

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Security Audit Report
for
GIAC Enterprises

Completed in partial fulfillment of
GIAC Securing Unix Certification (GCUX)

Prepared by
Carolyn L. Tarloff
19 February 2001

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

TABLE OF CONTENTS

Executive Summary 3
Audit Procedures 3
Potential Vulnerabilities 3
Recommended Actions 3
Phase I: Short Term 4
Phase II: Mid Term 5
Phase III: Long Term 6

Audit Details 1
Physical Security 1
Network Security 2
ISS Vulnerabilities 4
Backups and Disaster Recovery 5
Administrative Procedures and Practices 6
Use of root privileges 8
Securing root 9
Account Maintenance 12
Password Maintenance 13
Security Warning Banners 15
System Configuration Management 17
System Services 21
Network Services 21
Network Access Control 23
cron Security 25
Upgrades and Updates 26
System Logging 27
Process Auditing 27
Central Log Host 28
Login Attempts 28
Failed Logins 28
ftp 29
su 29
cron 29
mail 29
Connection Logging 29
Process Accounting 29
Recommended Log File Permissions and Ownerships 30

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix A: Security & Controls Audit Guidelines 1
Scope 1
Objectives 1
Constraints / Dependencies 1
Determining the Information 1
Technical Audit Material 2
Customer Policy / Procedures Needed for Audit 3
Cyber Insurance Checklist 4
Approach 4
REPORTING 5
Appendix B: Printer Vulnerabilities 1
Overview 1
How to correct a printer vulnerability 1
How a printer is connected to the network 1
How a printer is accessed 2
Printer Vulnerabilities 2
FTP CWD ~root login 3
FTP daemon with no password 3
SNMP_Set used Public Community Name to Change System Information 3
Telnet Available with No Login 4
ColdFusion web administration feature can be used by anyone to stop the CFserv~ 4
Echo service 4
FTP bounce attack could allow attackers to 'proxy' connections 4
FTP directories writeable 5
TCP sequence prediction 5
Anonymous FTP enabled 5
FTP Home Directory Bug 6
SNMP Agents Reveal Information About Network Interfaces 6
SNMP can reveal possibly sensitive information about hosts 6
SNMP_Get able to retrieve any Community Name 6
SNMP_Get able to retrieve Public Community Name 6
Example 7
Appendix C: World Writeable Files Exceptions 1
Appendix D: Additional Audit File Recommendations 1
Appendix E: Scripts used within the Audit 1
Appendix F: Internet Scanner Vulnerabilities 1
References 1

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Executive Summary

A security audit was performed for GIAC Enterprises from December 10, 2000 through January 10, 2001. The objectives of this security audit were to review:

- All (formal and non-formal) Security Procedures and Policies to ensure those procedures and all employees, contractors, and visitors are adhering to specified policies.
- The physical security of the site (internally and externally).
- The network security.
- The security within individual servers.

Given, GIAC Enterprises is a new start-up company, their intentions from the start were to tightly secure the network in the beginning, and then as their learnings increase restrictions may be loosened.

Audit Procedures

Audit procedures as documented in Appendix A, consisted of initial meetings to define the Scope and Objectives of the Audit, using Network Scanning Tools to scan specific servers and random servers and accessing server contents to verify configurations.

Potential Vulnerabilities

The potential vulnerabilities lay in the areas of:

- file system modes (ownership, group and permissions)
- Cyclic Redundancy Checking -- not knowing what has changed on a file system at any given time
- network configuration (IP Forwarding, /etc/ftpusers, etc.)
- manpower to implement Proactive Security -- (system and network) log analysis, Cyclic Redundancy Checks, Disaster Recovery Procedures, etc.)

Recommended Actions

As a result of this audit, the recommendations have been categorized into 3 Phases:

- Phase I: Short Term (within six months)
- Phase II: Medium Term (within one year)
- Phase III: Long Term (to be evaluated by GIAC Enterprises to determine when it is appropriate to consider implementation.)

Assuming, GIAC Enterprises will follow the company procedures of testing everything out in the lab prior to a production installation, the Short Term recommendations correspond to installing and testing designated quick fixes (i.e., the low hanging fruit) before using the Jumpstart Methodology them out to production. In addition to getting the quick fixes out to production in Phase I, the preliminary work needed for task items in Phase II is done in Phase I.

The outline below summarizes the changes and estimated work effort within each phase.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

PHASE I: SHORT TERM

1. Review the Printer vulnerabilities listed in Appendix B, and the Hardware Inventory to group the vulnerabilities by Printer Model. Devise a plan to get the critical vulnerabilities fixed before end of 4th Quarter 2001. The review of these vulnerabilities should take approximately 1 week depending on the size of and variation in the printer inventory. Obviously, if all the printers are exactly the same, it will not take weeks worth of effort. (Phase II effort will implement the fixes.)
2. Implement the changes necessary to close the detected ISS Vulnerabilities. (This work effort is minimal, approximately 2 to 3 days to implement and test.)
3. Begin plans to acquire additional resources to alleviate the workload on the experienced network administrators. Expectations should be set, so the additional resources are on-board and familiar with the environment within 8 months.
4. The experienced administrators mentioned in #2 above should determine the tools available to GIAC Enterprises for Network Log Analysis and begin steps for acquisition. Document the Network Logs Review Process to be implemented in Phase II. These task items are about a 1-month work effort, using no less than 3 people. (Phase II effort will implement the procedures and acquire the tools.)
5. Review the system logs that resulted from the audit period. Look at the footprints left by the scans done during the Audit. Begin reviewing other log analysis tools and see if GIAC Enterprises could benefit by incorporating one of these tools into the current environment or could one of these tools completely replace what GIAC Enterprises has today. This learning and review effort should take approximately eight weeks, which includes downloading and installing the evaluation tools. (Phase II effort will acquire the tools and implement any changes needed.) This is approximately a 3-week work effort using 2 experienced System Administrators.
6. Using the information acquired in #4 above, determine the System Log Analysis Tools available to GIAC Enterprises and begin steps for acquisition.
7. Update or create the configuration files specified in the Audit Detail section to secure the network or information about the network. (/etc/pam.conf, /etc/ftpusers, /etc/default/login, /etc/issue, etc.) Test the network configuration with existing applications to ensure everything still works. Given the audit details the updates should take no longer than 2 days, however testing the applications is dependent upon the number of applications needed to be tested and the experience the Admin has with those applications.
   As an example, here are some of changes:
   - Create the /etc/ftpusers file containing root and all disabled system accounts.
   - Remove OS Information from the /etc/issue file.
   - Enable cron logging
8. Incorporate the Audit Configuration file, outlining the permissions needed on System Files specified by Casper Dik, into the current scan and correct procedures.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Given the audit details this work effort should take no longer than 2 days. This will immediately address some of the setuid / setgid problems.

9. Correct the inetd.conf file in /etc/inet. Set up a link to /etc/inet/inetd.conf in /etc. This specific work effort is minimal, however there is always the on-going pruning effort, which should happen periodically.
10. Correct the services file in /etc/inet. Set up a link to /etc/inet/services in /etc. This specific work effort is minimal, one day at most, however remember there is always the on-going work effort associated with these files.
11. Determine the Cyclic Redundancy Tools available to GIAC Enterprises and begin steps for acquisition.
12. In all JumpStart environments, disable the startup scripts used to re-initialize or re-install the system, including S30sysid.net, S71sysid.sys and S72autoinstall.
13. Fully implement the GIAC Enterprises Network Policy on modifications to /etc/rc2.d/S69inet for variables such as:

```
ip_forwarding
ip_forward_src_routed
ip_forward_directed_broadcasts
ip_respond_to_echo_broadcast
```

14. Once all the changes in steps 1-13 have been made and tested in the lab push the changes out to production using the Jumpstart Methodology. Estimate a 2-day work effort to setup the Jumpstart scripts, and then it happens overnight.

PHASE II: MID TERM

1. Complete the Disaster Recovery Procedures.
2. Review each setuid / setgid programs not addressed in Phase I and determine the actions needed for each. Actions needed may include:
   - Removing setuid / setgid
   - Disabling the application – chmod 000 or remove the application from the system
   - Getting a vendor patch
   - Replacing the setuid / setgid application with a more secure application
3. Pick a representative host and review all un-owned, world-writeable, un-grouped, etc. files on each file system. Correct the file modes or document the exceptions and any associated risks before meeting with management to review the status and obtain approval on the exceptions. (Unless there will be multiple teams working, this work effort should be done on a group of files at a time. E.g., do all the files in /var before addressing the files in /opt. Estimate 2 to 3 days for each high level directory and start with the most critical system directories first.) The JumpStart Procedures will implement the changes on all Solaris 2.6 Systems unless noted.
4. Implement Phase I fixes for printers. (Work effort is outlined in the Phase I Documentation.)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5. Implement the Network Logs Review Process defined in Phase I. (Work effort is outlined in the Phase I Documentation.)
6. Install the Cyclic Redundancy Tool and test the installation before pushing it out to all systems.

PHASE III: LONG TERM

1. Replace /dev/null in the /etc/passwd file with the noshell program so that **all** failed login attempts are logged to syslogd
2. Invest in a product, like SecureID, to provide access to your systems using two-factor authentication rather than the single factor authentication. This would not eliminate products that are currently in house because PowerBroker™ and PowerPassword™ can be integrated with two-factor authentication mechanisms.
3. Continue the policy of Audit Reviews to ensure the company Security Policy is being implemented and is current.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Audit Details

Physical Security

The GIAC Enterprises Policies were reviewed for Physical Security and their Standard stated:

> There are to be physical security measures and operational processes to protect information, software, hardware and personnel from either accidental or intentional harm.
> The use of information, software, and hardware is to be based on authorization from the owner. The owner specifies who can have access, under what circumstances, and the type of access.
> The system of protection, authorization, and verification is to be tailored to the risks. Unless precluded by safety considerations, individual accountability for the use of such resources is to be ensured, and there is to be verification that these resources are used only by authorized individuals.

The GIAC Enterprises site consists of two high rise buildings. The company stays current with City / State Building, Electrical and Fire Codes / Regulations. Thus Building Safety was not an issue. One building, designated as the Main Building, has a Guarded Visitor's Entrance, where outside contacts would be met by an employee and signed in. Both buildings have multiple employee entrances (i.e., from the parking garage, from the street, etc.) which require card-key access. All entrances and various designated internal areas are on video displays viewed by Security Guards, and taped 24 / 7.

Personal computers and workstations are located in personnel offices where a card-key was required to obtain access to the building and a physical key required to get into the office. Employees are given strict guidelines regarding password security, and screens were automatically locked after 8-15 minutes of non-use. Employees are reminded about the Social Engineering Security Issues at a Mandatory Annual Security & Controls Meeting. This did not stop at least one employee from holding the door open for the Auditor when he stated he forgot his badge and was late for a meeting with Joe Jorgeson (the manager of the Internal Networks Department in GIAC Enterprises). Thus the Auditor was able to gain physical access to the second building via an employee entrance during normal working hours. Access was not attempted to the Main Building.

All network drops are located in personnel offices, or in "work rooms" which require addition card-key access. There were no network drops located in conference rooms or lobbies.

All the servers are located in the temperature-controlled Server Room in the Main Building, which requires card-key access, or a Security Guard to verify employment or "Access Permission" before allowing access via a temporary badge. To gain access to the server room requires both card-key access and a unique code to be entered on a keypad. The temporary badges/card-keys do not work on the Server Room so the Auditor had to be

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

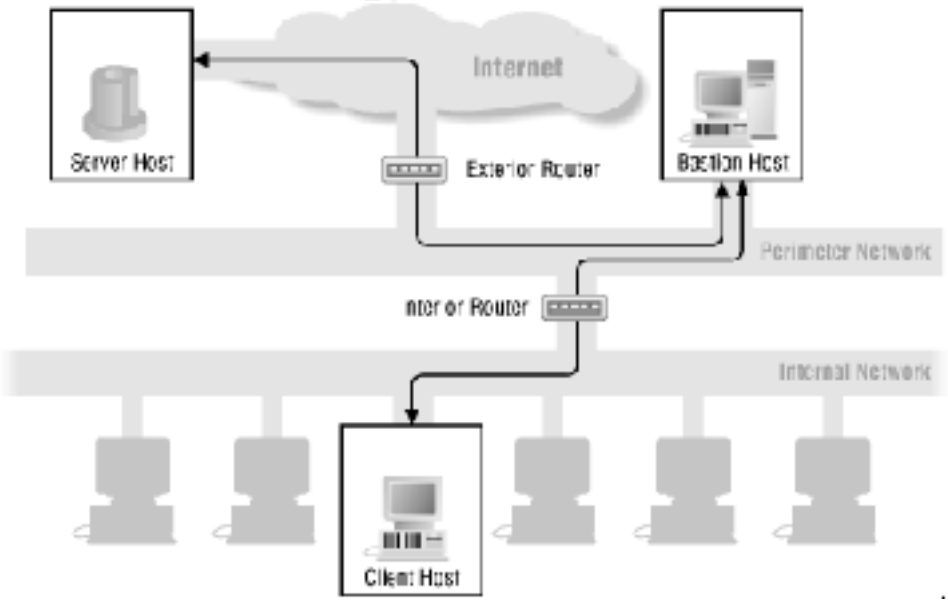
escorted in the Server Room at all times. The entry doors were metal with internal hinges and break-in resistant locks. Perimeter walls of the Server Room are true floor-to-ceiling walls constructed with a one-hour fire rating, and watertight seals at the ceiling and floor. All non-sprinkler water systems are routed around the Server Room. The Server Room was not labeled externally and there were no viewable areas into the Server Room from the External Perimeter. The card-key access to this room is strictly monitored and maintained. Access is taken off the badge with transfers, terminations, or leave of absence. The Auditor could not obtain access to the Server Room via Social Engineering or any other means other than escort.

Care was taken regarding the cabling of anything in or near the Server Room. Power and signal cables are always routed in separate conduits. Only electrical and signal cable with fire-resistant insulation that do not produce toxic products in extreme heat are used. Secondary air supplies are made available to aid personnel in escaping a fire. Very Early Smoke Detectors / Alarms are used in the sub-floor and other hidden spaces. Water detectors are also used in the sub-floor. The fire suppression system shuts off the power to the A/C and other ventilation equipment before activating the CO2 cabinets.

Other than the aspect of Social Engineering, the Auditor has no recommendations on Physical Security.

Network Security

The diagram, below is a generic model of GIAC Enterprises network.



GIAC Enterprises has set up their network to use two packet-filtering routers:

- The Exterior Router between the Bastion Host and the Internet advertises only the existence of the screened subnet (the Bastion Host subnet) and

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- The Interior Router between the Bastion Host and the Internal Network advertises only the existence of the screened subnet to the internal network.

This configuration creates an isolated subnet (the Bastion Host subnet)

- Which screens and blocks **all** data traffic going across. Given the Internet and the Internal Network have access to hosts on the Bastion Host all data traffic coming and going to either network is screened and blocked.
- Which prevents the systems on the Internal Network from constructing direct routes to the Internet.
- Should dial-in capability be required, modems and additional Information Servers would be added on this isolated subnet. By adding the modem capability onto this subnet we thus screen all data going to and from the modems. This would protect against attacks such as "war-dialing" or simply a cracker trying to get into the Internal Network.

Although GIAC Enterprises has set up the network securely, little or no monitoring of the network logs are being done. The Auditor did not observe any review of the logs done while on-site. Audit Interviews with employees disclosed that the logs are only reviewed if a problem is detected or suggested. Audit strongly recommends GIAC Enterprises practice proactive security by reviewing the network data regularly to find areas to strengthen the firewall and router rule-sets.

GIAC Enterprises could use a vendor product or freeware to monitor the logs and alert as needed. For example, the "alert.sh" script has been developed for Unix and can be downloaded from http://www.enteract.com/~lspitz/alert_1.4.4.tar.gz The goal of this script is to receive an email alert whenever someone is attempting to scan or probe your network. The information is then archived in a database for future use.

The Auditor scanned the Internal Network for Vulnerabilities using Internet Security Systems' Internet Scanner product. The main item discovered was the vulnerabilities documented in Appendix B showed up on all of the printers. This was due mainly in part to the process followed when installing a printer on the network – unpack the box, obtain an IP Address, and do whatever is needed to get it to function as a network printer. Appendix B: Printer Vulnerabilities lists the vulnerabilities found and some suggestions for addressing the vulnerability. The Auditor recommends GIAC Enterprises scan all their printers based on Manufacturer, and collect the data to address the Vulnerabilities with your Customer Support Personnel.

In addition to the printer vulnerabilities found on the network, the Auditor has listed those vulnerabilities, which are classified as High or Medium by ISS, and were detected on the Solaris Server.
High Vulnerabilities will:

- allow immediate access to a machine
- allow su privileges

For example: sendmail vulnerability that allows execution of commands on mail server.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Medium vulnerabilities will:

- have a high potential of giving access to an intruder
- degrade system performance

For example, ftp, nis guessable passwds

Low Vulnerabilities will:

- Provide information that may lead to compromise.

For example, finger, rstat, rusers

ISS Vulnerabilities

Audit detected these vulnerabilities on the GIAC Enterprises Network using the Internet Security Tool.

High

- **Solaris chkperm could allow local users to read files** -- Solaris /usr/vmsys/bin/chkperm could be used to read files owned by bin via the VMSYS environmental variable.
  Remedy:
  As a workaround**, remove the setuid** bits on the **/usr/vmsys/bin/chkperm** binary.
- **Solaris chkperm buffer overflow** -- Solaris versions 2.x chkperm executable contains a buffer overflow. An attacker could send executable code to the -n option to the chkperm executable and execute arbitrary commands as root.
  Remedy:
  As a workaround, remove the setuid bits on the /usr/vmsys/bin/chkperm binary.
- **Solaris lpset command contains a locally exploitable buffer overflow** -- A buffer overflow in the Solaris 2.x (both x86 and Sparc) lpset program could allow a local attacker to execute arbitrary code with root privileges.
  Remedy:
  Remove the suid bit from the '/usr/bin/lpset' command until Sun releases a patch for the vulnerability.
- **rdist buffer overflow allows execution of arbitrary code** -- a buffer overflow problem has been found in set-uid 'root' versions of rdist. It is possible to make rdist execute user created code as 'root', which results in the execution of arbitrary commands such as /usr/bin/csh.
  Remedy:
  Remove setuid bit from program, if you need to run rdist as root, obtain a patch from vendor.
- **TCP Sequence Prediction -** The TCP sequence was found to be predictable. When the TCP Sequence is predictable, an intruder can send packets that are forged to appear to come from trusted machines. These forged packets can compromise such services such as Rsh and Rlogin, because their authentication is based on IP addresses. The

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

percentages guessed is the likelihood that an intruder could predict the sequence and compromise the system.

Remedy:

- set the secure NFS flag in /etc/system (set nfssrv:nfs_portmon=1)
- move the daemon to a reserved port

Medium

- **NFS mount daemon operating on an unreserved port** -- the mountd daemon is running over a non-reserved port. This daemon may be vulnerable to port hijacking.

  Remedy:

  - set the secure NFS flag in /etc/system (set nfssrv:nfs_portmon=1)
  - move the daemon to a reserved port

SNMP public community name – an attacker can use a public community name to access system and change system information.

Remedy:

- Use private community name or disable SNMP
- In Solaris 2.6,

```
/etc/init.d/init.snmpdx stop
mv /etc/rc3.d/S76snmpdx /etc/rc3.d/DISABLED_S76snmpdx
```

The Auditor recommends addressing the above vulnerabilities by implementing the fixes. If GIAC Enterprises chooses not to implement the fix, appropriate risk analysis should be done, documented and approved by the appropriate level of management. If additional information is needed on any of the vulnerabilities, go to the Internet Security Systems website at http://www.iss.net, and review their Security Library. See Appendix F for a sample of other vulnerabilities that were discovered in the Library.

Backups and Disaster Recovery

GIAC Enterprises has classified all of the data stored on-line. Some data does not get backed because it does not legally belong to GIAC Enterprises and backing it up breaches contract agreements. For example, if they're evaluating a product and they have been given all of the software and associated licenses to run the product. Should they choose not to purchase that product, it would have to be removed from all media, including any backup media.

All data (e.g., the fortunes for the fortune cookies) determined to be worthy of backup is then categorized based on it's worth to the company to assist in the Disaster Recovery information. Generally, unless specified, a full backup of all data is done once a week, and incrementals are done daily. The data has been arranged across the disks so that the Data Retention requirements are easily addressable. Full Backups are sent off-site monthly and kept for the amount of time specified in the Data Retention Documents for that data. If the data is not specified, then it will fall into a general category and those retention guidelines will be followed. System Logs may be an example of data that falls under the general category of "System OS Data" kept for the period of time the OS is used in the company plus 2 years.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The Backup Team is separate from the System Administration Team because it was found the System Administration Team could not keep up with the workload of system administration and backups and restores. The Backup Team tests data restores randomly (i.e., one domain, or subnet) every 2 months to ensure a complete restore can be done. Each Restore Test is logged and the results are reported to Management. Problems with restores are addressed immediately, and stored data is assessed to determine how much data requires recovery.

Given the recent startup of GIAC Enterprises, fail-over servers have yet to be introduced. Work has begun on the Disaster Recovery Procedures, but has not finished to date. Since all data is categorized, the Auditor's recommends that GIAC Enterprises use the Disaster Recovery Requirements Analysis By Stan Stringfellow, obtained at http://www.sun.com/blueprints/0700/drra.pdf to begin to define their Disaster Recovery Plan. This paper discusses how to implement a disaster recovery program through an analysis of the disaster recovery requirements. It also provides a "Disaster Recovery Requirements Analysis Form" that can serve as the basis for the negotiation process that helps all parties to arrive at realistic expectations and well-understood disaster recovery service level agreements.

Administrative Procedures and Practices

The System Administrative Procedures and Practices have been clearly documented and distributed to all System Administrators. Given the System Administrators have access to root, all System Administrators are GIAC Enterprises Employees. No temporary employee or contractor will ever be given root access. All new System Administrators are trained on the systems and GIAC Enterprises Procedures for administering the networks. Each System Administrator is assigned to a team of administrators responsible for a defined set of systems. Each new System Administrator is assigned a mentor to keep things consistent beyond the training.

In the System Administration Training, the Admin learns about the System Administrator's Daily, Weekly, Monthly and Yearly Tasks. Some examples documented in the GIAC Enterprises System Administration Procedures:

Daily

- Update the hardware inventory if necessary
- On each system assigned, check root mail for error messages from cron and other sources.
- Review Work Queue of User/ Management Requests
- Review systems logs and other security related information that has been collected for you by GIAC's Security Infrastructure Tools. Based on the information, investigate, fix or document reasons not to address.
- Perform routine maintenance on user accounts.
  - Add new accounts and monitor permissions, groups, and ownership.
  - Disable old accounts and manage account policies.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Monitor event logs and services.
  - Don't forget routers and firewalls.
- Perform routine disk maintenance on servers. Make sure you have sufficient free space on all servers. Check and maintain disks, as long as you can do so without having to reboot.

Weekly

- Manage inactive accounts – delete inactive accounts, move associated data to a pre-determined location, notify Backup Team of account changes for record changes of backup data.
- Check for essential system updates and patches. (Use "showrev –p" option to display all the patches installed on your system.)
- Check performance on the network and on key servers.
- Use a Performance Monitor tool to log CPU, Memory, Network Utilization, and HDD Access at 10- to 15-minute intervals during business hours throughout the week. A quick review of these logs can help you quickly spot when something's not right.
- Purge temporary files on servers.
- Eliminate all core files in system directories and /tmp directories. If a core file is required, move it to a secure area or off-line until you are ready to use it.
- Perform routine disk maintenance on client systems.
- Check hard disks to identify problems before they become crises.
- Implement new policies, permissions, logon scripts, or scheduled script modifications.
- Audit the network for unauthorized changes, inside and outside.

Monthly

- Change admin/root passwords.
- Check for software updates.
- Review BIOS revisions.
- Check hardware performance. Check the hubs, switches, and routers for collisions or other network anomalies.
- Audit security settings.
- Pay special attention to service account and admin passwords.
- Gather and review statistics. This is a good opportunity to evaluate performance and procedures and identify any areas for upgrades and changes.

Annually

- Review all inventory information
- Review authorization of all accounts. Cleanup as necessary.

The Auditor noted the lack of task automation in the above training. The System Administrators were being taught what to do and what not to do but they were not given a decent toolset to perform their jobs efficiently and effectively. The Auditor recommends acquiring some Admin tools to automate as much as their jobs as possible. For example:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Monitoring patches can be automated by using **GASP!** [1] GASP! is software for Solaris/SunOS that automates the management of Recommended and Security patches from SunSolve. (I.e., automates Sun's Patchdiag tool. Generates a list of necessary patches and then prompts the user to download them.
- Monitoring the firewall logs could be assisted with a script such as alert.sh, which can be downloaded from http://www.enteract.com/~lspitz/alert_1.4.4.tar.gz The goal of this script is to receive an email alert whenever someone is attempting to scan or probe your network. The information is then archived in a database for future use.
- Although GIAC Enterprises has automated the monitoring of syslog, it is the Auditor's opinion that the monitoring could be improved by reviewing some of what others are doing and sharing what GIAC Enterprises is currently doing.

Use of root privileges

In addition to the work tasks, the System Administrator is trained on the usage of PowerBroker™. PowerBroker™ is a Vendor Solution to the management of root access. PowerBroker™ is a suite of programs that provides functionality to allow the full administrative powers of the root account to be selectively shared among many users without having to share the root password. It also provides a full audit trail of all actions occurring in important accounts such as root. PowerBroker™ sessions are automatically terminated if nothing has been typed for more than a specified amount of time thus reducing the problem of unauthorized use of a privileged user's terminal. PowerBroker™ was setup by GIAC Enterprises to encrypt all user input and control messages sent over the network, so that anyone using a network monitoring program will see encrypted data rather than clear text passwords and data.

When the tool was installed it was understood, there's always going to a situation where PowerBroker™ does not provide the access level needed, or it's simply not available (e.g., Networking Problems). In these limited situations, the System Administrator is given "the root" password after signing and reviewing the documented procedures on the use of root. The procedures clearly state that once the job is completed, the root password is to be entered back into the "GIAC Privileged Accounts System" where the root password will be changed, and available for sign-out again.

All root access (PowerBroker™ or su root) and all individual su's are logged and a System Administrator as well as a designated internal "Audit Person" is notified via mail of all su activity. For example, the following was extracted from one of those notifications:

```
Jan 11 07:09:38 server021 su: 'su root' succeeded for theodore on /dev/pts/2
Jan 11 07:10:09 server021 su: pam_authenticate: error Authentication failed
Jan 11 07:10:09 server021 su: 'su root' failed for theodore on /dev/pts/2
Jan 11 07:10:21 server021 su: 'su root' succeeded for theodore on /dev/pts/2
Jan 11 07:21:25 server021 su: 'su root' succeeded for theodore on /dev/pts/2
Jan 11 07:26:39 server021 su: 'su root' succeeded for theodore on /dev/pts/2
Jan 11 07:41:10 server021 su: 'su root' succeeded for theodore on /dev/pts/2
```

[1] http://www.georgetown.edu/reillyb/gasp/

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
Jan 11 07:48:00 server021 su: 'su root' succeeded for theodore on /dev/pts/2
Jan 11 10:11:54 server021 su: 'su root' succeeded for simon on /dev/pts/3
Jan 11 10:17:32 server021 su: 'su root' succeeded for simon on /dev/pts/4
Jan 11 10:20:30 server021 su: 'su root' succeeded for simon on /dev/pts/3
Jan 11 10:30:16 server021 su: 'su simon' succeeded for simon on /dev/pts/4
Jan 11 10:30:33 server021 su: 'su root' succeeded for simon on /dev/pts/4
Jan 12 08:24:51 server021 su: 'su root' succeeded for simon on /dev/pts/3
```

Given the procedures outlined above, the Auditor questioned both the designated Audit Person and the system administrator, theodore, why there were so many 'su root' in the logs, and if they had been authorized. Also, why did both theodore and simon had access to root on the same server on the same day at the same time? Root access had been documented, and signed out to the System Administrator, theodore. Apparently, the PowerBroker™ server was down, and root access could not be obtained using the pbrun command. Having the opportunity to give simon, on the job training, theodore was walking simon through the procedures.

Securing root

As stated above, to enhance the audit of root access, direct logon is denied for the root account. GIAC Enterprises uses the pbrun command to gain root privileges. Root access and other system accounts are denied via ftp and telnet. To prevent direct login with the userid root the **CONSOLE** variable has been set in /etc/default/login as shown:

```
% cat /etc/default/login
# PASSREQ determines if login requires a password.
PASSREQ=YES

# ALTSHELL determines if the SHELL environment variable should be set
ALTSHELL=YES

# IDLEWEEKS sets the amount of time an account with an expired password
# can remain unchanged before the account is automatically disabled.
#IDLEWEEKS=5

# TIMEOUT sets the number of seconds (between 0 and 900) to wait before
# abandoning a login session.
TIMEOUT=500

# SYSLOG determines whether the syslog(3) LOG_AUTH facility should be used
# to log all root logins at level LOG_NOTICE and multiple failed login
# attempts at LOG_CRIT.
#
SYSLOG=YES
# If CONSOLE is set, root can only login on that device.
# Comment the line below out to allow remote login by root.
CONSOLE=/dev/null
```

To defend against the accidental execution of a trojan horse program by root, the dot (.) or "current directory" is not allowed in the PATH environment variable set in root's .cshrc, .login, or .profile file. Root's search path is restricted to directories owned by root, such as /usr/bin:/sbin:/usr/sbin, and only fully justified filenames are used when executing applications. To ensure this policy is followed GIAC Enterprises runs scripts nightly to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ensure these files have not changed and specifically there is no dot (.) in root's path. If it appears in root's path, the System Administrator is notified via mail.

The Auditor ran check_path (in Appendix E) to see if the policy was being followed:

```
server001# check_path
TEST: Checking root's path for a dot (.)
  .login path is correct
  .cshrc path is correct
  .profile path is correct
------------ END OF TEST -------------------
```

To avoid having key strokes or display information inadvertently captured, GIAC Enterprises does not allow anyone in general, and specifically those with root access to use the "xhost +" command. The preferred authentication method is x-authentication / magic cookies, but the end users are allowed to issue an "xhost <machine_name>" which is why the xhost command has not been disabled. Displays are randomly scanned six to eight times a day to detect open displays. Displays are noted, and the scan notifies the end-user of the open display what the standard procedures are and who to contact for additional assistance.

The Auditor did not find any open displays when the Internet Scanner was run.

In addition to checking the `PATH` environment variable, GIAC Enterprises trains their system administrations to only source files owned by root which are not group or world writeable thus making it harder for a non-privileged user to subvert the root account.

Root's umask is set to 022 so that all files or directories created by root will have `rwxr-xr-x` permissions. This is verified, daily and a system administrator is notified via mail if it changes to anything other than 022.

```
server001# cd /
server001# grep umask .*
.cshrc:umask 022
```

GIAC Enterprises does not allow users at remote machines to log in without providing a password. Although GIAC Enterprises does not allow the use of /etc/hosts.equiv, the Auditor recommends taking advantage of Solaris 2.6 security by editing the PAM configuration policy file, pam.conf, to force users to provide a password even when a trust relationship has been defined using .rhosts or /etc/hosts.equiv. To do this, comment out the following lines in /etc/pam.conf:

```
rlogin  auth sufficient /usr/lib/security/pam_rhosts_auth.so.1
rlogin  auth required /usr/lib/security/pam_unix.so.1
rsh     auth required /usr/lib/security/pam_rhosts_auth.so.1
```

GIAC Enterprises /etc/pam.conf currently looks like:

```
# cat /etc/pam.conf
#ident  "@(#)pam.conf 1.19     95/11/30 SMI"
#
# PAM configuration
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
# Authentication management
#
login   auth required   /usr/lib/security/pam_unix.so.1
login   auth required   /usr/lib/security/pam_dial_auth.so.1
#
rlogin  auth sufficient /usr/lib/security/pam_rhosts_auth.so.1
rlogin  auth required   /usr/lib/security/pam_unix.so.1
#
dtlogin auth required /usr/lib/security/pam_mon.so.1 -threshold 3 -exec
/usr/lib/security/dtfail
dtlogin auth required   /usr/lib/security/pam_unix.so.1
#
rsh     auth required   /usr/lib/security/pam_rhosts_auth.so.1
other   auth required   /usr/lib/security/pam_unix.so.1
#
# Account management
login   account required        /usr/lib/security/pam_unix.so.1
dtlogin account required        /usr/lib/security/pam_unix.so.1
#
other   account required        /usr/lib/security/pam_unix.so.1
#
# Session management
other   session required        /usr/lib/security/pam_unix.so.1
#
# Password management
other   password required       /usr/lib/security/pam_unix.so.1
```

Even with the above change, the Auditor still recommends GIAC Enterprises scan user home directories for .rhosts files on a regular basis. The Auditor did not find any .rhosts files on the GIAC Enterprises systems. The check_rhosts script used is in Appendix E.

```
server001{root}26# ./check_rhosts
/                       has no .rhosts.
/apps                   has no .rhosts.
/users/mickey           has no .rhosts.
/users/minnie           has no .rhosts.
/users/theordore        has no .rhosts.
/usr/bin                has no .rhosts.
/usr/lib/uucp           has no .rhosts.
/usr/net/nls            has no .rhosts.
/usr/spool/lp           has no .rhosts.
/var/adm                has no .rhosts.
/var/spool/news         has no .rhosts.
/var/spool/uucppublic   has no .rhosts.
```

Audit also recommends GIAC Enterprises consider the following additions to /etc/system:

- Since GIAC Enterprises uses NFS on the Internal Network, force the NFS clients to connect from privileged ports by setting nfssrv:

  set nfssrv:nfs_portmon=1

- Eliminate the creation of core files by adding:

  set sys:coredumpsize=0

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

– Disable programs from using executable stacks.[2] Programs that attempt to execute code on their stack will be sent a SIGSEGV signal, which usually results in the program terminating with a core dump. Such programs also generate a warning message that includes the name of the offending program, the process ID, and real UID of the user who ran the program.

```
set noexec_user_stack=1
set noexec_user_stack_log=1
```

- Remove the ability to abort the system using the Stop-a keyboard sequence
  set abort_enable = 0

Account Maintenance

As part of Account Management, GIAC Enterprises tries to ensure the number of active accounts on each host is minimized and authorized. Before a system goes into production accounts such as guest & visitor are deleted and their existence is rechecked during Account Maintenance.

Default accounts created by installation programs are either deleted or the default passwords for these accounts are changed before the system goes into production.

GIAC Enterprises documentation states that all of the ids listed below should be reviewed. They were created during installation, and maybe required by the operating system, however they must be locked before any system goes into production:

- adm
- bin
- daemon
- listen
- lp
- nobody
- noaccess
- nuucp
- smtp
- sys
- uucp
- nobody4

Audit recommends eliminating those accounts that have no use, such as smtp.

GIAC Enterprises does not currently use the /etc/ftpusers file. Audit recommends that this file be created to contain root and the accounts listed above at a minimum. This will add to security of the system by preventing ftp access by any accounts listed in the file.

```
touch /etc/ftpusers
for user in root adm bin daemon listen lp nobody noaccess nuucp smtp sys uucp nobody4
  do
    echo $user >> /etc/ftpusers
  done
chown root /etc/ftpusers
chgrp root /etc/ftpusers
chmod 600 /etc/ftpusers
```

or for added security, cat /etc/passwd into /etc/ftpusers and remove those users authorized to use ftp:

```
cat /etc/passwd | awk -F: '{ print $1 }' >> /etc/ftpusers
chown root /etc/ftpusers
chgrp root /etc/ftpusers
```

[2] Note that there may be some applications, which will break if this security setting is configured – although we've not found any as yet – these settings must be done in a test environment prior to being put into production.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
chmod 600 /etc/ftpusers
```

Since the operating system will prevent login for an account that is assigned an invalid shell, GIAC Enterprises assigns the shell /dev/null as the shell for accounts that should never be allowed to log in. Audit recommends obtaining the "noshell" [3] program and replacing /dev/null with noshell to enable all failed login attempts to be logged to syslogd. All accounts with a null shell should also be added to the /etc/ftpusers file.

GIAC Enterprises does Account Maintenance for all accounts to ensure:

- all personnel with accounts have a valid need to access the system.
- access to the root account and other System Accounts is restricted (i.e., no user accounts have been assigned a UID of less than 100).
- all access to root is via a method other than direct login, and is always logged to syslogd
- all PowerBroker™ access accounts are verified at a minimum yearly, to ensure that the access is required.
- no accounts other than root and smtp have the user id (UID) of 0 (zero)
- Solaris' shadow password file is being used on all systems
- there are no accounts that do not require a password to log in
- all default passwords have been changed.
- duplicate uids or gids are eliminated or documented
- Invalid login attempts are logged.
- Inactive accounts, determined by the lack of a login within 3 months, are locked.
- accounts that have been inactive for 7 months or more are deleted. (GIAC Enterprises does not offer a leave of absence greater than 6 months, thus it is not expected for anyone to have an inactive account for more than 7 months.)

The Auditor spot-checked the above policy on a GIAC Enterprise server by issuing the following commands:

```
logins -p              - shows all accounts without passwords.  GIAC Enterprises did
                         not have any accounts without passwords.
cat /etc/passwd        - verified an x appeared in the password field of /etc/passwd
                         to  indicate shadow password was implemented
ls -al /etc/shadow     - verified the existence of the file along with the
                         permissions to be -r--------  and the ownership to be root.
cat /etc/default/login - verified the PASSREQ variable was set to YES and
                         uncommented.
cat /etc/default/passwd - verified the PASSLENGTH variable was set to a minimum of 6
                         characters and uncommented.  GIAC Enterprises had it set to
                         7.  Industry standards says that 6 to 8 is acceptable.
```

Password Maintenance

GIAC Enterprises uses the 3rd party software package PowerPassword™ to control machine access via passwords. The Auditor was shown how GIAC Enterprises uses PowerPassword™ to implement the GIAC Enterprises' requirements, such as:

[3] The noshell can be obtained from the TITAN security package at http://www.fish.com/titan.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- what time of day a user may log in to eliminate contractors from logging in during off hours,
- who may log in over modem lines or over the network,
- which machines a user can log in to, on a user, group, department, and machine level
- the amount of time for password-aging (minimum – how long does a user wait before he's allowed to change his password again; and maximum – how long can a user keep the same password before he is required to change it.)
- the requirements for the password history
- the login environment for each user
- what directory the user is placed in upon login
- what environment variables are set upon login
- whether a shell or some other program is invoked for the user
- the number of incorrect password attempts to allow before disabling the account
- minimum password quality standards (e.g., passwords must be a minimum of 7 characters containing at least 2 non-alphanumeric characters, and people cannot re-use a password they have used any time during the preceding 6 months, passwords cannot be any of the words in the dictionary and they cannot be concatenated short words (e.g., goodtime) or words with numbers concatenated (e.g., iamnum1 vs. I'm#1Dad))
- login banner to be displayed
- log failed login attempts

GIAC Enterprises also uses PowerPassword™ to maintain a complete trail of login activities to allow them to keep track of who has been accessing any given system at any given time. PowerPassword™ audit logs contain a full record of each login, successful or not.

GIAC Enterprises sends out reminders, quarterly, to all their staff with suggestions on choosing good passwords. For example, one tip circulated while the Auditor was on-site:

> ***Choosing Good Passwords***
>
> To generate secure passwords use the leading letters from poems or song lyrics, with non-alphanumeric characters (e.g. -, *, {, }) thrown in. This will help create a mnemonic strategy to make the password easy to remember, thus avoiding the need to have it written down. One should also make the constructed password is easy to type to make it harder for *shoulder surfers* to learn the password by observing you as you enter it.

The Auditor reviewed the system logs and found the following regarding passwords and failed login attempts:

```
Nov  4 04:17:22 server001 passwd_chk: MICKEY - Password REJECTED because needs at least 1 non-
alphabetic.
Nov  4 04:40:12 server001 passwd_chk: MINNIE - Password REJECTED because it is based on a dictionary
word.
Nov  4 08:17:22 server001 passwd_chk: GOOFY - Password REJECTED because needs at least 2 alphabetic.
Nov  4 08:18:22 server001 passwd_chk: GOOFY - Password REJECTED because it does not contain enough
DIFFERENT characters.
Nov  4 08:19:00 server001 passwd_chk: GOOFY - Password REJECTED because it is based on a (reversed)
dictionary word.
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
Nov  4 08:21:22 server001 passwd_chk: DISNEY - Password REJECTED because it is too
simplistic/systematic.
Nov  4 08:22:22 server001 passwd_chk: just_checking - Password accepted.
Nov  4 08:22:27 server001 last message repeated 2 times
Nov  4 08:22:29 server001 passwd_chk: just_checking - Password REJECTED because it is based on a
dictionary word.
Nov  4 08:33:28 server001 passwd_chk: just_checking - Password accepted.
Nov  4 08:35:29 server001 last message repeated 4 times
Nov 10 02:25:15 server001 pplogin2.2.3a: 1 LOGIN FAILURE FROM evilone001
Nov 10 03:08:11 server001 pplogin2.2.3a: 1 LOGIN FAILURE FROM evilone001
hmm ➔ Jan 29 08:00:38 server001 pplogin2.2.3a: 1 LOGIN FAILURE FROM evilone001, root
Feb 12 10:41:22 server001 pplogin2.2.3a: 1 LOGIN FAILURE FROM giacsrv008
Feb 12 10:42:14 server001 pplogin2.2.3a: 1 LOGIN FAILURE FROM giacsrv008, steven
```

When a GIAC Enterprises employee forgets their password, they call the centralized Help Desk. The Auditor obtained the information about an employee and tried to convince the Help Desk personnel to change the password. Although the Auditor convinced them to change the password, the Help Desk is not permitted to give the user the password over the phone. The Auditor told the Help Desk that he could not access his e-mail account without a new password, and the Help Desk said they'd leave the password via a phone message on the user's business answering system. The Auditor could not gain access to passwords via the Help Desk. The System Administrators are not authorized to change user's passwords, even though they have the capability. The System Administrators are trained on what the Help Desk is allowed to do, and they're instructed that they have too much to do to do the job of the Help Desk. Obviously, since the System Administrator knows his users he would not change the password for the Auditor either. When the Help Desk changes a user's password, the user is forced to change it immediately upon their first login.

After reviewing GIAC Enterprises Password Maintenance, the Auditor recommends two areas for future consideration:

1. Automate the log review of the LOGIN FAILUREs. How many times have you received LOGIN FAILUREs from the server evilone001? Automate reviewing all the log information for a pattern such as "<GIAC Machine> LOGIN FAILURE from <machine name>". If you're getting hit from the same machine with bogus userids, it's probably something worth looking into!
2. Consider two-factor authentication that will fit into GIAC Enterprise's pre-existing environment.

Security Warning Banners

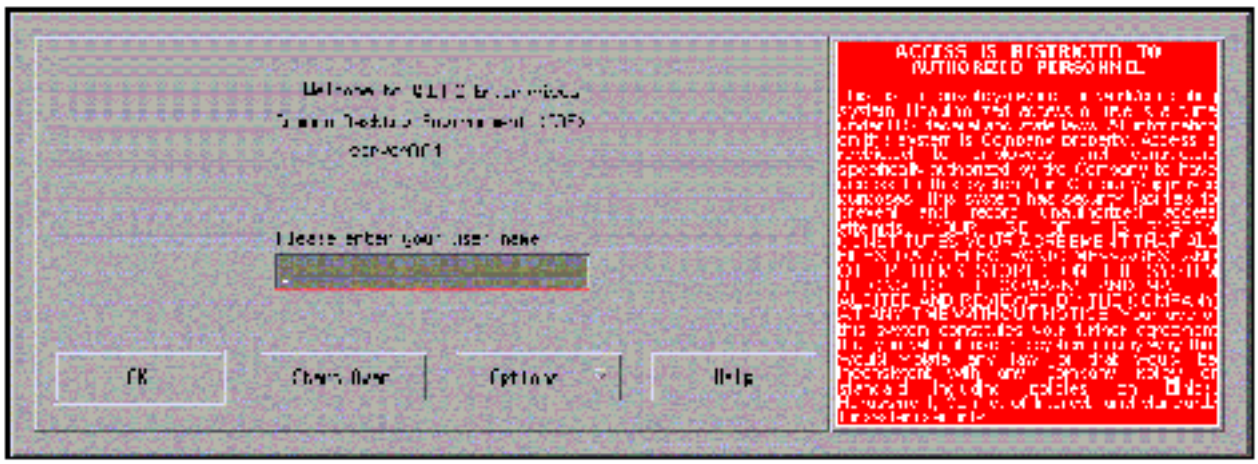
GIAC Enterprises is using the /etc/issue file as delivered with the Operating System. The Auditor recommends removing or changing the Operating System Version Information. It is not necessary to give away information.

```
%cat /etc/issue
Sun Microsystems Inc. SunOS 5.6                    Generic May 1998
**********************************************************************
*          ACCESS IS RESTRICTED TO AUTHORIZED PERSONNEL              *
*                                                                    *
* This is a privately-owned network/computing system. Unauthorized   *
* access or use is a crime under U.S. federal and state laws. All    *
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
* information on this system is Company property. Access is restricted *
* to employees and contractors specifically authorized by the Company  *
* to have access to this system for Company-approved purposes. This    *
* system has security facilities to prevent and record unauthorized    *
* access attempts. YOUR USE OF THIS SYSTEM CONSTITUTES YOUR AGREEMENT  *
* THAT ALL FILES, DATA, ELECTRONIC MESSAGES, AND OTHER ITEMS STORED ON *
* THE SYSTEM BELONG TO THE COMPANY AND MAY BE AUDITED AND REVIEWED BY  *
* THE COMPANY AT ANY TIME WITHOUT NOTICE. Your use of this system      *
* constitutes your further agreement that you will not use the system  *
* in any way that would violate any law, or that would be inconsistent *
* with any Company policy or standard including policies on Ethics,    *
* Harassment, Conflict of Interest, and standards for system security. *
************************************************************************
```

Except on systems using CDE for login, the block of text above will be displayed above the login prompt. For those systems using CDE, GIAC Enterprises modified the cde/app-defaults/C/Dtsession file to display the GIAC Enterprises modified Banner such as what is shown below.



The /etc/default/telnetd and /etc/default/ftpd files were modified to set the BANNER variable to null to stop the OS Information from being displayed upon a telnet session being initiated.

The /etc/motd file did not exist on any of the systems audited. Should GIAC Enterprises desire the /etc/motd file can be used as an additional resource to display additional Security Monitoring Warnings or Information to the users.

Audit recommends, to avoid giving away information regarding the sendmail version change the banner message that the sendmail process presents for incoming mail delivery connections. The Auditor searched the /etc/mail/sendmail.cf file and found the following line:

SmtpGreetingMessage=$j Sendmail $v/$Z; $b

Audit recommends changing it to something like:

SmtpGreetingMessage=Mail Server Ready

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

System Configuration Management

GIAC Enterprises restricts all the configuration changes to the System Administrative Team. Training the administrators and setting the permissions and ownerships of the system files appropriately enforces the policy.

GIAC Enterprises has set up configuration files specifying file permissions, ownership, and group for pre-determined files. Scripts are run daily via root's crontab to document changes and automatically set the file attributes back to the documented setting if they were changed. A report like the one below is mailed to the Administrator to alert him on changes made or possibly needed to be made.

The Auditor used a listing of Casper Dik's fix-modes settings acquired from http://www.usenix.org/sage/sysadmins/solaris/index.html and documented them in an audit configuration file. The audit configuration file was processed using GIAC Enterprise's internal scripts, to display and not correct the specified configuration. The following listing shows the results:

```
CRITICAL: Permissions (-rwsr-s---) incorrect for /usr/vmsys/bin/chkperm, expected (-rwsr-xr-x).
CRITICAL: Permissions (-rwsr-s---) incorrect for /usr/openwin/bin/xload, expected (-rwxr-xr-x).
CRITICAL: Permissions (-rwsr-s---) incorrect for /usr/openwin/bin/mailtool, expected (-r-xr-xr-x).
CRITICAL: Permissions (-rwsr-s---) incorrect for /usr/openwin/bin/ff.core, expected (-r-sr-xr-x).
CRITICAL: Permissions (-rwsr-s---) incorrect for /usr/sbin/wall, expected (-r-xr-xr-x).
CRITICAL: Permissions (-r-xr-sr-x) incorrect for /usr/sbin/sysdef, expected (-r-xr-xr-x).
CRITICAL: Permissions (-r-xr-sr-x) incorrect for /usr/sbin/swap, expected (-r-xr-xr-x).
CRITICAL: Permissions (-r-xr-sr-x) incorrect for /usr/sbin/prtconf, expected (-r-xr-xr-x).
CRITICAL: Permissions (-r-xr-sr-x) incorrect for /usr/sbin/dmesg, expected (-r-xr-xr-x).
CRITICAL: Permissions (-r-xr-sr-x) incorrect for /usr/sbin/arp, expected (-r-xr-xr-x).
CRITICAL: Permissions (-r-xr-sr-x) incorrect for /usr/bin/ipcs, expected (-r-xr-xr-x).
CRITICAL: Permissions (-r-xr-sr-x) incorrect for /usr/bin/netstat, expected (-r-xr-xr-x).
CRITICAL: Permissions (-r-xr-sr-x) incorrect for /usr/bin/write, expected (-r-xr-xr-x).
CRITICAL: Permissions (-r-x--s--x) incorrect for /usr/bin/mailx, expected (-r-x--x--x).
CRITICAL: Permissions (-r-x--s--x) incorrect for /usr/bin/mail, expected (-r-x--x--x).
CRITICAL: /usr/lib/uucp/uuxqt does not exist, or cannot be accessed.
CRITICAL: /usr/lib/uucp/uusched does not exist, or cannot be accessed.
CRITICAL: /usr/lib/uucp/uucico does not exist, or cannot be accessed.
CRITICAL: /usr/bin/uux does not exist, or cannot be accessed.
CRITICAL: /usr/bin/uustat does not exist, or cannot be accessed.
CRITICAL: /usr/bin/uuname does not exist, or cannot be accessed.
CRITICAL: /usr/bin/uuglist does not exist, or cannot be accessed.
CRITICAL: /usr/bin/uucp does not exist, or cannot be accessed.
CRITICAL: Permissions (-r-xr-xr-x) incorrect for /usr/bin/uuencode, expected (-r--------).
CRITICAL: Permissions (-r-xr-xr-x) incorrect for /usr/bin/uudecode, expected (-r--------).
CRITICAL: Permissions (-r-xr-xr-x) incorrect for /usr/sbin/sync, expected (-r--------).
CRITICAL: /usr/sbin/snoop does not exist, or cannot be accessed.
CRITICAL: Permissions (-r-sr-xr-x) incorrect for /usr/bin/rdist, expected (-r-x------).
CRITICAL: Permissions (-rwsr-xr-x) incorrect for /usr/bin/at, expected (----------).
CRITICAL: Permissions (drwxr-xr-x) incorrect for /etc/security, expected (drwxr-x---).
```

Audit recommends that GIAC Enterprises implement the expectations above in the tightest mode possible to limit access to root suid programs. This recommendation is minimal effort since the Auditor has already written the configuration file for this audit. GIAC Enterprises would need to incorporate it in as part of their daily checks and corrections already being done. Those files listed as "does not exist …" should remain in the configuration file as another detection method for files mysteriously showing up.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Many of the setuid and setgid programs on Solaris are used only by root, or by the user or the group-id to which they are set. As shown above, they can easily have setuid and setgid removed without diminishing the user's abilities to get their work done. Audit recommends, GIAC Enterprises review each of the setuid / setgid programs currently on their system and determine their necessary usage. Any programs not used should be removed, chmod'd to 000, or at a minimum the setuid / setgid should be removed. GIAC Enterprises should review the setuid snapshot taken by the Auditor to adjust the permissions or to document why the company chooses to leave the application setuid:

```
# find / -perm -4000 -print
/usr/lib/lp/bin/netpr
/usr/lib/fs/ufs/quota
/usr/lib/fs/ufs/ufsdump
/usr/lib/fs/ufs/ufsrestore
/usr/lib/exrecover
/usr/lib/pt_chmod
/usr/lib/sendmail
/usr/lib/utmp_update
/usr/lib/acct/accton
/usr/lib/fs/vxfs/vxdump
/usr/lib/fs/vxfs/vxquota
/usr/lib/fs/vxfs/vxrestore
/usr/lib/exrecover
/usr/lib/pt_chmod
/usr/lib/sendmail
/usr/lib/utmp_update
/usr/lib/acct/accton
/usr/lib/uucp/remote.unknown
/usr/lib/uucp/uucico
/usr/lib/uucp/uusched
/usr/lib/uucp/uuxqt
/usr/lib/sendmail.orig
/usr/openwin/lib/mkcookie
/usr/openwin/bin/xlock
/usr/openwin/bin/ff.core
/usr/openwin/bin/kcms_configure
/usr/openwin/bin/kcms_calibrate
/usr/openwin/bin/sys-suspend
        …
        …
        …
/usr/sbin/allocate
/usr/sbin/mkdevalloc
/usr/sbin/mkdevmaps
/usr/sbin/ping
/usr/sbin/sacadm
/usr/sbin/whodo
/usr/sbin/deallocate
/usr/sbin/list_devices
/usr/sbin/m64config
/usr/sbin/lpmove
/usr/sbin/pmconfig
/usr/sbin/static/rcp
/usr/sbin/vxprint
/usr/sbin/vxmkcdev
/usr/ucb/ps
/usr/vmsys/bin/chkperm
/etc/lp/alerts/printer
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Aside from the checking that has been described in the above sections, GIAC Enterprises does not check their file systems for security holes. At a minimum, GIAC Enterprises needs to check for files that could:

- be modified by unauthorized users,
- inadvertently grant users too many permissions, and
- inadvertently grant access to data considered being of value to the Corporation.

Audit recommends GIAC Enterprises verifies the file systems has:

- Proper file permissions
- Proper file ownership
- Proper file group settings
- Proper files

Audit agrees that it is important to check files for setuid and setgid, however GIAC Enterprises must consider scanning for and fixing the permissions on world-writeable files. World-writeable files become an extreme security risk even on an Internal Network. Appendix C lists Caper Dik's Solaris Exceptions for System World-writeable Files. **All** world-writeable files (system and user) should be reviewed to determine if world-write is needed within the GIAC Enterprises Environment. If world-write is not needed, it should be removed.

Audit has listed the world-writeable directories found on the GIAC Enterprises' server:

```
 # find / -type d -perm -2 -prune
/var/sadm/patch
/var/opt/SUNWdat/trc
/var/spool/lp/fifos/public
/var/spool/calendar
/var/tmp
/var/dt/tmp
/var/mail.old
/etc/Legato/nsr/tmp
/etc/Legato/nsr/applogs
/opt/SUNWrtvc/examples/rtvc_capture_movie
/opt/SUNWrtvc/examples/rtvc_display
/opt/SUNWrtvc/examples/rtvc_video_conference
/opt/SUNWdat
/tmp
```

"Improper Files" is the Auditor's term for files that are not incorrect in any means. Improper files include un-owned files, dangling links (i.e., link points to a file or directory that has been moved or deleted), invalid group specified, etc.

Finding files that are owned by nonexistent users can often be a clue that a cracker has gained access to your system. Even if this is not the case, searching for these files gives you an opportunity to clean up files that should have been deleted at the same time the user's account was deleted. The command to find un-owned files is:

```
# find / -nouser -print
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The -nouser option matches files that are owned by a user id not contained in the /etc/passwd database. A similar option, -nogroup, matches files owned by nonexistent groups. To find all files owned by nonexistent users or groups, you would use the –o option as follows:

```
# find / -nouser -o -nogroup -print
```

Appendix D lists other Audit recommendations for changes to current GIAC Enterprises System File permissions.

In addition to the System Files, Audit recommends GIAC Enterprises review all user files for items such as:

- Check for dot, startup files writable by others.
- Look for dot, startup files owned by other users.
- Check for executables with the same name as systems programs.
- Check for ".rhosts" and ".netrc" files – these should not exist, but if they do check to see if they are readable and writable by anyone other than the owner.
- Check to ensure the user directories are writable by the owner only, and all files are owned by the user.

Based on reviewing the required file configurations it is understood that unless there's an automated tool to assist in the review, it will never get done. Audit recommends GIAC Enterprises purchase a tool such as TripWire [4], or obtain a shareware package like cops to begin doing Cyclic Redundancy Checks (crc_chk as named in cops) on System Files. This would allow GIAC Enterprises to check for unexpected file system corruption or security breaches, using CRC values that are generated from your system files, then compared against previously calculated values. As Dan Farmer says: "It's nice to be able to say that you know all your files are as they should be."

If purchasing a 3rd Party Vendor Tool, or using COPs is not an option, GIAC Enterprises should consider using the software registry for configuration management, which is part of the Solaris Operating System. The software registry (pkgchk) can be used to:

- audit all files in the Solaris software registry
- audit installed software
- check installed files against the original package or patch
- check diskless clients or systems booted from alternate boot devices
- repair file attributes

To further protect the systems, GIAC Enterprises should consider using the nosuid option in /etc/vfstab when defining how the file systems should be mounted. When execution of setuid programs is required, as in the /usr file system which contains some setuid

[4] Tripwire is a file and directory integrity checker. Tripwire is a tool that aids system administrators and users in monitoring a designated set of files for any changes. Used with system files on a regular (e.g., daily) basis, Tripwire can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

executables essential to system operation, then consider mounting that file system read-only instead of using the nosuid option. A sample /etc/vfstab is shown for clarification:

```
% cat /etc/vfstab
#device             device              mount    FS     fsck   mount   mount
#to mount           to fsck             point    type   pass   at boot options
#========================================================================
/proc               -                   /proc    proc   -      no       -
fd                  -                   /dev/fd  fd     -      no       -
swap                -                   /tmp     tmpfs  -      yes      -
/dev/dsk/c0t3d0s1   -                   -        swap   -      no       -
/dev/dsk/c0t3d0s0   /dev/rdsk/c0t3d0s0  /        ufs    1      no   remount,nosuid
/dev/dsk/c0t3d0s4   /dev/rdsk/c0t3d0s4  /usr     ufs    1      no       ro
/dev/dsk/c0t3d0s5   /dev/rdsk/c0t3d0s5  /var     ufs    1      no       nosuid
```

System Services

With few exceptions, as listed in the sections above, GIAC Enterprises left a lot of the default system behavior. This includes the boot scripts. When the system is booted the **init** process uses entries in the **/etc/inittab** to bring the system to the desired state. It does this by executing the scripts (S for start and K for kill) in the appropriate **/etc/rc*.d** directories. The rc* directories are organized by run level, and many of the entries in these directories are links to files in the directory **/etc/init.d**. The Auditor recommends disabling all unnecessary system services by removing the service's startup script from the appropriate rc directory.

Network Services

GIAC Enterprises has implemented TCP Wrappers to monitor and filter incoming requests for network services such as: SYSTAT, FTP, TELNET, RLOGIN, RSH, EXEC, TFTP, and others.

With Solaris 2.6, inetd.conf now appears in /etc/inet. The /etc/inetd.conf file should be a link to /etc/inet/inetd.conf. GIAC Enterprises had two separate files, one in /etc and one in /etc/inet, which were not the same. Some applications still refer to /etc/inetd.conf while others have been updated to refer to /etc/inet/inetd.conf. Having a file in both directories is a security risk unless you know exactly what directory your applications are referencing. Since the two files were different, and they both had a lot of services enabled, Audit did not review the contents of either file for recommendations.

This is a perfect example of why crc checks were created. The Auditor could not find anyone who knew why the two files existed.

The Auditor recommends, GIAC Enterprises:

- Correct the inetd.conf file in /etc/inet.
- Set up a link to /etc/inet/inetd.conf in /etc.
- Disable the services listed below by commenting them out in **/etc/inet/inetd.conf** and restart the daemon (kill -hup inetd). These recommendations are based on CERT Advisors and recommendations from vendor tools such as ISS.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
#talk    dgram   udp     wait    root    /usr/sbin/in.talkd      in.talkd
#uucp    stream  tcp     nowait  root    /usr/sbin/in.uucpd      in.uucpd
# Tftp service is provided primarily for booting.  Most sites run this
# only on machines acting as "boot servers." Also required by X-Terms servers
#tftp   dgram  udp  wait root  /usr/sbin/in.tftpd   in.tftpd -s /tftpboot
#
# Finger, systat and netstat give out user information, which may be
# valuable to potential system crackers. Disable some or all of these
# services to improve security.
#finger   stream tcp  nowait  nobody  /usr/sbin/in.fingerd    in.fingerd
#systat   stream tcp  nowait  root    /usr/bin/ps             ps -ef
#netstat  stream tcp  nowait  root    /usr/bin/netstat        netstat -f inet
#
# Echo, discard, daytime, and chargen should not be used in a production system.
#echo      stream  tcp     nowait  root    internal
#echo      dgram   udp     wait    root    internal
#discard   stream  tcp     nowait  root    internal
#discard   dgram   udp     wait    root    internal
#daytime   stream  tcp     nowait  root    internal
#daytime   dgram   udp     wait    root    internal
#chargen   stream  tcp     nowait  root    internal
#chargen   dgram   udp     wait    root    internal
#
# Solstice system and network administration class agent server
#100232/10 tli   rpc/udp   wait    root    /usr/sbin/sadmind     sadmind
#
# The rusers service gives out user information.  Security conscious sites
# should disable it.
#rusersd/2-3 tli rpc/datagram_v,circuit_v wait root /usr/lib/netsvc/rusers/rpc.
#rusersd        rpc.#rusersd
#
# sprayd is used to record packets, disable it and use a reliable packet sniffer.
#sprayd/1  tli  rpc/datagram_v wait root /usr/lib/netsvc/spray/rpc.sprayd      rpc.sprayd
#
# RPC, by itself, can be used to provide an attacker with information about a system.
# While this may not be ideal, the real security problem is not the rpcbind daemon
# itself, but rather the many services that use RPC. Many of these services do not make
# use of the stronger authentication mechanisms available to them and default to weak
# authentication. In particular, rpc.cmsd, sadmind (running without -S 2), and rpc.rexd
# use weak authentication by default.  Network based attacks against these services pose
# a significant threat to the security of a server.
# testsvc
# sadmind
# rquotad
# rpc.rusersd
# rpc.rwalld
# rpc.rstatd
# rpc.rexd
# ufsd
# kcms.server
# fs
# cachefsd
# kerbd
# in.lpd
# dtspcd
# xaudio
# rpc.cmsd
# rpc.ttdbserver
```

The daemons and services, which use RPC on Solaris, include:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

From /etc/rc2.d/S71rpc:

```
- rpcbind
- keyserv
- rpc.nisd
- nis_cachemgr
- rpc.nispasswdd
```

From /etc/rc3.d/S15nfs.server:

```
- rpc.bootparamd
```

The RPC daemons started in /etc/rc2.d and /etc/rc3.d are for rpcbind, keyserv, various naming services (i.e., NIS and NIS+), and are also used by both the client and server components of NFS. The keyserv daemon must be run when AUTH_DES is used for stronger host and user authentication. The use of NIS is not recommended due to its weak encryption and authentication models.

Since GIAC Enterprises uses both NFS and NIS it is recommended to disable all RPC related links not relating to NFS in /etc/rc2.d/S71rpc.

In addition, since a system should never run in states other than "off", "single-user" and full multi-user mode, it is recommended to remove files for run states other than level 2:

```
rm –f /etc/rc[013].d/*
```

As shown with inetd.conf, Solaris 2.6 supports the services file located in /etc/inet. For backward compatibility, the /etc/services file should be a link to /etc/inet/services. Since GIAC Enterprises had two separate files, which were not the same, Audit did not review the contents of either.

Audit recommends eliminating all unnecessary services and setting secure options for those services that are enabled. For example, the ftp daemon can be setup to run with the –l flag so that each FTP session is logged to syslogd which gives the company additional information should a cracker ftp a rootkit onto one of the systems.

```
ftp      stream  tcp     nowait  root    /usr/sbin/in.ftpd -l    in.ftpd –l
```

Network Access Control

GIAC Enterprises has enabled the file /etc/notrouter[5] to disable IP forwarding at boot time. Since the ndd command allows IP forwarding to be switched on or off while the system is operating, GIAC Enterprises documented modifications to the /etc/init.d/inetinit to avoid attacks such as IP Masquerading. The following changes were observed in /etc/default/inetinit [6]:

```
% cat  /etc/default/inetinit
```

[5] Creating the /etc/notrouter file is equivalent to setting the ip_forwarding parameter to 0, however the Auditor recommends both should someone manage to delete the /etc/notrouter file

[6] It is important to note, ndd parameter documentation is not available from Sun, and Sun may also change the names of parameters in future versions of Solaris software.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
# @(#)inetinit.dfl 1.2 97/05/08
#
# TCP_STRONG_ISS sets the TCP initial sequence number generation parameters.
# Set TCP_STRONG_ISS to be:
#       0 = Old-fashioned sequential initial sequence number generation.
#       1 = Improved sequential generation, with random variance in increment.
#       2 = RFC 1948 sequence number generation, unique-per-connection-ID.
#
TCP_STRONG_ISS=2
```

GIAC Enterprises Network Policy outlined modifications to /etc/rc2.d/S69inet as follows:

```
# Turn off IP Forwarding  -- do not do the job of the routers
/usr/sbin/ndd -set /dev/ip ip_forwarding 0

# Source routing may be used to bypass security measures in the network
# topology. There is no reason to see source-routed packets in a network.
# Any host that does allow IP-forwarding should silently drop
# source-routed packets
/usr/sbin/ndd -set /dev/ip ip_forward_src_routed 0

# To prevent an attacker from probing or attacking the systems by
# taking advantage of forwarded directed broadcasts, disable directed
# broadcast forwarding [7]:
/usr/sbin/ndd -set /dev/ip ip_forward_directed_broadcasts 0


# To decrease the chances of a denial of service attack, disable the respond
# to echo broadcast by adding the following to the end of /etc/rc2.d/S69inet:
/usr/sbin/ndd -set /dev/ip ip_respond_to_echo_broadcast 0
```

The Auditor used the checking portion of the disable_ip_holes.sh from the TITAN project and put together the script, shown in Appendix E, to verify GIAC Enterprise's Network Policy. As shown, below, 5 out of 7 checks failed because the GIAC Enterprises Network Policy was not fully implemented.

```
server001{root}: ./ip_chks

IP source routing is currently set to 1
   System allows source routed packet forwarding - FAILS CHECK

IP forwarding is currently set to 0
   System does not Forward IP packets - PASSES CHECK

IP forwarding directed broadcast is currently set to 1
   System allows forwarding of directed broadcasts - FAILS CHECK

IP respond to echo broadcast packets set to 1
   System allows response to echo broadcasts - FAILS CHECK

IP ignore redirect is currently set to 0
   System is not set to ignore redirected packets - FAILS CHECK

 IP strict multihoming is currently set to 0
   System is not set to do strict destination multihoming - FAILS CHECK

/etc/notrouter exists.
         System configured as 'notrouter' - PASSES CHECK
```

[7] CERT Advisory CA-98.01

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
IP Settings are incorrect in /etc/rc2.d/S69inet -- please check.
```

The Auditor recommends GIAC Enterprises complete the implementation of the documented Network Policy.

Since all the machines are in a JumpStart Environment, the Auditor recommends disabling the startup scripts used to re-initialize or re-install the system as follows:

```
sh
cd /etc/rc2.d
for file in S30sysid.net S71sysid.sys S72autoinstall
   do
      mv $file DISABLED.$file
   done
```

These startup scripts will never be used in a JumpStart environment and should be disabled to prevent an intruder or any root user from reconfiguring the system.

cron *Security*

The Auditor recommends restricting access to cron. The access control files are stored in the /usr/lib/cron directory. The cron.deny and cron.allow files manage access to the cron system.

- To determine if the account is explicitly allowed access to this system, the "allow" file is checked first. If the file does not exist or the account is not listed in this file, the "deny" file is checked.
- If the account is explicitly listed in the "deny" file then access is refused. Otherwise, access is permitted.
- If neither the "deny" nor the "allow" files exist, then only the root account can use the cron system.

```
server001{root}32# pwd
/usr/lib/cron
eutsss001{root}33# ls -al
total 22
drwxr-xr-x   2 root     sys          512 Jan 20 07:41 ./
drwxr-xr-x  29 root     root        4096 Feb 13 07:20 ../
-rwxr--r--   1 root     sys           72 Jan  1  1970 .proto*
-rw-r--r--   1 root     sys           45 Aug 31 13:47 at.deny
-rw-r--r--   1 root     sys           45 Aug 31 13:47 cron.deny
prw-------   1 root     root           0 Feb 16 15:50 FIFO|
-r-xr-xr-x   1 bin      bin         1626 Aug 31 15:09 logchecker*
-rw-r--r--   1 root     sys           17 Jan  1  1970 queuedefs
```

As shown above, the Auditor reviewed what was on GIAC Enterprises systems. Since there is a cron.deny file, and no cron.allow file, it means that everyone except those listed in the cron.deny file has access to cron. By default, Solaris 2.6 includes the cron.deny file, which contain some system accounts. As shown below, that is all that GIAC Enterprises has entered in their cron.deny:

```
server001{root}38# cat cron.deny
daemon
bin
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
smtp
nuucp
listen
nobody
noaccess
```

To avoid internal user abuse or having a cracker plant a "time bomb", it is best to restrict access to the cron system. Any system or software specific accounts that do not require cron access should be added to the "deny" files. Restrict individual user accounts by listing them in the "deny" file or **to restrict all user account access, create an empty "allow" file** and then add only the accounts that need access to the "allow" file.

Keep a log of all actions taken by cron, by setting CRONLOG=YES in the /etc/default/cron file. If CRONLOG=NO is specified, no logging is done. GIAC Enterprises had this option set to NO and also allowed user cronjobs as was evident by the list in /var/spool/cron/crontabs. GIAC Enterprises stated that it is their policy to allow user cronjobs on the Internal Network and they did not want to fill up their logs with cron output.

```
server001: more /etc/default/cron
CRONLOG=NO
```

If users are going to be allowed to use cron, Audit recommends GIAC Enterprises set a requirement for the System Administrators to review all the cron jobs by reading the cron file of every system account in /var/spool/cron/crontabs.

Upgrades and Updates

GIAC Enterprises Upgrade policy requires a review of system requirements at a minimum annually. CERT Advisories are reviewed and a determination of the risk and criticality of the vulnerability in their environment is documented. If the Company risk or criticality is high, steps are taken to implement the fix immediately, otherwise, the implementation is delayed until the Quarterly System Update. Formal GIAC Enterprises Change Management Procedures are followed in all cases.

The Solaris patch releases are reviewed and implemented in the same manner as the Vulnerability Fixes above. The Change Management Procedures account for the critical (or emergency) patches to be implemented immediately (i.e., within 2 to 3 weeks of acquisition).

To implement the change, the System Administration Team, use a 2-system test methodology. The first test environment is exactly that, a test environment. The test environment is managed via a Change Management System but it is constantly changing as changes are being tested. The second test environment, simulates (as best as possible) the production environment. Any change must go through both test environments, a week each successfully, before production implementation is approved. The Jumpstart Methodology is used in all environments to push the changes into the environment. GIAC Enterprise's Jumpstart procedures account for the different architectures as well as the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

different operational purpose (i.e., NFS Servers, DNS Servers, Application Servers, Clients, etc.). Jumpstart gives the company additional documentation of what should be on each machine, as well as a controlled process to install upgrades and patches.

Third party software goes through a formal risk assessment prior to any approvals for installation into the Test Environments. The stringent procedures for installing and testing 3rd party software are clearly documented and easy to follow.

The Auditor was impressed by the conscious actions of all those involved in the Software Installations. All Company Procedures and Policies were followed and no short cuts were observed. The Auditor feels the Upgrades Procedures are adequate at this time.

System Logging

GIAC Enterprises' objective for logging is for purposes of audit trails, and to alert someone of a potential problem. As discussed in the sections above, GIAC Enterprises has enabled logging, however there are areas which can be turned on for additional information.

Process Auditing

The Auditor recommends always logging the following event-types, some of which are already implemented:

- network
- process
- administrative
- login / logout
- application
- exec
- other
- non_attrib

Given, at the current time, the System Administrators do not have the resources to proactively review the logs the Auditor recommends not enabling logging of the file_creation, file_deletion, file_attr_mod, file_write file_read and file_close classes or any other more extensive classes.

GIAC Enterprises has setup cronjobs to execute in-house scripts to parse syslog and other logs daily and **mail any extreme anomalies to the administrators.** This is the extent of GIAC Enterprises log analysis. Obviously, there are portions of the logs that are not being parsed or mailed. This means that no one is reviewing the daily logins that are being logged. No one is looking for a trend across the various systems so that an attempt can be proactively blocked before it becomes an intrusion. For example, since GIAC Enterprises centralizes the logs, it would be easy to grep out known accounts, like guest and quickly realize that someone tried to login to every system using the guest. If the connections were being logged we'd quickly be able to determine from where, and then block that address from the firewall. Audit strongly recommends hiring additional System

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Administrators to compare the current in-house scripts with some of the publicly available log-checking packages such as swatch or logcheck. After the review is complete, determine which one best fits GIAC Enterprise's security objectives. GIAC Enterprises may be surprised by the functionality provided by some of these tools.

As an additional point, it is extremely important to note that since CRONLOG was not set to YES, no one was monitoring root's crontab to see if the scripts were even running. If CRONLOG had been enabled, the Auditor would have expected at least one script to monitor root's crontab to ensure the other scripts were running without errors or worse yet, failures.

CENTRAL LOG HOST

Knowing that, one of the first actions an intruder will take upon successfully breaking into a system is to erase the logs, to remove all traces of the attack and the intruder's actions. GIAC Enterprises prevents this by having the syslog daemon log additional copies of system log entries to another host on the network. GIAC Enterprises has taken steps to make the Log Host as secure as possible (minimum Solaris OS configuration, only required services running, limited login accounts, etc.). Although additional steps from this Audit can be taken on the Log Host, GIAC Enterprises has done a good job in securing it. At a minimum, the Auditor recommends the Log Server log all requested connections to services being started out of the /etc/inetd.conf file by adding the -t option to the startup of inetd in /etc/rc2.d/S72inetsvc.

In the event of a log anomaly, there is now a tamper-proof copy of system logs, which will aid systems administrators in identifying the intruder and cleaning up the system.
As implied above, GIAC Enterprises has setup their log configuration such that there is a centralized location for all the logs. Steps have been documented and taken to ensure the necessary storage space and cpu cycles are available on each system managing logs and then of course.

The Backup Team is responsible for backing up the Log Host and storing the archives securely off-site.

LOGIN ATTEMPTS

GIAC Enterprises is currently setup to detect attacks such as root login attempts. The Auditor verified this was enabled via the SYSLOG option in the login configuration file **/etc/default/login** by setting the SYSLOG=YES entry.

FAILED LOGINS

GIAC Enterprises logs attempts after 5 failed logins to **/var/adm/loginlog**. The Auditor verified the file existed, was owned by root, had a mode of 600, and had a group owner of sys.

NOTE: **If "/var/adm/loginlog" does not exist (or gets deleted), logging will not occur**. Add the code below to one of the scripts currently running in root's cron.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
 if [ ! -f /var/adm/loginlog ]; then
    touch /var/adm/loginlog
    chmod 600 /var/adm/loginlog
   chown root /var/adm/loginlog
fi
```

FTP

The ftp daemon supports logging to syslogd via the -l option. The Auditor reviewed both **/etc/inetd.conf and /etc/inet/inetd.conf** and neither one had the -l option on the ftpd command line. Audit recommends that logging be enabled.

SU

Traditionally, su logging defaults to the sulog logfile - /var/adm/sulog. GIAC Enterprises configured the su configuration to log su events to syslogd. Logging of su events using syslogd was enabled via the SYSLOG=YES option in the su configuration file **/etc/default/su**.

CRON

By default, cron logs to the cron history file (**/var/cron/log**). Cron logging was disabled in the cron configuration file (**/etc/default/cron**). The Auditor recommends that cron logging be enabled by setting CRONLOG=YES. In addition, error messages from cron should be sent to syslog by setting the cron.err variable in the syslogd configuration file.

MAIL

sendmail logs to **syslogd** on all platforms, but the default loglevel varies based on vendor implementation. Since the loglevel controls the level and amount of detail logged, GIAC Enterprises had it set to 1 rather than the default of 9 to reduce the abundance of logging. The loglevel was set though the sendmail configuration file (**/etc/mail/sendmail.cf**) OL option. The following line was in the sendmail.cf file:

OL1

CONNECTION LOGGING

UNIX collects connection accounting information for users and terminals in two log files—utmp and wtmp.

- **utmp** contains current information on all logged-in users and terminal devices. The relevant connection information in utmp is appended to wtmp whenever a connection begins or ends.
- **wtmp** records accumulated connection history.

PROCESS ACCOUNTING

The UNIX kernel collects resource usage information for every process. When process accounting is enabled, this information is collected and recorded in a System Administrator-specified file (file argument of the "accton" command).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

In typical usage, accounting information is collected and consolidated into reports that are used for billing. The accounting scripts and programs provided by the vendor are customized to this purpose.

Accounting information is useful for other purposes. It is useful for performance analysis and resource planning. It is also useful in tracking down the specific set of activities that may have been part of a security incident.

Process accounting should be enabled when reasonable (on some high-activity servers, the volume of log activity may make this impractical), and the accounting information backed-up, archived, and cleared on a regular basis.

RECOMMENDED LOG FILE PERMISSIONS AND OWNERSHIPS

Audit recommends the permissions and ownerships listed in the table below as a first attempt. You may want to tighten the permissions if you're able in the GIAC Enterprises Environment. The tighter the permissions, the better prevention you have from the log information being tampered or destroyed. Depending upon business need and/or system restrictions, it would be best to limit read access to log files to those with PowerBroker™ access as appropriate. The group ownership can vary, but it should be a common system group (bin, sys, demon, adm, uucp, …) or a group restricted to authorized GIAC Enterprises personnel.

It is understood that ownerships and permissions of logs are not always well-defined or controllable by the Administrator. Some utilities have special requirements and may force the use of vendor-selected values. Other utilities may not explicitly set permissions or ownerships and default to the context of the process in which the logs are created or updated. For instance, the Solaris "accton" command always give the account file a mode of 644.

File	Backup Freq	Retention on Log Server	Archive Retention	Permissions	Ownership
/var/adm/syslog	daily	15 days	1 month	640	root
/var/adm/pacct	daily	15 days	1 month	644	root
/var/adm/wtmp(x)	daily	15 days	1 month	664	root
/var/adm/utmp(x)	never	NA	NA	644	root
/var/adm/loginlog	daily	15 days	1 month	600	root
/var/cron/log	daily	15 days	1 month	640	root
/var/adm/lastlog	never	NA	NA	644	root

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix A: Security & Controls Audit Guidelines

Scope

Due to the limitations of the client - server environment, special provisions are required to facilitate audits of UNIX and networked devices. These guidelines serve as a reference when meeting with our Customers to setup the audit.

The IS Auditor will have unrestricted access to information, equipment, applications and people in fulfilling its independent role for accessing the system of management controls and the security of the business. These guidelines are documented to facilitate an efficient and effective work/audit environment. Questions that may arise or are not addressed in this document should be elevated for resolution to the IS Audit Manager.

In this document, the term "infrastructure" refers to the UNIX Operating Systems and relevant services such as SQL, Oracle, etc. The term "application" refers to data and applications owned by the Customer.

Objectives

- Allow auditors to independently extract information to the extent possible
- Provide information needed on a timely basis
- Minimize Customer's work in response to ad hoc requests
- Minimize duplicate information requests or collection
- Provide Customer adequate advance notice of information requests to allow scheduling of work

Constraints / Dependencies

- Information provided by the IS Auditor will be based on availability of existing and supported tools, but does not preclude the use of future tools that may be available at the time of an audit.
- A list of the tools used by the IS Auditor will be provided to the Customer.
- Requests for information will be related to the audit and can cover any time period associated with the audit.
- The system specifics must be identified to the IS Auditor before the scanning of networks can begin.

Determining the Information

The assessment of what is material is a matter of professional judgment and includes consideration of the effect on the organization as a whole of errors, omissions, irregularities and illegal acts which may arise as a result of control weaknesses in the area being audited.

In assessing materiality, the IS Auditor will consider:

- The aggregate level of error acceptable to management, the IS Auditor and appropriate regulatory agencies

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- The potential for the cumulative effect of small errors or weaknesses to become material

In planning sufficient audit work to meet the specified audit objectives, the IS Auditor will identify the relevant control objectives and determine, based on materiality, which controls will be examined. Where the IS audit objective relates to systems or operations that process financial transactions, the value of the assets controlled by the system(s) or the value of transactions processed per day/week/month/year should be considered in assessing materiality.

Where financial transactions are not processed, the following are examples of measures, which should be considered to assess materiality:

- Criticality of the business processes supported by the system or operation
- Cost of the system or operation (hardware, software, staff, third-party services, overheads, or a combination of these)
- Potential cost of errors (possibly in terms of lost sales, warranty claims, irrecoverable development costs, cost of publicity required for warnings, rectification costs, health and safety costs, unnecessarily high costs of production, high wastage, etc.)
- Number of accesses / transactions / inquiries processed per period
- Nature, timing and extent of reports prepared and files maintained
- Nature and quantities of materials handled (e.g., where inventory movements are recorded without values)
- Service level agreement requirements and cost of potential penalties
- Penalties for failure to comply with legal and contractual requirements
- Penalties for failure to comply with public health and safety requirements

Technical Audit Material

Once the IS Auditor has determined, what the audit objectives are, this table lists the type of information you would gather to evaluate the security of an individual UNIX machine.

Information Needed

- Listing of all Ids and associated information (e.g., uids, gids, Name, Account Activation Information, etc.
- Group Information (/etc/groups)
- File ACLs - OS and support areas, not application data
- File ACLs – application / client data
- Account policy settings
- OS Configuration Files
- Services – Inetd, services
- Services (e.g., SQL, Oracle, FTP) configuration files and permissions
- Service Ids for each service
- Network and server configurations (Logical domain and physical)
- Trust Relationships
- Logs -- all OS logs - syslog, PowerBroker™, etc.)
- UNIX Patches
- Backup Inventories
- Hardware Inventory
- Software Inventory

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Customer Policy / Procedures Needed for Audit

To ensure the Customer's Security & Controls Strategies are implemented with good business practices, the following Customer Information (Documentation) is requested:

- Security Policies
  - Application
  - Operating System
  - Network Security
  - Data Access
- Security Risk Assessment
- Security Awareness -- new employee orientation, employee notification of viruses, social engineering awareness, etc.
- Software Acquisition Methodology
- Software Installation Methodology
- Contract Auditing and Negotiation
- Computer Security Incident Handling Process
- Preemptive Security
- Legal Rights and Ownerships for all data accessible on the network or on backups.
- Data Retention Policies
- Backup & Disaster Recovery
- E-Commerce Insurance Policies [8]

  Doing business over the Internet creates an entirely new set of risks that most basic business insurance policies will not cover. As listed in the reference, Cyber Insurance can be obtained for a variety of threats.

© SANS Institute 2000 - 2002, Author retains full rights.

[8] darwin – January 2001, Prepare for the Worst by Daintry Duffy; www.darwinmag.com

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Cyber Insurance Checklist

Coverage amount :	Up to $5M	Up to $10M	Up to $25M	Up to $100M	Up to $200M
Security audit required	*	*	*	*	*
Provides coverage for:					
– Internal violations		✓	✓	✓	✓
– Crackers and viruses		✓	✓	✓	✓
– Media liability	✓	✓	✓	✓	✓
– Privacy violations	✓	✓	✓	✓	✓
– Cyberextortion		✓	✓	✓	✓
– Crisis management	✓	✓	✓	✓	✓
– Global risks		✓	✓	✓	✓

* - Depends on the policy selected with the Insurer.
This sample data came from policies given by Insurers American International Group (www.aig.com), Chubb (www.chubb.com), InsureTrust.com (www.isuretrust.com), Lloyds (www.lloyds.com), Marsh (www.netsecuresite.com), and The St. Paul Companies (www.stpaul.com)

Approach

- The IS Auditor will install the specified tools on specified servers.
- The IS Auditor may need to have the router filters temporarily modified to allow running the network scans from a single IP Address within the Customer's domain. The IS Auditor and the Customer Contact will work together to identify any changes needed temporarily.
- The IS Auditor will generally communicate the intent to use scanning tools in our Audit Engagement letters, however, the Customer should assume that scanning tools will be used in all infrastructure audits.
- During the Audit Scope Phase, the IS Auditor will identify the potential scanning targets (servers, network components, desktops, etc.) and communicate these to our Customer designated Audit Contact as far in advance as possible to give the operation staff adequate time to schedule audit related work.
- When possible, the IS Auditor, will run scans during the Audit Scope Phase; e.g., 2-4 weeks prior to the start of actual fieldwork.
- The IS Auditor will provide the Customer with a list of the vulnerability tests that will be included in the scans. Denial-of-service and password cracking tests will not be performed without explicit agreement from the Customer. Where possible, the scans will be configured to exclude vulnerability tests that are not applicable to the Customer's environment.
- The IS Auditor will connect to the client's internal network and attempt to compromise the servers, workstations, and other devices. The Audit team will practice safe computing to ensure that viruses are not planted into the client network and to ensure that machines are not permanently damaged. Using compromised accounts or, if we are unable to gain access to the internal network, a normal account provided by the Customer, we will attempt to gain administrative access to servers, network equipment and other machines in the network. We will identify the damage that can be done

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

(place files, harvest files, etc.) if administrative or root access is achieved on any of these machines.

REPORTING

In determining the findings, conclusions and recommendations to be reported, the IS Auditor will consider both the substantiality of any errors found and the potential reality of errors which could arise as a result of the control weaknesses.

A control weakness should be considered material, and therefore reportable, if the absence of the control results in failure to provide reasonable assurance that the control objective will be met. If the audit work identifies material control weaknesses, the IS Auditor should consider issuing a qualified or adverse opinion on the audit objective.

Depending on the objectives of the audit, the IS Auditor should consider reporting to management weaknesses which are not material, particularly when the costs of strengthening the controls are low.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix B: Printer Vulnerabilities

Overview

The information in this appendix has been collected while using Internet Security Systems, Inc. iss product. Although the printers vary in make, model, size and usage; typically taking a printer out of the box and installing it onto a Production Network is not a good idea. Printers are getting smarter, which means they are (becoming) another device on your network that can be used to exploit well-known vulnerabilities.

With that said, not scanning the printers is a big mistake. Not addressing your network printer vulnerabilities is a bigger mistake. As with all vulnerabilities, printer vulnerability fixes have different levels of difficulty. Some are difficult to correct and require contacting the Printer Manufacturer or software driver vendor to correct. With this in mind, a good approach is to prioritize the printers into categories of importance. The printers that are used for printing confidential or proprietary information should be near the top of the list. Others, which print less sensitive information, are lower on the list.

How to correct a printer vulnerability

Generally the steps taken to correct vulnerability are:

1) Reproduce the problem manually.
2) Attempt to fix the vulnerability
3) Test. Again, check for the vulnerability manually and then with a Vulnerability Scanning Tool such as Internet Scanner (iss).

For printers at step 2, the following steps apply:

a) Change printer configuration. If for example a default password is found, then change the password. (*Note* this may also require changing all clients of the printer to use this password which may not be reasonable.) If ftp has no password, assign a password. Etc.
b) Contact the hardware/software vendor to see if there is a patch to the software. It maybe possible to change the version of the service daemon or driver on the printer to a public or patched version that does not have the vulnerability.
c) Contact the hardware vendor to get an upgrade to the hardware to solve the vulnerability.
d) Disable unnecessary services (telnet, http, ftp, etc.)
e) Replace with a more secure printer or remove the printer from network.

How a printer is connected to the network

There are generally three ways a printer is connected to the network.

1) Connected to a local host machine that is acting as the gateway to the printer. This host controls access to the printer and changing the access privileges at this machine can stop some unauthorized access.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2) Direct connection to the network. The hardware / software inside the printer is acting as the gateway to the printer. Here the hardware / software in the printer must be changed to control access.
3) Connected to a remote host machine within a dedicated printer domain. The domain controller is assigned the task of controlling access to the printer and all printing goes through the domain controller and then re-routed to the actual printer.

How a printer is accessed

Generally, a printer is controlled directly through an operating system service or daemon. When the service or daemon is running, it should have exclusive access to the printer. Some printers could provide other ways to access a print queue or printer configuration data.

For example, it is possible that some printers provide an FTP site where a client can upload a file to the printers print queue. (This method is not common.) It is most likely used for software that does not want to talk directly to the printer. The software could be a CAD or drawing tool or some shell script code that sends print files to a FTP print queue. Usually the FTP site is open to everyone so as to ease access to the print queue. It is easy for a cracker to gain access to the FTP site and get, view or update files in the print queue.

It is possible that some printers provide a telnet service (or SNMP or HTTP service) for access to the printer's configuration data. This is reasonable for printers that are connected directly to the network since they have no host machine with a monitor and keyboard. Again, it is easy for a cracker to gain access to the telnet site and view or update configuration data for the printer. He may or may not be able to view or update the files in the print queue.

Microsoft Windows clients use an operating system service to access the printer queue and communicate directly to the hardware / software on the printer. Windows clients can communicate to a printer using any of the above printer network connection methods, but this one is probably the most secure.

If the printer is used in a Unix environment, then these clients usually communicate with a local "lpd" daemon that in turn communicates with a "lpd" daemon on the remote printer or host machine. This daemon has control of the printer and should control most of the access to the printer.

Printer Vulnerabilities

Once a cracker has gained root or system privileges to a system (printer), he can do almost anything he wants to the system including:

- Retrieve information
- Destroy information
- Control the system
- Alter information
- Shut down the system

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

A cracker with a sniffer could capture network traffic and reconstruct a file that is being printed. Generally, a cracker would have to be on the same physical network segment as the printer to be able to capture a file. The cracker might have to decrypt the packets if the printer services are using some form of encrypted communication. In the opinion of the author, this scenario is not very likely and if it happened, it would usually be performed from inside the company.

The vulnerabilities listed below relate directly to Printer Vulnerabilities. The information regarding the Vulnerability was extracted from the Internet Scanner Policy Editor under the vulnerability help page and the WEB references. Some fixes require the setting of a not easily guessable password (e.g., CHANGE all DEFAULT PASSWORDS!!). For these, it's recommended a password of at least 7 characters with at least one character that is numeric and at least one special character (i.e., not alphanumeric).

FTP CWD ~root login

Very old versions of the FTP daemon contained a bug that allowed a malicious user to issue a "CWD ~root" command that would result in the attacker gaining root privileges on the system (printer). This is an old bug (1988) in the FTP package.
To fix, check with the Printer Manufacturer to get an upgrade of the printer software (specifically the FTP service). You may be able to use a public domain available FTP service in place of the one the Printer Manufacturer used; however, it cannot be determined if this is practical or reasonable. Check the Printer Documentation or Manufacturer for details**. If the FTP service is not required, disable the service.** This may affect some clients who will have to be reconfigured to use a different method to print.

FTP daemon with no password

The File Transfer Protocol (FTP) daemon ftpd allowed a login using a nonsensical username and password. An FTP daemon that does not require a username and password may allow attackers access to unauthorized areas of the computer.
This vulnerability is serious; it could allow anyone to gain root privileges to the system (printer). **This is a configuration issue.**
To fix, change the password to something that is not easy to guess. If clients depend on the password being well known, then see if the clients can be configured to use a different FTP password or a different print method.

SNMP_Set used Public Community Name to Change System Information

The SNMP default Public community name is specified, allowing anyone the ability to change the machine's system information if they use this default value. An attacker can use SNMP to obtain valuable information about the machine, such as information on network devices and current open connections. **This is a configuration issue**.
To fix, change the password to something that is not easy to guess. If clients depend on the password being well known, then see if the clients can be configured to use a

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

different SNMP password. **If the SNMP service is not required, disable the service**.

Telnet Available with No Login

Users can Telnet to this printer without a login. An attacker can access sensitive information through default accounts or easily guessed passwords. This vulnerability is serious and could allow anyone to gain valuable information about the system (printer). **This is a configuration issue.**

To fix, change the password to something that is not easy to guess. A guess as to the use of the Telnet service is to provide remote access to printer configuration data (or maybe to the print queue). Check the Printer Documentation to see what commands or options are provided via telnet. A standard telnet service can enforce a password login. **If the Telnet service is not required, disable the service.**

ColdFusion web administration feature can be used by anyone to stop the CFserv~

The ColdFusion Administrator includes a utility for starting and stopping the ColdFusion service from a web browser. A problem exists in this feature when Advanced Security is enabled, which allows any remote user to stop the ColdFusion server.

This vulnerability could be a false positive, unless the printer has an HTTP service that could be vulnerable. Check this out manually. Try to access the printer through your WEB browser. See what services are available to you. Check the Printer Documentation to determine the use of this service. Can you post information to the printer? Perhaps access to configuration data**. If the HTTP service is not required, disable the service.** If there is no HTTP service running then consider it a False Positive after reviewing the Printer Documentation.

Echo service

The echo service was detected as running. The echo (port 7) service can be spoofed into sending data from one service on one machine to another service on another machine. This action causes an infinite loop and creates a denial of service attack. The attack can consume increasing amounts of network bandwidth, causing loss of performance or a total shutdown of the affected network segments**. This is a configuration issue.**

Check the Printer Documentation or contact the Printer Manufacturer to determine the use of this service**. If the Echo service is not required, disable the service.**

FTP bounce attack could allow attackers to 'proxy' connections

A vulnerability exists in many FTP implementations regarding the use of the PORT command. An attacker could potentially use this command to connect to sites through the vulnerable host, effectively "bouncing" such connections allowing anyone to hide the origin of an attack using the system (printer). **This is a bug in the FTP package**. To fix, see "FTP CWD ~root login" above.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

FTP directories writeable

Writeable FTP directories were detected. These directories can be used as drop points for unauthorized or illegal material. An attacker can write files, such as .rhosts, that could provide access to the machine. It is also possible to inflict a denial of service attack by filling up the hard disk. **This is a bug in the FTP package**. To fix, see "FTP CWD ~root login" above.

TCP sequence prediction

The TCP sequence was found to be predictable. When the TCP sequence is predictable, an attacker can send packets that are forged to appear to come from trusted machines. These forged packets can compromise services, such as rsh and rlogin, because their authentication is based on IP addresses. Attackers can also perform session hijacking to gain access to unauthorized information. This vulnerability could allow a cracker to gain access to a system by creating packets that look like they came from an authenticated source. In theory, a cracker could change the contents of a printout as it is being sent to the printer since they are already creating their own packets. They may also be able to read the printer queue or configuration data. This type of attack is not simple.

This is a bug in the printer host operating system or possibly the printer operating system. Try to upgrade the printer driver software. It is difficult to eliminate the sequence prediction completely, so if you must use the device, always try to keep the drivers as up to date as possible. Report the problem to the printer vendor; they may not have heard of this problem before.

Anonymous FTP enabled

Anonymous FTP is enabled. If FTP services are present, allowing only anonymous access prevents valid user-password pairs from being passed across the network. Thus this vulnerability could allow anyone to gain information about the system (printer) if the Anonymous FTP is not setup correctly. This is a configuration issue. To fix, see the steps below. The fix involves removing all login accounts, except for the root and anonymous accounts. Check the Printer Documentation or Printer Manufacturer to see if the changes listed below are possible. **If the FTP service is not required, disable the service**.

Proper configuration of the FTP server is critical. If an anonymous login is permitted, be certain to:

- Create the correct home directories for exclusive use of ftpd, such as ~ftp/bin, ~ftp/etc, and ~ftp/pub.
- Place only actual files (rather than symbolic links) in the ftp home directories.
- Create a special ftp account that points to the ftp home directory.
- Alter the ftp passwd file to contain entries only for root and ftp.
- Alter the group file to contain only the ftp group.
- Use chown to apply the appropriate owners to the directories.
- Use chmod to apply the correct permissions to all directories and files.
- Secure any open repository directories so they cannot be used as drop points.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

FTP Home Directory Bug

The FTP daemon revealed the true path to the FTP user's home directory by issuing a quote CWD command. This information-gathering probe may give an attacker clues as to the basic structure of the victim's file system. Many modern FTP server packages have removed this flaw, but some (like wu-ftp) are still vulnerable. This is a configuration issue.

To fix, try to disable the CWD command for the FTP service. Check the Printer Documentation or Printer Manufacturer to see if this is possible. If the FTP service is not required, disable the service.

SNMP Agents Reveal Information About Network Interfaces

All SNMP agents support the standard MIB-II Table. This table contains the IP address and network mask of each interface that the machine supports. This information may be used to learn more about the connections to and from the networked device. **This is a configuration issue.**

To fix, set the SNMP community string to a value that is not easily guessed. Use uppercase, lowercase, numeric characters and special characters. If the agent supports View Access Control, limit the views that the agent may reveal. You may have to configure the SNMP manager software to use this new community string if you use the SNMP service for managing network devices. Check the Printer Documentation or Printer Manufacturer to see if it is possible to change the community string. This is not a very serious risk so this should be low on the priority list**. If the SNMP service is not required, disable the service**.

SNMP can reveal possibly sensitive information about hosts

The SNMP service was detected as running. An attacker can use SNMP (Simple Network Management Protocol) to gain valuable information about the machine (such as information on network devices, current open connections, etc.) when SNMP uses default words, such as public or private, for the community word. If no community is specified, then the SNMP server responds to queries from any machine. **This is a configuration issue**.

To fix, see "SNMP agents reveal information about network interfaces" above.

SNMP_Get able to retrieve any Community Name

No SNMP community name is specified, allowing anyone the ability to receive responses to queries from a system. An attacker can use SNMP to obtain valuable information about a system, such as information on network devices and current open connections. **This is a configuration issue.**

To fix, "SNMP agents reveal information about network interfaces" above.

SNMP_Get able to retrieve Public Community Name

The SNMP default Public community name is specified, allowing anyone the ability to receive responses to queries from the system if they use this default value. An attacker

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

can use SNMP to obtain valuable information about the machine, such as information on network devices and current open connections. **This is a configuration issue**. To fix, see ""SNMP agents reveal information about network interfaces" above.

Example

As an example that these vulnerabilities are out there, here is a discussion found on: http://archives.neohapsis.com/archives/bugtraq/2000-04/0209.html

> Subject: Re: DOS attack against HP JetDirect Printers
> From: Ben Greenbaum (bgreenbaum@SECURITYFOCUS.COM)
> Date: Mon Apr 24 2000 - 16:15:13 CDT
>
> This may be related to a previously-known issue regarding multiple connections. Try a 'nmap -sT -PT -M 1' and see what happens. The scan should be the same as previous but limit concurrent connections to one. According to the nmap docs I've got the default is 50.
>
> From an ISS advisory (Dec 10, 1998)
> http://www.securityfocus.com/advisories/526
> ----
> Syn "Dripping":
> Even though the JetDirect cards are not subject to syn flooding per se, due to the single threaded TCP/IP stack, even a single SYN packet can lock up the older interface for a significant period of time (tens of seconds to as much as a minute). Thus the printer can be subjected to a denial of service attack by slowly dripping SYN packets with non-responding "from" addresses directed to the older JetDirect interface. If this is directed at more than one of the JetDirect ports, the interface may lock up, as in the repeated rapid port scanning DoS described below. This problem was uncovered at Internet Security Systems during the analysis of other JetDirect problems. Newer multi-threaded versions of the JetDirect interfaces are not vulnerable to this problem.
>
> Repeated rapid port scanning:
> Some scanning tools use parallel port scanning to improve scanning speed. Parallel scanning of multiple ports on the older JetDirect cards has a high probability of causing a complete lockup of the JetDirect network interface. The fact that the DoS is not deterministic, and the failure rate is highly dependent on the timing and speed of the scan, indicates that this is a timing window or race condition in the TCP/IP stack on the older JetDirect.
> ----
> Ben Greenbaum
> Director of Site Content
> Security Focus
> http://www.securityfocus.com

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix C: World Writeable Files Exceptions

Casper Dik's exceptions.h file represents the list of acceptable world writeable files.

```
$Id: exceptions.h,v 1.9 1998/10/01 11:05:04 casper Exp $

/* List of files/directories supposed to be group/world writeable
May need to be updated for each OS release */

/etc/dumpdates
/etc/lp
/var/mail/:saved
/var/preserve

/* Lp stuff is chmod'ed back by the lp system; prevent pkgchk errors
later by listing them here. */
/etc/lp/Systems
/etc/lp/classes
/etc/lp/forms
/etc/lp/interfaces
/etc/lp/printers
/etc/lp/pwheels
/var/lp
/var/lp/logs
/var/spool/lp
/var/spool/lp/admins
/var/spool/lp/fifos
/var/spool/lp/fifos/private
/var/spool/lp/fifos/public
/var/spool/lp/requests
/var/spool/lp/system

/* another strange logfile */
/usr/oasys/tmp/TERRLOG

/* /var/adm stuff added because std cron jobs for sys/adm expect this */
/var/adm
/var/adm/acct
/var/adm/acct/fiscal
/var/adm/acct/nite
/var/adm/acct/sum
/var/adm/sa
/var/adm/spellhist

/* 5.1, 5.2 */
/devices/pseudo/clone:ip
/devices/pseudo/clone:ticlts
/devices/pseudo/clone:ticots
/devices/pseudo/clone:ticotsord
/devices/pseudo/clone:udp
/devices/pseudo/cn:console
/devices/pseudo/cn:syscon
/devices/pseudo/cn:systty
/devices/pseudo/log:conslog
/devices/pseudo/mm:null
/devices/pseudo/mm:zero
/devices/pseudo/sad:user
/devices/pseudo/sy:tty
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
/* 5.3 5.4 5.5 ... */
/devices/pseudo/clone@0:ip
/devices/pseudo/clone@0:ticlts
/devices/pseudo/clone@0:ticots
/devices/pseudo/clone@0:ticotsord
/devices/pseudo/clone@0:udp
/devices/pseudo/clone@0:tcp
/devices/pseudo/clone@0:rts
/devices/pseudo/cn@0:console
/devices/pseudo/cn@0:syscon
/devices/pseudo/cn@0:systty
/devices/pseudo/ksyms@0:ksyms
/devices/pseudo/log@0:conslog
/devices/pseudo/mm@0:null
/devices/pseudo/mm@0:zero
/devices/pseudo/sad@0:user
/devices/pseudo/sy@0:tty

/* 5.6 .... */
/devices/pseudo/tl@0:ticlts
/devices/pseudo/tl@0:ticots
/devices/pseudo/tl@0:ticotsord

/* Starfire console */
/devices/pseudo/cvc@0:cvc
/devices/pseudo/cvcredir@0:cvcredir
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix D: Additional Audit File Recommendations

The listing below represents additional findings and the Auditor's expectations for System Files on the GIAC Enterprises server001:

```
Permissions (-rw-r--r--) incorrect for /.rhosts,                    expected (-rw-------).
Permissions (-rw-r--r--) incorrect for /.new,                       expected (-rw-------).
Permissions (-rw-r--r--) incorrect for /.login,                     expected (-rw-------).
Permissions (-rw-r--r--) incorrect for /.kshrc,                     expected (-rw-------).
Permissions (-rwxr-xr-x) incorrect for /.dtprofile,                 expected (-rw-------).
Permissions (-rw-r--r--) incorrect for /.cshrc,                     expected (-rw-------).
Permissions (drwxr-xr-x) incorrect for /.dt/.,                      expected (drwx------).
Permissions (-r-x------) incorrect for /var/yp/updaters,            expected (-rw-r--r--).
Permissions (drwxrwxr-x) incorrect for /etc/rcS.d/.,                expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /etc/rc3.d/.,                expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /etc/rc2.d/.,                expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /etc/rc1.d/.,                expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /etc/rc0.d/.,                expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /etc/init.d/.,               expected (drwxr-xr-x).
Permissions (-r-xr-xr-x) incorrect for /usr/sbin/snoop,             expected (----------).
Owner (bin) incorrect for /usr/sbin/snoop,                          expected (root).
Permissions (-rwxrwxr-x) incorrect for /usr/openwin/bin/ttsnoop,    expected (----------).
Permissions (drwxrwxr-x) incorrect for /var/adm/.,                  expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /usr/sbin/.,                 expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /usr/bin/.,                  expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /usr/.,                      expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /sbin/.,                     expected (drwxr-xr-x).
Permissions (-rwxrw-r--) incorrect for /etc/opasswd,                expected (-rw-------).
Permissions (drwxrwxr-x) incorrect for /usr/share/lib/terminfo/.,   expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /usr/share/lib/sgml/.,       expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /usr/lib/snmp/.,             expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /usr/lib/dmi/.,              expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /usr/lib/acct/.,             expected (drwxr-xr-x).
Permissions (-rw-rw-rw-) incorrect for /var/snmp/snmpdx.st,         expected (-rw-rw-r--).
Permissions (-rw-rw-rw-) incorrect for /var/saf/_log,               expected (-rw-rw-r--).
Permissions (drwxrwxrwx) incorrect for /var/spool/pkg/.,            expected (drwxr-xr-x).
Permissions (drwxrwxrwx) incorrect for /var/preserve/.,             expected (drwxr-xr-x).
Permissions (-rw-rw-rw-) incorrect for /var/sadm/install/.pkg.lock, expected (-rw-rw-r--).
Permissions (drwxrwxr-x) incorrect for /var/news/.,                 expected (drwxr-xr-x).
Permissions (-rw-rw-rw-) incorrect for /var/adm/spellhist,          expected (-rw-rw-r--).
Permissions (-rw-rw-rw-) incorrect for /var/adm/vold.log,           expected (-rw-rw-r--).
Permissions (drwxrwxr-x) incorrect for /var/.,                      expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /usr/old/.,                  expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /usr/net/.,                  expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /usr/kvm/.,                  expected (drwxr-xr-x).
Owner (bin) incorrect for /usr/kvm/.,                               expected (root).
Permissions (drwxrwxr-x) incorrect for /usr/games/.,                expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /usr/demo/.,                 expected (drwxr-xr-x).
Permissions (-rw-r--r--) incorrect for /etc/remote,                 expected (-rw-r-----).
Permissions (drwxrwxr-x) incorrect for /usr/ucb/.,                  expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /usr/lib/.,                  expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /usr/include/.,              expected (drwxr-xr-x).
Group (other) incorrect for /etc/vfstab,                            expected (sys).
Owner (root) incorrect for /etc/mail/.,                             expected (bin).
Permissions (drwxrwxr-x) incorrect for /etc/lib/.,                  expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /etc/fs/.,                   expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /etc/dfs/.,                  expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /etc/default/.,              expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /opt/.,                      expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /devices/.,                  expected (drwxr-xr-x).
Permissions (drwxrwxr-x) incorrect for /dev/.,                      expected (drwxr-xr-x).
Group (other) incorrect for /var/log/syslog,                        expected (sys).
Permissions (drwxr-xr-x) incorrect for /var/log/.,                  expected (drwxr-x---).
Permissions (drwxrwxrwx) incorrect for /var/adm/log/.,              expected (drwxrwxr-x).
Group (staff) incorrect for /var/adm/log/.,                         expected (adm).
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix E: Scripts used within the Audit

```
#/bin/sh
# ip_chks
# These checks were extracted from the checking portion of the
# disable_ip_holes.sh script in the TITAN project

SOURCE=` /usr/sbin/ndd /dev/ip ip_forward_src_routed`
echo "IP source routing is currently set to $SOURCE"
if [ $SOURCE != 0 ] ; then
   echo "   System allows source routed packet forwarding - FAILS CHECK\n\n"
else
   echo "   System set to not forward source routed packets - PASSES CHECK\n\n"
fi

FORWARD=` /usr/sbin/ndd /dev/ip ip_forwarding`
echo "IP forwarding is currently set to $FORWARD"
if [ $FORWARD != 0 ] ; then
  echo "   System forwards IP packets - FAILS CHECK\n\n"
else
  echo "   System does not Forward IP packets - PASSES CHECK\n\n"
fi

FORWARD2=` /usr/sbin/ndd /dev/ip ip_forward_directed_broadcasts`
echo "IP forwarding directed broadcast is currently set to $FORWARD2"
if [ $FORWARD2 != 0 ] ; then
  echo "   System allows forwarding of directed broadcasts - FAILS CHECK\n\n"
else
  echo "   System does not forward directed broadcast packets - PASSES CHECK\n\n"
fi

BROADCAST=` /usr/sbin/ndd /dev/ip ip_respond_to_echo_broadcast`
echo "IP respond to echo broadcast packets set to $BROADCAST"
if [ $BROADCAST != 0 ] ; then
  echo "   System allows response to echo broadcasts - FAILS CHECK\n\n"
else
  echo "   System does not respond to echo broadcast packets - PASSES CHECK\n\n"
fi

IGNORE=` /usr/sbin/ndd /dev/ip ip_ignore_redirect`
echo "IP ignore redirect is currently set to $IGNORE"
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
if [ $IGNORE != 1 ] ; then
  echo "   System is not set to ignore redirected packets - FAILS CHECK\n\n"
else
  echo "   System is set to ignore redirected packets - PASSES CHECK\n\n"
fi

STRICT=` /usr/sbin/ndd  /dev/ip ip_strict_dst_multihoming`
  echo " IP strict multihoming is currently set to $STRICT"
if [ $STRICT != 1 ] ; then
echo "   System is not set to do strict destination multihoming - FAILS CHECK\n\n"
else
  echo "   System is set to do strict multihoming  - PASSES CHECK\n\n"
fi

if [ -f /etc/notrouter ]; then
  echo "/etc/notrouter exists."
  echo "         System configured as 'notrouter' - PASSES CHECK \n"
else
 echo "    Need to create /etc/notrouter to disable Routing "
fi

if [ -f /etc/rc2.d/S??inet -o /etc/rc3.d/S??inet ]; then
   for FILE in `ls /etc/rc*.d/S??inet`
      do
       egrep '(src_routed 0|ignore_redirect 1|broadcasts 0|multihoming 1)' $FILE >/dev/null 2>&-
          if [ $? -eq 0 ]; then
              echo "Settings look okay - PASSES CHECK \n"
          else
              echo "IP Settings are incorrect in $FILE -- please check.\n"
          fi
      done
else
  echo "No inet startup file found - ERROR\n "
fi
                                    ******************************
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
#!/bin/sh
################################################
#   run as root, check_path will check root's path for .
#
echo "TEST: Checking root's path for a dot (.)"
grep -i -s "path[^\.]*\." .login
if [ $? -eq 0 ]; then
        echo    "  .login contains a dot (.) in root's path."
else
        echo "   .login path is correct"
fi

grep -i -s "path[^\.]*\." /.cshrc
if [ $? -eq 0 ]; then
        echo "  .cshrc contains a dot (.) in root's path."
else
        echo  "  .cshrc path is correct"
fi

grep -i -s "path[^\.]*\." /profile
if [ $? -eq 0 ]; then
        echo "  profile contains a dot (.) in root's path."
else
        echo "   profile path is correct"
fi
echo " ------------ END OF TEST -------------------\n\n"
```

****

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
#!/bin/sh
# check_rhosts - Search for .rhosts files in user home directories

for user in `cat /etc/passwd | awk -F: 'length($6) > 0 { print $6 }' | sort -u`
do
  if [ -f $user/.rhosts ]; then
    echo "$user/.rhosts should be deleted."
  else
    echo "$user has no .rhosts."
  fi
done
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix F: Internet Scanner Vulnerabilities

This table lists additional vulnerabilities that can be detected on Solaris 2.6. This is by no means an exhaustive list, but you can see that the Solaris arp buffer overflow vulnerability was detected only one month prior to this report being written. The point? That vulnerability detection tools require constant updating, so if you scan periodically, you should always check for updates prior to beginning the scan.

Vulnerability	Systems	Date	Brief Description
ksh-redirection-symlink	Digital Unix (5.0) HPUX (9.0) IRIX (6.2) IRIX (6.5.x) Solaris (2.5.1) Solaris (2.6) Solaris (7)	Dec 2000	ksh redirection symlink attack
solaris-ffcore-modify-files	Solaris (2.5.1) Solaris (2.6) Solaris (7) Solaris (8)	Oct 1999	Solaris ff.core could allow local users to modify files
solaris-arp-bo	Solaris (2.4) Solaris (2.5) Solaris (2.5.1) Solaris (2.6) Solaris (7)	Jan 2001	Solaris arp buffer overflow
mantrap-identify-processes	ManTrap (1.6.1) Solaris	Jan 2001	ManTrap could allow attackers to identify real processes
mailx-lockfile-dos	Solaris (2.6) Solaris (7) Solaris (8)	Jan 2001	mailx lockfiles denial of service
solaris-exrecover-bo	Solaris (2.4) Solaris (2.5) Solaris (2.5.1) Solaris (2.6)	Jan 2001	Solaris exrecover buffer overflow
mantrap-pwd-reveal-information	ManTrap (1.6.1) Solaris	Jan 2001	ManTrap pwd command causes error revealing information

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Internet Scanner 5.3 for Unix Checks

This listing represents a good majority of the tests that can be done by ISS. The complete listing was not provided because the current version of the tool is up to 6.1

Critical Files Obtainable

- Files obtained tftp
- Files obtained via NIS
- Files obtained via ftp
- Files obtained via rexec
- Files obtained via rlogin
- Files obtained via rsh
- Files obtained via telnet
- Trusted host(s) found

DNS Checks

- Bind Version Check
- DNS -DALLOW_UPDATES
- DNS Bad Sequence Check
- DNS Service Reverse Lookup
- DNS honors zone transfer requests.
- DNS server supports inverse queries.

Denial Of Service Checks

- Data Flood
- Fingerd honors
- Land denial of service attack.
- NT DNS Denial-of-Service Attack
- Open/Close Connection Flood
- Ping packets of size 65k can be sent to machines and crash/reboot system.
- RWHO Daemon Overflow
- Rwho Daemon Overflow
- SMB Netbios Test: Possible NT dot..dot denial of service
- SYN flood DoS attack ties up network resources
- Syslog Flood
- Teardrop IP Fragmentation Overlap Check
- This exploit can be used to crash a Microsoft Exchange server (version 4.0 or version 5.0 with no patches applied).
- UDP Packet with Illegal Values Vulnerability
- Vulnerable to out of band DOS attack on port 139

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Email Checks

- Debug vulnerability allows attackers to gain root access.
- Imap2 buffer overflow vulnerability.
- Imap3 buffer overflow vulnerability.
- Imapd core vulnerability
- Open Defaults Found Through POP3
- Open Defaults Found Through POP3
- Pop2 buffer overflow vulnerability.
- Pop3 buffer overflow vulnerability.
- Possibly vulnerable SMTP host
- Qmail Length Denial of Service Attack
- Qmail RCPT Denial of Service Attack
- Remote Execution Hole through Syslog Buffer Overflow
- SMTP EXPN command
- SMTP daemons which support EHLO will give out useful information to attackers.
- Sendmail %style relaying.
- Sendmail WIZ attack allows intruders to gain root access.
- Sendmail daemon outdated
- Sendmail decode / uudecode vulnerability
- Sendmail remote execution.
- User forward file found.
- Verify Account Information About Users with Sendmail

FTP Checks

- Anonymous FTP enabled.
- Check for ftp daemon with no password
- FTP Bounce Attack
- FTP CWD buffer overflow
- FTP CWD ~root login
- FTP Getcwd() file descriptor leak
- FTP Proxy Penetrated
- FTP rnfr
- FTP site exec vulnerable.
- Ftp Home Directory Bug
- Ftp daemon with no password
- Ftp directories group writeable
- Ftp directories user writeable

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Ftp directories world writeable
- Ftp directories writeable by anonymous users
- Ftpd args core dump allows users to obtain accounts and encrypted passwords.
- Open Defaults Found Through FTP
- Open Defaults Found Through FTP
- Open Defaults Found Through FTP
- PASV Denial of Service
- WarFTPD Buffer Overflow Vulnerability
- Writeable ftp directories
- ftpd core dump

Firewall Checks

- Checkpoint Firewall has guessable password
- Checkpoint Firewall has no password
- MS Firewall has guessable password
- MS Firewall has no password
- Misconfigured SOCKS Daemon Permits System Access
- Misconfigured SOCKS v4 Daemon
- Misconfigured SOCKS v5 Daemon
- Raptor firewall has guessable password
- Raptor firewall has no password
- Squid proxy penetration
- Stealth Scan
- TIS Firewall has guessable password
- TIS Firewall has no password

Information Gathering

- Finger Output from Common Names
- ICMP netmask request response.
- ICMP timestamp requests
- Identd advertises users
- Rstat Output
- Rusers Output
- Traceroute
- Whois information

NFS Checks

- Guessable NFS filehandles

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Mountd File-Exist Vulnerability
- Mountd on unreserved port
- NFS .Rhosts
- NFS CD Vulnerability
- NFS Cache Poisoning
- NFS Exports
- NFS Mountable
- NFS Mountable Via Ultrix Remount Bug
- NFS Mounting Of Filesystems Supported
- NFS Service
- NFS UID Vulnerability
- NFS Writable
- NFS exports outside domain
- NFS exports outside domain to everyone
- NFS mknod
- NFS portmapper export
- Superfluous NFS daemon

NIS Checks

- NISd is running over a non-reserved port.
- Rpc.nisd buffer overflow in Solaris 2.5.1
- Ypbind is running over a non-reserved port
- Ypserv on unreserved port

NetBIOS

- SMB Netbios entire drive available
- Writeable NetBIOS Share Found
- Remote file access through selection service.

Network Device Checks

- Ascend Pipeline and MAX denial of service vulnerability
- Cicso IOS Access Control List Vulnerable
- Cisco IOS Access Control List Vulnerable
- Cisco IOS Remote Router Crash
- Cisco Vulnerable to Land Attack
- No Cisco Login Required
- Open Administrative Account Found on Cisco Device
- Open Defaults Found on Cisco Device

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- SNMP_Get Able to Guess Community Name
- Vulnerability in Cisco OS allows unathorized PPP connections.

Password Checks

- Accounts accessible through Rsh
- KerberosIV Brute Force
- Linux '+' root account vulnerability.
- Remote attackers can gain access to a username and information.
- Windows 95 Password Cache Files

Protocol Spoofing Checks

- ICMP Redirect Downed Host
- RIP tables modified
- Rlogin Vulnerable through TCP Seq Prediction Spoofing
- Rsh Vulnerable Through TCP Seq Prediction Spoofing
- Sequence ports are predictible.
- TCP Sequence Prediction

RPC Checks

- 3270 mapper Service
- RPC Database Service
- RPC NIS udpate
- RPC SNMP Service
- RPC Statd file creation and removal vulnerability
- RPC alis Service
- RPC keyserv Service
- RPC llockmgr Service
- RPC nlockmgr Service
- RPC sched Service
- RPC statmon Service
- Sunlink Mapper Service
- pcnfsd contains vulnerabilities that allow users to execute arbitrary commands as root.

Remote Service Checks

- .rhosts Authentication Vulnerability
- Accounts accessible through Rsh
- Admind Tool Is Running
- BackOrifice Default Install Check

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Bootparam Enabled - Allows Getting Domain Name Remotely
- Chargen Service
- DG/UX finger vulnerability
- Domain Names and NIS Server
- Dynamic Linker Telnet Vulnerability
- Echo Service
- Executable Module
- FSP Daemon
- Finger Service
- INN control message allows users to execute arbitrary commands.
- Irix FAM server to list files.
- Linux TFTP Vulnerability
- Linux ugidd Check
- NIS Maps
- NIS Passwd Via TCP
- NIS Passwd Via UDP
- NIS YPBind service is running
- NIS Yellow Pages (YP) service is running
- NNTP Posting
- NNTP Reading
- NetBus Installed
- Netstat Inet Service
- Open Defaults Found Through Rexec
- Open Defaults Found Through Telnet
- Pmap Unset Vulnerability
- Pmapsunset Vulnerable
- Popd/Imapd buffer overflow vulnerability.
- Portd running
- RPC bind service on improper port
- Remote Execution Hole Through Identd
- Rexd Running
- Rlogin -froot Vulnerability
- Routed Append Vulnerability
- Routed Service Active
- Rsh Vulnerable In Hosts.equiv
- Rstatd service
- Rusers Running
- SNMP

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- SNMP Public Information
- Samba buffer overflow
- Sshd 1.2.17 has known problems.
- Sshd advertises info upon connecting with clients.
- Sysstat
- TFTP
- Telnet Available With No Login
- UUCP available
- Vulnerable to Samba .. Bug - NT 3.5
- Vulnerable to Samba .. Bug - NT 3.51
- Wall Daemon Running
- X Check allows keystroke capturing.
- X11R6 MIT Magic cookie prediction
- X25 Daemon Running - Possible Gateway
- Yppasswdd Service
- bootparam gave out domain name
- eterstatd Service
- nsed Service
- nsemntd Service
- rje mapper Service
- rquotad Service
- showfhd Service
- sprayd Service
- stock fingerd running
- tfsd Service
- ypxfrd Service

Web Server Checks

- AnyForm cgi-bin remote execution vulnerability
- Apache cookies buffer overflow vulnerability
- CGI Program Executed an Arbitrary Command
- Campas cgi-bin file read vulnerability
- File listing from test-cgi
- FormMail remote execution vulnerability
- FormMail remote usage vulnerability
- Glimpse HTTP aglimpse remote execution vulnerability
- Guestbook vulnerability
- HTTP (WWW server) port active

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- HTTP (WWW server) port active
- HTTP .. attack allows users to gain access to the server root directory.
- HTTP Basic Authorization Password guessed.
- HTTP Proxy Detected
- HTTP Proxy Penetrated
- HTTP View source vulnerability
- Hole in ASP allows web clients to download ASP files.
- IIS .bat/.cmd bug
- IIS ASP DATA Bug in Windows NT Based Web Servers
- IIS ASP Dot Bug
- Irix cgi-bin handler remote execution vulnerability.
- Novell Convert.bas Web Server Script vulnerability
- Nph-test-cgi file listing vulnerability
- Php remote file read vulnerability
- Potential Glimpse HTTP aglimpse remote execution vulnerability
- SGI Irix cgi-bin wrap directory listing vulnerability
- SGI Webdist Vulnerable
- ScriptAlias Directive Web Server Vulnerability
- Server Could Not Find Some Referenced Local HTML Links
- Server Returned a File Listing For a Directory That Had No Index
- Server indicated presence of potentially exploitable program in /cgi-bin
- Vulnerability in the cgi test program, phf, allows unathorized access.
- WEBgais websendmail vulnerability
- WebSite 1.1 Uploader Vulnerability
- Website 1.1 for NT Winsample Vulnerability
- php.cgi Buffer Overflow

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

[1] William Stallings; **Network Security Essentials: Applications and Standards**; Prentice Hall; ©2000

[2] Internet Security Systems, Inc. - XFORCE Security Library; www.iss.net

[3] Daintry Duffy article in darwin – January 2001, Prepare for the Worst by; www.darwinmag.com

[4] Elizabeth D. Zwicky, Simon Cooper, & D. Brent Chapman **Building Internet Firewalls, Second Edition** 2nd Edition © June 2000 1-56592-871-7

[5] Chris Boyd; **UNIX Logging and Security (Systems Under Siege)**; November 9, 2000; http://www.sans.org/infosecFAQ/unix/unix_log.htm

[6] Stan Stringfellow; **Disaster Recovery Requirements Analysis**, Sun Blueprints On-line July 2000; http://www.sun.com/blueprints

[7] Paul D. J. Vandenberg and Susan D. Wyess; **Securing Solaris Servers - A Checklist Approach**; November 1998; http://www.usenix.org/sage/sysadmins/solaris/index.html

[8] **SANS Institute Track 6: Securing Unix Systems - Linux / Solaris Practicum**

[9] http://www.sun.com/blueprints/browsesubject.html#security

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.