



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

GIAC Enterprises

PUBLIC SERVERS VULNERABILITY ASSESSMENT REPORT

April 27, 2004

Prepared By
R. D. Smith

GCUX Assignment, V.1.9

This page intentionally left blank

© SANS Institute 2004, Author retains full rights.

SECURITY INFORMATION

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
1 INTRODUCTION.....	3
1.1 PURPOSE.....	3
1.2 SCOPE OF ASSESSMENT	3
1.3 LIMITATIONS AND CONSTRAINTS	3
2 INFORMATION SECURITY ASSESSMENT APPROACH	5
2.1 ASSESSMENT TEAM	5
2.2 INFORMATION COLLECTION TECHNIQUES	5
2.3 VULNERABILITY DETERMINATION	6
3 SYSTEM CHARACTERIZATION	7
3.1 SYSTEMS IDENTIFICATION	7
3.2 SYSTEMS AND DATA CATEGORIZATION	7
3.3 SYSTEM(S)/DATA SENSITIVITY	8
4 SECURITY REVIEW FINDINGS AND RECOMMENDATIONS	11
4.1 PLANS AND POLICIES FINDINGS.....	11
4.2 OPERATING SYSTEM (MAC OS X, v. 10.3) FINDINGS	15
4.3 APPLICATION FINDINGS.....	19
4.4 PHYSICAL AND OTHER.....	31
5 SUMMARY.....	35
ANNEX A – REFERENCES.....	37
ANNEX B – ACRONYMS	39
ANNEX C – NESSUS RESULTS	41
ANNEX D – NMAP RESULTS	57
ANNEX E – MAN PAGES.....	ERROR! BOOKMARK NOT DEFINED.

LIST OF TABLES

TABLE 1 – VULNERABILITY ASSESSMENT TEAM	5
TABLE 2 – LIKELIHOOD OF OCCURRENCE	6
TABLE 3 – VULNERABILITY SEVERITY	6
TABLE 4 – SYSTEMS IDENTIFICATION	7
TABLE 5 – CATEGORIZATION OF FEDERAL INFORMATION AND INFORMATION SYSTEMS	7
TABLE 6 – SYSTEM/DATA SENSITIVITY	8
TABLE 7 – NUMERICAL SUMMARY OF FINDINGS.....	35

SECURITY INFORMATION

LIST OF FIGURES

FIGURE 1 - DNS SETTINGS IN SERVER ADMIN	22
FIGURE 2 - FTP SETTINGS IN WORKGROUP MANAGER	28
FIGURE 3 - FTP SERVER SETTINGS IN SERVER ADMIN.....	29
FIGURE 4 - FTP SERVER BANNERS IN SERVER ADMIN.....	30

© SANS Institute 2004, Author retains full rights.

Executive Summary

GIAC Enterprises is a small company dealing in the manufacture and sales of fortune cookies. Their current market is the Mid-Atlantic region of the United States. Their strategic goal is to increase their market share in the region by winning contracts with the federal government and Department of Defense food service organizations to supply GIAC enterprises products. In order to achieve the strategic goal, GIAC Enterprises believes that their Internet presence needs to meet federal standards, within the fiscal constraints of their budget.

GIAC Enterprises retained the services of R.D. Smith Technical Services (RDS) to perform an information security review of their publicly accessible servers. During the review, RDS examined the public servers from both the network perspective as well as from the local host perspective. The network level review was performed from inside GIAC Enterprises' external enterprise firewall. The network review was designed to identify vulnerabilities exploitable from the GIAC Enterprises' internal network(s) and the Internet if the external enterprise firewall was compromised. The local host level review was performed as an authorized, privileged user to identify potentially insecure configuration settings. All testing was conducted using industry accepted open-source automated tools and manual system checks.

The major findings of this assessment include:

- Plans and Policies
 - Many of the information system plans and policies that should be in place are informal and have not been formally adopted by GIAC Enterprises' management team.
- Operating System
 - Operating Systems are not up to date with the latest System Update and security updates.
- Server Applications
 - The apache web server is vulnerable to attacks and is running a default configuration.
 - The DNS server configuration has not been locked down.
 - The FTP server authenticates users using insecure methods.
 - The mail server authenticates users in clear-text when encrypted methods are available.

The details of each finding and recommended corrective actions are presented in Section 4 of this report.

There are additional areas of the overall security of the public servers, such as the external and internal enterprise firewall rules, that should be assessed more fully. These areas were outside the scope of this risk assessment, however, an assessment of these areas would be necessary for to complete the assessment of the external servers' environment.

This page intentionally left blank

© SANS Institute 2004, Author retains full rights.

1 Introduction

This section presents the purpose, scope, and limitations of the vulnerability assessment.

1.1 Purpose

The purpose of this security review is to identify the vulnerabilities on the publicly accessible servers within their operational environment. The output of this security review is to provide GIAC Enterprises' Chief Information Officer (CIO) with an analysis of vulnerabilities and recommended countermeasures for reducing or mitigating the systems' risk of compromise.

1.2 Scope of Assessment

The scope of this information security vulnerability assessment is limited technical controls (system and application access control, audit, identification and authentication, etc.) implemented on the two servers identified in Section 3 of the report. Management (policy and plans) and Operational (procedures) Controls (in-place or planned) were not specifically included in the assessment as they were beyond the scope of work. However, if an assessment could be made based on the material gathered for the technical controls, the findings are presented in Section 4.

1.3 Limitations and Constraints

Due to scheduling conflict, the system administrator was not available to be interviewed. This limited the Assessment Team's ability collect necessary information and understanding of the some of the required operating system functionality on the servers. Therefore, some of the findings and recommendations may be inappropriate due to the assumptions made by the assessment team during the analysis of the raw data.

This page intentionally left blank

© SANS Institute 2004, Author retains full rights.

2 Information Security Assessment Approach

This Section describes the methodology employed by the Assessment Team during the conduct of this vulnerability assessment.

2.1 Assessment Team

The vulnerability assessment team consisted of the contractor and government personnel shown in Table 1.

Table 1 – Vulnerability Assessment Team

Name	Position	Organization	Phone
Rick Smith	Security Review Team Leader	Contractor –R.D. Smith Technical Services	(410) 555-6869
Ron Dumont	Deputy Chief Information Officer	GIAC Enterprises	(410) 555-1234

2.2 Information Collection Techniques

The Assessment Team used the following information collection techniques to gain an understanding of the database servers and identify vulnerabilities:

- Information was collected through physical inventory and interview:
 - Hardware;
 - Software;
 - Data and information; and
 - Persons who support and use the Information Technology (IT) systems.
- The following personnel were interviewed:
 - Mr. Ron Dumont, Deputy CIO;
 - Note: The system administrator for the two servers was unavailable while the RDS assessment team personnel were on site.
- The following automated discovery/collection tools were used on the servers to collect technical information:
 - Network Mapper (NMAP);
 - Nessus Vulnerability Scanner;
 - Personal observation; and
 - Manual inspection.
- Identification of potential threats that could adversely impact systems' or data's Confidentiality, Integrity, and/or Availability (CIA).
- Identification of vulnerabilities discovered.
- Estimation of the likelihood that threats would/could exploit identified vulnerabilities.
- Assess the impact to the systems' and/or data's CIA if a threat were to exploit a given vulnerability.

Provide corrective and/or mitigation recommendations.

2.3 Vulnerability Determination

2.3.1 Likelihood of Occurrence

The likelihood of occurrence is the estimation of the frequency or possibility of a threat exploiting the vulnerability. Therefore, the greater the likelihood of a threat exploiting a particular vulnerability, the greater the risk to the system and the data it contains. The definitions used for the levels of likelihood are shown in Table 2.

Table 2 – Likelihood of Occurrence

LIKELIHOOD	DEFINITION
HIGH	Vulnerability exists, is well known and well understood. Safeguards are not in place or do not exist to counter this threat.
MODERATE	Vulnerability exists, is moderately known but not well understood, and dependent on other vulnerabilities. Safeguards are in place but may be inadequate to counter this threat.
LOW	Vulnerability may exist, but not well understood, and may depend on the existence of other vulnerabilities. Safeguards are not in place to counter this threat.

2.3.2 Definition of Severity

Table 3 defines the severity of a given vulnerability and the urgency with which it must be addressed.

Table 3 – Vulnerability Severity

RISK LEVEL	VULNERABILITY DEFINITION AND URGENCY OF ACTION
HIGH	If an observation or finding is evaluated as high, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
MEDIUM	If an observation is rated as medium, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
LOW	If an observation is described as low, the system's authorizing official must determine whether corrective actions are still required or decide to accept the vulnerability.

3 System Characterization

This section presents a brief description of the evaluated systems, their categorization and the systems' data sensitivity. As part of GIAC Enterprises' efforts to improve security and adopt the "best practices" standards, the GIAC Enterprises' CIO requested that Federal Standards be used where possible. Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* [1], will be used to categorize the systems and the information that they contain.

3.1 Systems Identification

The two GIAC Enterprises systems that were assessed are identified in Table 4. The systems are production systems that located in GIAC Enterprises' DMZ. Both systems are located inside of GIAC Enterprises' external firewall but accessible from the Internet. The systems are isolated from the GIAC Enterprises' internal network by the internal firewall.

Table 4 – Systems Identification

Server Name	gala.giac.com	crispin.giac.com
IP Address	192.168.11.201	192.168.11.202
Function	DNS, SMTP	Web, FTP
Operating System	Mac OS X (v 10.3)	Mac OS X (v 10.3)
Application Version	BIND 9.2.2 Postfix 2.0.10 Cyrus 2.1.13	Apache 1.3.27 FTPD

3.2 Systems and Data Categorization

FIPS 199 provides a standard means of determining the baseline security controls for information and information systems. It defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The levels consider both impact and threat, but are more heavily weighted toward impact. The impact is based on the potential magnitude of harm that the loss of confidentiality, integrity, or availability would have on agency operations (including mission, functions, image or reputation), agency assets, or individuals (including privacy).

Table 5 defines the three levels of impact and associated descriptions for each security objective – confidentiality, integrity, and availability.

Table 5 – Categorization of Federal Information and Information Systems

Security Objective	Potential Impact		
	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations,	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations,	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on

SECURITY INFORMATION

Security Objective	Potential Impact		
	LOW	MODERATE	HIGH
protecting personal privacy and proprietary information. (FISMA [1])	organizational assets, or individuals.	organizational assets, or individuals.	organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (FISMA [1])	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. (FISMA [1])	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

3.3 System(s)/Data Sensitivity

The sensitivity of the data stored on the evaluated systems is considered proprietary data although some of the data is for public consumption. The systems process data that contains corporate proprietary information (potential fortune cookie fortunes, etc.). Categorization of the systems and data using the criteria defined in Table 5 yields the following: compromise of the data’s Confidentiality and Integrity would have a severe impact on GIAC Enterprises’ operations and image. The temporary loss of systems and data Availability would have a moderate impact on GIAC Enterprises’ operations. Table 6 is a graphic representation of the FIPS 199 categorization criteria applied to the evaluated systems.

Table 6 – System/Data Sensitivity

Data/Information Type	Impact
-----------------------	--------

SECURITY INFORMATION

	Confidentiality	Integrity	Availability
Public Web Site Data (<i>Pages used to advertise the GIAC Enterprises' products</i>)	LOW	MODERATE	MODERATE
FTP Data (<i>fortune cookie fortunes</i>)	HIGH	HIGH	LOW
Overall Sensitivity (<i>cumulative effect</i>)	HIGH	HIGH	MODERATE

© SANS Institute 2004, Author retains full rights.

This page intentionally left blank

© SANS Institute 2004, Author retains full rights.

4 Security Review Findings and Recommendations

This section provides detailed findings of the local site security review. Each finding identifies a specific problem, associated severity risk rating, impact to the organization, and recommendations to be taken in correcting or minimizing the security risk. The findings also list the applicable SANS Top 20 Internet Security Vulnerability [3].

The False Positives were included in the assessment to document the results of the research into the High Risk vulnerabilities reported by Nessus. In the case of these Nessus results, the research into the vulnerability showed the results were incorrect due to either incorrect default banner information or erroneous results from a Nessus plugin.

4.1 Plans and Policies Findings

4.1.1 Business Continuity and Disaster Recovery Plans have not been developed.

Finding: A Business Continuity Plan (BCP) is a formal plan to ensure that critical business functions will continue after an interruption of normal business activity. A Disaster Recovery Plan (DRP) is a comprehensive plan of consistent actions to be taken before, during and after a disruptive event that causes a significant loss of information system resources. [4]

Severity: HIGH

Impact: In the event of a manmade event or natural disaster, the BCP and DRP enhance GIAC Enterprises' ability to recover promptly and provide an organized method of making decisions.

Recommendations: Develop a BCP and DRP. These plans can be developed using the guidance in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34 [5] or by consulting with a Certified Business Continuity Professional [6] if necessary to develop these plans. Ensure that all employees are trained effectively on their responsibilities under these plans.

4.1.2 No formal backup procedures exist.

Finding: Formal backup procedures have not been established for the external servers. Backups are done on an ad hoc basis using CD-R disks.

Severity: HIGH

Impact: In the event of a system compromise or hardware failure, the affected server would be unavailable until the server configuration and data could be reconstructed.

Recommendations: Establish and follow backup procedures. The procedures should address the frequency and type of backups, storage of backup media, testing of backup and restore functions, and retention. Recommend installing commercial backup software on both servers and a DAT or DVD-RW drive in one server to be used for backing up both servers. Recommended scheduled backup frequencies and types:

SECURITY INFORMATION

Frequency	Type	Storage	Retention**
Daily	Incremental	Local	Two weeks (two sets of rotating media)
Weekly	Full	Local for one week then off-site for three weeks	Four weeks
Monthly (retain a weekly full backup)	Full	Off-site	One year

** Consult with legal counsel for legal requirements for record retention.

In addition to the scheduled backup, a full backup of the each server should be completed prior to upgrading the operating system or installing patches.

Storage facilities for the backup media should be fireproof and have controlled access. This recommendation can be accomplished by using a small fireproof safe for local storage. There are number of options for off-site backup media storage, including specialized secure storage companies that will pick-up and deliver the media and renting a secure storage and using employees to transport tapes.

4.1.3 Formal Incident Handling Policy or Procedures have not been developed or implemented.

Finding: An informal plan has been discussed between the CIO and the system administrator for actions to be taken if a server has been compromised. However, a formal Incident Handling Plan and related policies and procedures have not been established to cover the actions required during an incident.

Severity: HIGH

Impact: In the event of an incident, the lack of plans and procedures may prevent the system administrator from preserving the legal evidence of the compromise or may cause further problems that may increase the time to bring the server back into service.

Recommendations: Develop an Incident Response Plan and the supporting policies and procedures. NIST SP 800-61 [7] and Chapter 10 of Volume One of the SANS Security Essentials with CISSP CBK [8] provide guidance for developing of the policies and procedures.

4.1.4 A formal auditing policy has not been developed.

Finding: An informal requirement to review operating system and application logs. However, there is no formal policy for auditing system log or collecting for logs for later analysis. Also, based on the discussion with the CIO of the external servers, the informal requirements were not being carried out regularly. (Note: Mac OS X has no capability at this time to generate C2-type audit records although there are various system and application logs.)

Severity: HIGH

Impact: Although logging is enabled for both the operating system and the applications, no one regularly reviews the logs for signs of intrusion or misuse.

Recommendations: Establish and enforce a log auditing policy. The policy should include the logs that will be audited, roles and responsibilities for personnel auditing the logs, and log retention and storage requirements.

4.1.5 A formal Password Policy has not been developed.

Finding: An informal requirement to use secure passwords is in use throughout the company. However, there is no formal policy for password aging or complexity. Also, based on the manual examination of the external servers, the informal requirements were not being enforced. (See findings 4.2.3 and 4.2.4.)

Severity: Moderate

Impact: Weak or easily guessed passwords can be used on the servers and other company owned systems.

Recommendations: Establish and enforce a Password Policy. A sample password policy can be obtained from the SANS Security Policy Project [9].

4.1.6 A warning banner is not posted on company-owned systems.

Finding: A warning banner for system users is not posted at all logon points to company-owned computers and systems.

Severity: Moderate

Impact: Warning banners are not legally required or binding but may facilitate prosecution of attackers of a computer network by obtaining consent for keystroke monitoring.

Recommendations: A "sign-on warning banners" for employees and other system users should be posted at all logon points to company-owned computers and systems where they are technically practical [10]. This should include ssh and ftp logins to the systems. In addition, this policy should be included in all orientation materials for new/transferring users. Consult legal counsel about the content of the warning banner before posting on GIAC Enterprises' systems.

A free application that installs warning banners on the login screen of Mac OS X systems is available at from Center for Information Technology, National Institutes of Health [11]. To enable banners for ssh connections, edit `/etc/ssh_config`, uncomment the "Banner" line and provide a path to the text contain in the warning banner. For FTP logins, see finding 4.3.3.2.

4.1.7 A Privacy Policy is not posted on the company web site.

Finding: In the review of the content on the GIAC Enterprises' website, no Privacy Policy is posted for visitors to the site.

Severity: Moderate

Impact: There are legal requirements for use and protection of private information obtained from visitors to a web site. GIAC Enterprises' may be held legally liable in the case of violation of these requirements.

Recommendations: Establish a Privacy Policy. The Children's Online Privacy Protection Act [12] provides the requirements for privacy policies. Consult with legal counsel concerning the content of the Privacy Policy before posting the Privacy Policy on the web site.

4.1.8 No software configuration management on production servers.

Finding: Based on the findings on the servers, there appears to be no consistent configuration. Configuration management, control of application settings, and patching will enable the system administrators the servers are maintained in a secure configuration. Configuration management will also help the administrators and web application developers to control and understand the environment on the server.

Severity: Moderate

Impact: Configuration management will help prevent changes, both inadvertent and intentional, to the external servers that could cause corruption of data or a self-imposed denial of service.

Recommendation: Develop and implement a configuration management plan that covers at least basic operating system configuration, operating system and application software patch management, changes to the configuration of the applications, personnel who can authorize changes and the personnel who are authorized to actually make the changes or install patches. The production systems, in particular, require a standardized/secure configuration. Exceptions or deviation from the "standard/secure configuration" must be evaluated for the risks/vulnerabilities the deviation introduces. The exception must be documented and approved by the system owner and senior GIAC Enterprises' management.

4.1.9 An Acceptable Use Policy is not available to company employees.

Finding: A policy that defines the limits of acceptable use of company IT resources by employees has not been developed and given to employees.

Severity: Low

Impact: Misuse of company-owned systems and other IT resources by employees for the benefit of themselves.

Recommendations: Establish and enforce an Acceptable Policy. In addition, this policy should be included in all orientation materials for new/transferring users. A sample acceptable use policy can be obtained from the SANS Security Policy Project [9].

4.1.10 No hardware inventory of production servers.

Finding: Based on the discussion with the CIO, there appears to be no method or plan to maintain an inventory of server hardware.

Severity: Low

Impact: Hardware inventory management will help prevent long-term loss of availability due to theft of the server, a hardware failure, or other incident that damages the hardware occurs.

Recommendation: Develop and maintain up-to-date a physical inventory of each server machine. This will enable the IT staff to recover from the hardware incident more rapidly.

4.2 Operating System (Mac OS X, v. 10.3) Findings

Unless otherwise noted, the findings for the operating system exist on both servers.

4.2.1 Mac OS X patches are not current.

Finding: Several operating system updates and security patches are not installed on all servers. The servers have not been patched within one month of the security review.

Severity: HIGH

Impact: The patches that are missing cover a number of CVE vulnerabilities. The services affected by these updates and patches may allow an attacker to obtain additional information about the server or conduct denial of service attacks against other machines.

Recommendations:

1. Install the latest operating system update, Mac OS X Server Combined Update 10.3.3 [13], and security patch, Security Update 2004-04-05 [14]. The update and patch should be tested on development servers before installation on the production servers.
2. Subscribe to the Apple Security mailing list [15] for notification of security patches. A current list of patches is maintained at Apple Security Updates, (Knowledgebase Article ID 61798) [16].
3. Establish procedures for testing and installing patches on a regular basis, i.e., within 3 business days of release of the security update and upon approval of the configuration control board for other updates.

4.2.2 Common user accounts are being used.

Finding: Based on observation, users are logging on to the servers with common accounts, e.g., netadmin.

Severity: Moderate

Impact: Use of common accounts for logging on to the servers prevents accurate auditing of users actions and holding users accountable for their actions.

Recommendation: Give administrative users their own normal user account and an account with admin privileges. Configure sudo to allow the administrative users access to the minimum set command necessary for each user to perform their job. This will restrict the use of “root”

commands authorized to specific users and the logging and auditing of those actions. Ensure the root account is disabled.

4.2.3 Password aging not set.

Finding: Passwords for accounts on the machines do not have an expiration period set. Also, no reuse policy is set. (SANS Top 20 U4)

```
% pwpolicy -getglobalpolicy
usingHistory=0 usingExpirationDate=0 usingHardExpirationDate=0
requiresAlpha=0 requiresNumeric=0 expirationDateGMT=12/31/69
hardExpireDateGMT=12/31/69 maxMinutesUntilChangePassword=0
maxMinutesUntilDisabled=0 maxMinutesOfNonUse=0
maxFailedLoginAttempts=0 minChars=0 maxChars=0
passwordCannotBeName=0
```

Severity: Moderate

Impact: A malicious user can use any user account password that has been compromised indefinitely unless the password expires on a regular basis.

Recommendation: Use /usr/bin/pwpolicy to change set password aging settings for all accounts. Set the maximum password age, maxMinutesUntilChangePassword, to 129600 minutes (90 days) and set the password reuse policy, usingHistory, to 15 to prevent the last 15 passwords from being used. (This is the maximum number allowed by pwpolicy.).

```
%/usr/bin/pwpolicy -a <admin username> -setglobalpolicy \
    "maxMinutesUntilChangePassword=129600 usingHistory=15"
```

See the pwpolicy man page [17] for more information on the pwpolicy command.

4.2.4 Password complexity not set.

Finding: Passwords for accounts on the machines do not require the use of complex passwords. (SANS Top 20 U4)

Severity: Moderate

Impact: The time it takes a malicious user to crack or guess passwords is significantly reduced if password complexity requirements are enforced.

```
% pwpolicy -getglobalpolicy
usingHistory=0 usingExpirationDate=0 usingHardExpirationDate=0
requiresAlpha=0 requiresNumeric=0 expirationDateGMT=12/31/69
hardExpireDateGMT=12/31/69 maxMinutesUntilChangePassword=0
```

SECURITY INFORMATION

```
maxMinutesUntilDisabled=0 maxMinutesOfNonUse=0
maxFailedLoginAttempts=0 minChars=0 maxChars=0
passwordCannotBeName=0
```

Recommendation: Use `/usr/bin/pwpolicy` to change set password complexity settings for all accounts. Set the minimum password length, `minChars`, to 8, and require the use of alpha, `requiresAlpha`, and numeric characters, `requiresNumeric`. Pwpolicy does not have the capability to require the use of special characters; this must be done by written password policy.

```
%/usr/bin/pwpolicy -a <admin username> -setglobalpolicy \ "minChars=8
requiresAlpha requiresNumeric"
```

See the pwpolicy man page [17] for more information on the pwpolicy command.

4.2.5 The `/var/cron/allow` and `/var/cron/deny` files do not exist.

Finding: The `/var/cron/allow` file is a list of users who are allowed to run the crontab commands to submit jobs to be run at scheduled intervals. On many systems, only the system administrator needs the ability to schedule jobs. The file `/var/cron/allow` only controls administrative access to the crontab command for scheduling and modifying cron jobs. The list of denied users is contained in `/var/cron/deny`.

Severity: Moderate

Impact: If the `/var/cron/allow` and `/var/cron/deny` files do not exist, any user can schedule jobs to be run at any time.

Recommendation: Create `/var/cron/allow` and `/var/cron/deny`. Edit these files and insert a list of known user allowed and a list of users denied use of the cron facility in the respective files. Ensure `/var/cron/allow` and `/var/cron/deny` are owned by the user root and group root. Change permissions to 644 on `/var/cron/allow` and `/var/cron/deny`.

4.2.6 The Apple Password Server leaks information about its version.

Finding: The Apple Password Server leaks information about the software it is running through the login banner. The version of the server is:

```
"+OK ApplePasswordServer 10.1.0.0 password server at 192.168.11.202."
```

Severity: Low

Impact: The information leakage may assist an attacker in choosing an attack strategy.

Recommendation: None. The normal recommendation would be to change the login banner to something generic. However, "ApplePasswordServer" is defined in the Directory Services framework and changing the banner would require modifying the source code and recompiling the framework.

4.2.7 NTP server is reachable from the network.

Finding: The NTP daemon is responds to queries from the network. Information provided by the server:

```
“version='ntpd 4.1.1@1.786 Fri Sep 12 18:30:03 PDT 2003 (1)',  
processor='Power Macintosh', system='Darwin7.0.0', ...”
```

Severity: Low

Impact: The NTP server provides information about the machine when it responds to the queries. This information may be valuable to an attacker that is performing reconnaissance on the server.

Recommendation: Restrict the NTP from answering queries by adding a “restrict default ignore” line to the /etc/ntp.conf file and restarting the server.

4.2.8 Old version of OpenSSH running.

Finding: The version of OpenSSH is older than 3.71, which is vulnerable to a flaw in buffer management functions which might allow an attacker foe execute arbitrary commands on the server. (SANS Top 20 U8)

The version of the OpenSSH demon is

```
“OpenSSH_3.6.1p1+CAN-2003-0693, SSH protocols 1.5/2.0, OpenSSL  
0x0090702f.”
```

Severity: False Positive

Impact: This finding is here to document the False Positive “Security Hole” found by Nessus. Because Apple has chosen to patch OpenSSH but not update the version number, this false positive will remain in the Nessus results until Apple changes the version number.

An exploit for this buffer management flaw is rumored to exist. This would allow the attacker to remotely gain complete control of the server.

Recommendation: Apple has incorporated the patches for CVE CAN-2003-0682, CAN-2003-0693, and CAN-2003-0695 in this version [16].

4.2.9 An older version of OpenSSL is running.

Finding: An older version of OpenSSL protects The AppleShare Web Administration web site. The version of OpenSSL is 0.9.7b. (SANS Top 20 U10)

```
% openssl version  
OpenSSL 0.9.7b 10 Apr 2003
```

Severity: False Positive

Impact: This finding is here to document the False Positive “Security Hole” found by Nessus.

If this finding was not a False Positive, there are multiple vulnerabilities in the ASN.1 parsing code in OpenSSL older than 0.9.6k and 0.9.7c. These vulnerabilities could allow an attacker to gain a remote shell on the server. The vulnerabilities include:

- Integer overflow that allows remote attackers to cause a denial of service (crash) via an SSL client certificate with certain ASN.1 tag values.
- Improperly track the number of characters in certain ASN.1 inputs, which allows remote attackers to cause a denial of service (crash) via an SSL client certificate that causes OpenSSL to read past the end of a buffer when the long form is used.
- Double-free vulnerability that allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via an SSL client certificate with a certain invalid ASN.1 encoding.

Recommendation: None. Apple has corrected these vulnerabilities in were fixed in the initial release of Mac OS X Server 10.3. [16] Because Apple has chosen to patch OpenSSL but not update the version number, this false positive will remain in the Nessus results until Apple changes the version number.

4.3 Application Findings

4.3.1 DNS/BIND

4.3.1.1 BIND is not updated to current version.

Finding: The Berkeley Internet Name Domain (BIND) package, version 9.2.2, is installed on gala.giac.org. The BIND daemon, named, is has several bugs that have been fixed in BIND 9.2.3. Thei was reported by Nessus and nmap and verified throughn manual inspection. (SANS Top 20 U1)

```
%named -v
BIND 9.2.2
```

Severity: Low

Impact: BIND has had a long history of vulnerabilities, ensuring the latest bugs have bee fixed will help prevent exploitation of the DNS server by a zero day exploit.

Recommendation: Upgrade to the latest version of BIND, version 9.2.3, and configure the server securely.

4.3.1.2 The DNS Server allows recursive queries from unknown hosts.

Finding: The DNS server on gala.giac.org allows recursive queries to be performed by an untrusted host. This was reported by Nessus and verified by reviewing /etc/named.conf (see listing below). (SANS Top 20 U1)

SECURITY INFORMATION

```
% cat named.conf
// Declares control channels to be used by the rndc utility.
// It is recommended that 127.0.0.1 be the only address used.
// This also allows non-privileged users on the local host to manage
// your name server.
//
controls {
    inet 127.0.0.1 port 54 allow {any; };

};
options {
    directory "/var/named";
    recursion true;
    /*
    * If there is a firewall between you and nameservers you want
    * to talk to, you might need to uncomment the query-source
    * directive below. Previous versions of BIND always asked
    * questions using port 53, but BIND 8.1 uses an unprivileged
    * port by default.
    */
    // query-source address * port 53;
};

//
// a caching only nameserver config
//
zone "." IN {
    type hint;
    file "named.ca";
};

zone "localhost" IN {
    type master;
    file "localhost.zone";
    allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
```

```
    type master;
    file "named.local";
    allow-update { none; };
};

zone "giac.com" IN {
    file "giac.com.zone";
    type master;
};

zone "11.168.192.in-addr.arpa" IN {
    file "11.168.192.in-addr.arpa.zone";
    type master;
};
logging {
    channel _default_log {
        file "/Library/Logs/named.log";
        severity info;
        print-time yes;
    };
    category default {
        _default_log;
    };
};
```

Severity: Low

Impact: This allows anyone to use it to resolve third parties names (such as <http://www.sans.org/>). This allows hackers to do cache poisoning attacks against this name server. If the host allows these recursive queries via UDP, then the host can be used to 'bounce' Denial of Service attacks against another network or system.

Recommendation: Restrict recursive queries to only the authorized hosts that absolutely need it by editing `/etc/named.conf` and inserting the IP addresses of the authorized hosts in the “allow-recursion” option. If recursive queries can be completely disabled, change the “recursion” option in `named.conf` to “false” or uncheck the Recursion check box under the General Settings of the DNS service pane in Server Admin, see Figure 1

4.3.1.3 The DNS Server allows zone transfers.

Finding: The DNS server on gala.giac.org allows DNS zone transfers to be performed. This was tested with Nessus and verified by reviewing /etc/named.conf (see listing in 4.3.1.3) (SANS Top 20 U1)

Severity: Low

Impact: A zone transfer will allow the remote attacker to instantly populate a list of potential targets.

Recommendation: Restrict DNS zone transfers to only the authorized secondary name servers that absolutely need it by editing /etc/named.conf and inserting the IP addresses of the authorized secondary DNS servers in the “allow-transfer” option. If zone transfers can be completely disabled, uncheck the Zone transfer check box under the General Settings of the DNS service pane in Server Manager.app, see Figure 1.

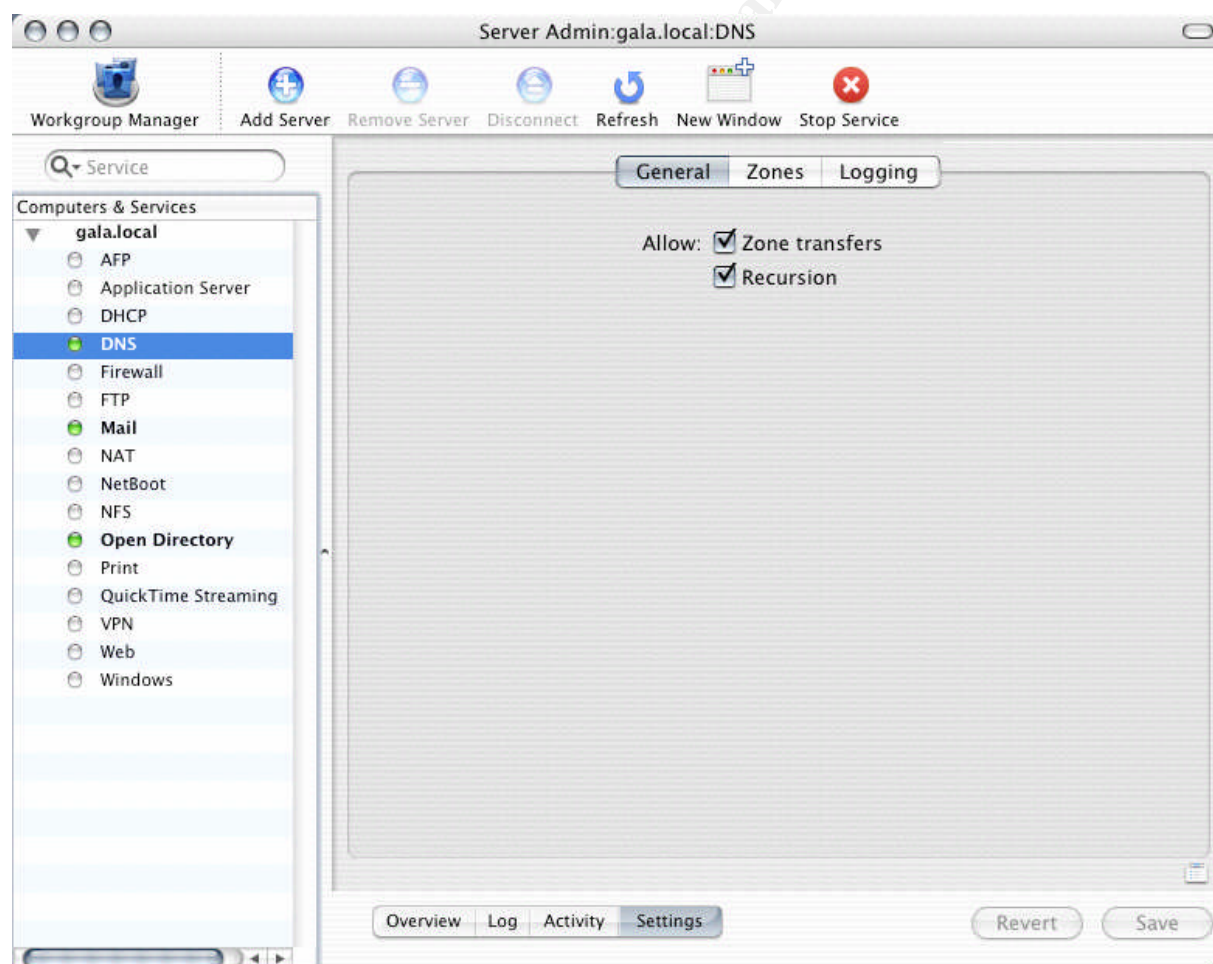


Figure 1 - DNS Settings in Server Admin

4.3.1.4 The DNS Server allows its version number and type to be queried.

Finding: The DNS server on gala.giac.org allows remote users to query for version and type information. The query of the CHAOS TXT record 'version.bind' will typically prompt the server to send the information back to the querying source. (SANS Top 20 U1)

Severity: Low

Impact: This provides an attacker with the additional information about the name server.

Recommendation: Use the "version" option in /etc/named.conf to obfuscate the version of BIND. The argument for the "version" option can be an arbitrary string.

4.3.2 Web/Apache

4.3.2.1 The Apache web servers are running an old version.

Finding: The webserver, crispin.giac.com, is running the Apache web server, version 1.3.28 on port 80/tcp. This was reported by Nessus and nmap and verified on the server. (SANS Top 20 U3)

```
% /usr/sbin/httpd -v
Server version: Apache/1.3.28 (Darwin)
Server built: Sep 12 2003 17:00:23
```

Severity: HIGH

Impact: Apache older than 1.3.29 are vulnerable to attack through the Apache Modules mod_rewrite and mod_alias. An attacker could gain remote super user access to the servers.

Recommendations: Update to Mac OS X 10.3.3 to upgrade Apache 1.3.29. The vulnerability in Apache 1.3.27 was corrected by Security Update 2004-01-26 for Mac OS X 10.3.2 "Panther" and Mac OS X Server 10.3.2 and is incorporated in Mac OS X Server 10.3.3. [16]

4.3.2.2 An older version of Apache is running.

Finding: The AppleShare web administration site, port 311/tcp, is running on Apache 1.3.27. (SANS Top 20 U3)

Severity: HIGH

Impact: Apache older than 1.3.29 are vulnerable to attack through the Apache Modules mod_rewrite and mod_alias. An attacker could gain remote super user access to the servers. Versions of Apache older than 1.3.28 are vulnerable to attacks that may allow the attacker to disable the Apache web server.

Recommendations:

1. Block ports 311/tcp and 311/udp on the external firewall.

SECURITY INFORMATION

2. Update to Mac OS X 10.3.3 to upgrade Apache 1.3.29. The vulnerability in Apache 1.3.27 was corrected by Security Update 2004-01-26 for Mac OS X 10.3.2 "Panther" and Mac OS X Server 10.3.2 and is incorporated in Mac OS X Server 10.3.3. [16]
3. Modify the AppleShare Web Administration web server configuration, /etc/servermgrd/servermgrd.conf, to allow access to port 311/tcp and 311/udp only from the administrator's machines. The /etc/servermgrd/servermgrd.conf is an Apple-modified Apache server configuration file.

4.3.2.3 Hidden Mac OS X files available via web server.

Finding: MacOS X creates a hidden file, '.DS_Store' in each directory that has been viewed with the 'Finder'.

Severity: Moderate

Impact: The .DS_Store contains a list of the contents of the directory, giving an attacker information on the structure and contents of your website.

Recommendation: Use a <FilesMatch> directive in httpd.conf to forbid retrieval of this file:

```
<FilesMatch '^\. [Dd][Ss]_[Ss]'>  
Order allow, deny  
Deny from all  
</FilesMatch>
```

and restart Apache. [18]

4.3.2.4 The mod_SSL module offers weak ciphersuites.

Finding: The mod_ssl module SSLv2 server offers 2 weak "export class" cipher suites, EXP-RC4-MD5 and EXP-RC2-CBC-MD5. The server also accepts SSLv3 and TLSv1 connections. (SANS Top 20 U3)

```
% openssl s_client -connect 192.168.11.201:311 -debug -ssl2  
CONNECTED(00000003)  
<uninteresting debug and certificate information removed>  
---  
Server certificate  
-----BEGIN CERTIFICATE-----  
MIID0zCCAzygAwIBAgIBADANBgkqhkiG9w0BAQQFADCBqDELMAkGA1UEBhMCVVMx  
EzARBgNVBAGTCkNhbgGImb3JuaWExEjAQBgNVBAcTCUN1cGVydGlubzEdMBSGA1UE  
ChMUQXBwGUGQ29tcHV0ZXIsIEluYy4xETAPBgNVBAcTCG1TZjJ2ZXJzMRgwFgYD  
VQQDEw93d3cuZXhhbXBsZS5jb20xJDAiBgkqhkiG9w0BCQEFWFXdIYm1hc3RlckBl  
eGFtcGxILmNvbTAeFw0wMTA4MjQyMTAxNTIaFw0wMTA4MjUyMTAxNTIaMIGoMQsw  
CQYDVQQGEWJlVUzETMBEGA1UECBMKQ2FsaWZlcml5Y29udGV0eS5pYTESMBAGA1UEBxMJQ3VwZXJ0  
aW5vMR0wGwYDVQQKEExRBcHBsZS5BDBb21wdXRlciwgSW5jLjJERMA8GA1UECXMlaVNI
```

SECURITY INFORMATION

```
cnZlcnMxGDAWBgNVBAMTD3d3dy5leGFtcGxILmNvbTEkMCIGCSqGSib3DQEJARYV
d2VibWFzdGVyQGV4YW1wbGUuY29tMIGfMA0GCSqGSib3DQEBAQUAA4GNADCBiQKB
gQCZBw7fA5W2LvRQDYNGbrWEZxu3a7ErBSwnE7e9nykwZ0lu6pidqa8yKp5sWRLh
5WuDE3TeHgtLjCgj/HzrkZleVDn3wyipJXiGwYDdr1MkiCU2m3wdi+Srm1Afkhs
8l4vHI8A27idzrGiYMax+WnXRbAa6OUlyvMil2pCpaJWiwIDAQABo4IBCTCCAQUw
HQYDVR0OBBYEFpd8qxrDlouPXBnueOb87hibSj/NMIHVBgNVHSMGc0wgcqAFPd8
qxrDlouPXBnueOb87hibSj/NoYGuplGrMIGoMQswCQYDVQQGEWJVUzETMBEGA1UE
CBMKQ2FsaWZvcn5pYTESMBAGA1UEBxMjQ3VwZXJ0aW5vMR0wGwYDVQQKEExRBcHBs
ZSBDb21wdXRlciwgSW5jLjERMA8GA1UECzMlcnZlcnMxGDAWBgNVBAMTD3d3
dy5leGFtcGxILmNvbTEkMCIGCSqGSib3DQEJARYVd2VibWFzdGVyQGV4YW1wbGUu
Y29tggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEEBQADgYEAJVsbfY9NPXuK
qC47ogme7y5BBJNwxK5WieCoJOij97WIHK3gDexJ3tMbHnyGyl0fXHsITVxeCATo
HkngDADzhC1jHnOjNLJVbhdN3KRSNHduY+f37NU8edV6Artv/eldNRsw6pR8ebE
oobn0ysW2wKEnVFYoBOPDlpRWsDViz0=
```

-----END CERTIFICATE-----

```
subject=/C=US/ST=California/L=Cupertino/O=Apple Computer,
Inc./OU=iServers/CN=www.example.com/emailAddress=webmaster@example.com
issuer=/C=US/ST=California/L=Cupertino/O=Apple Computer,
Inc./OU=iServers/CN=www.example.com/emailAddress=webmaster@example.com
```

No client certificate CA names sent

Ciphers common between both SSL endpoints:

```
RC4-MD5      EXP-RC4-MD5  RC2-CBC-MD5
EXP-RC2-CBC-MD5  DES-CBC-MD5  DES-CBC3-MD5
RC4-64-MD5
```

SSL handshake has read 1119 bytes and written 239 bytes

New, SSLv2, Cipher is DES-CBC3-MD5

Server public key is 1024 bit

SSL-Session:

Protocol : SSLv2

Cipher : DES-CBC3-MD5

Session-ID: B7E6AC596A8AECF0CF2333DA5D4B3034

Session-ID-ctx:

Master-Key: 5ED0679CC31CA4C05225754B9964DBE0DDF1691194B358A8

Key-Arg : A20227410B5736FD

Start Time: 1083060144

Timeout : 300 (sec)

Verify return code: 10 (certificate has expired)

<more uninteresting debug information removed>

Severity: Moderate

Impact: An attacker could break the encryption of the session between the administrator's machine and the AppleShare Web Administration web site on the server.

Recommendation: Disable SSLv2 and SSLv3 in the AppleShare Web Administration web server configuration, `/etc/servermgrd/servermgrd.conf`, by setting the `SSLProtocol` configuration directive to `TLSv1`. Require high strength cipher suites by setting the `SSLCipherSuite` configuration directive to `HIGH` in the Apache server configuration. [19]

Additional Information: The server certificate for both servers are the default installation certificates created by Apple for testing purposes. More information on creating and installing your own SSL certificates is outlined on the AFP548 website [20].

4.3.2.5 The web server leaks information about the version of Apache is running.

Finding: The web server on `crispin.giac.com` provides version information about itself and components. Version information provided is:

“Apache/1.3.28 (Darwin) PHP/4.3.4 mod_jk/1.2.4 mod_ssl/2.8.15
OpenSSL/0.9.7b.”
(SANS Top 20 U3)

Severity: Low

Impact: Information leakage to an attacker that allows further targeting of vulnerabilities of specific versions of the Apache web server.

Recommendations:

Modify `/etc/httpd.conf` and set the directive `“ServerTokens Prod”` to limit the information leakage from the server in its response headers.

4.3.2.6 The web server potentially leaks information about the user names.

Finding: An information leak occurs on Apache based web servers whenever the `UserDir` module is enabled. (SANS Top 20 U3)

Severity: Low

Impact: Information leakage to an attacker that allows an external attacker to enumerate existing accounts by requesting access to their home directory and monitoring the response.

Recommendations: Modify `/etc/httpd.conf` and set the directive `“UserDir”` to `“disabled.”`

4.3.3 FTP

4.3.3.1 Anonymous logins to the FTP server are disabled.

Finding: FTP server is being used to allow remote writers of fortune cookies fortunes to transfer their work to the company headquarters and allow remote sales representatives to access information and data. The writers and sales personnel currently log in to the server using usernames and passwords. (SANS Top 20 U5)

Severity: HIGH

Impact: This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the FTP client and the FTP server. This includes user names and passwords. An attacker could gain remote super user access to the servers.

Recommendation:

1. For the writers, configure the FTP server to allow anonymous access. Configure an “uploads” directory to be a “drop box.”
 - a. Using Workgroup Manager, remove the default FTP sharing and FTP guest access of the Groups, Users and Public directories. (See Figure 2.)
 - b. Remove the aliases in /Library/FTPServer/FTPRoot
 - c. Create the “uploads” directory in /Library/FTPServer/FTPRoot directory. Change the file permissions on the “uploads” directory to 703.
 - d. Using Server Admin, check the box next to Enable anonymous access. Change the maximum number of anonymous users as necessary. Reduce the maximum number of authenticated users to 1 (this is the minimum Server Admin will allow). Note: The maximum number of authenticated users can be set in /Library/FTPServer/Configuration/ftpaccess but this value may be overwritten by the Server Admin application, see Figure 3.
2. For the sales personnel, use sftp clients for file transfers. The sftp client accesses the server via OpenSSH and thus encrypts the session between the client and the server. The usernames and passwords are safe from sniffing.

SECURITY INFORMATION

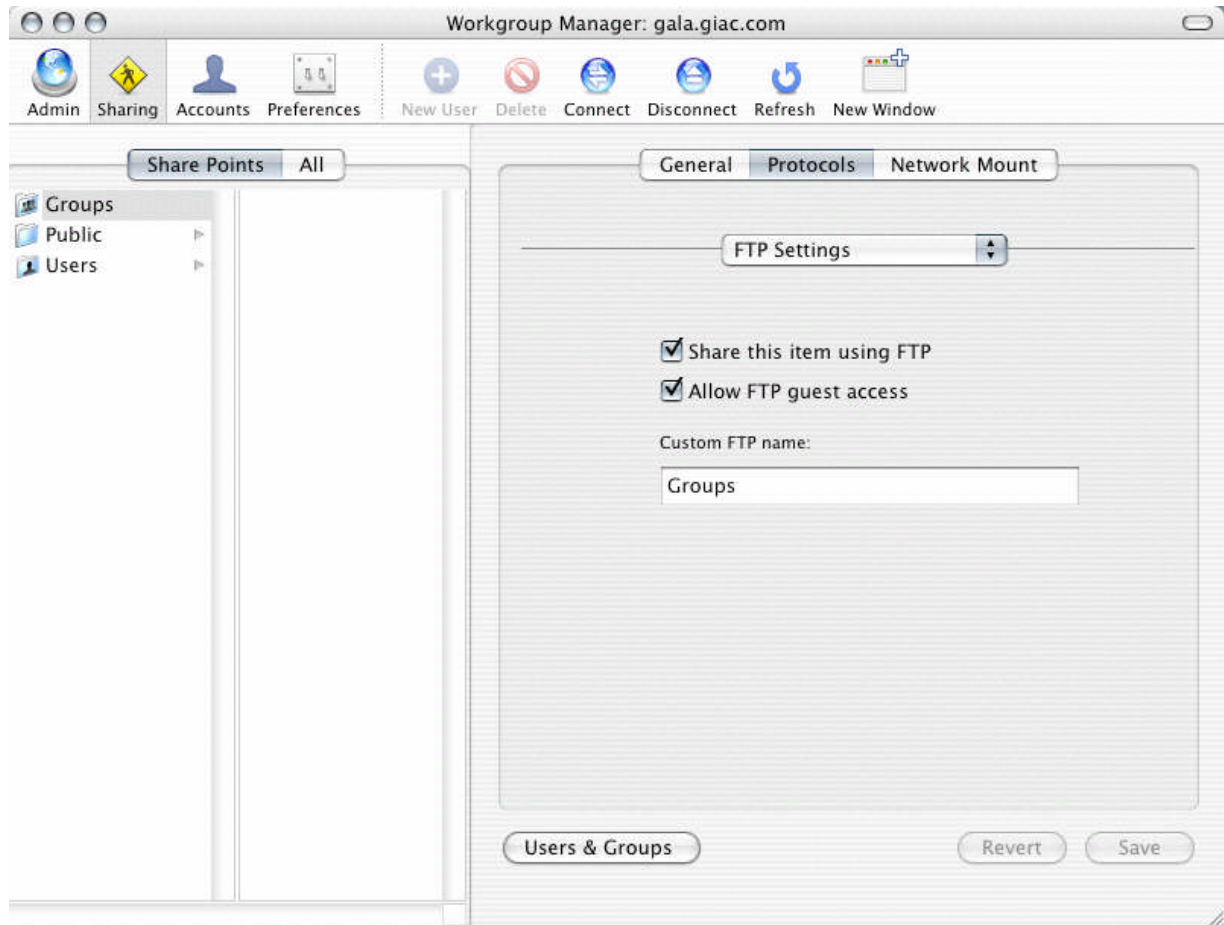


Figure 2 - FTP Settings in Workgroup Manager

4.3.3.2

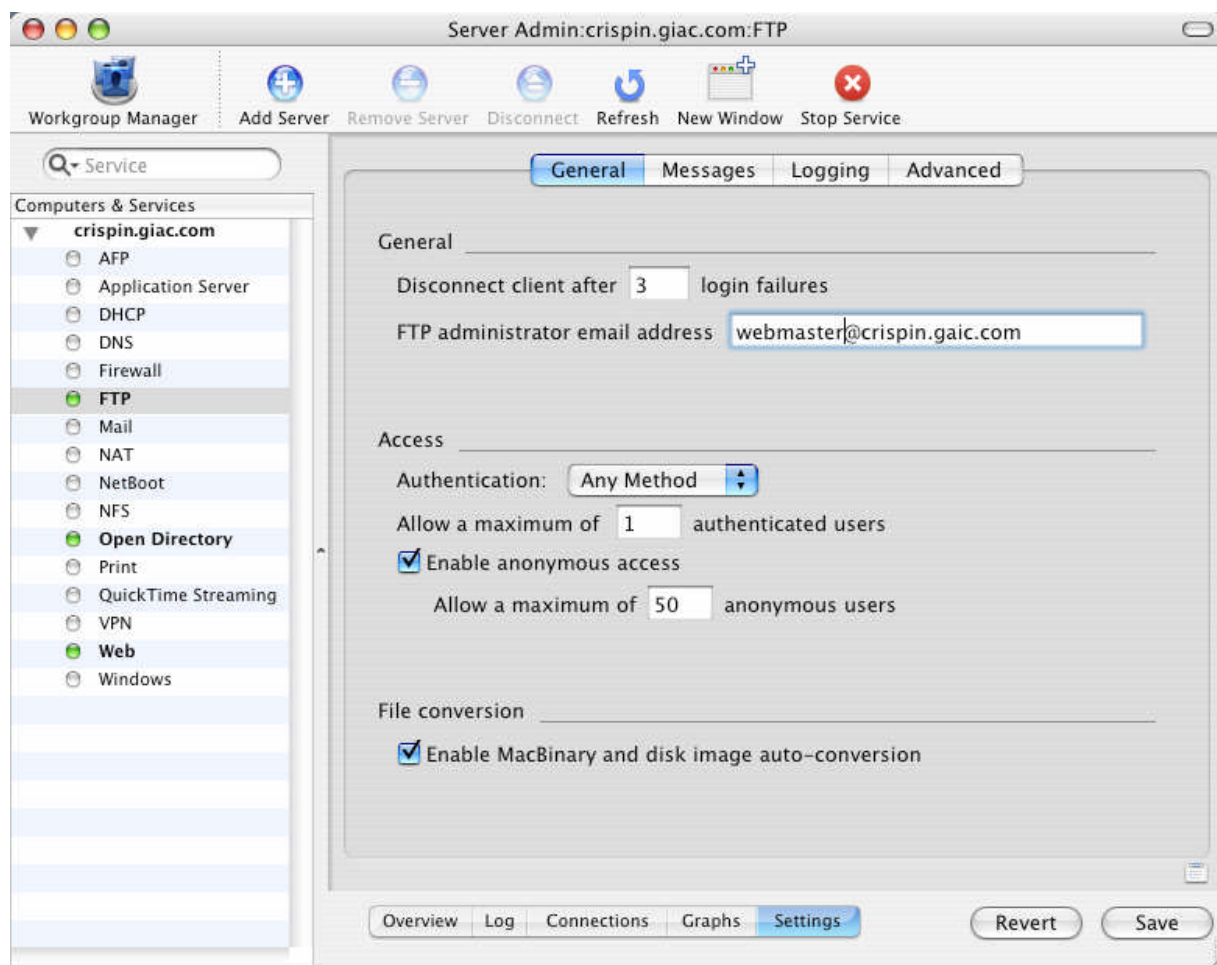


Figure 3 - FTP Server Settings in Server Admin

4.3.3.3 The banners for the FTP server are the default banners.

Finding: The default Mac OS X 10.3.xftpd banner and welcome messages are still set.

Severity: Low

Impact: These messages do not serve any useful function until modified. In fact in this case, they show that the system administrator shows a lack of attention to detail, which may encourage an attacker to target this machine.

Recommendation: Modify banner.txt and welcome.txt in /Library/FTPService/Message/ to provide an acceptable use policy and a consent to monitoring statement to users accessing the FTP server. These banners can also be modified using the Server Admin application, see Figure 4. Check with the Legal Department for the correct wording.

SECURITY INFORMATION

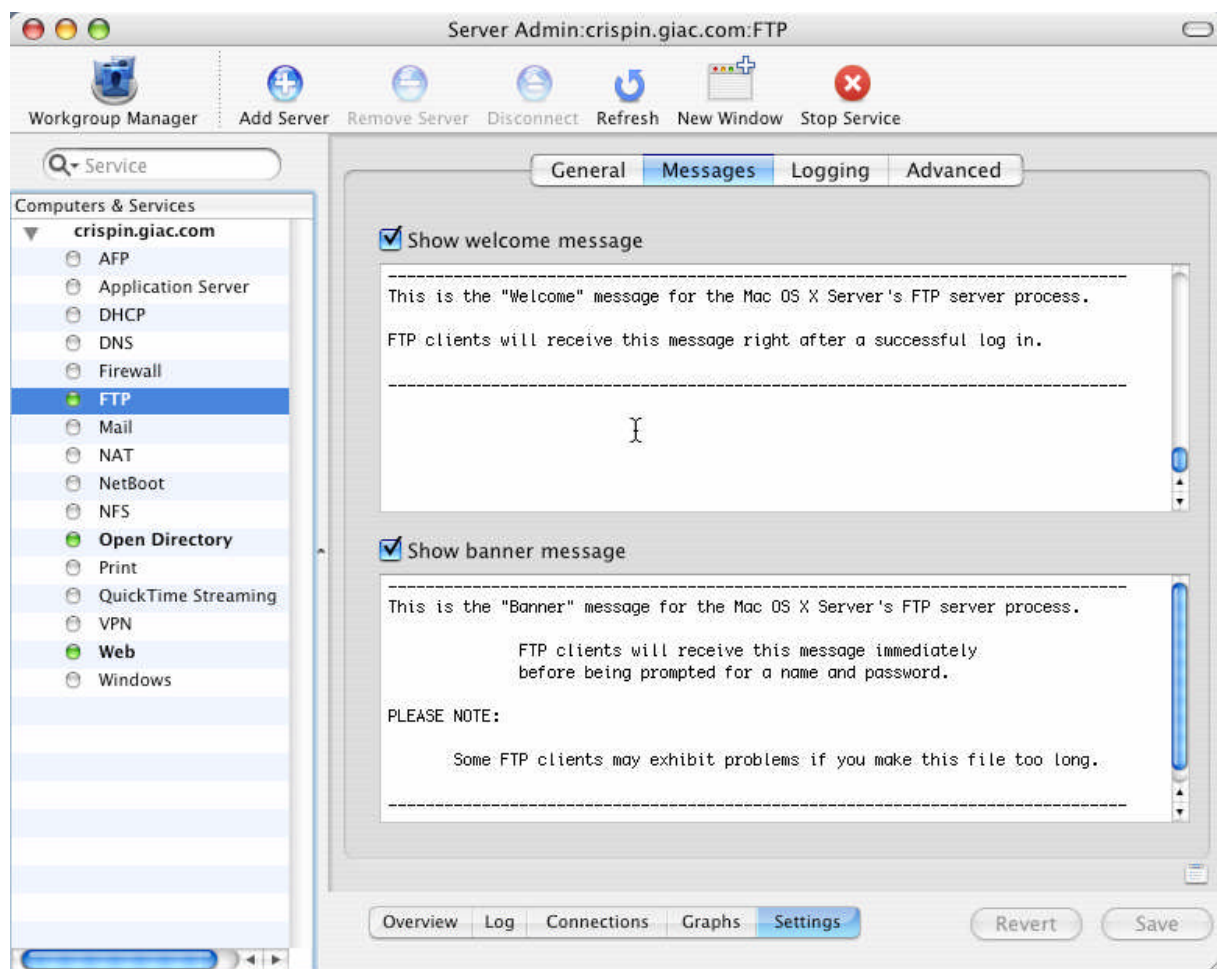


Figure 4 - FTP Server Banners in Server Admin

4.3.4 Mail/Postfix, Cyrus

4.3.4.1 The POP3 and IMAP mail servers allow unencrypted logons.

Finding: The Postfix SMTP server and Cyrus IMAP/POP3 server are not SSL-enabled. All of these protocols are clear text and any login to these servers requires that the username and password cross the network in plain text. (SANS Top 20 U5)

Severity: HIGH

Impact: An attacker may gain a valid user name and password pair that allows taking over a user account. The attacker might be able to use the valid user account on the machine gain super user access remotely.

Recommendation: Install and configure a SSL server certificate for both servers. Information on installing and configuring SSL certificates with Postfix and Cyrus is available at AFP548.com [19].

4.3.4.2 The POP3 and IMAP mail server leaks information about its version.

Finding: The Cyrus POP3 server leaks information about the software it is running through the login banner. The version of the remote POP3 server is “Cyrus v2.1.13 server.” The IMAP server version is “Cyrus IMAP4 v2.1.13.”

Severity: Low

Impact: The information leakage may assist an attacker in choosing an attack strategy.

Recommendation: None. The normal recommendation would be to change the login banner to something generic. However, removing the vendor and version number requires editing the source code and recompiling Cyrus [20].

4.3.4.3 A valid POP3 account and password were found.

Finding: Numerous “valid” user names and passwords were found.

Severity: False Positive

Impact: This documents the fact that the Nessus plugin for Hydra creates false positives in this situation. Hydra is an open source tool that attempts to “brute force” several internet protocols by sending large number of logon requests to the server.

Manual checks of the user accounts on gala.giac.com showed that none of the accounts that were “found” by Hydra exist.

Recommendation: None.

4.4 Physical and Other

4.4.1 Physical Security.

Finding: Physical security was examined during the site visit. The servers reside in GIAC Enterprises’ server room along with the internal network servers. The server room has four solid walls from floor to roof, i.e., no access route over the walls. The room has does not have a raised floor. Access to the room is through a door that is secured with a mechanical combination lock. The door is monitored 24 x7 by a closed-circuit surveillance camera monitored by the security company responsible for building security. There is no controls placed on who can enter the server room other than knowledge of the combination of the door lock.

Severity: Low

Impact: An attacker could gain access to the room by obtaining the combination to the lock through social engineering or piggy-back on an authorized users opening of the door.

Recommendation: Develop and implement a physical security policy that requires all personnel log entry in to the server room until an electronic system can be installed, personnel should

prevent other personnel from gaining access by piggy-backing into the room. It should also create a list of personnel authorized to enter the server room and have a requirement to that all personnel who are not on the list will be escorted at all times.

4.4.2 Fire Prevention.

Finding: Fire prevention and monitoring system in the GIAC Enterprises' building were adequate with a wet pipe sprinkler system in the server room. The servers and other networking equipment in the server room are mounted in open racks.

Severity: Low

Impact: An inadvertent activation of the sprinkler system in the server room could result in loss of all servers and the network equipment.

Recommendation: Convert the wet pipe sprinkler system to a dry pipe or preaction system if it can be negotiated with the building owner. A preaction system is combination of a wet and dry pipe systems that fills the pipe when heat is sensed (dry pipe) and releases water when the link in the nozzle melts (wet pipe). [4]

© SANS Institute 2004, Author retains full rights

5

This page intentionally left blank

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, Author retains full rights.

6 Summary

Overall, thirty-five findings were identified. Grouping the findings by severity, there were 8 High, 12 Moderate and 12 Low with 3 False Positives. The majority of the findings are related to the configuration of the applications.

The overall breakdown of the findings is presented in Table 7.

Table 7 – Numerical Summary of Findings

Area	High	Moderate	Low	False Positive	Total
Plans and Policies	4	4	2		10
Operating System	1	4	3	2	10
Applications	4	2	8	1	15
Physical and Other			2		2
Total	9	10	15	3	37

The most significant and most time consuming to correct are the Plans and Policies findings. The development of comprehensive documentation is a challenging task. In order to assure that the plans and policies will be embraced at all levels of GIAC Enterprises, the development team will require the involvement of almost all GIAC Enterprises' employees to some degree. Once the development is complete, senior management must wholly adopt and give their full backing to the plans and policies to ensure that they are followed and maintained current.

The majority of the application findings result from not performing a post-installation lock down of the applications. Although, some of the findings about the applications would be corrected when the operating system is upgraded to Mac OS X, v10.3.3, and the latest security updates are applied. Most of the findings directly correspond to the common UNIX vulnerabilities identified in the SANS Top 20 Internet Security Vulnerabilities. Further information on securing the applications, can be found at the SANS Top 20 web site (<http://www.sans.org/top20>).

Additionally, the IT staff will be required to develop and implement backup and configuration management programs for production servers. In the long run this will assist in maintaining the security of GIAC Enterprises' network security. If the patch levels on each system are the same and the security features and the configurations are uniformly applied, this will help the system administrators "know their systems" and recognize problems and identify incidents more rapidly.

This page intentionally left blank

© SANS Institute 2004, Author retains full rights.

ANNEX A – REFERENCES

- [1] National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 199, “Standards for Security Categorization of Federal Information and Information Systems.” February 2004.
<http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>
- [2] Public Law (P.L.) 107-347, The E-Government Act of 2002, Title III, Information Security, Commonly known as the Federal Information Security Management Act of 2002 (FISMA).<http://www.fedcirc.gov/library/legislation/FISMA.html>
- [3] The SANS/FBI Top 20 Internet Security Vulnerabilities, <http://www.sans.org/top20>
- [4] The CISSP Prep Guide, Gold Edition. R. L. Krutz, R. D. Vines, Wiley Publishing, Inc, Indianapolis, IN, 2003
- [5] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, “Contingency Planning Guide for Information Technology Systems,” June 2002.
<http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf>
- [6] DRI International (DRII), April 26, 2004, <http://www.drii.org>.
- [7] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, “Computer Security Incident Handling Guide,” January 2004.
<http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>
- [8] SANS Security Essentials with CISSP CBK, Version 2.1. E. Cole, et al, SANS Press, 2003
- [9] The SANS Security Policy Project, <http://www.sans.org/resources/policies/>
- [10] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-14, “Generally Accepted Principles and Practices for Securing Information Technology Systems,” September 1996. <http://csrc.nist.gov/publications/nistpubs/800-14/sp800-14.pdf>
- [11] “NIH Policy on Warning Banners,” Center for Information Technology, National Institutes of Health (NIH), December 18, 2003,
<http://www.oir.nih.gov/policy/warnbanners.html>.
- [12] Children's Online Privacy Protection Act of 1998, 6 C.F.R. Part 312,
http://www.access.gpo.gov/nara/cfr/waisidx_03/16cfr312_03.html
- [13] Mac OS X Server Combined Update 10.3.3, Apple Computer, Inc., March 16, 2003,
<http://www.apple.com/support/downloads/macossxservercombinedupdate.html>.
- [14] Security Update 2004-04-05 (10.3.3), Apple Computer, Inc., April 5 2004,
[http://www.apple.com/support/downloads/securityupdate_2004-04-05_\(10_3_3\).html](http://www.apple.com/support/downloads/securityupdate_2004-04-05_(10_3_3).html).
- [15] Apple Product Security, Apple Computer, Inc., April 27, 2004,
<http://www.info.apple.com/usen/security/index.html>.
- [16] Apple Security Updates, Apple Computer Knowledgebase Article ID 61798, Apple Computer, Inc., April 6, 2004, <http://docs.info.apple.com/article.html?artnum=61798>.

SECURITY INFORMATION

- [17] Pwpolicy Man Page, Apple Computer, Inc., April 27, 2004, <http://developer.apple.com/documentation/Darwin/Reference/ManPages/html/pwpolicy.8.html>.
- [18] "More security problems in Apache on Mac OS X," Jacques Distler, Aug 8, 2001, <http://www.macintouch.com/mosxreaderreports46.html>.
- [19] mod_ssl User Manual, The Apache Interface to OpenSSL, Ralf S. Engelschall, 2001 http://www.modssl.org/docs/2.8/ssl_reference.html.
- [20] "The Great Big Mac OS X Panther Server and SSL article," Joel Rennich, December 16, 2003, <http://www.afp548.com/Articles/Panther/sslinfo.html>.
- [21] "Re: removing banners from cyrus," Info-Cyrus Mailing List, Clifford Thurber, April 2 2002, <http://asg.web.cmu.edu/archive/message.php?mailbox=archive.info-cyrus&msg=13486>.

© SANS Institute 2004, Author retains full rights.

ANNEX B – ACRONYMS

AO	Authorizing Official
C&A	Certification and Authorization
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CIS	Center for Internet Security
DB	Database
DBA	Database Administrator
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act of 2002
I&A	Identification and Authentication
IP	Internet Protocol
IPSEC	Internet Protocol Security
IT	Information Technology
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OS	Operating System
SA	System Administrator
SAIC	Science Applications International Corporation
SP	Service Pack or Special Publication

© SANS Institute 2004, Author retains full rights.

This page intentionally left blank

© SANS Institute 2004, Author retains full rights.

ANNEX C – NESSUS RESULTS

Nessus Scan Report

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

Scan Details

Hosts which were alive and responding during test	2
Number of security holes found	755
Number of security warnings found	8

Host List

Host(s)	Possible Issue
crispin.giac.com	Security hole(s) found
gala.giac.com	Security hole(s) found

[\[return to top \]](#)

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
crispin.giac.com	ssh (22/tcp)	Security hole found
crispin.giac.com	ftp (21/tcp)	Security notes found
crispin.giac.com	http (80/tcp)	Security hole found
crispin.giac.com	pop3pw (106/tcp)	Security hole found
crispin.giac.com	asip-webadmin (311/tcp)	Security hole found
crispin.giac.com	svrloc (427/tcp)	No Information
crispin.giac.com	general/tcp	Security hole found
crispin.giac.com	general/udp	Security notes found
crispin.giac.com	ntp (123/udp)	Security notes found

Security Issues and Fixes: crispin.giac.com

Type	Port	Issue and Fix
Vulnerability	ssh (22/tcp)	<p>You are running a version of OpenSSH which is older than 3.7.1</p> <p>Versions older than 3.7.1 are vulnerable to a flaw in the buffer management functions which might allow an attacker to execute arbitrary commands on this host.</p> <p>An exploit for this issue is rumored to exist.</p>

SECURITY INFORMATION

Note that several distribution patched this hole without changing the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.

If you are running a RedHat host, make sure that the command :
rpm -q openssh-server

Returns :
openssh-server-3.1p1-13 (RedHat 7.x)
openssh-server-3.4p1-7 (RedHat 8.0)
openssh-server-3.5p1-11 (RedHat 9)

Solution : Upgrade to OpenSSH 3.7.1

See also : <http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375452423794&w=2>
<http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375456923804&w=2>

Risk factor : High

CVE : [CAN-2003-0682](#), [CAN-2003-0693](#), [CAN-2003-0695](#)

BID : [8628](#)

Other references : RHSA:RHSA-2003:279-02, SuSE:SUSE-SA:2003:039

Nessus ID : [11837](#)

Warning ssh (22/tcp)

You are running OpenSSH-portable 3.6.1p1 or older.

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

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

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

Solution : Upgrade to OpenSSH-portable 3.6.1p2 or newer

Risk Factor : Low

CVE : [CAN-2003-0190](#)

BID : [7482](#), [7467](#), [7342](#)

Other references : RHSA:RHSA-2003:222-01

Nessus ID : [11574](#)

Informational ssh (22/tcp)

An ssh server is running on this port

Nessus ID : [10330](#)

Informational ssh (22/tcp)

Remote SSH version : SSH-2.0-OpenSSH_3.6.1p1+CAN-2003-0693

Nessus ID : [10267](#)

Informational ssh (22/tcp)

The remote SSH daemon supports the following versions of the SSH protocol :

. 1.99
. 2.0

Nessus ID : [10881](#)

Informational ftp (21/tcp)

An unknown service is running on this port.

It is usually reserved for FTP

Nessus ID : [10330](#)

Vulnerability http (80/tcp)

The remote host appears to be running a version of Apache which is older than 1.3.29

There are several flaws in this version, which may allow an attacker to possibly execute arbitrary code through mod_alias and mod_rewrite.

SECURITY INFORMATION

		<p>You should upgrade to 1.3.29 or newer.</p> <p>*** Note that Nessus solely relied on the version number *** of the remote server to issue this warning. This might *** be a false positive</p> <p>Solution : Upgrade to version 1.3.29 See also : http://www.apache.org/dist/httpd/Announcement.html Risk factor : High CVE : CAN-2003-0542 Nessus ID : 11915</p>
Vulnerability	http (80/tcp)	<p>MacOS X creates a hidden file, '.DS_Store' in each directory that has been viewed with the 'Finder'. This file contains a list of the contents of the directory, giving an attacker information on the structure and contents of your website.</p> <p>Solution: Use a <FilesMatch> directive in httpd.conf to forbid retrieval of this file:</p> <pre><FilesMatch '^\. [Dd][Ss]_[Ss]'\> Order allow, deny Deny from all </FilesMatch></pre> <p>and restart Apache.</p> <p>Risk factor : Medium / High (depending on the sensitivity of your web content)</p> <p>References:</p> <p>www.macintouch.com/mosxreaderreports46.html</p> <p>BID : 3316 Nessus ID : 10756</p>
Warning	http (80/tcp)	<p>Requesting the URI /server-status gives information about the currently running Apache.</p> <p>Risk factor : Low Solution : If you don't use this feature, comment the appropriate section in your httpd.conf file. If you really need it, limit its access to the administrator's machine. Nessus ID : 10677</p>
Warning	http (80/tcp)	<p>The following files are calling the function phpinfo() which disclose potentially sensitive information to the remote attacker :</p> <pre>/info.php /test/phpinfo.php /test/info.php /info/phpinfo.php /info/info.php</pre> <p>Solution : Delete them or restrict access to them Risk factor : Low Nessus ID : 11229</p>
Informational	http (80/tcp)	<p>A web server is running on this port Nessus ID : 10330</p>
Informational	http (80/tcp)	<p>The following directories were discovered: <code>/cgi-bin, /icons, /info, /manual, /new, /server-status, /source, /template, /test</code></p> <p>While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards</p>

SECURITY INFORMATION

	Nessus ID : 11032
Informational http (80/tcp)	The following CGI have been discovered : Syntax : cginame (arguments [default value]) /source.php (page_url [example.2-1.php]) Nessus ID : 10662
Informational http (80/tcp)	Nessus was not able to exactly identify this server. It might be: Apache/1.3.27 (Darwin) The fingerprint differs from these known signatures on 1 point(s) If you know what this server is and if you are using an up to date version of this script, please send this signature to www-signatures@nessus.org : HTM:200:200:200:400:400:---:501:400:---:---:---:---:400:400:400:404: \ 405:404:200:403:404:501:---:Apache/1.3.28 (Darwin) PHP/4.3.4 mod_jk/ \ 1.2.4 mod_ssl/2.8.15 OpenSSL/0.9.7b Including these headers: ETag: "12693-95a-3ee65c06" Try to provide as much information as you can: software & operating release, sub-version, patch numbers, and specific configuration option, if any. Nessus ID : 11919
Informational http (80/tcp)	The remote web server type is : Apache/1.3.28 (Darwin) PHP/4.3.4 mod_jk/1.2.4 mod_ssl/2.8.15 OpenSSL/0.9.7b Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers. Nessus ID : 10107
Informational http (80/tcp)	An information leak occurs on Apache based web servers whenever the UserDir module is enabled. The vulnerability allows an external attacker to enumerate existing accounts by requesting access to their home directory and monitoring the response. Solution: 1) Disable this feature by changing 'UserDir public_html' (or whatever) to 'UserDir disabled'. Or 2) Use a RedirectMatch rewrite rule under Apache -- this works even if there is no such entry in the password file, e.g.: RedirectMatch ^/~(.*)\$ http://my-target-webserver.somewhere.org/\$1 Or 3) Add into httpd.conf: ErrorDocument 404 http://localhost/sample.html ErrorDocument 403 http://localhost/sample.html (NOTE: You need to use a FQDN inside the URL for it to work properly). Additional Information: http://www.securiteam.com/unixfocus/5WP0C1F5FI.html Risk factor : Low CVE : CAN-2001-1013 BID : 3335 Nessus ID : 10766
Vulnerability pop3pw	A valid pop3 account has been found by brute force :

SECURITY INFORMATION

	(106/tcp)	login: 1 password: AMISSETUP
		Solution: Use strong passwords and difficult to guess usernames Risk factor : High CVE : CAN-1999-0502 , CAN-1999-0505 , CAN-1999-0516 , CAN-1999-0518 Nessus ID : 10909
Vulnerability	pop3pw (106/tcp)	A valid pop3 account has been found by brute force : login: VM3812 password: accounting
		Solution: Use strong passwords and difficult to guess usernames Risk factor : High CVE : CAN-1999-0502 , CAN-1999-0505 , CAN-1999-0516 , CAN-1999-0518 Nessus ID : 10909
Informational	pop3pw (106/tcp)	A pop3 server is running on this port Nessus ID : 10330
Informational	pop3pw (106/tcp)	The remote POP3 servers leak information about the software it is running, through the login banner. This may assist an attacker in choosing an attack strategy.
		Versions and types should be omitted where possible.
		The version of the remote POP3 server is : +OK ApplePasswordServer 10.1.0.0 password server at 192.168.11.202 ready
		Solution : Change the login banner to something generic. Risk factor : Low Nessus ID : 10185
Vulnerability	asip- webadmin (311/tcp)	The remote host seem to be running a version of OpenSSL which is older than 0.9.6k or 0.9.7c. There is a heap corruption bug in this version which might be exploited by an attacker to gain a shell on this host.
		Solution : If you are running OpenSSL, Upgrade to version 0.9.6k or 0.9.7c or newer Risk factor : High CVE : CVE-2003-0543 , CVE-2003-0544 , CVE-2003-0545 BID : 8732 Other references : IAVA:2003-A-0027, RHSA:RHSA-2003:291-01, SuSE:SUSE-SA:2003:043 Nessus ID : 11875
Vulnerability	asip- webadmin (311/tcp)	The remote host appears to be running a version of Apache which is older than 1.3.29 There are several flaws in this version, which may allow an attacker to possibly execute arbitrary code through mod_alias and mod_rewrite. You should upgrade to 1.3.29 or newer. *** Note that Nessus solely relied on the version number *** of the remote server to issue this warning. This might *** be a false positive
		Solution : Upgrade to version 1.3.29 See also : http://www.apache.org/dist/httpd/Announcement.html Risk factor : High CVE : CAN-2003-0542 Nessus ID : 11915
Vulnerability	asip- webadmin (311/tcp)	The remote host appears to be running a version of Apache which is older than 1.3.28

SECURITY INFORMATION

		<p>There are several flaws in this version, which may allow an attacker to disable the remote server remotely. You should upgrade to 1.3.28 or newer.</p> <p>*** Note that Nessus solely relied on the version number *** of the remote server to issue this warning. This might *** be a false positive</p> <p>Solution : Upgrade to version 1.3.28 See also : http://www.apache.org/dist/httpd/Announcement.html Risk factor : High CVE : CAN-2003-0460, CAN-2002-0061 BID : 8226 Nessus ID : 11793</p>
Warning	asip-webadmin (311/tcp)	<p>The SSLv2 server offers 5 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack</p> <p>Solution: disable those ciphers and upgrade your client software if necessary Nessus ID : 10863</p>
Informational	asip-webadmin (311/tcp)	<p>A SSLv2 server answered on this port Nessus ID : 10330</p>
Informational	asip-webadmin (311/tcp)	<p>A web server is running on this port through SSL Nessus ID : 10330</p>
Informational	asip-webadmin (311/tcp)	<p>Nessus was not able to exactly identify this server. It might be: Apache/1.3.27 (Unix) The fingerprint differs from these known signatures on 3 point(s)</p> <p>If you know what this server is and if you are using an up to date version of this script, please send this signature to www-signatures@nessus.org : HTM:200:200:200:400:400:HTM:200:400:200:HTM:HTM:200:400:400:400: \ 400:200:200:200:200:200:200:200:200:Apache/1.3.27 (Darwin) mod_ssl/ \ 2.8.12 OpenSSL/0.9.7b</p> <p>Try to provide as much information as you can: software & operating release, sub-version, patch numbers, and specific configuration option, if any. Nessus ID : 11919</p>
Informational	asip-webadmin (311/tcp)	<p>The remote web server type is : Apache/1.3.27 (Darwin) mod_ssl/2.8.12 OpenSSL/0.9.7b</p>
Informational	asip-webadmin (311/tcp)	<p>Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers. Nessus ID : 10107</p>
Informational	asip-webadmin (311/tcp)	<p>Here is the SSLv2 server certificate: Certificate: Data: Version: 3 (0x2) Serial Number: 0 (0x0) Signature Algorithm: md5WithRSAEncryption Issuer: C=US, ST=California, L=Cupertino, O=Apple Computer, Inc., OU=iServers, CN=www.example.com/emailAddress=webmaster@example.com Validity Not Before: Aug 24 21:01:59 2001 GMT Not After : Aug 25 21:01:59 2001 GMT Subject: C=US, ST=California, L=Cupertino, O=Apple Computer, Inc., OU=iServers,</p>

SECURITY INFORMATION

		<p>CN=www.example.com/emailAddress=webmaster@example.com Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:99:07:0e:df:03:95:b6:2e:f4:50:0d:83:46:6e: b5:84:67:1b:b7:6b:b1:2b:05:2c:27:13:b7:bd:9f: 29:30:67:49:6e:ea:98:9d:a9:af:32:2a:9e:6c:59: 12:e1:e5:6b:83:13:74:de:1e:0b:4b:8c:28:23:fc: 7c:eb:91:92:1e:54:39:f7:c3:28:a9:25:78:86:bf: 06:03:76:bd:4c:92:20:94:da:6d:f0:76:2f:92:ae: 6d:40:7e:48:6c:f2:5e:2f:1e:5f:00:db:b8:9d:ce: b1:a2:60:c6:b1:f9:69:d7:45:b0:1a:e8:e5:25:ca: f3:22:23:6a:42:a5:a2:56:8b Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Subject Key Identifier: F7:7C:AB:1A:C3:96:8B:8F:5C:19:EE:78:E6:FC:EE:18:9B:4A:3F:CD X509v3 Authority Key Identifier: keyid:F7:7C:AB:1A:C3:96:8B:8F:5C:19:EE:78:E6:FC:EE:18:9B:4A:3F:CD DirName:/C=US/ST=California/L=Cupertino/O=Apple Computer, Inc./OU=iServers/CN=www.example.com/emailAddress=webmaster@example.com serial:00</p> <p>X509v3 Basic Constraints: CA:TRUE Signature Algorithm: md5WithRSAEncryption 25:5b:1b:7d:8f:4d:3d:7b:8a:a8:2e:3b:a2:09:9e:ef:2e:41: 04:93:70:c4:ae:56:89:e0:a8:24:e8:a3:f7:b5:88:1c:ad:e0: 0d:ec:49:de:d3:1b:1e:7c:86:ca:5d:1f:5c:7b:08:4d:5c:5e: 08:04:e8:1e:49:e0:0c:07:03:66:10:b5:8c:79:ce:8c:d2:c9: 55:b8:43:37:72:91:48:d1:c3:53:2f:9f:df:b3:54:f1:e7:55: e8:0a:ed:bf:f7:a5:74:d4:6c:c3:aa:51:f1:e6:c4:a2:86:e7: d3:2b:16:db:02:84:9d:51:58:a0:13:8f:0e:5a:51:5a:c0:d5: 8b:3d</p> <p>Nessus ID : 10863</p>
Informational	asip-webadmin (311/tcp)	<p>Here is the list of available SSLv2 ciphers: RC4-MD5 EXP-RC4-MD5 RC2-CBC-MD5 EXP-RC2-CBC-MD5 DES-CBC-MD5 DES-CBC3-MD5 RC4-64-MD5 Nessus ID : 10863</p>
Informational	asip-webadmin (311/tcp)	<p>This SSLv2 server also accepts SSLv3 connections. This SSLv2 server also accepts TLSv1 connections. Nessus ID : 10863</p>
Vulnerability	general/tcp	<p>A valid 106 account has been found by brute force : [pop3] login: 1 password: AMIAMI</p> <p>Solution: Use strong passwords and difficult to guess usernames Risk factor : High CVE : CAN-1999-0502, CAN-1999-0505, CAN-1999-0516, CAN-1999-0518 Nessus ID : 10909</p>
Informational	general/tcp	<p>Nmap found that this host is running Apple Mac OS X 10.3.0 - 10.3.2 (Panther) Nessus ID : 10336</p>
Informational	general/tcp	<p>HTTP NIDS evasion functions are enabled. You may get some false negative results Nessus ID : 10890</p>

SECURITY INFORMATION

Informational	general/tcp	Nessus was not able to reliably identify the remote operating system. It might be: MacOS X 10.3 The fingerprint differs from these known signatures on 1 points. If you know what operating system this host is running, please send this signature to os-signatures@nessus.org : :1:1:1:64:0:64:1:0:64:1:0:64:1:8:64:1:1:0:1:1:1:1:1:1:64:33304:MNWNNT:0:1:1 Nessus ID : 11936
Informational	general/udp	For your information, here is the traceroute to 192.168.11.202 : 192.168.11.199 192.168.11.202 Nessus ID : 10287
Informational	ntp (123/udp)	It is possible to determine a lot of information about the remote host by querying the NTP (Network Time Protocol) variables - these include OS descriptor, and time settings. It was possible to gather the following information from the remote NTP host : version='ntpd 4.1.1@1.786 Fri Sep 12 18:30:03 PDT 2003 (1)', processor='Power Macintosh', system='Darwin7.0.0', leap=3, stratum=16, precision=-18, rootdelay=0.000, rootdispersion=79.680, peer=0, refid=0.0.0.0, reftime=0x00000000.00000000, poll=4, clock=0xc401f4b5.468ab4fa, state=0, offset=0.000, frequency=0.000, jitter=0.004, stability=0.000 Quickfix: Set NTP to restrict default access to ignore all info packets: restrict default ignore Risk factor : Low Nessus ID : 10884

[\[return to top \]](#)

Analysis of Host		
Address of Host	Port/Service	Issue regarding Port
gala.giac.com	smtp (25/tcp)	Security notes found
gala.giac.com	ssh (22/tcp)	Security hole found
gala.giac.com	domain (53/tcp)	Security warning(s) found
gala.giac.com	pop3pw (106/tcp)	Security notes found
gala.giac.com	pop3 (110/tcp)	Security notes found
gala.giac.com	imap (143/tcp)	Security notes found
gala.giac.com	asip-webadmin (311/tcp)	Security hole found
gala.giac.com	svrloc (427/tcp)	No Information
gala.giac.com	general/tcp	Security notes found
gala.giac.com	domain (53/udp)	Security notes found
gala.giac.com	general/udp	Security notes found
gala.giac.com	ntp (123/udp)	Security notes found

Security Issues and Fixes: gala.giac.com

SECURITY INFORMATION

Type	Port	Issue and Fix
Informational	smtp (25/tcp)	An SMTP server is running on this port Here is its banner : 220 gala.giac.com ESMTP Postfix Nessus ID : 10330
Informational	smtp (25/tcp)	Remote SMTP server banner : 220 gala.giac.com ESMTP Postfix This is probably: Postfix Nessus ID : 10263
Informational	smtp (25/tcp)	This server could be fingerprinted as being Postfix Nessus ID : 11421
Vulnerability	ssh (22/tcp)	You are running a version of OpenSSH which is older than 3.7.1 Versions older than 3.7.1 are vulnerable to a flaw in the buffer management functions which might allow an attacker to execute arbitrary commands on this host. An exploit for this issue is rumored to exist. Note that several distributions patched this hole without changing the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive. If you are running a RedHat host, make sure that the command : rpm -q openssh-server Returns : openssh-server-3.1p1-13 (RedHat 7.x) openssh-server-3.4p1-7 (RedHat 8.0) openssh-server-3.5p1-11 (RedHat 9) Solution : Upgrade to OpenSSH 3.7.1 See also : http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375452423794&w=2 http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375456923804&w=2 Risk factor : High CVE : CAN-2003-0682 , CAN-2003-0693 , CAN-2003-0695 BID : 8628 Other references : RHSA:RHSA-2003:279-02, SuSE:SUSE-SA:2003:039 Nessus ID : 11837
Warning	ssh (22/tcp)	You are running OpenSSH-portable 3.6.1p1 or older. If PAM support is enabled, an attacker may use a flaw in this version to determine the existence of a given login name by comparing the times the remote sshd daemon takes to refuse a bad password for a non-existent login compared to the time it takes to refuse a bad password for a valid login. An attacker may use this flaw to set up a brute force attack against the remote host. *** Nessus did not check whether the remote SSH daemon is actually using PAM or not, so this might be a false positive Solution : Upgrade to OpenSSH-portable 3.6.1p2 or newer Risk Factor : Low CVE : CAN-2003-0190

SECURITY INFORMATION

		<p>BID : 7482, 7467, 7342 Other references : RHSA:RHSA-2003:222-01 Nessus ID : 11574</p>
Informational	ssh (22/tcp)	<p>An ssh server is running on this port Nessus ID : 10330</p>
Informational	ssh (22/tcp)	<p>Remote SSH version : SSH-2.0-OpenSSH_3.6.1p1+CAN-2003-0693 Nessus ID : 10267</p>
Informational	ssh (22/tcp)	<p>The remote SSH daemon supports the following versions of the SSH protocol :</p> <ul style="list-style-type: none">. 1.99. 2.0 <p>Nessus ID : 10881</p>
Warning	domain (53/tcp)	<p>The remote name server allows DNS zone transfers to be performed. A zone transfer will allow the remote attacker to instantly populate a list of potential targets. In addition, companies often use a naming convention which can give hints as to a servers primary application (for instance, proxy.company.com, payroll.company.com, b2b.company.com, etc.).</p> <p>As such, this information is of great use to an attacker who may use it to gain information about the topology of your network and spot new targets.</p> <p>Solution: Restrict DNS zone transfers to only the servers that absolutely need it.</p> <p>Risk factor : Medium CVE : CAN-1999-0532 Nessus ID : 10595</p>
Warning	domain (53/tcp)	<p>The remote name server allows recursive queries to be performed by the host running nssusd.</p> <p>If this is your internal nameserver, then forget this warning.</p> <p>If you are probing a remote nameserver, then it allows anyone to use it to resolve third parties names (such as www.nessus.org). This allows hackers to do cache poisoning attacks against this nameserver.</p> <p>If the host allows these recursive queries via UDP, then the host can be used to 'bounce' Denial of Service attacks against another network or system.</p> <p>See also : http://www.cert.org/advisories/CA-1997-22.html</p> <p>Solution : Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it).</p> <p>If you are using bind 8, you can do this by using the instruction 'allow-recursion' in the 'options' section of your named.conf</p> <p>If you are using bind 9, you can define a grouping of internal addresses using the 'acl' command</p> <p>Then, within the options block, you can explicitly state: 'allow-recursion { hosts_defined_in_acl }'</p> <p>For more info on Bind 9 administration (to include recursion), see: http://www.nominum.com/content/documents/bind9arm.pdf</p> <p>If you are using another name server, consult its documentation.</p>

SECURITY INFORMATION

		Risk factor : Serious CVE : CVE-1999-0024 BID : 678 Nessus ID : 10539
Informational	domain (53/tcp)	A DNS server is running on this port. If you do not use it, disable it.
		Risk factor : Low Nessus ID : 11002
Informational	domain (53/tcp)	BIND 'NAMED' is an open-source DNS server from ISC.org. Many proprietary DNS servers are based on BIND source code. The BIND based NAMED servers (or DNS servers) allow remote users to query for version and type information. The query of the CHAOS TXT record 'version.bind', will typically prompt the server to send the information back to the querying source. The remote bind version is : 9.2.2 Solution : Using the 'version' directive in the 'options' section will block the 'version.bind' query, but it will not log such attempts. Nessus ID : 10028
Informational	pop3pw (106/tcp)	A pop3 server is running on this port Nessus ID : 10330
Informational	pop3pw (106/tcp)	The remote POP3 servers leak information about the software it is running, through the login banner. This may assist an attacker in choosing an attack strategy. Versions and types should be omitted where possible. The version of the remote POP3 server is : +OK ApplePasswordServer 10.1.0.0 password server at gala.giac.com ready Solution : Change the login banner to something generic. Risk factor : Low Nessus ID : 10185
Informational	pop3 (110/tcp)	A pop3 server is running on this port Nessus ID : 10330
Informational	pop3 (110/tcp)	The remote POP3 servers leak information about the software it is running, through the login banner. This may assist an attacker in choosing an attack strategy. Versions and types should be omitted where possible. The version of the remote POP3 server is : +OK gala.giac.com Cyrus v2.1.13 server ready Solution : Change the login banner to something generic. Risk factor : Low Nessus ID : 10185
Informational	imap (143/tcp)	An IMAP server is running on this port Nessus ID : 10330
Informational	imap (143/tcp)	The remote imap server banner is : * OK gala.giac.com Cyrus IMAP4 v2.1.13 server ready Versions and types should be omitted where possible. Change the imap banner to something generic. Nessus ID : 11414

SECURITY INFORMATION

Vulnerability	asip-webadmin (311/tcp)	<p>The remote host seem to be running a version of OpenSSL which is older than 0.9.6k or 0.9.7c.</p> <p>There is a heap corruption bug in this version which might be exploited by an attacker to gain a shell on this host.</p> <p>Solution : If you are running OpenSSL, Upgrade to version 0.9.6k or 0.9.7c or newer Risk factor : High CVE : CVE-2003-0543, CVE-2003-0544, CVE-2003-0545 BID : 8732 Other references : IAVA:2003-A-0027, RHSA:RHSA-2003:291-01, SuSE:SUSE-SA:2003:043 Nessus ID : 11875</p>
Vulnerability	asip-webadmin (311/tcp)	<p>The remote host appears to be running a version of Apache which is older than 1.3.29</p> <p>There are several flaws in this version, which may allow an attacker to possibly execute arbitrary code through mod_alias and mod_rewrite.</p> <p>You should upgrade to 1.3.29 or newer.</p> <p>*** Note that Nessus solely relied on the version number *** of the remote server to issue this warning. This might *** be a false positive</p> <p>Solution : Upgrade to version 1.3.29 See also : http://www.apache.org/dist/httpd/Announcement.html Risk factor : High CVE : CAN-2003-0542 Nessus ID : 11915</p>
Vulnerability	asip-webadmin (311/tcp)	<p>The remote host appears to be running a version of Apache which is older than 1.3.28</p> <p>There are several flaws in this version, which may allow an attacker to disable the remote server remotely. You should upgrade to 1.3.28 or newer.</p> <p>*** Note that Nessus solely relied on the version number *** of the remote server to issue this warning. This might *** be a false positive</p> <p>Solution : Upgrade to version 1.3.28 See also : http://www.apache.org/dist/httpd/Announcement.html Risk factor : High CVE : CAN-2003-0460, CAN-2002-0061 BID : 8226 Nessus ID : 11793</p>
Warning	asip-webadmin (311/tcp)	<p>The SSLv2 server offers 5 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack</p> <p>Solution: disable those ciphers and upgrade your client software if necessary Nessus ID : 10863</p>
Informational	asip-webadmin (311/tcp)	<p>A SSLv2 server answered on this port Nessus ID : 10330</p>
Informational	asip-webadmin (311/tcp)	<p>A web server is running on this port through SSL Nessus ID : 10330</p>
Informational	asip-	<p>Here is the SSLv2 server certificate:</p>

SECURITY INFORMATION

	webadmin (311/tcp)	Certificate: Data: Version: 3 (0x2) Serial Number: 0 (0x0) Signature Algorithm: md5WithRSAEncryption Issuer: C=US, ST=California, L=Cupertino, O=Apple Computer, Inc., OU=iServers, CN=www.example.com/emailAddress=webmaster@example.com Validity Not Before: Aug 24 21:01:59 2001 GMT Not After : Aug 25 21:01:59 2001 GMT Subject: C=US, ST=California, L=Cupertino, O=Apple Computer, Inc., OU=iServers, CN=www.example.com/emailAddress=webmaster@example.com Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:99:07:0e:df:03:95:b6:2e:f4:50:0d:83:46:6e: b5:84:67:1b:b7:6b:b1:2b:05:2c:27:13:b7:bd:9f: 29:30:67:49:6e:ea:98:9d:a9:af:32:2a:9e:6c:59: 12:e1:e5:6b:83:13:74:de:1e:0b:4b:8c:28:23:fc: 7c:eb:91:92:1e:54:39:f7:c3:28:a9:25:78:86:bf: 06:03:76:bd:4c:92:20:94:da:6d:f0:76:2f:92:ae: 6d:40:7e:48:6c:f2:5e:2f:1e:5f:00:db:b8:9d:ce: b1:a2:60:c6:b1:f9:69:d7:45:b0:1a:e8:e5:25:ca: f3:22:23:6a:42:a5:a2:56:8b Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Subject Key Identifier: F7:7C:AB:1A:C3:96:8B:8F:5C:19:EE:78:E6:FC:EE:18:9B:4A:3F:CD X509v3 Authority Key Identifier: keyid:F7:7C:AB:1A:C3:96:8B:8F:5C:19:EE:78:E6:FC:EE:18:9B:4A:3F:CD DirName:/C=US/ST=California/L=Cupertino/O=Apple Computer, Inc./OU=iServers/CN=www.example.com/emailAddress=webmaster@example.com serial:00 X509v3 Basic Constraints: CA:TRUE Signature Algorithm: md5WithRSAEncryption 25:5b:1b:7d:8f:4d:3d:7b:8a:a8:2e:3b:a2:09:9e:ef:2e:41: 04:93:70:c4:ae:56:89:e0:a8:24:e8:a3:f7:b5:88:1c:ad:e0: 0d:ec:49:de:d3:1b:1e:7c:86:ca:5d:1f:5c:7b:08:4d:5c:5e: 08:04:e8:1e:49:e0:0c:07:03:66:10:b5:8c:79:ce:8c:d2:c9: 55:b8:43:37:72:91:48:d1:c3:53:2f:9f:df:b3:54:f1:e7:55: e8:0a:ed:bf:f7:a5:74:d4:6c:c3:aa:51:f1:e6:c4:a2:86:e7: d3:2b:16:db:02:84:9d:51:58:a0:13:8f:0e:5a:51:5a:c0:d5: 8b:3d Nessus ID : 10863
Informational	asip- webadmin (311/tcp)	Here is the list of available SSLv2 ciphers: RC4-MD5 EXP-RC4-MD5 RC2-CBC-MD5 EXP-RC2-CBC-MD5 DES-CBC-MD5 DES-CBC3-MD5 RC4-64-MD5 Nessus ID : 10863
Informational	asip- webadmin (311/tcp)	This SSLv2 server also accepts SSLv3 connections. This SSLv2 server also accepts TLSv1 connections. Nessus ID : 10863
Informational	asip- webadmin (311/tcp)	Nessus was not able to exactly identify this server. It might be: Apache/1.3.27 (Unix) The fingerprint differs from these known signatures on 3 point(s)

SECURITY INFORMATION

		Risk factor : Low Nessus ID : 11002
Informational	domain (53/udp)	The remote name server could be fingerprinted as being one of the following : ISC BIND 9.2.1 ISC BIND 9.2.2 Nessus ID : 11951
Informational	general/udp	For your information, here is the traceroute to 192.168.11.201 : 192.168.11.199 192.168.11.201 Nessus ID : 10287
Informational	ntp (123/udp)	It is possible to determine a lot of information about the remote host by querying the NTP (Network Time Protocol) variables - these include OS descriptor, and time settings. It was possible to gather the following information from the remote NTP host : version='ntpd 4.1.1@1.786 Fri Sep 12 18:30:03 PDT 2003 (1)', processor='Power Macintosh', system='Darwin7.0.0', leap=3, stratum=16, precision=-17, rootdelay=0.000, rootdispersion=715.545, peer=0, refid=0.0.0.0, reftime=0x00000000.00000000, poll=4, clock=0xc4029cb0.c51c0874, state=0, offset=0.000, frequency=0.000, jitter=0.008, stability=0.000 Quickfix: Set NTP to restrict default access to ignore all info packets: restrict default ignore Risk factor : Low Nessus ID : 10884

This file was generated by [Nessus](#), the open-sourced security scanner.

This page intentionally left blank

© SANS Institute 2004, Author retains full rights.

ANNEX D – NMAP RESULTS

```
# nmap 3.50 scan initiated wed mar 24 19:15:23
2004 as: nmap -ss -sr -sv -o -pi -pt -t4 -oa
/users/smithrd/giac.com/nmap-
20040324/giac.com_external 192.168.11.201
192.168.11.202
```

Interesting ports on 192.168.11.201:
(The 1386 ports scanned but not shown below
are in state: closed)

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

18/tcp	filtered	misp	
20/tcp	filtered	ftp-data	
22/tcp	open	ssh	OpenSSH 3.6.1p1+CAN-2003-0693 (protocol 2.0)
25/tcp	open	smtp	Postfix smtpd
33/tcp	filtered	dsp	
36/tcp	filtered	unknown	
42/tcp	filtered	nameserver	
43/tcp	filtered	whois	
46/tcp	filtered	mpm-snd	
47/tcp	filtered	ni-ftp	
50/tcp	filtered	re-mail-ck	
51/tcp	filtered	la-maint	
52/tcp	filtered	xns-time	
53/tcp	open	domain	ISC Bind 9.2.2
54/tcp	filtered	xns-ch	
55/tcp	filtered	isi-gl	
77/tcp	filtered	priv-rje	
88/tcp	filtered	kerberos-sec	
96/tcp	filtered	dixie	
100/tcp	filtered	newacct	
106/tcp	open	pop3pw	
ApplePasswordServer pop3 password change daemon 10.1.0.0			
109/tcp	filtered	pop2	
110/tcp	open	pop3	Cyrus pop3d 2.1.13
112/tcp	filtered	mcidas	
116/tcp	filtered	ansanotify	
123/tcp	filtered	ntp	
130/tcp	filtered	cisco-fna	
134/tcp	filtered	ingres-net	
141/tcp	filtered	emfis-ctrl	
143/tcp	open	imap	Cyrus IMAP4 server 2.1.13

155/tcp	filtered	netsc-dev	
168/tcp	filtered	rsvd	
172/tcp	filtered	cl-1	
186/tcp	filtered	kis	
188/tcp	filtered	mumps	
200/tcp	filtered	src	
202/tcp	filtered	at-nbp	
233/tcp	filtered	unknown	
234/tcp	filtered	unknown	
236/tcp	filtered	unknown	
247/tcp	filtered	subntbcst_tftp	
263/tcp	filtered	hdap	
264/tcp	filtered	bgmp	
270/tcp	filtered	unknown	
282/tcp	filtered	cableport-ax	
284/tcp	filtered	unknown	
305/tcp	filtered	unknown	
309/tcp	filtered	entrusttime	
311/tcp	open	http	Apache httpd 1.3.27 ((Darwin) mod_ssl/2.8.12 OpenSSL/0.9.7b)
314/tcp	filtered	opalis-robot	
322/tcp	filtered	unknown	
324/tcp	filtered	unknown	
335/tcp	filtered	unknown	
348/tcp	filtered	csi-sgwp	
350/tcp	filtered	matip-type-a	
355/tcp	filtered	datex-asn	
361/tcp	filtered	semantix	
365/tcp	filtered	dtk	
370/tcp	filtered	codaaauth2	
375/tcp	filtered	hassle	
376/tcp	filtered	nip	
377/tcp	filtered	tnETOS	
384/tcp	filtered	arns	
398/tcp	filtered	kryptolan	
399/tcp	filtered	iso-tsap-c2	
401/tcp	filtered	ups	
402/tcp	filtered	genie	
403/tcp	filtered	decap	
406/tcp	filtered	imsp	
408/tcp	filtered	prm-sm	
413/tcp	filtered	smssp	
415/tcp	filtered	bnet	

SECURITY INFORMATION

417/tcp	filtered onmux			700/tcp	filtered unknown
424/tcp	filtered opc-job-track			719/tcp	filtered unknown
427/tcp	open svrloc	Apple	slpd	741/tcp	filtered netgw
431/tcp	filtered utmpcd			763/tcp	filtered cycleserv
433/tcp	filtered nnspp			765/tcp	filtered webster
438/tcp	filtered dsfgw			766/tcp	filtered unknown
444/tcp	filtered snpp			768/tcp	filtered unknown
446/tcp	filtered ddm-rdb			769/tcp	filtered vid
452/tcp	filtered sfs-config			773/tcp	filtered submit
454/tcp	filtered contentserver			779/tcp	filtered unknown
456/tcp	filtered macon-tcp			785/tcp	filtered unknown
461/tcp	filtered datasurfsrv			796/tcp	filtered unknown
494/tcp	filtered pov-ray			816/tcp	filtered unknown
509/tcp	filtered snare			821/tcp	filtered unknown
512/tcp	filtered exec			829/tcp	filtered unknown
522/tcp	filtered ulp			835/tcp	filtered unknown
527/tcp	filtered stx			843/tcp	filtered unknown
531/tcp	filtered conference			861/tcp	filtered unknown
538/tcp	filtered gdomap			867/tcp	filtered unknown
541/tcp	filtered uucp-rlogin			869/tcp	filtered unknown
547/tcp	filtered dhcpv6-server			880/tcp	filtered unknown
551/tcp	filtered cybercash			884/tcp	filtered unknown
560/tcp	filtered rmonitor			887/tcp	filtered unknown
567/tcp	filtered banyan-rpc			894/tcp	filtered unknown
570/tcp	filtered meter			895/tcp	filtered unknown
572/tcp	filtered sonar			897/tcp	filtered unknown
581/tcp	filtered bdp			899/tcp	filtered unknown
582/tcp	filtered scc-security			904/tcp	filtered unknown
583/tcp	filtered philips-vc			906/tcp	filtered unknown
589/tcp	filtered eyelink			914/tcp	filtered unknown
592/tcp	filtered eudora-set			929/tcp	filtered unknown
597/tcp	filtered ptcnameservice			933/tcp	filtered unknown
602/tcp	filtered unknown			934/tcp	filtered unknown
614/tcp	filtered unknown			936/tcp	filtered unknown
621/tcp	filtered unknown			938/tcp	filtered unknown
625/tcp	open unknown			946/tcp	filtered unknown
639/tcp	filtered unknown			950/tcp	filtered oftep-rpc
641/tcp	filtered unknown			953/tcp	filtered rndc
651/tcp	filtered unknown			956/tcp	filtered unknown
661/tcp	filtered unknown			961/tcp	filtered unknown
668/tcp	filtered unknown			969/tcp	filtered unknown
685/tcp	filtered unknown			976/tcp	filtered unknown
687/tcp	open http	Apache	httpd	982/tcp	filtered unknown
1.3.27 ((Darwin) mod_ssl/2.8.12				989/tcp	filtered ftps-data
OpenSSL/0.9.7b)				994/tcp	filtered ircs
699/tcp	filtered unknown			997/tcp	filtered maitrd

SECURITY INFORMATION

998/tcp	filtered busboy	1665/tcp	filtered netview-aix-5
999/tcp	filtered garcon	1669/tcp	filtered netview-aix-9
1002/tcp	filtered windows-icfw	1672/tcp	filtered netview-aix-12
1006/tcp	filtered unknown	1720/tcp	filtered H.323/Q.931
1017/tcp	filtered unknown	1764/tcp	filtered landesk-rc
1018/tcp	filtered unknown	1900/tcp	filtered UPnP
1025/tcp	filtered NFS-or-IIS	1999/tcp	filtered tcp-id-port
1080/tcp	filtered socks	2002/tcp	filtered globe
1109/tcp	filtered kpop	2004/tcp	filtered mailbox
1127/tcp	filtered supfiledbg	2010/tcp	filtered search
1178/tcp	filtered skkserv	2018/tcp	filtered terminaldb
1347/tcp	filtered bbn-mmcc	2025/tcp	filtered ellpack
1349/tcp	filtered sbook	2026/tcp	filtered scrabble
1360/tcp	filtered mimer	2028/tcp	filtered submitserver
1361/tcp	filtered linx	2032/tcp	filtered blackboard
1363/tcp	filtered ndm-requester	2108/tcp	filtered rkinit
1366/tcp	filtered netware-csp	2433/tcp	filtered codasrv-se
1367/tcp	filtered dcs	2564/tcp	filtered hp-3000-telnet
1380/tcp	filtered telesis-licman	2601/tcp	filtered zebra
1397/tcp	filtered audio-activmail	2602/tcp	filtered ripd
1413/tcp	filtered innosys-acl	2903/tcp	filtered extensisportfolio
1416/tcp	filtered novell-lu6.2	3000/tcp	filtered ppp
1423/tcp	filtered essbase	3049/tcp	filtered cfs
1433/tcp	filtered ms-sql-s	3064/tcp	filtered dnet-tstproxy
1435/tcp	filtered ibm-cics	3141/tcp	filtered vmodem
1437/tcp	filtered tabula	3264/tcp	filtered ccmil
1442/tcp	filtered cadis-2	3292/tcp	filtered meetingmaker
1448/tcp	filtered oc-lm	3333/tcp	filtered dec-notes
1449/tcp	filtered peport	3455/tcp	filtered prsvp
1456/tcp	filtered dca	3999/tcp	filtered remoteanything
1457/tcp	filtered valisys-lm	4444/tcp	filtered krb524
1471/tcp	filtered csdmbase	4672/tcp	filtered rfa
1480/tcp	filtered pacerforum	4899/tcp	filtered radmin
1496/tcp	filtered liberty-lm	5102/tcp	filtered admeng
1499/tcp	filtered fhc	5191/tcp	filtered aol-1
1513/tcp	filtered fujitsu-dtc	5192/tcp	filtered aol-2
1522/tcp	filtered rna-lm	5193/tcp	filtered aol-3
1525/tcp	filtered orasrv	5400/tcp	filtered pcduo-old
1531/tcp	filtered rap-listen	5530/tcp	filtered sdserv
1534/tcp	filtered micromuse-lm	5800/tcp	filtered vnc-http
1537/tcp	filtered sdsc-lm	5801/tcp	filtered vnc-http-1
1540/tcp	filtered rds	5803/tcp	filtered vnc-http-3
1547/tcp	filtered laplink	6000/tcp	filtered X11
1549/tcp	filtered shivahose	6002/tcp	filtered X11:2
1650/tcp	filtered nkd	6003/tcp	filtered X11:3
1651/tcp	filtered shiva_confsvr	6106/tcp	filtered isdninfo

SECURITY INFORMATION

6400/tcp filtered crystalreports
8009/tcp filtered ajp13
8080/tcp filtered http-proxy
8082/tcp filtered blackice-alerts
8443/tcp filtered https-alt
11371/tcp filtered pkcsd
13715/tcp filtered VeritasNetbackup
13720/tcp filtered VeritasNetbackup
13782/tcp filtered VeritasNetbackup
15126/tcp filtered swgps
18181/tcp filtered opsec_cvps
18182/tcp filtered opsec_ufp
18185/tcp filtered opsec_omi
22305/tcp filtered wnn6_Kr
27006/tcp filtered flexlm6
27010/tcp filtered flexlm10
32780/tcp filtered sometimes-rpc23
32786/tcp filtered sometimes-rpc25
43188/tcp filtered reachout
Device type: general purpose
Running: Apple Mac OS X 10.3.X
OS details: Apple Mac OS X 10.3.0 - 10.3.2
(Panther)

Interesting ports on 192.168.11.202:
(The 1397 ports scanned but not shown below
are in state: closed)

PORT	STATE	SERVICE	VERSION
18/tcp	filtered	misp	
21/tcp	open	ftp	
22/tcp	open	ssh	OpenSSH 3.6.1p1+CAN-2003-0693 (protocol 2.0)
29/tcp	filtered	msg-icp	
30/tcp	filtered	unknown	
33/tcp	filtered	dsp	
42/tcp	filtered	nameserver	
46/tcp	filtered	mpm-snd	
47/tcp	filtered	ni-ftp	
50/tcp	filtered	re-mail-ck	
51/tcp	filtered	la-maint	
52/tcp	filtered	xns-time	
69/tcp	filtered	tftp	
80/tcp	open	http	Apache httpd 1.3.28 ((Darwin) PHP/4.3.4 mod_jk/1.2.4 mod_ssl/2.8.15 OpenSSL/0.9.7b)
88/tcp	filtered	kerberos-sec	
91/tcp	filtered	mit-dov	
96/tcp	filtered	dixie	
100/tcp	filtered	newacct	
106/tcp	open	pop3pw	ApplePasswordServer pop3 password change daemon 10.1.0.0
109/tcp	filtered	pop2	
110/tcp	filtered	pop3	
123/tcp	filtered	ntp	
132/tcp	filtered	cisco-sys	
134/tcp	filtered	ingres-net	
135/tcp	filtered	msrpc	
144/tcp	filtered	news	
168/tcp	filtered	rsvd	
172/tcp	filtered	cl-1	
173/tcp	filtered	xyplex-mux	
176/tcp	filtered	genrad-mux	
186/tcp	filtered	kis	
188/tcp	filtered	mumps	
202/tcp	filtered	at-nbp	
214/tcp	filtered	vmpwscs	
215/tcp	filtered	softpc	
233/tcp	filtered	unknown	
247/tcp	filtered	subntbcst_tftp	
255/tcp	filtered	unknown	
263/tcp	filtered	hdap	
270/tcp	filtered	unknown	
284/tcp	filtered	unknown	
305/tcp	filtered	unknown	
311/tcp	open	http	Apache httpd 1.3.27 ((Darwin) mod_ssl/2.8.12 OpenSSL/0.9.7b)
319/tcp	filtered	unknown	
325/tcp	filtered	unknown	
329/tcp	filtered	unknown	
339/tcp	filtered	unknown	
346/tcp	filtered	zserv	
359/tcp	filtered	tenebris_nts	
370/tcp	filtered	codaaauth2	
375/tcp	filtered	hassle	
376/tcp	filtered	nip	
377/tcp	filtered	tnETOS	
392/tcp	filtered	synotics-broker	
398/tcp	filtered	kryptolan	
399/tcp	filtered	iso-tsap-c2	
403/tcp	filtered	decap	

SECURITY INFORMATION

409/tcp	filtered prn-nm		685/tcp	filtered unknown	
415/tcp	filtered bnet		687/tcp	open http	Apache httpd
417/tcp	filtered onmux			1.3.27 ((Darwin) mod_ssl/2.8.12	
418/tcp	filtered hyper-g			OpenSSL/0.9.7b)	
425/tcp	filtered icad-el		692/tcp	filtered unknown	
427/tcp	open svrloc	Apple slpd	697/tcp	filtered unknown	
431/tcp	filtered utmpcd		699/tcp	filtered unknown	
438/tcp	filtered dsfgw		700/tcp	filtered unknown	
444/tcp	filtered snpp		713/tcp	filtered unknown	
448/tcp	filtered ddm-ssl		719/tcp	filtered unknown	
454/tcp	filtered contentserver		730/tcp	filtered netviewdm2	
456/tcp	filtered macon-tcp		745/tcp	filtered unknown	
461/tcp	filtered datasurfsrv		764/tcp	filtered omserv	
469/tcp	filtered rcp		765/tcp	filtered webster	
486/tcp	filtered sstats		766/tcp	filtered unknown	
491/tcp	filtered go-login		768/tcp	filtered unknown	
494/tcp	filtered pov-ray		773/tcp	filtered submit	
501/tcp	filtered stmf		775/tcp	filtered entomb	
509/tcp	filtered snare		793/tcp	filtered unknown	
512/tcp	filtered exec		815/tcp	filtered unknown	
522/tcp	filtered ulp		823/tcp	filtered unknown	
530/tcp	filtered courier		829/tcp	filtered unknown	
531/tcp	filtered conference		835/tcp	filtered unknown	
538/tcp	filtered gdomap		843/tcp	filtered unknown	
541/tcp	filtered uucp-rlogin		855/tcp	filtered unknown	
545/tcp	filtered ekshell		867/tcp	filtered unknown	
547/tcp	filtered dhcpv6-server		880/tcp	filtered unknown	
563/tcp	filtered snews		887/tcp	filtered unknown	
567/tcp	filtered banyan-rpc		891/tcp	filtered unknown	
570/tcp	filtered meter		894/tcp	filtered unknown	
572/tcp	filtered sonar		895/tcp	filtered unknown	
579/tcp	filtered decbsrv		897/tcp	filtered unknown	
582/tcp	filtered scc-security		899/tcp	filtered unknown	
583/tcp	filtered philips-vc		901/tcp	filtered samba-swat	
588/tcp	filtered cal		908/tcp	filtered unknown	
589/tcp	filtered eyelink		929/tcp	filtered unknown	
597/tcp	filtered ptcnameservice		933/tcp	filtered unknown	
615/tcp	filtered unknown		934/tcp	filtered unknown	
621/tcp	filtered unknown		938/tcp	filtered unknown	
625/tcp	open unknown		946/tcp	filtered unknown	
634/tcp	filtered ginad		950/tcp	filtered oftep-rpc	
639/tcp	filtered unknown		953/tcp	filtered rndc	
641/tcp	filtered unknown		956/tcp	filtered unknown	
651/tcp	filtered unknown		959/tcp	filtered unknown	
668/tcp	filtered unknown		961/tcp	filtered unknown	
682/tcp	filtered unknown		976/tcp	filtered unknown	

SECURITY INFORMATION

985/tcp	filtered unknown	1540/tcp	filtered rds
989/tcp	filtered ftps-data	1549/tcp	filtered shivahose
992/tcp	filtered telnets	1650/tcp	filtered nkd
994/tcp	filtered ircs	1651/tcp	filtered shiva_confsvr
999/tcp	filtered garcon	1663/tcp	filtered netview-aix-3
1002/tcp	filtered windows-icfw	1665/tcp	filtered netview-aix-5
1004/tcp	filtered unknown	1669/tcp	filtered netview-aix-9
1006/tcp	filtered unknown	1672/tcp	filtered netview-aix-12
1025/tcp	filtered NFS-or-IIS	1720/tcp	filtered H.323/Q.931
1029/tcp	filtered ms-lsa	1764/tcp	filtered landesk-rc
1080/tcp	filtered socks	1900/tcp	filtered UPnP
1110/tcp	filtered nfsd-status	1999/tcp	filtered tcp-id-port
1127/tcp	filtered supfiledbg	2002/tcp	filtered globe
1347/tcp	filtered bbn-mmc	2004/tcp	filtered mailbox
1356/tcp	filtered cuillamartin	2018/tcp	filtered terminaldb
1360/tcp	filtered mimer	2025/tcp	filtered ellpack
1361/tcp	filtered linx	2026/tcp	filtered scrabble
1363/tcp	filtered ndm-requester	2028/tcp	filtered submitserver
1366/tcp	filtered netware-csp	2034/tcp	filtered scoremgr
1367/tcp	filtered dcs	2108/tcp	filtered rkinit
1380/tcp	filtered telesis-licman	2121/tcp	filtered ccproxy-ftp
1381/tcp	filtered apple-licman	2564/tcp	filtered hp-3000-telnet
1386/tcp	filtered checksum	3000/tcp	filtered ppp
1387/tcp	filtered cadsim-lm	3049/tcp	filtered cfs
1394/tcp	filtered iclpv-nlc	3086/tcp	filtered sj3
1399/tcp	filtered cadkey-licman	3264/tcp	filtered ccmail
1418/tcp	filtered timbuktu-srv2	3269/tcp	filtered globalcatLDAPssl
1419/tcp	filtered timbuktu-srv3	3455/tcp	filtered prsvp
1426/tcp	filtered sas-1	3689/tcp	filtered rendezvous
1442/tcp	filtered cadis-2	3999/tcp	filtered remoteanything
1444/tcp	filtered marcam-lm	4008/tcp	filtered netcheque
1448/tcp	filtered oc-lm	4444/tcp	filtered krb524
1449/tcp	filtered peport	4500/tcp	filtered sae-urn
1457/tcp	filtered valisys-lm	4899/tcp	filtered radmin
1466/tcp	filtered oceansoft-lm	5191/tcp	filtered aol-1
1471/tcp	filtered csdmbase	5192/tcp	filtered aol-2
1480/tcp	filtered pacerforum	5193/tcp	filtered aol-3
1481/tcp	filtered airs	5305/tcp	filtered hacl-test
1483/tcp	filtered afs	5308/tcp	filtered cfengine
1487/tcp	filtered localinfosrvr	5400/tcp	filtered pcduo-old
1513/tcp	filtered fujitsu-dtc	5530/tcp	filtered sdserv
1522/tcp	filtered rna-lm	5715/tcp	filtered prosharedata
1525/tcp	filtered orasrv	5800/tcp	filtered vnc-http
1531/tcp	filtered rap-listen	5803/tcp	filtered vnc-http-3
1534/tcp	filtered micromuse-lm	6000/tcp	filtered X11
1537/tcp	filtered sdsc-lm	6002/tcp	filtered X11:2

SECURITY INFORMATION

6003/tcp filtered X11:3
6143/tcp filtered watershed-lm
6400/tcp filtered crystalreports
7464/tcp filtered pythonds
8081/tcp filtered blackice-icecap
8082/tcp filtered blackice-alerts
8443/tcp filtered https-alt
8888/tcp filtered sun-answerbook
9999/tcp filtered abyss
11371/tcp filtered pksd
12000/tcp filtered cce4x
13712/tcp filtered VeritasNetbackup
13716/tcp filtered VeritasNetbackup
13717/tcp filtered VeritasNetbackup
13782/tcp filtered VeritasNetbackup
15126/tcp filtered swgps

18181/tcp filtered opsec_cvp
18182/tcp filtered opsec_ufp
18184/tcp filtered opsec_lea
22305/tcp filtered wnn6_Kr
27008/tcp filtered flexlm8
31337/tcp filtered Elite
38292/tcp filtered landesk-cba
Device type: general purpose
Running: Apple Mac OS X 10.3.X
OS details: Apple Mac OX X 10.3.0 - 10.3.2
(Panther)

Nmap run completed at Wed Mar 24 19:17:42
2004 -- 2 IP addresses (2 hosts up) scanned in
139.378 seconds

© SANS Institute 2004, Author retains full rights.

This page intentionally left blank

© SANS Institute 2004, Author retains full rights.