# Securing an IBM AIX Server

SANS GSNA Practical V4.0 Option 1
Topic 1 – “Testing”
Charles John
April 6, 2005

Table of Contents

# 1. Abstract

In order to satisfy the computing needs of its corporate departments, the Information Technology (IT) department of ABC Financial Corporation provides centralized management of the ABC corporate network, midrange systems, and servers. Specifically, the IT department provides all departments with the following services:

- Physical Security
- Environmental Controls
- Network Services (routing, firewall, IDS, DHCP, DNS)
- Server Installation
- Configuration Management including Patch Management
- Capacity and Performance Monitoring
- Backup and Recovery
- Business Continuity Planning and Disaster Recovery planning

Each department of ABC Financial Corporation manages the development of their own applications. This hybrid approach allows ABC Financial Corporation to achieve economies of scale through efficient centralized purchasing and management of systems. At the same time, corporate departments are able to respond quickly to changing business needs, building and managing their individual applications.

The Marketing Department's Windows 2000 server Oracle database application, a pilot application, is ready for migration to one of the corporation's midrange systems. The IT department recommends an existing IBM AIX server that has sufficient capacity to support both the existing needs and future growth of the marketing department.

The Marketing Department wants to ensure that the IBM AIX server managed by the IT Department is secure, that the Marketing Department's application can not be compromised through any IBM AIX operating system related vulnerability.

The Marketing Department has requested the corporate internal auditors to evaluate the security of the proposed IBM AIX server. The internal auditor's choose three areas to focus their attention on:

1. The Configuration and Patch Management process
2. IBM AIX Operating System file integrity
3. Business Continuity and Disaster Recovery

**Note:** All names, physical addresses, locations, phone numbers, email addresses, and IP addresses are fictitious, created for illustration only.

# 2. System Identification

This section characterizes the audited system, an IBM AIX server.

## 2.1 Responsible Organization

ABC Financial Corporation
Department of Information Technology
Corporate Systems Division
111 Any Road
Any Town, MD 12345

## 2.2 Physical Location

The IBM AIX server is housed in Building 100 of the ABC corporate headquarters complex located in Any Town, MD at the address listed in Section 2.1. The headquarters facilities are owned and managed by ABC Financial Corporation. Office space is not shared with other organizations.

Access to the headquarters complex is restricted to employees of ABC Financial Corporation. Employees are required to present an employee photo ID badge when arriving at the complex. Employees with access to the computer center swipe their employee badge through a magnetic card reader and enter a PIN.

## 2.3 Points of Contact

| Contact/ Title | Building | Room | Phone | Email |
|---|---|---|---|---|
| CIO | | | | |
| John Doe | 100 | A-10 | (301)-111-1111 | John.Doe@abc.com |
| | | | | |
| System Manager | | | | |
| Jane Smith | 100 | B-11 | (301) 111-2222 | Jane.Smith@abc.com |
| | | | | |
| Operations Contacts | | | | |
| Bill Jones | 100 | E-15 | (301) 111-3333 | Bill.Jones@abc.com |
| Fred Johnson | 100 | E-15 | (301) 111-4444 | Fred.johnson@abc.com |
| | | | | |
| Security Contacts | | | | |
| Sarah Wilson | 100 | C-10 | (301) 111-5555 | Sarah.wilson@abc.com |

## 2.4 Hardware Description

The AIX server is a pSeries 660 Model 6M1 server with two RS64 IV processors. The processors are 64-bit 750 MHz processors. Other system components include:

- Redundant power supplies (AC #9172)
- A power regulator (# 6164)
- Model T00 Enterprise Rack
- IBM 7316-TF1 Rack Console
- 2 GB Memory
- SCSI 9100 MB boot disk
- CD-ROM
- Diskette Drive
- Tape
- One 10/100 Mb/s Ethernet port
- Four 230 Kb/s serial ports
- One bidirectional parallel port

## 2.5 AIX Operating System

The server runs the IBM AIX 5L version 5.3 operating system.

## 2.6 Network Architectural Diagram

Appendix M includes a basic network architectural diagram. The IBM AIX server is connected to a departmental switch which in turn is connected to a backbone router. To access the AIX server, workstations connected to their respective departmental switch are routed through the backbone router to the AIX server.

## 2.7 Secure Shell (SSH)

The AIX server supports OpenSSH.

OpenSSH replaces FTP and telnet which are clear-text authentication protocols. Both FTP and telnet are disabled on the AIX server. For more information on building OpenSSH from source, see URL: http://www.openssh.com. (15 March 2005).

Additional information regarding OpenSSH and AIX is available at URL: http://sourceforge.net/projects/openssh-aix (15 March 2005).

## 2.8 TCP Wrappers

TCP Wrappers is installed on the IBM AIX server.

TCP Wrappers allow the administrator to control who has access to various network services based on the IP address of the source. TCP Wrappers also provide logging information via Syslog about both successful and unsuccessful connections.

TCP Wrappers only provides filtering on standard TCP-based services that are spawned by inetd. [1]

## 2.9 Trusted Computing Base

During initial installation, the Trusted Computing Base (TCB) was installed on the IBM AIX server. An AIX server requires complete re-installation to include TCB if TCB is not initially installed.

TCB enforces system wide security policies. Every file in the **/dev** directory is monitored. TCB monitors 600 additional files and stores critical information about these files in **/etc/security/syschk.cfg**. The AIX systems administrator created an offline copy of this file to ensure that the contents are protected from any unauthorized attempts to alter this file.

The AIX systems administrator periodically runs the command **tcbck –y ALL** to ensure that files included in **/etc/security/syschk.cfg** have not had their attributes altered. The systems administrator runs the command interactively and established a schedule through **cron**. This command will report and fix all errors.

Details regarding TCB are found at URL:
http://publib.boulder.ibm.com/infocenter/pseries/index.jsp?topic=/com.ibm.aix.doc/aixbman/security/installing_configuring_tcb.htm
(15 March 2005).

## 2.10 System Services

The services running on the AIX server are listed in Appendix A of this document. The server runs only those services required to support the applications.

## 2.11 Applications

This server is centrally managed by the ABC Financial Corporation headquarters IT department. The IT department provides information services to other departments of the ABC Financial Corporation. The server supports several Oracle 9i database

[1] http://www.redbooks.ibm.com/redbooks/pdfs/sg245971.pdf (15 March 2005)

applications hosted by the Accounting and Sales Departments. Pending the outcome of the AIX audit, the Marketing department intends to host their research database application on the AIX server.

### 2.12 Sensitivity of Information

| Application | Confidentiality | Integrity | Availability |
|---|---|---|---|
| | | | |
| Accounting | High | High | High |
| Sales | High | Medium | Medium |
| Marketing | High | High | Medium |

The Accounting database contains the internal financial data of the corporation including the Accounts Receivables, Accounts Payables, and General Ledger data. Disclosure of this information to unauthorized parties would damage the company's reputation and reduce their competitive edge. A compromise of the accounting database's integrity would hinder the company's ability to process internal financial data, collect receivables, and pay bills. The Accounting database must be available between the hours of 08:00am and 06:00pm EST Monday through Friday and for extended hours during the first week of each month including the weekend for closeout of the prior month's transactions. If the AIX server is not available, delays in processing internal financial transactions and producing the financial statements would harm the company's financial position.

The Sales database is a list of customers, potential customers, contact history, and a tickler system to remind sales people when to next contact their assigned customers. Unauthorized access to this database could provide competitors with key customer information. Several years ago there was an instance of a salesperson leaving the company with a printout of customer information including accounts that were not directly assigned to this salesperson. Since this incident, the application was reengineered to restrict access to information based on assignment. The Sales database must be available between the hours of 08:00am and 6:00pm EST Monday through Friday.

The database Marketing proposes to migrate to the AIX server contains detailed customer financial history that will be used to analyze trends and evaluate corporate financial products. Unauthorized access to the database could lead to loss of credibility with the public, loss of customers to competitors, and lawsuits from customers who are victimized through the exposure of their personal financial data. A compromise of data integrity could result in poor analysis leading to missed trends and the failure of new financial product offerings. The Marketing database must be available between the hours of 08:00am and 06:00pm EST Monday through Friday.

### 2.13 Applicable Laws, Regulations, and Guidelines

The CIO, Marketing Department representative, and Legal Department representative reviewed the information content of the database to determine what laws and regulations are applicable to the information contained within the database.

As the database contains detailed customer financial information, the parties agree that the database is subject to The Financial Modernization Act of 1999 also known as the Gramm-Leach-Bliley Act (GLB).[2]

The applicable corporate policies, the operational rules, and internal service fee structure are listed in a Service Level Agreement signed by both the IT and the Marketing Departments.

[2] http://www.ftc.gov/privacy/glbact/glbsub1.htm (15 March 2005)

# 3. Risk Analysis

Appendix B provides a comprehensive list of risks. From this list, three risks with serious impacts were selected for audit review. The selected risks include:

- Failure to apply security patches to the IBM AIX server in a timely fashion
- Failure to ensure IBM AIX server operating system file integrity
- Failure to ensure a reliable backup strategy and Business Contingency Plan

## 3.1 Configuration/Patch Management

The CIO of ABC Financial Corporation recognizes that Configuration Management including Patch Management are essential system management responsibilities necessary to ensure that the IBM AIX server cannot be exploited by a known vulnerability. Many hacker sites publish vulnerabilities as well as exploit code.

Should an unauthorized individual gain root access of the IBM AIX server through the successful exploitation of vulnerability, the individual may gain access to applications and data through other user accounts. Root kit programs could be installed, replacing legitimate programs, with the intention of monitoring system use and avoiding detection. System integrity could be compromised through data alteration. Users could be denied access through file deletion.

IT policy requires the AIX system administrators to evaluate all critical fixes within five days after receipt of a notice from IBM. System Administrators subscribe to the IBM notification service found at URL:
https://techsupport.services.ibm.com/server/pseries.subscriptionSvcs
(15 March 2005).

System administrators are required to submit a Configuration/Patch Change Proposal Form (CPCP) to the IT Configuration Management Change Control Board (CCB) for review and approval before any patch or configuration change can be made. The form identifies the following:

- Proposed date and time for performing the installation/upgrade/configuration change
- The reason for implementing the change
- The criticality of the change (High, Medium, Low)
- The users impacted
- The test results of the change applied to a non-production system
- Alternative mitigating strategies should it be necessary to delay implementing the change
- A recovery strategy should the change result in an unforeseen negative impact

to users

A sample form is included in Appendix D.

The IBM AIX system administrators check several sources on a monthly basis to ensure that there are no new vulnerabilities and that all known vulnerabilities are patched. Although they receive notifications through the IBM subscription service, the system administrators feel that is important to check additional sources for unconfirmed vulnerabilities.

Sites they visit include:

- The IBM subscription site for the IBM AIX 5L version 5.3 server at URL: http://www-1.ibm.com/servers/eserver/support/pseries/criticalfixes.html (15 March 2005)

- The Mitre Common Vulnerabilities and Exposures database available at URL: http://cve.mitre.org (15 March 2005)

- The National Institute of Standards and Technology (NIST) ICAT vulnerability database available at URL: http://icat.nist.gov (15 March 2005)

- The Bugtraq database available at URL: http://www.securityfocus.com (15 March 2005)

- The Secunia database available at URL: http://www.secunia.com (15 March 2005)

A search of the IBM website indicated the last Maintenance Level (ML) 5300-01 was December 2004. There have been no critical fixes for this release.

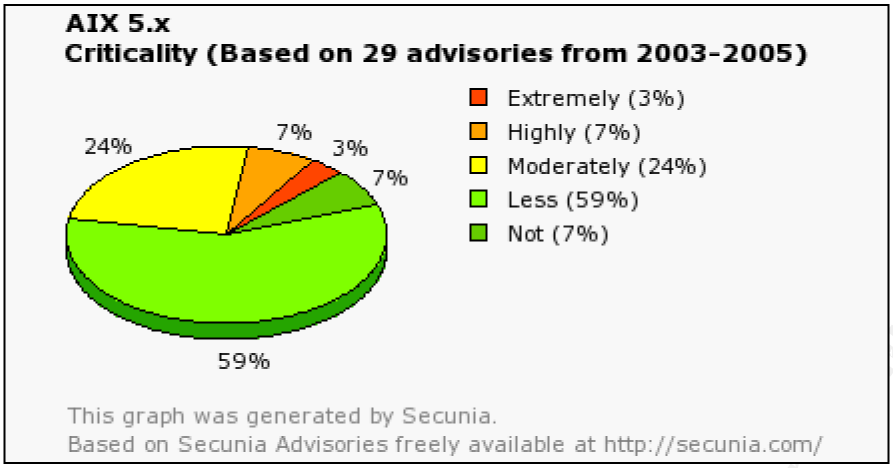
The table listed below was copied from the URL listed in the first bulleted item above.

| Critical fixes for AIX 5.3 | | |
|---|---|---|
| **Maintenance level** | **ML release** | **Critfix list updated** |
| Systems at 5300-01* | December, 2004 | |
| Systems at 5300-00 | | January 14, 2005 |

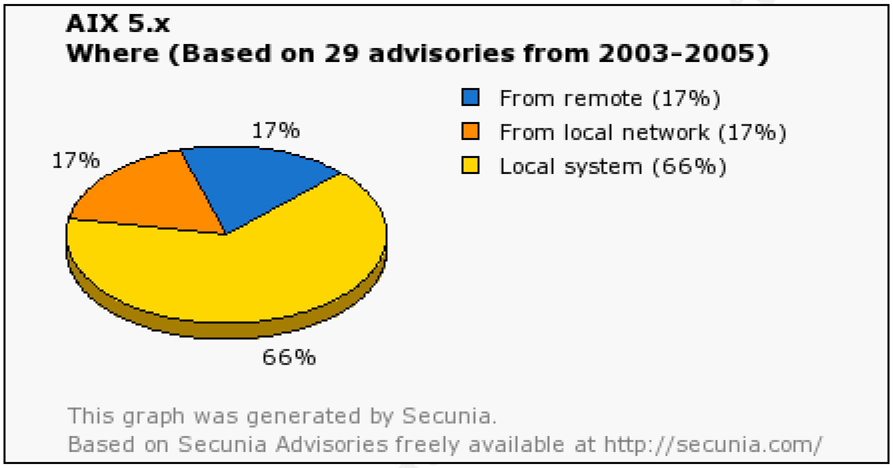
Appendix C lists the known vulnerabilities for IBM AIX 5.3 from the Mitre CVE, the NIST ICAT database, and the Secunia database.

Several of these reported vulnerabilities are buffer overflow vulnerabilities. Successful exploitation would allow the hacker to run arbitrary code. Note that not all acknowledged vulnerabilities have available patches. Secunia lists a vulnerability for Perl on an IBM AIX 5.3 server, acknowledged by IBM, with an approximate APAR date of 05/2005.

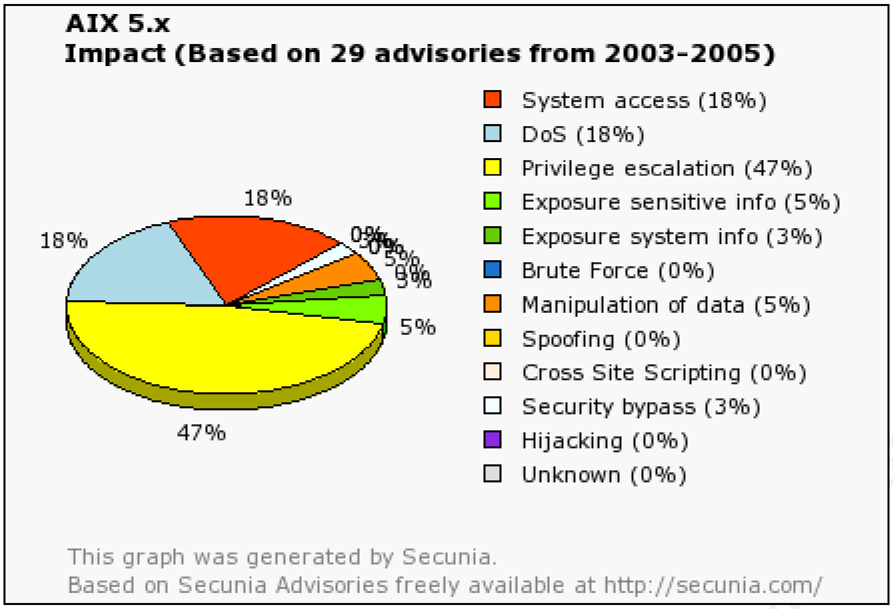
Secunia offers the following graphs related to IBM AIX 5.x vulnerability advisories:


AIX 5.x
Criticality (Based on 29 advisories from 2003-2005)

This graph was generated by Secunia.
Based on Secunia Advisories freely available at http://secunia.com/


AIX 5.x
Where (Based on 29 advisories from 2003-2005)

This graph was generated by Secunia.
Based on Secunia Advisories freely available at http://secunia.com/



This graph was generated by Secunia.
Based on Secunia Advisories freely available at http://secunia.com/

The graphs above was taken from the following URL:
http://secunia.com/graph/?type=cri&period=all&prod=213
(15 March 2005)

Successful exploit of most known vulnerabilities requires access directly on the system (66%) or access from the local network (17%). Privilege escalation (47%) and system access (18%) are the most serious impacts.

The Marketing Department of ABC Financial Corporation considers a Configuration/Patch management process as crucial to the successful migration and on-going operation of their database application. The IT Department has assured Marketing that IT is a service organization and that the Marketing Department will have representation on the IT Configuration Control Board.

## 3.2 File Integrity

As stated in the previous section, a compromise of the IBM AIX operating system could result in the replacement of valid programs with Trojan programs designed to gather system information, report that information to the hacker, and cover the tracks of the hacker by manipulating log files.

A hacker could exploit vulnerability in a service running on the AIX server perhaps due to a missing patch. With escalated privileges, a hacker could overwrite files. Several UNIX based services have a history of vulnerability. The SANS/FBI Top 20 lists a number of services (SMTP, SNMP, SSL, NIS/NFS) with known vulnerabilities.[3] To

[3] http://www.sans.org/top20/ (15 March 2005)

reduce risk, only those services necessary to support the AIX server applications are allowed to run. All other services must be removed or disabled.

The Marketing Department of ABC Financial Corporation is concerned with competitors being able to obtain the research and as a result, offer similar products to ABC Financial Corporation's customer base. The Marketing Department is also concerned that a competitor could alter the data leading ABC Corporation to incorrect conclusions. ABC Financial Corporation might miss key marketing opportunities or adjust existing products to its detriment.

As the IBM AIX server is managed by the IT Department and shared by several other departments, the Marketing Department is concerned about the 'insider' threat. The Marketing Department wants assurance that other users on the system will not be able to access the Marketing Department's files, that the AIX system administrators will not grant excessive rights to these users. The research has great value and could be sold to a competitor or emailed anonymously to a competitor by a disgruntled employee.

## 3.3 Backup Strategy and Contingency Plan

Maintaining a valid backup is a critical component of any Business Contingency Plan (BCP). Without a valid backup, ABC Financial Corporation will not be able to recover should an emergency arise. Given that the IBM AIX server is shared by multiple departments and managed by the IT Department, the Marketing Department wants assurances that their data can be recovered in the event of a disaster. The Marketing Department has identified a number of events that could occur resulting in the need to recover data from a backup tape. See the Risk Analysis in Appendix B. Scenarios that the Marketing Department views as possible include:

- Database corruption due to a programming error
- Accidental file deletion or overwrite
- Intentional file deletion or overwrite
- System patch issues
- Server hardware failure
- Site failures including:
    - Flooding
    - Fire damage
    - Power outages

The Marketing Department requires the IT Department to maintain a BCP that includes plans for both local restoration and recovery as well as plans for offsite hosting and recovery should facility damage necessitate moving operations to an alternate site. Marketing has provided IT with a Business Impact Analysis (BIA) indicating what Marketing's tolerance is for downtime and what functions need to be restored first to minimize the loss.

According to the Disaster Recovery Institute International (DRII)[4] about 50% of Business Continuity Plans are never tested and 85% of the plans that are tested fail when first tested.[5]

Given the high rate of plan failure and the serious impact on the organization should an incident disrupt business for an extended period, the Marketing Department has requested the internal auditors to assess the BCP.

[4] Disaster Recovery Institute International (DRII)
http://www.drii.org (15 March 2005)

[5] Roessing, Rolf von. Auditing Business Continuity **p. ix**

# 4. System Testing

The Internal Auditors engaged by the Marketing Department consider four testing methodologies valid for performing tests. These methods include:

1. **Reviewing documentation**: Appendix E lists documents that are typically requested when an audit is conducted. The absence of current and complete documentation is evidence that informal practices are followed. The auditors may need to perform more extensive testing to confirm actual practices.

2. **Conducting Interviews**: Managers, Operational personnel, and Technical personnel are selected. The auditors prefer to conduct in-person interviews. Interviews are conducted with managers to determine if formal policies exist. Operational personnel are interviewed to determine if written procedures exist and to determine if the procedures align with policy. Interviews with technical personnel identify the security controls in place and determine how effective the controls are in achieving policy goals.

3. **Making Observations**: Auditors request system administrators to enter specific commands and then confirm the anticipated results. Physical inspections are conducted. System counts are taken.

4. **Using Automatic testing tools**: Custom scripts, port scanners, and vulnerability scanners are used to provide results.

## 4.1 Configuration/Patch Management Testing

To confirm that the Configuration/Patch Management procedures function as intended and that the IBM AIX server has the latest patches the Internal Auditors performed the following actions:

1. Requested a copy of the IT Department's written policy for Configuration/Patch Management. The auditor's can refer to the policy if deficiencies are found that require remediation. Often resistance is met if a department is required to spend significant time, effort, and funds to resolve an issue. The department required to correct the problem may question the necessity to do so. The auditors can refer to the policy if the audit finding is challenged. The IT Department passes this test if a written policy is provided. The auditors may comment on the quality of the policy if clarity is lacking.

2. Requested a copy of the IT Department's written procedures for performing Configuration/Patch management. The IT Department passes this test if written procedures are provided. The auditors may comment on the quality of the

procedures if they appear to be incomplete.

3. Requested copies of the CPCP forms completed over the last six months. (Appendix D contains a sample form.) The forms provide evidence that the procedures are followed. The IT Department passes this test if written forms are provided.

4. Requested copies of emails that the IBM AIX system administrators received from the IBM Subscription Notification service. This confirms that the AIX system administrators receive timely security notices from the vendor and are aware of new vulnerabilities. The IT Department passes this test if the AIX system administrators are able to demonstrate that they subscribe to the Subscription Notification service.

5. Interviewed Control Board members from the Accounting and Sales Departments to ensure that board members are informed when any system changes are planned. This confirms that the IT Department informs other departments whose applications are impacted by proposed configuration changes and patch installations. Positive comments received from representatives from both the Accounting and Sales Departments indicate that the IT Department is providing the service documented in the Service Level Agreement.

6. Determined the latest critical fixes from the IBM subscription site as documented in Section 3.1 of this project. The auditors plan to use this information to determine if in fact the latest OS level is installed including any post OS level patches.

7. Requested an IBM AIX system administrator enter commands to indicate the patch level currently installed. The auditors observed and recorded the results. The system commands identified in this section were entered to confirm the latest OS level and post OS level patches are installed. If the OS level installed on the AIX server is thirty days or older than the current IBM AIX OS Maintenance Level release, the IT Department fails the test. If the AIX server does not include all post OS Maintenance Level patches, known as Authorized Problem Analysis Reports (APAR), that are thirty days or older, the IT Department fails the test. An exception occurs if the IT Department indicates that the patch is not installed in order to accommodate the requirements of an application and that other compensatory measures are taken.

   The auditors use a standard work paper to define the details for conducting each test. See Appendix H test 1 for the recording of the test details, results, and recommendations.

8. Performed automatic tests using the Nessus scan tool to determine what, if any,

patches are missing. The scan tool is used to identify security vulnerabilities associated with third-party and open source programs installed on the IBM AIX server. Patches for these programs may not be provided by IBM. It is not anticipated that Nessus will find any missing IBM AIX patches given that the AIX commands do not indicate that any patches are missing. Specific Nessus plugins were selected for testing. Nessus plugins are available at URL: http://www.nessus.org/plugins/ (15 March 2005). The IT Department fails the test if any of the Nessus plugins selected for testing identify a vulnerability and that vulnerability is not a false positive.

See Appendix H test 2 for the recording of the test details, results, and recommendations.

Appendix I lists the Nessus plugins that were chosen to test the IBM AIX server.

Steps 1 through 6 involve research and preparation necessary to design specific tests. It is not sufficient to just identify missing patches and then recommend the implementation of these patches. The auditors examine policies and procedures to ensure that when future vulnerabilities are identified and as patches are made available, these patches are tested and implemented. The auditors may recommend changes to procedures if weak procedures appear to be the root cause of a failure to apply patches.

To accomplish Step 7, the Internal Auditors requested the IBM AIX system administrator to enter the following commands:[6]

**# oslevel –r**

This command was entered to determine what the current release was. The Internal Auditors had the system administrator then enter command:

**# instfix –ik <apar#>**

The command was repeated for each of the following security Authorized Problem Analysis Reports (APARs):

| Security | | |
|---|---|---|
| **Download by APAR** | **APAR abstract** | **APAR details** |
| IY61956 | SECURITY VULNERABILITIES IN XPM CODE | View |
| IY59205 | /SBIN/RC.BOOT INSECURELY HANDLES TEMPORARY FILES | View |
| IY64277 | SECURITY VULNERABILITY IN DIAG. COMMANDS. | View |

[6] http://www-1.ibm.com/servers/eserver/support/pseries/critfixes/5300-00.html (15 March 2005)

|  |  |  |
|---|---|---|
| IY64354 | SECURITY: POSSIBILE SECURITY EXPOSURE IN CHCOD COMMAND | View |
| IY64820 | SECURITY VULNERABILITY IN LSVPD | View |
| IY64312 | BUFFER OVERFLOW VULNERABILITY IN PAGINIT | View |

The table listed above was copied from the following URL:
http://www-1.ibm.com/servers/eserver/support/pseries/critfixes/5300-00.html
(15 March 2005)

## 4.2 File Integrity Testing

To ensure that AIX system files are not compromised, the auditors decided to perform the following steps:

1. Ensure that only the approved services as documented in Appendix A are running. Services that are not necessary, that do not support any application running on the AIX server, may be exploited through either a known vulnerability or a vulnerability yet to be discovered. A successful exploit may provide the hacker with escalated privileges allowing the hacker to run arbitrary code. The IT Department passes this test if the services documented in Appendix A as being disabled are in fact disabled.

2. Confirm that the Trusted Computing Base (TCB) is installed. The IT Department fails the test if TCB is not installed.

3. Assuming that TCB is installed, the auditor's will review the TCB configuration file to determine which files and commands are protected. If the default system files are not listed in the configuration file, the IT Department fails the test. These files are included in the configuration file when TCB is first installed. The absence of any of these files would be an indicator that the configuration file has been manipulated perhaps to cover the fact that one or more system files have been replaced with Trojan programs.

4. The auditors will run a TCB command to check for inconsistencies between entries in the configuration file and the actual file attributes. If no inconsistencies are found, the IT Department passes the test.

5. The auditors will review user account stanzas in the **/etc/security/users** file to determine if any user accounts have privileges that are not required. The principle of least privilege requires users to have only the privileges they need to perform their jobs. Users with escalated privileges may be able to access files they do not require. This has the potential to violate confidentiality and integrity. If any users other than the two system administrators, Bill Jones and Fred Johnson, have admin or su privileges, the IT Department fails the test. These two individuals are the only individuals approved to have these rights.

6. The auditors will review user account stanzas in the **/etc/security/limits** file to ensure that processes users may run will not consume system resources. In the event that a user account is compromised, the account could be used to run arbitrary code, compromising file integrity and/or availability. Placing restrictions on memory and disk use will prevent a process from denying resources to others. The internal auditors want to ensure that the **stack** and **rss** settings for users do not permit unlimited use. The IT Department passes this test if there is a stanza for each user account in this file that places restrictions on the use of memory and disk space in accordance with the documented limits. Appendix L documents the limits the IT Department applies to user accounts. The two system administrator accounts are permitted to have higher limits.

Step 1 is achieved by:

- Reviewing the **/etc/inetd.conf** file to ensure that unnecessary services and daemons are removed.[7]

- Reviewing the **/etc/inittab** file to ensure that unnecessary services and daemons are removed.

- Reviewing the **/etc/rc.nfs** file to ensure that unnecessary NFS and NIS/NIS+ services and daemons are removed.

- Reviewing the **/etc/rc.tcpip** file to ensure that unnecessary TCP/IP services such as support for IPv6 and routing are removed.

- Inspecting the **/etc/inetd.conf** file to confirm that TCP Wrappers is installed. The auditors will determine if **tcpd** is specified.[8]

- Inspecting the **/etc/hosts.allow** file to ensure that only internal IP addresses are permitted to access services running on the IBM AIX server. The IP addresses should be those of the IT, Accounting, Sales, and Marketing subnets.

- Inspecting the **/etc/hosts.deny** file to ensure that all other IP addresses are not permitted to access services running on the IBM AIX server.

- Running the command **ps –ef** and recording the results. The auditors will look for any unexpected processes running on the AIX server.

[7] AIX 5L version 5.3 Security Guide, p. 279 http://publib.boulder.ibm.com/infocenter/pseries/topic/com.ibm.aix.doc/aixbman/security/security.pdf (15 March 2005)

[8] Managing AIX Server Farms, p. 128 http://www.redbooks.ibm.com/redbooks/pdfs/sg246606.pdf (15 March 2005)

- Examining the Nessus scan results for unknown processes running on ports. RPC may have assigned these ports to processes. Trojan software may also be responsible. To resolve this, the internal auditors will request an AIX system administrator to run the following commands:[9]

```
# netstat –af inet

# lsof –l | egrep “COMMAND|LISTEN|UDP”

# ps –fp pid#
```

The first command displays services waiting for incoming requests. These services are in the LISTEN state.

The second command will display TCP sockets in the LISTEN state and UDP sockets in the IDLE state. An example of the output is shown below.[10]

```
Command     PID  USER FD TYPE DEVICE      SIZE/OFF NODE NAME
Dtlogin     2122 root 5u IPv4 0x70053c00  0t0      UDP  *:xdmcp
Dtlogin     2122 root 6u IPv4 0x70054adc  0t0      TCP  *:32768(LISTEN)
Syslogd     2730 root 4u IPv4 0x70053600  0t0      UDP  *:syslog
```

Using the process ID (PID), the third command is entered to display the path to the command name.

Step 2 is achieved by entering command:

```
# /usr/bin/tcbck
```

If TCB is not installed, an error message displays:[11]

```
“3001-101 The Trusted Computing Base is not installed on this machine.
To enable the Trusted Computing Base, you must reinstall and
Set the ‘Install Trusted Computing Base’ option to YES.
No checking is being performed.”
```

Step 3 is achieved by examining the TCB configuration file:

[9] http://publib.boulder.ibm.com/infocenter/pseries/index.jsp?topic=/com.ibm.aix.doc/aixbman/security/network_services.htm (15 March 2005)

[10] http://publib.boulder.ibm.com/infocenter/pseries/index.jsp?topic=/com.ibm.aix.doc/aixbman/security/network_services.htm (15 march 2005)

[11] Michael, Randal K.. AIX 5L Administration p. 508

**# cat /etc/security/sysck.cfg**

For each file protected, the configuration contains a stanza, i.e., a list of settings. The table below lists the typical settings:[12]

| Option | Description |
|---|---|
| | |
| Acl | The access control list for the file |
| Checksum | The checksum of the file generated by command **sum -r** |
| Class | The class or classes this entry is in |
| Group | The GID or name of the file's group |
| Links | A list of hard links to the file |
| Mode | A comma-separated list containing the file permissions and special modes (SUID, SGID, SVTX, TCB) |
| Owner | The UID or name of the file's owner |
| Program | The path, name, and flags to the program used to check this entry |
| Size | The size of the file |
| Source | The source for the file |
| Symlinks | A list of symbolic links to this file |
| Target | For entries that are symbolic links, this contains a value for the file that the entry is linked from |
| Type | Can be FILE, DIRECTORY, FIFO, BLK_DEV, CHAR_DEV, or MPX_DEV |

To accomplish Step 4, the auditors will perform a consistency check, reporting problems but making no corrective changes. It is the responsibility of IT management to respond to the auditors' recommendations and approve changes in accordance with the documented Configuration/Patch Management procedures. The command used is:

**# /usr/bin/tcbck –n ALL**

This will check all files that have stanzas in **/etc/security/sysck.cfg[13].** The auditors are interested in confirming that the checksums and file sizes as recorded in the configuration file match those of the actual files.

Step 5 and 6 are accomplished by:

[12] Michael, Randal K. p. 509

[13] AIX 5L version 5.3 Security Guide, p. 5 http://publib.boulder.ibm.com/infocenter/pseries/topic/com.ibm.aix.doc/aixbman/security/security.pdf (15 March 2005)

- Reviewing the file **/etc/security/group.** This file has a stanza for each group in the file **/etc/group**. The stanzas indicate who is permitted to administer the group other than root. For example an entry of:

  ```
  accounting:
          admin = true
  ```

  indicates that the accounting group attributes can only be changed by the root account.

- Reviewing the file **/etc/security/user** to determine if any user accounts have inappropriate extended attributes, which could violate the principle of least privilege. Appendix K contains a list of the attributes that can be set for each user account.[14] The auditors are interested in determining who has **admin, rlogin,** and/or **su** privileges.

- Reviewing the file **/usr/lib/security/mkuser.default**. This file contains the default attribute settings used to create a stanza in the **/etc/security/user** file when an AIX system administrator uses the **mkuser** command to create a user account.

- Reviewing the file **/etc/security/limits** to ensure that user accounts are not able to create a denial of service by consuming system resources. Appendix L lists the standards set by ABC Financial Corporation to limit users' consumption of system resources.[15]

- Entering the command '**grpck –n ALL'** to ensure that all group members and administrators exist in the user database.[16]

- Entering the command '**grpchk –n install'** to ensure the uniqueness of each group name and GID.

- Entering the command '**pwdck –y ALL'** to ensure that all users have valid passwords.

- Entering the command '**usrck –n ALL'** to ensure that all user accounts have

[14] http://publib.boulder.ibm.com/infocenter/pseries/index.jsp?topic=/com.ibm.aix.doc/cmds/aixcmds2/grpck.htm (15 March 2005)

[15] http://publib.boulder.ibm.com/infocenter/pseries/index.jsp?topic=/com.ibm.aix.doc/files/aixfiles/limits.htm (15 March 2005)

[16] http://publib.boulder.ibm.com/infocenter/pseries/index.jsp?topic=/com.ibm.aix.doc/cmds/aixcmds2/grpck.htm (15 March 2005)

entries in the files **/etc/security/passwd, /etc/security/user,** and, **/etc/security/limits.**

**Note:** The switches used with these commands report problems without making any corrections.

## 4.3 Backup/Business Contingency Plan Testing

A valid backup is a requirement for a BCP. The auditors developed a survey form for evaluating system backup. The survey form was used for conducting in-person interviews with operational and technical personnel. Appendix F contains a list of survey questions. Once the questionnaire was completed, the auditors elected to perform the following tests:

1. Review several backup logs for evidence of any backup failures. The IT Department passes this test if the logs reviewed do not indicate backup failures, or if the logs do indicate failure, the IT Department can produce additional logs indicating that an additional backup was performed to compensate for the original backup failure.

2. Perform a restore of several test files to ensure that backup media can be restored. The IT Department passes this test if the test files selected for restoration are successfully restored. The auditors are concerned about extended permissions. The AIX system administrators use Access Control Lists (ACL) to permit and deny members of the Accounting and Sales groups from accessing each other's files. The internal auditors confirmed the use of extended permissions through use of the **aclget** command.[17] Entering this command followed by a file name displays the extended permissions. To preserve these extended permissions, the AIX system administrators must use the AIX **backup** command. Use of the AIX **restore** command will restore the file and the extended permissions. The **tar** and **cpio** commands do not backup the extended permissions, and thus, cannot restore them.[18] To pass this test, the restored files must include the extended permissions.

3. Interview operational personnel to test their understanding of backup procedures thus ensuring compliance with written procedures. The IT Department passes this test if each person interviewed is able to accurately state what they are required to do as defined in the backup procedure.

4. Inspect the locations where backup tapes are kept to ensure that the tapes are

[17] http://publib.boulder.ibm.com/infocenter/pseries/index.jsp?topic=/com.ibm.aix.doc/aixbman/security/network_services.htm (15 march 2005)

[18] Michael, Randal K., p. 508

physically protected and environmentally safe. The IT department passes this test if tapes are locked in a vault/area with controlled access and there are no observable contaminants (heat, water, chemicals, magnets) that could damage the tapes.

5. Inventory the physical backup media and reconcile the count with the Inventory Master Report to ensure that all backup media are accounted for. The physical count includes both onsite and offsite locations. The IT Department passes this test if all tapes listed on the Inventory Master Report are accounted for when the tapes are physically counted and there are no additional labeled tapes found that are not listed in the report. Failure to reconcile inventory may indicate that one or more tapes are lost or that procedures for creating inventory records are not being followed. Tapes that can be easily "borrowed" without creating a tracking record might be copied and restored to another system.

Once the auditors completed their review of the IBM AIX server backup procedures and the testing, the auditors proceeded with a review of the AIX server BCP. The auditor's created a checklist of the items a BCP plan should have and compared the checklist with the actual plan to identify any missing elements. Appendix G contains the auditor's BCP checklist. Once the checklist was complete, the auditor's performed the following tests:

6. Verified that the points of contact were accurate (employee names, telephone numbers, page numbers, and email addresses). The auditor's sent an email to each employee listed in the BCP requesting them to verify the data. The IT Department passes this test if at least 95% of all contact information is correct.

7. Verified that each employee listed in the BCP had a copy of the plan. The IT Department passes this test if at least 95% of the employees questioned confirm that they have the current version of the BCP.

8. Tested employee's knowledge of the plan by comparing the answers to interview questions with the documented plan. The IT Department passes this test if the people interviewed are able to accurately state their responsibilities as documented in the BCP.

# 5. System Auditing

## 5.1 Configuration/Patch Management Audit Results

The auditors found that the AIX server has the latest Maintenance Level and APRs installed. The Nessus scan results indicate that the open source software Apache and OpenSSL are not the latest versions. Appendix J contains the scan results. Appendix H contains the work papers that describe the tests performed. A further review determined that the latest version of Apache, version 1.3.33 is not installed.[19] However, the version is not as old as suggested by the scan results. The patch procedures for Oracle include an upgrade of Apache. However, the Apache banner is not updated. The Nessus scan results are false positives. The auditors recommend that the IT Department either upgrade to the latest version of Apache 1.3.x or consider the latest version of Apache 2 (2.0.53).

## 5.2 File Integrity Audit Results

Based on the file integrity tests, the auditors believe that the AIX operating system files are secure. Checksums and file sizes listed in the TCB configuration file, **/etc/security/syschk.cfg,** match those values computed for these files. However, the open source programs do not include stanzas in the TCB configuration file. The auditors recommend that stanzas for open source program files be added to the TCB configuration file to track file sizes and checksums, ensuring that the integrity of these files is preserved.

The auditors found one unnecessary service running on the AIX server, XDMCP, reported by Nessus. The IT Department acknowledged this as an oversight. The service is related to X-Window, which is not used.

All unknown processes running on open ports were initiated by RPC. The programs requesting port assignments are valid programs.

TCP Wrappers is installed and configured to permit only internal IP addresses to run inetd services.

All of the user accounts have passwords and stanzas in the **/etc/security/passwd, /etc/security/user,** and **/etc/security/limits** files. Only the two AIX system administrators have **admin** and **su** privileges. All user accounts are limited in terms of the system resources the processes they run can consume.

[19] http://httpd.apache.org/download.cgi (15 March 2005)

The auditors questioned the AIX system administrators regarding the possible use of Tripwire, a commercial tool used to ensure file integrity.[20] The auditors were informed that Tripwire was considered. However, due to budget limitations, discussion was put on hold. The AIX server is accessible by internal IP addresses only. User accounts are tightly controlled and user activity monitored. There are only two individuals with administrator rights. Background checks were conducted and duties are rotated. Although Tripwire would provide additional security, it was necessary to fund other priorities.

The AIX system administrators are considering porting the freeware version of Tripwire to the AIX system assuming funds for the commercial version are not available this year.[21] Another alternative is the software Advanced Intrusion Detection Environment (AIDE). This software also provides file integrity.[22]

Based on a review of the user accounts, the auditors believe that users are not granted excess rights that could be used to compromise file integrity. Extended permissions are set to deny members of the Accounting and Sales groups from accessing each others' files. Assuming the Marketing Department agrees to host their application on the IT Department's AIX server, similar ACLs can be created.

## 5.3 Backup/Business Continuity Planning Audit Results

The auditors successfully restored test files from a backup tape. The extended permissions for the test files were restored as well. A physical inspection of the onsite and offsite storage locations indicated that physical access to the backup tapes is restricted and that environmental controls are satisfactory. Inventory reconciliation matched the physical tape count with the master inventory tape list.

The auditors found that several individuals needed to have their contact information (phone numbers, pager numbers, personal email addresses) updated. A review of the BCP indicates a comprehensive document that identifies possible scenarios, roles and responsibilities, restoration priorities, and procedures for accomplishing specific tasks.

The BCP as a whole is updated annually. The auditors recommend that the contact list be reviewed and updated quarterly and replacement pages issued if necessary. In addition, the auditors recommend that summary flowcharts be added to the detailed procedures. Such flowcharts can be quickly scanned by individuals familiar with the plan. When time is the critical factor, a visual aide may save time.

[20] http://www.tripwire.com/practices/index.cfm (15 March 2005)

[21] http://www.tripwire.org (15 March 2005)

[22] http://sourceforge.net/projects/aide/ (15 March 2005)

# 6. References

This section provides a list of references used in developing this document.

1. Hiles, Andrew. Business Continuity: Best Practices
   Rothstein Associates, Inc. Connecticut, 2004

2. Michael, Randal K. AIX 5L Administration,
   McGraw-Hill/Osborne, New York, 2002

3. Roessing, Rolf von. Auditing Business Continuity
   Rothstein Associates Inc. Connecticut, 2003

4. IBM Publications
   "AIX 5L Version 5.3 Security Guide"
   August 2004
   URL:
   http://publib.boulder.ibm.com/infocenter/pseries/topic/com.ibm.aix.doc/aixbman/security/security.pdf (15 March 2005)

5. IBM Redbooks
   "Additional AIX Security Tools on IBM eServer, pSeries, IBM RS/6000 and SP/Cluster"
   December 2000
   URL: http://www.redbooks.ibm.com/redbooks/pdfs/sg245971.pdf
   (15 March 2005)

6. IBM Redbooks
   "Managing AIX Server Farms"
   June 2002
   URL: http://www.redbooks.ibm.com/redbooks/pdfs/sg246606.pdf
   (15 March 2005)

7. IBM whitepaper
   "Strengthening AIX Security: A System-Hardening Approach"
   March 2002
   URL: http://www-1.ibm.com/servers/aix/whitepapers/aix_security.pdf
   (15 March 2005)

8. IBM Redbook
   "Accounting and Auditing on AIX"
   October 2000
   URL: http://www.redbooks.ibm.com/redbooks/pdfs/sg246020.pdf
   (15 March 2005)

9. Defense Information Systems Agency (DISA)
"UNIX Security Technical Implementation Guide"
Version 4 Release 4
September 15, 2003
URL: http://www.disa.mil (15 March 2005)

10. NIST Special Publication 800-34
"Contingency Planning Guide for Information Technology Systems"
URL: http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf
(15 March 2005)

11. NIST Special Publication 800-40
"Procedures for Handling Security Patches"
URL: http://csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf
(15 March 2005)

12. NIST ICAT Vulnerability database
URL: http://icat.nist.gov
(15 March 2005)

13. Mitre Common Vulnerabilities and Exposures Database
URL: http://cve.mitre.org
(15 March 2005)

14. SecurityFocus Bugtraq Database
URL: http://www.securityfocus.com
(15 March 2005)

15. Secunia Vulnerability Database
URL: http://www.secunia.com
(15 March 2005)

16. The Disaster Recovery Institute International
URL: http://www.drii.org

# A. Appendix: IBM AIX System Services

The table of IBM AIX system services begins on the next page.

Information in this table was taken from the IBM AIX 5L version 5.3 Security Guide, Appendix C which is listed as Reference 4 in Section 6 of this document.

Following the table is a brief description of each inetd, inittab, NFS, and TCP/IP service including an explanation as to why the service is disabled. Any exception, where the service is enabled, is noted.

| Service | Daemon | Started by | Function | Enabled / Disabled |
|---|---|---|---|---|
| | | | | |
| inetd/bootps | inetd | /etc/inetd.conf | Bootp services to diskless clients | Disabled |
| inetd/chargen | inetd | /etc/inetd.conf | Character generator | Disabled |
| inetd/cmsd | inetd | /etc/inetd.conf | Calendar service used by CDE | Disabled |
| inetd/comsat | inetd | /etc/inetd.conf | Notifies incoming electronic mail | Disabled |
| inetd/daytime | inetd | /etc/inetd.conf | Obsolete time service | Disabled |
| inetd/discard | inetd | /etc/inetd.conf | /dev/null service | Disabled |
| inetd/dtspc | inetd | /etc/inetd.conf | CDE subprocess control | Disabled |
| inetd/echo | inetd | /etc/inetd.conf | Echo service | Disabled |
| inetd/exec | inetd | /etc/inetd.conf | Remote execution | Disabled |
| inetd/finger | inetd | /etc/inetd.conf | Finger service | Disabled |
| inetd/ftp | inetd | /etc/inetd.conf | File transfer protocol | Disabled |
| inetd/imap2 | inetd | /etc/inetd.conf | Internet Mail Access Protocol | Enabled |
| inetd/klogin | inetd | /etc/inetd.conf | Kerberos login | Disabled |
| inetd/kshell | inetd | /etc/inetd.conf | Kerberos shell | Disabled |
| inetd/login | inetd | /etc/inetd.conf | rlogin service | Disabled |
| inetd/netstat | inetd | /etc/inetd.conf | Network status | Disabled |
| inetd/ntalk | inetd | /etc/inetd.conf | Allows users to talk to each other | Disabled |

| | | | | |
|---|---|---|---|---|
| inetd/pcnfsd | inetd | /etc/inetd.conf | PC NFS file services | Disabled |
| inetd/pop3 | inetd | /etc/inetd.conf | Post Office Protocol | Disabled |
| inetd/quotad | inetd | /etc/inetd.conf | NFS File quota reporting | Disabled |
| inetd/rexd | inetd | /etc/inetd.conf | Remote execution | Disabled |
| inetd/rstatd | inetd | /etc/inetd.conf | Kernel statistics server | Disabled |
| inetd/rusersd | inetd | /etc/inetd.conf | Information about user logged in | Disabled |
| inetd/rwalld | inetd | /etc/inetd.conf | Write to all users | Disabled |
| inetd/shell | inetd | /etc/inetd.conf | rsh service | Disabled |
| inetd/sprayd | inetd | /etc/inetd.conf | RPC spray tests | Disabled |
| inetd/systat | inetd | /etc/inetd.conf | ps –ef status report | Disabled |
| inetd/talk | inetd | /etc/inetd.conf | Split screen | Disabled |
| inetd/telnet | inetd | /etc/inetd.conf | telnet service | Disabled |
| inetd/tftp | inetd | /etc/inetd.conf | Trivial file transfer | Disabled |
| inetd/time | inetd | /etc/inetd.conf | Obsolete time service | Disabled |
| inetdd/ttdbserver | inetd | /etc/inetd.conf | Tool-talk database server CDE | Disabled |
| inetd/uucp | inetd | /etc/inetd.conf | UUCP network | Disabled |
| inittab/dt | init | /etc/rc.dt script in /etc/inittab | Desktop login CDE | Disabled |
| inittab/dt_nogb | init | /etc/inittab | Desktop login to CDE | Disabled |
| inittab/httpdlite | init | /etc/inittab | Web server for docsearch | Disabled |

| | | | | |
|---|---|---|---|---|
| inittab/i4ls | init | /etc/inittab | License manager servers | Disabled |
| inittab/imqss | init | /etc/inittab | Search engine for docsearch | Disabled |
| inittab/lpd | init | /etc/inittab | BSD line printer | Disabled |
| inittab/nfs | init | /etc/inittab | Network File System | Enabled |
| inittab/piobe | init | /etc/inittab | Printer IO Back End | Disabled |
| inittab/qdaemon | init | /etc/inittab | Queue daemon for printing | Enabled |
| inittab/uprintfd | init | /etc/inittab | Kernel messages | Disabled |
| inittab/writesrv | init | /etc/inittab | Writing notes to ttys | Enabled |
| inittab/xdm | init | /etc/inittab | X11 Display management | Disabled |
| rc.nfs/automountd | | /etc/rc.nfs | Automatic file systems | Enabled |
| rc.nfs/biod | | /etc/rc.nfs | Block IO Daemon (NFS) | Enabled |
| rc.nfs/keyserv | | /etc/rc.nfs | Secure RPC key server | Disabled |
| rc.nfs/nfsd | | /etc/rc.nfs | NFS services | Disabled |
| rc.nfs/rpc.lockd | | /etc/rc.nfs | NFS file locks | Enabled |
| rc.nfs/rpc.mountd | | /etc/rc.nfs | NFS file mounts | Disabled |
| rc.nfs/rpc.statd | | /etc/rc.nfs | NFS file locks recover | Disabled |
| rc.nfs/rpc.yppasswdd | | /etc/rc.nfs | NIS password daemon | Disabled |
| rc.nfs/ypupdated | | /etc/rc.nfs | NIS Update daemon | Disabled |
| rc.tcpip/autoconf6 | | /etc/rc.tcpip | Ipv6 Interfaces | Disabled |
| rc.tcpip/dhcpcd | | /etc/rc.tcpip | Dynamic Host Configuration Protocol Client | Disabled |

| | | | | |
|---|---|---|---|---|
| rc.tcpip/dhcprd | | /etc/rc.tcpip | Dynamic Host Configuration Protocol relay | Disabled |
| rc.tcpip/dhcpsd | | /etc/rc.tcpip | Dynamic Host Configuration Protocol server | Disabled |
| rc.tcpip/dpid2 | | /etc/rc.tcpip | Outdated SNMP service | Disabled |
| rc.tcpip/gated | | /etc/rc.tcpip | Gated routing between interfaces | Disabled |
| rc.tcpip/inetd | | /etc/rc.tcpip | Inetd services | Enabled |
| rc.tcpip/mrouted | | /etc/rc.tcpip | Multi-cast routing | Disabled |
| rc.tcpip/names | | /etc/rc.tcpip | DNS name server | Disabled |
| rc.tcpip/ndp-host | | /etc/rc.tcpip | IPv6 host | Disabled |
| rc.tcpip/ndp-router | | /etc/rc.tcpip | IPv6 routing | Disabled |
| rc.tcpip/portmap | | /etc/rc.tcpip | RPC services | Enabled |
| rc.tcpip/routed | | /etc/rc.tcpip | RIP routing between interfaces | Disabled |
| rc.tcpip/rwhod | | /etc/rc.tcpip | Remote who daemon | Disabled |
| rc.tcpip/sendmail | | /etc/rc.tcpip | Mail services | Enabled |
| rc.tcpip/snmpd | | /etc/rc.tcpip | Simple Network Management Protocol | Enabled |
| rc.tcpip/syslogd | | /etc/rc.tcpip | System log events | Enabled |
| rc.tcpip/timed | | /etc/rc.tcpip | Old Time Daemon | Disabled |
| rc.tcpip/xntpd | | /etc/rc.tcpip | New Time Daemon | Disabled |
| dt login | | /usr/dt/config/Xaccess | Unrestricted CDE | Disabled |

|  |  |  |  |  |
|---|---|---|---|---|
| root.access |  | /etc/security/user | rlogin/telnet to root account | Disabled |
| snmp.readWrite |  | /etc/snmpd.conf | SNMP read write communities | Enabled<br>Modified for public, requires a special password |

## A description of inetd services

Refer to the following IBM URL for more information including service options: http://publib.boulder.ibm.com/infocenter/pseries/index.jsp?topic=/com.ibm.aix.doc/cmds/aixcmds3/inetd.htm
(15 March 2005)

The **bootps** provides bootp services to diskless clients. This service is disabled as the ABC Financial Corporation desktop standard does not include diskless workstations.

The **chargen** command is used to echo back a character stream. This service may be run as either a TCP or a UDP service. The service could be run to create a denial of service.

The **cmsd** service is a calendar service used by the Common Desktop Environment (CDE) a GUI.

The **comsat** service is a server process which listens for reports of incoming mail and notifies users who have requested to be told when mail arrives. The service is obsolete.

The **daytime** command calculates the time by the number of seconds since midnight January 1, 1900. The command is similar to the **time** command. The output of the **daytime** command is in human readable form. The **daytime** command can be used to identify that the server is running the AIX operating system.

The **discard** service as its name indicates tosses anything it receives. The service is not required and may be used to consume sockets in a denial of service attack.

The **dtspc** service provides CDE sub process control. The service is started in response to a CDE client requesting a CDE service on the server. This service is not required.

The **echo** service sends back to the originating source any data it receives. This service may be used to create a denial of service. An attacker could spoof a source IP address.

The **exec** service is the remote execution service. The user enters an account and password that are passed in the clear.

The **fingerd** service daemon makes personal information available to users on the network. Hackers use this feature to obtain and exploit information about users and to help obtain unauthorized access to accounts. The syntax is simple: A user enters the command —**finger user@host**. The output contains information about the user.

The **ftpd** file transfer protocol daemon permits clear-text password authentication and is replaced by Secure Shell, SSH.

The **imap2** service (Internet Message Access Protocol) service is used for email services. Note: ABC Financial Corporation has enabled this. Several applications issue email alerts.

The **klogin** service is required only if the server runs Kerberos.

The **kshell** service is the Kerberos shell, required only if the server runs Kerberos.

The **login** service daemon establishes a remote login session from one system to another. Users with the same username on both the local and remote machine may **login** from the machines listed in the remote machine's **/etc/hosts.equiv** file without supplying a password. Individual users may set up a similar private equivalence list with the file **.rhosts** in their home directories.

The TCP **netstat** service allows for remote access to the network status of a system.

The **ntalk** service (new talk) runs as root allowing users to talk to each other across the network. This service is disabled.

The **pcnfsd** service daemon is the PC NFS file system daemon. When file sharing with personal computers is required, Samba is typically used. Disable this service.

The **pop3** service (Post Office Protocol) service is used for email services.

The **quotad** is the remote quota daemon. It manages quotas for local file systems mounted on remote systems, and returns the info to the remote system.

The **rexd** service daemon is the remote execution server. It's similar to rlogin and rexec, as it allows a user to remotely execute commands, and for interactive commands spawning a pseudo-terminal to handle the request.

The **rstatd** service daemon is an RPC service that returns performance statistics received from the kernel.

The **rusersd** service daemon can be used to list users who are logged into a remote host.

The **rwalld** is a RPC service which is used to send messages to all terminals which are connected to the system. **rwalld** listens on a port specified by the RPC portmapper, and calls the wall program on the local machine to distribute messages `which` it receives.

The **shell** command connects to a remote host and executes the command specified on that host.

The **sprayd** service daemon sends a one-way stream of packets to *host* using RPC, and reports how many were received, as well as the transfer rate. The *host* argument can be either a name or an Internet address. Spray is not useful as a networking benchmark, as it uses unreliable connectionless transports, UDP for example. Spray can report a large number of packets dropped when the drops were caused by spray sending packets faster than they can be buffered locally, that is, before the packets get to the network medium.

The **sysstat** service allows for remote sites to see the process status on your system. This service is disabled by default.

The **talk** service allows users to remotely connect to a server and initiate talk sessions with resident users. The service is typically not used and has the potential to be exploited.

The **telnet** service permits clear-text password authentication remote access to a system and is replaced by Secure Shell, SSH.

The **tftp** service (trivial file transfer protocol) is a UDP service that has no support for identification and authentication. A Cisco router may be configured to download an image or configuration from a server running this service. Generally, the service is not required.

The **time** service calculates time by the number of seconds since midnight January 1, 1900. The service is generally not used and may be accessed to reveal the operating system that is running on the server.

The **ttdbserver** service is the CDE Tooltalk Database Server. Tooltalk is an integrated application environment, acting as a mediator of communication between applications, and allowing them to exchange data. Tooltalk additionally allows the launching of applications with different respective data types. For example, a .txt file, when double clicked upon, goes to Tooltalk, which in turn launches a text editor. If a hyperlink is contained in this document, clicking upon the hyperlink could additionally launch a web browser, and so forth. Disable this service.

The **uucp** service daemon allows files to be copied from one AIX server to another. The **uuname** command can be used to list systems that **uucp** is aware of.

### Disabled inittab services (unless indicated otherwise)

The **dt** service is used to start the CDE desktop service. This is intended for workstations running CDE and must not be installed on a server. The service is started by the **/etc/rc.dt** script in the file **/etc/inittab**.

The **dt_nogb** service is used to prevent the CDE desktop graphical display from being seen until the service is fully up and running. This service is intended for workstations running CDE and must not be installed on a server.

The **httpdlite** service is a web service used by the documents search engine.

The **i4ls** service is the license manager service. The service is disabled on the ABC Financial Corporation production AIX server.

The **imqss** service is part of the default web server for the documents search engine. The service is disabled.

The **lpd** service is the BSD line printer service. The service accepts print jobs from other systems. The system is still able to submit print jobs if this service is disabled.

The **nfs** service is the Network File System service, a service that provides minimal authentication. Note: ABC Financial Corporation uses NFS but has disabled the components that are not required.

The **piobe** service is the printer IO back end service, which handles the scheduling and spooling of print jobs.

The **qdaemon** service hands print jobs to the **piobe** service.

The **uprintfd** service constructs, formats, converts, and writes kernel messages to processes controlling terminals and is generally not required.

The **writesrv** service writes notes to ttys. This service is used by workstations, not servers. Note: ABC Financial Corporation system administrators enabled this service to communicate among themselves.

The **xdm** service is the X11 display management service for X-Window.

### Disabled NFS Services (unless indicated otherwise)

The **automountd** daemon processes requests from the automatic file systems. This daemon uses local files or name service maps to locate file systems to be mounted. Because the daemon does not verify that requests are actually from the kernel extension, local non-root users and remote users can request automountd services.

The **biod** daemon is the block IO daemon and part of NFS. Note: ABC Financial Corporation has enabled this to support NFS.

The **keyserv** service is the secure RPC key server. This service stores the private encryption key of each user who logs into the system. Keys are decrypted when a user logs in using **keylogin**. The decrypted keys allow users to access services such as NFS. This service must be disabled if NFS and NIS/NIS+ are not enabled. IBM is recommending that customers migrate to LDAP.

The **nfsd** daemon is the NFS (Network File System) daemon that supports shared file systems. Note: ABC Financial Corporation uses NFS.

The **lockd** daemon locks NFS files. Note: ABC Financial Corporation enabled this to support NFS.

The **mountd** daemon performs NFS file mounts.

The **statd** daemon performs NFS file lock recovery.

The **yppasswdd** daemon is the yellow pages password daemon which supports NIS/NIS+ user authentication.

The **ypupdated** daemon is the yellow pages NIS/NIS+ update daemon, which updates information in NIS/NIS+ maps.

### Disabled TCP/IP services (unless indicated otherwise)

The **autoconf6** service supports IPv6, bringing up all IPv6 interfaces when run.

The **dhcpcd** daemon is the Dynamic Host Configuration Protocol (DHCP) client, which attempts to acquire an IP address from a DHCP server. The ABC Financial Corporation AIX server has a static IP Address. The service is not required.

The **dhcprd** daemon is the Dynamic Host Configuration Protocol (DHCP) relay, which forwards BOOTP and DHCP packets off the local subnet. DHCP is a broadcast protocol; packets are restricted to the originating subnet. Forwarding these DHCP packets allows a remote DHCP server to respond to a request for an IP address. This service is disabled as the ABC Financial Corporation AIX server does not function as a DHCP relay server.

The **dhcpsd** is the DHCP server daemon. This service provides IP addresses and configuration information to the requesting DHCP clients.

The **dpid2** is an outdated version of the Simple Network Management Protocol (SNMP).

The **gated** service provides gated routing. Functions are provided for the RIP, RIPng, EGP, BGP, BGP4+, HELLO, IS-IS, ICMP, ICMPv6, and SNMP protocols. The file **/etc/gated.conf** is used to configure the services. AIX hosts can detect when a gateway is down and adjust their routing tables accordingly. AIX servers must not be configured to make routing decisions.

The **inetd** services must be disabled if no RPC services are required. Note: ABC Financial Corporation supports several RPC services, so this is not disabled.

The **mrouted** daemon supports multi-cast routing. This service is disabled.

The **names** service is disabled inasmuch as the ABC Financial Corporation AIX server does not provide Domain Name System (DNS) support.

The **ndp-host** service is related to IPv6 and is disabled.

The **ndp-router** service is related to IPv6 routing and is disabled.

The **portmap** service tracks the services registered by RPC.  Clients requesting an RPC service query the **portmap** service. Note: ABC Financial Corporation's AIX server does support several RPC services, so this is enabled.

The **routed** daemon manages the Routing Internet Protocol (RIP) between interfaces.

The ABC Financial Corporation AIX server does not function as a router.

The **rwhod** daemon is the remote who service collects and broadcasts data to peer servers on the same network.

The **sendmail** service is enabled on the ABC Financial Corporation AIX server to support applications that issue email alerts.

The **snmpd** daemon, Simple Network Management Protocol (SNMP), is used by host management systems to query the status of services running on a server. The default community strings ‘public’ and ‘private’ are changed. The current version of SNMP with all patches is installed. The number of host management systems permitted to query an AIX server is kept to a minimum. The SNMP read/write communities are maintained in the file **/etc/snmpd.conf**. Note: ABC Financial Corporation uses SNMP tools to monitor the AIX system. The service is enabled.

The **syslogd** daemon ensures that system log details as defined in the configuration file **/etc/syslog.conf** are recorded in the syslog. The IT Department requires this service.

The **timed** daemon is an out of date time service for keeping system clocks synchronized. This service is disabled.

The **xntpd** daemon is the New Time daemon used to keep system clocks synchronized. This service must not be enabled on all AIX servers, just those required to provide time services.

The services configured in the **/etc/rc.tcpip** file may be started and stopped by the AIX command **chrctcp**.

# B. Appendix: IBM AIX Server Risk Analysis

Risks are listed in the table beginning on the next page. The table identifies the following:

1. A description of the risk
2. The threat source
3. The likelihood of exploit given the existing countermeasures
4. The Impact should a vulnerability be successfully exploited
5. The risk as a function of likelihood and impact
6. Existing countermeasures

Impact and likelihood are assigned qualitative values using the following scale:

Scale (1-10): Low 1-3, Medium 4-6, High 7-10

A value from 1 to 3 is assigned to a Low Likelihood that a specific vulnerability will be successfully exploited taking into consideration the existing and planned countermeasures. Very Low would be assigned a value of 1.

A value from 4 to 6 is assigned to a Medium Likelihood that a specific vulnerability will be successfully exploited taking into consideration the existing and planned countermeasures.

A value from 7 to 10 is assigned to a High Likelihood that a specific vulnerability will be successfully exploited taking into consideration the existing and planned countermeasures.

A value from 1 to 3 is assigned to a Low Impact taking into consideration the extent of intangible damage (e.g., loss of reputation) and tangible damage (e.g., cost to replace equipment, labor to repair).

A value from 4 to 6 is assigned to a Medium Impact taking into consideration the extent of intangible damage (e.g., loss of reputation) and tangible damage (e.g., cost to replace equipment, labor to repair).

A value from 7 to 10 is assigned to a High Impact taking into consideration the extent of intangible damage (e.g., loss of reputation) and tangible damage (e.g., cost to replace equipment, labor to repair)

The Risk Factor is computed by multiplying the value assigned to the Likelihood and the value assigned to the Impact. This provides a rank (1-100) for each risk, establishing priorities for addressing risk.

| Source | Threat | Likelihood (1-10) | Impact (1-10) | Risk Factor (1-100) | Existing Countermeasures |
|---|---|---|---|---|---|
| | | | | | |
| Missing AIX security patch | Insider | 4 | 8 | 32 | Vendor Notice;<br>Change Control Board;<br>Monthly scan;<br>Quarterly pen test |
| Weak or missing user account passwords; | Insider | 3 | 8 | 24 | Complex passwords are required |
| Compromised passwords | Insider | 4 | 6 | 24 | Employee exit procedures;<br>Policy against password sharing;<br>Periodic password change requirements;<br>Log file review |
| Default Vendor user accounts and passwords | Insider<br>Outside hacker | 2 | 8 | 16 | Account review procedures |
| Excess user rights | System administrators | 5 | 6 | 30 | Creation of groups;<br>Assignment of users to groups;<br>Log file review |

| | | | | | |
|---|---|---|---|---|---|
| Vulnerable AIX service | Insider | 4 | 8 | 32 | Disable unnecessary services;<br>Apply patches |
| Vulnerable AIX TCP/IP configuration | Insider;<br>Outside hacker | 4 | 8 | 32 | AIX TCP/IP hardened Stack;<br>TCP Wrappers;<br>Packet filtering router;<br>Stateful firewall;<br>IDS |
| Invalid Tape Backups | IT operations Personnel error | 2 | 10 | 20 | Backup Log review;<br>Scheduled Testing;<br>Rotation of assigned backup personnel |
| Failure of Environmental Controls (air conditioning, power, fire/water detection) | Facility Maintenance personnel error | 2 | 9 | 18 | Scheduled inspections;<br>Server UPS;<br>Backup Generator;<br>Smoke alarms;<br>Water detection sensors |

| | | | | | |
|---|---|---|---|---|---|
| Hardware failure | Faulty component | 4 | 7 | 28 | Fault Tolerance (RAID drives);<br>Redundant power supplies;<br>Scheduled preventive maintenance |
| Physical Security | Security Office personnel error;<br>Criminal theft;<br>Insider theft | 2 | 9 | 18 | Guards;<br>Identity badges;<br>Key coded access;<br>Security cameras;<br>Scheduled equipment maintenance |
| File Integrity compromise | Insider;<br>Outside hacker | 2 | 10 | 20 | Trusted Computing Base;<br>File checksums |
| Inadequate contingency plan | Nature (flood, storm, lightning);<br>Accident (fire, structure collapse, pipe burst, power surge) | 1 | 10 | 10 | Periodic plan review and audit;<br>Periodic plan testing and revision |
| Logic Bomb | Programmer staff | 3 | 9 | 27 | Code Inspection and review;<br>Separation of duties (development from production) |
| Trojan Software | Malicious web sites | 2 | 9 | 18 | Validate vendor patch checksums |

## C. Appendix: IBM AIX 5L version 5.3 Vulnerabilities

The table on the following page was created by querying the Mitre CVE database for IBM AIX 5L version 5.3 vulnerabilities and copying the results. As of the date of this paper, Mitre reports seven known vulnerabilities.

The Mitre CVE database is found at URL: http://www.mitre.org
(15 March 2005)

The second page of this Appendix was created by querying the NIST ICAT vulnerability database selecting IBM as the vendor, AIX as the product, and 5.3 L as the version. The results were copied.

**Note:** Selection criteria are important in identifying the relevant vulnerabilities. Choosing 5.3 L as the version provided two vulnerabilities. Choosing 5.3 as the version provided twenty-four vulnerabilities. Version 5.3 L is the correct version for this project.

The NIST ICAT database is found at URL: http://icat.nist.gov
(15 March 2005)

The Secunia Vulnerability database results for AIX 5.3 follows. This database is available at URL: http://www.secunia.com
(15 March 2005)

**CVE version: 20040901**

URL: http://cve.mitre.org (15 March 2005)

| Name | Description |
|---|---|
| CAN-2004-0828 | The ctstrtcasd program in RSCT 2.3.0.0 and earlier on IBM AIX 5.2 and 5.3 does not properly drop privileges before executing the -f option, which allows local users to modify or create arbitrary files. |
| CAN-2004-1329 | Untrusted execution path vulnerability in the diag commands (1) lsmcode, (2) diag_exec, (3) invscout, and (4) invscoutd in AIX 5.1 through 5.3 allows local users to execute arbitrary programs by modifying the DIAGNOSTICS environment variable to point to a malicious Dctrl program. |
| CAN-2004-1330 | Buffer overflow in paginit in AIX 5.1 through 5.3 allows local users to execute arbitrary code via a long username. |
| CAN-2005-0250 | Format string vulnerability in auditselect on IBM AIX 5.1, 5.2, and 5.3 allows local users to execute arbitrary code via format string specifiers in a command line argument. |
| CAN-2005-0261 | lspath in AIX 5.2, 5.3, and possibly earlier versions, does not drop privileges before processing the -f option, which allows local users to read one line of arbitrary files. |
| CAN-2005-0262 | Buffer overflow in ipl_varyon on AIX 5.1, 5.2, and 5.3 allows local users to execute arbitrary code via a long -d argument. |
| CAN-2005-0263 | Buffer overflow in netpmon on AIX 5.1, 5.2, and 5.3 allows local users to execute arbitrary code via a long -O argument. |

### NIST ICAT Database for IBM AIX 5.3 vulnerabilities

URL: http://icat.nist.gov (15 March 2005)

There are **2** matching records. Displaying matches **1** through **2**.

**CAN-2004-1054**

| | |
|---|---|
| ***Summary:*** | Untrusted execution path vulnerability in invscout in IBM AIX 5.1.0, 5.2.0, and 5.3.0 allows local users to gain privileges by modifying the PATH environment variable to point to a malicious "uname" program, which is executed from lsvpd after lsvpd has been invoked by invscout. |
| ***Published Before:*** | 1/10/2005 |
| ***Severity:*** | High |

**CAN-2004-1028**

| | |
|---|---|
| ***Summary:*** | Untrusted execution path vulnerability in chcod on AIX IBM 5.1.0, 5.2.0, and 5.3.0 allows local users to execute arbitrary programs by modifying the PATH environment variable to point to a malicious "grep" program, which is executed from chcod. |
| ***Published Before:*** | 1/10/2005 |
| ***Severity:*** | High |

### Secunia IBM AIX 5.3 Advisories 2005

This table was copied from URL: http://secunia.com/product/213/
(15 March 2005)

**2005 - 7 Secunia Advisories**

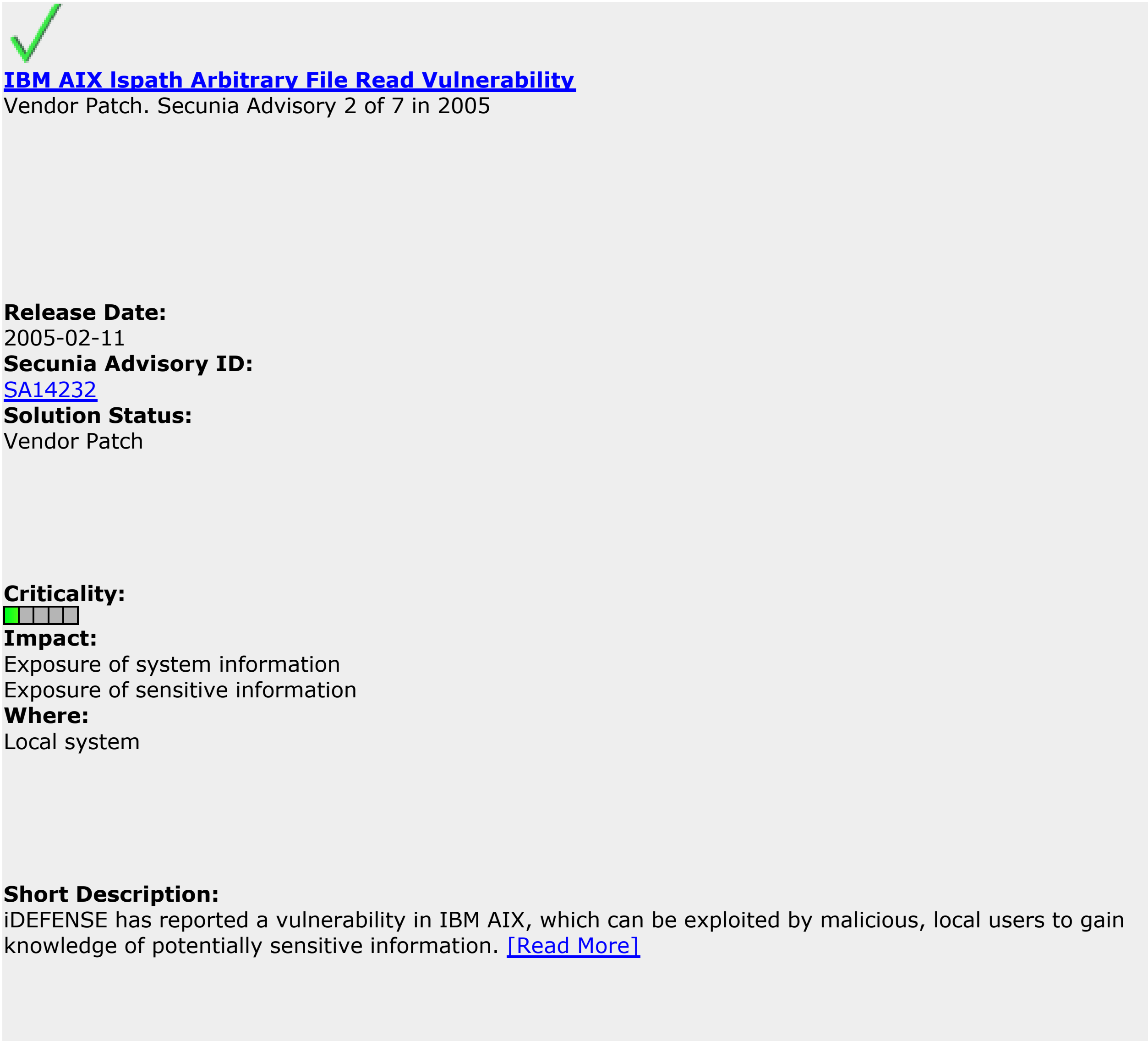
✓

**IBM AIX Perl Interpreter Privilege Escalation Vulnerabilities**
Vendor Patch. Secunia Advisory 1 of 7 in 2005

**Release Date:**
2005-02-21
**Secunia Advisory ID:**
SA14345
**Solution Status:**
Vendor Patch

**Criticality:**
🟩🟩⬜⬜⬜
**Impact:**
Privilege escalation
**Where:**
Local system

**Short Description:**
IBM has acknowledged two vulnerabilities in the perl interpreter in AIX. These can be exploited by malicious, local users to gain escalated privileges. [Read More]



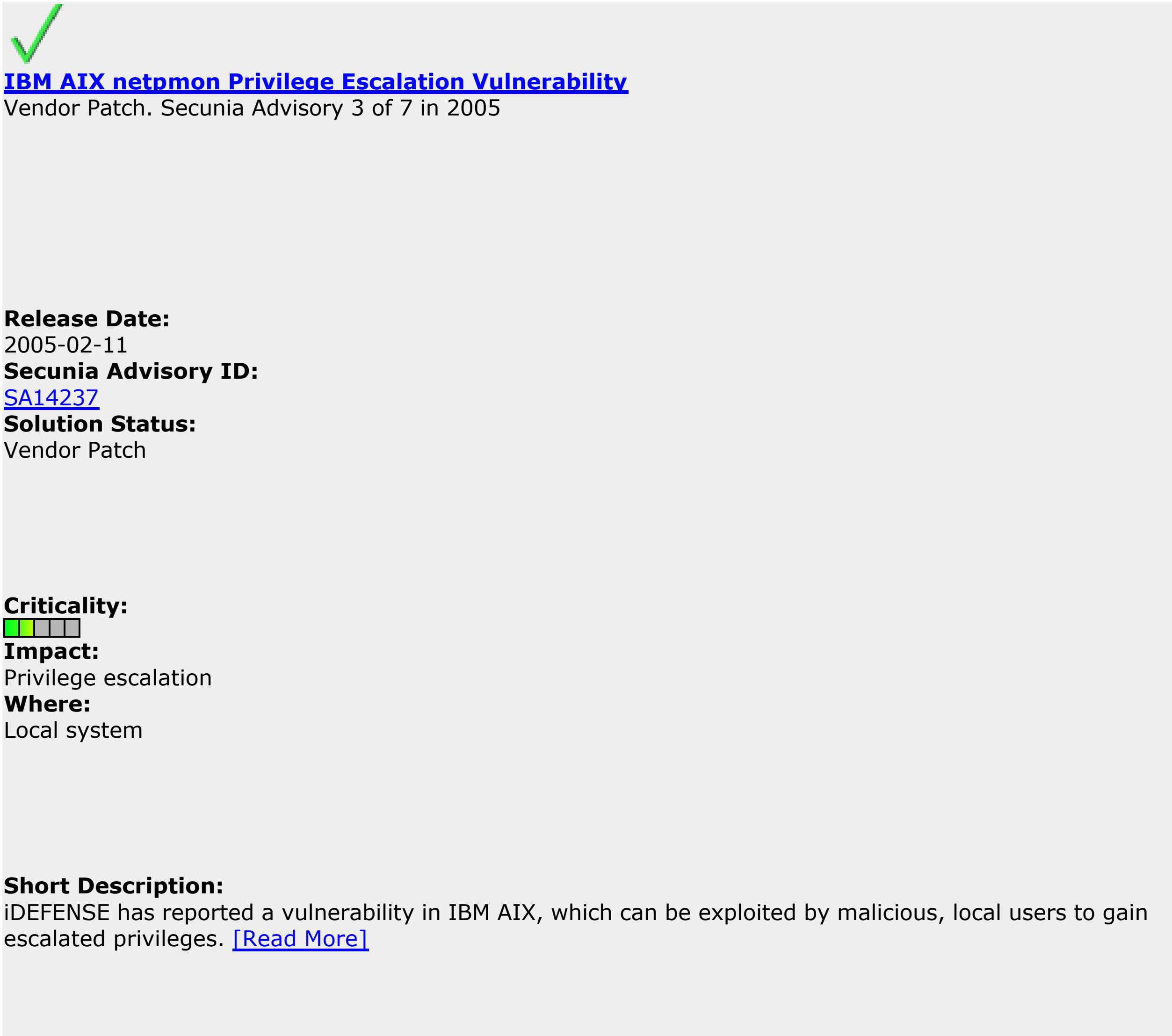
✓

**IBM AIX lspath Arbitrary File Read Vulnerability**
Vendor Patch. Secunia Advisory 2 of 7 in 2005

**Release Date:**
2005-02-11
**Secunia Advisory ID:**
SA14232
**Solution Status:**
Vendor Patch

**Criticality:**
🟩▨▨▨▨
**Impact:**
Exposure of system information
Exposure of sensitive information
**Where:**
Local system

**Short Description:**
iDEFENSE has reported a vulnerability in IBM AIX, which can be exploited by malicious, local users to gain knowledge of potentially sensitive information. [Read More]



✓

IBM AIX netpmon Privilege Escalation Vulnerability
Vendor Patch. Secunia Advisory 3 of 7 in 2005

**Release Date:**
2005-02-11
**Secunia Advisory ID:**
SA14237
**Solution Status:**
Vendor Patch

**Criticality:**
🟩🟩⬜⬜⬜
**Impact:**
Privilege escalation
**Where:**
Local system

**Short Description:**
iDEFENSE has reported a vulnerability in IBM AIX, which can be exploited by malicious, local users to gain escalated privileges. [Read More]

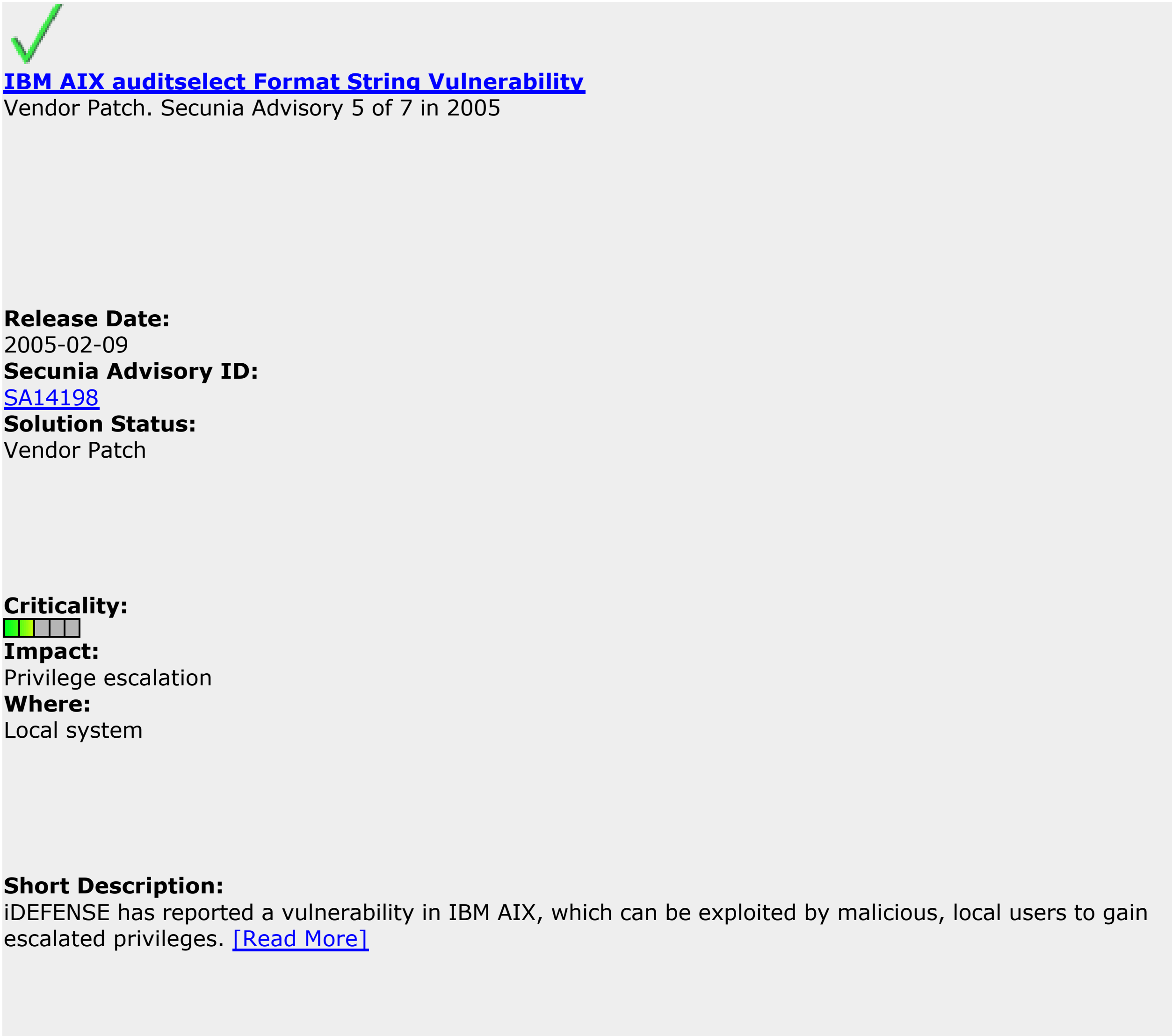
✓

**IBM AIX ipl_varyon Privilege Escalation Vulnerability**
Vendor Patch. Secunia Advisory 4 of 7 in 2005

**Release Date:**
2005-02-11
**Secunia Advisory ID:**
SA14231
**Solution Status:**
Vendor Patch

**Criticality:**
🟩🟩⬜⬜⬜
**Impact:**
Privilege escalation
**Where:**
Local system

**Short Description:**
iDEFENSE has reported a vulnerability in IBM AIX, which can be exploited by malicious, local users to gain escalated privileges. [Read More]



✓

**IBM AIX auditselect Format String Vulnerability**
Vendor Patch. Secunia Advisory 5 of 7 in 2005

**Release Date:**
2005-02-09
**Secunia Advisory ID:**
SA14198
**Solution Status:**
Vendor Patch

**Criticality:**
🟩🟩⬜⬜⬜
**Impact:**
Privilege escalation
**Where:**
Local system

**Short Description:**
iDEFENSE has reported a vulnerability in IBM AIX, which can be exploited by malicious, local users to gain escalated privileges. [Read More]

✓

**IBM AIX chdev/mkdev/rmdev Format String Vulnerability**
Vendor Patch. Secunia Advisory 6 of 7 in 2005

**Release Date:**
2005-02-08
**Secunia Advisory ID:**
SA14173
**Solution Status:**
Vendor Patch

**Criticality:**
🟩🟩⬜⬜⬜
**Impact:**
Privilege escalation
**Where:**
Local system

**Short Description:**
iDEFENSE has reported a vulnerability in AIX, which can be exploited by malicious, local users to gain escalated privileges. [Read More]

✓

**AIX Unspecified NIS Client System Compromise Vulnerability**
Vendor Patch. Secunia Advisory 7 of 7 in 2005

**Release Date:**
2005-02-01
**Secunia Advisory ID:**
SA14095
**Solution Status:**
Vendor Patch

**Criticality:**
🟩🟩🟨⬜⬜
**Impact:**
Privilege escalation
System access
**Where:**
From local network

**Short Description:**
A vulnerability has been reported in AIX, which can be exploited by malicious people to compromise a vulnerable system. [Read More]

# D. Appendix: Configuration – Patch Management Change Control Form

A sample Configuration Patch Management Change Control Form is provided on the next page. The form is completed by a systems administrator and submitted to a Change Control Board for approval. The form is part of the permanent system documentation.

# CONFIGURATION PATCH CHANGE PROPOSAL (CPCP)
# (INFORMATION)

**This CPCP form is used for sharing information on new requirements, modifications or enhancements, and upgrades to current Operating Communities within the ABC Financial Corporation Information Technology (IT) Department. These "Information" CPCPs will be distributed to members of the Change Control Board (CCB) for review, information, and distribution. If this CPCP has any IMPACT on your area; RETURN it to the CM Secretariat ASAP to be reentered as a controlled "RED" CPCP.**

| | | |
|---|---|---|
| **Date/Time Submitted:** | **Date/Time Cleared:** | CPCP Request Number |

**Submitter/Organization/Phone:**

**Proposal Manager/Phone:**

**Title:**

**Description: (Include software/hardware/systems involved. Provide as much details as possible)**

**Summary of Changes:**

**Impact Statement:**

**Test Results on non-production server:**

**Alternative Strategy:**

**Recovery Procedures and Plans:**

**Additional Information:**

## E. Appendix: Document Call Checklist

The following page contains a form used by the ABC Financial Corporation Internal Auditors to collect and track documentation received from the IT Department. A check in the ‘Yes’ column indicates that the document was received. A check in the ‘No’ column indicates that the document does not exist. This may indicate a deficiency. A check in the ‘N/A’ column indicates that the document is not applicable to the specific engagement and was not requested. The Comments column is used by the auditor for any special notes such as indicating the completeness of the document received.

**Document Call Checklist**

| | |
|---|---|
| System | IBM AIX Server |
| Department | Information Technology (IT) |
| Reviewer | A. Smith |
| Date | 15 March 2005 |

| Document Name | Yes | No | N/A | Comments |
|---|---|---|---|---|
| | | | | |
| IT Organization Chart | X | | | |
| Mission Statement | X | | | |
| | | | | |
| Standard Operating Procedures: | | | | |
| User Account Creation | X | | | |
| User Account Termination | X | | | |
| Password Change Request | X | | | |
| Use of root account | X | | | |
| Configuration/Patch Mngt. | X | | | |
| Backup / Recovery | X | | | |
| Capacity Management | | | X | |
| Performance Management | | | X | |
| Preventive Maintenance | | | X | |
| Log File Review | X | | | |
| Incident Handling | X | | | |
| Emergency Shutdown | X | | | |
| | | | | |
| | | | | |
| CPCP Forms | X | | | All forms for prior 6 months were reviewed |
| | | | | |
| Risk Analysis | X | | | |
| Business Contingency Plan | X | | | |
| | | | | |
| Programming: | | | | |
| System Flow Charts | | | X | |
| Data Flow Diagrams | | | X | |
| Database ERD Diagrams | | | X | |
| Software Standards | | | X | |
| User Manuals | | | X | |
| | | | | |

|  |  |  |  |  |
|---|---|---|---|---|
| **Network Diagram** | X |  |  |  |

## F. Appendix: Server Backup Questionnaire

The survey questions the auditors asked the operational and technical personnel are listed on the next page.

**Server Backup Questionnaire**

1. Please identify the hardware used to perform the server backup. Include any hardware configuration settings.
2. Please identify the software used to perform the server backup. Include any software configuration settings, i.e., compression, encryption.
3. Please provide the update procedures for implementing any patches or new versions of the backup software.
4. Please provide information regarding the media used in the backup process, tapes, cartridges, and/or tape libraries. Is the media approved by the hardware and software vendors?
5. Please provide the media formatting and labeling procedures.
6. Please provide the media rotation, replacement, and archiving procedures.
7. Please provide the media sanitization procedures.
8. Please provide the onsite media handling and storage procedures.
9. Please provide the offsite media handling and storage procedures.
10. Please provide a physical inventory of backup media.
11. Please provide a copy of procedures for maintaining an inventory of backup media.
12. Please provide a copy of the Service Level Agreement for each department that maintains an application on the server.
13. Please provide a list of the volumes that are backed up.
14. Please provide a copy of the backup schedule.
15. Please provide information as to the type of backups performed, i.e., full, differential, incremental.

16. Please provide a copy of the test procedures used to validate the backup media.

17. Please provide a copy of the procedures used to provide file and/or directory restoration.

18. Please provide a copy of the procedures for reviewing the backup log.

19. Please provide a copy of the backup failure procedures including notification procedures and alternative backup plans.

## G. Appendix: Business Plan Continuity Checklist

The checklist begins on the next page. This checklist is used to compare an actual BCP to determine if there are any missing items that would hinder the success of the plan.

A check in the 'Yes' column indicates that the element exists in the actual BCP.  A check in the 'No' column indicates that the element does not exist in the BCP. This may indicate a deficiency. A check in the 'N/A' column indicates that the element is not applicable to the specific BCP. The Comments column is used by the auditor for any special notes such as whether the element is covered in sufficient detail.

Following the checklist is a definition of the items listed in the checklist.

**Contingency Plan Document**

| | |
|---|---|
| **System** | **IBM AIX Server** |
| **Department** | **IT Department** |
| **Reviewer** | **CRJ** |
| **Date** | **03/15/05** |

| **Element** | **Yes** | **No** | **N/A** | **Reviewer's Comments** |
|---|---|---|---|---|
| | | | | |
| **Plan Execution:** | | | | |
| Activation events defined | **X** | | | |
| De-activation defined | **X** | | | |
| Recovery priorities defined | **X** | | | |
| Maximum allowed outage defined | **X** | | | |
| Individual(s) authorized to activate plan identified | **X** | | | |
| Line of succession defined | **X** | | | |
| Assumptions stated | **X** | | | |
| Plan risks identified | **X** | | | |
| Roles & Responsibilities defined | **X** | | | |
| Points of Contact Listed: | **X** | | | 2 Individuals of the sixty surveyed needed to have contact information updated in the BCP. |
| Work Phone | **X** | | | |
| Home Phone | **X** | | | |
| Cell Phone | **X** | | | |
| Work email address | **X** | | | |
| Personal email address | **X** | | | |
| Vendor Contacts listed | **X** | | | |
| Alternate facility location(s) identified | **X** | | | |
| Spare Equipment location(s) identified | **X** | | | |
| Backup records location(s) identified | **X** | | | |
| Management Team identified | **X** | | | |
| Emergency Evacuation Team identified | **X** | | | |
| Assessment Team identified | **X** | | | |
| Salvage Team identified | **X** | | | |

| | | | | |
|---|---|---|---|---|
| Public Relations and Media Team identified | **X** | | | Users need specific training to refer questions from the media to public relations |
| Alternate Facility Team identified | **X** | | | |
| Transportation Team identified | **X** | | | |
| Telecommunications Recovery Team identified | **X** | | | |
| Network Recovery Team identified | **X** | | | |
| Server Recovery Team identified | **X** | | | |
| Application Recovery Team identified | **X** | | | |
| Desktop Recovery Team identified | **X** | | | |
| Records Retrieval Team identified | **X** | | | |
| Security Team identified | **X** | | | |
| | | | | |
| **Plan Maintenance:** | **X** | | | |
| Update frequency defined | **X** | | | |
| Responsible parties identified | **X** | | | |
| Test frequency defined | **X** | | | |
| Test methodology defined | **X** | | | |
| Test results indicated | **X** | | | |
| Training requirements identified | **X** | | | |
| | | | | |

**BCP Checklist Definition of Terms**

Activation events defined:
Are the events and conditions that will cause the plan to be activated defined in the BCP?

De-activation defined:
Does the BCP define the level of restoration required to de-activate the plan?

Recovery priorities defined:
Does the BCP reference a Business Impact Analysis (BIA)? The priorities for restoration need to be defined in the BIA.

Maximum allowed outage defined:
Does the BCP define the maximum allowed outage permitted? If this time is exceeded the permanent loss (revenue, customers, credibility) is deemed to be unacceptable.

Individual(s) authorized to activate plan identified:
Does the BCP include the individual(s) authorized to activate the plan?

Line of succession defined:
Does the BCP include a line of succession indicating who may activate the plan if the primary authority is incapacitated?

Assumptions stated:
Does the BCP include all assumptions? (Extent of damage, availability of alternate site, availability of key personnel, availability of equipment)

Plan risks identified:
Does the BCP address risk? Are issues that might cause the plan to fail addressed?

Roles & Responsibilities defined:
Does the BCP define roles and responsibilities, i.e., team leaders, members, assigned functions?

Points of Contact Listed:
Does the BCP list the telephone number(s), page number(s) and email addresses of each person who needs to be alerted?

Vendor Contacts listed:
Does the BCP list vendor points of contacts for all vendors who need to supply hardware, software, supplies, and services?

Alternate facility location(s) identified:
Does the BCP identify alternate facilities from which operations will be conducted, assuming the existing facility is uninhabitable?

Spare Equipment location(s) identified:
Does the BCP identify the spare equipment necessary for the restoration of operations as well as the location of this equipment?

Backup records location(s) identified:
Does the BCP identify critical business records and their locations(s)?

Management Team identified:
Does the BCP identify the management team, those individuals authorized to approve purchases and make decisions?

Emergency Evacuation Team identified:
Does the BCP identify members of the emergency evacuation team, those individuals responsible for ensuring that all personnel have left the damaged facility?

Assessment Team identified:
Does the BCP identify members of the assessment team, those individuals responsible for determining the extent of the damage and advising the management team on whether to activate the BCP and move operations to an alternate site?

Salvage Team identified:
Does the BCP identify members of the salvage team, those individuals responsible for recovering equipment and evaluating whether the equipment is usable or must be replaced?

Public Relations and Media Team identified:
Does the BCP identify members of the public relations team, those individuals responsible for addressing questions from the media, customers, stockholders, and corporate board members?

Alternate Facility Team identified:
Does the BCP identify members of the alternate facility team, those individuals responsible for preparing the alternate site to receive equipment, personnel, and initiate operations?

Transportation Team:
Does the BCP identify members of the transportation team, those individuals responsible for acquiring vehicles to transport equipment and personnel to the alternate site?

Telecommunications Recovery Team identified:
Does the BCP identify members of the telecommunications team, those individuals responsible for contacting vendors to arrange for phone services, and data circuits at the alternate facility?

Network Recovery Team identified:
Does the BCP identify members of the network recovery team, those individuals responsible for installing routers, switches, and cabling at the alternate facility?

Server Recovery Team identified:
Does the BCP identify members of the server recovery team, those individuals responsible for restoring servers and/or building new servers at the alternate facility?

Application Recovery Team identified:
Does the BCP identify members of the application recovery team, those individuals responsible for installing software applications on new/recovered servers at the alternate facility?

Desktop Recovery Team identified:
Does the BCP identify members of the desktop recovery team, those individuals responsible for building and delivering desktop systems to personnel assigned to work at the alternate facility?

Records Retrieval Team identified:
Does the BCP identify members of the records retrieval team, those individuals responsible for retrieving and transporting vital records to the alternate facility?

Security Team identified:
Does the BCP identify members of the security team, those individuals responsible for ensuring that access to records, systems, and applications as well as network and Internet traffic include an acceptable level of security while operations are conducted at the alternate facility?

Update frequency defined:
Does the BCP define the frequency as to when the entire plan and/or just sections of the plan will be updated? For example points of contact may be updated quarterly; while the entire plan may be updated annually.

Responsible parties identified:
Does the BCP identify individuals responsible for updating each section of the plan?

Test frequency defined:
Does the BCP identify the frequency for testing the entire plan and/or sections of

the plan?

Test methodology defined:
Does the BCP identify the test scenarios and methodology to validate the plan?

Test results indicated:
Does the BCP identify how test results are to be documented, distributed, and used for improving the plan?

Training requirements identified:
Does the BCP identify the training requirements each team will need to ensure the plan will be successfully implemented?

## H. Appendix: Auditing Work Papers

The Internal Auditors use a standard work paper for documenting test procedures and test results. The use of a standard work paper ensures that each test is adequately documented.

The auditor can use standard work papers to ensure that testing is balanced, i.e., that the testing process includes test elements for confidentiality, integrity, and availability and that test methods vary to include document reviews, interviews, observations/inspections, and automated tests.

Below are sample work papers for several of the tests.

# Audit Test Work Paper

**Project No/ID**: 2005-03-IT-01

**Department: Information Technology (IT)**

**System Name: ABC Financial Corporation IBM AIX**

| **Test Date:** | **Test No:** | **Tester ID:** | **Policy / Directive:** |
|---|---|---|---|
| 03/15/05 | 1 | CRJ | NIST SP 800-40 |

**Test Element: Management Control Operational Procedure Technical Control**

**Test Control: Confidentiality Integrity Availability**

**Non-repudiation Authentication Access Control Audit**

**Test Method: Interview Document Review Observation Automated**

## ST&E Description:

**Hypothesis:** The IBM AIX server managed by the IT Department has the current IBM OS Maintenance Level installed and all APAR post patches are installed.

**Test Method:**

1. Enter the command: **oslevel –r** and record the results.
2. Enter the command: **instfix –ik <apar#>** for each post OS level and record the results

## ST&E Results:

The results indicate that the latest OS Maintenance Level is installed and there are no missing APARs.

## ST&E Recommendations for Corrective Actions:

No recommendations, the OS level and all patches provided by IBM are current.

# Audit Test Work Paper

**Project No/ID**: 2005-03-IT-01

**Department: Information Technology (IT)**

**System Name: ABC Financial Corporation IBM AIX**

| Test Date: | Test No: | Tester ID: | Policy / Directive: |
|---|---|---|---|
| 03/15/05 | 2 | CRJ | NIST SP 800-40 |

**Test Element:** **Management Control** **Operational Procedure** **Technical Control**

**Test Control: Confidentiality** **Integrity** **Availability**

**Non-repudiation** **Authentication** **Access Control** **Audit**

**Test Method: Interview** **Document Review** **Observation** **Automated**

## ST&E Description:

**Hypothesis:** The IBM AIX server maintained by the IT Department has no missing patches or configuration issues for third-party and open source programs installed on the server.

**Test Method:** Scan the IBM AIX server using Nessus with plugins for AIX 5.3, WebSphere, HTTP, FTP, SNMP, and LPD.

## ST&E Results:

Results are recorded in detail in a Nessus document.
Apache and OpenSSL are reported to be vulnerable. There are a number of open ports running unknown services.

## ST&E Recommendations for Corrective Actions:

Nessus may be reporting false positives. Nessus determines the version by examining the banners. The Apache and OpenSSL banners may not have been updated when patches were applied. RPC may be using the open ports. Review the Nessus results with the AIX system administrators.

## Audit Test Work Paper

| |
|---|
| **Project No/ID**: 2005-03-IT-01 |

| |
|---|
| **Department: Information Technology (IT)** |

| |
|---|
| **System Name: ABC Financial Corporation IBM AIX** |

| **Test Date:** | **Test No:** | **Tester ID:** | **Policy / Directive:** |
|---|---|---|---|
| 03/15/05 | 3 | CRJ | N/A |

**Test Element: Management Control Operational Procedure Technical Control**

**Test Control: Confidentiality Integrity Availability**

**Non-repudiation Authentication Access Control Audit**

**Test Method: Interview Document Review Observation Automated**

### ST&E Description:

**Hypothesis:** The Trusted Computing Base (TCB) is installed.

**Test Method:** Run the /usr/bin/tcbck command. If an error message appears, TCB is not installed. Check the TCB configuration file /etc/security/syschk.cfg to obtain a list of files.

### ST&E Results:

No error message was displayed. TCB is installed.

### ST&E Recommendations for Corrective Actions:

None.

# Audit Test Work Paper

**Project No/ID**: 2005-03-IT-01

**Department: Information Technology (IT)**

**System Name: ABC Financial Corporation IBM AIX**

| Test Date: | Test No: | Tester ID: | Policy / Directive: |
|---|---|---|---|
| 03/15/05 | 4 | CRJ | N/A |

**Test Element: Management Control Operational Procedure Technical Control**

**Test Control: Confidentiality Integrity Availability**

**Non-repudiation Authentication Access Control Audit**

**Test Method: Interview Document Review Observation Automated**

## ST&E Description:

**Hypothesis:** There are no inconsistencies for files with stanzas in the TCB configuration file and the actual files. Checksums and file sizes as recorded in the TCB configuration file match those computed for these files.

**Test Method:** Run the **/usr/bin/tcbck –y ALL** command. Record and analyze the results.

## ST&E Results:

No inconsistencies of checksums or file sizes were reported. However, it is noted that stanzas for open source program files are not included in the TCB

## ST&E Recommendations for Corrective Actions:

Consider adding stanzas for open source program files to the TCB configuration file.

# Audit Test Work Paper

**Project No/ID**: 2005-03-IT-01

**Department: Information Technology (IT)**

**System Name: ABC Financial Corporation IBM AIX**

| **Test Date:** | **Test No:** | **Tester ID:** | **Policy / Directive:** |
|---|---|---|---|
| 03/15/05 | 5 | CRJ | N/A |

**Test Element:** **Management Control** **Operational Procedure** **Technical Control**

**Test Control: Confidentiality** **Integrity** **Availability**

**Non-repudiation** **Authentication** **Access Control** **Audit**

**Test Method: Interview** **Document Review** **Observation** **Automated**

## ST&E Description:

**Hypothesis:** The use of admin, rlogin, and su privileges are restricted to a minimum number of user accounts.

**Test Method:** Inspect the file **/etc/security/user** to determine which user accounts have these privileges.

## ST&E Results:

Only two administrators, Bill Jones and Fred Johnson have admin and su privileges. No user account has rlogin privileges. The administrators use SSH to connect to the AIX server from the internal network. The rlogin service is disabled.

## ST&E Recommendations for Corrective Actions:

None

# Audit Test Work Paper

**Project No/ID**: 2005-03-IT-01

**Department: Information Technology (IT)**

**System Name: ABC Financial Corporation IBM AIX**

| **Test Date:** | **Test No:** | **Tester ID:** | **Policy / Directive:** |
|---|---|---|---|
| 03/15/05 | 6 | CRJ | NIST SP 800-34 |

**Test Element: Management Control Operational Procedure Technical Control**

**Test Control: Confidentiality Integrity Availability**

**Non-repudiation Authentication Access Control Audit**

**Test Method: Interview Document Review Observation Automated**

## ST&E Description:

**Hypothesis:** The Business Continuity Plan is up-to-date with the current points of contact including telephone numbers, pager numbers, and email addresses.

**Test Method:** Send a confirming email to each individual listed in the BCP requesting each individual to confirm that their contact information is correct. Call individuals who do not send a reply within one week.

## ST&E Results:

Of the sixty people contacted 48 replied by email indicating that their contact information was correct. Of the twelve individuals who failed to send an email reply, ten were successfully contacted by telephone and eight of the ten individuals confirmed that their contact information is correct. Two of the ten individuals contacted by telephone indicated that their contact information changed since the last BCP review. The information was corrected in the BCP. One individual recently left the company. This individual’s email user accounts were disabled once it was determined that the individual left the company. A replacement was identified, added to the BCP, and provided with a copy of the plan. The last individual changed job functions within a department. This person’s assigned BCP responsibilities were transferred to another person active with the BCP.

### ST&E Recommendations for Corrective Actions:

1. Conduct a quarterly confirmation of the BCP point of contacts rather than just an annual review.
2. Human Resources should notify the BCP plan manager when an individual with BCP responsibilities leaves the company.

# I. Appendix: Nessus Plugins Used for Testing

The following page contains a table of the Nessus plugins used with the scan tool to test the IBM AIX server.

Nessus plugins are found at URL: http://www.nessus.org/plugins
(15 March 2005)

There is only one Nessus plugin (15863) for AIX 5.3. Numerous plugins are available for AIX 5.1 and 5.2. These were not selected as the IBM AIX server is running 5.3.

One plugin (14611) was selected as this plugin tests for the current AIX maintenance Level.

Several plugins related to AIX services (10009 ftp, 11355 lpd) were selected as they test specific services, ftp and lpd.

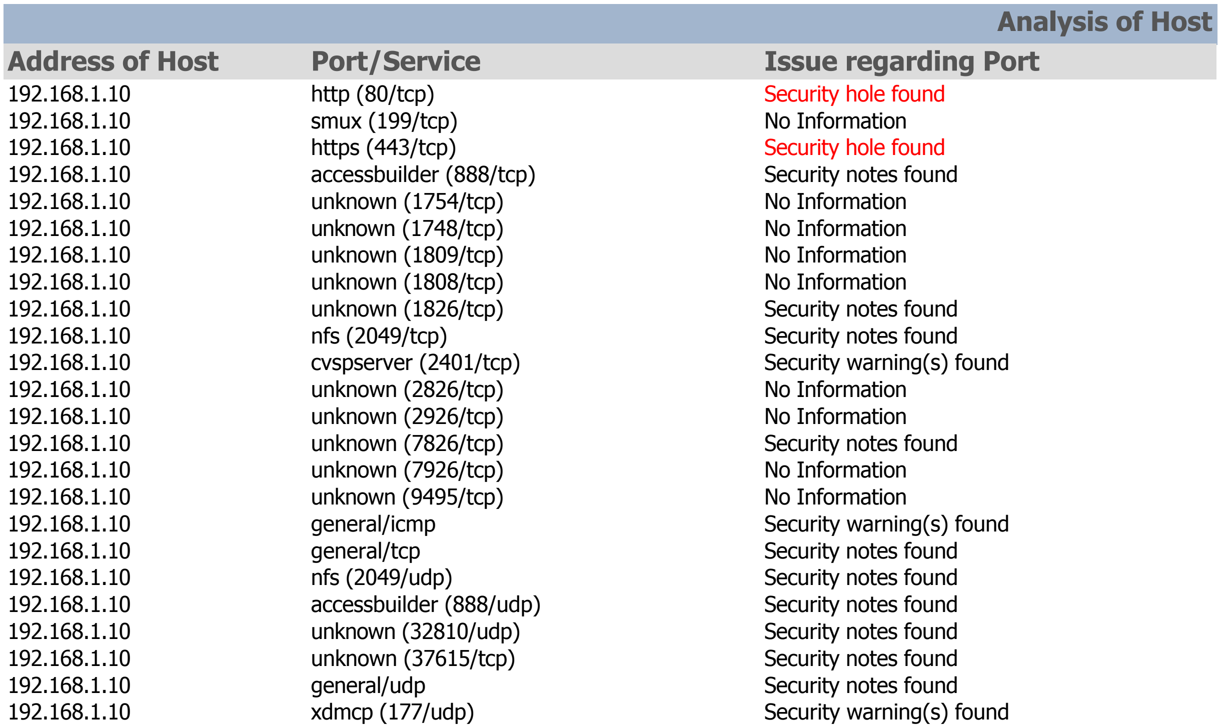
Other plugins were selected to test specific services including http, OpenSSH, OpenSSL, RPC, and SNMP.

**Nessus Plugins**

| Nessus Plugin No. | Family | Description |
|---|---|---|
| | | |
| 10009 | FTP | AIX FTPd buffer overflow |
| 10107 | General | HTTP Server type |
| 10114 | Firewalls | icmp timestamp |
| 10264 | SNMP | Default community names |
| 10330 | Services | Service Detection |
| 10823 | Gain Root Remotely | OpenSSH version < 3.0.2 |
| 10863 | General | SSL |
| 10883 | Gain Root Remotely | OpenSSH Channel Code |
| 10888 | CGI Abuses | mod_ssl overflow |
| 10891 | Useless services | XDMCP |
| 11010 | CGI Abuses | WebSphere Cross Site |
| 11030 | Gain Shell Remotely | Apache chunked encoding |
| 11031 | Gain Root Remotely | OpenSSH version <= 3.3 |
| 11032 | Miscellaneous | Directory Scanner |
| 11039 | CGI Abuses | mod_ssl off by 1 |
| 11111 | RPC | rpcinfo -p |
| 11157 | Backdoors | Trojan horses |
| 11181 | Denial of Service | WebSphere Host Header |
| 11213 | CGI Abuses | XSS |
| 11222 | Useless services | writesrv |
| 11226 | CGI Abuses | Oracle 9iAS default information |
| 11267 | Miscellaneous | OpenSSL password interception |
| 11355 | Gain Rote Remotely | Buffer overflow in AIX lpd |
| 11622 | CGI Abuses | Version of mod_ssl older than 2.8.10 |
| 14611 | AIX Local Security | Maintenance Level |
| 15863 | AIX 5.3 Local Security | APAR: IY58143 |
| 16173 | CGI Abuses | WebSphere default user information leak |
| 17337 | CGI Abuses | WebSphere APAR: IY60949 |

## J. Appendix: Nessus Scan Results

The Nessus scan results begin on the next page. The IP address has been changed to a fictitious address to mask the identity of the system.



Analysis of Host

| Address of Host | Port/Service | Issue regarding Port |
|---|---|---|
| 192.168.1.10 | http (80/tcp) | Security hole found |
| 192.168.1.10 | smux (199/tcp) | No Information |
| 192.168.1.10 | https (443/tcp) | Security hole found |
| 192.168.1.10 | accessbuilder (888/tcp) | Security notes found |
| 192.168.1.10 | unknown (1754/tcp) | No Information |
| 192.168.1.10 | unknown (1748/tcp) | No Information |
| 192.168.1.10 | unknown (1809/tcp) | No Information |
| 192.168.1.10 | unknown (1808/tcp) | No Information |
| 192.168.1.10 | unknown (1826/tcp) | Security notes found |
| 192.168.1.10 | nfs (2049/tcp) | Security notes found |
| 192.168.1.10 | cvspserver (2401/tcp) | Security warning(s) found |
| 192.168.1.10 | unknown (2826/tcp) | No Information |
| 192.168.1.10 | unknown (2926/tcp) | No Information |
| 192.168.1.10 | unknown (7826/tcp) | Security notes found |
| 192.168.1.10 | unknown (7926/tcp) | No Information |
| 192.168.1.10 | unknown (9495/tcp) | No Information |
| 192.168.1.10 | general/icmp | Security warning(s) found |
| 192.168.1.10 | general/tcp | Security notes found |
| 192.168.1.10 | nfs (2049/udp) | Security notes found |
| 192.168.1.10 | accessbuilder (888/udp) | Security notes found |
| 192.168.1.10 | unknown (32810/udp) | Security notes found |
| 192.168.1.10 | unknown (37615/tcp) | Security notes found |
| 192.168.1.10 | general/udp | Security notes found |
| 192.168.1.10 | xdmcp (177/udp) | Security warning(s) found |

### Security Issues and Fixes: 192.168.1.10

**Type**
**Port**
**Issue and Fix**

Vulnerability
http (80/tcp)

The remote host is using a version of mod_ssl which is
older than 2.8.7.

This version is vulnerable to a buffer overflow which,
albeit difficult to exploit, may allow an attacker
to obtain a shell on this host.

*** Some vendors patched older versions of mod_ssl, so this
*** might be a false positive. Check with your vendor to determine
*** if you have a version of mod_ssl that is patched for this
*** vulnerability

Solution : Upgrade to version 2.8.7 or newer
Risk factor : High
CVE : CVE-2002-0082
BID : 4189
Nessus ID : 10888

Vulnerability
http (80/tcp)

The remote host is using a version of mod_ssl which is
older than 2.8.10.

This version is vulnerable to an off by one buffer overflow
which may allow a user with write access to .htaccess files
to execute abritrary code on the system with permissions
of the web server.

*** Note that several Linux distributions (such as RedHat)
*** patched the old version of this module. Therefore, this
*** might be a false positive. Please check with your vendor
*** to determine if you really are vulnerable to this flaw

Solution : Upgrade to version 2.8.10 or newer
Risk factor : High
CVE : CAN-2002-0653
BID : 5084
Nessus ID : 11039

Vulnerability
http (80/tcp)
The web root physical is <H3>Exception:</H3>javax.servlet.ServletException:
/u07/app11i/p11icomn/portal
CVE : CAN-2001-1372
BID : 3341
Nessus ID : 11226

Vulnerability
http (80/tcp)

The remote host appears to be vulnerable to the Apache
Web Server Chunk Handling Vulnerability.

If Safe Checks are enabled, this may be a false positive
since it is based on the version of Apache. Although
unpatched Apache versions 1.2.2 and above, 1.3 through
1.3.24 and 2.0 through 2.0.36, the remote server may
be running a patched version of
Apache

## K. Appendix: Attributes of file /etc/security/user

The table beginning on the next page describes the settings for attributes found in the /etc/security/user file. These attributes may extend the privileges permitted to users. The values used by ABC Financial Corporation are listed.

Details for each setting are available at:
http://publib.boulder.ibm.com/infocenter/pseries/topic/com.ibm.aix.doc/aixbman/security/security.pdf

| Parameter | Description | Expected Value |
|---|---|---|
| | | |
| admin | True if the user account is an administrator account else false | false for most accounts |
| umask | This is the file creation mask. The setting prevents file sharing among users | 022 |
| pswrdwarntime | The number of days before a user is required to change their password that the user receives a warning informing them of the impending requirement to change their password | 7 |
| loginretries | This is the number of unsuccessful login attempts that are allowed before locking out the user's account | 3 |
| histexpire | This is the number of weeks that a user must wait before a previous password can be reused | 26 |
| histsize | The number of previous passwords that are tracked to ensure that previous passwords are not reused | 10 |
| minage | The number of weeks a user must wait to change their password again once the user has made a password change | 1 |
| maxage | The maximum number of weeks before a password must be changed | 13 |
| maxexpired | This is the maximum number of weeks after the user's password has expired that the user is allowed to change their password | 1 |
| minalpha | This is the minimum number of alphabetic characters required in a password | 2 |
| minother | This is the minimum number of non-alphabetic characters required in a password | 2 |
| minlen | This is the minimum length required for a password | 8 |
| mindiff | This is the minimum number of characters that must be changed from the previous password | 4 |
| maxrepeats | The maximum number of repeated characters allowed in a password | 2 |
| dictionlist | Setup a file of dictionary words and strings that a user may not select when creating a password<br>/usr/share/dict/words | |

| | | |
|---|---|---|
| rlogin | The value of this is either true or false. The parameter determines if the account can be accessed remotely through telnet or rlogin. The default value, true, must be changed to false. | false |
| su | The value of this is either true or false. The parameter determines if the account can switch to the superuser account. The default is true. Most user accounts should be set to false. | false (most accounts) |
| ttys | Most user accounts should be prohibited from logging into the console. To deny a user login access at the console but allow the user to login at other devices, enter the following:<br>ttys=!/dev/console, ALL | |

## L. Appendix: Attributes of file /etc/security/limits

Attributes are set in the **/etc/security/limits** file to prevent individual users from running processes that consume an excess of system resources thereby creating a denial of service (DoS) condition.

The table beginning on the next page lists the attribute settings defined for ABC Financial Corporation.

Information about the **/etc/security/limits** file can be found at:
http://publib.boulder.ibm.com/infocenter/pseries/index.jsp?topic=/com.ibm.aix.doc/files/aixfiles/limits.htm

| Variable | Description | Expected Value |
|---|---|---|
| | | |
| fsize | Identifies the soft limit for the largest file a user's process can create or extend. | 8192 |
| core | Specifies the soft limit for the largest core file a user's process can create. | 4096 |
| cpu | Sets the soft limit for the largest amount of system unit time (in seconds) that a user's process can use. | 3600 |
| data | Identifies the soft limit for the largest process data segment for a user's process. | 1272 |
| stack | Specifies the soft limit for the largest process stack segment for a user's process. | 1024 |
| rss | Sets the soft limit for the largest amount of physical memory a user's process can allocate. This limit is not enforced by the system. | 1024 |
| nofiles | Sets the soft limit for the number of file descriptors a user process may have open at one time. | 2000 |
| core_hard | Specifies the largest core file a user's process can create. | |
| cpu_hard | Sets the largest amount of system unit time (in seconds) that a user's process can use. | |
| data_hard | Identifies the largest process data segment for a user's process. | |
| fsize_hard | Identifies the largest file a user's process can create or extend. | |
| rss_hard | Sets the largest amount of physical memory a user's process can allocate. This limit is not enforced by the system. | |
| stack_hard | Specifies the largest process stack segment for a user's process. | |
| nofiles_hard | Sets the soft limit for the number of file descriptors a user process may have open at one time. | |

If the hard values are not explicitly defined in the **/etc/security/limits** file but the soft values are, the system substitutes the following values for the hard limits:

| Resource | Hard Value |
|---|---|
| | |
| Core Size | Unlimited (As indicated by a value of -1) |
| CPU Time | cpu |

| | |
|---|---|
| Data Size | Unlimited (As indicated by a value of -1) |
| File Size | fsize |
| Memory Size | Unlimited (As indicated by a value of -1) |
| Stack Size | 4194304 |
| File Descriptors | Unlimited (As indicated by a value of -1) |

If the hard values are explicitly defined but the soft values are not, the system sets the soft values equal to the hard values.

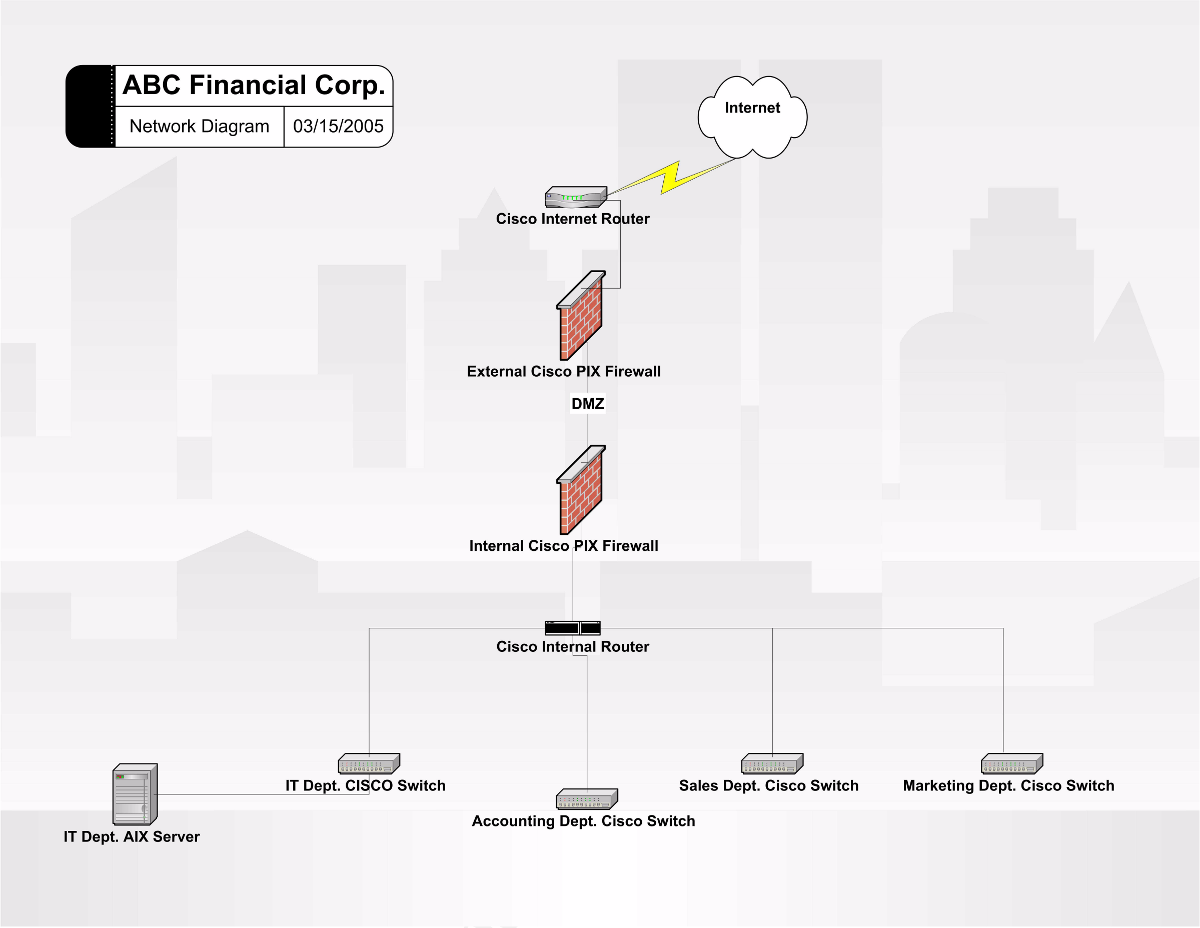
The value of the **cpu** resource represents the number of seconds; while the values for the other resources represent the number of 512 byte blocks.

The AIX command **mkuser** will create a user account and add an entry to the **/etc/security/limits** file for the user just created. The AIX command **chuser** will change the values created for the user in the **/etc/security/limits** file; while the **lsuser** command will list these values. The command **rmuser** will remove a user as well as the value from the **/etc/security/limits** file.

## M. Appendix: Network Diagram

The next page contains a basic network architectural diagram.

The diagram shows each department connected to an internal router through departmental switches. The internal backbone router is connected to an internal firewall. Between the internal and external firewalls is a DMZ where the corporate web server is positioned. An external router connects ABC Financial Corporation to the Internet.


ABC Financial Corp.
Network Diagram
03/15/2005
Internet
Cisco Internet Router
External Cisco PIX Firewall
DMZ
Internal Cisco PIX Firewall
Cisco Internal Router
IT Dept. CISCO Switch
Accounting Dept. Cisco Switch
Sales Dept. Cisco Switch
Marketing Dept. Cisco Switch
IT Dept. AIX Server