Global Information Assurance Certification Paper

UNIX Security Audit: GIAC Enterprises

Initial audit of the DNS server galleta

Brent A. House
Secure Enterprise Associates

February 6, 2001

Executive Summary

As we discussed in the entrance conference, I have spent the past three days auditing the AIX server "galleta", verifying the level of protection it provides. I am now prepared with recommendations to improve the system security before it is connected to the Internet through the company firewall. The purpose of this report is to detail the fieldwork completed, the results, and then to present my recommendations. According to Dan Farmer, noted security expert, there are three times to conduct an audit on a system: before you go live, on an on-going scheduled basis, and during emergencies (e.g. after a break-in). This is the audit before you go live. Notice that I recommend shutting off many of the default system services. You should question the business need for every service running on the system since many services are included to provide backward compatibility and may not even apply to your situation. Only allow the services required to perform your business and continue to adjust your security policies and practices to conform to changes in your working environment.

As is our practice, one week before I arrived on-site for fieldwork, I e-mailed to the lead SA (system administrator) an audit scope document and a listing of the commands to execute on the system (see Appendix A). During the week the SA stepped through the checklist and ran each command by hand and sent the output to a file. On my first day at GIAC Enterprises, the lead SA and I reviewed the printed output of the commands, noting any commands that failed, and areas of concern. This security audit is based on the output of the checklist of commands, physical access to GIAC Enterprises and interviews with your staff. To demonstrate to your staff how to check for vulnerabilities and verify later that they have been fixed, I helped them setup the Nessus security scanner on an administrative Linux server.

I have found several vulnerabilities in your DNS server machine that are common and easy to fix. The top issues are listed in the section "Prioritized list of security vulnerabilities". The critical issues include BIND problems, using telnet and ftp instead of ssh, unnecessary services like snmp are running on the server and password administration needs attention.

This initial audit will be followed by an audit one month from today to verify that the areas of concern have been corrected. I will conduct the audit in the presence of the lead SA, and leave him a set of automated tools that he can review for his own use, as he will be conducting the regular monthly audits. As our contract states, the lead SA will conduct monthly audits and I will conduct the quarterly audits.

I want to commend you on the work that has gone into building a secure location with staff to provide protection for the system. Everybody I met had a concern for security and felt responsible for their role in security. GIAC Enterprises has a system administration team with above average knowledge regarding system security.

Analysis of the computer system and findings

System Hardware

IBM RS/6000 Model H50 with 4 processors
Disks:
2 ea. 8 GB FW SCSI RAID-1
8 ea. 9 GB IBM SSA RAID-1

Physical Memory (RAM):
2048 MB

Adapters:
2 ea. IBM 10/100 Mbps Ethernet PCI Adapter

Operating System Software

IBM AIX 4.3.2.0

3rd Party Application Software

BIND – Berkeley Implementation of DNS

Operating system vulnerabilities

It is important to keep the operating system up to the latest maintenance level to prevent system exploitation from known/easy vulnerabilities. The best method is to regularly apply the latest AIX maintenance levels. A maintenance level is a collection of fixes called APARs (Authorized Program Analysis Report - Fix Numbers assigned by IBM) all rolled up into one PTF (Program Temporary Fix). When I checked your level using the command `oslevel` it reported "4.3.2.0", where the last digit determines the maintenance level to be 0. You may request the latest maintenance media from IBM at any time. After applying the maintenance media, oslevel will report the last digit as a "2", for maintenance level 2, which happens to be the latest maintenance release available.

To keep current with the latest vulnerabilities, IBM offers an e-mail subscription service at http://service.software.ibm.com/rs6k/listserv.html. One of the many subscription offerings is "Lists of Security Related Fixes". I suggest that you sign up for this free service and read the security notifications to keep up with any issues that apply to your system.

You may also go to bugtraq at www.securityfocus.com and search for AIX 4.3.2 security vulnerabilities. Check this periodically. Bugtraq allows a search in the vulnerabilities database by vendor, title and version. When searching for vulnerabilities for your version of AIX, choose:

Vendor=IBM
Title=AIX
Version=4.3.2

One of the latest vulnerabilities is avoided by simply turning off the piobe service (this you may do on your server since it doesn't need to offer printing services). The best approach to security is to simply turn off unnecessary services.
The vulnerability as reported by bugtraq is as follows:

Bugtraq

AIX piobe Buffer Overflow Vulnerability

bugtraq id 2037
object piobe (exec)
class Boundary Condition Error
cve GENERIC-MAP-NOMATCH
remote No
local Yes
published December 01, 2000
updated December 01, 2000
vulnerable IBM AIX 4.3.3
IBM AIX 4.3.2
IBM AIX 4.3.1
IBM AIX 4.3

IBM APAR IY12638
http://techsupport.services.ibm.com/rs6k/fixes.html

The problem exists in the piobe program. Due to the insufficient handling of the PIOSTATUSFILE, PIOTITLE and PIOVARDIR environment variables it's possible to overwrite stack variables. This makes it possible for a malicious user to pass specially formatted strings to the program, via environment variables, and potentially gain administrative access.

Configuration vulnerabilities

After reviewing the printout produced by the system administrator, I verified the following areas of protection and offer some suggestions for improvement. I will begin by checking three common problems: poor passwords, suid programs, and directory permissions.

Passwords

You are protected by an /etc/passwd file that is shadowed. After reviewing the /etc/security/user file, I found several areas to be changed. Following GIAC Enterprises security policy, it is necessary to have all passwords on systems a minimum length of 8 characters (minlen=8), each account password should be changed every 8 weeks (maxage=8), require both alpha (minalpha=2) and numeric (minother=1) characters in the password. Also an account should be disabled after 3 unsuccessful login attempts (loginretries=3).

In order to comply with the security policy, make the following changes to /etc/security/user, under the "default:" heading:
loginretries=3
maxage=8
minalpha=2
minother=1
minlen=8

Suid programs

Checking for the existence of suid files on a regular basis will help you know when your system has been compromised. An ordinary user can execute an suid file and assume superuser status. You should minimize the number of suid files on the system and nobody should be adding them without your knowledge. As galleta is currently managed, there is no method to check for intrusion and suid file creation. Create a data file of all the suid files on your system, keep it on a floppy disk and compare it regularly with the mounted filesystems.

Here are the steps modified from "Auditing Review" by Carla Wendt for creating a data file.
Step 1. find /\(-perm -00400 -o -perm -00200 \) -type f\ > -fls /tmp/suidfiles.dat
Step 2. mount /floppy
Step 3. cp /tmp/suidfiles.dat /floppy/suidfiles.dat; ls -l /floppy/suidfiles.dat; rm /tmp/suidfiles.dat
Step 4. umount /floppy
Step 5. label the floppy, slide to read-only, and lock it away.

To check for changes in suid files
Step 1. find /\(-perm -00400 -o -perm -00200 \) -type f\ > -fls /tmp/suidfiles.dat
Step 2. mount /floppy
Step 3. diff /floppy/suidfiles.dat /tmp/suidfiles.dat > /tmp/suid_diff.out
Step 4. Check for any changed files in /tmp/suid_diff.out

Use the list of files generated by the previous steps to create a list so that you may review the need to have certain files available with suid permissions.

The best method to keep track of all filesystem changes is by setting up a file integrity

tool like Tripwire and saving the data to a floppy diskette. With Tripwire you setup a policy file listing binaries that shouldn't change and directories to check. Tripwire will scan all the objects and report any violations encountered. Whenever you suspected a system compromise, pull out the diskette and run Tripwire. For additional information on Tripwire, see "Additional AIX Security Tools …", pg. 122.

Directory permissions

It is important to verify the current directory permissions, since errors could allow unprivileged users to copy, move, or overwrite files. The permissions on the mounted filesystems in general are appropriate. I did, however, notice that the filesystem "/archive" had permissions 777. With 777, everybody on the system has read/write/execute permissions. I suggest that you change the permissions on the filesystem mount point to 700. Changing permissions to 700 allows read/write/execute to only the directory owner; no other user has any rights to the directory.

Another area of concern with configuration has to do with the processes running on the system. I will now review the services running on the system.

From a default installation, AIX starts several unnecessary server and network services. I noticed the following services that you should disable on your server. They are divided in two sections: operating system services and networking services.

Operating System Services

Limiting the number of programs running on your system will make it simpler to identify unusual processes and also free up memory and processors. Here are the details regarding which operating system services you may safely remove:

Startup scripts /etc/rc.net.serial and /etc/rc.nfs
To prevent startup scripts for NFS and serial SLIP access from even starting in the first place, rename the files:
mv rc.net.serial Xrc.net.serial
mv rc.nfs Xrc.nfs

/etc/inittab
The inittab file contains entries for starting and restarting programs at specific operating system run levels. Delete or comment out the following lines with a ":", as they deal with services not necessary for a DNS server machine. As a strictly DNS server, there is no need for print services (piobe and qdaemon), write services between servers (writesrv), kernel messages to controlling terminals (uprintfd), or CDE X-windows services (dt).

For a detailed description of each service and information on how to uninstall or change permissions on the binaries, refer to pg. 152-154 "Additional AIX Security Tools …".

If the following lines exist, they may be removed or commented out from /etc/inittab:

```
rcnfs:2:wait:/etc/rc.nfs > /dev/console 2>&1 # Start NFS daemons
piobe:2:wait:/usr/lib/lpd/pio/etc/pioinit >/dev/null 2>&1 # pb cleanup
qdaemon:2:wait:/usr/bin/startsrc -sqdaemon
writesrv:2:wait:/usr/bin/startsrc -swritesrv
uprintfd:2:respawn:/usr/sbin/uprintfd
httpdlite:2:once:/usr/IMNSearch/httpdlite/httpdlite –r
/etc/IMNSearch/httpdlite/httpdlite.conf & > /dev/console 2>&1
dt:2:wait:/etc/rc.dt
imnss:2:once:/usr/IMNSearch/bin/imnss -start imnhelp >/dev/console 2>&1
imqss:2:once:/usr/IMNSearch/bin/imq_start >/dev/console 2>&1
```

Use the command rmitab to safely remove each line. Here is an example of how to remove the line for qdaemon:

```
# rmitab qdaemon
```

Networking Services

Turning off unnecessary networking services minimizes the potential break-in points. Here are the details of which services you may safely disable:

/etc/rc.tcpip
Comment out lines for sendmail.

```
qpi=30m  # 30 minute interval
start /usr/lib/sendmail "$src_running" "-bd –q${qpi}"
```

also the lines for snmp:

```
start /usr/sbin/snmpd "$src_running"
```

Before removing unnecessary services from this startup file for the TCP/IP daemons, be sure to visit http://techsupport.services.ibm.com for the latest TCP/IP updates or request the media from IBM support. Apply the latest fixes to be sure you are up-to-date. Be aware that if you decide to remove any binaries, it may cause problems when you apply future maintenance fixes. A simple option to disable binaries is by removing the executable permission from the file.

You may turn off dynamic host configuration (dhcpcd, dhcpsd, dhcprd), since galleta is only a DNS server. Turn off unnecessary IP version 6 lines (autoconf6, ndpd-host, ndnpd-router) since you are using IP version 4.

On galleta, I suggest you keep commented out the following lines, unless you absolutely need these services:

```
# Start up dhcpcd daemon
#start /usr/sbin/dhcpcd "$src_running"
```

```
# Start up autoconf6 process
#start /usr/sbin/autoconf6 ""
# Start up ndpd-host daemon
#start /usr/sbin/ndpd-host "$src_running"
# Start up the ndpd-router daemon
#start /usr/sbin/ndpd-router "$src_running"
# Start up print daemon
#start /usr/sbin/lpd "$src_running"
# Start up routing daemon (only start ONE)
#start /usr/sbin/routed "$src_running" -q
#start /usr/sbin/gated "$src_running"
# Start up time daemon
#start /usr/sbin/timed "$src_running"
# Start up Network Time Protocol (NTP) daemon
#start /usr/sbin/xntpd "$src_running"
# Start up rwhod daemon (a time waster)
#start /usr/sbin/rwhod "$src_running"
# Start up the Simple Network Management Protocol (SNMP) daemon
# start /usr/sbin/snmpd "$src_running"
# Start up the DHCP Server
#start /usr/sbin/dhcpsd "$src_running"
# Start up the DHCP Relay Agent
#start /usr/sbin/dhcprd "$src_running"
# Start up the DPID2 daemon
start /usr/sbin/dpid2 "$src_running"
# Start up the mrouted daemon
#start /usr/sbin/mrouted "$src_running"
```

Removing entries from /etc/inetd.conf
You should really install and configure ssh. Once you are comfortable with ssh, comment out the telnet, rsh, and ftp services in /etc/inetd.conf.

Here is a sample of what the /etc/inetd.conf files should look like after you are done commenting out internet services that are not already commented out.

```
#ftp     stream  tcp6    nowait  root    /usr/sbin/ftpd          ftpd
#telnet  stream  tcp6    nowait  root    /usr/sbin/telnetd       telnetd -a
#shell   stream  tcp6    nowait  root    /usr/sbin/rshd          rshd
#kshell  stream  tcp     nowait  root    /usr/sbin/krshd         krshd
#login   stream  tcp6    nowait  root    /usr/sbin/rlogind       rlogind
#klogin  stream  tcp     nowait  root    /usr/sbin/krlogind      krlogind
#exec    stream  tcp6    nowait  root    /usr/sbin/rexecd        rexecd
#ntalk   dgram   udp     wait    root    /usr/sbin/talkd         talkd
#rstatd  sunrpc_udp     udp     wait     root     /usr/sbin/rpc.rstatd rstatd 100001 1-3
```

```
#rusersd sunrpc_udp  udp     wait    root    /usr/lib/netsvc/rusers/rpc.rusersd rusersd
100002 1-2
#rwalld         sunrpc_udp   udp     wait    root    /usr/lib/netsvc/rwall/rpc.rwalld
rwalld 100008 1
#sprayd         sunrpc_udp   udp     wait    root    /usr/lib/netsvc/spray/rpc.sprayd
sprayd 100012 1
#pcnfsd         sunrpc_udp   udp     wait    root    /usr/sbin/rpc.pcnfsd pcnfsd 150001
1-2
#echo  stream tcp     nowait root    internal
#discard        stream tcp     nowait root    internal
#chargen        stream tcp     nowait root    internal
#daytime        stream tcp     nowait root    internal
#time   stream tcp     nowait root    internal
#echo  dgram  udp     wait    root    internal
#discard        dgram  udp     wait    root    internal
#chargen        dgram  udp     wait    root    internal
#daytime        dgram  udp     wait    root    internal
#time   dgram  udp     wait    root    internal

#/tmp/netinstalllog /u/netinst/scripts
#ttdbserver     sunrpc_tcp      tcp     wait    root    /usr/dt/bin/rpc.ttdbserver
#rpc.ttdbserver 100083 1
#dtspc stream tcp     nowait root    /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd
#cmsd  sunrpc_udp    udp     wait    root    /usr/dt/bin/rpc.cmsd cmsd 100068 2-5
```

After discussing the services that should be turned off, we had a demonstration with the Nessus Security Scanner. Since both white and black hats use Nessus, it is imperative that the system administrators regularly check each system on your network for known vulnerabilities.

What we discovered from the scan backed up the configuration vulnerability discussions about unnecessary services running. Nessus reported on bind, smtp, a web server, snmp, statd RPC service, and the cmsd RPC service. I left the system administrators with a copy of the Nessus report to compare with the report they produced after they implement the changes I suggested in this section of the audit.

Checklist of to-do items for Operating System Vulnerabilities and Configuration

1. Keep up to date on AIX maintenance software.
2. Turn off / remove unnecessary services.
3. Review and enforce password policy.
4. Install Tripwire, check regularly.
5. Document/cleanup suid and sgid files.
7. Document/cleanup world writeable files and directories.
8. Run Nessus Security Scanner regularly.

Risks from installed third-party software

The version of BIND that ships with AIX 4.3.2 has a fix. Since BIND is run on machines worldwide offering DNS services, it is a constant source of attacks. See ftp://aix.software.ibm.com/aix/efixes/security for updated fixes.

Administrative practices

During my three-day fieldwork, I interviewed several system administrators and computer operators. The following issues need to be addressed and/or resolved:

Issue: All the passwords have a common Star Trek theme.

Solution: GIAC Enterprises policy requires monthly password changes and a minimum password length of 8 alphanumeric characters. While the password theme is not explicitly against the company policy, it is possible for somebody to guess all the passwords after learning the first.

Issue: The hardware/software inventory is outdated and doesn't include SSA disks added a year ago. The cabling to the new disks drawers is not labeled.

Solution: Complete an annual inventory of hardware/software and label all cables.

Security patches up to date

On January 29, 2001, I received an e-mail notification from CERT (Computer Emergency Response Team) that had been forwarded by IBM. The notification was a warning of vulnerabilities with BIND (Berkeley Internet Name Domain). Since galleta will be a DNS (Domain Name System) server, and the implementation of DNS for UNIX is BIND, you will want to immediately implement this and any other patch that becomes available for BIND. This is an example of the type of warning you will receive from CERT, forwarded by IBM.

This file contains security alerts published by the Computer Emergency Response Team (CERT) that apply to AIX. These alerts (and more) are available directly from CERT on the world-wide web at the following URL:

http://www.cert.org/

In order to keep the size of this file reasonable, it contains only advisories for the current year. You can obtain a list of previous advisories either from the above URL, or by requesting on of the "CERT_YYYY" documents from this mail server.

The fixes mentioned in this document, when available, will be available from FixDist. Information on obtaining and using FixDist is available

by requesting the 'FixDist' document from this mail server, or at the following URL on the world-wide web:

http://techsupport.services.ibm.com/rs6k/fixes.html

IBM Corporation

VU#325431 - Queries to ISC BIND servers may disclose environment variables

IBM's AIX operating system may be vulnerable to this "inverse query" exploitation. We are working to understand the technical nature of this exploit; when done, we expect to verify AIX's vulnerability. We will provide updates to this page as we progress [in] studying this exploit.

VU#572183 - ISC BIND 4 contains buffer overflow in nslookupComplain()

IBM's AIX operating system is vulnerable to this potential exploit in named4. We are working to fix this quickly and we intend to post an emergency fix ASAP.

VU#868916 - ISC BIND 4 contains input validation error in nslookupComplain()

IBM's AIX operating system is vulnerable to this potential exploit and is working quickly toward a fix.

Sensitive data is stored encrypted and how

No files on galleta are being encrypted since his main purpose in life is to server DNS queries. According to the company policy this is acceptable. The policy states that encryption must be considered when data is transmitted outside the network, is in physically unsecured areas, is on a laptop hard drive, or is being transported via removable media.

If you must install encryption software, test out PGP from www-frec.bull.com. Install PGP according to the instructions in “Additional AIX Security Tools …” pg. 136-146.

Data is sent over the Internet encrypted

Issue: One area of concern is the use of telnet and ftp to this server. You are unnecessarily transmitting the root password across the network in cleartext. The SA and

I had a discussion about ssh and how it is used for encrypted network traffic. He said that the push to implement ssh network wide was stalled by the Windows developers because of concerns that their programs might not work well with ssh. I have helped developers at other companies overcome obstacles to implementing ssh and can provide you with the information or spend some time with the developers discussing the solutions.

Solution: Turn off telnetd and ftpd on the server. Implement ssh and require all remote users to use ssh. Setup securessh on Windows machines for developers to update web pages and code using scp.

Access is restricted to those with a need to know

This policy is being enforced by physically restricting access to the computer room and only giving the root password to the system administrators. I suggest that a copy of the root password be kept in a sealed envelope in your safe to be used in the case of emergency. After the emergency situation is resolved, change the password and reseal another envelope.

Another access restriction option is to use RSA SecurID cards for authentication to galleta. SecurID provides remote user authentication services where a unique password is generated for each login.

Backup Policies and Disaster Preparedness

This server is backed up regularly with a full backup each Sunday night with incremental backups during the week. The backups are written to a TSM server library. Weekly operating system backups are performed using sysback 6000 and saved on 8 mm tape. An operator checks all of the logs daily, and reports any problems to management.

When working with critical data, it is wise to make at least one extra backup to tape and test a restore of the backup before assuming it is valid. Monthly restores should be scheduled to verify the backups, and that can be automated using cron. Since the last sysadmin left six months ago, so did the knowledge of how to restore from the sysback server. Procedures with step-by-step instructions need to be prepared for operating system restores from sysback and individual file restores from TSM.

The off-site tape storage policy needs to be addressed to verify that it is consistent with the corporate data retention policy. Find out how long to keep backup media and schedule a monthly purge of data that drops off the retention period. Be sure that a separate set of instructions is shipped out with the backups (hardcopy and softcopy) to assist in restoring data. A project to contract with a hot-site and test restoring to their servers needs to be a priority to assure that your business can continue after a disaster. Plan and execute yearly disaster recovery tests to be sure that the documentation and procedures are current.

Checklist of to-do for Backup Policies and Disaster Preparedness.
1. Monthly restores.
2. Step-by-step guides for restoring from Sysback and TSM.
3. Contract with a hot-site for disaster recovery.
4. Yearly disaster recovery testing.

See also:
Go to web site http://www.cert.org/tech_tips/root_compromise.html
CERT® Coordination Center
Steps for Recovering from a UNIX or NT System Compromise

Site Security Handbook
ftp://ftp.isi.edu/in-notes/rfc2196.txt

Other issues/vulnerabilities as appropriate

Issue: NTP is installed only on the application servers, the time disagrees with galleta, the adminstration servers and routers.

Solution: Install and configure NTP on all servers. This will become an issue if you need to create a timeline of events to demonstrate the sequence of events for a break-in. Proving that your system has been compromised is easier when the logs of each system violated have time synchronized.

Prioritized list of security vulnerabilities

1. BIND has a known vulnerability.
2. Telnet and ftp transmit passwords in plain text. These shouldn't be running on a DNS server.
3. Unnecessary services are running on galleta.
4. Weak passwords are allowed, not following corporate policies.
5. Directory permissions allow other users write access to the /archive directory.

Prioritized list of recommended fixes and estimated costs to implement the recommendation

Breakdown of fixes and individual costs

1. Apply fixes to BIND application for DNS server. **1 hour**
2. Turn off telnetd and ftpd, then install and configure ssh. **3 hours**
3. Unnecessary services need to be turned off in configuration files. **1 hour**
4. Password policies need to be enforced. Teach everybody how to create a secure password. **3 hours**
5. Restrict non-system directory permissions. **1 hour**

Summary Information

Hourly rate = **$100**
Total hours to implement recommended fixes = **9**
Total cost to implement recommended fixes = **$900**

Resources

"Auditing Review", Carla Wendt, optional evening class at Capitol SANS 2000.
"Practical UNIX Security", Simson Garfinkel and Gene Spafford, O'Reilly & Associates, Inc. 1991
"AIX 4.3 Elements of Security: Effective and Efficient Implementation", IBM Redbook SG24-5962-00
"Additional AIX Security Tools on IBM pSeries, IBM RS/6000, and SP/Cluster", IBM Redbook SG24-5971-00
"System Security Audit", *Submitted by:* Jason Everett, http://www.sans.org/giactc/gcux.htm
"UNIX Security Auditing: A Practical Guide", Jack Maynard, SysAdmin Magazine, June 1997.

Appendix A

This is the checklist your system administrator used to create the output I examined in the audit.

Security Audit Checklist

Execute the following commands on the server as root user, redirect all output to a text file.
Example: "hostname >> /tmp/output.txt 2>&1"

```
hostname
oslevel
cat /etc/passwd
cat /etc/group
cat /etc/hosts.equiv
cat /etc/ftpusers
cat /etc/inittab
cat /etc/rc.tcpip
cat /etc/syslog.conf
cat /etc/exports
df -k
ls -al /
ls -al /dev
ls -al /usr
ls -al /usr/bin
ls -al /var
ls -al /etc
ls -al /etc/security
find / -name .rhosts -exec ls -l {} \;
find / \( -perm -2000 -o -perm -4000 \) -user 0 -ls
env
whereis sudo
netstat -an
ps -auxww
telnet localhost
ftp localhost
```