# Global Information Assurance Certification Paper

# Security Audit Report

# For

# GIAC Enterprises

# ISP Division

***Prepared by***

**Gary Needham**

## Executive Summary

The security of GIAC Enterprises ISP division is paramount to the success of the company; therefore, it is crucial that the servers be consistently up to the industry security standards. The purpose of this evaluation is to point out weaknesses of the division's servers to help perpetuate the success of the enterprise.

The ISP division consists of three major servers, each of which has at least one distinct role in the network. They provide several services found at ISPs, including e-mail, web hosting, DNS, web caching, and others.

### *Audit Procedures*

Audit procedures comprised discussions with IT personnel, views of existing policies and documentation, security software scans of the network and machines, password cracking attempts, and evaluations of system daemons and configuration files.

### *Vulnerability Findings*

The vulnerabilities discovered fit into four major categories, each of which have some major problems. Categorized weaknesses appear here, while a prioritized list of specific vulnerabilities is summarized at the end of the report. Lax password policies and plain-text network logins abound. Administrative security policies are almost non-existent. Physical access to servers, especially in one of the rooms, was far too easy. System configuration errors and extra installed software run rampant.

### *Recommended Action*

Action to be taken in light of these vulnerabilities is multi-faceted. System administrators need to take immediate action to rectify password problems that have a likelihood of current exploitation. Significant user education will be involved as well. They should also begin taking steps to remove unnecessary software and configuration options from each server.

Simultaneously, IT management should take appropriate steps to secure the rooms physically. Further, management and systems staff should work together to formulate security policies for the network that can be implemented in the near future. These policies should be reviewed on a regular basis—annually or as major changes are made.

## Audit Report

GIAC Enterprises has decided to provide extra services to premium customers by providing them Internet services in addition to the online fortune cookie sales. As a result, they have set up an appropriate network for the number and network use of their customers. This report is concerned with the security of the servers that provide the Internet services in their current setting. It is not concerned with the security that may be provided with other network designs, proper (or improper) firewall rulesets, and the like. Rather, the company wants to ensure that even if there are problems or failures in those technologies the servers will be as secure as possible.

### *Network Description*

The ISP portion of the network has been set up in two separate rooms due to the geography of the network and the target customers of each server. Room 1 contains the main server and high-speed network connections to several customers. Room 2 contains smaller servers of specific function, some slower customer links, and the Internet access circuits. Both rooms also contain other equipment on and for other segments of the network.

The main server (Server 1) has several functions on the network. Running on Solaris 8, it is the primary e-mail server for the ISP, forwarding mail for other smaller servers on the network and hosting accounts for some users as well. It also serves web pages for the users and acts as a web server for several virtual hosts of customer organizations. It provides primary authentication for some other remote devices and a logging server for other devices which have no ability to log themselves. Finally, it provides DNS service for certain segments of the network.

One of the smaller servers (Server 2) provides only DNS and NTP service for the network. The current operating system is Red Hat Linux 7.

The final server (Server 3) is a web caching server. The current operating system is Red Hat Linux 6.1

### *Physical Security*

The building is secured by an electronic alarm system.

#### Room 1

Security for Room 1 is lacking in a few ways.

- The lock uses a key which is shared with other rooms in the remainder of the building. This means that all employees who have keys to the building are able to access the room.
- Employees have workstations in the same room. While they are trusted with full server access, they also interact with customers in the room, which poses a slight danger.
- The room contains a false ceiling whose access is shared with the surrounding hallway.

- The ventilation system is shared with unsecured rooms.
- The sprinkler system is wet and shared with the rest of the building. The UPS is not connected to the fire detection system.

### Room 2

Security for Room 2 is handled by a different organization in cooperation with the ISP division. Therefore, the security issues surrounding this room are substantially different.

- The room has a unique lock and sparsely distributed key. However, the door is generally left open due to poor ventilation and no air conditioning to the room.
- While it is well known among building employees that the room is for authorized personnel only, it is possible to enter the building and travel to the room with little sight or interruption by building employees. This would be a smaller issue if the former issue were resolved.
- The same false ceiling and fire prevention situations exist for this room as for Room 1.

## *Administrative Policies*

### Backups and Disaster Recovery

The backups for Server 1 are well handled. The process and backup log are well documented, and while not specifically assigned to a person in writing, there is a general understanding about who is responsible for backups (both a primary person and in his absence) within the department. There is always at least one recent backup off site for disaster recovery purposes. Failover hardware is also under consideration but has not yet been implemented.

Backups for the other two servers are currently non-existent. Server 2 requires little for backups because two or three configuration files and a list of installed RPMs would make reinstallation a quick process. These should be manually backed up to a server with external backup media and periodically checked for changes, both in case of intrusion and to keep backups current.

Server 3 contains log files and several large and highly specialized configuration files. While the cache itself is not necessary to back up, the remaining disks have enough changing files for regular backups. A tape drive has been purchased but not yet installed for this system. At the present time, this machine would be difficult to rebuild in the case of a major crash.

Disaster recovery has been discussed frequently and a written policy has been partially developed, but has not been reviewed to include recent server upgrades. Because the ISP portion of the business is not the main business, and because the price break is great enough for GIAC Enterprises customers, disaster recovery plans do not need to provide complete failover capabilities. They should, however, be revised to include recent network and server hardware changes.

### Configuration Changes

Changes in configuration files are mostly restricted to the network administrative team, all of whom share an office. Those changes not done by this team are restricted to isolated files managed by specific users. Administrative policy states that changes are to be logged in the company problem tracking and project management software, but a review of the changes and software entries suggests that the changes are not always logged. No file changing checkout system has been implemented. Further, some system administrators have not been properly trained to check the system logs to verify that the changes made (a) have the desired effect or (b) don't affect other crucial operations of the software.

### Upgrades and Updates

All of the systems have been kept fairly up-to-date. Upgrade policy requires a review of each system's needs at least once each year. Necessary or helpful major upgrades are applied at that time. The systems administrators monitor various bug tracking lists to stay abreast of current developments in software vulnerability.

Server 1 runs Solaris 8, with several third-party software applications installed. Major security holes in the third-party software (such as BIND) are applied shortly after they are announced. Major operating system upgrades are made regularly but patches in between are rarely applied. They need to be more closely monitored and applied.

Server 2 runs Red Hat Linux 7 and only has RPM packages installed, so security updates on this machine have been made easy. This is partly due to its vulnerability as a DNS server and past intrusions into this system.

Server 3 runs Red Hat 6.1 and caching software. Due to the complexity in their configuration files, updates in software are less frequent and more closely scrutinized on this system, and they are applied less often. Unfortunately, the pattern has also followed for the operating system, and this system is not completely up to date on its patches.

### Software Deployment

Software is usually compiled and tested on the production machines. The machines may often have the code in isolated places, but this means that additional, unnecessary software may be running on the system, as even "temporary" installations don't always get removed properly. Further, this means that compilers and development tools are installed on the production machines.

Server 2 is a noticeable exception to this practice. This server has been installed more securely due to the previous problems it has posed to the network.

It would be wise to have extra machines off the main network for development, compiling, and testing of software and software packages before deployment. Further, a rigorous testing and debugging process should be implemented to ensure that new applications will not open up the server to further vulnerability. This is especially true for locally developed applications, which may have security holes open as testing and

development is going on. Incomplete or buggy software that is available to any user that can find it poses a major intrusion threat. In the meantime, for current projects, the development areas should be secured with user- or network-based restrictions on applicable directories.

### *System and User Concerns*

#### Use of root privileges

While the number of people with root privileges is somewhat high, the close proximity of the people that have those privileges offsets the lack of accountability that may come from such a policy. This does increase the possibility that configurations could be simultaneously edited and other, similar problems, though. Each additional root-level account does increase the chances of an intruder gaining root access, though.

Good logs are generally kept of who uses root access, though not necessarily the commands run or the duration of the session. The use of direct login as root from the console is discouraged except during major upgrades or times of network outage.

#### Passwords

The password enforcement for Servers 2 and 3 was not evaluated as closely because (a) only system administrators have accounts on the other machines, and (b) the sheer number of accounts and applications on Server 1. The password policies on servers 2 and 3 are stronger, so vulnerabilities in the systems administrators' passwords are also more likely on Server 1. This lighter evaluation should not be taken as an indication that password security on these machines is less important; there is just a much greater vulnerability on Server 1 due to the lax password rule sets.

On Server 1, the user password scheme has some major security problems. Because of the widespread access to the system (discussed in a later section), the password policy would be expected to be proportionally strict. However, that is not the case. Shadow passwords are used to enhance security, but password-changing procedures do not rule out dictionary words, login names, and common modifications of them. This needs to be remedied immediately, as a recent review of the password file by john-the-ripper (http://www.openwall.com/john/) revealed 25 per cent of the passwords were easily crackable. This represents a huge security problem on the network, and these users should be required to change their passwords as soon as better password choices can be enforced system-wide. Fortunately, none of these accounts have administrative privileges.

#### Installed Libraries and System Utilities

Server 1 currently has a full installation of the operating system on it, including all compilers, extra binaries, and system libraries. This leaves the system slightly more vulnerable to holes, and much more vulnerable to exploits once an intruder has gained access to the system. With the compilers and libraries more restricted, less experienced hackers could have a more difficult time installing rootshell kits and other exploits once in the system. At the very least, they may take more time and have to use someone else's

resources to get the programs installed, which increases their chances of detection. Due to the number of functions on this server, the administrators should consider a development and deployment policy which consists of at least one separate machine used only for that purpose.

A further check with Tiger (http://www.net.tamu.edu/network/tools/tiger.html) reveals that there are several binaries with questionable permissions. A review of the file list indicates that the binaries are original system files, so they probably just need to have the modes and owners changed by the administrator or with a tool such as Casper Dik's fix-modes (ftp://ftp.fwi.uva.nl/pub/solaris/fix-modes.tar.gz). (However, to be more thoroughly safe, the administrator should consider reinstalling the files from the original media while offline and then running fix-modes.)

Server 2 has been installed securely, with only system libraries and utilities necessary for the server function. Tiger found only one exception to this in that /etc/rc.d is installed group writable by default. Because the scan was performed on RedHat 7 and the Tiger signature is not available for the new operating system, Tiger also falsely reported that many system binaries didn't match the binaries that come with the installation. The Server 2 Tiger scan is shown in Appendix A.

Server 3 also has compilers and extra libraries installed, and while they might not be quite as extensive as Server 1, they are certainly sufficient to aid an intruder in his tasks.

### Installed Applications

Server 1 has many operating system and third-party applications running on it. Some of these are required based on the function of the server as a mail and web server for customers. These daemons are generally related to mail and web services and pose no major problems in themselves. However, the sheer number of applications running on the system makes the entire thing much more vulnerable.

A listing of the processes on the system and a review of the various system configuration files, including a check with Tiger reveals the following major applications and daemons on the system.

- Mail applications
  - Sendmail
  - Qpopper
  - WU IMAP
  - getty (for telnet connections) with Pine
- Web applications
  - Apache with DSO support
  - PHP 4
  - Perl 5
  - Webmin
  - WebEvent
  - TWIG
  - Homegrown perl scripts

- Other Service Applications
  - WU FTP
  - MySQL
  - sshd 2
  - BIND
  - Xntpd
  - RADIUS
  - TACACS
- Other Management and Miscellaneous Applications
  - syslog
  - idled
  - snmp services
  - NFS & RPC services
  - IPv6 related daemons
  - Sun Answerbook
  - sadmind
  - Smart Card server
  - LP related daemons

An evaluation of the applications by category reveals some further vulnerabilities that should be addressed as well. First, a review of the configurations and attempting connections for the mail programs reveals that sendmail has the EXPN and VRFY commands enabled. The vulnerabilities with telnet and allowing shell access are well known. It would be wise to impose a restricted shell on all users that use the accounts strictly for mail. Further, if accounts don't use the shell but only check mail by other methods, the shell should be changed for them as well to entirely disallow shell access.

The web applications list reveals a wide array of possibilities, but the list itself doesn't speak for the system security. Apache's configuration is as secure as can be expected considering the server usage. Having PHP and Perl installed implies that there could be a lot of CGI applications running on the system. Members of the system administrative team primarily write these applications, but there are deployment issues that need to be addressed, mentioned earlier in the report. Users are not allowed to post their own CGIs. Requests from customers for CGI scripts on their sites are individually evaluated before being approved, and are rarely implemented.

Notable exceptions to the home-grown CGI applications are WebEvent and TWIG. WebEvent, a calendar-management program, is a purchased application whose source has not been evaluated. TWIG is an open-source web-based mail program that has been growing in popularity and security. TWIG uses IMAP to check mail so relies on IMAP security to access mail. It also connects to a database server (MySQL) which resides on the local server. Finally, WebMin is a separate web server which is used to perform administrative actions on the server via a web browser. All three of these programs rely on password authentication, yet none are currently using SSL.

Several other services are running on the server. All are installed as securely as possible for their given functions. There was a directory in the FTP uploads area (which has been disabled for some time) which could have caused a problem, but uploading was restricted to one legitimate user who had permission to post home pages in a separate location on the system.

As to the management and other applications, an evaluation of the intended server functions reveals that only syslog, idled (an automatic logout checker for telnet sessions), and NFS are currently in use. Further, NFS services are only used for a small backup function of one of the machines on the network. All of the extra services and applications should be disabled.

Server 1 may have the resources to handle all of these services, but to have all of them running together adds vulnerability to the network. Ideally, these services would be separated into at least three major servers. One would be the main mail server, which would also provide web-based mail services, remote authentication, and user home pages. The second would be a web server which provides the main organization and major customer web sites, especially those sites that have CGI and scripting. The third server would basically be like the current Server 2, running DNS and time synchronization services. If separating them is not feasible, the next best option is to run as many of the services as possible in a chrooted environment.

Server 2 is running only the necessary applications and services, with one exception. Because SSH is installed and the server should only authenticate administrative users, even inetd has been disabled. The auth service (identd) has been installed, and the usefulness of this service is questionable.

Server 3 has been almost securely installed from a running process perspective. The extra installed items have been disabled. Because SSH has been recently installed, inetd should also now be turned off. This would eliminate telnet connections as well as anonymous FTP connections, which the administrators didn't realize were enabled.

### Log analysis

While adequate activity logs are kept on all systems, they are not adequately monitored. There is virtually no automated log monitoring in place on Server 1 and Server 2. Server 3 has some monitoring in place but is also lacking. Software such as logcheck (http://www.psionic.com/abacus/logcheck/) should be installed and configured to assist with reading logs and automate the process.

Further, the systems have no extra security logging tools such as tripwire installed. This is already a problem because there is no baseline established to compare against. However, installing such tools now would still help for potential intrusions.

### *Network Vulnerabilities*

#### Open Ports and Connections

Nessus (http://www.nessus.org/) was used to scan the servers and generate a report of open ports and the relative security of those ports. Each server was found to have at least some vulnerability. With a few exceptions, many of these would have been prevented by disabling or not installing extra applications. The nessus report for Server 3 is provided in Appendix B.

Server 1 vulnerabilities, at least those not known from erroneously installed software, include a missing patch on the FTP daemon, allowance of recursive requests to the DNS server (used by attackers for cache poisoning), and some vulnerable default CGI scripts for apache. The report also included the sendmail EXPN and VRFY warnings and NFS & RPC warnings, both of which were already known. Finally, it contained several false positives for some of the other daemons.

Server 2 also had the DNS recursion vulnerability and a warning about the ident service. Since connections should not normally be initiated from this machine, the service is not necessary. Finally, an ICMP timestamp warning was issued.

The report for Server 3 warned of the presence of anonymous FTP and allowed telnet connections, both of which should be turned off. SNMP was running on the system; given the proper community strings, an intruder may be able to gain (or set) valuable network information. The ICMP timestamp warning was also present. Some false positives were given for the caching servers as well.

#### Methods of user connection

Server 1 again presents the greatest vulnerability due to the large number of services running on it. With the exception of telnet, which is described immediately below, all connections are treated equally from within and without the network. This treatment is due to the access allowed to each server by multiple customers. Assuming that "within" the network is different from "without" would potentially allow extra vulnerability to one customer's information by another customer.

Due to past policy, most users have shell access to the machines, although login scripts do guide them to only using specific applications and no prompt. This access is restricted to customer networks—they are not allowed such access from the Internet.

They are, however, allowed FTP access to their accounts from the Internet and POP and IMAP access as well. System administrators are not required (at least through the technology restrictions) to use ssh to connect to the systems, but they use it instead of telnet as a rule.

TCP Wrappers is used for all connections that run through inetd. This further restricts access in only a few cases; it is primarily used for logging purposes. Currently it logs to the default facility (mail), so the logs are intermingled with mail and some other

functions. It would be wise to reconfigure the daemon to log to it's own log file or the LOG_AUTH facility.

The network interfaces are configured properly; however, in a fashion typical with this machine, the software is over-installed. The Ethernet interface is running IP multicast, which has not been utilized on this network, as well as IP version 6, again not utilized.

Server 2, staying true to its installation, is secure on the network side. Libwrap is compiled into the ssh daemon, and other connections are logged. One problem the administrators have faced is some difficulty implementing ntpd version 4, which came with the operating system. Due to these difficulties, they should consider downgrading to the latest version 3 release, with which they are more familiar and which is known to be more stable.

Server 3 has a few openings, though not as many as Server 1. Most crucial is the need to shut off inetd. All inbound connections should be proxy and administrative ssh connections. Therefore, any other listening ports can be shut off. The services which inetd leaves open, while they may not have any direct holes, do open possibilities for retrieving information or attacking the server that may otherwise be closed.

## Vulnerability Summary and Recommended Action

Vulnerabilities cannot be summarized without assuming that action needs to be taken to correct them. Therefore, the vulnerabilities are classified below based on the need for action. Critical vulnerabilities are items that pose an imminent threat to one or more systems on the network and where steps may be needed immediately to secure the network. Serious classification warrants action, but the action is largely needed to maintain security rather than verify it. The moderate vulnerabilities should be addressed like the others, but are not as immediate in nature. Finally, there may be other items suggested throughout the report but not listed specifically here. They are lower-level vulnerabilities but are suggested because there is some risk involved with their current status.

Server 2 has far fewer vulnerabilities than the other systems. It is obvious that the systems administrators both took the past intrusion seriously and researched security issues in the process of reinstalling the system.

### *Critical Needs*

- Correct the password policies on Server 1 and enforce immediate password changes for all accounts as soon as this is done. Especially considering the allowed shell access, each account with a crackable password is a major vulnerability.
- Fix the ventilation system in Room 2. Physical access to machines that critical is a tremendous security threat.
- Utilize encryption over the network as often as possible when passwords are involved. This includes employing SSL for necessary web sites and encouraging and educating users to use clients that support encryption for e-mail.
- Eliminate "Miscellaneous Applications" not needed on Server 1. This task especially includes NFS and other RPC services.
- Reconfigure sendmail without EXPN and VRFY options.

### *Serious Needs*

- Install operating system patches and regularly check for new ones. Specifically, run fix-modes and install patches on Server 1 and install patches on Server 3.
- Re-key the lock in Room 1. Only persons who should have trusted access to the room should be able to get in without a system administrator present.
- Isolate software development and testing. The development should be on separate hardware on a network that is inaccessible from normal users. In the meantime (while that is being implemented), the development area on Server 1 should be isolated from the rest of the applications as much as possible, both through physical (directory) separation and network and user access restrictions.
- Restrict shell access on Server 1 more appropriately for user needs. This is not an imminent need only because shell access has already been restricted for users.
- Develop a written backup and disaster recovery policy for each server, based on hardware needs and necessary recovery time frames.

- Install log checking software (logcheck) and system status software (tripwire) to regularly verify system integrity.

### *Moderate Needs*

- Consider securing the rooms further with walls that prevent access to the false ceilings.
- Train system administrators to properly check logs for the desired effects (and no adverse effects) when making system configuration changes.
- Review the source code of third-party CGIs.
- Reduce the number of installed applications and libraries on Servers 1 and 3. On Server 1, the software development will have to be moved off of the server before this can take place.
- Disable inetd on Server 3 to eliminate anonymous FTP and telnet connections.
- Separate Server 1 applications over multiple servers.

## Appendix A: Server 2 Tiger Scan

Security scripts *** 2.2.3, 1994.0309.2038 ***
Tue Nov 21 15:01:37 CST 2000
15:01> Beginning security report for <servername> (i686 Linux 2.2.16-22).

# Performing check of passwd files...

# Performing check of group files...

# Performing check of user accounts...
# Checking accounts from /etc/passwd.
--WARN-- [acc001w] Login ID adm is disabled, but still has a valid shell (/bin/sh).
--WARN-- [acc001w] Login ID bin is disabled, but still has a valid shell (/bin/sh).
--WARN-- [acc001w] Login ID daemon is disabled, but still has a valid shell (/bin/sh).
--WARN-- [acc001w] Login ID ftp is disabled, but still has a valid shell (/bin/sh).
--WARN-- [acc001w] Login ID games is disabled, but still has a valid shell (/bin/sh).
--WARN-- [acc001w] Login ID <username> is disabled, but still has a valid shell (/bin/bash).
--WARN-- [acc001w] Login ID gopher is disabled, but still has a valid shell (/bin/sh).
--INFO-- [acc002i] Login ID halt is disabled, and has a shell of /sbin/halt.
--WARN-- [acc001w] Login ID <username> is disabled, but still has a valid shell (/bin/bash).
--WARN-- [acc001w] Login ID lp is disabled, but still has a valid shell (/bin/sh).
--INFO-- [acc002i] Login ID named is disabled, and has a shell of /bin/false.
--WARN-- [acc001w] Login ID news is disabled, but still has a valid shell (/bin/sh).
--WARN-- [acc001w] Login ID nobody is disabled, but still has a valid shell (/bin/sh).
--WARN-- [acc001w] Login ID operator is disabled, but still has a valid shell (/bin/sh).
--WARN-- [acc001w] Login ID root is disabled, but still has a valid shell (/bin/bash).
--INFO-- [acc002i] Login ID shutdown is disabled, and has a shell of /sbin/shutdown.
--INFO-- [acc002i] Login ID sync is disabled, and has a shell of /bin/sync.
--WARN-- [acc001w] Login ID uucp is disabled, but still has a valid shell (/bin/sh).
--INFO-- [acc002i] Login ID xfs is disabled, and has a shell of /bin/false.

```
# Performing check of /etc/hosts.equiv and .rhosts files...

# Checking accounts from /etc/passwd...

# Performing check of .netrc files...

# Checking accounts from /etc/passwd...

# Performing check of PATH components...
# Only checking user 'root'

# Performing check of anonymous FTP...
--WARN-- [ftp006w] Anonymous FTP enabled, but directory does not exist.

# Performing checks of mail aliases...
# Checking aliases from /etc/aliases.

# Performing check of `cron' entries...

# Performing check of 'services' and 'inetd'...
# Checking services from /etc/services.
--FAIL-- [inet002f] Service echo is assigned to port 4/ddp which should be
        7/tcp.
--FAIL-- [inet002f] Service echo is assigned to port 4/ddp which should be
        7/udp.
--FAIL-- [inet002f] Service irc is assigned to port 194/tcp which should be
        6667/tcp.
--FAIL-- [inet002f] Service irc is assigned to port 194/udp which should be
        6667/tcp.
--FAIL-- [inet003f] The port for service dos is assigned to service bbs.
--FAIL-- [inet003f] The port for service irc is assigned to service ircd.
--FAIL-- [inet003f] The port for service nfs is assigned to service nfsd.
--FAIL-- [inet003f] The port for service pop-2 is assigned to service pop2.
--FAIL-- [inet003f] The port for service pop-3 is assigned to service pop3.
--FAIL-- [inet003f] The port for service http is assigned to service www.
--INFO-- [inet004i] is (local addition).
--INFO-- [inet004i] afbackup is 2988/tcp (local addition).
--INFO-- [inet004i] afbackup is 2988/udp (local addition).
--INFO-- [inet004i] afpovertcp is 548/tcp (local addition).
--INFO-- [inet004i] afpovertcp is 548/udp (local addition).
--INFO-- [inet004i] amanda is 10080/udp (local addition).
--INFO-- [inet004i] amandaidx is 10082/tcp (local addition).
--INFO-- [inet004i] amidxtape is 10083/tcp (local addition).
--INFO-- [inet004i] asp is 27374/tcp (local addition).
--INFO-- [inet004i] asp is 27374/udp (local addition).
```

--INFO-- [inet004i] at-echo is 204/tcp (local addition).
--INFO-- [inet004i] at-echo is 204/udp (local addition).
--INFO-- [inet004i] at-nbp is 202/tcp (local addition).
--INFO-- [inet004i] at-nbp is 202/udp (local addition).
--INFO-- [inet004i] at-rtmp is 201/tcp (local addition).
--INFO-- [inet004i] at-rtmp is 201/udp (local addition).
--INFO-- [inet004i] at-zis is 206/tcp (local addition).
--INFO-- [inet004i] at-zis is 206/udp (local addition).
--INFO-- [inet004i] auth is 113/tcp (local addition).
--INFO-- [inet004i] bbs is 7000/tcp (local addition).
--INFO-- [inet004i] bgp is 179/tcp (local addition).
--INFO-- [inet004i] bgp is 179/udp (local addition).
--INFO-- [inet004i] biff is 512/udp (local addition).
--INFO-- [inet004i] binkp is 24554/tcp (local addition).
--INFO-- [inet004i] binkp is 24554/udp (local addition).
--INFO-- [inet004i] bootpc is 68/tcp (local addition).
--INFO-- [inet004i] bootpc is 68/udp (local addition).
--INFO-- [inet004i] bootps is 67/tcp (local addition).
--INFO-- [inet004i] bootps is 67/udp (local addition).
--INFO-- [inet004i] cfengine is 5308/tcp (local addition).
--INFO-- [inet004i] cfengine is 5308/udp (local addition).
--INFO-- [inet004i] cfinger is 2003/tcp (local addition).
--INFO-- [inet004i] chargen is 19/tcp (local addition).
--INFO-- [inet004i] chargen is 19/udp (local addition).
--INFO-- [inet004i] cmip-agent is 164/tcp (local addition).
--INFO-- [inet004i] cmip-agent is 164/udp (local addition).
--INFO-- [inet004i] cmip-man is 163/tcp (local addition).
--INFO-- [inet004i] cmip-man is 163/udp (local addition).
--INFO-- [inet004i] codaauth2 is 370/tcp (local addition).
--INFO-- [inet004i] codaauth2 is 370/udp (local addition).
--INFO-- [inet004i] codasrv is 2432/tcp (local addition).
--INFO-- [inet004i] codasrv is 2432/udp (local addition).
--INFO-- [inet004i] codasrv-se is 2433/tcp (local addition).
--INFO-- [inet004i] codasrv-se is 2433/udp (local addition).
--INFO-- [inet004i] conference is 531/tcp (local addition).
--INFO-- [inet004i] courier is 530/tcp (local addition).
--INFO-- [inet004i] csnet-ns is 105/tcp (local addition).
--INFO-- [inet004i] csnet-ns is 105/udp (local addition).
--INFO-- [inet004i] cvspserver is 2401/tcp (local addition).
--INFO-- [inet004i] cvspserver is 2401/udp (local addition).
--INFO-- [inet004i] datametrics is 1645/tcp (local addition).
--INFO-- [inet004i] datametrics is 1645/udp (local addition).
--INFO-- [inet004i] daytime is 13/tcp (local addition).
--INFO-- [inet004i] daytime is 13/udp (local addition).
--INFO-- [inet004i] discard is 9/tcp (local addition).
--INFO-- [inet004i] discard is 9/udp (local addition).

```
--INFO-- [inet004i] domain is 53/tcp (local addition).
--INFO-- [inet004i] domain is 53/udp (local addition).
--INFO-- [inet004i] echo is 4/ddp (local addition).
--INFO-- [inet004i] echo is 7/tcp (local addition).
--INFO-- [inet004i] echo is 7/udp (local addition).
--INFO-- [inet004i] eklogin is 2105/tcp (local addition).
--INFO-- [inet004i] exec is 512/tcp (local addition).
--INFO-- [inet004i] fax is 4557/tcp (local addition).
--INFO-- [inet004i] fido is 60179/tcp (local addition).
--INFO-- [inet004i] fido is 60179/udp (local addition).
--INFO-- [inet004i] finger is 79/tcp (local addition).
--INFO-- [inet004i] fsp is 21/udp (local addition).
--INFO-- [inet004i] ftp is 21/tcp (local addition).
--INFO-- [inet004i] ftp-data is 20/tcp (local addition).
--INFO-- [inet004i] gdomap is 538/tcp (local addition).
--INFO-- [inet004i] gdomap is 538/udp (local addition).
--INFO-- [inet004i] gopher is 70/tcp (local addition).
--INFO-- [inet004i] gopher is 70/udp (local addition).
--INFO-- [inet004i] hmmp-ind is 612/tcp (local addition).
--INFO-- [inet004i] hmmp-ind is 612/udp (local addition).
--INFO-- [inet004i] hostmon is 5355/tcp (local addition).
--INFO-- [inet004i] hostmon is 5355/udp (local addition).
--INFO-- [inet004i] hostnames is 101/tcp (local addition).
--INFO-- [inet004i] https is 443/tcp (local addition).
--INFO-- [inet004i] https is 443/udp (local addition).
--INFO-- [inet004i] hylafax is 4559/tcp (local addition).
--INFO-- [inet004i] icp is 3130/tcp (local addition).
--INFO-- [inet004i] icp is 3130/udp (local addition).
--INFO-- [inet004i] imap2 is 143/tcp (local addition).
--INFO-- [inet004i] imap2 is 143/udp (local addition).
--INFO-- [inet004i] imap3 is 220/tcp (local addition).
--INFO-- [inet004i] imap3 is 220/udp (local addition).
--INFO-- [inet004i] imaps is 993/tcp (local addition).
--INFO-- [inet004i] ingreslock is 1524/tcp (local addition).
--INFO-- [inet004i] ingreslock is 1524/udp (local addition).
--INFO-- [inet004i] ipx is 213/tcp (local addition).
--INFO-- [inet004i] ipx is 213/udp (local addition).
--INFO-- [inet004i] irc is 194/tcp (local addition).
--INFO-- [inet004i] irc is 194/udp (local addition).
--INFO-- [inet004i] ircd is 6667/tcp (local addition).
--INFO-- [inet004i] ircd is 6667/udp (local addition).
--INFO-- [inet004i] isdnlog is 20011/tcp (local addition).
--INFO-- [inet004i] isdnlog is 20011/udp (local addition).
--INFO-- [inet004i] iso-tsap is 102/tcp (local addition).
--INFO-- [inet004i] kamanda is 10081/tcp (local addition).
--INFO-- [inet004i] kamanda is 10081/udp (local addition).
```

```
--INFO-- [inet004i] kerberos is 88/tcp (local addition).
--INFO-- [inet004i] kerberos is 88/udp (local addition).
--INFO-- [inet004i] kerberos-adm is 749/tcp (local addition).
--INFO-- [inet004i] kerberos-iv is 750/tcp (local addition).
--INFO-- [inet004i] kerberos-iv is 750/udp (local addition).
--INFO-- [inet004i] kerberos_master is 751/tcp (local addition).
--INFO-- [inet004i] kerberos_master is 751/udp (local addition).
--INFO-- [inet004i] klogin is 543/tcp (local addition).
--INFO-- [inet004i] knetd is 2053/tcp (local addition).
--INFO-- [inet004i] kpasswd is 761/tcp (local addition).
--INFO-- [inet004i] kpop is 1109/tcp (local addition).
--INFO-- [inet004i] krb524 is 4444/tcp (local addition).
--INFO-- [inet004i] krb5_prop is 754/tcp (local addition).
--INFO-- [inet004i] krb_prop is 754/tcp (local addition).
--INFO-- [inet004i] krbupdate is 760/tcp (local addition).
--INFO-- [inet004i] kshell is 544/tcp (local addition).
--INFO-- [inet004i] laserjet is 9100/tcp (local addition).
--INFO-- [inet004i] ldap is 389/tcp (local addition).
--INFO-- [inet004i] ldap is 389/udp (local addition).
--INFO-- [inet004i] link is 87/tcp (local addition).
--INFO-- [inet004i] linuxconf is 98/tcp (local addition).
--INFO-- [inet004i] login is 513/tcp (local addition).
--INFO-- [inet004i] mailq is 174/tcp (local addition).
--INFO-- [inet004i] mailq is 174/udp (local addition).
--INFO-- [inet004i] mandelspawn is 9359/udp (local addition).
--INFO-- [inet004i] msp is 18/tcp (local addition).
--INFO-- [inet004i] msp is 18/udp (local addition).
--INFO-- [inet004i] mtp is 57/tcp (local addition).
--INFO-- [inet004i] mysql is 3306/tcp (local addition).
--INFO-- [inet004i] mysql is 3306/udp (local addition).
--INFO-- [inet004i] nameserver is 42/tcp (local addition).
--INFO-- [inet004i] nbp is 2/ddp (local addition).
--INFO-- [inet004i] netbios-dgm is 138/tcp (local addition).
--INFO-- [inet004i] netbios-dgm is 138/udp (local addition).
--INFO-- [inet004i] netbios-ns is 137/tcp (local addition).
--INFO-- [inet004i] netbios-ns is 137/udp (local addition).
--INFO-- [inet004i] netbios-ssn is 139/tcp (local addition).
--INFO-- [inet004i] netbios-ssn is 139/udp (local addition).
--INFO-- [inet004i] netnews is 532/tcp (local addition).
--INFO-- [inet004i] netstat is 15/tcp (local addition).
--INFO-- [inet004i] netwall is 533/udp (local addition).
--INFO-- [inet004i] nextstep is 178/tcp (local addition).
--INFO-- [inet004i] nextstep is 178/udp (local addition).
--INFO-- [inet004i] nfsd is 2049/udp (local addition).
--INFO-- [inet004i] ninstall is 2150/tcp (local addition).
--INFO-- [inet004i] ninstall is 2150/udp (local addition).
```

--INFO-- [inet004i] noclog is 5354/tcp (local addition).
--INFO-- [inet004i] noclog is 5354/udp (local addition).
--INFO-- [inet004i] npmp-gui is 611/tcp (local addition).
--INFO-- [inet004i] npmp-gui is 611/udp (local addition).
--INFO-- [inet004i] npmp-local is 610/tcp (local addition).
--INFO-- [inet004i] npmp-local is 610/udp (local addition).
--INFO-- [inet004i] omirr is 808/tcp (local addition).
--INFO-- [inet004i] omirr is 808/udp (local addition).
--INFO-- [inet004i] passwd_server is 752/udp (local addition).
--INFO-- [inet004i] pop2 is 109/tcp (local addition).
--INFO-- [inet004i] pop2 is 109/udp (local addition).
--INFO-- [inet004i] pop3 is 110/tcp (local addition).
--INFO-- [inet004i] pop3 is 110/udp (local addition).
--INFO-- [inet004i] pop3s is 995/tcp (local addition).
--INFO-- [inet004i] poppassd is 106/tcp (local addition).
--INFO-- [inet004i] poppassd is 106/udp (local addition).
--INFO-- [inet004i] postgres is 5432/tcp (local addition).
--INFO-- [inet004i] postgres is 5432/udp (local addition).
--INFO-- [inet004i] prospero is 191/tcp (local addition).
--INFO-- [inet004i] prospero is 191/udp (local addition).
--INFO-- [inet004i] prospero-np is 1525/tcp (local addition).
--INFO-- [inet004i] prospero-np is 1525/udp (local addition).
--INFO-- [inet004i] qmtp is 209/tcp (local addition).
--INFO-- [inet004i] qmtp is 209/udp (local addition).
--INFO-- [inet004i] radacct is 1813/tcp (local addition).
--INFO-- [inet004i] radacct is 1813/udp (local addition).
--INFO-- [inet004i] radius is 1812/tcp (local addition).
--INFO-- [inet004i] radius is 1812/udp (local addition).
--INFO-- [inet004i] re-mail-ck is 50/tcp (local addition).
--INFO-- [inet004i] re-mail-ck is 50/udp (local addition).
--INFO-- [inet004i] rfe is 5002/tcp (local addition).
--INFO-- [inet004i] rfe is 5002/udp (local addition).
--INFO-- [inet004i] rmtcfg is 1236/tcp (local addition).
--INFO-- [inet004i] rpc2portmap is 369/tcp (local addition).
--INFO-- [inet004i] rpc2portmap is 369/udp (local addition).
--INFO-- [inet004i] rsync is 873/tcp (local addition).
--INFO-- [inet004i] rsync is 873/udp (local addition).
--INFO-- [inet004i] rtelnet is 107/tcp (local addition).
--INFO-- [inet004i] rtelnet is 107/udp (local addition).
--INFO-- [inet004i] rtmp is 1/ddp (local addition).
--INFO-- [inet004i] saft is 487/tcp (local addition).
--INFO-- [inet004i] saft is 487/udp (local addition).
--INFO-- [inet004i] sa-msg-port is 1646/tcp (local addition).
--INFO-- [inet004i] sa-msg-port is 1646/udp (local addition).
--INFO-- [inet004i] smux is 199/tcp (local addition).
--INFO-- [inet004i] smux is 199/udp (local addition).

```
--INFO-- [inet004i] snews is 563/tcp (local addition).
--INFO-- [inet004i] snpp is 444/tcp (local addition).
--INFO-- [inet004i] snpp is 444/udp (local addition).
--INFO-- [inet004i] socks is 1080/tcp (local addition).
--INFO-- [inet004i] socks is 1080/udp (local addition).
--INFO-- [inet004i] squid is 3128/tcp (local addition).
--INFO-- [inet004i] ssh is 22/udp (local addition).
--INFO-- [inet004i] ssl-ldap is 636/tcp (local addition).
--INFO-- [inet004i] ssmtp is 465/tcp (local addition).
--INFO-- [inet004i] supfiledbg is 1127/tcp (local addition).
--INFO-- [inet004i] supfilesrv is 871/tcp (local addition).
--INFO-- [inet004i] support is 1529/tcp (local addition).
--INFO-- [inet004i] swat is 901/tcp (local addition).
--INFO-- [inet004i] tfido is 60177/tcp (local addition).
--INFO-- [inet004i] tfido is 60177/udp (local addition).
--INFO-- [inet004i] tproxy is 8081/tcp (local addition).
--INFO-- [inet004i] tproxy is 8081/udp (local addition).
--INFO-- [inet004i] ulistserv is 372/tcp (local addition).
--INFO-- [inet004i] ulistserv is 372/udp (local addition).
--INFO-- [inet004i] vboxd is 20012/tcp (local addition).
--INFO-- [inet004i] vboxd is 20012/udp (local addition).
--INFO-- [inet004i] venus is 2430/tcp (local addition).
--INFO-- [inet004i] venus is 2430/udp (local addition).
--INFO-- [inet004i] venus-se is 2431/tcp (local addition).
--INFO-- [inet004i] venus-se is 2431/udp (local addition).
--INFO-- [inet004i] webcache is 8080/tcp (local addition).
--INFO-- [inet004i] webcache is 8080/udp (local addition).
--INFO-- [inet004i] webster is 765/tcp (local addition).
--INFO-- [inet004i] webster is 765/udp (local addition).
--INFO-- [inet004i] www is 80/tcp (local addition).
--INFO-- [inet004i] www is 80/udp (local addition).
--INFO-- [inet004i] X is 6000/tcp (local addition).
--INFO-- [inet004i] xdmcp is 177/tcp (local addition).
--INFO-- [inet004i] xdmcp is 177/udp (local addition).
--INFO-- [inet004i] xfs is 7100/tcp (local addition).
--INFO-- [inet004i] xtel is 1313/tcp (local addition).
--INFO-- [inet004i] z3950 is 210/tcp (local addition).
--INFO-- [inet004i] z3950 is 210/udp (local addition).
--INFO-- [inet004i] zephyr-clt is 2103/tcp (local addition).
--INFO-- [inet004i] zephyr-clt is 2103/udp (local addition).
--INFO-- [inet004i] zephyr-hm is 2104/tcp (local addition).
--INFO-- [inet004i] zephyr-hm is 2104/udp (local addition).
--INFO-- [inet004i] zephyr-srv is 2102/tcp (local addition).
--INFO-- [inet004i] zephyr-srv is 2102/udp (local addition).
--INFO-- [inet004i] zip is 6/ddp (local addition).
# Checking inetd entries from /etc/inetd.conf
```

```
# Performing NFS exports check...

# Performing check of system file permissions...
--WARN-- [perm006w] /root/.bashrc should not have group read.
--WARN-- [perm006w] /root/.bashrc should not have world read.
--WARN-- [perm006w] /root/.cshrc should not have group read.
--WARN-- [perm006w] /root/.cshrc should not have world read.
--FAIL-- [perm007f] /etc/aliases should not have group read.
--FAIL-- [perm007f] /etc/aliases should not have world read.
--FAIL-- [perm007f] /etc/aliases.db should not have group read.
--FAIL-- [perm007f] /etc/aliases.db should not have world read.
--WARN-- [perm008w] /etc/exports should not have group read.
--WARN-- [perm008w] /etc/exports should not have world read.
--WARN-- [perm003w] /etc/fstab should not have group read.
--WARN-- [perm003w] /etc/fstab should not have world read.
--FAIL-- [perm015f] /etc/rc.d should not have group read.
--FAIL-- [perm015f] /etc/rc.d should not have group search.
--FAIL-- [perm015f] /etc/rc.d should not have world read.
--FAIL-- [perm015f] /etc/rc.d should not have world search.
--WARN-- [perm017w] /var/run/utmp should not have group write.
--WARN-- [perm021w] Disk device /dev/sda1 has read/write access for group
        disk.
--WARN-- [perm021w] Disk device /dev/sdb5 has read/write access for group
        disk.
--WARN-- [perm021w] Disk device /dev/sda6 has read/write access for group
        disk.

# Performing signature check of system binaries...
--WARN-- [sig004w] None of the following versions of /bin/bash (-rwxr-xr-x)
        matched the /bin/bash on this machine.
        >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /bin/login (-rwxr-xr-x)
        matched the /bin/login on this machine.
        >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /bin/mount (-rwsr-xr-x)
        matched the /bin/mount on this machine.
        >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /bin/ping (-rwsr-xr-x)
        matched the /bin/ping on this machine.
        >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /bin/su (-rwsr-xr-x)
```

matched the /bin/su on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /bin/tcsh (-rwxr-xr-x)
matched the /bin/tcsh on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /bin/umount (-rwsr-xr-x)
matched the /bin/umount on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /sbin/cardctl
(-rwxr-xr-x) matched the /sbin/cardctl on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /sbin/netreport
(-rwxr-sr-x) matched the /sbin/netreport on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /sbin/pwdb_chkpwd
(-r-sr-xr-x) matched the /sbin/pwdb_chkpwd on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/bin/at (-rwsr-xr-x)
matched the /usr/bin/at on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/bin/chage
(-rwsr-xr-x) matched the /usr/bin/chage on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/bin/chfn
(-rws--x--x) matched the /usr/bin/chfn on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/bin/chsh
(-rws--x--x) matched the /usr/bin/chsh on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/bin/crontab
(-rwsr-xr-x) matched the /usr/bin/crontab on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/bin/gpasswd
(-rwsr-xr-x) matched the /usr/bin/gpasswd on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/bin/lockfile
(-rwxr-sr-x) matched the /usr/bin/lockfile on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/bin/man (-rwxr-sr-x)
matched the /usr/bin/man on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/bin/newgrp
(-rws--x--x) matched the /usr/bin/newgrp on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/bin/passwd
(-r-s--x--x) matched the /usr/bin/passwd on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/bin/procmail
(-rwsr-sr-x) matched the /usr/bin/procmail on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/bin/suidperl
(-rws--x--x) matched the /usr/bin/suidperl on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/bin/telnet
(-rwxr-xr-x) matched the /usr/bin/telnet on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/bin/wall
(-r-xr-sr-x) matched the /usr/bin/wall on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/bin/write
(-rwxr-sr-x) matched the /usr/bin/write on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/local/bin/ssh
(lrwxrwxrwx) matched the /usr/local/bin/ssh on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/local/sbin/sshd
(lrwxrwxrwx) matched the /usr/local/sbin/sshd on this machine.
>>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/sbin/named

```
        (-rwxr-xr-x) matched the /usr/sbin/named on this machine.
        >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/sbin/ntpdate
        (-rwxr-xr-x) matched the /usr/sbin/ntpdate on this machine.
        >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/sbin/sendmail
        (-r-sr-xr-x) matched the /usr/sbin/sendmail on this machine.
        >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/sbin/tcpd
        (-rwx--x--x) matched the /usr/sbin/tcpd on this machine.
        >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/sbin/traceroute
        (-rwsr-xr-x) matched the /usr/sbin/traceroute on this machine.
        >>>>>> Linux 2.0.35

--WARN-- [sig004w] None of the following versions of /usr/sbin/usernetctl
        (-rwsr-xr-x) matched the /usr/sbin/usernetctl on this machine.
        >>>>>> Linux 2.0.35


# Checking for known intrusion signs...

# Performing check of files in system mail spool...

# Performing system specific checks...
# Performing checks for Linux/2...
# Running './scripts/check_sendmail'...

# Checking sendmail...

# Performing check of embedded pathnames...
--WARN-- [embed001w] Path `/proc/self/exe' contains `/home/gneedham' which is
        not owned by root (owned by gneedham).
        Embedded references in: /bin/ash.static->/default(PATH)
                        /bin/rpm->/default(PATH)
--WARN-- [embed001w] Path `/proc/self/exe' contains
        `/home/gneedham/tiger-2.2.4p1' which is not owned by root (owned by
        2566).
        Embedded references in: /bin/ash.static->/default(PATH)
                        /bin/rpm->/default(PATH)
--WARN-- [embed001w] Path `/proc/self/exe' contains
        `/home/gneedham/tiger-2.2.4p1/bin' which is not owned by root (owned
```

```
        by 2566).
        Embedded references in: /bin/ash.static->/default(PATH)
                        /bin/rpm->/default(PATH)
--WARN-- [embed001w] Path `/proc/self/exe' contains
        `/home/gneedham/tiger-2.2.4p1/bin/realpath' which is not owned by
        root (owned by 2566).
        Embedded references in: /bin/ash.static->/default(PATH)
                        /bin/rpm->/default(PATH)

# Checking setuid executables...
--WARN-- [fsys002w] setuid program /usr/bin/sperl5.6.0 has relative pathnames.
--WARN-- [fsys002w] setuid program /usr/bin/suidperl has relative pathnames.
--WARN-- [fsys002w] setuid program /usr/local/bin/ssh-signer2 has relative
        pathnames.

--INFO-- [fsys004i] The following setuid programs are non-standard:
-r-sr-xr-x root     root     /sbin/unix_chkpwd
-rws--x--x root     root     /usr/bin/sperl5.6.0
-rws--x--x root     root     /usr/local/bin/ssh-signer2


# Checking setgid executables...


# Checking unusual file names...

# Looking for unusual device files...

# Checking symbolic links...
```

## Appendix B: Server 3 Nessus Scan

+ xxx.xxx.xxx.xxx :
. List of open ports :
o ftp (21/tcp) (Security warnings found)
o ssh (22/tcp) (Security notes found)
o telnet (23/tcp) (Security warnings found)
o sunrpc (111/tcp)
o unknown (3128/tcp) (Security hole found)
o webcache (8080/tcp) (Security hole found)
o general/tcp (Security warnings found)
o general/udp (Security notes found)
o snmp (161/udp) (Security warnings found)
o general/icmp (Security warnings found)

. Warning found on port ftp (21/tcp)

The FTP service allows anonymous logins. If you do not
want to share data with anyone you do not know, then you should deactivate
the anonymous account, since it can only cause troubles.
Under most Unix system, doing :
echo ftp >> /etc/ftpusers
will correct this.

Risk factor : Low
CVE : CAN-1999-0497

. Information found on port ftp (21/tcp)

Remote FTP server banner :
localhost.localdomain ftp server (version wu-2.6.0(1) fri jun 23 09:17:44
edt 2000) ready.

. Information found on port ssh (22/tcp)

Remote SSH version : SSH-2.0-2.0.13 (non-commercial)

. Warning found on port 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

. Information found on port telnet (23/tcp)

Remote telnet banner :

<Servername>: <Server Description>

. Vulnerability found on port unknown (3128/tcp) :

The KW whois cgi is installed. This CGI has
a well known security flaw that lets anyone execute arbitrary
commands with the privileges of the http daemon (root or nobody).

Solution : remove it from /cgi-bin or upgrade to version 1.1

Risk factor : Serious

. Warning found on port unknown (3128/tcp)

a web server is running on this
port

. Information found on port unknown (3128/tcp)

The remote web server type is :

Squid/2.3.STABLE4

We recommend that you configure your web server to return
bogus versions, so that it makes the cracker job more difficult

. Vulnerability found on port webcache (8080/tcp) :

The KW whois cgi is installed. This CGI has
a well known security flaw that lets anyone execute arbitrary
commands with the privileges of the http daemon (root or nobody).

Solution : remove it from /cgi-bin or upgrade to version 1.1

Risk factor : Serious

. Warning found on port webcache (8080/tcp)

a web server is running on this
port

. Warning found on port webcache (8080/tcp)

The misconfigured proxy accepts requests coming
from anywhere. This allows attackers to gain some anonymity when browsing
some sensitive sites using your proxy, making the remote sites think that
the requests come from your network.

Solution: Reconfigure the remote proxy so that it only accepts coming
from inside your network.

Risk factor : Low/Medium

. Information found on port webcache (8080/tcp)

The remote web server type is :
Squid/2.3.STABLE4

We recommend that you configure your web server to return
bogus versions, so that it makes the cracker job more difficult

. Warning found on port 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

. Information found on port general/tcp

Nmap found that this host is running Linux 2.1.122 - 2.2.14

. Information found on port general/udp

For your information, here is the traceroute to xxx.xxx.xxx.xxx :
xxx.xxx.xxx.xxx
xxx.xxx.xxx.xxx

. Warning found on port snmp (161/udp)

SNMP Agent port open, it is possible to execute
SNMP GET and SET, (with the proper community
names)

. Warning found on port 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 authentifications protocols.

Solution : filter out the icmp timestamp requests (13), and the outgoing icmp timestamp replies (14).

Risk factor : Low
CVE : CAN-1999-0524

## References

Frisch, Æleen; Essential System Administration, Second Edition; O'Reilly and Associates, Inc.; ©1995

"Internet Software Consortium—BIND," ISC BIND; http://www.isc.org/products/BIND/; Internet Software Consortium; 10 November 2000.

"John the Ripper: Password Cracker," John the Ripper: Password Cracker; http://www.openwall.com/john/; 17 November 2000

"Nessus," Nessus; http://www.nessus.org/; 20 November 2000.

"SunWorld," SunWorld; http://www.sunworld.com; ITWorld.com; ©2000; 16 November 2000.

"Tiger," TAMU Security Tools; http://www.net.tamu.edu/network/tools/tiger.html; CIS Network Group, Texas A&M University; 17 November 2000.

Last Updated: September 23rd, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| **SANS 2018** | **Orlando, FL** | **Apr 03, 2018 - Apr 10, 2018** | **Live Event** |
| **SANS OnDemand** | **Online** | **Anytime** | **Self Paced** |
| **SANS SelfStudy** | **Books & MP3s Only** | **Anytime** | **Self Paced** |