Global Information Assurance Certification Paper

IT's Crystal Ball:
Unix Security in a Systems Administrator's Playground

Andrew C. Nelson
GCUX Practical Assignment
Version 1.9, Option 2 (June 13, 2003)

Abstract

This paper presents a security audit of an IBM pSeries 630 server running AIX 5.1. The server is used by systems administrators to centrally manage and monitor a production environment of geographically distributed hosts and applications. The audit examines a variety of applications and services running on the server, the users who connect to it, the network environment in which it resides, and procedures and policies used in day-to-day operations. The report provides recommendations for addressing security issues found in the services running, management practices, firewall policies, the implementation of public key-based authentication, and protection of sensitive data.

This paper has been written to fulfill the requirements for the GIAC Certified Unix Security Administrator (GCUX) Practical Assignment, Version 1.9.

Table of Contents

Executive Overview
Introduction
- Business Model
- Role of IT-MGT-01 in GIAC Enterprises' Production Environment
- Risks and Concerns
- Audit Methodology
  - Method
  - Location
  - Interviews
  - Documents
  - Commands and Configuration Files
  - Topics

Analysis
- Description of System
  - Hardware and Platform Specifications
  - Software OS and Version
- Corporate Policies
  - Personnel Policy
  - Security Policy
  - Change Control
  - Budgets
- Physical Environment
- Operating System
  - Version
  - Trusted Computing Base
  - Maintenance and Support
  - Patch Management
    - OS and Maintenance
    - 3rd Party Software
- User Management
  - Local Standard System Accounts

- Login Banner
- Default Shell, Group, Home Directory
- Path and Environment
- Passwords
- sudo
- Utility and Service Accounts
- NIS Accounts
- GIACE IT Staff
- Datacenter Operators

Storage Management
- Backups
- Disks
- Partitions and Volumes
- File Systems
- File Ownership
- SetUID and SetGID Files
- Quotas and Limits
- Removable Storage

Sensitive Data
- Authentication
- Documentation
- Monitoring

Network Environment and Services
- Topology
- Network Access from Other Hosts
- Network Options
- Network Client
- IP Address
- DNS
- SMTP
- NTP

Network Services
- Top 10 Vulnerabilities to Unix Systems
- /etc/inittab
- /etc/rc.tcpip
- syslogd
- sendmail
- portmap
- inetd
- ftp, telnet, shell, login, exec, cvspserver
- bootps, tftp
- ntalk, daytime, time, ttdbserver, cmsd
- wsmserver
- dtspc
- xntpd
- snmpd, dpid2, and hostmibd
- NIM (/usr/sbin/nim), NFS and NIS (/etc/rc.nfs)
- writesrv

- rc (/etc/rc.d/rc 2)
- Secure Shell (OpenSSH)
- /etc/rc.dt
- httpdlite (/usr/IMNSearch/httpdlite/httpdlite)
- apache (/etc/rc.apache)
- Listening Processes
- Other Processes
  - brc (/sbin/rc.boot)
  - powerfail (/etc/rc.powerfail)
  - load64bit (/etc/methods/cfg64)
  - rc (/etc/rc)
  - fbcheck (/usr/sbin/fbcheck)
  - srcmstr (/usr/sbin/srcmstr)
  - cron
  - piobe, qdaemon
  - uprintfd
  - shdaemon
  - ctrmc
  - logsymptom
  - itess
- Applications
  - Apache, v2.0.43
  - CGI Scripts
  - Concurrent Versions System (CVS), v1.11.1p1
  - Network Installation Management (NIM)
  - Network Information Service (NIS)
  - Scripting (Perl v5.6.0 and Korn Shell)
  - dbmonitor, v1.0 and Cricket, v1.03
  - Progress, v9.1
  - Sendmail, v8.11.0
  - X11 Applications
  - Cron Jobs
- Logging and Monitoring
- Disaster Recovery

Critical Issues and Recommendations
- Top Ten Recommendations
- Other Recommendations
- Long Term Recommendations.

References

Executive Overview

GIAC Enterprises' E-fortune subsidiary (GIACE) is an online vendor of fortune cookie sayings, whose operations are centrally managed but geographically distributed. GIACE provides application services to a loose federation of remote franchises, partners and affiliates over a network of Virtual Private Networks (VPN's). The company has declared a strategy of local presence and community involvement in its technical services offerings to ensure the colloquiality, topicality and resonance of the fortunes it delivers to regional markets.

This report examines the security of IT-MGT-01, a Unix computer used by GIACE's IT staff to manage and

monitor the application services environment. The system is critical to delivery of services to customers, and offers services to GIACE IT staff as well. It is a plum target due to its location in GIACE's network and its role in management of production resources. Were an attacker to gain access to this system, all production systems would be in the palm of her hand. This document sets out the scope and methods used for auditing the security of the system, and follows with a detailed analysis of the configuration, applications, network environment, and methods and practices of the staff who use this system. The report concludes with a summary of critical issues and recommendations for their resolution.

Significant security vulnerabilities in the configuration and use of this system require immediate attention. Additional measures must be implemented to provide a defense in depth, above and beyond the existing reliance on border firewalls. Some changes are simply to shut down services, others require removal or reconfiguration of software and moving monitoring functions to different accounts. The backup strategy is inadequate, the use of Network Installation Services (NIS) is problematic, and the repository of systems documentation is inadequately protected. Many issues result from a corporate emphasis on meeting aggressive deployment deadlines, and addressing them will require that GIACE's management conjure up additional resources, or rechannel staff energies. This report attempts to bring focus to a critical component of the production environment, and provide a clear vision of a secure future for GIACE's fortunes.

Introduction

This security audit focuses on IT-MGT-01, a Unix server that manages and monitors GIACE's production database servers. Several areas of risk and concern are brought to light in the course of describing and investigating the system's role in support of GIACE's business model. The report concludes with concrete measures that should be taken to address existing risks and vulnerabilities, and improve security in the future.

Business Model

GIAC Enterprises (GIACE) offers remote desktop productivity applications and services to local organizations through cost and profit sharing agreements. Among the more popular of GIACE's offerings are the on-line eFortune eXchanges, a beguiling mixture of chat rooms, match-making, e-voyeurism and the lottery. Each day, thousands of participants eagerly log in from coffee shops and Internet cafes across the country to provide their insight on others' fortunes.

Local organizations resell the applications and services in local markets, and host GIACE servers in a data center environment. The back end databases and applications for eFortune are written in Progress, and hosted on a dozen RS6000's running AIX 4.3.3. Each data center owns the resources installed at its location, but they are managed by eFortune staff from a central facility. The applications hosted on IT-MGT-01 provide the tools GIACE's staff needs to deliver accurate fortunes in a timely fashion.

Role of IT-MGT-01 in GIAC Enterprises' Production Environment: The Crystal Ball and the Playground

IT-MGT-01 is central to management of GIACE's Unix environment because of its role as the hub of a hub-and-spoke network and administrative topology - it is the "crystal ball" through which administrators access and interpret their world. System and database administrators enjoy the system's speed, storage, and convenient network connections, and depend upon the management and monitoring tools it hosts. It is also their playground, where they can experiment, tweak, learn and test. The cost of the system adds an impetus to maximize its use, and security has often taken a back seat to expedience. The applications and services in use include Network Information Services (NIS) for Unix account management, IBM's Network Installation Management (NIM) for operating system maintenance, an installation of Progress for database management, a CVS repository of systems documentation, monitoring scripts run from crontab, an Apache web server, and Sendmail.

The system was installed three months ago during rollouts of GIACE's operations to data centers nationwide. Its role has been defined partly by carefully planned functions and partly by growth and opportunity. Except for user account administration the deployments have not been implemented under the guidance of a security policy. This has brought quick turnaround and delivery of service to the organization, and GIACE has decided it is time to reckon the cost, address the security risks, and solidify its gains.

Risks and Concerns

IT-MGT-01 has a number of vulnerabilities because of the network services it runs, the activities in which it participates, and the applications it hosts. These attributes make it an attractive target, because compromise of this system opens the door to the entire production environment. These concerns are heightened by GIACE's policies, which focus on network perimeter firewalls, place implicit trust in internal hosts, and value on-time delivery above security.

Many of the network services running on this system are present as part of the default installation of the operating system and are insecure. Most are not used and can be retired without significant effort or cost. Other settings can be adjusted to reduce vulnerabilities.

The variety of activities that take place on this host presents a significant challenge to administrators, who must maintain separation of duties and a policy of least privilege. Users log in to the system from several network addresses, using various authentication methods to gain access to multiple services. IT-MGT-01 hosts monitoring applications and batch processes that use SSH and public-key authentication, and the private keys used in these SSH connections are a delicious target. Monitoring functions typically require staid, steady, continuous operation, which is not foremost in the thoughts of systems administrators and dba's doing testing and experimentation. This system hosts valuable data in a Concurrent Versions System (CVS) repository of scripts, event logs, and documentation about the production environment, conveniently assembled in one spot.

Most of the applications running on this server have security vulnerabilities. The use of NIS for account management has introduced a number of administrative headaches and security risks. NIM uses tftp, "R"-commands and the Network File System (NFS). Progress' database environment has several documented local compromises. CVS repository access is offered through the insecure pserver authentication service. The Apache web server serves dynamic content using Common Gateway Interface (CGI) scripts. Finally, Sendmail is running as a daemon

Of particular concern is the focus of existing security efforts, which concentrate on firewalls and VPN's at the perimeters separating GIACE's networks from the Internet. Internal network and host security relies primarily on trust among the LANs of the data centers, GIACE's corporate offices, and the management subnet on which this system is addressed.

Finally, the corporate culture has historically favored short time to market over security considerations. This has worked well in establishing market share, but the supporting infrastructure now relies on insecure and problematic services that place the enterprise at risk, and that will require time and resources to address.

Audit Methodology

This audit examines security of IT-MGT-01 in a number of areas, which are detailed in the Topics section below. IT-MGT-01 plays a central role in managing the production environment that delivers products and services to customers. Examining its security requires consideration of the production environment and the corporate LAN. While the focus is on configuration details for one particular system, this audit also considers pertinent user administration practices, network security and corporate policies and goals.[1] A ranked list of recommendations concludes the report.

Method

In the course of this audit, data about the system has been acquired through interviews, reading product and systems administration documentation, searching the Internet, and querying the system directly.

Location

Most of the documentation for this report was gathered on site. GIACE provided a cubicle in the IT staff area, a badge with access to all computer facilities, a user account, a network drop for the auditor's laptop, and a printer with a parallel cable. Paper was free, but coffee cost a quarter.

Interviews

GIACE staff were supportive of the audit process, and made themselves available over a 3-day period to answer questions and assist in research.

Documents

GIACE staff provided copies of official forms and paperwork, and access to their document repository. The latter and was immensely helpful in understanding the environment. In addition, staff offered build and installation notes that had not been committed to the repository.

Commands and Configuration Files

Configuration files and the output of commands were gathered using the local auditor account GIACE provided. This account was a member of the system group, and provided access to almost all information. In cases where root access was required, GIACE staff would login and run the commands at the auditor's request. The commands and output have been included as part of the discussion. Ellipses are used to avoid unecessary clutter, and the "\" character is used to indicate line continuation. Recommendations have a grey background to set them apart.

Topics

The following broad topics are covered in the Analysis section:

Description of System
Corporate Policies
Physical Environment
Operating system
User Management
Storage Management
Sensitive Data
Network Environment and Services
Other Processes
Applications
Logging and Monitoring
Disaster Recovery

Analysis

Description of System

Hardware and Platform Specifications

The system is an IBM pSeries630, characterized by IBM as an "affordable, small package with enterprise-class reliability," with the following specifications:[2]

Make and Model	IBM pSeries 630 Model 6C4
Form factor	Rack-mounted (19", 4 rack units), 4 hot-swappable disk bays
Processor	single Power4 1.0GHz (powerpc)
Memory	2 GB ECC
Bus	1.33 MHz PCI
SCSI Controllers	two integrated Wide/Ultra3 SCSI, one Wide/Fast-20 SCSI
Storage	two 36GB and two 72GB LVD SCSI drives
Network	two integrated 10/100 ethernet

Serial	three serial ports
Parallel	one parallel port
Power	single 110/220 VAC power supply
Location	rack-mounted in data center
Purpose	administrative, management, and monitoring services for IT staff.
Maintenance	Under warranty and maintenance
Cost	Approximately $20k

The processor is capable of running a 64-bit kernel:

```
[auditman@IT-MGT-01] /home/auditman $ /usr/sbin/prtconf -c
CPU Type: 64-bit
```

or

```
[root@IT-MGT-01] / # /usr/sbin/bootinfo -y
64
```

Software OS and Version

The Operating System is AIX 5L for POWER, Version 5.1, release maintenance level 5100-03.

The installed kernel is 32-bit,

```
[root@IT-MGT-01] / # /usr/sbin/bootinfo -K
32
```

and 64-bit kernel extensions are enabled:[3a]

```
[root@IT-MGT-01] / # genkex | grep 64
2040090              2c0 /usr/lib/drivers/syscalls64.ext
. . .
```

Recommendations: AIX 5.1 has the feel of an interim version, with many features that have been brought forward from version 4.3, and others that first appeared in version 5.2. Consider upgrading this system to AIX 5.2.

Corporate Policies

GIACE's E-fortune product line is in its infancy, and corporate polices are largely informal and ad hoc.

Recommendations: GIACE should extend its risk assessment beyond this system to the entire production environment, to define what information technology assets need to be protected and in what manner.[4]

Personnel Policy

At hire, all employees are required to sign a document indicating they will exhibit good behavior. This policy does not cover employees of affiliated organizations, who have access to production systems in remote data centers. Visitors are required sign a Non-Disclosure Agreement.

Recommendations: GIACE's IT staff should document the perceived obligations of data center operators, and these should be incorporated in future agreements with affiliated organizations.

Security Policy

There are no documents that detail security practices or configuration of corporate or production systems. While GIACE may have legal recourse in the event of a security breach by employees, it is left to IT staff to preserve and protect business property as they see fit.

Recommendations: Articulate existing security practices, develop guidelines for implementing secure systems, and establish a process for periodically reviewing conformance. Use checklists and examples to make security a routine and practical affair.

Change Control

Change control at GIACE is an informal process. Scheduled maintenance windows have been prescribed for the second weekend in each month, but testing, notification, coordination, verification and rollback efforts are only loosely coordinated. IT staff indicate a reluctance to conform to scheduled windows because updates to GIACE's applications are released during those periods, and it is difficult to troubleshoot problems if systems modifications are performed concurrently.

Recommendations: Institute a formal change control process, of which security reviews are an integral part, and create a maintenance window for systems changes that is separate and distinct from application releases.

Budgets

The cost of hardware, software, maintenance, and personnel to support GIACE's production environment is significant, and GIACE is a for-profit company. This has an adverse affect on the installation and configuration of systems because of the pressure to maximize the use of resources and reduce time to market of new products.

Recommendations: Establish a policy that recognizes monetary pressures, and explicitly states that bypassing or ignoring security is not an acceptable method of delivering products, and in fact reduces the value of GIACE's capital.

Physical Environment

IT-MGT-01 is located in a data center with raised floors, air and power conditioning, an emergency generator, and intrusion and fire alarms that are connected to local emergency response services. The data center is staffed 24x7 by operators who perform tape backups, management of printing services, and basic system monitoring duties. Access to the facility is secured by key cards with picture ID, and is centrally tracked. Video surveillance cameras record ingress and egress through all doors to the facility. After business hours motion detectors trigger an alarm monitored by a security company that will call local law enforcement.

This data center has a unique relationship with GIACE. It is located on the premises of GIACE’s main corporate facility, and houses two sets of servers. One set is GIACE’s corporate and production management servers, for which GIACE pays the datacenter a hosting fee. The other is the data center’s own set of E-fortune servers, that it operates under a reseller agreement with GIACE -- in this respect it is like the data centers of other partners. The datacenter also participates in ventures independently of GIACE. Thus, access to the facility is occasionally granted to third parties that, while they have a legitimate business reason to be on the premises, are thereby granted undue physical access to GIACE’s hardware.

The security of this system is also affected by the physical environment in each remote data center to which it is connected by wide-area network links. This system monitors hosts at remote datacenters, and datacenter operator accounts are managed on this system. The independent nature of data centers and resulting lack of control by GIACE of physical access to data center hardware is of great concern. If GIACE does not have authority over data center operators, yet must allow those operators access to services on this system, they must be considered a security risk.

This system has a Common Hardware Reference Platform ("chrp") architecture:

```
/usr/sbin $ lscfg
. . .
Model Architecture: chrp
```

and does not have a hardware keylock. The cabinet has a front door but no back door. An SMS password has not been set. All hosts are scheduled to reboot every six months.

There is no active physical security in the sense of guards. Visitors must sign in at the front desk, but there are a number of people entering and leaving in the morning, evening and lunch, and in any case the receptionist has not been charged with security duties.

In /etc/security/users, the list of ttys is the default of ALL. A power-on password has not been set, nor has a supervisory password. The bootlist is:

```
# /usr/bin/bootlist -m normal -o
hdisk0
hdisk1

# /usr/bin/bootlist -m service -o
cd0
hdisk0
hdisk1
ent0
```

Recommendations: The physical environment is excellent and provides a reasonable degree of physical security. In the absence of the physical deterrent of a key or a locked cabinet, set a supervisory password to prevent an unauthorized user from power cycling the system, booting off of a CD, and entering maintenance mode. Ensure that hosting agreements specify physical security requirements for GIACE's hardware, such as locked cages, and procedures for scheduling and confirmation of service visits.

Operating System

Version

The system is running AIX 5L for POWER, Version 5.1.[5]

```
[auditman@IT-MGT-01] /home/auditman $ oslevel
5.1.0.0
[auditman@IT-MGT-01] /home/auditman $ uname -vr
1 5
```

The release maintenance level is 5100-03:

```
[auditman@IT-MGT-01] /home/auditman $ oslevel -r
5100-03
```

Check the filesets installed:

```
[auditman@IT-MGT-01] /home/auditman $ instfix -i | grep AIX
    All filesets for 5.0.0.0_AIX_ML were found.
    All filesets for 5.1.0.0_AIX_ML were found.
    All filesets for 5.1.0.0_AIX_ML were found.
    All filesets for 5100-01_AIX_ML were found.
    All filesets for 5100-02_AIX_ML were found.
    All filesets for 5100-03_AIX_ML were found.
    Not all filesets for 5100-04_AIX_ML were found.
```

Recommendations: Bring the operating system to AIX 5.1 Maintenance Level 4 (ML4).

Trusted Computing Base

The Trusted Computing Base is installed. However, it is not currently used for monitoring purposes. The output of the command `tcbck -n ALL` indicates the user and group "lp" have been removed, ownership of files related to the Documentation Library Service has been modified, and a number of pseudo-terminal related slave character devices in /dev/pts/ are in use. The grpck and usrck commands complain bitterly because entries made in /etc/passwd for creation of NIS maps do not appear in /etc/security/passwd.

Recommendations: Run the command

```
tcbck -n ALL
```

to check the system against the file definitions in /etc/security/sysck.cfg, and the command

```
tcbck -n tree
```

to examine security settings in the file system tree. Bring the system to a known state by correcting file permissions and adding files to the sysck.cfg database. After updating the sysck.cfg database, copy it off the server and store it in a secure location. The command

```
# tcbck -n tree 2>/home/auditman/work/tcbck_tree.txt
```

will create a list of files that are candidates for addition because they are suid or sgid (see SetUID and SetGID Files), linked to a file in the tcbck database, or a device special file. Also add files for installed applications and scripts. Schedule the tcbck command to run several times a day, copy the results off the box using scp, and review the results.

Maintenance and Support

This system is under an IBM Hardware Maintenance contract with 24-hour response time for hardware, and an IBM Software Supportline contract that provides support from 8:00am - 5:00pm, Monday-Friday.

Patch Management

GIACE policy states that systems must be brought to the latest possible patch level (IBM calls these APARS) before deployment in the production environment, and maintained thereafter on a monthly basis.

OS and Maintenance

The administrators of this system use IBM's fix delivery center[6] to compare filesets installed on the system with those available from IBM, and download the files necessary to bring the system to a required target level. These are deployed either manually or using IBM’s Network Information Management (NIM). In practice the administrators are somewhat leery of installing non-critical patches immediately, and prefer to wait a couple of weeks.

The administrators of this system subscribe to IBM's subscription services[7] for support bulletins containing security advisories, maintenance release information, and the latest software fixes. Security bulletins are sent immediately, while general maintenance and fix bulletins are sent monthly. These are reviewed by the systems administrators and scheduled for testing and installation as needed.

3rd Party Software

The administrators also subscribe to notification services provided by security organizations and software vendors. These include:

CERT	http://www.cert.org/contact_cert/certmaillist.html
Progress	http://www.progress.com/support/links.htm
Apache	http://httpd.apache.org/lists.html
Cricket	http://lists.sourceforge.net/lists/listinfo/cricket-announce
Perl	http://lists.cpan.org
OpenSSH	http://www.mindrot.org/mailman/listinfo/openssh-unix-announce

User Management

User administration for this system is performed by a lead and a second systems engineer who hold primary responsibility for all IBM and AIX production hardware. This system is the Network Information Services (NIS) master server for a set of a dozen or so Unix servers hosted at remote datacenters, and is the focal point for account management for all hosts in the production environment. On each host there are two basic sets of accounts: (1) local system accounts used by AIX processes, service personnel, and datacenter staff, and (2) accounts managed through NIS. There are two categories of NIS accounts: GIACE staff and datacenter staff.

Local Standard System Accounts

Accounts created during installation of the operating system are not included in NIS. These are: root, daemon, bin, sys, adm, lpd, uucp, guest, and nobody. The user ipsec, created with the installation of IP Security filesets, is also not included. Root's password is used only by systems administrators. The root account is not restricted from logging in directly. The only person other than GIACE IT staff who has access to the root password is a corporate security officer.

Other local accounts have been created on production hosts for use via sudo by data center personnel (see Utility and Service Accounts). These are used to perform backups and various database maintenance tasks. The accounts are created on IT-MGT-01 as well, to maintain consistency of uid's and gid's. In addition, local accounts have been created to run scripts that gather and process data and statistics from production hosts for monitoring purposes. GIACE staff log in to these accounts to configure and adjust scripts and configuration files. In one case, the Apache web server executes cgi scripts and accesses data stored in a local user's account (see dbmonitor, v1.0 and Cricket, v1.03).

Recommendations: Disable the uucp, lpd and guest accounts. Set root's account to disallow direct logins, and require users to su to root or use sudo. Apply the same restriction to accounts used for data gathering and monitoring functions. Unfortunately, this means an additional user will have to be created locally that is allowed to su to root, as a hedge against the possible inaccessibility of NIS.

Login Banner

AIX allows the login banner to be changed in /etc/security/login.cfg by adding a line to the Default stanza:

```
Herald = "warning text"
```

When telneting to the system, the Herald text is displayed prior to the login prompt, and the /etc/motd file is displayed after logging in.[8]

However, sshd on this system disregards the login.cfg file, and instead displays the file specified with the keyword "banner" in /etc/ssh/sshd_config. After successful login, /etc/motd is displayed.

Recommendations: Create a file in /etc with a warning banner concerning unauthorized use of the system, and a reference to it in /etc/ssh/sshd_config. Replace the text of /etc/motd with a similar warning.

Default Shell, Group, Home Directory

The default shell for this system is /user/bin/sh, which is used if no shell is specified in the user's entry in /etc/passwd or the NIS passwd map. The preferred shell is ksh, which is specified in /usr/lib/security/mkuser.default. This file also contains home directory, primary group and other group membership defaults.

Path and Environment

The path and environment are initially determined by the contents of /etc/environment, and are augmented by additional global settings in /etc/profile and user-specific settings in ~/.profile. A script is called from /etc/profile that sets environment variables and appends to the search path:

```
export PATH=$PATH:$DLC/bin:$DLC:/exch/bin:/exch/giace: \
/exch/occular:/exch/occular/javawow:.
```

The called script is owned by dbmng, a utility account accessed by database administrators.

In addition, an IT staff user has placed an alias to her own ~/.profile in root's .profile.

Recommendations: Scripts that modify root's environment should not be writable by any other account. Appending an environment variable and a dot to the search path can allow unintended execution of files in the current directory, a classic method of compromise. Remove the call to this script from /etc/profile so that root's path will not be modified. If necessary, place a call to this script in ~/.profile for dbmng and other database administrator accounts. Also remove the alias to another user's .profile from root's .profile. As a matter of good practice, remove the dot from the end of the path in the called script.

Passwords

Password policies are defined for local accounts in /etc/security/user. The mkuser command creates a user-specific stanza in this file which is combined with (and overrides) a list of default parameters at the beginning of the file. The important settings here are:

umask = 022	
expires = 0	
SYSTEM = "compat"	
logintimes =	
loginretries = 0	no limit (if limit exceeded, reset count in /etc/security/lastlog)
histexpire = 0	no time restriction (weeks) on password reuse
histsize = 0	no restriction on number of unique pwds before reuse
minage = 0	no min age before pwd can be changed
maxage = 0	no max age for pwds
maxexpired = 4	user can change pwd that has been expired for 4 weeks
minalpha = 4	at least 4 chars
minother = 1	require at least 1 non-alpha char
minlen = 6	
mindiff = 3	must have 3 chars different from previous pwd
maxrepeats = 0	no restriction (IBM says this is meaningless, 8 = no restriction)
dictionlist =	common words are allowed
pwdchecks =	executables (absolute path, or in /usr/lib) for additional checks

These are AIX-specific settings, and only pertain to local accounts -- accounts maintained in NIS do not use these settings (and also ignore user-specific stanzas in /etc/security/login.cfg).

Recommendations: although changes to these defaults will only affect newly created local users, it would still be

a good idea to tighten them up. In the event NIS is replaced, these settings should be applied to all accounts. Suggested changes are:

umask = 027	
loginretries = 3	three tries
histexpire = 3	number of weeks before password can be reused
histsize = 3	number of unique passwords necessary before reuse
maxexpired = 0	expired passwords will have to be reset by an administrator
minlen = 8	two more characters will make the password significantly more secure
dictionlist =	supply a dictionary to disallow use of common words as passwords

System, service, and root passwords are maintained in concert with a corporate security officer. Upon changing a non-personal password, GIACE IT staff inform the officer, who updates and prints a text document from his workstation (a member of the corporate Windows 2000 domain), and stores it in his wallet. Password distribution is an informal affair that takes place upon request. Each staff member maintains their own password list as they see fit, and no formal policy exists as to how or where passwords should be stored. In general, IT staff synchronize their passwords for accounts in the Corporate Windows 2000 domain to those on Unix hosts and the production environment.

Recommendations: The password list should not be stored or generated on a computer connected to the corporate or production networks. It should be maintained on a standalone computer with an encrypted hard disk and locally attached printer. The printed password list should be stored in a secure location such as a safe or safety-deposit box.

GIACE should recognize that passwords for production systems are a critical asset that must be preserved and protected. Just as source code is often placed in escrow to protect a customer’s investment in an application, a formal procedure for maintaining passwords is critical to GIACE’s ability to fulfill its partnership agreements. Secure storage of passwords should be viewed as an honorable duty, rather than a hassle and expense. When you have to change passwords, it is always better to know which passwords need to be changed!

Encourage and enable prompt and accurate dissemination of passwords by providing GIACE staff standardized printed password sheets. Obfuscate the printed lists by using an algorithm to change specific characters, by leaving out account or system names, and so forth -- the algorithm can be distributed verbally. Without this sort of mechanism, and unless individuals are tasked with fulfilling such a role, password inertia and complacency are inevitable.

Request that staff maintain separate passwords for corporate, production, and personal (e.g., home) accounts.

Establish a procedure for periodically testing passwords using a password cracking tool such as John the Ripper.[9] This must be done with the full knowledge and explicit written consent of GIACE's administration.

sudo

The sudo program is used to simplify account administration and control user activities in the production environment, as specified in the file /etc/sudoers. Staff at remote datacenters login to the host at their site with an NIS account, and perform assigned duties by invoking scripts that use sudo to issue commands as one of a set of utility and service accounts. This allows each datacenter staff member to have a personalized account, and logs their activity to syslog while constraining their actions to a specific set of commands.

Utility and Service Accounts

In addition to standard system users and groups, GIACE administrators maintain a set of local utility accounts, not included in NIS, on all hosts in the production environment. These are:

Users:

sysadm	for system maintenance tasks
dbmng	for database administrative tasks
ibmce	for IBM service engineers
dcopr	for backups
dcmgr	for reports and status information
dbuser	for database maintenance
relmgr	for releasing data and applications to the production environment
sshd	for the SSH daemon
cricket	for monitoring and data gathering functions (this user only exists on IT-MGT-01)

On all production hosts including IT-MGT-01, local user accounts and NIS accounts are granted membership in local groups as follows.

Groups:

system	a standard system group for system administrators. All GIACE IT staff are members of this group, which allows various system administration tasks without logging in as root, such as mounting filesystems and creating backups.
staff	the default group for non-administrative users. This group is empty
bin	a standard system group. This group contains the sysadm account.
sys	a standard system group. This group contains the sysadm account.
security	a standard system group that allows members sysadm and root to administer other accounts.
cron	a standard system group. This group contains the sysadm account.
perf	a standard system group. This group contains dcmgr and dcopr and is used for performance monitoring.
shutdown	a standard system group. This group contains sysadm, dcmgr, ibmce, and dcopr.

Standardization of uid's and gid's across all production hosts enables software packaging, deploying scripts, restoring backups, testing software and similar activities that benefit from a uniform, predictable environment.

NIS Accounts

NIS accounts are invoked by placing a "+" entry in /etc/passwd and /etc/group on each host, in which case the ypbind daemon appends information from NIS maps to these files. The user accounts of GIACE's IT staff and those of operators in remote data centers are distributed to all hosts in the environment, in a single NIS domain. This has the advantage of central control and consistency across hosts in the production environment, at the cost of the security risks inherent in NIS (see Network Information Service). The following accounts are maintained in NIS:

Users:

auditman	the author of this paper
billybob, bobbyjo, danbob	GIACE IT Staff
danpierr	a programmer
scottbon	a remote datacenter staff member

Groups:

imnadm	the only member of this group is imnadm, used by the documentation library service.
dbmng	database administrators. All GIACE IT staff are members of this group.
operator	this group contains all data center staff user accounts. NIS netgroups are used to restrict logins to specific production hosts.
develop	this group contains GIACE programmer accounts.
sshd	this group contains only the user sshd
cvs	a group added to grant access to the GIACE IT documentation repository. All GIACE IT staff are members.
cvsadmin	CVS administrators can run CVS administrative commands. A pair of designated GIACE IT staff are members.

Recommendations: Remove the cvs and cvsadmin groups from NIS, and leave them as local groups. Their inclusion here is probably the result of the inherent difficulty of managing both local and NIS users and groups. Each regeneration of NIS maps requires copying IT-MGT-01's passwd and group files to an alternate location and running various NIS processes. The intermediate step of weeding out local accounts unique to IT-MGT-01 is likely to be overlooked. See Network Information Service.

GIACE IT Staff

IT staff that are responsible for system administration of the production environment use their NIS accounts on this system as well as all others in production. They use this system for scripting, documentation, monitoring, data collection, database administration, and gateway services.

Several GIACE programmers also have NIS accounts, and are members of netgroups that have access to production systems. This is evidently a holdover from the initial development and deployment of GIACE's software to production systems.

Recommendations: Remove all programmer accounts from the production environment. If this is not feasible, place their accounts under the same sudo regimen as data center staff.

GIACE IT staff perform the following activities on this system:

Database Administration

The Database Administrators ("dba's") support the database infrastructure and work closely with GIACE's programming staff.

Scripting

GIACE IT staff attempt to automate as much as they can of daily tasks using the korn shell, /usr/bin/ksh, and perl, /usr/bin/perl. Most scripts are created and executed as staff users. Standard templates are used that contain header information and prescribe naming conventions and formats to be followed.

Documentation

All GIACE IT staff use the CVS document repository on this machine on a regular basis. All documents in the repository are owned by the cvs group, of which all IT staff are members.

Gateway Services

IT staff use the resources of this system for daily administrative tasks in the production environment. This system enjoys network access to all machines in the production environment, and at least one account (dbmng) uses SSH keys for passwordless authentication for use in scripts. Database administrators move large amounts of data across the WAN to this system, where they can take advantage of large amounts of storage space and dedicated

processing power. The preferred method of accessing the production environment is from a session on this system, though this is not enforced by routing or firewall policies.

Recommendations: Remove all accounts from this system that do not directly support the production environment (e.g., the developers). Disallow direct login to the dbmng account:

```
chuser login=false dbmng
```

Restrict access to dbmng's private key file to root:

```
chown root:dbmng /home/dbmng/.ssh/id_dsa
chmod 640 /home/dbmng/.ssh/id_dsa
```

and add the key to the TCB database:

```
tcbck -a /home/dbmng/.ssh/id_dsa acl checksum class=audit group owner
```

In addition, place restrictions on the deployed public keys (ip address, no agent forwarding, no X11 forwarding), to render the private key useless from other addresses. See Secure Shell.

Data Collection

The dbmonitor script that gathers production server database statistics runs from the cricket user's crontab. The script logs in to standard user accounts on the target systems. These connections are made with SSH, using a pair of private and public keys with a blank passphrase for all targets.

Recommendations: Create a dedicated account to run this script, and do not use the cricket user. The script can then save the html status pages and data files in a location where the web server and Cricket data collecting and querying scripts can process them. (See dbmonitor, v1.0 and Cricket, v1.03 regarding the private SSH keys.)

Monitoring

IT staff monitor the status of production servers and applications using a web site on this system that serves frequently updated static web pages. No authentication requirements or address restrictions are in place for this site. Personnel in remote data centers have indirect access to this site through a specific server on the local subnet that provides proxying and portal services.

Recommendations: Configure the web server to accept requests for this site only from the portal server's address and from IT-MGT-01 itself (e.g., via portforwarding over SSH). See also dbmonitor, v1.0 and Cricket, v1.03 and Apache in the Applications section.

Datacenter Operators

Remote Datacenter staff are not employees of GIACE, but of individual organizations with whom GIACE has contractual agreements. The accounts for these users are centrally administered by GIACE staff, using NIS. Remote Datacenter staff account logins are restricted to particular hosts by inclusion in NIS netgroup maps, which allow one group access while explicitly denying every other group. Datacenter staff use their accounts to run menu driven utility scripts, which sudo to a local utility account to execute commands permitted in the sudo configuration file (and log all activity). Their duties are to rotate backup tapes, stop and start databases, and assist with occasional hardware maintenance tasks such as replacing drives, power supplies and memory. The degree of trust and familiarity between GIACE and Datacenter staff has at times been strained due to aggressive deployment schedules and hasty installations. Again, the security of user accounts at remote datacenters is not under GIACE's direct control.

Recommendations: Make security considerations a priority in all partnership agreements,[10] and explicitly state

the responsibilities and obligations of remote datacenter staff to abide by GIACE policies.

Storage Management

The hard disk storage on this system has been configured for redundancy and divided among file systems in support of the various activities that it hosts.

Backups

There is no dedicated backup device. Backups are currently performed by tarring and ftping files to another host that has a tape drive. Backup media for corporate and datacenter hosts are rotated offsite using a data storage service. The media are picked up each weekday, and a weekly archive is stored for 2 months, a monthly archive is stored for 6 months, and yearly archives are stored permanently.

Recommendations: Dedicate a backup device to this system, and include backups in an off-site rotation with a data-storage service. The ftp protocol is insecure, and should not be used with sensitive data. Storing this host's backups on the media of another system, one that does not have the same schedules and priorities, is confusing and risky.

Disks

The system has two pairs of equally sized disks:

```
[auditman@IT-MGT-01] /home/auditman/work/ssec $ lscfg | grep Disk

+ fda0             01-D1            Standard I/O Diskette Adapter
+ hdisk0           1S-08-00-8,0     16 Bit LVD SCSI Disk Drive (36400
+ hdisk1           1S-08-00-9,0     16 Bit LVD SCSI Disk Drive (36400
+ hdisk2           1S-08-00-10,0    16 Bit LVD SCSI Disk Drive (73400
+ hdisk3           1S-08-00-11,0    16 Bit LVD SCSI Disk Drive (73400
```

Partitions and Volumes

The disks are configured as two volume groups (VGs), rootvg and datavg, each containing a dozen or so logical volumes and file systems.

```
[auditman@IT-MGT-01] /home/auditman/work/ssec $ lsvg
rootvg
datavg
```

From the output of the command lspv, the assignment of physical volumes (e.g., hard disks) to volume groups is:

```
[auditman@IT-MGT-01] /home/auditman/work/ssec $ lspv
hdisk0          000408cac91f364c                    rootvg
hdisk1          000408caeba1536e                    rootvg
hdisk2          000408cae54fad6e                    datavg
hdisk3          000408caebcd0974                    datavg
```

The command:

```
lsvg -o | lsvg -i -l
```

provides a summary of the physical volumes (PV's) that make up rootvg and datavg, the physical partitions (PP's) into which they are divided, and the logical partitions (LP's) created by mirroring (there are 2 PP's for every LP). hdisk0 and hdisk1 have been mirrored to create rootvg, and hdisk2 and hdisk3 have been mirrored to create datavg.

```
[auditman@IT-MGT-01] /home/auditman $ lsvg -o | lsvg -i -l

datavg:

LV NAME             TYPE       LPs   PPs   PVs  LV STATE      MOUNT POINT
lv_data             jfs        80    160   2    open/syncd    /data
lv_logs             jfs        8     16    2    open/syncd    /logs
lv_stats            jfs        8     16    2    open/syncd    /stats
lv_www              jfs        8     16    2    open/syncd    /www
lv_wise             jfs        40    80    2    open/syncd    /wise
lv_source           jfs        80    160   2    open/syncd    /export/lpp_source
lv_spot             jfs        40    80    2    open/syncd    /export/spot
lv_backup           jfs        160   320   2    open/syncd    /backup
loglv00             jfslog     1     2     2    open/syncd    N/A
lv_scripts          jfs        8     16    2    open/syncd    /scripts
lv_cvswsipc         jfs        8     16    2    open/syncd    /cvswsipc
rootvg:
LV NAME             TYPE       LPs   PPs   PVs  LV STATE      MOUNT POINT
hd5                 boot       1     2     2    closed/syncd  N/A
hd6                 paging     8     16    2    open/syncd    N/A
hd8                 jfslog     1     2     2    open/syncd    N/A
hd4                 jfs        2     4     2    open/syncd    /
hd2                 jfs        15    30    2    open/syncd    /usr
hd9var              jfs        1     2     2    open/syncd    /var
hd3                 jfs        1     2     2    open/syncd    /tmp
hd1                 jfs        16    32    2    open/syncd    /home
hd10opt             jfs        16    32    2    open/syncd    /opt
lv_local            jfs        16    32    2    open/syncd    /usr/local
lv_images           jfs        16    32    2    open/syncd    /usr/sys/inst.images
lv_dump             jfs        16    32    2    open/syncd    /var/adm/dump
lv_work             jfs        80    160   2    open/syncd    /work
lv_swdist           jfs        80    160   2    open/syncd    /work/swdist
lv_makebff          jfs        80    160   2    open/syncd    /work/makebff
```

File Systems

This system provides software and work areas for system administrators, and hosts databases, a repository of documentation about the environment, and web sites that publish documentation and status information. The mounted filesystems correspond roughly to these uses of the system. The mount command lists filesystems and their attributes. (Note that all filesystems are mounted "rw".)

```
[auditman@IT-MGT-01] /home/auditman/work/ssec $ mount
  node       mounted        mounted over    vfs       date        options
-------- ---------------  ---------------  ------ ------------ ---------------
         /dev/hd4         /                jfs    May 02 22:06 rw,log=/dev/hd8
         /dev/hd2         /usr             jfs    May 02 22:06 rw,log=/dev/hd8
         /dev/hd9var      /var             jfs    May 02 22:06 rw,log=/dev/hd8
         /dev/hd3         /tmp             jfs    May 02 22:06 rw,log=/dev/hd8
         /dev/hd1         /home            jfs    May 02 22:07 rw,log=/dev/hd8
         /proc            /proc            procfs May 02 22:07 rw
         /dev/hd10opt     /opt             jfs    May 02 22:07 rw,log=/dev/hd8
         /dev/lv_local    /usr/local       jfs    May 02 22:07 rw,log=/dev/hd8
         /dev/lv_images   /usr/sys/inst.images jfs    May 02 22:07 rw,log=/dev/hd8
         /dev/lv_dump     /var/adm/dump    jfs    May 02 22:07 rw,log=/dev/hd8
         /dev/lv_work     /work            jfs    May 02 22:07 rw,log=/dev/hd8
         /dev/lv_swdist   /work/swdist     jfs    May 02 22:07 rw,log=/dev/hd8
         /dev/lv_makebff  /work/makebff    jfs    May 02 22:07 rw,log=/dev/hd8
         /dev/lv_source   /export/lpp_source jfs    May 02 22:07 rw,log=/dev/loglv00
         /dev/lv_spot     /export/spot     jfs    May 02 22:07 rw,log=/dev/loglv00
         /dev/lv_scripts  /scripts         jfs    May 02 22:07 rw,log=/dev/loglv00
         /dev/lv_data     /data            jfs    May 02 22:07 rw,log=/dev/loglv00
         /dev/lv_logs     /logs            jfs    May 02 22:07 rw,log=/dev/loglv00
         /dev/lv_stats    /stats           jfs    May 02 22:07 rw,log=/dev/loglv00
         /dev/lv_www      /www             jfs    May 02 22:07 rw,log=/dev/loglv00
         /dev/lv_exch     /exch            jfs    May 02 22:07 rw,log=/dev/loglv00
```

```
/dev/lv_backup   /backup          jfs    May 02 22:07 rw,log=/dev/loglv00
/dev/lv_cvsgiace /cvsgiace        jfs    May 02 22:07 rw,log=/dev/loglv00
```

The df command gives an indication of size and usage:

```
[auditman@IT-MGT-01] /home/auditman/.ssh $ df -k
Filesystem    1024-blocks      Free %Used    Iused %Iused Mounted on
/dev/hd4           131072     80512   39%     1773     3% /
/dev/hd2           983040    159356   84%    25465    11% /usr
/dev/hd9var         65536     35884   46%      796     5% /var
/dev/hd3            65536     63352    4%       55     1% /tmp
/dev/hd1          1048576    855752   19%     7119     3% /home
brroc                   -         -    -        -     -  brroc
/dev/hd10opt      1048576    858068   19%     3019     2% /opt
/dev/lv_local     1048576    923904   12%     1006     1% /usr/local
/dev/lv_images     1048576    982792    7%       41     1% /usr/sys/inst.images
/dev/lv_dump      1048576   1015612    4%       17     1% /var/adm/dump
/dev/lv_work      5242880   3189340   40%     5331     1% /work
/dev/lv_swdist     5242880   5078268    4%       17     1% /work/swdist
/dev/lv_makebff     5242880   4160308   21%      539     1% /work/makebff
/dev/lv_source    10485760   3462780   67%     4167     1% /export/lpp_source
/dev/lv_spot      5242880   4650400   12%    15146     2% /export/spot
/dev/lv_scripts     1048576   1014980    4%      140     1% /scripts
/dev/lv_data     10485760   7191256   32%      893     1% /data
/dev/lv_logs      1048576   1015160    4%       90     1% /logs
/dev/lv_stats     1048576   1015564    4%       29     1% /stats
/dev/lv_www       1048576   1015612    4%       17     1% /www
/dev/lv_exch      5242880   4441712   16%    12502     1% /exch
/dev/lv_backup    20971520  12399024   41%      256     1% /backup
/dev/lv_cvsgiace     1048576    946884   10%     1682     1% /cvsgiace
```

Recommendations: Mount all jfs filesystems with the nosuid option, except / (root), /exch, /opt, /usr, and /usr/local, to disable execution of setuid and setgid programs (see SetUID and SetGID Files). Mount all jfs filesystems with the nodev option to disable opening of devices, except / (root).

File Ownership

Here are the intended purposes of these filesystems and a summary of user and group ownership. This list was generated by recursively listing files (ls -lR) underneath each mount point, using awk to extract the uid and gid fields, and piping to sort and uniq.

mount point	purpose	uid	gid
/	root of the tree	various files, owned by root, sys, bin, 11, 188, and individual users	root, bin, sys, system, adm, audit, security, ipsec, 11, 188
/backup	online backups	root	sys
/cvsgiace	IT management document repository	root, GIACE IT staff users	cvs, cvsadmin, system
/data	user data - each user has a directory here, linked to their home directory	root, GIACE IT staff users, sshd	dbmng, staff, sys, system
/exch	giace db environment (contains Progress suid programs)	306, 35968, bin, dbmng, GIACE IT staff users, nobody, relmgr, root, sysadm	203, 99, adm, bin, dbmng, develop, nobody, security, sys, system
/export/lpp_source	staging point for NIM resources	root	sys, system
/export/spot	staging point for NIM resources	11, adm, bin, guest, root, sys, uucp	11, adm, audit, bin, cron, mail, printq, security, shutdown, staff,

			sys, system, usr, uucp
/home	parent for user home directories	auditman, GIACE IT staff users, danpierr, dbmng, dbuser, dcmgr, dcopr, guest, ibmce, root, sshd, sysadm	102, cvs, dbmng, develop, operator, staff, sys, system, usr
/logs	database log file archives	sys, system	dbmng, root, sys
/opt	AIX Linux toolbox	bin, root	bin, system
/scripts	scripts (not currently in use)	GIACE IT staff users, dbmng, root	dbmng, sys, system
/stats	production host statistics data storage (not currently in use)	root	sys, system
/tmp	temporary files	adm, GIACE staff users, bin, root	adm, bin, system
/usr	universal shared resources	11, 1134, 177, 188, 517, 987, adm, bin, nobody, root, sys, uucp	102, 11, 1134, 188, 517, 987, adm, audit, bin, cron, imnadm, mail, nobody, printq, security, shutdown, staff, sys, system, usr, uucp
/usr/local	common installation point for shared software	1134, 517, bb, bin, nobody, root	102, 1134, 517, bin, nobody, sys, system, usr
/usr/sys/inst.images	AIX software staging	root	sys
/var	system logs, spool filess, mail queues	188, adm, auditman, bin, daemon, dbmng, ipsec, nuucp, root, sys, sysadm, uucp	188, adm, bin, cron, dbmng, mail, printq, staff, sys, system, uucp
/var/adm/dump	AIX dump copy area	root	system
/work	work space for sysadmins (linked from home dirs)	101, 1029, 119, 360, auditman, GIACE IT staff users, root, sys	203, bb, dbmng, imnadm, perf, sys, system, usr,
/work/makebff	sysadmin	root	system
/work/swdist	software distribution point (not currently in use)	root	system
/www	web content (not currently in use)	root	system

Recommendations: Clean up individual users' files in the root filesystem. Many of these file systems have files with unknown users and groups -- their uid's and gid's lack entries in /etc/passwd, /etc/group, /etc/nis/passwd, and /etc/nis/group. These files appear to be from application distributions extracted from tar files. Examine the files using the find command and chown them to the users/groups who unpacked them, or remove them if not in use. For example:

```
find /work -user 1029
find /work -group 203
```

SetUID and SetGID Files

Files that execute programs with an effective user or group id different from their own are known as "set uid" (suid) and/or "set gid" (sgid), and can be a security risk. The following command lists suid and sgid files.

```
find / -type f \( -perm -4000 -o -perm -2000 \) -exec ls -l {} \;
```

There are quite a few!

Recommendations: Remove all unused suid and sgid files, in particular those associated with lp or lpd, dt (CDE), and IMNSearch (Documentation Library). Confirm that all suid and sgid files are monitored as suggested in the discussion of the Trusted Computing Base.

Quotas and Limits

Quotas are enabled with the chfs command, which adds quota attributes to /etc/filesystems. On IT-MGT-01, only the /home filesystem has quotas:

```
# grep -p home /etc/filesystems
 /home:
        dev             = /dev/hd1
        vfs             = jfs
        log             = /dev/hd8
        mount           = true
        check           = true
        vol             = /home
        free            = false
        quota           = userquota
```

User quotas for the /home file system are stored in the file /home/quota.user using the edquota command. Quota statistics can be displayed with the command repquota -a. Quotas for GIACE IT staff are set for a soft limit of 75MB and a hard limit of 100MB. Quotas are enabled at boot by the following entries in the /etc/rc script, called by init as specified in /etc/inittab:

```
# echo "Enabling filesystem quotas"
/usr/sbin/quotacheck -a
/usr/sbin/quotaon -a
```

The file /etc/security/limits defines process resource limits for users. The default limits are:

```
default:
        fsize = -1
        core = 2097151
        cpu = -1
        data = 262144
        rss = 65536
        stack = 65536
        nofiles = 2000
```

Removable Storage

This system has no floppy disk drive. The CDROM drive can only be mounted by root, and the stanza in /etc/filesystems specifies no mount at boot. See recommendation in the discussion of the Physical Environment regarding a supervisory password and console access.

Sensitive Data

This system stores files that are critical to authentication, documentation, and monitoring operations in GIACE's production environment. These files are all included in the daily backup routine (see Backups and Disaster Recovery).

Authentication

Password files and NIS maps are stored in /etc, /etc/security, and /etc/nis, on the / (root) file system. These are used to manage user accounts throughout the production environment, for GIACE IT staff and remote datacenter

staff.

Private keys for individual users and utility accounts are stored in /home/[username]/.ssh/id_dsa. Individual users' keys are required to have passphrases, while those used by utility accounts (dbmng and cricket) are not. Corresponding public keys are distributed throughout the production environment; this is what qualifies the private keys as sensitive.

Recommendations: See dbmonitor, v1.0 and Cricket, v1.03 and Secure Shell regarding key use and management.

Documentation

GIACE staff maintain a CVS repository stored in /cvsgiace/systems, on the /cvsgiace file system. All systems documentation is committed to the repository, including configuration files, policies, training materials, event logs, scripts, and so forth. All GIACE staff have access to the entire repository, through membership in the group cvs. Passwords and SSH keys are not stored in the repository.

Recommendations: See cvspserver and Concurrent Versions System.

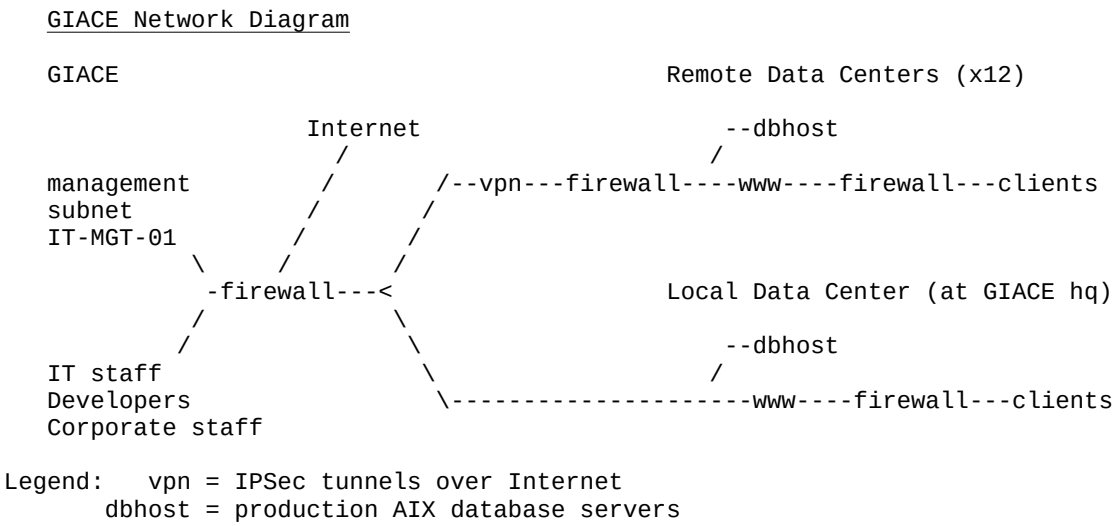
Monitoring

Data collected from hosts in the production environment are stored in /home/cricket/rawdata/ on the /home file system, and are used to provide GIACE and remote datacenter staff with status and historical information. The data files are owned by the user cricket and the group systems. The staff depend on the real-time status information the data provides in order to respond to problems in the production environment. The data itself are considered valuable for generating alerts. The historical statistics and graphs that are generated from this data by another process are not considered particularly sensitive.

Recommendations: See Disaster Recovery regarding a backup device, and in dbmonitor, v1.0 and Cricket, v1.03 regarding use of separate accounts for collecting and displaying data.

Network Environment and Services

GIACE's network connects a loose federation of remote data centers to a primary facility that houses one of the affiliated data centers and GIACE's LAN. The LAN consists of the management subnet upon which IT-MGT-01 is addressed, and a subnet hosting the workstations of GIACE's IT staff, programmers, and various corporate departments such as Human Resources and Marketing.



```
    www = web server
clients = end user hosts, connecting across Internet
```

Topology

The network is TCP/IP, with a Cisco 6509 switch at its core. VLANs on the switch cascade to 100Mb switches that provide connections to all resources in the facility. A Netscreen firewall provides stateful packet filtering of Internet traffic, inter-VLAN routing, and VPN services.

Remote data centers also have Netscreen firewalls, and are connected in a hub-and-spoke topology to the primary facility with VPN tunnels across the public Internet. While the resources and environment managed by eFortune within remote data centers is standardized and fairly homogenous, each remote data center also has independent ventures that share the Internet pipe and compete for bandwidth with eFortune's aspirations. All resources in the eFortune data center environment are privately addressed, and the VPN's interconnect only private address space. The Netscreen at each data center also provides a DMZ interface for a privately addressed subnet, and address translation for inbound requests for publicly accessible resources.

Network Access from Other Hosts

IT-MGT-01 is located on the IT management subnet, which is dedicated to servers. GIACE IT staff workstations are located on the Corporate LAN. Firewall policies place no restrictions on inbound or outbound traffic from this host to all production hosts and to all hosts on the corporate LAN. Inbound traffic from the Internet is blocked at the border firewall.

Recommendations: At the firewall for the management subnet on which this host is addressed, restrict connections as follows:

source	destination	protocol	source port	dest port	action
IT Staff Workstations	IT-MGT-01	ssh	any	TCP/22	permit
Prod NIS hosts	IT-MGT-01	any	any	any	permit
any	IT-MGT-01	any	any	any	deny
IT-MGT-01	Production hosts	ssh	any	TCP/22	permit
IT-MGT-01	Production NIS hosts	any	any	any	permit
IT-MGT-01	DNS server	dns	any	UDP/53	permit
IT-MGT-01	NTP-server	ntp	any	UDP/123	permit
IT-MGT-01	SMTP-server	smtp	any	TCP/25	permit
IT-MGT-01	syslog-server	syslog	any	UDP/514	permit
IT-MGT-01	any	any	any	any	deny

On IT-MGT-01 and every host configured as an NIS server, create the file /etc/securenets and add the host's loopback and host addresses. This will restrict each NIS server to only serving itself as a client.

```
#/etc/securenets
255.255.255.255         127.0.0.1
255.255.255.255         10.211.254.61
```

Until such time that NIS can be retired, all participating hosts must be servers and clients, and communications between IT-MGT-01 and other hosts must be secured by firewalls and VPN's. These policies will allow NIM to

function as well, but NIM must be disabled except during maintenance windows when no other traffic is allowed to remote hosts.

Two other methods of restricting network access to this host are TCP Wrappers and AIX's IP Security feature. TCP Wrappers provides service-specific access control for a default suite of applications -- systat, finger, ftp, telnet, rlogin, rsh, exec, tftp, and talk -- that should not be used on this system. The systems administrators are reluctant to recompile daemons for IT-MGT-01 with the wrapper's access controls, because doing so would complicate upgrades and support.[11]

AIX's IP Security software provides host-based packet filtering (installed as part of ipsec tunnel file sets.[12] If policies on the firewalls cannot be adjusted as desired, the *filt commands (genfilt, mkfilt, lsfilt, etc.) installed with the ipsec filesets will allow manual creation and manipulation of IP Security rules to achieve the same result.

In this situation, the firewalls that control LAN traffic and encrypt WAN traffic are the natural points for administering network policy.

Network Options

A number of denial of service attacks can be avoided by modifying the default behavior of the TCP/IP stack.

Recommendations: The following network options should be set each time the system boots using the network options command, /usr/sbin/no. Add the following to the /etc/rc.tcpip script:

```
/usr/sbin/no   -o clean_partial_conns=1
/usr/sbin/no   -o bcastping=0
/usr/sbin/no   -o directed_broadcast=0
/usr/sbin/no   -o ipignoreredirects=1
/usr/sbin/no   -o ipsendredirects=0
/usr/sbin/no   -o ipsrcroutesend=0
/usr/sbin/no   -o ipsrcrouterecv=0
/usr/sbin/no   -o ipsrcrouteforward=0
/usr/sbin/no   -o ip6srcrouteforward=0
/usr/sbin/no   -o icmpaddressmask=0
/usr/sbin/no   -o nonlocsrcroute=0
/usr/sbin/no   -o tcp_pmtu_discover=0
/usr/sbin/no   -o udp_pmtu_discover=0
/usr/sbin/no   -o ipforwarding=0
```

Network Client

IT-MGT-01 uses TCP/IP, and relies on DNS for name resolution, SMTP to send (but not receive) mail, and NTP to maintain accurate time.

IP Address

IT-MGT-01's IP address is 10.211.254.61/24, and its default route is through 10.1.254.1.

DNS

This system uses a Windows 2000 Domain Controller on the same subnet for DNS resolution of production resources:

```
# cat /etc/resolv.conf
nameserver 10.1.254.89
nameserver 10.1.254.90
domain exch.giace.net
```

Resolution is controlled by the file /etc/netsvc.conf:

```
# cat /etc/netsvc.conf
hosts=local,bind4
```

The local hosts file contains all production hosts with which this system routinely communicates, as well as ntp and smtp servers, so the DNS nameserver is rarely queried.

SMTP

The primary MX record for sending smtp mail to corporate addresses is an external, publicly accessible server.

```
# nslookup
Default Server:  giace-dom-02.exch.giace.net
Address:  10.1.254.89

> set type=MX
> giace.net
Server:  giace-dom-02.exch.giace.net
Address:  10.1.254.89

Non-authoritative answer:
giace.net       preference = 10, mail exchanger = billy.giace.net
giace.net       preference = 20, mail exchanger = bob.giace.net

Authoritative answers can be found from:
ns1.giace.wednet.edu  internet address = 172.16.13.5
ns2.giace.wednet.edu  internet address = 172.16.13.6
> quit
```

Recommendations: Change the primary and secondary MX records to an internal server, so that mail does not leave the trusted segment. Do not allow mail from this system to external addresses. Run sendmail from the command line rather than as a daemon (see Sendmail, v8.11.0).

NTP

This system is an ntp client, running xntp version 3.4y, and is synchronized with an internal stratum 2 server (see xntpd).

Network Services

Network services are among those started by the init command at boot, according to entries in /etc/inittab (http://publibn.boulder.ibm.com/doc_link/en_US/a_doc_lib/cmds/aixcmds5/telinit.htm).

Top 10 Vulnerabilities to Unix Systems

Before plunging into the details of individual services, here is a brief overview of IT-MGT-01 with regard to the SANS/FBI top 10 Unix vulnerabilities.[13] Eight of these are discussed in this report as noted.

1. Remote Procedure Calls — almost all of the RPC services listed are running (see inetd).
2. Apache Web Server — running (see Apache, v2.0.43).
3. Secure Shell — running (see Secure Shell (OpenSSH)).
4. SNMP — running (see rc.tcpip).
5. FTP — running (see ftp, telnet, shell, login, exec, cvspserver).
6. R-Services — running (see ftp, telnet, shell, login, exec, cvspserver).
7. Line Printer Daemon — commented out in rc.tcip and not running.

8.	Sendmail	running as a daemon (see Sendmail, v8.11.0).
9.	Bind/DNS	not installed.
10.	General Unix Authentication	clear text authentication methods are in use (see Concurrent Versions System Apache, v2.0.43, and also Network Information Service)

/etc/inittab

These are the entries in /etc/inittab that start network-related services (see Other Processes for the remaining /etc/inittab entries):

```
init:2:initdefault:
srcmstr:23456789:respawn:/usr/sbin/srcmstr # System Resource Controller
rctcpip:23456789:wait:/etc/rc.tcpip > /dev/console 2>&1 # Start TCP/IP daemons
nim:2:wait:/usr/bin/startsrc -g nim >/dev/console 2>&1
rcnfs:23456789:wait:/etc/rc.nfs > /dev/console 2>&1 # Start NFS Daemons
writesrv:23456789:wait:/usr/bin/startsrc -swritesrv
l2:2:wait:/etc/rc.d/rc 2
itess:23456789:once:/usr/IMNSearch/bin/itess -start search >/dev/null 2>&1
dt:2:wait:/etc/rc.dt
:httpdlite:23456789:once:/usr/IMNSearch/httpdlite/httpdlite -r /etc/IMNSearch/httpdlite/
apache:2:once:/etc/rc.apache >/dev/console 2>&1 # Apache Server start
```

The default run level is "2", multiuser, which determines the entries in inittab to be processed in the absence of a command-line parameter. Note that the mkitab command should be used to create records in /etc/inittab, and rmitab should be used to remove them.[14] A colon (":"), rather than a pound sign ("#") is required to disable entries.

We will examine each of these (and all the other services they start in turn).

/etc/rc.tcpip

This script checks whether SRC is running, starts it if necessary, and then issues a list of commands to start various daemons:

```
# Start up syslog daemon (for error and event logging)
start /usr/sbin/syslogd "$src_running"

# Start up the sendmail daemon.
qpi=30m  # 30 minute interval
#
start /usr/lib/sendmail "$src_running" "-bd -q${qpi}"

# Start up Portmapper
start /usr/sbin/portmap "$src_running"

# Start up socket-based daemons
start /usr/sbin/inetd "$src_running"

# Start up Network Time Protocol (NTP) daemon
start /usr/sbin/xntpd "$src_running"

# Start up the Simple Network Management Protocol (SNMP) daemon
start /usr/sbin/snmpd "$src_running"

# Start up the DPID2 daemon
start /usr/sbin/dpid2 "$src_running"

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

syslogd

Syslog is a valuable service for logging messages according to criteria specified in /etc/syslog.conf. See discussion of logs in Logging and Monitoring.

Recommendations: The production environment has not designated this system as the destination for syslog messages. As started from rc.tcpip, syslog listens for incoming messages on UDP port 514. Change rc.tcpip to configure syslogd to reject messages from other hosts with the "-r" flag:

```
start /usr/sbin/syslogd "$src_running" -r
```

(Note that some versions of syslogd have reversed the default, and use -r to enable receipt of messages.)

sendmail

Sendmail is started as a daemon, which listens on TCP port 25, the standard SMTP port.

Recommendations: This system does not need to receive smtp mail. Stop the sendmail daemon (stopsrc -s sendmail). Comment or delete this line from rc.tcpip.

portmap

The portmap daemon listens on TCP port 111, and responds to RPC requests for registered services by providing the port upon which a named service is running.

Recommendations: NIS and NIM related services are the only ones that should be served by portmap on this system, and in the event NIS is replaced and NIM is not being used, this entry should be commented out. All other RPC services, usually listed in /etc/inetd.conf, should be disabled. The command rpcinfo -p provides a list of services and ports that have registered with the portmapper.

inetd

The inetd daemon (/usr/sbin/inetd) manages network services, waiting for requests and starting processes to serve them. When started, inetd reads configuration information from /etc/inetd.conf. The following services are configured to start:

```
ftp     stream  tcp6    nowait  root    /usr/sbin/ftpd         ftpd
telnet  stream  tcp6    nowait  root    /usr/sbin/telnetd      telnetd -a
shell   stream  tcp6    nowait  root    /usr/sbin/rshd         rshd
login   stream  tcp6    nowait  root    /usr/sbin/rlogind      rlogind
exec    stream  tcp6    nowait  root    /usr/sbin/rexecd       rexecd
bootps  dgram   udp     wait    root    /usr/sbin/bootpd       bootpd /etc/bootptab
tftp     dgram  udp6    SRC     nobody  /usr/sbin/tftpd         tftpd -n
ntalk   dgram   udp     wait    root    /usr/sbin/talkd         talkd
daytime stream  tcp     nowait  root    internal
time    stream  tcp     nowait  root    internal
daytime dgram   udp     wait    root    internal
time    dgram   udp     wait    root    internal
ttdbserver      sunrpc_tcp      tcp     wait    root    /usr/dt/bin/rpc.ttdbserver rpc.t
wsmserver       stream  tcp     nowait  root    /usr/websm/bin/wsmserver wsmserver -star
dtspc   stream  tcp     nowait  root    /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd
cmsd    sunrpc_udp      udp     wait    root    /usr/dt/bin/rpc.cmsd cmsd 100068 2-5
cvspserver stream tcp nowait.100 root /usr/bin/env env - /usr/bin/cvs -f --allow-root=/c
```

According to the AIX documentation, /etc/inetd.conf can be updated with SMIT or edited manually. In the case of manual edits, force inetd to reread the file by issuing "refresh -s inetd". Here are recommendations for these services:

ftp, telnet, shell, login, exec, cvspserver

Recommendations: These services use insecure authentication and authorization methods, and should be disabled. Instead use SSH and scp, which provide secure replacements for each of these services, often with identical syntax.

bootps, tftp

These services are used by NIM for network-based installations.

Recommendations: These should be disabled in inetd.conf and started from the command line on an as-needed basis.

ntalk, daytime, time, ttdbserver, cmsd

Recommendations: These services are not used and should be disabled.

wsmserver

This is the web-based system manager. It is also available as an XWindow application.

Recommendations: Disable this service. If this application is required run the standalone version, /usr/websm/bin/wsm, and use X11-forwarding over SSH.

dtspc

This service launches applications and is part of the CDE.

Recommendations: This service is not used on this system. Disable this service.

xntpd

The xntpd daemon (which is started from rc.tcpip) sets and maintains time using version 3 of the Network Time Protocol (NTP). This system communicates with an ntp server specified in /etc/ntp.conf:

```
server 10.1.254.2
broadcastclient
driftfile /etc/ntp.drift
tracefile /etc/ntp.trace
```

The status of time synchronization looks good, as queried with the ntpq command:

```
# ntpq
ntpq> peers
     remote           refid      st t when poll reach   delay   offset    disp
==============================================================================
*10.1.254.2      onetime.giace.o  2 u   13   64  377     0.31   -0.080    0.53
ntpq> q
```

Recommendations: Add one or two more ntp servers to /etc/ntp.conf to increase accuracy and redundancy.

snmpd, dpid2, and hostmibd

The Simple Network Management Protocol daemon, snmpd, responds to SNMP queries for status information,

and can also be configured to send alerts to other hosts. The dpid2 assists in SNMP communications, and hostmibd is an agent that maintains the Management Information Base (MIB) for a client. At present, SNMP monitoring is not in use.

Recommendations: Disable these services. If SNMP is enabled in the future, configure /etc/snmpd.conf with specific community strings and filter SNMP traffic at all firewalls.

NIM (/usr/sbin/nim), NFS and NIS (/etc/rc.nfs)

See Network Installation Management (NIM) for discussion. NFS is only used on this system in conjunction with NIM. The yp daemons for Network Information Service (NIS) are started from the rc.nfs script.

Recommendations: Disable this service and its supporting services of tftpd, bootp, nfs, and rsh, and only enable as needed during maintenance windows. Separate the startup of NIS from NFS by copying rc.nfs to a new script. Comment out the yp commands in rc.nfs, and the nfs commands in the new script. Add an entry in /etc/inittab for the new script.

writesrv

The writesrv daemon allows users to send/receive messages to/from remote systems.

Recommendations: This service is not used, and should be disabled.

rc (/etc/rc.d/rc 2)

The /etc/rc.d/rc script accepts a run level parameter, which it uses to enumerate and then run all the scripts in the corresponding subdirectory of rc.d. In the case of run level 2, all the scripts in /etc/rc.d/rc2.d/ that start with "K" (for kill) are run first, followed by all the scripts that start with "S" (for start). The only scripts present on this system in any subdirectory under /etc/rc.d/ are the K and S scripts for the Secure Shell daemon, sshd.

Secure Shell (OpenSSH)

OpenSSH for AIX 5.1 (OpenSSH_3.4p1) has been installed with an IBM-provided fileset for AIX 5.1, and is started at boot via the /etc/rc.d/rc script, which calls /etc/rc.d/rc2.d/Ssshd. The sshd daemon provides authentication and encrypted transport services to clients using SSH. Though ssh and scp effectively replace telnet, ftp, rlogin, rsh and rcp, both new and old methods are in use. Scripts used to manage the production environment are being rewritten to use SSH and key-based authentication rather than plaintext passwords stored in files. However, this process is not complete, and many routines used to initialize applications at new datacenters rely on ftp.

System administrators stated the following informal policy for use of SSH keys on production hosts: If the keys are used to support the production infrastructure, they must be generated, installed and managed by a designated administrator. Otherwise, individuals are responsible for managing their own keys, which they may only use to connect to their own accounts. Only infrastructure keys may have blank passphrases. The infrastructure keys and associated configuration files are periodically collected, tarred, and stored on a corporate fileshare to which only the designated administrator has access.

Recommendations: Disable telnet, ftp, rlogin, rsh and rcp on this system and every production host, and require SSH for remote connections by scripts and users. Educate the programming staff with regard to the benefits and uses of ssh and scp.

Public-key based authentication is a powerful tool that should be tightly controlled by systems administrators and not left to individual users.[15] Carefully document the matrix of private and public keys used in support of the production infrastructure. In /etc/sshd/sshd_config, centralize and restrict access to authorized_keys files with an entry such as:

```
AuthorizedKeysFile   /etc/ssh/keys/%u/authorized_keys
```

This specifies user-specific directories under /etc/ssh/keys/. GIACE should establish a process with which users implement passphrase-protected key-pairs. Users can generate the keys, store their private key in a specific, well-secured location on their workstations, and provide the public key to a systems administrator for distribution to the production environment.

Consider also imposing user, group, and authentication method restrictions. Accounts used by automated processes should not be able to login interactively. In the authorized_keys files, use options to control source addresses, X11 forwarding, agent forwarding, pseudo-terminal allocation, and the commands the client is permitted to run.[16]

Do not store the tarred keys on a corporate fileshare. Rather, burn them to a CD and store them offsite.

An SSH agent enhances the use of keys by responding to authentication requests on the user's behalf. Once public keys are in place, GIACE staff that launch an agent on their workstations can access production resources without repeatedly typing a password, and the private key does not need to be stored on any production system. Agent forwarding would allow the same agent to handle authentication requests from an initial connection to IT-MGT-01, and subsequent connections to other production hosts. This would be particularly useful if firewall policies required that all connections to production hosts be made from IT-MGT-01.

Consider these questions when developing policies for keys:

1. How secure are the private keys?

Stronger than passwords alone, as long as they have long passphrases and restrictions are placed on the public keys. A better question might be "How secure are the workstations?"

2. Isn't it dangerous to allow access to the entire production environment with only one password?

Perhaps, if the user's workstation is left logged in and unattended. The user must have the private key and the passphrase, and access will be constrained by sshd configuration settings. One option would be to combine unfettered access with no rights, and require sudo to do anything.

3. Won't generation and distribution of keypairs be a headache?

Yes. However, it's worth it. Just as with password lists, it is better to know what's out there.

/etc/rc.dt

Login service for the Common Desktop Environment.

Recommendations: This service is not used on this system, and should be disabled.

httpdlite (/usr/IMNSearch/httpdlite/httpdlite)

This is an http server included with the Documentation Library Service.

Recommendations: Do not use this server. Leave it disabled (with the leading ":") in /etc/inittab.

apache (/etc/rc.apache)

This is a startup script for the Apache HTTP Server. See Apache, v2.0.43.

Listening Processes

A port scan using insecure.org's Nmap scanner, run from a server on the same subnet as IT-MGT-01, lists the following open TCP ports:

```
$nmap -sT 10.211.254.61
Starting nmap 3.27 ( www.insecure.org/nmap/ ) at 2003-06-08 16:05 PDT
Interesting ports on 10.211.254.61:
(The 1599 ports scanned but not shown below are in state: closed)
Port       State       Service
13/tcp     open        daytime
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     open        telnet
37/tcp     open        time
80/tcp     open        http
111/tcp    open        sunrpc
199/tcp    open        smux
512/tcp    open        exec
513/tcp    open        login
514/tcp    open        shell
657/tcp    open        unknown
683/tcp    open        unknown
766/tcp    open        unknown
938/tcp    open        unknown
1058/tcp   open        nim
1059/tcp   open        nimreg
2049/tcp   open        nfs
2401/tcp   open        cvspserver
6000/tcp   open        X11
6112/tcp   open        dtspc
9090/tcp   open        zeus-admin
32771/tcp  open        sometimes-rpc5

Nmap run completed -- 1 IP address (1 host up) scanned in 0.863 seconds
```

The lsof command, installed from lsof-4.61-2.aix5.1.ppc.rpm from IBM's site, is a valuable tool to identify the unknown services:

```
[auditman@IT-MGT-01] /home/auditman $ lsof -i tcp:657
COMMAND  PID USER   FD   TYPE     DEVICE SIZE/OFF NODE NAME
rmcd    4410 root   10u  IPv4 0x706071e4      0t0  TCP *:rmc (LISTEN)

[auditman@IT-MGT-01] /home/auditman $ lsof -i tcp:683
COMMAND   PID USER   FD   TYPE     DEVICE SIZE/OFF NODE NAME
ypserv  11098 root    4u  IPv4 0x706601e4      0t0  TCP *:683 (LISTEN)

[auditman@IT-MGT-01] /home/auditman $ lsof -i tcp:766
COMMAND   PID USER   FD   TYPE     DEVICE SIZE/OFF NODE NAME
ypbind  11614 root   20u  IPv4 0x7064e9e4      0t0  TCP *:766 (LISTEN)

[auditman@IT-MGT-01] /home/auditman $ lsof -i tcp:938
COMMAND     PID USER   FD   TYPE     DEVICE SIZE/OFF NODE NAME
rpc.ypupd 11362 root   20u  IPv4 0x7064e1e4      0t0  TCP *:938 (LISTEN)

[auditman@IT-MGT-01] /home/auditman $ lsof -i TCP:9090
COMMAND  PID USER   FD   TYPE     DEVICE SIZE/OFF NODE NAME
inetd   7998 root   17u  IPv4 0x7056dde4      0t0  TCP *:wsmserver (LISTEN)

[auditman@IT-MGT-01] /home/auditman $ lsof -i TCP:32771
COMMAND   PID USER   FD   TYPE     DEVICE SIZE/OFF NODE NAME
dpid2    9288 root    5u  IPv4 0x7066d5e4      0t0  TCP *:32771 (LISTEN)
```

These services are all expected. A scan of UDP ports yields the following:

```
[root@localhost root]# nmap -sU 10.211.254.61

Starting nmap 3.27 ( www.insecure.org/nmap/ ) at 2003-06-08 16:54 PDT
Interesting ports on 10.211.254.61:
(The 1430 ports scanned but not shown below are in state: closed)
Port       State       Service
13/udp     open        daytime
37/udp     open        time
67/udp     open        dhcpserver
69/udp     open        tftp
111/udp    open        sunrpc
123/udp    open        ntp
161/udp    open        snmp
177/udp    open        xdmcp
514/udp    open        syslog
518/udp    open        ntalk
602/udp    open        unknown
651/udp    open        unknown
652/udp    open        unknown
653/udp    open        unknown
683/udp    open        unknown
712/udp    open        unknown
713/udp    open        unknown
755/udp    open        unknown
766/udp    open        unknown
768/udp    open        unknown
777/udp    open        unknown
778/udp    open        unknown
784/udp    open        unknown
804/udp    open        unknown
806/udp    open        unknown
834/udp    open        unknown
848/udp    open        unknown
889/udp    open        unknown
894/udp    open        unknown
898/udp    open        unknown
930/udp    open        unknown
932/udp    open        unknown
938/udp    open        unknown
942/udp    open        unknown
946/udp    open        unknown
962/udp    open        unknown
978/udp    open        unknown
1006/udp   open        unknown
1023/udp   open        unknown
2049/udp   open        nfs
32774/udp  open        sometimes-rpc12

Nmap run completed -- 1 IP address (1 host up) scanned in 12.361 seconds
```

Again, lsof can be used to determine the unknown services, as seen in the summarized output of the command:

```
lsof -i udp:[portnumber]

COMMAND   PID USER   FD   TYPE     DEVICE SIZE/OFF NODE NAME
bootpd  11870 root   21u  IPv4 0x70776200      0t0  UDP *:602
bootpd  11870 root   21u  IPv4 0x70776200      0t0  UDP *:602
httpd   19094 nobody   20u  IPv4 0x70788400      0t0  UDP *:651
httpd   17834 nobody   20u  IPv4 0x70788d00      0t0  UDP *:652
sshd    35222 root   20u  IPv4 0x74f1db00      0t0  UDP *:653
ypserv  11098 root   20u  IPv4 0x70776500      0t0  UDP *:683
httpd   18344 nobody   20u  IPv4 0x70788300      0t0  UDP *:712
sshd    27672 root   20u  IPv4 0x707be600      0t0  UDP *:713
sshd    19658 danbob   20u  IPv4 0x70550600      0t0  UDP *:755
ypbind  11614 root   21u  IPv4 0x70776600      0t0  UDP *:766
httpd   17546 nobody   20u  IPv4 0x70788600      0t0  UDP *:768
```

```
sshd    22632 root   20u  IPv4 0x70791700      0t0  UDP *:777
httpd   25192 nobody   20u  IPv4 0x707d0200      0t0  UDP *:778
sshd    35362 root   20u  IPv4 0x7271e500      0t0  UDP *:784
sshd    33700 auditman   20u  IPv4 0x74f32a00      0t0  UDP *:804
sshd    24374 root   20u  IPv4 0x707c7d00      0t0  UDP *:806
sshd    32458 auditman   20u  IPv4 0x75094700      0t0  UDP *:834
sshd    27384 danbob   20u  IPv4 0x707b5a00      0t0  UDP *:848
sshd    16824 root   20u  IPv4 0x70322900      0t0  UDP *:889
httpd   26582 nobody   20u  IPv4 0x70791600      0t0  UDP *:894
sshd    32522 root   20u  IPv4 0x707c3600      0t0  UDP *:898
httpd   17290 nobody   20u  IPv4 0x70788100      0t0  UDP *:930
sshd    30012 danbob   20u  IPv4 0x707edd00      0t0  UDP *:932
rpc.ypupd 11362 root   21u  IPv4 0x70776f00      0t0  UDP *:938
sshd    30446 auditman   20u  IPv4 0x7502b400      0t0  UDP *:942
sshd    33418 root   20u  IPv4 0x7502b600      0t0  UDP *:946
httpd   24954 nobody   20u  IPv4 0x707e2a00      0t0  UDP *:962
sshd    22850 danbob   20u  IPv4 0x707b5200      0t0  UDP *:978
httpd   27966 nobody   20u  IPv4 0x707c7c00      0t0  UDP *:1006
rpc.yppas 12660 root    3u  IPv4 0x70788800      0t0  UDP *:1023
```

These services are expected. (A UDP scan is often misleading because ports are deemed "open" due to non-receipt of a reset packet.)

Recommendations: The lsof utility is installed sgid and world executable.

```
[auditman@IT-MGT-01] /home/auditman $ lsof -h
lsof 4.61
 latest revision: ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/
. . .
Anyone can list all files; /dev warnings enabled; kernel ID check enabled.


[auditman@IT-MGT-01] /home/auditman/ $ ls -al `which lsof`
lrwxrwxrwx   1 root     system           28 Jan 06 12:57 /usr/sbin/lsof -> \
../../opt/freeware/sbin/lsof

[auditman@IT-MGT-01] /home/auditman/ # ls -al /opt/freeware/sbin/lsof
-rwxr-sr-x   1 root     system       136711 Sep 09 2002  /opt/freeware/sbin/lsof
```

Restrict execution of lsof to root and the system group:

```
chmod 0750 /opt/freeware/sbin/lsof
```

Other Processes

These non-network processes are started by init as listed in /etc/inittab.

```
init:2:initdefault:
brc::sysinit:/sbin/rc.boot 3 >/dev/console 2>&1 # Phase 3 of system boot
powerfail::powerfail:/etc/rc.powerfail 2>&1 | alog -tboot > /dev/console \
                                                # Power Failure Detection
load64bit:2:wait:/etc/methods/cfg64 >/dev/console 2>&1 # Enable 64-bit execs
rc:23456789:wait:/etc/rc 2>&1 | alog -tboot > /dev/console # Multi-User checks
fbcheck:23456789:wait:/usr/sbin/fbcheck 2>&1 | alog -tboot > /dev/console \
                                                # run /etc/firstboot
srcmstr:23456789:respawn:/usr/sbin/srcmstr # System Resource Controller
cron:23456789:respawn:/usr/sbin/cron
piobe:2:wait:/usr/lib/lpd/pio/etc/pioinit >/dev/null 2>&1  # pb cleanup
qdaemon:23456789:wait:/usr/bin/startsrc -sqdaemon
uprintfd:23456789:respawn:/usr/sbin/uprintfd
shdaemon:2:off:/usr/sbin/shdaemon >/dev/console 2>&1 # High availability daemon
l2:2:wait:/etc/rc.d/rc 2
```

```
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
l7:7:wait:/etc/rc.d/rc 7
l8:8:wait:/etc/rc.d/rc 8
l9:9:wait:/etc/rc.d/rc 9
ctrmc:2:once:/usr/bin/startsrc -s ctrmc > /dev/console 2>&1
logsymp:2:once:/usr/lib/ras/logsymptom # for system dumps
pmd:2:wait:/usr/bin/pmd > /dev/console 2>&1 # Start PM daemon
diagd:2:once:/usr/lpp/diagnostics/bin/diagd >/dev/console 2>&1
cons:0123456789:respawn:/usr/sbin/getty /dev/console
```

brc (/sbin/rc.boot)

This startup script performs critical base device configuration.

powerfail (/etc/rc.powerfail)

An extensive script used to gracefully shutdown the system "when init receives a SIGPWR signal from the kernel."[17] (rc.powerfail Command)

load64bit (/etc/methods/cfg64)

Enable AIX 5.1's 64-bit kernel extensions (note: this is not the 64-bit kernel).[3b]

rc (/etc/rc)

The script /etc/rc performs a laundry list of startup functions including setting environment variables, varying-on volume groups, activating swap space, configuring dump devices, checking file systems, mounting filesystems, cleaning up login and vi editor session leftovers, and enabling filesystem quotas. The results are piped to "alog -tboot", which logs to /var/adm/ras/bootlog, as shown by the query:

```
[root@IT-MGT-01] /etc/rc.d # alog -L -t boot
#file:size:verbosity
/var/adm/ras/bootlog:8192:1
[root@IT-MGT-01] /etc/rc.d #
```

fbcheck (/usr/sbin/fbcheck)

This script checks for the file "/etc/firstboot", which it renames and executes if found. Software installations often rely on this check.

srcmstr (/usr/sbin/srcmstr)

The System Resource Controller daemon spawns and controls subsystems.[18]

cron

The cron daemon runs scheduled shell commands. See the discussion of currently scheduled crontab entries in Cron Jobs.

piobe, qdaemon

qdaemon is used to schedule printing jobs, and calls piobe to spool them.

Recommendations: These services are not in use and should be disabled.

uprintfd

The uprintfd daemon is used to write kernel messages to processes' controlling terminals.

shdaemon

The shdaemon is a daemon that runs at the highest process priority, to detect and allow a systems administrator to recover from situations in which many high priority processes hog the CPU.

ctrmc

This daemon is a subsytem of IBM's Reliable Scalable Cluster Technology Resource Monitoring and Control application.

logsymptom

This daemon manages system dumps.

itess

This is part of IBM's Documentation Library Service, a cgi and web-based client/server application which IBM recommends installing even if you don't want to, because other applications might depend on it for their documentation.[19]

Recommendations: Disable this service. Use the Internet for documentation, or install this service on a non-production system.

Applications

A variety of applications have been installed on this system in support of its many roles in GIACE's production environment. While there is no explicit policy regarding installation of software, in interviews IT staff articulated a defacto policy that any changes to installed applications must be requested of and performed by the primary system administrators for this system. The system administrators state that the software's functionality and support, cleanliness of installation, and non-interference with OS upgrades are considerations for new installations.

Recommendations: Identify specific personnel who are authorized to install applications on this system. Charge those persons with the responsibility to verify signatures of open source applications, test an application on some other system, identify which accounts will have access, and document the installation.

Apache, v2.0.43

The Apache web server[20] was compiled from open source. It serves database status html pages generated by Perl script dbmonitor, Cricket's cgi scripts for graphing data, and CVSWeb.cgi for access to the CVS document repository. Recommendations for Apache have been collected at the end of this section.

```
[auditman@IT-MGT-01] /usr/local/apache-2.0.43/bin $ httpd -v
Server version: Apache/2.0.43
Server built:   Dec  4 2002 12:45:57
```

The server's root is the absolute path to the parent of the configuration, error and log file directories:

```
ServerRoot "/usr/local/apache-2.0.43"
```

The server root is owned by root:sys.

```
[root@IT-MGT-01] /usr/local # ls -dl apache-2.0.4
drwxr-sr-x  15 root     sys             512 May 09 12:09 apache-2.0.43
```

The server is run under the user account nobody, thus only world-readable files will be served.

```
User nobody
Group nobody
```

The server name is set to an IP address:

```
ServerName 10.211.254.61:80
```

The document root is the default:

```
DocumentRoot "/usr/local/apache-2.0.43/htdocs"
```

The default settings for directory permissions:

```
<Directory />
    Options FollowSymLinks
    AllowOverride None
    Order Allow,Deny
    Deny from All
</Directory>
```

Specific directory permissions have been set on the document root. These restrict access to workstations on the corporate LAN, and require basic authentication with a username/password. A single shared username/password combination has been generated and stored in a file in the conf directory. SSL encryption is not used.

```
<Directory "/usr/local/apache-2.0.43/htdocs">
    AuthType Basic
    AuthName "GIACE Systems and Network Management"
    AuthUserFile /usr/local/apache-2.0.43/conf/passwords
    Require valid-user
    Order Allow,Deny
    Allow from 10.211.254.0/24
    Allow from 172.18.12.0/24
    Allow from 172.3.4.0/24
    Allow from 172.3.5.129/23
    Satisfy All
    Options FollowSymLinks
    AllowOverride None
</Directory>
```

Identical permissions have been set for the Apache manual:

```
<Directory "/usr/local/apache-2.0.43/manual">
    Options Indexes FollowSymLinks MultiViews IncludesNoExec
    AddOutputFilter Includes html
    AllowOverride None
    AuthType Basic
    AuthName "GIACE Systems and Network Management"
    AuthUserFile /usr/local/apache-2.0.43/conf/passwords
    Require valid-user
    Order Allow,Deny
    Allow from 10.211.254.0/24
```

```
    Allow from 172.18.12.0/24
    Allow from 172.3.4.0/24
    Allow from 172.3.5.129/23
    Satisfy All
</Directory>
```

The absolute path for the cgi script directory is aliased as cgi-bin, and has the same set of permissions. This directory contains the CVSWeb.cgi script for read access to the CVS repository.

```
ScriptAlias /cgi-bin/ "/usr/local/apache-2.0.43/cgi-bin/"

<Directory "/usr/local/apache-2.0.43/cgi-bin">
    AuthType Basic
    AuthName "GIACE Systems and Network Management"
    AuthUserFile /usr/local/apache-2.0.43/conf/passwords
    Require valid-user
    Order Allow,Deny
    Allow from 10.211.254.0/24
    Allow from 172.18.12.0/24
    Allow from 172.3.4.0/24
    Allow from 172.3.5.129/23
    Satisfy All
    Options FollowSymLinks
    AllowOverride None
</Directory>
```

Error and access logs are sent to the default, a file in the logs directory under the server root, with a level of warn.

```
ErrorLog logs/error_log

LogLevel warn

CustomLog logs/access_log common
```

The server returns the default verbose information regarding OS-Type and modules in HTTP response headers, and includes a signature with additional information on error documents.

```
ServerTokens Full
ServerSignature On
```

The following entries in httpd.conf support publishing static html pages generated by the dbmonitor script, and graphs of round-robin database data via Cricket's cgi scripts. The cgi scripts accessed from http://IT-MGT-01/cricket/ are links to scripts in /home/cricket/cricket/.

```
<Directory "/usr/local/apache-2.0.43/htdocs/cricket">
    Options Indexes FollowSymLinks ExecCGI
    AddHandler cgi-script *.cgi
    Order allow,deny
    Allow from all
</Directory>
```

This site is not currently in use. It is a remnant of an installation of Cricket that was tabled because the systems administrators encountered difficulties compiling the various software components. (See dbmonitor, v1.0 and Cricket, v1.03).

Recommendations: Upgrade to the latest version, currently 2.0.45 (http://httpd.apache.org/download.cgi).

Create a separate, dedicated user and group with which to run Apache. Do not use the user nobody.

The default settings for directory permissions should not include "FollowSymLinks".

Disable ServerTokens and ServerSignature.

Remove the directory for the Apache manual.

Remove the links, cgi-scripts, and directives in httpd.conf created for the installation of Cricket. The dbmonitor script creates html files in the http://IT-MGT-01/cricket/ directory for status displays--the script should be changed to use a dedicated directory such as http://IT-MGT-01/dbmonitor.

Instead of using basic authentication, require that connections to this web server be tunneled over SSH sessions (which should be mandated as the only method of connecting to this system). This will make use of existing GIACE staff user accounts, remove the security risk of a shared username/password that is transmitted in clear text with each http request, and reduce exposure to Apache server vulnerabilities in general. Client addresses in httpd.conf can then be restricted to the address of IT-MGT-01 itself, because that is the source address the server will see for connections that have been port forwarded over SSH. A sample client SSH connection string would be:

```
ssh -L 8080:10.211.254.61:80 auditman@10.211.254.61
```

And a sample url would then be:

```
http://localhost:8080/cricket/somewebpage.html
```

Remote datacenter staff have indirect access to this web server through a portal server. Permit or deny the address of the portal server in the configuration sections for directories to which they are granted or denied access.

CGI Scripts

CGI, or Common Gateway Interface, scripts allow the Apache web server to provide invaluable dynamic access to information on this server. The following CGI scripts are installed on this system (see Concurrent Versions System and dbmonitor, v1.0 and Cricket, v1.03).

FreeBSD CVSweb v2.0.6[21] provides http access to the IT department document repository.

Cricket v1.0.3[22] is a set of flexible open source Perl scripts that store and query data using round-robin databases. Data is displayed in time-series graphs using Tobi Oetiker's RRDTool.[23] The systems administrators have encountered difficulties compiling the necessary components, and Cricket is not in use on this system.

CGI scripts are a security risk because they allow commands to be issued as the web server user, and there are no guarantees that the programmers who wrote the scripts had security issues in mind. On this system, the cgi scripts are permitted from specific locations, and execute as the user nobody, who has only read access at most to any files.

Recommendations: CGI scripts should not be used until access to the Apache server is restricted to connections tunneled over SSH (see Apache, v2.0.43).

To ensure that only intended data will be accessed through CGI scripts, it is critical to keep it separate and distinct from sensitive data on the system. Do not rely solely on the web server's configuration, but segregate the data in the filesystem and separate the users and processes that gather the data.

To this end, remove data gathering functions from the Cricket user. Should the Cricket installation eventually prove successful, only use Cricket's scripts and home directories to prepare and present data to be delivered by the web server (see dbmonitor, v1.0 and Cricket, v1.03 for further detail). Create a dedicated user whose sole purpose is to gather data, and allow that user to store it where Cricket can access it.

Remove any unused cgi scripts (such as test-cgi).

Concurrent Versions System (CVS), v1.11.1p1

The open source Concurrent Versions System[24] offers version control of documentation for eFortune staff.

```
[auditman@IT-MGT-01] /home/auditman $ cvs -v
Concurrent Versions System (CVS) 1.11.1p1 (client/server)
Copyright (c) 1989-2001 Brian Berliner, david d `zoo' zuhn,
                        Jeff Polk, and other authors
CVS may be copied only under the terms of the GNU General Public License,
a copy of which can be found with the CVS distribution kit.
```

The IT Department has implemented a CVS repository for storing documents about the production environment, including configuration files, policies, training materials, event logs, scripts, etc. IT staff use Windows 2000 desktops and TortoiseCVS, an extension to Windows Explorer, to access the repository. The repository is a gold standard of critical information about the entire environment - across operating systems -- and provides a useful resource for daily operations. It is also key to disaster recovery of any production server. While the individual files in the repository are mundane, the repository in its entirety is a formidable collection of documentation.

GIACE IT staff have full access to all documents in the repository as members of the local group cvs (see recommendation in User Management regarding removal of this group from NIS), and no other accounts have access. Currently, the pserver service is used to authenticate clients and checkout and update local copies on Windows 2000 workstations. There are no restrictions on client addresses. The repository is accessible for reading through a cgi script, /usr/local/apache-2.0.43/cgi-bin/cvsweb.cgi, using a single shared username and password, and basic authentication. Settings in Apache's httpd.conf restrict clients to specific subnets, which include the corporate offices and the remote access VPN server.

Recommendations: Disable the pserver service in inetd.conf by commenting out the entry in /etc/inetd.conf, then run the command

```
refresh -s inetd
```

Require the use of public-key based authentication with SSH for remote access to the repository (see Secure Shell (OpenSSH)). Limit access to the web server and cvsweb.cgi script to clients connected with SSH as described in the section on Apache, v2.0.43.

In addition, it is very important to secure the checked-out copies of CVS documentation on IT staff workstations. Notify staff of the value and sensitivity of the data, restrict access permissions on the workstation, and encrypt the disks or folders that hold the checked-out copies. A box could be surplused without being wiped, or leave you nonplused after it's swiped. These steps can all be taken without modification to the repository itself.

These measures require additional effort in client configuration, but are worth it to protect the repository data.

Network Installation Management (NIM)

Filesets bos.sysmgt.nim.client, .master and .spot, Level 5.1.0.35

This system is the master server for AIX's Network Installation Management (NIM) software, which manages installation of the operating system and software on AIX hosts. GIACE system administrators use NIM for OS upgrades, patches, and software maintenance. As a server it provides NIM resources--ordinary file system objects--to clients via Network File System (NFS) software. Installation of NIM client software configures root's .rhosts file and enables the server to use rsh to issue configuration commands and install files on the client. By default, bootpd and tftpd are enabled to support configuration of diskless workstations.

This is a worrisome stew of insecure authentication and access protocols to have active on production hosts.

However, NIM is only used during maintenance windows, at which time firewall policies are changed to isolate hosts and only permit management traffic between the server and clients. It is also IBM's supported method of deploying software.

Recommendations: Develop procedures for coordinating firewall and NIM activities during maintenance windows. Ensure that all NIM related services are turned off before resumption of production services (see NIM (/usr/sbin/nim), NFS and NIS (/etc/rc.nfs)).

Network Information Service (NIS)

Network Information Service (NIS) provides centralized management of user accounts for production Unix hosts. This system is the master server, and all other Unix hosts, located at remote datacenters, are slave servers. The ypset command lists master and slave servers that have been configured for an NIS domain. Master and slave hostnames or ip addresses are entered during configuration of NIS servers, and stored in binary files in the /var/yp/bindings/ directory. Every other host in the production environment is an NIS slave server and an NIS client of itself; there are no clients that are not also servers. The master and slave servers communicate via RPC calls, using the portmapper service. This provides continued operation of datacenter hosts in the event network connections to this system are lost. Netgroups are used to restrict user access to the host(s) in their datacenter by explicitly denying access to all others.

NIS authenticates hosts on the basis of source IP addresses, trusts usernames as submitted and relies on RPC calls that are difficult to firewall. However, GIACE's equipment at remote datacenters is isolated in dedicated racks and switches. Hosts in the NIS domain are connected to switches, and WAN connections are secured with firewall-based IPSEC tunnels. Entries in /etc/securenets on each host specify host addresses permitted to participate as clients and/or servers, and firewall rules block invalid source addresses. This renders sniffing and spoofing attacks unlikely, because client to server communications are always local to the host, and master to slave server communications are secured by encrypted tunnels.

While NIS enables consistent, standardized administration of accounts, there are drawbacks. The single namespace requires all user and netgroup accounts to be available to all clients, and thus exposes every system's account information to all other hosts in production--running ypcat exposes the password file. (ypcat has been chmod'ed to 500 and chowned to root, but there is always the possibility a user could upload a copy.) NIS accounts are not bound by AIX-specific account and password restrictions. Systems administrators will always have to manage local accounts on each host in addition to global accounts in NIS, which introduces complexity and opportunities for error.

Recommendations: NIS does not offer sufficient administrative benefits to compensate for its drawbacks,[25] and GIACE should pursue an alternate method of administering accounts such as scripted file distribution using SSH, or LDAP. The existing environment is reasonably secure from a network standpoint, but places trust in users who are not subject to GIACE's authority. (Administrators alluded to pressure from the programming and testing departments to extend NIS management to development systems, which are not rigorously managed or monitored. If NIS administration of development systems is required, this system should not participate in that NIS domain.) Removing NIS would place a modest additional administrative burden on GIACE staff, but there are only a few users at each remote data center and they do not change frequently. Scripted or manual distribution of configuration files and account updates would provide the same benefits as NIS, without the security risks and loss of native AIX functionality. (See Secure Shell).

Scripting (Perl v5.6.0 and Korn Shell)

GIACE staff use the Korn shell (/usr/bin/ksh) for shell scripting tasks, and Perl for larger, more involved programs. The database environment is mature and enjoys a number of well-worn routines that have been polished over the years, but most other activities in support of the production environment are still nascent. No formal guidelines beyond header templates and variable naming conventions are in place for script development, and deployment to the production environment (and ongoing support) is usually the responsibility of individual staff members.

Recommendations: The focus of systems administrators is traditionally on getting the job done, not worrying about security. Scripts used on this system should be subject to a code review that addresses security issues

such as privilege, access, data integrity, and error-checking. Scripts should only be released to the production environment through a change control process.

At a minimum, require that all scripts explicitly clear and reset environment variables, which will help to avoid unintended execution of files in an inherited path. For example:[26]

```
# cleanvars
        IFS='
        '                           # space, tab, newline
        export IFS
        for var in `/usr/bin/env | /usr/bin/cut -f1 -d=`
        do
                [ "$var" != "IFS" ] && unset "$var"
        done
        PATH=/bin:/usr/bin:/sbin               # update to what's needed
        SHELL=/usr/bin/ksh
        export PATH SHELL
        `/exch/bin/setvar`                      # set variables afresh
```

(Pomeranz, 29)

dbmonitor, v1.0 and Cricket, v1.03

dbmonitor is a home grown Perl script, run every 5 minutes, that gathers, stores, and formats data from the database environment to create a status display. The script uses SSH and public/private keys to connect to the dbmng account on every database-related host in the production environment. The public key entries in the target hosts' authorized_keys files contain SSH options that restrict connections to a specific source ip address and disallow tunneling and interactive shells.

This script is run from the cricket account. The collected data is stored in temporary files under /home/cricket/rawdata/, and is used to generate html status pages that are saved in /usr/local/apache2/htdocs/cricket/.

dbmonitor was developed on a Linux server underneath a systems administrator's desk, and was designed to work in concert with Cricket, which provides on-demand graphs of the collected data. dbmonitor writes out its html status pages, and then writes the data to temporary files under /home/cricket/rawdata/ where they are processed by Cricket's scripts (run from cron) and stored in Round Robin Database (rrd) files.

dbmonitor was migrated from the Linux server to IT-MGT-01 without difficulty, but problems were encountered while moving Cricket. In order to continue storing data in the rrd files and avoid gaps in history, the systems administrators decided to preserve the working Cricket installation, and simply copy the temporary files from IT-MGT-01 to the Linux box. This was accomplished by using cron to run a script on the Linux box that uses scp and a private/public key pair (with no passphrase) to copy the files.

Recommendations: Accounts used to gather data should be separate from those used to view it, and no direct logins should be permitted. In this particular case, the cricket user on IT-MGT-01 holds the keys to the kingdom, and it is very risky to allow an unknown entity (the Linux box) to login in this fashion. Reverse the direction and have IT-MGT-01's cricket user scp the files to the Linux box.

The restrictions placed on the public keys will only prevent using cricket's private key from another computer. Were IT-MGT-01 compromised, cricket's private key could be used to remove restrictions on target hosts and gain an interactive shell on every production server in the environment. dbmonitor connects to one of the utility accounts, dbmng, on the target systems, rather than a dedicated account. Without the keys, this utility account cannot be logged into directly, but must be su'd to with sudo. Thus, the current configuration of dbmonitor places the utility account dbmng at risk if cricket's account is compromised, and bypasses the audit trail provided by sudo.

dbmonitor should be run from a dedicated account on IT-MGT-01, to separate the privileges of the account

accessing collected data from those of the account used for data collection. In addition, the target account should be dedicated to data collection, and not used by any other users for any other purpose. In this case, additional restrictions could be placed on the public keys, such as specifying which commands can be run. Also, consider modifying the script to operate without cron, and to use an SSH agent with a private key that requires a passphrase upon startup.

Progress, v9.1

Progress is a relational database language and development environment, produced by Progress Software Corporation. eFortune uses Progress AppServer and WebSpeed technologies to allow web servers to broker transactions from clients to databases.

Progress is installed on the /exch filesystem, which contains 5GB of space devoted to database administration activities. The dba's perform various maintenance and repair functions on databases moved to this system, and also query and maintain remote systems using SSH connections. On occasion, they run Progress nameserver and database services that listen for network connections. These are run as root. Databases running on production hosts must remain in sync with client application code, which means the version of Progress can only be changed in coordination with programming staff and third party software vendors. This prevents the dba's from upgrading the Progress installation on IT-MGT-01 to the most recent version.

Recommendations: GIACE should upgrade to the latest possible version of Progress as soon as possible. Several vulnerabilities in Progress databases have been patched in later versions.[27][28] The firewall restrictions specified in the section Network Access from Other Hosts must be implemented to limit connections to Progress database services started by the dba's. The dba's should not use native Progress administration tools across the network unless they can do so over SSH.

Sendmail, v8.11.0

Sendmail is running as a daemon. It is used only occasionally from this system, and then only to send mail.

```
[auditman@IT-MGT-01] /home/auditman $ sendmail -d0.4 -bv root
Version AIX5.1/8.11.0
 Compiled with: LDAPMAP MAP_REGEX LOG MATCHGECOS MIME7TO8 MIME8TO7
                NAMED_BIND NDBM NETINET NETINET6 NETUNIX NEWDB NIS
                NISPLUS QUEUE SCANF SMTP USERDB XDEBUG
canonical name: IT-MGT-01.exch.giace.net
        a.k.a.: IT-MGT-01
        a.k.a.: IT-MGT-01.exch
 UUCP nodename: IT-MGT-01
        a.k.a.: [10.211.254.61]
        a.k.a.: [127.0.0.1]
        a.k.a.: [::1]

============ SYSTEM IDENTITY (after readcf) ============
      (short domain name) $w = IT-MGT-01
  (canonical domain name) $j = IT-MGT-01.exch.giace.net
         (subdomain name) $m = exch.giace.net
              (node name) $k = IT-MGT-01
========================================================

root... deliverable: mailer local, user root

[auditman@IT-MGT-01] /home/auditman $ telnet localhost 25
Trying...
Connected to loopback.
Escape character is '^]'.
220 IT-MGT-01 ESMTP Sendmail AIX5.1/8.11.0/8.11.0; Mon, \
                              31 Mar 2003 22:09:59 -0800
```

Recommendations: Do not run Sendmail as a daemon. Disable the entry for sendmail in /etc/tcpip

(see /etc/rc.tcpip). Run from the command line as needed. Consider updating to the latest version (8.12.9 at the time of writing).[29]

X11 Applications

Users are permitted to run X11 programs (clients) on this system, and export the display to an X11 server running on their workstations.

Recommendations: Implement SSH as the only method of connecting to this system, and implement the firewall restrictions specified in the section Network Access from Other Hosts. This will restrict use of X11 programs to those tunneled over SSH. For additional security, remove or restrict to root (chmod 700) the files /usr/bin/X11/xwd and /usr/bin/X11/xwud, which allow monitoring of remote X11 servers.

Cron Jobs

Files containing jobs scheduled to be run by the cron daemon are stored in /var/spool/cron/crontabs:

```
/var/spool/cron/crontabs # ls -al
total 13
drwxrwx---   2 bin      cron            512 May 23 13:24 .
drwxr-xr-x   4 bin      cron            512 Mar 20 2002  ..
-rw-------   1 root     cron           1888 Apr 01 12:54 adm
-rw-------   1 root     cron            391 May 08 14:39 dbmng
-rw-------   1 root     cron           1117 May 02 15:39 root
-rw-r--r--   1 sys      cron            441 Apr 05 2001  sys
-rw-------   1 root     cron              0 Feb 26 09:58 sysadm
-rw-r--r--   1 root     cron            703 Nov 27 12:17 uucp
```

Crontab entries follow the format:

```
minute  hour  day_of_month  month  weekday  command
```

Crontab for user adm:

```
[root@IT-MGT-01] /var/spool/cron/crontabs # grep -v "^#" adm
0 8-17 * * 1-5 /usr/lib/sa/sa1 900 4 &
0 13-23 * * 1-5 /usr/lib/sa/sa1 900 4 &
0 * * * 0,6 /usr/lib/sa/sa1 &
0 18-7 * * 1-5 /usr/lib/sa/sa1 &
5 18 * * 1-5 /usr/lib/sa/sa2 -s 8:00 -e 18:01 -i 3600 -ubcwyaqvm &
0  9 * * 1-5   /usr/sbin/perf/diag_tool/Driver_ daily
0 10 * * 1-5   /usr/sbin/perf/diag_tool/Driver_ daily2
0 21 * * 6     /usr/sbin/perf/diag_tool/Driver_ offweekly
```

These commands record system activity information, and configuration, availability, workload and performance data using the Performance Diagnostic Tool (PDT).

Crontab for user dbmng:

```
[root@IT-MGT-01] /var/spool/cron/crontabs # grep -v "^#" dbmng
0 23 * * * /home/dbmng/prd_log_rev save
10 23 * * * /home/dbmng/prd_log_rev_web save
```

This pair of scripts creates a daily compilation of errors and exceptions from database logs on production hosts at remote datacenters. The scripts use SSH and keys to issue remote commands to collect data, then store the results in files under /home/dbmng.

Recommendations: The private/public keypair used to access remote systems has no passphrase. Create a user for the specific purpose of running this cron job--this could be the same user that assumes Cricket's current data collection role. Ensure that remote systems place restrictions in their authorized_keys files as suggested in the discussion of Secure Shell (OpenSSH).

In addition, consider restricting access to the dbmng account by requiring sudo.

Crontab for user root:

```
[root@IT-MGT-01] /var/spool/cron/crontabs # grep -v "^#" root
0 3 * * * /usr/sbin/skulker
45 2 * * 0 /usr/lib/spell/compress
45 23 * * * ulimit 5000; /usr/lib/smdemon.cleanu > /dev/null
0 11 * * * /usr/bin/errclear -d S,O 30
0 12 * * * /usr/bin/errclear -d H 90
0 15 * * *  /usr/lib/ras/dumpcheck >/dev/null 2>&1
0 22 * * * /scripts/local/mgt01_bu >/dev/null 2>&1
05 10 * * * /scripts/local/mgt01_bu >/dev/null 2>&1
0,15,30,45 * * * * /exch/bin/error_check >/dev/null 2>&1
0 0 * * 0 /scripts/local/syslog_rotate >/dev/null 2>&1
0 22 2 5 5 /usr/sbin/shutdown -Fr >/work/shutdown.log 2>&1
```

Skulker is a standard script used to clean up temporary files.

The compress command compresses the spell program's history log.

The smdemon.cleanu command cleans up the sendmail command queue and maintains the /var/spool/mqueue/log file.

The errclear commands remove software and hardware error entries from the error-log.

The dumpcheck command checks that the dump device and copy directory are large enough to store a system dump.

The mgt01_bu script tars specific directories and ftp's them to another host for backups. See Backups, File Systems and Disaster Recovery.

The error_check script watches for a file produced by an ODM error report. If found, the script sends an advisory email to system administrators.

The syslog_rotate script rotates logs in /var/adm, then refreshes the syslog daemon.

Crontab for user sys has all entries commented, and for sysadm it's empty.

Crontab for user uucp has all entries commented.

Logging and Monitoring

AIX uses two facilities for logging, errdemon (/usr/lib/errdemon), a daemon that is part of the OS and started during system initialization, and syslog (/usr/sbin/syslogd).

The errdemon daemon lies in wait for device driver errors written to /dev/error, and acts upon them according to settings in the error notification database, /etc/objrepos/errnotify. By default, system errors are written to /var/adm/ras/errlog. The system administrators for IT-MGT-01 have modified the ODM error report to respond by creating a file, which is watched for and acted upon by the error_check script run from cron every 15 minutes.

The syslog daemon handles all other messages according to the following rules in /etc/syslog.conf:

```
#  is one of (from high to low):
#       emerg/panic,alert,crit,err(or),warn(ing),notice,info,debug
#       (meaning all messages of this priority or higher)

mail.debug                                                  /var/adm/maillog
mail.none                                                   /var/adm/maillog
auth.notice                                                 /var/adm/authlog
lpr.debug                                                   /var/adm/lpd-errs
kern.debug                                                  /var/adm/messages
*.emerg;*.alert;*.crit;*.warning;*.err;*.notice;*.info      /var/adm/messages
```

There are 4 files, which are rotated weekly by a cron job to give 3 weeks of history. The messages file is a catchall for messages that don't meet criteria for the other three. This includes messages from the sudo utility.

The sshd daemon writes to logs according to settings in /etc/ssh/sshd_config:

```
SyslogFacility AUTH

LogLevel INFO
```

A priority of INFO does not meet the criteria ("auth.notice") for writing to /var/adm/authlog, so logins handled by sshd are recorded in /var/adm/messages.

Recommendations: Send sshd log messages to authlog by either increasing the LogLevel setting in sshd_config to NOTICE, or decreasing the setting for authlog in syslog.conf to INFO.

Send sudo activity to authlog as well by placing the following entry in /etc/sudoers:

```
DEFAULTS syslog=auth
```

By default, sudo will send a syslog priority of "notice" for successful logins (syslog_goodpri=notice), and a priority of "alert" for failures (syslog_badpri=alert).[30]

Send log files from this server to another host on a regular schedule. Secure the data during transmission with switches and firewalls if syslog is used, or use SSH and scp to copy the files. For syslog, update /etc/syslog.conf by appending a comma, a space, and "@sysloghostname" to the existing destination entries.

Other files record login and user access activity:

/etc/utmp	a record of users currently logged into the system
var/adm/wtmp	connect accounting information
/etc/security/lastlog	attributes of last login for users
/etc/security/failedlogin	failed logins

Recommendations: Install a script to watch the failedlogin file for excessive activity. The failedlogin file is in wtmp format, which can be converted to ascii with the fwtmp command. For example, the count of failures for the current date could be tested hourly and used to trigger notification:

```
/usr/sbin/acct/fwtmp < /etc/security/failedlogin | \
grep -c "`date +'%a %b %e'`"
```

Disaster Recovery

It is critical to GIACE's operations to be able to recover from a disastrous event that affects this system. The systems administrators of IT-MGT-01 are responsible for re-creating the system and reproducing all the functions it performs, and to this end have carefully adhered to a mainstream installation and avoided extensive customization of the operating system.

Recommendations: The absence of a dedicated backup device puts a crimp in any disaster recovery plan for this system. In the event of total loss of this system, the current backup strategy of tarring and ftp'ing backups to other hosts will require the equivalent machinations to retrieve the files. It will be much faster and more reliable if the device to which backups are committed is physically attached, available as a boot device, and the files can be restored directly rather than to an intermediate host.

GIACE does not have a second system that is identical to IT-MGT-01, but this should not prevent a test recovery of this system to another machine. Such an exercise is always instructive, and lessons learned in the lab are worth their weight in gold in the unfortunate event of a real disaster. GIACE should mandate periodic test recoveries of this system be performed in the future, to ensure the systems administrators have the resources, knowledge and experience should such a recovery be required.

In addition to the practical aspects of a recovery, such as spare hardware, installation media, and configuration documentation, care should be taken to assemble contact, maintenance contract, and notification path information so that even in the case of a disaster GIACE can maintain control of its destiny.

Critical Issues and Recommendations

IT-MGT-01's security vulnerabilities result from services that are started by a default installation of AIX, the use of insecure protocols and services for user access and management, a lack of network access restrictions, and inadequate protection of sensitive data. These are critical issues that must be addressed through corporate policies, user education and participation, and configuration changes to IT-MGT-01 and other hosts with which it connects.

GIACE IT staff have a solid understanding of their systems and applications. Their planning, standardization, and thorough documentation of the production environment have brought repeated success in application rollouts under demanding schedules. With the support of GIACE's management, they will have no trouble including security considerations in their efforts. However, maintaining security requires an ongoing commitment of resources, and success will be measured by the absence of problems, rather than tangibles such as revenue or production statistics. Management must incorporate security into policies, procedures and budgets so that it is part of the infrastructure and not an ad hoc task.

Systems administrators must balance security and productivity when restricting user and network access to IT-MGT-01. This will be an ongoing challenge because of the multiplicity of services this system provides and its central location on the network. IT-MGT-01's security will be greatly improved by removing unused services and replacing insecure services with secure alternatives. Restricting network and user account access to only that which is necessary should clarify and simplify administration. Carrying out the recommendations in this report will require changes to users' workstations and daily activities, but security efforts must involve the users if they are to succeed, and their productivity will not be diminished.

The Top Ten Recommendations below will greatly reduce current security risks, and provide a basis for continued secure operation of GIACE's production environment. Following these, a summary of Other Recommendations made in this report fleshes out the vision, and the concluding Long-Term Recommendations set the course for GIACE to fulfill its destiny.

Top Ten Recommendations

1.	Backup Device	Purchase a dedicated backup device and engage an off-site storage service for this system (see Backups and Disaster Recovery).
2.	Network Access	Apply firewall policies to only allow specific addresses or address ranges to

		connect to specific ports on this system (see Network Access from Other Hosts).
3.	Network Encryption	Encrypt all traffic to and from this host. Require SSH for remote logins and scp for file transfers (see Secure Shell (OpenSSH)).
4.	Disable Unused and Insecure Services	Turn off the following in /etc/inetd.conf (see inetd): ftp, telnet, rshd, rlogind, rexecd, bootpd, tftpd, talkd, daytime, time, ttdbserver, wsmserver, dtspcd, cmsd, pserver Turn off the following in /etc/rc.tcpip (see /etc/rc.tcpip): snmpd dpid2 hostmibd Turn off the following in /etc/inittab (see /etc/inittab and Other Processes): writesrv rc.dt piobe qdaemon itess
4.	Private key security	Provide separate, dedicated accounts and data storage areas for use by monitoring processes that use public-key based authentication (see dbmonitor, v1.0 and Cricket, v1.03 and Secure Shell (OpenSSH)).
5.	CVS Repository	Use SSH and public-key based authentication to access the repository, and secure checked out copies on client machines (see Concurrent Versions System (CVS), v1.11.1p1).
7.	Apache server	Tunnel access to the Apache web server over SSH, remove unused sites, and restrict client addresses on a per-site basis (see Apache, v2.0.43).
8.	Network Information Services	GIACE should actively pursue a replacement for NIS, such as scripted file distribution and synchronization over SSH, or LDAP (see Network Information Service (NIS)).
9.	Sendmail	Disable Sendmail as a daemon, only allow outgoing mail, and change the primary MX record in DNS for the destination corporate mail server to an internal address (see Sendmail, v8.11.0).
10.	Network Installation Management	Disable NIM when it is not in use, and only use it in concert with firewall policies that deny all other access to the target hosts (see NIM (/usr/sbin/nim), NFS and NIS (/etc/rc.nfs) and Network Installation Management (NIM)).

Other Recommendations

Bring OS to Maintenance Level 4 (see Version).

Upgrade to AIX 5.2 (see Software OS and Version).

Include Data Center staff responsibilities in ASP agreements (see Personnel Policy and Datacenter Operators).

Increase physical security of IT-MGT-01 (see Physical Environment).

Disable unused accounts (see Local Standard System Accounts).

Remove developer accounts (see GIACE IT Staff.

Remove CVS accounts from NIS (see NIS Accounts).

Update default password settings for new accounts, and formalize password distribution and storage (see Passwords).

Create a login banner (see Login Banner).

Remove unsafe entries in users (and especially root's) path (see Path and Environment).

Use the Trusted Computing Base to monitor files. (see Trusted Computing Base).

Mount filesystems with the options nosuid and nodev (see File Systems).

Clean up ownership of files (see File Ownership).

Remove unused suid and sgid files (see SetUID and SetGID Files).

Restrict access to the lsof utility (see Listening Processes).

Update TCP/IP network options (see Network Options).

Change MX records to keep smtp mail internal (see SMTP).

Disable receipt of syslog messages (see syslogd).

Until NIS is replaced, direct logs of user activity throughout the environment to a separate system, and review them daily (see Logging and Monitoring).

Add variable-cleansing code to scripts (see Scripting (Perl v5.6.0 and Korn Shell)).

Upgrade Progress (see Progress, v9.1).

Test recovery procedures (see Disaster Recovery).

Long Term Recommendations

1. Change control. The variety of activities that take place on this system cry out for a formal process to ensure coordination of changes in the production environment. A good change control process has: "an identified owner, a path for customer input, an audit trail to account for all changes, a clear announcement and review period, testing procedures, and a well understood rollback plan."[31] (Patch Management and Change Management, Chapter 8)

2. Resources for Development and Testing. Provide IT staff with hardware resources for developing and testing scripts and software, to assure the success of software rollouts and changes to the production environment and avoid introduction of unintended security vulnerabilities. IT-MGT-01 is in fact a production server, and should be included in the production change-control regimen.

3. Security Awareness. Articulate security policies for all of GIACE's production systems, and require users to understand and participate in their enforcement. Include security considerations as part and parcel of all third party agreements. Plan for security in the budget process. Do not bypass security in order to achieve short-term goals.

References

1 Mookhey, K. K., The Unix Auditor's Practical Handbook. Network Intelligence India Pvt. Ltd. May 2003. <http://www.nii.co.in/tuaph1.html>.

2 "Description: pSeries 630 Models 6C4 and 6E4." Unix Servers, Entry. IBM. May 2003. <http://www-1.ibm.com/servers/eserver/pseries/hardware/entry/p630_desc.html>.

3a, 3b "hintsTips0214: 64-bit Mode on AIX Version 4.33 to 5.x." IBM Server Group. 7 April 2003. <http://www-1.ibm.com/support/docview.wss?uid=isg1hintsTips0214>.

4 Barman, Scott. Writing Information Security Policies. Indianapolis: New Riders, 2002. 4.

5 "General FAQ." IBM pSeries Information Center. IBM. 1 April 2002. <http://publib16.boulder.ibm.com/pseries/en_US/infocenter/base/faq.htm#general>.

6 "Fix Delivery Center for AIX Version 5." IBM eServer pSeries Support. IBM. 2003. <https://techsupport.services.ibm.com/server/aix.fdc>.

7 "Subcription service: Overview." IBM eServer pSeries Support. IBM. 2003. <https://techsupport.services.ibm.com/server/pseries.subscriptionSvcs>.

8 "Security Guide - Login Control." AIX 5L Version 5.2 Security Guide. IBM. 2003. <http://publib16.boulder.ibm.com/pseries/en_US/aixbman/security/login_control.htm>.

9 John the Ripper. Openwall Project. Accessed June 2003. <http://www.openwall.com/john/>.

10 Hughes, Kim. Security Issues Your Company Faces When Storing Data at an ASP. SANS Institute. 2002. <http://www.giac.org/practical/gsec/Kim_Hughes_GSEC.pdf>.

11 "Updated: OpenSSH for AIXL 5L Version 1 (5.1) Available." IBM developerWorks: Open source projects. Online posting RE: tcp wrappers. IBM. 4 November 2002. <http://oss.software.ibm.com/developerworks/forum/forum.php?forum_id=531>.

12 "IP Security Installation." AIX 5L Version 5.1 System Management Guide: Communications and Networks. Fifth Edition. April 2001. <http://publibn.boulder.ibm.com/doc_link/en_US/a_doc_lib/aixbman/commadmn/ipsec_install.htm#HDRA3F4CF3B420ENDR>.

13 SANS/FBI Top 20 List. SANS Institute. Version 3.23. 29 May 2003. <http://www.sans.org/top20>.

14 Taylor, Simon. "Securing IBM's AIX: Practical unix security." ROOTVG.NET: Section 1.1 AIX vs. Other unix variants. January 2002. <http://rootvg.net/count.php?url=column_Securing_AIX.htm>.

15 Han, Michael. Security Considerations of Secure Shell (SSH). Version 1.6. 2002. <http://www.mikehan.com/ssh/security.html>.

16 Barrett, Daniel J., and Richard E. Silverman. SSH, the Secure Shell: The Definitive Guide. Sebastopol: O'Reilly, 2001.

17 "rc.powerfail Command." AIX 5L Version 5.1 Commands Reference, Volume 4. IBM. 1999. <http://publibn.boulder.ibm.com/doc_link/en_US/a_doc_lib/cmds/ \ aixcmds4/rc.powerfail.htm>.

18 "srcmstr Daemon." AIX 5L Version 5.1 Commands Reference, Volume 5. IBM. 1999. <http://publibn.boulder.ibm.com/doc_link/en_US/a_doc_lib/cmds/aixcmds5/srcmstr.htm>.

19 "Installation Guide - Documentation Library Service and Online Documentation." AIX 5L Version 5.1 Installation Guide. IBM. 2001. <http://publibn.boulder.ibm.com/doc_link/en_US/a_doc_lib/aixins/ \ aixinsgd/inst_doc_PI.htm#HDRA97NEWLMS45>.

20 Apache HTTP Server Project. 2002. <http://httpd.apache.org/>.

21 FreeBSD CVSweb Project. FreeBSD.org. 2003. <http://www.freebsd.org/projects/cvsweb.html>.

22 Cricket. GNU General Public License, hosted by SourceForge. 21 April 2003. <http://cricket.sourceforge.net/>.

23 Oetiker, Tobi. RRDTool. GNU General Public License. 27 February 2003. <http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/>.

24 Price, Derek, CollabNet, and others. GNU Concurrent Versions System. GNU General Public License. 2002. <http://www.cvshome.org>.

25 Nemeth, Evi, Garth Snyder, Scott Seebass, and Trent R. Hein. Unix System Administration Handbook. Upper Saddle River: Prentice Hall, 1995. 549.

26 Pomeranz, Hal. "The Untrustworthy File System." Unix Vulnerabilities - Unix Security Track - SANS GIAC Training Materials. Oakland: Deer Run Associates. 2001.

27 Security Advisories. Progress Software Corporation. 2003. <http://www.progress.com/support/downloads/security.htm>.

28 Vulnerabilities. Security Focus. 2003. <http://www.securityfocus.com/cgi-bin/sfonline/vulns.pl>. Search for vendor=Progress.

29 Sendmail, v8.12.9. Sendmail.org. 29 March 2003. <http://www.sendmail.org/8.12.9.html>.

30 Miller, Todd C., and Chris Jepeway. "Examples." Sudoers Manual. 2003. <http://www.courtesan.com/sudo/man/sudoers.html#examples>.

31 "Patch Management and Change Management, Chapter 8 - Patch Management, Microsoft Solution for Securing Windows 2000 Server." Microsoft Technet. 2003. <http://www.microsoft.com/technet/treeview/default.asp? \

url=/technet/security/prodtech/Windows/SecWin2k/08patman.asp>.