:sshd -> mr-hat.dep.univ.EDU:11141
(ESTABLISHED)
sshd 7938 bhp 5u IPv4 0x30004a051c0 0:2718916 TCP BigDog.Dep.univ.EDU:sshd -> mr-hat.dep.univ.EDU:11141
(ESTABLISHED)
sshd 7938 bhp 10x IPv4 0x30004a051c0 0:00 TCP localhost:6010 (LISTEN)
sshd 7938 bhp 12x IPv4 0x30004a051c0 0:178180 TCP localhost:6010 -> localhost:52406 (ESTABLISHED)
titrax 10041 bhp 3u IPv4 0x30004a051c0 0:178180 TCP localhost:52406 -> localhost:6010 (ESTABLISHED)
mntDog 12532 root 12u IPv4 0x30004a051c0 0:1364 TCP BigDog.Dep.univ.EDU:netbios-ssn->tc128-173.dep.univ.EDU:2239
(ESTABLISHED)
permit ip host 209.147.190.126 host dep.univ128.46
permit ip host 209.147.191.62 host dep.univ128.46
permit ip 2dep.univ.248.0 0.0.0.255 host dep.univ128.46
permit ip 2dep.univ.42.0 0.0.0.255 host dep.univ128.46
permit ip host 209.147.190.126 host dep.univ128.46
permit ip host 209.147.191.62 host dep.univ128.46

Appendix B

# CAUTION: this access list must be uploaded to BOTH woody
# AND jessie, as this vlan appears on both for redundancy.
# no ip access-list extended vlan300-out
ip access-list extended vlan300-out
#
# # dep.univsubnet and others....
#
# # Allow reply packets - reflexive would be better, but
# # with non-telcom nets on this vlan, its just plain too hairy
# # for me - Ric 4/5/2002.
permit tcp any any established
#
# # permit co-lo nets
# permit ip any dep.univ69.0.0.0.255
# permit ip any dep.univ13.16.0.0.7
# permit ip dep.univ128.0.0.0.255 dep.univ.128.0.0.0.255
# # Prevent unexpected access to network management server - it has
# # lots of open ports, and, worse, OV procs running as "bin".
# allow telcom equipment subnets.,
# permit ip dep.univ0.0.0.255.255 host dep.univ128.46
# permit ip 1dep.univ.0.0.0.255.255 host dep.univ128.46
# permit ip dep.univ.0.0.0.255.255 host dep.univ128.46
# permit ip 172.17.0.0.0.0.0.255.255 host dep.univ128.46
# permit ip 172.18.0.0.0.0.0.0.255.255 host dep.univ128.46
# permit ip 192.12.69.0.0.0.0.0.255.255 host dep.univ128.46
# permit ip 192.80.43.0.0.0.0.0.255.255 host dep.univ128.46
# permit ip 199.104.147.0.0.0.0.0.255.255 host dep.univ128.46
# permit ip 199.104.246.0.0.0.0.0.255.255 host dep.univ128.46
# permit ip 199.104.254.0.0.0.0.0.255.255 host dep.univ128.46
# permit ip 206.206.223.0.0.0.0.0.255.255 host dep.univ128.46
# permit ip 2dep.univ.42.0.0.0.0.0.0.0.255.255 host dep.univ128.46
# permit ip 2dep.univ.248.0.0.0.0.0.0.0.255.255 host dep.univ128.46
# permit ip host 209.147.190.126 host dep.univ128.46
# permit ip host 209.147.191.62 host dep.univ128.46

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.
# allow ssh
permit tcp any host dep.univ128.46 eq 22
#
# allow mail
permit tcp any host dep.univ128.46 eq smtp
#
# allow tacacs
permit tcp any host dep.univ128.46 eq tacacs
permit udp any host dep.univ128.46 eq tacacs
#
# Allow dns
permit tcp any eq domain host dep.univ128.46
permit udp any eq domain host dep.univ128.46
#
# allow syslog
permit udp any host dep.univ128.46 eq syslog
#
# allow snmp
permit udp any eq snmp host dep.univ128.46
permit any host dep.univ128.46 eq smntrap
#
# allow tftp
permit udp any host dep.univ128.46 eq tftp
#
# allow pings and other such things.
permit icmp any host dep.univ128.46
#
# prevent unexpected access to Oracle server. Nothing outside
# the netops subnet or the sirt subnet should be trying to
# reach this system, except on specific ports.
permit ip dep.univ128.0 0.0.0.255 host dep.univ128.48
permit ip dep.univ128 0.0.0.127 host dep.univ128.48
#
# Allow dns
permit tcp any eq domain host dep.univ128.48
permit udp any eq domain host dep.univ128.48
#
# allow syslog
permit udp any host dep.univ128.48 eq syslog
#
# allow tacacs
permit tcp any host dep.univ128.48 eq tacacs
permit udp any host dep.univ128.48 eq tacacs
#
# allow pings and other such things.
permit icmp any host dep.univ128.48
#
# prevent unexpected access to web server ports.
# Temp Access for IDSbeta
permit tcp dep.univ128.0.0.0.127 host dep.univ128.44 eq 80
permit tcp dep.univ128.0.0.0.127 host dep.univ128.44 eq 443
# Allow web access to www.dep.univ.edu
permit tcp any host dep.univ128.49 eq 80
permit tcp any host dep.univ128.49 eq 443
# Allow web access to www.dep.univ.edu
permit tcp any host dep.univ128.38 eq 80
permit tcp any host dep.univ128.38 eq 443
# Allow web access to page.dep.univ.edu
permit tcp any host dep.univ128.28 eq 80
# Allow web access to maggie.dep.univ.edu
permit tcp any host dep.univ128.233 eq 80
# Allow web access to Hopey.dep.univ.edu
permit tcp any host dep.univ128.234 eq 80
# Allow web access to vms.dep.univ.edu
permit tcp any host dep.univ128.131 eq 80
# Allow web access to kuat-audio.dep.univ.edu
permit tcp any host dep.univ.128.56 eq 80
permit tcp any host dep.univ.128.56 eq 8080
# allow web access to scanner1.dep.univ.edu
permit tcp any host dep.univ.130 eq 80
#
# Block the rest of common web stuff.
deny tcp any any eq 80
deny tcp any any eq 443
deny tcp any any eq 8080
#
# Prevent unexpected access to rpc port.
permit tcp host dep.univ.11.233 any eq sunrpc
permit tcp host dep.univ.11.234 any eq sunrpc
permit tcp host dep.univ.11.235 any eq sunrpc
permit tcp host dep.univ.138 any eq sunrpc
permit tcp host dep.univ.144 any eq sunrpc
permit tcp host dep.univ.152 any eq sunrpc
permit tcp host dep.univ.252.8 any eq sunrpc
permit tcp host dep.univ.252.47 any eq sunrpc
permit tcp host dep.univ.252.252 any eq sunrpc
permit tcp host dep.univ.100.34 any eq sunrpc
permit tcp host dep.univ.128.200 any eq sunrpc
permit tcp host 2dep.univ.248.30 any eq sunrpc
deny tcp any any eq sunrpc
permit udp host dep.univ.11.233 any eq sunrpc
permit udp host dep.univ.11.234 any eq sunrpc
permit udp host dep.univ.11.235 any eq sunrpc
permit udp host dep.univ.138 any eq sunrpc
permit udp host dep.univ.144 any eq sunrpc
permit udp host dep.univ.152 any eq sunrpc
permit udp host dep.univ.252.8 any eq sunrpc
permit udp host dep.univ.252.47 any eq sunrpc
permit udp host dep.univ.252.252 any eq sunrpc
permit udp host 1dep.univ.100.34 any eq sunrpc
permit udp host dep.univ.128.200 any eq sunrpc
permit udp host 2dep.univ.248.30 any eq sunrpc
deny udp any any eq sunrpc
#
# Prevent unexpected access to NFS well known port.
permit tcp host dep.univ.11.233 any eq 2049
permit tcp host dep.univ.11.234 any eq 2049
permit tcp host dep.univ.11.235 any eq 2049
permit tcp host dep.univ.138 any eq 2049
permit tcp host dep.univ.144 any eq 2049
permit tcp host dep.univ.152 any eq 2049
permit tcp host dep.univ.252.8 any eq 2049
permit tcp host dep.univ.252.47 any eq 2049
permit tcp host dep.univ.252.252 any eq 2049
permit tcp host 1dep.univ.100.34 any eq 2049
permit tcp host dep.univ.128.200 any eq 2049
permit tcp host 2dep.univ.248.30 any eq 2049
deny tcp any any eq 2049 log
permit udp host dep.univ.11.233 any eq 2049
permit udp host dep.univ.11.234 any eq 2049
permit udp host dep.univ.11.235 any eq 2049
permit udp host dep.univ.138 any eq 2049
permit udp host dep.univ.144 any eq 2049
permit udp host dep.univ.152 any eq 2049
permit udp host dep.univ.252.8 any eq 2049
permit udp host dep.univ.252.47 any eq 2049
permit udp host dep.univ.252.252 any eq 2049
permit udp host 1dep.univ.100.34 any eq 2049
permit udp host dep.univ.128.200 any eq 2049
permit udp host 2dep.univ.248.30 any eq 2049
deny udp any any eq 2049 log
#
# Prevent unexpected access to font server well known port.
permit tcp host dep.univ.11.233 any eq 7100
permit tcp host dep.univ.11.234 any eq 7100
permit tcp host dep.univ11.235 any eq 7100
permit tcp host dep.univ.138 any eq 7100
permit tcp host dep.univ.144 any eq 7100
permit tcp host dep.univ.152 any eq 7100
permit tcp host dep.univ.252.8 any eq 7100
permit tcp host dep.univ.252.47 any eq 7100
permit tcp host dep.univ.252.252 any eq 7100
deny tcp any any eq 7100 log
#
# Prevent unexpected access to oracle listener.
deny tcp any any eq 1521
#
# Prevent access to steel belted radius admin port
deny tcp any any eq 1646
#
# Prevent access to APC PowerChute (APC UPS software) ports.
deny tcp any any eq 5454
deny udp any any eq 5454
deny tcp any any eq 5455
deny udp any any eq 5455
deny tcp any any eq 5456
deny udp any any eq 5456
#
# Following is powerchute for windows...
deny tcp any any eq 6666
deny udp any any eq 6666
#
# permit ted X11 access from home
# tsf, Fri May 25 10:17:12 MST 2001
permit tcp 2dep.univ.248.176 0.0.0.15 any eq 6000
#
# permit wimmer X11 access from home
# ric, Fri May 25 10:17:12 MST 2001
permit tcp 1dep.univ.100.32 0.0.0.15 any eq 6000
#
# SIRT systems.
permit tcp dep.univ.128 0.0.0.127 any eq 6000
#
# Prevent unexpected X11 access
deny tcp any any eq 6000
#
# ric, Wed May 10 15:20:18 MST 2000 stop snmp traps to wrong machines.
deny udp any any eq snmptrap log
#
# Deny bozo with misconfigured NTP server
# 9-sep-2002 chd
deny ip host 207.236.117.254 host dep.univ.128.234
#
permit udp 224.0.0.0 15.255.255.255 any
permit pim any any
permit ip any any
end

Appendix C

> more /etc/hosts.allow
/with/hosts/allow: No such file or directory
> more /private/with/hosts/allow
/private/with/host/allow: No such file or directory
> more /private/with/host/allow
/private/with/host/allow: No such file or directory
> more /private/with/host/allow
# hosts/allow for daemons front-ended by the tcp wrapper
# "/usr/local/sbin/tcpd" in inetd.conf. See hosts_access(5) for
# more info on this file.
#
# This is mastered from /dfs/src/etc/wrappers/allow.master. Edit
# there, then "make install".
#
# $Id: allow.master,v 1.177 2003/05/28 22:10:36 root Exp $
# Allow local users
ALL: .dep.univ.edu .Dep.univ.EDU .duna.Dep.univ.edu 
    .VPN.Dep.univ.edu localhost
# list Dep.univ.edu machines we control.
    page.Dep.univ.edu vms.Dep.univ.edu
# Employee home net
ALL: xxx.xx.xxx.
# Tom home net
ALL: xxx.xx.xxx..176/255.255.255.240
# Steve home net
ALL: xxx.xx.xxx.144/255.255.255.240
# Bob home net
ALL: xxx.xx.xxx.208/255.255.255.240
# John home net
ALL: iteratorx.sycraft.net hitmark.sycraft.net
# Webserver for gigapop - it has to be able to run ufsdump to BigDog's
# tape drive.
in.rshd: webserver xxx.xx.xxx.
#
# Test lab network, lower half.
ALL: dep.univ129.0/255.255.255.128
#
# Allow ssh from anywhere, but make noise about external connections.
sshd: ALL : spawn /usr/bin/mailx
    -s "%H:%d connect from %h [%a] user %u"
    staff</dev/null> /dev/null 2>&1
# rpcbind (portmap on linux) needs some extra goodies...
# dns3.Dep.univ.edu
rpcbind: dep.univ11.233
# dns4.Dep.univ.edu
rpcbind: dep.univ11.234
# dns5.Dep.univ.edu
rpcbind: dep.univ11.235
# tick.Dep.univ.EDU
rpcbind: dep.univ128.4
# hobbes.Dep.univ.EDU
rpcbind: dep.univ128.12
# quiver.Dep.univ.EDU
rpcbind: dep.univ128.13
# page.Dep.univ.EDU
rpcbind: dep.univ128.26
# batman.Dep.univ.EDU
rpcbind: dep.univ128.46
# booboo.dep.univ.EDU
rpcbind: dep.univ128.47
# robin.Dep.univ.EDU
rpcbind: dep.univ128.48
# BigDog.Dep.univ.EDU
rpcbind: dep.univ128.49
# calvin.Dep.univ.EDU
rpcbind: dep.univ128.54
# megatron.Dep.univ.EDU
rpcbind: dep.univ128.80
# nermal.Dep.univ.EDU
rpcbind: dep.univ128.91
# wily.Dep.univ.EDU
rpcbind: dep.univ128.238
# littledog.dep.univ.EDU
rpcbind: dep.univ138
# opus.dep.univ.EDU
rpcbind: dep.univ.144
# backsrv2.dep.univ.EDU
rpcbind: dep.univ.152
# garfield.Dep.univ.EDU
rpcbind: dep.univ.252
# yogi.dep.univ.EDU
rpcbind: dep.univ.252.47
# odie.Dep.univ.EDU
appendix d

list of setuid/setgid files from oldsuid:
ctime: sep 21 05:54 2002 -r-x---r-x 1 lp lp 203 dec 16 15:21 1999 /etc/lp/alerts/printer
ctime: feb 24 09:27 2003 -rxr-r-x 1 root siteadm 1590 nov 5 12:37 2000
/export/bigdog/clusmgt/src/xautolock-pl15/rcs/makefile,v
/export/bigdog/clusmgt/src/xautolock-pl15/contrib/idlefile.tgz
ctime: feb 24 09:27 2003 -rwxrwxr-x 1 root root 507904 sep 22 09:01 1997
/export/bigdog/u1/nms/sun4/snm/bin/snm_discover.2.2.1
ctime: sep 28 06:44 2002 -rwxr-x-x 1 sas sasgrp 756792 aug 13 14:03 1998
/opt/sas/sa60/bin/saserv_ora
ctime: sep 28 06:44 2002 -rw-r-xr-x 1 sas sasgrp 824888 aug 13 14:03 1998
/opt/sas/sa60/bin/saserv_odbc
ctime: sep 28 06:44 2002 -rwxr-xr-x 1 sas sasgrp 2537420 aug 13 14:03 1998
/opt/sas/sa60/bin/saserv_oracle
ctime: sep 28 06:44 2002 -rwxr-xr-x 1 sas sasgrp 507904 aug 13 14:03 1998
/opt/sas/sa60/bin/saserv_pg
ctime: mar 10 07:03 2003 -rwxrwxr-x 1 root siteadm 342148 nov 1 07:03 2001 /usr/bin/admintool
ctime: sep 21 08:25 2002 -rwxr-xr-x 1 root root 81920 aug 22 09:01 1997
/etc/passwd
ctime: sep 21 08:25 2002 -rwxr-xr-x 1 root root 507904 aug 22 09:01 1997
/export/bigdog/clusmgt/src/xautolock-pl15/contrib/README
ctime: sep 28 07:46 2002 -rwxr-xr-x 1 root root 29320 dec 7 01:09 1998
/export/bigdog/u1/3com/3com/scp/bin/ntping
ctime: sep 21 05:48 2002 -rwxr-xr-x 1 root sys 342148 nov 1 07:03 2001 /usr/bin/admintool
ctime: sep 21 08:25 2002 -rwxr-xr-x 1 root sys 37784 aug 27 15:03 2002 /usr/bin/at
ctime: sep 21 08:25 2002 -rwxr-xr-x 1 root sys 13732 aug 27 15:03 2002 /usr/bin/atq
ctime: sep 21 08:25 2002 -rwxr-xr-x 1 root sys 12692 aug 27 15:03 2002 /usr/bin/atrm

rpcbind: dep.univ252.252
# woodstock.dep.univ.edu (wimmer's home machine)
rpcbind: fdep.univ.100.34
# batman.Dep.univ.EDU - New Address
rpcbind: dep.univ.128.46
# robin.Dep.univ.EDU - New Address
rpcbind: dep.univ.128.48
# broadcasts (all ones and all zeros).
rpcbind: 255.255.255.255 0.0.0.0

# end of tcpd hosts.allow.
> more /private/etc/hosts.deny
# hosts.deny for daemons front-ended by the tcp wrapper
# "/usr/local/sbin/tcpd" in inetd.conf. See hosts_access(5) for
# more info on this file.
#
# This is mastered from /dfs/src/etc/wrappers/deny.master. Edit
# there, then "make install".
#
# $Id: deny.master,v 1.16 2003/05/23 17:43:32 root Exp $
#
# Cannot twist rpcbind (portmap on linux) as it is a resident process;
# don't bother with %h since rpcbind/portmap never prints anything but
# addresses anyway.
rpcbind: ALL : spawn /usr/bin/mailx
       "%H
       %d attempt from %a user %u"
       staff <dev/null >dev/null 2>&1

# Don't allow anything in by default.
ALL: ALL : twist /usr/bin/mailx
       "%H
       %d attempt from %h %a user %u"
       staff <dev/null >dev/null 2>&1

# end of tcpd hosts.deny.
Appendix E

------begin ../logs/modules/add-umask.sh.V.rpt------
No umask file /etc/init.d/umask.sh found - FAILS CHECK
------end ../logs/modules/add-umask.sh.V.rpt------

------begin ../logs/modules/adjust-arp-timers2.8.sh.V.rpt------
ARP timers are not set - FAILS CHECK
------end ../logs/modules/adjust-arp-timers2.8.sh.V.rpt------

------begin ../logs/modules/aset.sh.V.rpt------
ASET installed - PASSES CHECK
------end ../logs/modules/aset.sh.V.rpt------

------begin ../logs/modules/automount.sh.V.rpt------
Automounter = /usr/lib/autofs/automountd /usr/sbin/automount /usr/bin/pkill - FAILS CHECK
------end ../logs/modules/automount.sh.V.rpt------

------begin ../logs/modules/automount2.sh.V.rpt------
Automounter = /usr/lib/autofs/automountd /usr/sbin/automount /usr/bin/pkill - FAILS CHECK
------end ../logs/modules/automount2.sh.V.rpt------

------begin ../logs/modules/bsm.sh.V.rpt------
auditing not configured - FAILS CHECK
------end ../logs/modules/bsm.sh.V.rpt------

------begin ../logs/modules/cde.sh.V.rpt------
/usr/dt/config/Xaccess allows XDMCP login connections. - FAILS CHECK 1
/etc/dt/config allows XDMCP login connections. - FAILS CHECK 2
------end ../logs/modules/cde.sh.V.rpt------

------begin ../logs/modules/create-issu...e.sh.V.rpt------
Cannot read /etc/issue - FAILS CHECK
------end ../logs/modules/create-issu...e.sh.V.rpt------

------begin ../logs/modules/cronset.sh.V.rpt------
CRONLOG entry found - PASSES CHECK
/var/cron permissions - FAILS CHECK
/etc/cron.d/logchecke LIMIT - FAILS CHECK
------end ../logs/modules/cronset.sh.V.rpt------

------begin ../logs/modules/decode.sh.V.rpt------
No aliases use pipes - PASSES CHECK
------end ../logs/modules/decode.sh.V.rpt------

------begin ../logs/modules/defloginpara...sh.V.rpt------
login defaults CONSOLE - PASSES CHECK
login defaults UMASK - PASSES CHECK
login defaults SYSLOG - PASSES CHECK
login defaults TIME-OUT - FAILS CHECK
login defaults PASSREQ - PASSES CHECK
login defaults ALT-SHELL - PASSES CHECK
login defaults P.-T. - FAILS CHECK
login defaults SLEEP-TIME - FAILS CHECK
login defaults RETRIES - FAILS CHECK
login defaults SYSLOG_FAILED_LOGINS - PASSES CHECK

-------end ../logs/modules/defloginparams.sh.V.rpt-------

passwd MINWEEKS - FAILS CHECK
passwd MAXWEEKS - FAILS CHECK
passwd WARNWEEKS - FAILS CHECK
passwd PASSLENGTH - PASSES CHECK

-------end ../logs/modules/defpwparams.sh.V.rpt-------

begin ../logs/modules/disable-L1-A.sh.V.rpt
Abort sequence set to enable - FAILS CHECK

-------end ../logs/modules/disable-L1-A.sh.V.rpt-------

demon shell = /usr/local/sbin/nologin - FAILS CHECK
bin shell = /usr/local/sbin/nologin - FAILS CHECK
sys shell = /bin/sh - FAILS CHECK
adm shell = /usr/local/sbin/nologin - FAILS CHECK
ucp shell = /usr/local/sbin/nologin - FAILS CHECK
listen shell = /usr/local/sbin/nologin - FAILS CHECK
nobody shell = /usr/local/sbin/nologin - FAILS CHECK
noaccess shell = /usr/local/sbin/nologin - FAILS CHECK
nobody4 shell = /usr/local/sbin/nologin - FAILS CHECK

-------end ../logs/modules/disable-accounts.sh.V.rpt-------

afbinit daemon Service is disabled from starting - PASSES CHECK

-------end ../logs/modules/disable-afbinit.sh.V.rpt-------

Cache Filesystem Service is enabled in /etc/rc2.d/S73cachefs.daemon - FAILS CHECK
Cache Filesystem Service is enabled in /etc/rc2.d/S93cacheos.finish - FAILS CHECK

-------end ../logs/modules/disable-cachefs.sh.V.rpt-------

flashprom daemon Service is disabled from starting - PASSES CHECK

-------end ../logs/modules/disable-flaspm.sh.V.rpt-------

afbinit daemon Service is disabled from starting - PASSES CHECK

-------end ../logs/modules/disable-afbinit.sh.V.rpt-------
llc2 Service is enabled in /etc/rc2.d/S40llc2 - FAILS CHECK

Ncad daemon Service is enabled in /etc/rc2.d/S95ncad - FAILS CHECK

ncalogd daemon Service is enabled in /etc/rc2.d/S94ncalogd - FAILS CHECK

Ping echo response allowed - FAILS CHECK

PPP daemon Service is disabled from starting - PASSES CHECK

Service S73nfs.client still active in /etc/rc2.d - FAILS CHECK
Service S74autofs still active in /etc/rc2.d - FAILS CHECK
Service S80lp still active in /etc/rc2.d - FAILS CHECK
Service S71rpc still active in /etc/rc2.d - FAILS CHECK
Service S99dlogin still active in /etc/rc2.d - FAILS CHECK
Service S15nfs.server still active in /etc/rc3.d - FAILS CHECK
Service S76snmpdx disabled - PASSES CHECK

System set to not forward source routed packets - PASSES CHECK
System does not forward directed broadcast packets - PASSES CHECK
System is not set to ignore redirected packets - FAILS CHECK
System configured as 'notrouter' - PASSES CHECK

Found 15908 files in /usr that should be root owned - FAILS CHECK
Found 0 files in /sbin that should be root owned - PASSES CHECK
Found 0 files in /usr that should be set group g-w - PASSES CHECK
Found 0 files in /opt that should be set group g-w - PASSES CHECK

-----begin ../logs/modules/fix-cronpath.sh.V.rpt-------
Appendix F

Nessus Scan Report

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

Scan Details

- Number of security holes found: 7
- Number of security warnings found: 25

Host List

- BigDog.dep.univ.edu: Security hole(s) found

Analysis of Host

<table>
<thead>
<tr>
<th>Address of Host</th>
<th>Port/Service</th>
<th>Issue regarding Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>ftp (21/tcp)</td>
<td>Security hole found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>ssh (22/tcp)</td>
<td>Security warning(s) found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>telnet (23/tcp)</td>
<td>Security hole found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>smtp (25/tcp)</td>
<td>Security notes found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>time (37/tcp)</td>
<td>Security notes found</td>
</tr>
<tr>
<td>Host</td>
<td>Service</td>
<td>Action</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>finger (79/tcp)</td>
<td>Security warning(s) found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>http (80/tcp)</td>
<td>Security warning(s) found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>sunrpc (111/tcp)</td>
<td>Security warning(s) found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>netbios-ssn (139/tcp)</td>
<td>Security hole found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>https (443/tcp)</td>
<td>Security warning(s) found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>exec (512/tcp)</td>
<td>Security warning(s) found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>login (513/tcp)</td>
<td>Security warning(s) found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>shell (514/tcp)</td>
<td>Security warning(s) found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>printer (515/tcp)</td>
<td>Security notes found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>nfs (2049/tcp)</td>
<td>Security warning(s) found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>unknown (2056/tcp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>mysql (3306/tcp)</td>
<td>Security hole found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>lockd (4045/tcp)</td>
<td>Security warning(s) found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>sometimes-rpc (32771/tcp)</td>
<td>Security warning(s) found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>unknown (49680/tcp)</td>
<td>Security warning(s) found</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>time (37/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>srnpc (111/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>ntp (123/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>netbios-ns (137/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>netbios-dgm (138/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>xdmcp (177/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>biff (512/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>syslog (514/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>talk (517/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>unknown (978/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>unknown (1002/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>unknown (1003/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>unknown (1004/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>unknown (1005/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>unknown (1006/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>unknown (1007/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>ufsd (1008/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>unknown (1009/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>unknown (1010/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>unknown (1011/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>BigDog.dep.univ.edu</td>
<td>unknown (1018/udp)</td>
<td>No Information</td>
</tr>
<tr>
<td>Type</td>
<td>Port</td>
<td>Issue and Fix</td>
</tr>
<tr>
<td>----------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>ftp (21/tcp)</td>
<td>You seem to be running an FTP server which is vulnerable to the 'glob heap corruption' flaw. An attacker may use this problem to execute arbitrary commands on this host. <em><strong>Nessus relied solely on the banner of the server to issue this warning,</strong></em> so this alert might be a false positive.</td>
</tr>
<tr>
<td>Information</td>
<td>ftp (21/tcp)</td>
<td>An FTP server is running on this port. Nessus ID: 10330. If your FTP client crashes or hangs shortly after login, try using a 220- dash (-) as the first character of your password. This will turn off</td>
</tr>
</tbody>
</table>
220-
220- Anonymous access is not allowed.
220-

Nessus ID : 10092

Warning  ssh (22/tcp)  You are running OpenSSH-portable 3.6.1p1 or older.

If PAM support is enabled, an attacker may use a flaw in this version to determine the existence or a given login name by comparing the times the remote sshd daemon takes to refuse a bad password for a non-existant login compared to the time it takes to refuse a bad password for an existant login.

An attacker may use this flaw to set up a brute force attack against the remote host.

*** Nessus did not check whether the remote SSH daemon is actually using PAM or not, so this might be a false positive

Solution : Upgrade to OpenSSH-portable 3.6.1p2 or newer
Risk Factor : Low
CVE : CAN-2003-0190
Nessus ID : 11574

Informational  ssh (22/tcp)  An ssh server is running on this port
Nessus ID : 10330

Informational  ssh (22/tcp)  Remote SSH version : SSH-2.0-OpenSSH_3.5p1
Nessus ID : 10267

Informational  ssh (22/tcp)  The remote SSH daemon supports the following versions of the SSH protocol :
  . 1.99
  . 2.0

Nessus ID : 10881

Vulnerability  telnet (23/tcp)  The Telnet server does not return an expected number of replies when it receives a long sequence of 'Are You There' commands. This probably means it overflows one of its internal buffers and crashes. It is likely an attacker could abuse this bug to gain control over the remote host's superuser.

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

Solution: Comment out the 'telnet' line in /etc/inetd.conf.
Risk factor : High
CVE : CVE-2001-0554
BID : 3064, 4061
Nessus ID : 10709

Warning  telnet (23/tcp)  The Telnet service is running.
This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the telnet client and the telnet server. This includes logins and passwords.

You should disable this service and use OpenSSH instead. (www.openssh.com)
Solution: Comment out the 'telnet' line in /etc/inetd.conf.

Risk factor: Low
CVE: CAN-1999-0619
Nessus ID: 10280

Informational telnet
(23/tcp)
A telnet server seems to be running on this port
Nessus ID: 10330

Informational telnet
(23/tcp)
Remote telnet banner:
Nessus ID: 10281

Informational smtp
(25/tcp)
An SMTP server is running on this port
Here is its banner:
Nessus ID: 10330

Informational smtp
(25/tcp)
Remote SMTP server banner:
Nessus ID: 10330

This is probably: Sendmail version 8.12.9
Nessus ID: 10263

Informational smtp
(25/tcp)
This server could be fingerprinted as being Sendmail 8.12.2-8.12.5
Nessus ID: 11421

Informational smtp
(25/tcp)
For some reason, we could not send the EICAR test string to this MTA
Nessus ID: 11034

Informational smtp
(25/tcp)
For some reason, we could not send the 42.zip file to this MTA
BID: 3027
Nessus ID: 11036

Informational time
(37/tcp)
A time server seems to be running on this port
Nessus ID: 10330

Warning finger
(79/tcp)
The remote finger daemon accepts to redirect requests. That is, users can perform requests like:
finger user@host@victim

This allows an attacker to use your computer as a relay to gather information on another network, making the other network think you are making the requests.

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

Risk factor: Low
CVE: CAN-1999-0105
Nessus ID: 10073

Informational finger
(79/tcp)
An unknown service is running on this port.
It is usually reserved for Finger
Nessus ID: 10330

Informational finger
(79/tcp)
An unknown service runs on this port.
It is sometimes opened by this/these Trojan horse(s):
CDK
Firehotcker

Here is the service banner:
Login name: get In real life: ???
Unless you know for sure what is behind it, you'd better check your system.

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

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

### Informational

**finger**

(79/tcp)

An unknown server is running on this port.
If you know what it is, please send this banner to the Nessus team:

00: 4c 6f 67 69 6e 20 6e 61 6d 65 3a 20 67 65 74 20 Login name: get
10: 20 20 20 20 20 09 09 09 49 6e 20 72 65 61 6c ...In real
20: 20 6c 69 66 65 3a 20 3f 3f 3f 0d 0a life: ???.

Nessus ID : 11154

### Warning

http (80/tcp)

The remote host is running a version of PHP which is older than 4.3.2

There is a flaw in this version which may allow an attacker who has the ability to inject an arbitrary argument to the function socket_iovec_alloc() to crash the remote service and possibly to execute arbitrary code

For this attack to work, PHP has to be compiled with the option --enable-sockets (which is disabled by default), and an attacker needs to be able to pass arbitrary values to socket_iovec_alloc().

Other functions are vulnerable to such flaws : openlog(), socket_recvfrom(), and emalloc()

Solution : Upgrade to PHP 4.3.2
Risk factor : Low
CVE : CAN-2003-0172
BID : 7187, 7197, 7198, 7199, 7210, 7256, 7259
Nessus ID : 11468

### Warning

http (80/tcp)

The remote host is running a version of PHP earlier than 4.2.2.

The mail() function does not properly sanitize user input. This allows users to forge email to make it look like it is coming from a different source other than the server.

Users can exploit this even if SAFE_MODE is enabled.

Solution : Contact your vendor for the latest PHP release.

Risk factor : Medium
CVE : CAN-2002-0985
BID : 5562
Nessus ID : 11444

### Warning

http (80/tcp)

The remote host is using a version of OpenSSL which is older than 0.9.6j or 0.9.7b

This version is vulnerable to a timing based attack which may allow an attacker to guess the content of fixed data blocks and may eventually be able to guess the value of the private RSA key of the server.
An attacker may use this implementation flaw to sniff the data going to this host and decrypt some parts of it, as well as impersonate your server and perform man in the middle attacks.

*** Nessus solely relied on the banner of the remote host ***

to issue this warning

See also:  
http://www.openssl.org/news/secadv_20030219.txt  
http://lasecwww.epfl.ch/memo_ssl.shtml  
http://eprint.iacr.org/2003/052/  

Solution: Upgrade to version 0.9.6j (0.9.7b) or newer
Risk factor: Medium
CVE: CAN-2003-0078, CAN-2003-0131
BID: 6884, 7148
Nessus ID: 11267

Informational http (80/tcp) A web server is running on this port  
Nessus ID: 10330

Warning sunrpc (111/tcp)  
The RPC service rpcbind V2-4 is running on this port  
If you do not use it, disable it, as it is a potential security risk  
Nessus ID: 10336

Vulnerability netbios-ssn (139/tcp)  
. It was possible to log into the remote host using a NULL session.  
The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access  

To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and Q246261 (Windows 2000).  
Note that this won't completely disable null sessions, but will prevent them from connecting to IPC$  
Please see http://msgs.securepoint.com/cgi-bin/get/nessus-0204/50/1.html

. All the smb tests will be done as "/whatever"  
BID: 990
Nessus ID: 10394

Vulnerability netbios-ssn (139/tcp)  
The remote Samba server, according to its version number, has a bug in the length checking for encrypted password change requests from clients. A client could potentially send an encrypted password, which, when decrypted with the old hashed password could be used as a buffer overrun attack on the stack of smbd.

Solution: upgrade to Samba 2.2.7  
Risk factor: High  
Nessus ID: 11168

Vulnerability netbios-ssn (139/tcp)  
The following shares can be accessed using a NULL session:  
- IPC$ - (readable?, writeable?)  
- home - (readable, writeable)

Solution: To restrict their access under WindowsNT, open the explorer, do a right click on each, go to the 'sharing' tab, and click on 'permissions'  
Risk factor: High  
CVE: CAN-1999-0519, CAN-1999-0520  
Nessus ID: 10396

Vulnerability netbios-ssn (139/tcp)  
The remote Samba server, according to its version number, may be vulnerable to a remote buffer overflow when receiving
warning

specially crafted SMB fragment packets.

An attacker needs to be able to access at least one share to exploit this flaw.

Solution: upgrade to Samba 2.2.8
Risk factor: High
BID: 7106, 7107
Nessus ID: 11398

Warning netbios-ssn (139/tcp)

The remote registry can be accessed remotely using the login/password combination used for the SMB tests.

Having the registry accessible to the world is not a good thing as it gives extra knowledge to a hacker.

Solution: Apply service pack 3 if not done already, and set the key HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg to restrict what can be browsed by non administrators.

In addition to this, you should consider filtering incoming packets to this port.

Risk factor: Low
CVE: CAN-1999-0562
Nessus ID: 10400

Warning netbios-ssn (139/tcp)

The host SID can be obtained remotely. Its value is:

BIGDOG: 5-21-1408797127-1758474578--1254199900

An attacker can use it to obtain the list of the local users of this host
Solution: filter the ports 137 to 139 and 445
Risk factor: Low
CVE: CVE-2000-1200
BID: 959
Nessus ID: 10859

Warning netbios-ssn (139/tcp)

Here is the list of the SMB shares of this host:

- home
- visio
- IPC$
- ADMIN$

This is potentially dangerous as this may help the attack of a potential hacker.

Solution: filter incoming traffic to this port
Risk factor: Medium
Nessus ID: 10395

Warning netbios-ssn (139/tcp)

Here is the browse list of the remote host:

BIGDOG

This is potentially dangerous as this may help the attack of a potential hacker by giving him extra targets to check for
<table>
<thead>
<tr>
<th>Type</th>
<th>Port</th>
<th>Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning</td>
<td>139</td>
<td>A 'rfpoison' packet has been sent to the remote host. This packet is supposed</td>
<td>Filter incoming traffic to this port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>to crash the 'services.exe' process, rendering the system instable. If you</td>
<td>Risk factor: Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>see that this attack was successful, have a look at this page: <a href="http://www">http://www</a></td>
<td>Nessus ID: 10397</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wiretrip.net/rfp/p/doc.asp?id=23&amp;iface=2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CVE: CVE-1999-0980 BID: 754</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Nessus ID: 10204</td>
<td></td>
</tr>
<tr>
<td>Informational</td>
<td>139</td>
<td>The remote native lan manager is: Samba 2.2.5</td>
<td>Upgrade to PHP 4.3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The remote Operating System is: Unix</td>
<td>Risk factor: Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The remote SMB Domain Name is: TELCOM</td>
<td>Nessus ID: 10785</td>
</tr>
<tr>
<td>Warning</td>
<td>443</td>
<td>The remote host is running a version of PHP which is older than 4.3.2</td>
<td>Upgrade to PHP 4.3.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>There is a flaw in this version which may allow an attacker who has the</td>
<td>Risk factor: Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ability to inject an arbitrary argument to the function</td>
<td>Nessus ID: 11468</td>
</tr>
<tr>
<td></td>
<td></td>
<td>socket_iovec_alloc() to crash the remote service and possibly to execute</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>arbitrary code</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For this attack to work, PHP has to be compiled with the option --enable-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>sockets (which is disabled by default), and an attacker needs to be able</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>to pass arbitrary values to socket_iovec_alloc().</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other functions are vulnerable to such flaws: openlog(),</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>socket_recvfrom() and emalloc()</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Solution: Upgrade to PHP 4.3.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk factor: Low</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CVE: CAN-2003-0172 BID: 7187, 7197, 7198, 7199, 7210, 7256, 7259</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Nessus ID: 11448</td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>443</td>
<td>The remote host is running a version of PHP earlier than 4.2.2.</td>
<td>Contact your vendor for the latest PHP release.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The mail() function does not properly sanitize user input. This allows</td>
<td>Risk factor: Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>users to forge email to make it look like it is coming from a different</td>
<td>CVE: CAN-2002-0985</td>
</tr>
<tr>
<td></td>
<td></td>
<td>source other than the server. Users can exploit this even if SAFE_MODE is</td>
<td>BID: 5562</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enabled.</td>
<td>Nessus ID: 11444</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Solution: Contact your vendor for the latest PHP release.</td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>443</td>
<td>The SSLv2 server offers 5 strong ciphers, but also 0 medium strength and 2</td>
<td>Disable those ciphers and upgrade your client software if necessary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>weak &quot;export class&quot; ciphers. The weak/medium ciphers may be chosen by a</td>
<td>Risk factor: Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>export-grade or badly configured client software. They only offer a limited</td>
<td>CVE: CAN-2002-0985</td>
</tr>
<tr>
<td></td>
<td></td>
<td>protection against a brute force attack</td>
<td>BID: 5562</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Solution: disable those ciphers and upgrade your client software if</td>
<td>Nessus ID: 10863</td>
</tr>
<tr>
<td></td>
<td></td>
<td>necessary</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Protocol</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td>https</td>
<td>The remote host is using a version of OpenSSL which is older than 0.9.6j or 0.9.7b</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(443/tcp)</td>
<td>This version is vulnerable to a timing based attack which may allow an attacker to guess the</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>content of fixed data blocks and may eventually be able to guess the value of the private RSA</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>key of the server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>An attacker may use this implementation flaw to sniff the data going to this host and decrypt</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>some parts of it, as well as impersonate your server and perform man in the middle attacks.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>*** Nessus solely relied on the banner of the remote host</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>*** to issue this warning</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>See also: <a href="http://www.openssl.org/news/secadv_20030219.txt">http://www.openssl.org/news/secadv_20030219.txt</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://lassecwww.epfl.ch/memo_ssl.shtml">http://lassecwww.epfl.ch/memo_ssl.shtml</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://eprint.iacr.org/2003/052/">http://eprint.iacr.org/2003/052/</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Solution: Upgrade to version 0.9.6j (0.9.7b) or newer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk factor: Medium</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CVE: CAN-2003-0078, CAN-2003-0131</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>BID: 6884, 7148</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Nessus ID: 11267</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informational</td>
<td>https</td>
<td>A TLSv1 server answered on this port</td>
</tr>
<tr>
<td></td>
<td>(443/tcp)</td>
<td>Nessus ID: 10330</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informational</td>
<td>https</td>
<td>A web server is running on this port through SSL</td>
</tr>
<tr>
<td></td>
<td>(443/tcp)</td>
<td>Nessus ID: 10330</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informational</td>
<td>https</td>
<td>Here is the SSLv2 server certificate:</td>
</tr>
<tr>
<td></td>
<td>(443/tcp)</td>
<td>Certificate:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Version: 3 (0x2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Serial Number: 2 (0x2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Signature Algorithm: md5WithRSAEncryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Issuer: C=US, ST=Arizona, L=Tucson, O=University of Arizona, OU=Telecommunications, CN=Dep.univ.EDU/Email=<a href="mailto:staff@ms.Dep.univ.EDU">staff@ms.Dep.univ.EDU</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Validity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not Before: Jan 15 22:24:12 2002 GMT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not After: Jul 8 22:24:12 2007 GMT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Subject: C=US, ST=Arizona, O=University of Arizona, OU=Telecommunications, CN=www.Dep.univ.EDU/Email=<a href="mailto:staff@ms.Dep.univ.EDU">staff@ms.Dep.univ.EDU</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Subject Public Key Info:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public Key Algorithm: rsaEncryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RSA Public Key: (512 bit)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>dc:49:41:b7:a5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Exponent: 65537 (0x10001)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X509v3 extensions:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X509v3 Basic Constraints:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA:FALSE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Netscape Comment:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OpenSSL Generated Certificate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X509v3 Subject Key Identifier:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>X509v3 Authority Key Identifier:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DirName:/C=US/ST=Arizona/L=Tucson/O=University of Arizona/OU=Telecommunications/CN=Dep.univ.EDU/Email=<a href="mailto:staff@ms.Dep.univ.EDU">staff@ms.Dep.univ.EDU</a></td>
</tr>
</tbody>
</table>
Informational  https  (443/tcp)
Here is the list of available SSLv2 ciphers:
RC4-MD5
EXP-RC4-MD5
RC2-CBC-MD5
EXP-RC2-CBC-MD5
DES-CBC-MD5
DES-CBC3-MD5
RC4-64-MD5
Nessus ID : 10863

Informational  https  (443/tcp)
This TLSv1 server also accepts SSLv2 connections.
This TLSv1 server also accepts SSLv3 connections.
Nessus ID : 10863

Warning  exec  (512/tcp)
The rexecd service is open.
Because rexecd does not provide any good means of authentication, it can be used by an attacker to scan a third party host, giving you troubles or bypassing your firewall.

Solution : comment out the 'exec' line in /etc/inetd.conf.
Risk factor : Medium
CVE : CAN-1999-0618
Nessus ID : 10203

Warning  login  (513/tcp)
The rlogin service is running.
This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the rlogin client and the rlogin server. This includes logins and passwords.

You should disable this service and use openssh instead (www.openssh.com)

Solution : Comment out the 'rlogin' line in /etc/inetd.conf.
Risk factor : Low
CVE : CAN-1999-0651
Nessus ID : 10205

Warning  shell  (514/tcp)
The rsh service is running.
This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the rsh client and the rsh server. This includes logins and passwords.

You should disable this service and use ssh instead.
Solution: Comment out the 'rsh' line in /etc/inetd.conf.

Risk factor: Low
CVE: CAN-1999-0651
Nessus ID: 10245

Informational printer
(515/tcp)
A LPD server seems to be running on this port
Nessus ID: 10330

Warning nfs
(2049/tcp)
The RPC service nfs V2-3 is running on this port
If you do not use it, disable it, as it is a potential security risk
Nessus ID: 10336

Vulnerability mysql
(3306/tcp)
You are running a version of MySQL which is older than version 3.23.56. It is vulnerable to a vulnerability that may allow the mysqld service to start with elevated privileges.

An attacker can exploit this vulnerability by creating a DATADIR/my.cnf that includes the line 'user=root' under the '[mysqld]' option section.

When the mysqld service is executed, it will run as the root user instead of the default user.

Risk factor: High
Solution: Upgrade to at least version 3.23.56
CVE: CAN-2003-0150
BID: 7052
Nessus ID: 11378

Informational mysql
(3306/tcp)
It is usually reserved for MySQL
Nessus ID: 10330

Informational mysql
(3306/tcp)
Remote MySQL version: 3.23.54
Nessus ID: 10719

Informational mysql
(3306/tcp)
This MySQL server is temporarily refusing connections.
Nessus ID: 10481

Warning lockd
(4045/tcp)
The RPC service nlockmgr V1-4 is running on this port
If you do not use it, disable it, as it is a potential security risk
Nessus ID: 10336

Warning sometimes-rpc5
(32771/tcp)
The RPC service status V1 is running on this port
If you do not use it, disable it, as it is a potential security risk
Nessus ID: 10336

Warning unknown
(49680/tcp)
The RPC service mountd V1-3 is running on this port
If you do not use it, disable it, as it is a potential security risk
Nessus ID: 10336

Warning general/tcp
The remote host does not discard TCP SYN packets which have the FIN flag set.

Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.

See also: http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html
http://www.kb.cert.org/vuls/id/464113

Solution: Contact your vendor for a patch
Risk factor: Medium
BID: 7487
Nessus ID: 11618
Nessus ID : **11618**

Informational  general/tcp  
Nmap found that this host is running Solaris 8 early access beta through actual release

Nessus ID : **10336**

Informational  general/tcp  
TCP split NIDS evasion function is enabled. Some tests might run slowly and you may get some false negative results

Nessus ID : **10889**

Informational  general/tcp  
TCP fake RST NIDS evasion function is enabled. Some tests might run slowly and you may get some false negative results.

Nessus ID : **10889**

Informational  general/tcp  
HTTP NIDS evasion functions are enabled.
You may get some false negative results

Nessus ID : **10890**

Informational  general/tcp  
Remote OS guess : Solaris 8 early access beta through actual release

**CVE** : **CAN-1999-0454**

Nessus ID : **11268**

Informational  general/udp  
For your information, here is the traceroute to dep.univ128.49:

Nessus ID : **10287**

Warning  general/icmp  
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentication protocols.

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

Risk factor : Low

**CVE** : **CAN-1999-0524**

Nessus ID : **10114**

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

### Appendix G

**Solaris 8 Recommended Patches:**

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>108434-12</td>
<td>32-Bit Shared library patch for C++</td>
</tr>
<tr>
<td>108435-12</td>
<td>64-Bit Shared library patch for C++</td>
</tr>
<tr>
<td>108528-21</td>
<td>SunOS 5.8: kernel update patch</td>
</tr>
<tr>
<td>108652-66</td>
<td>X11 6.4.1: Xsun patch</td>
</tr>
<tr>
<td>108725-13</td>
<td>SunOS 5.8: st driver patch</td>
</tr>
<tr>
<td>108727-25</td>
<td>SunOS 5.8: /kernel/fs/nfs and /kernel/fs/sparcv9/nfs patch</td>
</tr>
<tr>
<td>108806-15</td>
<td>SunOS 5.8: Sun Quad FastEthernet qfe driver</td>
</tr>
<tr>
<td>108869-19</td>
<td>SunOS 5.8: snmpd/mibiisa/libssasnp/snmplib patch</td>
</tr>
<tr>
<td>108899-04</td>
<td>SunOS 5.8: /usr/bin/ftp patch</td>
</tr>
<tr>
<td>108901-06</td>
<td>SunOS 5.8: /kernel/sys/rpcmod and /kernel/strmod/rpcmod patch</td>
</tr>
<tr>
<td>108919-18</td>
<td>CDE 1.4: dtlogin patch</td>
</tr>
<tr>
<td>108949-07</td>
<td>CDE 1.4: libDtHelp/libDtSvc patch</td>
</tr>
<tr>
<td>108968-08</td>
<td>SunOS 5.8: vol/vold/ rmmount/dev_pcmem.so.1 patch</td>
</tr>
<tr>
<td>108974-30</td>
<td>SunOS 5.8: dada,  uata, dad, sd, ssd and scsi drivers patch</td>
</tr>
<tr>
<td>108975-08</td>
<td>SunOS 5.8: /usr/bin/rmformat and /usr/sbin/format patch</td>
</tr>
<tr>
<td>108977-02</td>
<td>SunOS 5.8: libsmedia patch</td>
</tr>
<tr>
<td>Patch</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>SunOS 5.8: /kernel/drv/arp patch</td>
<td>SunOS 5.8: bsmunconv overwrites root cron tab if cu created /tmp/root</td>
</tr>
<tr>
<td>SunOS 5.8: /kernel/drv/hme and /kernel/drv/sparcv9/hme patch</td>
<td>SunOS 5.8: LDAP2 Patch</td>
</tr>
<tr>
<td>SunOS 5.8: Patch for patchadd and patchrm</td>
<td>SunOS 5.8: libexacct and libproject patch</td>
</tr>
<tr>
<td>SunOS 5.8: /usr/sbin/in.rshd patch</td>
<td>SunOS 5.8: libauth and libproject patch</td>
</tr>
<tr>
<td>SunOS 5.8: at/atrm/batch/cron patch</td>
<td>SunOS 5.8: /usr/lib/libdhcpcd.so.1 patch</td>
</tr>
<tr>
<td>SunOS 5.8: /usr/kernel/sys/acctctctl and /usr/kernel/sys/exacctsys patch</td>
<td>SunOS 5.8: /usr/lib/libdhcpagent.so.1 patch</td>
</tr>
<tr>
<td>SunOS 5.8: LDAP2 Patch</td>
<td>SunOS 5.8: patch finger</td>
</tr>
<tr>
<td>SunOS 5.8: libexacct and libproject patch</td>
<td>SunOS 5.8: patch in.named patch</td>
</tr>
<tr>
<td>SunOS 5.8: /usr/kernel/sys/acctctctl and /usr/kernel/sys/exacctsys patch</td>
<td>SunOS 5.8: patch in.named patch</td>
</tr>
<tr>
<td>SunOS 5.8: Patch for patchadd and patchrm</td>
<td>SunOS 5.8: /usr/lib/libdhcpcd.so.1 patch</td>
</tr>
<tr>
<td>SunOS 5.8: LDAP2 Patch</td>
<td>SunOS 5.8: patch finger</td>
</tr>
<tr>
<td>SunOS 5.8: libexacct and libproject patch</td>
<td>SunOS 5.8: patch in.named patch</td>
</tr>
<tr>
<td>SunOS 5.8: /usr/kernel/sys/acctctctl and /usr/kernel/sys/exacctsys patch</td>
<td>SunOS 5.8: patch in.named patch</td>
</tr>
<tr>
<td>SunOS 5.8: LDAP2 Patch</td>
<td>SunOS 5.8: patch finger</td>
</tr>
<tr>
<td>SunOS 5.8: libexacct and libproject patch</td>
<td>SunOS 5.8: patch in.named patch</td>
</tr>
<tr>
<td>SunOS 5.8: /usr/kernel/sys/acctctctl and /usr/kernel/sys/exacctsys patch</td>
<td>SunOS 5.8: patch in.named patch</td>
</tr>
<tr>
<td>SunOS 5.8: LDAP2 Patch</td>
<td>SunOS 5.8: patch finger</td>
</tr>
<tr>
<td>SunOS 5.8: libexacct and libproject patch</td>
<td>SunOS 5.8: patch in.named patch</td>
</tr>
<tr>
<td>SunOS 5.8: /usr/kernel/sys/acctctctl and /usr/kernel/sys/exacctsys patch</td>
<td>SunOS 5.8: patch in.named patch</td>
</tr>
<tr>
<td>SunOS 5.8: LDAP2 Patch</td>
<td>SunOS 5.8: patch finger</td>
</tr>
<tr>
<td>SunOS 5.8: libexacct and libproject patch</td>
<td>SunOS 5.8: patch in.named patch</td>
</tr>
<tr>
<td>SunOS 5.8: /usr/kernel/sys/acctctctl and /usr/kernel/sys/exacctsys patch</td>
<td>SunOS 5.8: patch in.named patch</td>
</tr>
<tr>
<td>SunOS 5.8: LDAP2 Patch</td>
<td>SunOS 5.8: patch finger</td>
</tr>
<tr>
<td>SunOS 5.8: libexacct and libproject patch</td>
<td>SunOS 5.8: patch in.named patch</td>
</tr>
<tr>
<td>SunOS 5.8: /usr/kernel/sys/acctctctl and /usr/kernel/sys/exacctsys patch</td>
<td>SunOS 5.8: patch in.named patch</td>
</tr>
<tr>
<td>SunOS 5.8: LDAP2 Patch</td>
<td>SunOS 5.8: patch finger</td>
</tr>
<tr>
<td>SunOS 5.8: libexacct and libproject patch</td>
<td>SunOS 5.8: patch in.named patch</td>
</tr>
<tr>
<td>SunOS 5.8: /usr/kernel/sys/acctctctl and /usr/kernel/sys/exacctsys patch</td>
<td>SunOS 5.8: patch in.named patch</td>
</tr>
<tr>
<td>SunOS 5.8: LDAP2 Patch</td>
<td>SunOS 5.8: patch finger</td>
</tr>
<tr>
<td>SunOS 5.8: libexacct and libproject patch</td>
<td>SunOS 5.8: patch in.named patch</td>
</tr>
<tr>
<td>SunOS 5.8: /usr/kernel/sys/acctctctl and /usr/kernel/sys/exacctsys patch</td>
<td>SunOS 5.8: patch in.named patch</td>
</tr>
<tr>
<td>SunOS 5.8: LDAP2 Patch</td>
<td>SunOS 5.8: patch finger</td>
</tr>
<tr>
<td>SunOS 5.8: libexacct and libproject patch</td>
<td>SunOS 5.8: patch in.named packet</td>
</tr>
<tr>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>111325-02</td>
<td>SunOS 5.8: /usr/lib/saf/ttymon patch</td>
</tr>
<tr>
<td>111327-05</td>
<td>SunOS 5.8: libsocket patch</td>
</tr>
<tr>
<td>111504-01</td>
<td>SunOS 5.8: /usr/bin/tip patch</td>
</tr>
<tr>
<td>111548-01</td>
<td>SunOS 5.8: catman, man, whatis, apropos and makewhatis patch</td>
</tr>
<tr>
<td>111570-02</td>
<td>SunOS 5.8: uucp patch</td>
</tr>
<tr>
<td>111596-03</td>
<td>SunOS 5.8: /usr/lib/netsvc/yp/rpc.yppasswdd patch</td>
</tr>
<tr>
<td>111606-03</td>
<td>SunOS 5.8: /usr/sbin/in.ftpd patch</td>
</tr>
<tr>
<td>111626-03</td>
<td>OpenWindows 3.6.2: Xview Patch</td>
</tr>
<tr>
<td>111826-01</td>
<td>SunOS 5.8: /usr/sbin/sparcv7/whodo &amp; /usr/sbin/sparcv9/whodo patch</td>
</tr>
<tr>
<td>111874-06</td>
<td>SunOS 5.8: /usr/bin/mail patch</td>
</tr>
<tr>
<td>111879-01</td>
<td>SunOS 5.8: Solaris Product Registry patch SUNWwsr</td>
</tr>
<tr>
<td>111881-03</td>
<td>SunOS 5.8: /usr/kernel/strmod/telmod patch</td>
</tr>
<tr>
<td>111883-16</td>
<td>SunOS 5.8: Sun GigaSwift Ethernet 1.0 driver patch</td>
</tr>
<tr>
<td>111958-02</td>
<td>SunOS 5.8: /usr/lib/nfs/statd patch</td>
</tr>
<tr>
<td>112138-01</td>
<td>SunOS 5.8: /usr/sbin/sparcv7/whodo &amp; /usr/sbin/sparcv9/whodo patch</td>
</tr>
<tr>
<td>112237-07</td>
<td>SunOS 5.8: mech_krb5.so.1 patch</td>
</tr>
<tr>
<td>112254-01</td>
<td>SunOS 5.8: /kernel/sched/TS patch</td>
</tr>
<tr>
<td>112279-02</td>
<td>SunOS 5.8: pkgrm failed during upgrade from Solaris 8 to Solaris 9 with DSR</td>
</tr>
<tr>
<td>112325-01</td>
<td>SunOS 5.8: /kernel/fs/udfs and /kernel/fs/sparcv9/udfs patch</td>
</tr>
<tr>
<td>112396-02</td>
<td>SunOS 5.8: /usr/bin/fgrep patch</td>
</tr>
<tr>
<td>112425-01</td>
<td>SunOS 5.8: /usr/lib/fs/ufs/mount and /etc/fs/ufs/mount patch</td>
</tr>
<tr>
<td>112459-01</td>
<td>SunOS 5.8: /usr/lib/pt_chmod patch</td>
</tr>
<tr>
<td>112611-01</td>
<td>SunOS 5.8: /usr/lib/iblz.so.1 patch</td>
</tr>
<tr>
<td>112668-01</td>
<td>SunOS 5.8: /usr/bin/gzip patch</td>
</tr>
<tr>
<td>112796-01</td>
<td>SunOS 5.8: /usr/sbin/in.talkd patch</td>
</tr>
<tr>
<td>112846-01</td>
<td>SunOS 5.8: /usr/lib/netsvc/rwall/rpc.rwalld patch</td>
</tr>
<tr>
<td>113650-02</td>
<td>SunOS 5.8: /usr/lib/utmp_update patch</td>
</tr>
<tr>
<td>113792-01</td>
<td>OpenWindows 3.6.2: mailtool patch</td>
</tr>
<tr>
<td>113886-08</td>
<td>OpenGL 1.3: OpenGL Patch for Solaris (32-bit)</td>
</tr>
<tr>
<td>113887-08</td>
<td>OpenGL 1.3: OpenGL Patch for Solaris (64-bit)</td>
</tr>
<tr>
<td>114152-01</td>
<td>SunOS 5.8: Japanese SunOS 4.x Binary Compatibility (BCP) patch</td>
</tr>
<tr>
<td>114162-01</td>
<td>SunOS 5.8: /kernel/drv/lofi drivers and /usr/sbin/lofiadm patch</td>
</tr>
<tr>
<td>114251-01</td>
<td>SunOS 5.8: pkgrm failed if upgrade from S8U7 to upper release with DSR</td>
</tr>
<tr>
<td>114673-01</td>
<td>SunOS 5.8: /usr/sbin/wall patch</td>
</tr>
</tbody>
</table>
Solaris 8 Patches Containing Security Fixes:

<table>
<thead>
<tr>
<th>Patch Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>108773-18</td>
<td>SunOS 5.8: IIIM and X Input &amp; Output Method patch</td>
</tr>
<tr>
<td>108835-04</td>
<td>CDE 1.4: dtcm patch</td>
</tr>
<tr>
<td>108909-13</td>
<td>CDE 1.4: Smart Card Administration GUI patch</td>
</tr>
<tr>
<td>109005-05</td>
<td>SunOS 5.8: /sbin/su.static and /usr/bin/su patch</td>
</tr>
<tr>
<td>109077-12</td>
<td>SunOS 5.8: dhcp server and admin patch</td>
</tr>
<tr>
<td>109149-02</td>
<td>SunOS 5.8: /usr/sbin/mkdevmaps and /usr/sbin/mkdevalloc patch</td>
</tr>
<tr>
<td>109152-02</td>
<td>SunOS 5.8: /usr/lib/libc.so.x.9 and libdbm patch</td>
</tr>
<tr>
<td>109202-04</td>
<td>SunOS 5.8: /kernel/misc/gld and /kernel/misc/sparcv9/gld patch</td>
</tr>
<tr>
<td>109458-03</td>
<td>SunOS 5.8: /kernel/strmod/idterm patch</td>
</tr>
<tr>
<td>109695-03</td>
<td>SunOS 5.8: /etc/smartcard/opencard.properties patch</td>
</tr>
<tr>
<td>109815-15</td>
<td>SunOS 5.8: se, acebus, pcf8574, pcf8591 and scsb patch</td>
</tr>
<tr>
<td>109887-17</td>
<td>SunOS 5.8: smartcard and usr/sbin/ocfserv patch</td>
</tr>
<tr>
<td>109893-04</td>
<td>SunOS 5.8: stc driver patch</td>
</tr>
<tr>
<td>109894-01</td>
<td>SunOS 5.8: /kernel/driv/sparcv9/bpp driver patch</td>
</tr>
<tr>
<td>109896-14</td>
<td>SunOS 5.8: USB and Audio Framework patch</td>
</tr>
<tr>
<td>109922-04</td>
<td>SunOS 5.8: pcelx and pcser driver patch</td>
</tr>
<tr>
<td>110068-02</td>
<td>CDE 1.4: PDASync patch</td>
</tr>
<tr>
<td>110389-05</td>
<td>SunOS 5.8: cvc CPU signature</td>
</tr>
<tr>
<td>110416-03</td>
<td>SunOS 5.8: ATOM12 patch</td>
</tr>
<tr>
<td>110461-03</td>
<td>SunOS 5.8: ttcompat patch</td>
</tr>
<tr>
<td>110820-10</td>
<td>SunOS 5.8: /platform/SUNW,Sun-Fire-15000/kernel/driv/sparcv9/dman patch</td>
</tr>
<tr>
<td>110953-04</td>
<td>SunOS 5.8: /usr/kernel/driv/lisc2 patch</td>
</tr>
<tr>
<td>110955-04</td>
<td>SunOS 5.8: /kernel/strmod/timod patch</td>
</tr>
<tr>
<td>111332-06</td>
<td>SunOS 5.8: /usr/lib/docs patch</td>
</tr>
<tr>
<td>111400-01</td>
<td>SunOS 5.8: KCM2 configure tool has a security vulnerability</td>
</tr>
<tr>
<td>111588-04</td>
<td>SunOS 5.8: /kernel/driv/ws and /kernel/fs/specfs patch</td>
</tr>
<tr>
<td>111624-04</td>
<td>SunOS 5.8: /usr/sbin/inetd patch</td>
</tr>
<tr>
<td>111647-01</td>
<td>BCP l1hmle buffer overflow</td>
</tr>
<tr>
<td>112039-01</td>
<td>SunOS 5.8: /usr/bin/ckitem patch</td>
</tr>
<tr>
<td>112390-07</td>
<td>SunOS 5.8: Supplemental Encryption Kerberos V5: mech_krb5.so.1 patch</td>
</tr>
<tr>
<td>112438-01</td>
<td>SunOS 5.8: /kernel/driv/random patch</td>
</tr>
<tr>
<td>112609-02</td>
<td>SunOS 5.8: /kernel/driv/le and /kernel/driv/sparcv9/le patch</td>
</tr>
<tr>
<td>112792-01</td>
<td>SunOS 5.8: /usr/lib/pcmciad patch</td>
</tr>
<tr>
<td>113652-03</td>
<td>SunOS 5.8: Supplemental Kernel Update Patch for 108528-17</td>
</tr>
<tr>
<td>113685-02</td>
<td>SunOS 5.8: logindmx/ptsl/ms/bufmod/lisc1/kb/zs/zsh/ptem patch</td>
</tr>
<tr>
<td>113687-01</td>
<td>SunOS 5.8: /kernel/misc/kbtrans patch</td>
</tr>
<tr>
<td>114045-03</td>
<td>SunOS 5.8: Netscape Portable Runtime(4.1.4)/Network Security System(3.3.4)</td>
</tr>
<tr>
<td>114146-01</td>
<td>SunOS 5.8: Supplemental Kernel Update Patch for 108528-16</td>
</tr>
<tr>
<td>114984-01</td>
<td>SunOS 5.8: /usr/kernel/fs/namefs patch</td>
</tr>
</tbody>
</table>
## Upcoming Training

<table>
<thead>
<tr>
<th>Course Type</th>
<th>Location</th>
<th>Dates</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS 2020</td>
<td>Orlando, FL</td>
<td>Apr 03, 2020 - Apr 10, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Online</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>