Global Information Assurance Certification Paper

HIPAA/ISO 17799 Security Audit of GIAC Enterprises Onsite Employee Health Clinic Database Server

Sherry Cummins
June 20, 2003
GCUX Practical Assignment 1.9

Submitted in Partial Fulfillment of the GIAC GCUX Certification Requirements

Executive Summary

Cardinal Associates is an independent IT security auditing and consulting firm which was engaged by the GIAC Enterprises Onsite Employee Health Clinic to perform an server security audit on the clinic's Sun Microsystems Ultra Enterprise 250 server running the Solaris 8 operating system. The server, named horatio.giacfc.com, is used by clinic personnel as a database server for storage of patient health information and occupational health data, and is the platform used for connecting to and outside billing service for transmission of insurance billing information. This audit was conducted in response to the corporate policy that requires an independent audit of all servers by an external agency on a biannual basis.

Because of the recent finalization of the HIPAA Security rules, the clinic management asked that this audit be structured in a way that would target both standard IT security issues and the requirements posed by HIPAA. In order to structure the audit process to comply with this request, the audit team built a methodology around a model which maps the ten domains of the International Standards Organization's ISO 17799 standard into the four major categories defined by the HIPAA Security rules. The mapping of corresponding categories is as follows:

Administrative Procedures
- Organizational Security
- Security Policy
- Compliance
- Personnel Security
- Business Continuity Management

Technical Security Services
- Asset Classification and Control
- Access Control

Technical Security Mechanisms and Electronic Signatures
- Communications and Operations Management
- System Development and Maintenance

Physical Safeguards
- Physical and Environmental Security

Within this methodology, the audit team gathered data by questionnaire, subject interview, computerized vulnerability scanning, and examination of the hardware and software. After the results were analyzed, findings and recommendations were documented by the ten subcategories. Of these, the 10 most critical findings and recommendations are:

1. **No disaster recovery plan exists for the server:** Develop, document, and test a formal disaster recovery plan to fit the needs and resources of the clinic.
2. **Lack of system administrator training hinders the performance of administrative and security duties:** Provide operating system and security training for the system administrator to improve his ability to perform his job function, and allow sufficient time to accomplish administrative tasks.
3. **Patches are not being applied:** As soon as possible have patches reviewed and applied on the server to bring the operating system security up to an acceptable level.
4. **Logs and OS events are not being monitored regularly:** Institute a regular schedule of log review and system monitoring by the administrator.
5. **Unused, vulnerable remote access services are running:** Remove or disable unneeded remote access services. Limit direct root logins to the console only to reduce the chance of remote exploitation of the root account.
6. **Too many people have physical access to the server hardware:** Limit physical access to the server by removing clinic supplies from the server room and storing server access keys away from the hardware.
7. **About 50% of user passwords are too weak:** Implement and enforce a departmental policy of strong password use, providing users with guidelines for choosing strong passwords and using a password cracker on a regular basis to test password security.
8. **Assigned user home directories do not provide file and data security:** Change the user home directory structure so that all users have their own home directory to reduce file loss and corruption and to keep users from having access to sensitive data they are not authorized to view
9. **Programs used to connect to the server send data unencrypted:** To help protect data confidentiality, install and implement encrypted remote access software such as Secure Shell (*ssh*) and transition users away from insecure protocols such as telnet.
10. **User training in security and handling sensitive information is limited:** Create a process or procedure to ensure each employee has a working knowledge of the policies and procedures that apply to information security and secure data handling.

The overall security of the Horatio server is enhanced by the implementation of a host-based firewall called IPFilter. This firewall adds a layer of security that is not commonly implemented on servers, and effectively reduces the possibility of exploitation from outside the server's departmental Virtual LAN (VLAN). However this one security mechanism could fail and should not be relied on as the sole means of protecting the server. Therefore we advise that the issues and recommendations listed above be addressed and the system re-evaluated after remediation is made.

Introduction

The director of the Onsite Employee Health Clinic at GIAC Enterprises requested the services of Cardinal Associates, Inc. to conduct an Information Security Audit on their primary server. The goals of this assessment were to:

- identify information security concerns within the department's computing, patient record, and administrative environment,
- identify security concerns regarding Health Information Privacy and Accountability Act (HIPAA) security compliance
- provide security and remediation recommendations.

Company policies for computer and data security were previously developed following the ISO17799 standard and are published in the GIAC Enterprises "Guide to Operating Procedure and Policy". GIAC Policy 2.3.2, "Audit Procedures", requires that all database servers undergo an annual procedures audit conducted by GIAC Enterprises' Internal Audit Office. In addition, the policy requires that server and network security audits must be conducted on all servers by an external audit agency on at least a biannual basis. The external audit is intended to both verify the annual internal procedures audits and to provide an independent, expert analysis of server and associated network security as compared to current industry trends. This audit by Cardinal Associates, Inc. has been conducted in order to meet the requirement for the biannual external audit.

System Description

Server Function

The system to be evaluated is a server used in GIAC Enterprises' Onsite Employee Health Clinic. This clinic is staffed by two nurse practitioners and various support personnel, and provides emergency care and first aid for injuries and illnesses that occur while at work. Preventive medical services such as blood pressure checks and diet counseling are also available, and the clinic monitors and documents many workplace-related occupational health issues for the corporation. As a part of the corporation's cutting-edge occupational health and safety program, data is being collected and analyzed regarding two common workplace hazards: caffeine addiction and repetitive strain injuries (i.e. Carpal Tunnel Syndrome). Databases of employee health records regarding these conditions are stored on this server.

Because the clinic is not a "regular" health care entity but rather a limited-scope clinic for the convenience of employees and the company, clinic and corporate management were not sure whether this clinic is bound by the HIPAA regulations that apply to hospitals and large medical practices providing and billing for services to thousands of patients. To determine the answer to this question, the

audit staff evaluated the clinic's operation against the HHS Centers for Medicare and Medicaid Services "Covered Entity Decision Tool", provided free of charge on the CMMS website at the link:

http://cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp

The tool named "Is a Person, Business, or Agency a Covered Health Care Provider?" is an interactive questionnaire that leads the user through the questions necessary to determining the HIPAA regulatory status of a particular health care entity. The algorithm used is illustrated in the flowchart shown in Figure 1 below.

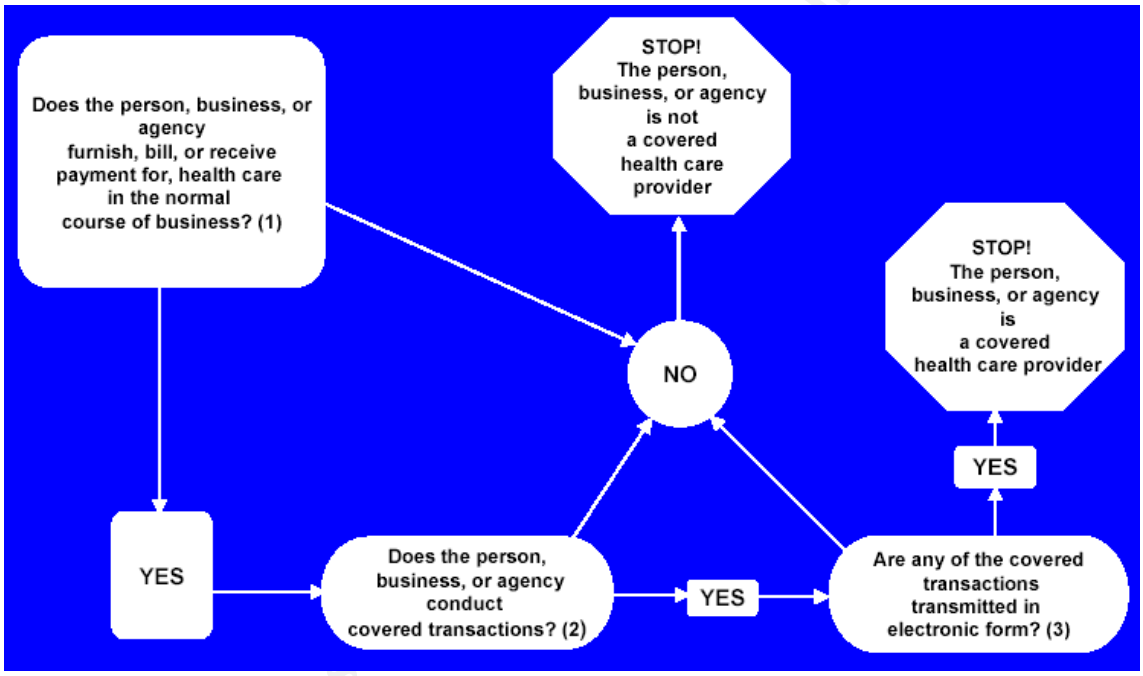

Figure 1: Covered Entity Flowchart for Persons, Businesses, or Agencies
Source: "Covered Entity Decision Tool", HHS Centers for Medicare and Medicaid Services.
URL: http://cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp

This clinic does provide some billable services to employees, and in many cases the employee's health insurance or Medicare/Medicaid covers those services. Because this small clinic does not have its own onsite insurance and billing staff, billing is outsourced to a commercial billing service. The billing service provides electronic forms through a VPN connection to their server. Technicians at the clinic are responsible for filling out the electronic forms for billable patient services and transmitting them to the billing service for processing. Under the conditions described, this clinic does qualify as a covered entity for HIPAA.

Hardware

The server is a Sun Microsystems Ultra Enterprise 250 server with one Ultrasparc 450 CPU and 1.5 GB RAM. It has an external 8MM tape drive, internal 3.5" floppy drive, and internal CD-ROM reader. The monitor is an entry-level 17" Sun color monitor that is attached to a video card in the server. Aside from the Sun keyboard and optical mouse, the server does not have any directly connected input or output devices. The default printer for this system is a networked Hewlett-Packard LaserJet 4500N that is managed by another server on-site. It also has access to several other networked printers made available by the company.

Operating System

The server operating system is Solaris 8, with selected patches applied as the system administrator deemed necessary.

Applications

Databases containing the employee health information are maintained in Informix SE version 7.2 with custom-written forms and views for data entry, viewing, and management. Analysis of the data is conducted using SAS version 8.2. The IPFilter software is installed for use as a host-based firewall.

Network Connectivity

The server has a single onboard RJ45 network interface card that is connected to the company's 100mbps local area network. Aside from this, there are no modems, wireless access points, or other remote access devices connected to the server.

The corporate network uses addresses in a group of contiguous class C networks in the range 199.22.1.x – 199.22.50.x, and is managed by an on-site corporate network team. The network has been designed so that major corporate departments are segregated by routers into virtual local area networks (VLANs). Router access control lists (ACLs) can be set up to block traffic by IP address into or out of the VLAN, however in most cases these ACLs are not very restrictive. A firewall at the border of the network is more tightly controlled, and prevents a large amount of traffic originating from high-end ports from entering the network. This eliminates many potential attacks through trojans, backdoors, and other malicious code that targets these high-numbered ports. Low-numbered ports are currently mostly available through the firewall, which leaves devices on the network at risk for some very common exploits that target FTP (port 21), Telnet (port 23), HTTP (port 80) and other services often found running on computers.

Audit Focus

Because the data maintained on this server qualifies both as sensitive employee information and identifiable health information, the security measures taken to protect the data must meet both the standards defined by HIPAA as well as the data privacy and computer security standards required by other state and federal law and set forth by GIAC Enterprises' corporate policy. This audit evaluates the server's HIPAA compliance within the framework of the company's existing ISO 17799 based policy framework and examines the server's security profile in comparison to both HIPAA and ISO 17799.

Audit Methodology

Although the ISO 17799 standard is divided into ten subdomains, those subdomains can be mapped with reasonable correspondence into the four HIPAA security categories. An example of this mapping was produced by the IT security firm Treadstone71 and is illustrated in Figure 2.

HIPAA Requirement	ISO 17799 Feature
Administrative Procedures Documented, formal practices to manage the selection and execution of security measures to protect data and the conduct of staff relative to the protection of data	• **Organizational Security** • **Security Policy** • **Compliance** • **Personnel Security** • **Business Continuity Management**
Technical Security Services Control and monitor information access	• **Asset Classification and Control** • **Access Control**
Technical Security Mechanisms and Electronic Signatures Prevent unauthorized access to data that is transmitted over a network	• **Communications and Operations Management** • **System Development and Maintenance**
Physical Safeguards Protect physical computer systems, related buildings and equipment	• **Physical and Environmental Security**

Figure 2: HIPAA and ISO 17799
Source: "HIPAA and ISO17799", Treadstone71 IT Governance and Information Security Services. URL: http://cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp

This audit uses the HIPAA/ISO 17799 mapping model as the basis for the audit design. In the process of the audit, the four categories of the HIPAA Security standards were visited, with each of the mapped ISO 17799 subdomains treated as subcategories.

The audit was conducted in four phases:

- Pre-Assessment Activities
- Data Collection
- Data Analysis
- Final Report

The audit team limited its activities to passive data collection, in that team members did not target the server with denial of service (Does) attacks, or attacks and penetration tests that would disrupt the department's network, systems, or business operations. Team members did not modify system configurations, nor modify any files on the server. The team ensured that our scans were confined to the network addresses in the VLAN occupied by the clinic. All activity was coordinated with the clinic personnel, GIAC networking support personnel, and the GIAC Security department.

As a part of pre-assessment activities, the system administrator filled out and returned a HIPAA/ISO 17799 Security Audit Questionnaire. A copy of the blank questionnaire is shown for reference in Appendix A. During this time, security analysts also to conducted non-intrusive scanning of the system from outside the network.

Following review and evaluation of the questionnaire, security analysts spent two days on-site conducting interviews and performing scans from within the network. The information gathered from all of these efforts was then analyzed and consolidated into this report. The components and techniques used in each section of the audit is explained in more detail below, outlined by HIPAA/ISO 17799 categories.

1. Administrative Procedures

Organizational Security
Security Policy
Compliance
Personnel Security
Business Continuity Management

Evaluation of all of the five subcategories within this category relied heavily on the questionnaire and on interviews conducted by the audit team with system administrators, managers, and users of the server and its applications. Existing organizational policy, usage rules, employee training and compliance, and backup procedures and schedules were among the topics examined.

2. Technical Security Services

Asset Classification and Control – Issues within this subcategory were addressed by questionnaire and interviews, and by examination of company policy regarding inventory and labeling, data classification, data retention policies, release of data to outside entities, and collaboration policies.

Access Control – System administrators were asked questions regarding procedure for obtaining a user account, password policy, lockout policies, workstation security, and account management procedures. Password strength testing was done using **John the Ripper 1.6** by the Openwall Project (http://www.openwall.com/john/) to crack the password database.

3. Technical Security Mechanisms and Electronic Signatures

Communications and Operations Management – Evaluation of this subcategory included questionnaire and interview information regarding network structure and connections, services offered, login, file transfer, mail, and sharing/mapping capabilities, and Internet access.

Based on information gained by these interviews regarding the configuration of the network and the server, it was decided that scans would be conducted from three different points:

- Outside the network firewall (the Internet)
- Inside the firewall but outside of the virtual local area network (VLAN) containing the server
- Inside the VLAN where the server resides

SuperScan 3.0 *by Foundstone, Inc. (http://www.foundstone.com/) was used to map all available ports.* ***Nessus 2.0*** *by the Nessus Project (http://www.nessus.org/) and* ***LANguard Network Security Scanner 3.0*** *by GFI Software Ltd. (http://www.gfi.com/lannetscan/) were used to scan the server for known vulnerabilities.*

Systems Development and Maintenance – Procedures for system upgrades, patch management, design of database systems and custom applications were reviewed. Sun's **patchcheck** was used to check the patch level and verify that important security patches were being applied.

4. Physical Safeguards

Physical and Environmental Security – Physical inspection, questionnaire, and interview data were used to determine the overall physical security profile of this server.

Analysis of System

Organizational Security

Review of corporate policy and subject interviews reveal that while information security is a prominent concern for both the corporation and the clinic, no formal security infrastructure is in place. Individual system administrators are responsible for the security configurations of their own devices with very little actual guidance from the corporation. Upper-level management in most divisions makes the decisions regarding details of security procedures and handling of sensitive data. In both of these cases, security is a part-time additional duty assigned to staff members whose primary job function is something other than security.

Security Policy

The corporation's handbook, "Guide to Operating Procedure and Policy", includes some policies that apply to computer and information security. These policies were examined for their applicability to the HIPAA/ISO 17799 guidelines, and were placed in the following subcategories:

Organizational Security

None Published

Security Policy

5.8.3 Information Security Incident Reporting Policy
5.8.4 Computer Incident Response Policy

Compliance

4.10.1 Compliance Training
5.5.8 Software Policy

Personnel Security

4.4.1 Criminal Background Checks for Security Sensitive Positions
5.5.9 E-mail Use
5.5.10 Internet Use
5.8.5 Corporate Network Use

Business Continuity Management

None Published

Asset Classification and Control

2.2.1 Records and Information Management and Retention
2.2.6 Release of Records and Requests for Personal Information
2.4.2 Personal Use of Resources, Equipment and Assets
2.6.1 Intellectual Properties
5.5.7 Electronic Information Retention
6.1.1 Uses and Disclosures of Protected Health Information

Access Control

5.8.2 Access Control and Password Management

Communications and Operations Management

5.2.9 Computer Networking Policies
5.5.5 Guidelines for Central Computing Use
5.5.6 Data Ownership and Client Responsibility

System Development and Maintenance

None Published

Physical and Environmental Security

None Published

These existing policies are published both in hardcopy and electronically on the corporate website. Departmental administrators are required to have a hardcopy handbook available for access by employees within the department.

Compliance

The corporation has a compliance function within the Internal Audit office, which oversees issues of compliance with corporate policy and local, state, and federal regulations. New employees sign a form stating that they will follow the policies set forth in the handbook. Required online compliance training is required for all employees at the beginning of each fiscal year.

Personnel Security

Corporate policy dictates that staff members hired into security-sensitive positions undergo a security check before employment to rule out candidates who have criminal records or possible ethical issues or

conflicts that might affect the security of the data and resources. All employees are required to wear picture ID badges at all times while on company property. Visitors, vendors, and contractors are required to check in at the front entrance desk and obtain a temporary ID. If non-employees need access to secure areas, they must be escorted at all times by corporate staff.

Business Continuity Management

The corporation's central computing department maintains both local and offsite backups of central and administrative systems. However, non-centralized systems such as the server in the clinic are not covered by the central computing department's backup capability. System administrators of decentralized servers must develop and maintain their own backup plan, and must make their own arrangements for storage of backup media.

The system administrator of the Horatio server in the Clinic has developed a regular backup plan that is implemented for this server. The *ufsdump* command is used for these backups, and the backups are run automatically by a *cron* job that schedules the backups to run nightly at 2:00 AM. The backup schedule is as follows:

Monday – Thursday	Level 9 daily incremental
Friday	Level 5 weekly incremental
Last day of the Month	Level 0 full

The server's crontab file is used to set up these automatic backups by calling shell script files that run the backup tasks for a given night.

Three backup script files are used by cron. These three files are exactly the same format except for backup level. The contents of the level 9 backup file (/usr/local/cronscripts/level9back) is shown below:

```
clear
mt rewind
ufsdump –9ucf /dev/rmt/0n /dev/rdsk/c0t0d0s1    # root partition
ufsdump –9ucf /dev/rmt/0n /dev/rdsk/c0t0d0s4    # /var partition
ufsdump –9ucf /dev/rmt/0n /dev/rdsk/c0t0d0s6    # /usr partition
ufsdump –9ucf /dev/rmt/0n /dev/rdsk/c0t0d0s7    # User data partition
mt rewoffl
```

The system administrator does not formally test backups on a regular schedule, but does occasionally recover files from the backup tapes, which have always proven to be good.

Tapes are stored in a fireproof safe in the server room. There is no provision for offsite storage by the department or the company, so each month the system administrator takes home the previous month's tape to provide some level of offsite backup storage and data recovery potential in case of disaster.

Neither the central computing department nor the Clinic has documented business continuity management (disaster recovery) plans developed. There is no redundancy in the server hardware in the clinic, and in the past when hardware problems occurred, users had to wait up to 4 working days for the problem to be corrected before they could use the server. In the case of a catastrophic event that destroyed or incapacitated the server, a significant amount of loss could be expected in both equipment repair or replacement, loss of effort, and possibly data loss or corruption.

Asset Classification and Control

According to company policy, corporate physical assets above $500 in value are inventoried and tagged as they are received, before they can be delivered to the receiving department. Annual inventories are conducted to review the location of assets, and centralized company processes are in place to dispose of unneeded equipment.

Before computer equipment can be disposed of, the hard drive must be destroyed or cleaned effectively of all data. For Windows-based computers there is a custom-written utility that is available to all employees for use in wiping hard drives before disposal, however no such utility is available for other operating systems including Unix.

Both hardcopy and paper information assets are subject to corporate policy regarding distribution and retention, and disposal. No classification of data type takes place within a uniform system, which sometimes makes it difficult for employees to know exactly what kind of data they are dealing with and which rules apply to it.

Access Control

According to company policy, each user on a computer system must have an individual username and password in order to access that system, and may not share their password or allow any other user to access any system with their login credentials. This policy is strictly enforced across the corporation, and employees report that violation of this policy has in the past resulted in disciplinary action and termination. Company policy does not, however, define any rules for password strength, composition, change frequency, or re-use of passwords.

Each of the Horatio users has a unique username and password assigned, and there is no reported sharing of usernames and passwords. The server's password The audit team used John the Ripper 1.6 in order to test the strength of the root and user passwords on the server. The result of this test was that of 10 user passwords, 5 were cracked in less than 15 minutes. This 50% password-cracking rate was apparently due to the tendency of the users to use of names, with or without preceding or trailing numbers, as their passwords. The root password was not cracked in the 12 hours that John the Ripper was allowed to run.

One thing that was noted when working with the */etc/passwd* file in preparation for cracking was the fact that all of the users have the same home directory, */export/home/userhome*, which is owned by root but has permissions of 776 (u=rwx, g=rwx, o=rw):

smithn:x:5000:10:Nancy Smith:/export/home/userhome:/bin/csh
jonesb:x:5001:10:Bob Jones:/export/home/userhome:/bin/csh
whitem:x:5002:10:Morgan White:/export/home/userhome:/bin/csh
blacks:x:5003:10:Sylvia Black:/export/home/userhome:/bin/csh
gravesm:x:5004:10:Melissa Graves:/export/home/userhome:/bin/csh
mcbealh:x:5005:10:Harriet McBeal:/export/home/userhome:/bin/csh
cloudt:x:5006:10:Terry Cloud:/export/home/userhome:/bin/csh
rouldj:x:5007:10:Jeremy Rould:/export/home/userhome:/bin/csh
millerm:x:5008:10:Mike Miller:/export/home/userhome:/bin/csh
jamisons:x:5009:10:Sarah Jamison:/export/home/userhome:/bin/csh

A listing of this directory using *ls –l* shows that the directory is filled with many files belonging to the 10 current users and some belonging to past users, along with the Informix database directories where patient data tables are kept. The *umask* of 002 in the */etc/.login* file causes new files for all users to be created with permissions of 664 (u=rw, g=rw, o=r). Because all users belong to the same group (10), this allows all users to see and change all of the files in the directory.

The audit staff asked the system administrator and users about this setup and discussed the problems associated with keeping all user files in a single home directory. Users report no problem with seeing everyone else's files when they get a directory listing using a command called *dir*. Examination of the user environment files shows that at some point, an administrator put a line into the */etc/.login* file which sets up an aliased *dir* command as follows:

alias dir "ls –l | grep $USER"

This command allows users to get a directory listing of the common user directory filtered for the presence of their username, which in most cases

shows only the files owned by them. If users need to see files owned by other users, they use the regular *ls* command to list the full directory.

Although this setup allows all users easy access to everyone's files, there are two basic problems with this home directory structure:

- deleted, overwritten, or corrupted files
- inappropriate access to files according to job function

Users report that on occasion, files they have been working unexpectedly disappear, are changed, or are overwritten by other user's files. The audit team suspects that the cause of this is that most users forget that there are other files in the directory besides theirs, and accidentally choose file names that correspond to the name of an existing file they can't see with the *dir* command.

This home directory configuration also makes all files available to all users, unless the owner of the file deliberately sets the permissions to exclude use by anyone else. In most cases users do not bother to change the default permissions and all users can access all files in the directory. This may be a problem in terms of privacy and confidentiality, since the job function of some users may not necessarily require access to sensitive health information or other data kept in this directory.

Communications and Operations Management

Access to the system from non-console locations is primarily through *telnet* sessions and *ftp* for file transfers. Although X11 services and remote services (*rsh*, etc.) are available, they are not frequently used. Inspection of the */etc/default/login* file shows that the *CONSOLE=/dev/console* line is commented out, allowing root users direct login to the system via remote access such as *telnet* and *rsh.*

Although the system administrator has downloaded the Secure Shell Server package for Unix, the software has never been implemented, and the server offers no encrypted login or file transfer capability. The VPN connection to the remote server at the billing service is accessed through a proprietary package with a VPN client and web client installed on Horatio by the billing service's tech support office. This VPN connection is outgoing only and cannot be used to connect to any other site because of access restrictions set on the billing service server.

NFS services are available but there are currently no remotely mounted resources from any other system. The Nessus scan reported that a directory on the server named */export/home/userhome* was available for

mounting by everyone through an NFS share, as shown in the following output:

Vulnerability	nfs (2049/tcp)	Here is the export list of horatio.v32.giacfc.edu : /export/home/userhome (mountable by everyone) CVE : CAN-1999-0554

When asked, the system administrator was not aware that this directory was being shared. Examination of the */etc/dfs/dfstab* file shows the entry:

share –f nfs –o rw,nosuid,nosub userhome:/export/home/userhome

To check for clients connected to the shared partition, the system administrator ran the command:

 # showmount –a

No connected clients were returned, indicating that the shared directory was not currently mounted by any remote client. Later investigation into the matter by the system administrator discovered that this nfs share had been set up by a past system administrator for remote access by clients, but the shared resource had never been used.

Users report that although they have no trouble connecting to Horatio from their workstations, they cannot connect to the server from workstations in other departments or outside the corporate network. According to investigation of the system setup, this access limitation is caused by the configuration of the IPFilter host-based firewall, which is set to allow only connections from within the VLAN:

 # allow access only from 199.22.33.0/24
pass in quick proto tcp from 199.22.33.0/24 to any flags S keep state
block in log quick proto tcp/udp from any to 199.22.33.44/32

The IPFilter package was installed and configured by the system's previous administrator, and the current administrator had no knowledge of its presence or the effect it has on access and security. Appendix C gives a sample of the *ipf.log* file that shows blocked connection attempts during the audit team's external scanning effort.

The Nessus, LANguard, and SuperScan results all showed a lack of any type of mail service running on the server. None of the standard ports associated with mail service (SMTP 25, POP3 110, IMAP 143, etc.) were shown as being available by any of the scans. The interview conducted with the system administrator revealed that in the past year, *sendmail* services, which had been allowed in the IPFilter configuration file, had

been disabled by the administrator because they were notified by SpamCop.net that the server was being used as an open SMTP relay. This had been done by removing the */etc/rc2.d/S88sendmail* file from the startup files and by changing the permissions on */usr/lib/sendmail* to make it non-executable (*chmod 400 /usr/lib/sendmail*).

The audit team, knowing that Solaris 8 is generally distributed with a version of *sendmail* (8.9.3 or above) that is set by default not to allow relaying, probed further for information on this incident. They discovered that when the server was upgraded to Solaris 8, part of the upgrade process was to backup certain system configuration files that had been modified by the system administrator. After upgrade, these files were restored onto the server so that system services would retain these site-specific changes. One of the files restored was an old *sendmail.cf* file. When this configuration file did not work with the newly installed version of *sendmail*, the old */usr/lib/sendmail* (version 8.8) file was retrieved from backup tapes. With some minor tweaking this allowed *sendmail* to run on the server but made the server vulnerable to relaying. When the relay incident was reported, it was determined that mail services were not needed on this server and *sendmail* was disabled.

Systems Development and Maintenance

The system administrator who manages this server is one of the staff technicians, for whom system administration is an additional duty executed in his spare time. He has only recently been appointed as the system administrator, following the departure of the previous administrator. He reports that he has very little time to dedicate to administration of the server, and has not received any training in system administration of Solaris servers. He is self-taught and relies on online resources and knowledgeable friends for information and tips. He does subscribe to several mailing lists including CERT and SANS for vulnerability notification, and receives the Sun Patch Report by mail. He does not make a habit of applying patches as they become available unless the patch applies to a specific operational problem they are having. He only checks system logs on occasion, if a particular problem has been noticed.

The results of vulnerability scans run against Horatio vary widely depending on the location of the computer on which the scans were run. Because of the network setup, the decision was made to perform scans 3 times; from outside the corporate network, from inside the network but outside the VLAN, and from inside the VLAN. All scan attempts from both of the locations outside the VLAN show few results if any, which is a good sign that the host-based IPFilter firewall is effectively filtering out connection attempts from external addresses. Scans from within the

VLAN show multiple vulnerabilities that could be exploited by hackers if they ever gained access to the server. Selected listings of the vulnerability scan results are shown in Appendix B.

Composite analysis of the scan results indicates serious vulnerabilities in the following services on the Horatio server:

ftp
nfs shares
snmp
remote execution (rlogin and rsh)
smnpXdmid
statd
walld
in.lpd
CDE desktop applications
dtspcd
cachefsd
cmsd
tooltalk

In addition there are several services running, including telnet and finger, which can pose a risk to systems either in terms of remote connection or reconnaissance.

According to the system administrator, patches have not been applied since the upgrade of the server to Solaris 8. The patchcheck tool was used to check the system's patch status, and verifies that the system is not up to date with patches and could be at serious risk if a hacker were to gain access to the server. The list below edited from the patchcheck listing, shows the security patches that were found to be missing:

108919 CDE 1.4: dtlogin patch
108949 CDE 1.4: libDtHelp/libDtSvc patch
109154 SunOS 5.8: PGX32 Graphics
109221 Obsoleted by: 109318-12 SunOS 5.8: Patch for sysidnet
109354 CDE 1.4: dtsession patch
109470 CDE 1.4: Actions Patch
109951 SunOS 5.8: jserver buffer overflow
110670 SunOS 5.8: usr/sbin/static/rcp patch
110939 SunOS 5.8: /usr/lib/acct/closewtmp patch
110943 SunOS 5.8: /usr/bin/tcsh patch
110949 Obsoleted by: 110934-04 SunOS 5.8: /usr/sadm/install/bin/pkgremove
111071 SunOS 5.8: cu patch
111090 Obsoleted by: 108993-05 SunOS 5.8: /usr/lib/libsldap.so.1 patch
111177 Obsoleted by: 108827-15 SunOS 5.8: /usr/lib/lwp/libthread.so.1 pat
111363 Obsoleted by: 110934-04 SunOS 5.8: /usr/sbin/installf patch

111570 SunOS 5.8: uucp patch
111596 SunOS 5.8: /usr/lib/netsvc/yp/rpc.yppasswdd patch
111626 OpenWindows 3.6.2: Xview Patch
111879 SunOS 5.8: Solaris Product Registry patch SUNWwsr
111883 SunOS 5.8: Sun GigaSwift Ethernet 1.0 driver patch
112279 SunOS 5.8: pkgrm failed during upgrade from Solaris 8 to Solaris 9
113650 SunOS 5.8: /usr/lib/utmp_update patch
113792 OpenWindows 3.6.2: mailtool patch
114162 SunOS 5.8: /kernel/drv/lofi drivers and /usr/sbin/lofiadm patch
114251 SunOS 5.8: pkgrm failed if upgrade from S8U7 to upper release with
114673 SunOS 5.8: /usr/sbin/wall patch

Both the vulnerability scans and the results of the patch check show that the server security profile in and of itself is very poor, primarily because of neglect in the maintenance of patches and weaknesses in configuration. This server is protected from most routes of intrusion by the host-based firewall, which blocks all traffic from outside the VLAN. However this server is not the only device in the VLAN. If the IPFilter firewall were to be compromised or accidentally disabled, or if another computer in the VLAN were to be hacked and become the platform for further reconnaissance and hacking, Horatio's firewall would not be able to protect it from exploitation of the multiple vulnerabilities that were found.

Physical and Environmental Security

This server is housed in a small utility room at the back of the clinic building. The door to the room is locked, and the system administrator and the clinic director control the keys that open the door. Clinic supplies are stored in this room on occasion, and other staff members can gain unescorted access to the server room by asking for one of the keys.

The server room has the same environmental controls for heating, cooling, and humidity control as the rest of the building. A temperature monitor is kept in the room to record the room's ambient temperature, but no problems have been noted in either temperature or humidity.

The room is wired into GIAC Enterprises' emergency power system to provide power in case of blackouts or other interruptions in regular electrical service. A Best Fortress 650 UPS provides both power filtering and backup battery power for the system for short interruptions in power availability.

Critical Issues and Recommendations

Overview

Following analysis of the audit findings, the Cardinal Associates audit team makes the following recommendations. These recommendations are presented in two ways. The first list is organized by the top ten issues and recommendations. The second list is more detailed and is organized within HIPAA/ISO 17799 subcategory with some of the top 10 recommendations further broken out. These are presented within each category in order from most critical to least critical.

Top Ten Overall Issues and Recommendations Ranked by Importance

1. **No disaster recovery plan exists for the server:** Develop, document, and test a formal disaster recovery plan to fit the needs and resources of the clinic.
2. **Lack of system administrator training hinders the performance of administrative and security duties:** Provide operating system and security training for the system administrator to improve his ability to perform his job function, and allow sufficient time to accomplish administrative tasks.
3. **Patches are not being applied:** As soon as possible have patches reviewed and applied on the server to bring the operating system security up to an acceptable level.
4. **Logs and OS events are not being monitored regularly:** Institute a regular schedule of log review and system monitoring by the administrator.
5. **Unused, vulnerable remote access services are running:** Remove or disable unneeded remote access services. Limit direct root logins to the console only to reduce the chance of remote exploitation of the root account.
6. **Too many people have physical access to the server hardware:** Limit physical access to the server by removing clinic supplies from the server room and storing server access keys away from the hardware.
7. **About 50% of user passwords are too weak:** Implement and enforce a departmental policy of strong password use, providing users with guidelines for choosing strong passwords and using a password cracker on a regular basis to test password security.
8. **Assigned user home directories do not provide file and data security:** Change the user home directory structure so that all users have their own home directory to reduce file loss and corruption and to keep users from having access to sensitive data they are not authorized to view
9. **Programs used to connect to the server send data unencrypted:** To help protect data confidentiality, install and implement encrypted remote access software such as Secure Shell (*ssh*) and transition users away from insecure protocols such as telnet.

10. **User training in security and handling sensitive information is limited:** Create a process or procedure to ensure each employee has a working knowledge of the policies and procedures that apply to information security and secure data handling.

Recommendations by HIPAA/ISO 17799 Control Areas

Organizational Security

1. Although GIAC Enterprises professes an interest in information security, there is no designated person such as an organizational Information Security Officer (ISO) who is invested with responsibility for the development of an information security program. Cardinal Associates recommends that in the absence of this, a departmental ISO should be designated and be given the authority to develop and enforce departmental policies and training in information security to cover the regulatory requirements not addressed by corporate policy.

Security Policy

1. It is recommends that the department create and implement department policies and procedures that address the following issues not covered by corporate policy:

    a. Internal Business Operations Procedures
    b. Physical Security Policy
    c. A detailed System Security Policy
    d. Disaster Recovery Plan with accompanying Backup Procedures
    e. The primary institutional E-Mail policy applies, however the department should augment (make more stringent) the policy by addressing specific patient information issues regarding email.
    f. System Access Policy
    g. Remote Access Policy
    h. Acceptable Use Policy
    i. Change Control Policy/Change Management Program
    j. Chain of Trust Agreements with Identified Providers (such as the billing company)

Compliance

1. Implement all of the policy, procedure, process, and verification measures stated above, to establish a compliance baseline with HIPAA and ISO 17799.
2. Conduct an audit to measure level of compliance upon completion of remediation.

Personnel Security

1. Create a process or procedure to ensure each employee has a working knowledge of the policies and procedures listed above under "Security Policy."
2. Create or outsource a user security training program to increase all users' awareness of HIPAA and other related security issues.

Business Continuity Management

1. Develop and document a formal disaster recovery plan to fit the needs and resources of the clinic.
2. Test the plan on a regularly scheduled basis.
3. Make arrangements for secure offsite storage of backup tapes. Make sure that the offsite storage site would be available for retrieval of the tapes on short notice should a disaster occur.

Asset Classification and Control

1. A document should be created which defines classification levels and data sensitivities for departmental information assets and how those assets are protected.
2. Identify locations of all of the databases and files that contain protected health information on the server, and ensure security and privacy measures are put in place to protect those resources. In many cases this will entail setting file permissions with the proper restrictions or using the "set" command within the Informix database software to permit or deny access to specific information to users according to their job function.
3. If possible, modify database structure to keep patient identifiable information (such as name, address, and SSN) separate from patient health information. Relational database models enable this to be done while providing for a common identifier that can be used to link the records in those cases where the patient must be identified. This separation can reduce the likelihood that patient data will be exposed or compromised in a manner that violates HIPAA regulations.

Access Control

1. Implement and enforce a departmental policy of strong password use. Provide users with guidelines for choosing strong passwords.
2. Use a password cracker on a regular basis to check for weak or empty passwords.
3. Change the use home directory structure so that all users have their own home directory. This will largely eliminate the problem users have had with accidental file deletion and corruption. Home directories should be

set to exclude reading and/or changing by other users as appropriate for the level of sensitivity. Common-use files such as the patient databases can be kept in the common directory for access by all.

Communications and Operations Management

1. Remove the unneeded NFS share of the directory */export/home/userhome.*
2. Limit remote root access to the server by uncommenting the *CONSOLE=/dev/console* entry in the */etc/default/login* file. Legitimate root users will still be able to perform remote administration by logging into their own account and doing an *su* to root. Managing remote root access this way provides for user accountability and tracking.
3. Disable unused remote execution services such as *rsh.*
4. Unencrypted access protocols such as *telnet* and *ftp* send passwords and other sensitive information across the network in cleartext, which can be intercepted and read by malicious persons using sniffers. In the interest of confidentiality of sensitive data, install the Secure Shell software on the server and begin transitioning users away from *telnet* and *ftp* and into using *ssh* and *sftp.*
5. Create a business operations procedures document that addresses functional requirements for both workstations and servers.
6. Ensure that the business operations procedures are addressed in the Disaster Recovery Plan (DRP).

System Development and Maintenance

1. Limited system administration training and security awareness on the part of the designated administrator place this system at considerable risk. Cardinal Associates recommends that the company either:
    a. Provide training for the system administrator targeted toward increasing his knowledge of Solaris administration and security to a level sufficient to perform his required duties, or
    b. Arrange for the server to be administered by some other entity either within the corporation or as an outside vendor, by Service Level Agreement (SLA).
2. System administration is a demanding job function. The designated system administrator must be given sufficient time and resources to dedicate to the task of overseeing the administration and security of the server, or the server's security profile will suffer and the resources will be at increased risk.
3. In spite of the protection provided by the host-based firewall, the patch status of this server creates significant risk. Patches should be reviewed and updated as soon as possible to bring this system up-to-date and reduce its vulnerability. Many of the vulnerabilities noted by the scanning tools are very commonly exploited using buffer overflow scripts and other

methods. After this first patching effort is completed, patches should be reviewed and applied as appropriate on at least a monthly basis to maintain the system's operating system security.

4. It is strongly recommended that the system administrator immediately document and institute a regular schedule of system log review, application monitoring, and user access monitoring. At the very least, the following should be regularly monitored in order to remain aware of both external threats and hardware and operating system problems:
    a. system events - */var/adm/messages*
    b. failed logins - */var/adm/loginlog*
    c. su changes from one account to another - */var/adm/sulog*
    d. running processes – the *ps* command
    e. recent login attempts – the *last* command
    f. firewall events - */var/log/ipf.log*
5. If possible, host-based change detection software such as Tripwire should be installed and used, with change comparisons done on a regular basis, so that compromised files can be discovered and restored. This type of software protects not only against changes made by hackers, but also against accidental deletions and modifications by the system administrator and users.
6. Subscribe to mailing lists and resources that relate to maintenance and security vulnerabilities of the installed application software such as Informix and SAS.

Physical and Environmental Security

1. Move clinic supplies out of the server enclosure and do not allow access to the server room by the majority of clinic staff.
2. Remove front panel key and system startup key from the server and secure them in a location away from the server to prevent physical tampering.
3. Secure the server to the floor, wall, or other fixed object with a locking cable device.
4. Ensure each employee is familiar with policy documents and departmental procedures.
5. Develop a procedure to physically safeguard media and documents within the department.
6. Implement a departmental incident reporting procedure based on the physical security policy requirements..

Appendix A: HIPAA/ISO 17799 Security Audit Questionnaire

HIPAA/ISO 17799
Server Audit Questionnaire

This questionnaire should be completed by the server's primary system administrator or the technical contact most familiar with overall server operation.

Server Information

Server Name: _____ System Administrator: _____

IP Address: _____ Sysadmin Phone #: _____

Hardware Type: _____ Sysadmin Emergency #: _____

Operating System: _____ Secondary Sysadmin: _____

Company: _____ Secondary Phone #: _____

Department: _____

Location: _____

System Functional Classes

What services can this server potentially offer? Mark as many as appropriate:

Web server _____ FTP server_____ File server_____ Database server _____

Mail server _____ Other (specify) _____

Criticality

A critical system is defined as a system that hosts applications or data resources that, if confidentiality or integrity of the data were compromised or the resources were unavailable for any period of time would seriously endanger an organization's ability to carry out its mission.

Is this system considered to be a critical system? YES NO

Data Functional Classes

Does this server contain:

Confidential Sensitive - Patient Health Information: YES NO
Clinical patient records, research patient records, especially in combination with Patient Identifiable Information (PII).

Confidential Sensitive - Non-patient Research Information: YES NO
Research records that do not contain PHI or PII but are part of a body of data with real or intrinsic value that must

be protected.

Confidential Sensitive - Personnel Information: Departmental or institutional personnel records.	YES	NO
Confidential: Individual user files, non-patient research records, institutional financial records, internal web content, internal ftp content, private or internal publications or informational media.	YES	NO
Public: public web content, public ftp content, documents or informational media intended for public access, openly available distance learning content	YES	NO

Primary Application

What is the application or process most commonly used on this server?

Secondary Applications

What are the major secondary applications or processes used on the server?

Authentication

Are usernames and passwords always necessary in order to access this server?	YES	NO
Does this server have guest accounts or other login account names that are not assigned to a single user?	YES	NO
Are there documented procedures for creating, managing, and removing user access to the server?	YES	NO
Are default OS and application accounts deleted, renamed, or have their passwords changed?	YES	NO

Password Policies

Is password policy for server accounts specified by any existing company policy?	YES	NO
What is the minimum password length and allowed character set?	YES	NO
What is the mandatory password change frequency?	YES	NO
Is password history set to prevent re-use of passwords?	YES	NO

Backup Procedures

Is system backup policy for servers specified by any	YES	NO

existing company policy?

Are backups tested regularly to assure that data can be recovered? YES NO

How often are backups performed? (Attach documented backup schedule if it exists):

What media is used for backups?

Where are backups kept?

Disaster Recovery

Is there any offsite storage location where backups are stored to provide for recovery of data in case of disaster? YES NO

Are copies of important operating system software, application software, documentation, and system configuration records kept at the remote site? YES NO

Is there a documented disaster recovery plan for this server? YES NO

Has the disaster recovery plan been tested? YES NO

Remote Access

What types of access are allowed from non-console locations inside the local network (mark all that apply)?

Telnet _____ FTP _____ Anonymous FTP _____ SSH _____

SFTP _____ HTTP _____ HTTPS _____ VPN _____ Dialup _____

RAS (PCAnywhere, Timbuktu, etc.) _____ Other (Specify) _____

What types of access are allowed from locations outside the local network (internet)?

Telnet _____ FTP _____ Anonymous FTP _____ SSH _____

SFTP _____ HTTP _____ HTTPS _____ VPN _____ Dialup _____

RAS (PCAnywhere, Timbuktu, etc.) _____ Other (Specify) _____

Does this server allow its resources to be remotely mapped or shared? YES NO

Does this server use remotely mapped or shared resources from another machine? YES NO

OS Maintenance: General

Does the system administrator have a set time or percentage of effort that is to be dedicated to system maintenance?	YES	NO
Does the system administrator subscribe to or monitor software-specific sites, mailing lists, bulletin boards, or other resources that provide information on vulnerabilities, OS upgrades, and patch releases?	YES	NO
Does the system administrator subscribe to or monitor any non-vendor resources such as Bugtraq, CERT, or SANS that provide information on system administration, maintenance, and security?	YES	NO

OS Maintenance: Patches

Is patch application policy for servers specified by any existing company policy?	YES	NO
Are critical functional or security-related patches reviewed and applied on at least a monthly basis?	YES	NO
Are non-critical patches reviewed and applied on a regular basis?	YES	NO

OS Maintenance: Upgrades

Is OS upgrade policy for servers specified by any existing company policy?	YES	NO
Are OS upgrades applied ASAP or within a few months of being issued by the vendor?	YES	NO
Is the need for OS upgrade reviewed on a regular basis?	YES	NO
Does this server run any specially written, legacy, Or resource-dependent applications or processes that prevent OS upgrades from being done because the application would cease to function?	YES	NO

System Logging and Monitoring

Are logs or audit trails maintained for the OS and important applications?	**YES**	**NO**
Are logs reviewed on at least a weekly basis?	YES	NO
Are logs backed up or stored remotely to avoid loss of information through tampering?	YES	NO

What type of OS event logging is enabled on the machine?

Login success/failure _____ Connection history _____ OS events _____

Process (mail, printing, etc.) _____ Other (specify) _____

Virus Scanning

Does this server have virus scanning or filtering software installed and functional?	YES	NO
Is the virus scanning software upgraded and maintained on a regular basis?	YES	NO
Are virus definition files updated on at least a weekly basis?	YES	NO

Intrusion and Compromise Detection/Prevention

Does the server run any host-based firewall (IPFilter, ZoneAlarm, Norton, etc.)?	YES	NO
Does the server run any change auditing software (such as Tripwire)?	YES	NO
Does the server run any extended access control and auditing software (such as TCPwrappers)	YES	NO
Does the server run any host-based intrusion detection software (Snort, etc.).	YES	NO
Is the server provided with any network-based protection via router or firewall ACL, network IDS or other non host-based protective device?	YES	NO

Warning Banners

Are warning banners displayed before login to inform potential users about authorized access, monitoring, and other limitations on use of the resources?	YES	NO
Is a banner displayed for every possible method of accessing the server (i.e. telnet and ssh logins, and ftp)?	**YES**	**NO**

Physical Security

Is the server located in a secure, limited-access site?	YES	NO
Are servers physically secured with anti-theft devices?	YES	NO
Are anti-theft device keys, panel keys and system control keys secured at a location away from the server to prevent theft or tampering with the hardware?	YES	NO
Is there adequate power protection (UPS or other backup power)?	YES	NO

Is environmental control available to avoid overheating or humidity problems?	YES	NO

User training

Are users trained on proper use of the system and applications?	**YES**	**NO**
Are users trained in proper handling and protection of sensitive information?	YES	NO

Questionnaire Completed by: _____ _____
Name Title

_____ _____
Signature Date

Appendix B: Vulnerability Scan Listings

SuperScan Open Port Lists (from inside VLAN)

```
  7  Echo
  9  Discard
 13  Daytime
        |___ Thu Jun 19 13:27:53 2003..
 19  Character Generator
        |___  !"#$%&'()*+,-
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefg..
 21  File Transfer Protocol [Control]
        |___ 220 horatio FTP server (SunOS 5.8) ready...
 23  Telnet
        |___ ........#..'..$
 37  Time
        |___ ...*
 79  Finger
111  SUN Remote Procedure Call
512  remote process execution;
513  remote login a la telnet;
514  cmd
515  spooler
540  uucpd
        |___ login:
878
880
898
```

Nessus scan from inside the corporate network, outside the VLAN:

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 where alive and responding during test	1
Number of security holes found	0
Number of security warnings found	1

Host List	
Host(s)	**Possible Issue**
199.22.33.44	Security warning(s) found

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
199.22.33.44	general/tcp	Security warning(s) found
199.22.33.44	general/udp	Security notes found

Security Issues and Fixes: 199.22.33.44		
Type	**Port**	**Issue and Fix**
Warning	general/tcp	The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host. An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things. Solution : Contact your vendor for a patch Risk factor : Low
Informational	general/udp	For your information, here is the traceroute to 199.22.33.44 : 199.22.33.5 199.22.33.44

This file was generated by Nessus, the open-sourced security scanner.

Nessus scan from inside the VLAN:

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 where alive and responding during test	1
Number of security holes found	12
Number of security warnings found	22

Host List	
Host(s)	**Possible Issue**
199.22.33.44	Security hole(s) found

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
199.22.33.44	echo (7/tcp)	Security warning(s) found
199.22.33.44	discard (9/tcp)	No Information
199.22.33.44	daytime (13/tcp)	Security warning(s) found
199.22.33.44	chargen (19/tcp)	Security warning(s) found
199.22.33.44	ftp (21/tcp)	Security hole found
199.22.33.44	telnet (23/tcp)	Security warning(s) found
199.22.33.44	time (37/tcp)	Security notes found
199.22.33.44	finger (79/tcp)	Security notes found
199.22.33.44	sunrpc (111/tcp)	Security notes found
199.22.33.44	exec (512/tcp)	Security warning(s) found
199.22.33.44	login (513/tcp)	Security warning(s) found
199.22.33.44	shell (514/tcp)	Security warning(s) found
199.22.33.44	printer (515/tcp)	No Information
199.22.33.44	uucp (540/tcp)	No Information

199.22.33.44	unknown (878/tcp)	Security notes found
199.22.33.44	unknown (880/tcp)	Security notes found
199.22.33.44	unknown (898/tcp)	Security hole found
199.22.33.44	nfs (2049/tcp)	Security hole found
199.22.33.44	unknown (2200/tcp)	No Information
199.22.33.44	unknown (2201/tcp)	No Information
199.22.33.44	unknown (4045/tcp)	Security notes found
199.22.33.44	unknown (5987/tcp)	No Information
199.22.33.44	x11 (6000/tcp)	Security warning(s) found
199.22.33.44	unknown (6112/tcp)	Security hole found
199.22.33.44	xfs (7100/tcp)	No Information
199.22.33.44	unknown (8888/tcp)	Security notes found
199.22.33.44	unknown (9010/tcp)	No Information
199.22.33.44	general/tcp	Security notes found
199.22.33.44	snmp (161/udp)	Security hole found
199.22.33.44	unknown (32775/tcp)	Security hole found
199.22.33.44	daytime (13/udp)	Security warning(s) found
199.22.33.44	echo (7/udp)	Security warning(s) found
199.22.33.44	general/icmp	Security warning(s) found
199.22.33.44	ntp (123/udp)	Security warning(s) found
199.22.33.44	unknown (32779/udp)	Security hole found
199.22.33.44	sunrpc (111/udp)	Security notes found
199.22.33.44	unknown (32772/udp)	Security hole found
199.22.33.44	unknown (32773/udp)	Security warning(s) found
199.22.33.44	unknown (32774/udp)	Security warning(s) found
199.22.33.44	unknown (32771/tcp)	Security notes found
199.22.33.44	unknown (32775/udp)	Security warning(s) found
199.22.33.44	unknown (32776/udp)	Security hole found
199.22.33.44	unknown (32777/udp)	Security warning(s) found
199.22.33.44	nfs (2049/udp)	Security warning(s) found
199.22.33.44	unknown (32778/udp)	Security hole found
199.22.33.44	unknown (32772/tcp)	Security notes found
199.22.33.44	unknown (32773/tcp)	Security hole found
199.22.33.44	unknown (32774/tcp)	Security notes found
199.22.33.44	unknown (32780/udp)	Security notes found
199.22.33.44	unknown (32776/tcp)	Security notes found
199.22.33.44	unknown (32777/tcp)	Security notes found

199.22.33.44	unknown (4045/udp)	Security notes found
199.22.33.44	unknown (864/udp)	Security notes found
199.22.33.44	unknown (32782/udp)	Security notes found
199.22.33.44	unknown (32779/tcp)	Security notes found
199.22.33.44	unknown (32784/udp)	Security notes found
199.22.33.44	unknown (32781/tcp)	Security notes found
199.22.33.44	unknown (32785/udp)	Security notes found
199.22.33.44	unknown (32782/tcp)	Security hole found
199.22.33.44	general/udp	Security notes found
199.22.33.44	xdmcp (177/udp)	Security warning(s) found

Security Issues and Fixes: 199.22.33.44

Informational	chargen (19/tcp)	Chargen is running on this port
Vulnerability	ftp (21/tcp)	You seem to be running an FTP server which is vulnerable to the 'glob heap corruption' flaw. An attacker may use this problem to execute arbitrary commands on this host. *** As Nessus solely relied on the banner of the server to issue this warning, *** so this alert might be a false positive Solution : Upgrade your ftp server software to the latest version. Risk factor : High CVE : CVE-2001-0550
Informational	ftp (21/tcp)	An FTP server is running on this port. Here is its banner : 220 horatio FTP server (SunOS 5.8) ready.
Informational	ftp (21/tcp)	Remote FTP server banner : 220 horatio FTP server (SunOS 5.8) ready.
Warning	telnet (23/tcp)	The Telnet service is running. This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the telnet client and the telnet server. This includes logins and passwords. You should disable this service and use OpenSSH instead. (www.openssh.com) Solution : Comment out the 'telnet' line in /etc/inetd.conf. Risk factor : Low CVE : CAN-1999-0619
Informational	telnet (23/tcp)	A telnet server seems to be running on this port
Informational	time (37/tcp)	A time server seems to be running on this port
Informational	finger (79/tcp)	An unknown service is running on this port. It is usually reserved for Finger
Informational	sunrpc (111/tcp)	RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port
Informational	sunrpc (111/tcp)	RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port
Informational	sunrpc (111/tcp)	RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port
Warning	exec (512/tcp)	The rexecd service is open. Because rexecd does not provide any good means of authentication, it can be used by an attacker to scan a third party host, giving you troubles or bypassing your firewall. Solution : comment out the 'exec' line in /etc/inetd.conf. Risk factor : Medium CVE : CAN-1999-0618
		The rlogin service is running. This service is dangerous in the sense that

		it is not ciphered - that is, everyone can sniff the data that passes between the rlogin client and the rlogin server. This includes logins and passwords. You should disable this service and use openssh instead (www.openssh.com) Solution : Comment out the 'rlogin' line in /etc/inetd.conf. Risk factor : Low CVE : CAN-1999-0651
Warning	shell (514/tcp)	The rsh service is running. This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the rsh client and the rsh server. This includes logins and passwords. You should disable this service and use ssh instead. Solution : Comment out the 'rsh' line in /etc/inetd.conf. Risk factor : Low CVE : CAN-1999-0651
Informational	unknown (878/tcp)	RPC program #300384 version 3 is running on this port
Informational	unknown (880/tcp)	RPC program #300385 version 1 is running on this port
Vulnerability	unknown (898/tcp)	Older versions of JServ (including the version shipped with Oracle9i App Server v1.0.2) are vulnerable to a cross site scripting attack using a request for a non-existent .JSP file. Solution: Upgrade to that latest (and final) version of JServ (available at java.apache.org), or, for preference use TomCat as JServ is no longer maintained. Risk factor : Medium
Warning	unknown (898/tcp)	The remote web server seems to be vulnerable to the Cross Site Scripting vulnerability (XSS). The vulnerability is caused by the result returned to the user when a non-existing file is requested (e.g. the result contains the JavaScript provided in the request). The vulnerability would allow an attacker to make the server present the user with the attacker's JavaScript/HTML code. Since the content is presented by the server, the user will give it the trust level of the server (for example, the trust level of banks, shopping centers, etc. would usually be high). Risk factor : Medium Solutions: Allaire/Macromedia Jrun: http://www.macromedia.com/software/jrun/download/update/ http://www.securiteam.com/windowsntfocus/Allaire_fixes_Cross-Site_Scripting_security_vulnerability.html Microsoft IIS: http://www.securiteam.com/windowsntfocus/IIS_Cross-Site_scripting_vulnerability__Patch_available_.html Apache: http://httpd.apache.org/info/css-security/ ColdFusion: http://www.macromedia.com/v1/handlers/index.cfm?ID=23047 General:

		http://www.securiteam.com/exploits/Security_concerns_when_developing_a_dynamically_generated_web_site.html http://www.cert.org/advisories/CA-2000-02.html
Informational	unknown (898/tcp)	A web server is running on this port
Informational	unknown (898/tcp)	The remote web server type is : Tomcat/2.1 We recommend that you configure your web server to return bogus versions in order to not leak information
Informational	unknown (898/tcp)	The following directories were discovered: /help /images, /servlet
Vulnerability	nfs (2049/tcp)	Here is the export list of horatio.v32.giacfc.edu : /export/home/userhome (mountable by everyone) CVE : CAN-1999-0554
Informational	nfs (2049/tcp)	RPC program #100003 version 2 'nfs' (nfsprog) is running on this port
Informational	nfs (2049/tcp)	RPC program #100003 version 3 'nfs' (nfsprog) is running on this port
Informational	nfs (2049/tcp)	RPC program #100227 version 2 'nfs_acl' is running on this port
Informational	nfs (2049/tcp)	RPC program #100227 version 3 'nfs_acl' is running on this port
Informational	unknown (4045/tcp)	This port was detected as being open by port scanner but is now closed. This service was probably crashed by the port scanner
Informational	unknown (4045/tcp)	RPC program #100021 version 1 'nlockmgr' is running on this port
Informational	unknown (4045/tcp)	RPC program #100021 version 2 'nlockmgr' is running on this port
Informational	unknown (4045/tcp)	RPC program #100021 version 3 'nlockmgr' is running on this port
Informational	unknown (4045/tcp)	RPC program #100021 version 4 'nlockmgr' is running on this port
Warning	x11 (6000/tcp)	This X server does *not* allow any client to connect to it however it is recommended that you filter incoming connections to this port as attacker may send garbage data and slow down your X session or even kill the server. Here is the server version : 11.0 Here is the message we received : Client is not authorized to connect to Server Solution : filter incoming connections to ports 6000-6009 Risk factor : Low CVE : CVE-1999-0526
Vulnerability	unknown (6112/tcp)	The 'dtspcd' service is running. Some versions of this daemon are vulnerable to a buffer overflow attack which allows an attacker to gain root privileges *** This warning might be a false positive, *** as no real overflow was performed Solution : See http://www.cert.org/advisories/CA-2001-31.html to determine if you are vulnerable or deactivate

		this service (comment out the line 'dtspc' in /etc/inetd.conf) Risk factor : High CVE : CVE-2001-0803
Informational	unknown (8888/tcp)	A web server is running on this port The remote web server type is : dwhttpd/4.2a7 (Inso; sun5) We recommend that you configure your web server to return bogus versions in order to not leak information
Informational	general/tcp	Nmap found that this host is running Sun Solaris 8 early acces beta through actual release
Vulnerability	snmp (161/udp)	SNMP Agent responded as expected with community name: public SNMP Agent responded as expected with community name: private CVE : CAN-1999-0517
Vulnerability	unknown (32775/tcp)	The cachefsd RPC service is running. Some versions of this server allow an attacker to gain root access remotely, by consuming the resources of the remote host then sending a specially formed packet with format strings to this host. Solaris 2.5.1, 2.6, 7 and 8 are vulnerable to this issue. Other operating systems might be affected as well. *** Nessus did not check for this vulnerability, *** so this might be a false positive Solution : Deactivate this service - there is no patch at this time /etc/init.d/cachefs.daemon stop Risk factor : High CVE : CAN-2002-0084
Informational	unknown (32775/tcp)	RPC program #100235 version 1 is running on this port
Warning	daytime (13/udp)	The daytime service is running. The date format issued by this service may sometimes help an attacker to guess the operating system type. In addition to that, when the UDP version of daytime is running, an attacker may link it to the echo port using spoofing, thus creating a possible denial of service. Solution : disable this service in /etc/inetd.conf. Risk factor : Low CVE : CVE-1999-0103
Warning	echo (7/udp)	The 'echo' port is open. This port is not of any use nowadays, and may be a source of problems, since it can be used along with other ports to perform a denial of service. You should really disable this service. Risk factor : Low Solution : comment out 'echo' in /etc/inetd.conf CVE : CVE-1999-0103
		The remote host answered to an ICMP_MASKREQ

		query and sent us its netmask (255.255.0.0) An attacker can use this information to understand how your network is set up and how the routing is done. This may help him to bypass your filters. Solution : reconfigure the remote host so that it does not answer to those requests. Set up filters that deny ICMP packets of type 17. Risk factor : Low CVE : CAN-1999-0524
Warning	general/icmp	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols. Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14). Risk factor : Low CVE : CAN-1999-0524
Warning	ntp (123/udp)	An NTP server is running on the remote host. Make sure that you are running the latest version of your NTP server, has some versions have been found out to be vulnerable to buffer overflows. *** Nessus reports this vulnerability using only *** information that was gathered. Use caution *** when testing without safe checks enabled. If you happen to be vulnerable : upgrade Solution : Upgrade Risk factor : High CVE : CVE-2001-0414
Informational	ntp (123/udp)	It is possible to determine a lot of information about the remote host by querying the NTP variables - these include OS descriptor, and time settings. Theoretically one could work out the NTP peer relationships and track back network settings from this. Quickfix: Set NTP to restrict default access to ignore all info packets: restrict default ignore Risk factor : Low
Vulnerability	unknown (32779/udp)	The cmsd RPC service is running. This service has a long history of security holes, so you should really know what you are doing if you decide to let it run. * NO SECURITY HOLE REGARDING THIS PROGRAM HAS BEEN TESTED, SO THIS MIGHT BE A FALSE POSITIVE *

		We suggest you to disable this service. Risk factor : High CVE : CVE-1999-0320
Informational	unknown (32779/udp)	RPC program #100068 version 2 is running on this port
Informational	unknown (32779/udp)	RPC program #100068 version 3 is running on this port
Informational	unknown (32779/udp)	RPC program #100068 version 4 is running on this port
Informational	unknown (32779/udp)	RPC program #100068 version 5 is running on this port
Informational	sunrpc (111/udp)	RPC program #100000 version 4 'portmapper' (portmap sunrpc rpcbind) is running on this port
Informational	sunrpc (111/udp)	RPC program #100000 version 3 'portmapper' (portmap sunrpc rpcbind) is running on this port
Informational	sunrpc (111/udp)	RPC program #100000 version 2 'portmapper' (portmap sunrpc rpcbind) is running on this port
Vulnerability	unknown (32772/udp)	The sadmin RPC service is running. There is a bug in Solaris versions of this service that allow an intruder to execute arbitrary commands on your system. Solution : disable this service Risk factor : High CVE : CVE-1999-0977
Informational	unknown (32772/udp)	RPC program #100232 version 10 'sadmind' is running on this port
Warning	unknown (32773/udp)	The rquotad RPC service is running. If you do not use this service, then disable it as it may become a security threat in the future, if a vulnerability is discovered. Risk factor : Low CVE : CAN-1999-0625
Informational	unknown (32773/udp)	RPC program #100011 version 1 'rquotad' (rquotaprog quota rquota) is running on this port
Warning	unknown (32774/udp)	The rusersd RPC service is running. It provides an attacker interesting information such as how often the system is being used, the names of the users, and so on. It usually not a good idea to leave this service open. Risk factor : Low CVE : CVE-1999-0626
Informational	unknown (32774/udp)	RPC program #100002 version 2 'rusersd' (rusers) is running on this port

Informational	unknown (32774/udp)	RPC program #100002 version 3 'rusersd' (rusers) is running on this port
Informational	unknown (32771/tcp)	RPC program #100002 version 2 'rusersd' (rusers) is running on this port
Informational	unknown (32771/tcp)	RPC program #100002 version 3 'rusersd' (rusers) is running on this port
Warning	unknown (32775/udp)	The sprayd RPC service is running. If you do not use this service, then disable it as it may become a security threat in the future, if a vulnerability is discovered. Risk factor : Low CVE : CAN-1999-0613
Informational	unknown (32775/udp)	RPC program #100012 version 1 'sprayd' (spray) is running on this port
Vulnerability	unknown (32776/udp)	The rpc.walld RPC service is running. Some versions of this server allow an attacker to gain root access remotely, by consuming the resources of the remote host then sending a specially formed packet with format strings to this host. Solaris 2.5.1, 2.6, 7 and 8 are vulnerable to this issue. Other operating systems might be affected as well. *** Nessus did not check for this vulnerability, *** so this might be a false positive Solution : Deactivate this service. Risk factor : High CVE : CAN-2002-0573
Warning	unknown (32776/udp)	The walld RPC service is running. It is usually used by the administrator to tell something to the users of a network by making a message appear on their screen. Since this service lacks any kind of authentication, an attacker may use it to trick users into doing something (change their password, leave the console, or worse), by sending a message which would appear to be written by the administrator. It can also be used as a denial of service attack, by continually sending garbage to the users screens, preventing them from working properly. Solution : Deactivate this service. Risk factor : Medium CVE : CVE-1999-0181
Informational	unknown (32776/udp)	RPC program #100008 version 1 'walld' (rwall shutdown) is running on this port
		The rstatd RPC service is running. It provides an attacker interesting

		information such as : - the CPU usage - the system uptime - its network usage - and more Usually, it is not a good idea to let this service open Risk factor : Low CVE : CAN-1999-0624
Informational	unknown (32777/udp)	RPC program #100001 version 2 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port
Informational	unknown (32777/udp)	RPC program #100001 version 3 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port
Informational	unknown (32777/udp)	RPC program #100001 version 4 'rstatd' (rstat rup perfmeter rstat_svc) is running on this port
Warning	nfs (2049/udp)	The nfsd RPC service is running. There is a bug in older versions of this service that allow an intruder to execute arbitrary commands on your system. Make sure that you have the latest version of nfsd Risk factor : High CVE : CVE-1999-0832
Informational	nfs (2049/udp)	RPC program #100003 version 2 'nfs' (nfsprog) is running on this port
Informational	nfs (2049/udp)	RPC program #100003 version 3 'nfs' (nfsprog) is running on this port
Informational	nfs (2049/udp)	RPC program #100227 version 2 'nfs_acl' is running on this port
Informational	nfs (2049/udp)	RPC program #100227 version 3 'nfs_acl' is running on this port
Vulnerability	unknown (32778/udp)	The remote statd service may be vulnerable to a format string attack. This means that an attacker may execute arbitrary code thanks to a bug in this daemon. *** Nessus reports this vulnerability using only *** information that was gathered. Use caution *** when testing without safe checks enabled. Solution : upgrade to the latest version of rpc.statd Risk factor : High CVE : CVE-2000-0666
Warning	unknown (32778/udp)	The statd RPC service is running. This service has a long history of security holes, so you should really know what you are doing if you decide to let it run. * NO SECURITY HOLE REGARDING THIS PROGRAM HAVE BEEN TESTED, SO

		THIS MIGHT BE A FALSE POSITIVE * We suggest you to disable this service. Risk factor : High CVE : CVE-1999-0018
Informational	unknown (32778/udp)	RPC program #100024 version 1 'status' is running on this port
Informational	unknown (32778/udp)	RPC program #100133 version 1 is running on this port
Informational	unknown (32772/tcp)	RPC program #100024 version 1 'status' is running on this port
Informational	unknown (32772/tcp)	RPC program #100133 version 1 is running on this port
Vulnerability	unknown (32773/tcp)	The tooltalk RPC service is running. There is a format string bug in many versions of this service, which allow an attacker to gain root remotely. *** This warning may be a false positive since the presence *** of the bug was not verified locally. Solution : Disable this service or patch it See also : CERT Advisory CA-2001-27 Risk factor : High CVE : CVE-2001-0717
Informational	unknown (32773/tcp)	RPC program #100083 version 1 is running on this port
Informational	unknown (32774/tcp)	RPC program #100221 version 1 is running on this port
Informational	unknown (32780/udp)	RPC program #100153 version 1 is running on this port
Informational	unknown (32776/tcp)	RPC program #100229 version 1 is running on this port
Informational	unknown (32777/tcp)	RPC program #100230 version 1 is running on this port
Informational	unknown (4045/udp)	RPC program #100021 version 1 'nlockmgr' is running on this port
Informational	unknown (4045/udp)	RPC program #100021 version 2 'nlockmgr' is running on this port
Informational	unknown (4045/udp)	RPC program #100021 version 3 'nlockmgr' is running on this port
Informational	unknown (4045/udp)	RPC program #100021 version 4 'nlockmgr' is running on this port
Informational	unknown (864/udp)	RPC program #160002 version 1 is running on this port
Informational	unknown (32782/udp)	RPC program #100005 version 1 'mountd' (mount showmount) is running on this port
Informational	unknown (32782/udp)	RPC program #100005 version 2 'mountd' (mount showmount) is running on this port
Informational	unknown	RPC program #100005 version 3 'mountd' (mount showmount) is running on this port

	(32782/udp)	
Informational	unknown (32779/tcp)	RPC program #100005 version 1 'mountd' (mount showmount) is running on this port
Informational	unknown (32779/tcp)	RPC program #100005 version 2 'mountd' (mount showmount) is running on this port
Informational	unknown (32779/tcp)	RPC program #100005 version 3 'mountd' (mount showmount) is running on this port
Informational	unknown (32784/udp)	RPC program #300598 version 1 is running on this port
Informational	unknown (32784/udp)	RPC program #805306368 version 1 is running on this port
Informational	unknown (32781/tcp)	RPC program #300598 version 1 is running on this port
Informational	unknown (32781/tcp)	RPC program #805306368 version 1 is running on this port
Informational	unknown (32785/udp)	RPC program #100249 version 1 is running on this port
Vulnerability	unknown (32782/tcp)	The remote RPC service 100249 (snmpXdmid) may be vulnerable to a heap overflow which allows any user to obtain a root shell on this host. *** Nessus reports this vulnerability using only *** information that was gathered. Use caution *** when testing without safe checks enabled. Solution : disable this service (/etc/init.d/init.dmi stop) if you don't use it, or contact Sun for a patch Risk factor : High CVE : CVE-2001-0236
Informational	unknown (32782/tcp)	RPC program #100249 version 1 is running on this port
Informational	general/udp	For your information, here is the traceroute to 199.22.33.44 : 199.22.33.5 199.22.33.44
Warning	xdmcp (177/udp)	The remote host is running XDMCP. This protocol is used to provide X display connections for X terminals. XDMCP is completely insecure, since the traffic and passwords are not encrypted. An attacker may use this flaw to capture all the keystrokes of the users using this host through their X terminal, including passwords. Risk factor : Medium Solution : Disable XDMCP

This file was generated by Nessus, the open-sourced security scanner.

LanGuard Scan from inside the VLAN:

LANguard Network Scanner

Print this page

Scan target : **199.22.33.44** [**1** computers found]

IP Address	Details	Hostname	Username	Operating System
199.22.33.44				SunOS 5.8

199.22.33.44 [ ] SunOS 5.8

IP Address : **199.22.33.44**
Resolved : **horatio.giacfc.com**
Operating System : **SunOS 5.8**
Time to live : **255**

SNMP info (system)

sysUpTime - 101 days, 2 hours, 48 minutes, 19 seconds

sprayd, Ver : 1, Proto : UDP, Port : 32775
walld, Ver : 1, Proto : UDP, Port : 32776
rstatd, Ver : 2, Proto : UDP, Port : 32777
rstatd, Ver : 3, Proto : UDP, Port : 32777
rstatd, Ver : 4, Proto : UDP, Port : 32777
status, Ver : 1, Proto : UDP, Port : 32778
status, Ver : 1, Proto : TCP, Port : 32772
100133, Ver : 1, Proto : UDP, Port : 32778
100133, Ver : 1, Proto : TCP, Port : 32772
100083, Ver : 1, Proto : TCP, Port : 32773
100221, Ver : 1, Proto : TCP, Port : 32774
cachefsd, Ver : 1, Proto : TCP, Port : 32775
dtcalendar, Ver : 2, Proto : UDP, Port : 32779
dtcalendar, Ver : 3, Proto : UDP, Port : 32779
dtcalendar, Ver : 4, Proto : UDP, Port : 32779
dtcalendar, Ver : 5, Proto : UDP, Port : 32779
100153, Ver : 1, Proto : UDP, Port : 32780
100229, Ver : 1, Proto : TCP, Port : 32776
100230, Ver : 1, Proto : TCP, Port : 32777
160002, Ver : 1, Proto : UDP, Port : 864
300384, Ver : 3, Proto : TCP, Port : 878
300385, Ver : 1, Proto : TCP, Port : 880
mountd, Ver : 1, Proto : UDP, Port : 32782
mountd, Ver : 2, Proto : UDP, Port : 32782
mountd, Ver : 3, Proto : UDP, Port : 32782
mountd, Ver : 1, Proto : TCP, Port : 32779
mountd, Ver : 2, Proto : TCP, Port : 32779
mountd, Ver : 3, Proto : TCP, Port : 32779
nfs, Ver : 2, Proto : UDP, Port : 2049
nfs, Ver : 3, Proto : UDP, Port : 2049
nfs_acl, Ver : 2, Proto : UDP, Port : 2049
nfs_acl, Ver : 3, Proto : UDP, Port : 2049
nfs, Ver : 2, Proto : TCP, Port : 2049
nfs, Ver : 3, Proto : TCP, Port : 2049
nfs_acl, Ver : 2, Proto : TCP, Port : 2049
nfs_acl, Ver : 3, Proto : TCP, Port : 2049
300598, Ver : 1, Proto : UDP, Port : 32784
300598, Ver : 1, Proto : TCP, Port : 32781
805306368, Ver : 1, Proto : UDP, Port : 32784
805306368, Ver : 1, Proto : TCP, Port : 32781
snmpXdmid, Ver : 1, Proto : UDP, Port : 32785
snmpXdmid, Ver : 1, Proto : TCP, Port : 32782

512 [Exec => Remote process execution]

513 [Login => Remote login (a la telnet)]

67 [bootps => Bootstrap Protocol Server]

514 [Shell => cmd]

UDP ports - 8 open ports

42 [Name => Name Server]

[illegible] [[illegible]]

[illegible] [[illegible]]

[illegible] [[illegible]]

[illegible] [[illegible]]

[illegible] [[illegible]]

[illegible] [[illegible]]

[illegible] [[illegible]]

[illegible] [[illegible]]

This service is vulnerable to TCP spoofing attacks. If possible use SSH instead.
http://www.cert.org/tech_tips/usc20_full.html#2.4

RLOGIN service enabled

This service is vulnerable to TCP spoofing attacks. If possible use SSH instead.
http://www.cert.org/tech_tips/usc20_full.html#2.4

RSH service enabled

This service is vulnerable to TCP spoofing attacks. If possible use SSH instead.
http://www.cert.org/tech_tips/usc20_full.html#2.4

Telnet service is running

This service is dangerous because it doesn't encrypt data. Sensitive information (usernames+passwords) can be sniffed. If possible use SSH instead.

RPC alerts

Possible snmpXdmid SunOS buffer overflow

Some versions of this service are vulnerable (Run arbitrary commands as root)
http://www.securityfocus.com/bid/2417

Possible statd format string attack

Some versions of this service are vulnerable (Run arbitrary commands as root)
http://www.securityfocus.com/bid/1480

walld message spoofing

An attacker can use this service for spoofing console messages

Miscellaneous alerts

Possible Remote Buffer Overflow Vulnerability in Solaris Print Protocol Daemon

Allow a remote or local attacker to crash the daemon (in.lpd) or execute arbitrary code with super user privilege
http://xforce.iss.net/alerts/advise80.php

Possible Vulnerability in CDE Subprocess Control Service

An attacker can execute arbitrary code with root privileges
http://www.cert.org/advisories/CA-2002-01.html

Thursday, 1 June 2003 - 05:56 PM
Generated by **LANguard Network Security Scanner v(3.0)**

www.gfisoftware.com/lannetscan

References

1. Author Unknown. “docs.sun.com Solaris 8 System Administrator Collection”. Sun Microsystems. Date Unknown. URL: http://docs.sun.com/db/coll/47.11?q=alias (June 18, 2003).

2. Author Unknown. “Covered Entity Decision Tool”. HHS Centers for Medicare and Medicaid Services. Date Unknown. URL: http://cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp. (May 10, 2003).

3. Author Unknown. “HIPAA and ISO 17799”. Treadstone 71. Date Unknown. URL: http://www.treadstone71.com/corpinfo/HIPAA%20and%20ISO%2017799.pdf. (June 15, 2003).

4. Author Unknown. “Securing Solaris”. Admin’s Choice. 2002. URL: http://www.adminschoice.com/docs/securing_solaris.htm. (June 15, 2003).

5. Author Unknown. “The Contents of ISO 17799”. Information Security Policy World. Date Unknown. URL: http://www.information-security-policies-and-standards.com/iso17799what.htm. (May 10, 2003)

6. McClure, Stuart, Scambray, Joel, & Kurtz, George. Hacking Exposed, Third Edition. Berkley: Osborne/McGraw-Hill, 2001. 313-385, 479 - 500.

7. Ross, Keith W. & Kurose, James F. Computer Networking: A Top-Down Approach Featuring the Internet. Addison Wesley, 2002. 650 – 663.