Global Information Assurance Certification Paper

Security Audit of the GIAC Enterprises Batch Computing Farm

October 10th, 2002

Performed by
David J. Bianco
Fictional Audit and Security Team, Inc.

Table of Contents

1 Introduction and Executive Summary

The management at GIAC Enterprises has contracted with Fictional Audit and Security Team, Inc. (FAST) to conduct a security audit of its batch computing farm. After interviewing the system's administrators, collecting various pieces of technical data and interpreting the output of several security analysis tools, FAST has conducted a thorough analysis of the system.

1.1 Purpose of This Document

This document details the auditor's findings and presents several recommendations to improve the security of the batch farm system.

1.2 Audit Methodology

FAST employs a three-pronged methodology to ensure that the audit is as complete as possible. The process includes evaluations of system policies and data flow as well as a detailed technical audit of system configuration and settings. The technical audit evaluates the system's compliance with generally-accepted best practices in the Information Security field. It includes the use of port scanning, security benchmarking and vulnerability analysis tools as well as a considerable amount of manual information gathering, all of which help to gather a complete picture of a system. The results from all phases are collected and then analyzed in context with each other to provide the basis for this report.

1.3 Recommendations

In all, FAST made 38 recommendations, with 14 of them classified as high priority fixes. The recommendations run the gamut from general policy to administrative documentation to setting specific parameters for system software. Although we have found nothing that could accurately be referred to as a "gaping security hole", there are several items that should be addressed immediately, including implementing perimeter and host-based firewalling on the farm system, drastically paring back the amount of software installed with the default OS build and improving the physical security of the computer room by installing electronic card key readers on the two doors which do not already have them. Section 8, entitled Issues and Recommendations, summarizes and prioritizes all recommendations for easy reference.

2 System Description

2.1 Purpose

GIAC Enterprises is the leading manufacturer of online fortune cookie sayings in the world. In the physical realm, fortune cookies just aren't complete without personalized lucky numbers and GIAC Enterprises believes that they are a vital component of fortunes in the online world as well. The system in question is a batch computing farm ("the farm") used by GIAC Enterprises to compute the luckiest numbers for a wide range of circumstances. GIAC and its worldwide network of business/research partners also use it to do basic research in the field of Luck Optimization.

2.2 Components

There are approximately 150 nodes in this farm, the exact number of which varies from day to day according to system maintenance schedules. Each node can be classified into one of four types, as indicated in Table 1. These types reflect the various phases during which new nodes were added to the farm. Note that although each node has a local disk, it is used only for the OS and for swap space. All user home directories, third party applications, scratch space for computations, etc. are hosted on GIAC's high-speed NFS file servers and are therefore identical on each system.

Node Type	Processor	Num CPUs	RAM (MB)	Swap (MB)
Type 1	500 MHz Pentium III	1	256	512
Type 2	750 MHz Pentium III	2	256	512
Type 3	1 GHz Pentium III	2	512	512
Type 4	1.8 GHz Xeon	4	1024	512

Table 1: Types of Farm Nodes

2.3 Operating System

Each farm node runs RedHat Linux 7.2, using a standard kickstart-based installation similar to those used by GIAC's other Linux servers and desktop workstations. It is, therefore, well understood by the administrators, who have customized it extensively. All nodes use a custom built kernel, which is the same across the entire farm. This kernel is based on the standard Linux 2.4.18 kernel plus patches provided by the Linux Kernel Patch Collection[1] project. The LKPC patches include, among other things, support for the XFS journaling file system

and a new, improved process scheduling algorithm, both of which are explicitly desired on these nodes.

Accounts are shared among the nodes via GIAC Enterprises' site-wide NIS database. Enterprise file service is provided by a small collection of various dedicated NFS fileservers.

2.4 Typical Usage

Since the farm is a batch computing resource, jobs arrive via the batch scheduler and are assigned to individual nodes based on a fair sharing policy determined by the system administrator. All input data is contained on NFS mounted file systems served by the site's dedicated file servers, and is read in as needed. Output data is stored on the same file servers at the end of an individual process' lifetime. A small amount of local data may be temporarily stored on the node running a particular job, though this is considered temporary storage and is not guaranteed to be saved after the process completes.

No interactive processing is allowed except for system maintenance. End users cannot log on to the machines and obtain shells. On occasion, the system staff must perform troubleshooting or maintenance on the farm nodes, so they each support SSH servers to facilitate this.

2.5 Network Topology and Access Controls

Each node connects to a 100 Mb/s Ethernet switch. There are a total of 8 switches, each of which connects via gigabit Ethernet to a central interconnect switch. GIAC Enterprises' central NFS file servers also connect via gigabit Ethernet to this switch.

The central switch, in turn, connects to two routers, each also over gigabit Ethernet. The *site router* carries traffic to and from the rest of the GIAC Enterprises LAN, while the *farm router* connects to specialized research and development enclaves run by GIAC's business and research partners elsewhere.

In terms of network access controls, there is no single point where they could conveniently be applied in the current topology. There is no firewall in place at either the farm or the site routers, nor any sort of ingress or egress filtering.

3 Audit Methodology

FAST employs a three-pronged audit methodology to ensure that the audit is as complete as possible. The first prong involves examining the system security, risk management and administration policies to ensure that an organization's approach to security is sound. There are certain commonly accepted criteria for designing information security policies, and although not every criterion applies to each situation, this part of the audit points out those areas of the policy that could be strengthened. It also reveals the intentions of the system's designers and guides the evaluation criteria for the rest of the audit.

The second prong examines the system from a data-flow point of view to determine what data exists, where it is stored and how it is transferred from place to place. This approach showcases the most likely points of attack and helps identify areas that require further scrutiny.

Finally, the third prong of the audit addresses technical vulnerabilities in the underlying hardware and software. This involves a comprehensive audit of the OS security. This is the most complex part of the entire process since it is these vulnerabilities that typically provide the means to exploit any weaknesses found in the other two phases. This process consists of a number of specific checks designed to ensure the system's compliance with current industry-recognized best practices. In addition, several automated tools (port mappers, vulnerability scanners, etc) provide detailed reports, which are then analyzed in context with other data to determine potential vulnerabilities that may be exploited by an attacker.

The end result of the process is this report, which provides summaries of the acceptable findings (often with explanations of why they are acceptable if this is not immediately obvious) along with detailed analyses of instances where a deficiency should be addressed.

Note: Due to the large number of hosts that make up the farm system, technical security checks were not performed on each machine. Instead, a semi-random sampling of the machines was tested. FAST believes that these machines are representative of typical farm nodes, and thus the findings for these nodes will be treated as though they apply to the entire system.

As a result of the audit analysis, FAST has made several recommendations for improving the security of the audited system. In order to make it easier for the reader to quickly locate them in the text, these recommendations are marked with icons in the left margin. High priority items are marked with the lock icon () because they are important parts of locking down your system. Medium and low priority items are marked with the light bulb icon () because they are bright ideas for improving the security of your system overall. In general, these icons appear only with the full discussion of a recommendation. In some cases, recommendations may also be mentioned elsewhere in the text, in which case no icon will be present.

4 Policy Analysis

GIAC Enterprises has established a detailed security and risk management plan. The document is entitled *GIAC Enterprises E-Security Program Plan*[4]. The current revision is version 3.2, dated May 29th, 2002.

4.1 Security Policy

The security policy is quite detailed and conforms to commonly accepted principles as to its content and coverage. It clearly defines the systems it covers

(including the batch farm), the roles and responsibilities of the administration and security teams, protection techniques to be applied, and incident response procedures. In general, the policy is quite complete.

This does not imply that the policy is perfect. There are some areas that could benefit from further scrutiny. In particular, GIAC Enterprises is cooperating with other lucky number researchers around the world to establish a compute grid for cooperative resource sharing. Before the establishment of the grid, all farm users were local and well known to GIAC. The security policy will need to be updated to take into consideration the fact that an increasing number of users from other institutions will be making use of the farm. Although each remote user will still be well known to their home institution, and each home institution will need to enter into an agreement with GIAC to use their resources, the greater level of trust GIAC will be placing in the other institutions should be accounted for and the risks, procedures and countermeasures enumerated.

There also seems to be a logical error in the security policy. The section entitled *Machine Administration Guidelines* defines six classes of machine according to their function. The classes are then referenced elsewhere in the document to specify which security policies apply to them. The class labeled "General Interactive Systems" specifically includes "batch computation servers" (i.e., the farm), but the policies that apply to these nodes are not appropriate. For instance, interactive servers are to "allow logins from all registered users", a policy which is not desired for the farm and doesn't match what is currently implemented.

Aside from these areas, one of which is a minor error and the other is a future consideration, the security policy seems well written, appropriate and complete. It was developed in consultation with the other organizations within GIAC Enterprises, so enjoys site-wide acceptance. The fact that it is only available in hard copy tends to limit its availability, but copies are available in all departments and additional copies can be obtained upon request.

4.2 Risk Management Policy

FAST's audit finds GIAC Enterprises' risk management policy to be sound, though focused a bit more on risks from attack via the Internet than those from internal sources. It follows a prevention/detection/reaction/recovery model and classifies risks into four levels of severity (low, medium, high, very high). The policy correctly identifies the risks associated with a denial of service (DoS) on individual nodes as a low level of concern, though a DoS against the entire system is less likely but more serious. Breach of confidentiality of the data is classed as a medium-level risk, since lucky numbers are notoriously unreliable anyway. Loss of data (e.g. unauthorized deletion) is considered a low risk because it can be mathematically regenerated in a short amount of time. Unauthorized use of the system is termed a risk of medium level, and loss of control of the system by the administrators (i.e. a root-level compromise) is considered a very high risk. GIAC Enterprises is very concerned that these farm nodes not be compromised and turned into a platform from which to launch

further attacks, either to other GIAC systems or to Internet destinations. Unauthorized use and loss of control are the most serious risks addressed by GIAC's risk analysis, and the focus of many of their risk management procedures.

4.3 Administrative Policies and Documentation

This is perhaps GIAC Enterprises' weakest area. Very little written documentation exists in regards to administration policies and procedures for the farm nodes. In fact, very little written documentation exists for any of GIAC's systems. The documentation that does exist is rarely maintained and quickly outdated. The system administration team is quite small and has excellent internal communication, which helps to offset the lack of documentation, but it is difficult to audit compliance with a standard that exists only as a common understanding between administrators.

FAST recommends that GIAC Enterprises develop more comprehensive system administration documentation and keep it up to date. This should be assigned a high priority.

4.4 Backup Policy and Disaster Preparedness

Due to the nature of a batch farm, all nodes are identical (or nearly so), and the loss of one or even several nodes is not considered a major event. No backups are performed since each node can more easily be rebuilt from scratch when necessary, using GIAC's existing automated kickstart configuration process. The output of the batch jobs is saved on the file server, which is regularly backed up.

Disaster preparedness is not such a large issue here, either. Since the primary purpose of the farm is research, short- or medium-term downtime is not a primary concern. In fact, system staff members have occasionally taken the entire farm out of service for periods of up to one week without serious consequence, albeit for scheduled maintenance coordinated in advance with the farm user community. A one week reserve of lucky numbers is kept on hand at all times, which should mitigate any risk of loss of production lucky number generator service associated with short or medium-term outages. Long-term outages (more than one week) should, however, be addressed by the plan.

5 Identification and Protection of Sensitive Data

This section discusses the protection of data, both as it resides on the hosts and as it enters or leaves the host via the network.

5.1 Data on the Host

As discussed in section 4.4, GIAC does not consider the data residing on the server to be at all critical. Unauthorized disclosure of lucky numbers is at best a medium risk since the "luck" associated with a particular number is not an absolutely reliable quality anyway. Unauthorized deletion of the data is of almost no concern, since the numbers can easily be regenerated at any time.

The most critical data on each node is the system password file. Although NIS is the primary repository of user accounts (and comes with its own set of risks outlined below), root's password hash is stored in */etc/passwd* for any user to see. This could allow the system to be compromised by a simple password cracking routine if the administrators are careless in choosing their root password. This is of special concern because the root password on these machines is the same as the one used for most other infrastructure servers. If the password can be guessed, a successful attacker could have her pick of many choice systems on the GIAC LAN. See section 6.5 for more information on our shadow password recommendations.

5.2 Data Transmitted via the Network

In general, network transmissions are limited to batch job submissions, NIS password information, NFS file system traffic and the occasional administrative login session.

Batch submissions can arrive from virtually any machine on the GIAC Enterprises LAN. They are typically of little concern because they consist solely of the name of a program to run, the names of its associated data files and whatever command line parameters are required. Although interception of this data could lead to unauthorized disclosure of some file names that are valid on the system, this information is of little use to an attacker.

Administrative login sessions are likewise of little concern because the site has standardized on SSH for its remote login capability. All sessions are encrypted using strong algorithms (typically Blowfish and 3DES) in combination with SSH protocol 2. These sessions include secure X tunneling, which allows the administrators to use virtually any administration tool on the nodes without fear of network eavesdropping.

Of all these capabilities, NIS and NFS traffic are the most vulnerable to attack. NIS is notorious for transmitting system account information in the clear. GIAC Enterprises' entire Unix network infrastructure relies on NIS, though, so replacement is not an option, at least not in the short term. The nodes use NFSv3 without any special authentication or encryption of the data stream. Each node is part of the farm's private switched network, though, as are the file servers themselves. None of this file system traffic flows through the general GIAC Enterprises LAN and the switched network topology makes sniffing NFS traffic more difficult, though not impossible. Given the previously-stated value of the data, though, FAST finds this to be an appropriate level of protection.

6 Detailed Technical Analysis

Before any system can be considered "secure", adequate physical security must exist to restrict unauthorized access to the system and its components. An attacker with physical access to a system has a great deal of power and may be able to reboot the machine or otherwise bypass access controls which might be

effective in other circumstances. This section discusses the physical and boot-time security of the system.

6.1 Physical Security of the System

The farm nodes are rack mounted in a specialized computer room that also houses other elements of GIAC Enterprises' IT infrastructure. The facility provides adequate climate control, with the average temperature under 70 degrees Fahrenheit even during the summer months with all computers operating at peak capacity. UPS protection and an emergency generator are also provided which can power the facility indefinitely in the event of an interruption to the regular building power.

Access to the room is by means of three doors. The main entrance is controlled by means of an electronic lock keyed to the employees' badges. This is the same system in wide use at the site. Entrance requires an employee to badge in, which generates an audit trail on a central access computer elsewhere. Exit from the main door is controlled via a proximity sensor and does not generate an audit log entry. FAST recommends that all visitors to the room be required to badge out as well as to badge in. The current audit trail is nearly useless, as there is no way to tell how long someone stayed in the room.

Physical keys control the two other entrances, one on the side and one in the rear. The side entrance also has a combination lock that can be used instead of a key to open the door. The same keys which open the computer center doors also open a number of other computer and network related spaces around the site, all of which were at one time operated by computer center staff but some of which are now operated by employees in other departments. Anyone with access to these other areas can still access the computer center through two of its three doors without leaving any sort of audit trail.

The combination to the side door is even more problematic. For some years it has been given out to employees with temporary or casual need to enter the room, so many outside the computer center staff know it and can likewise enter and exit without leaving an audit trail.

FAST recommends that the side and rear entrances be changed over to the electronic badge systems as soon as possible. Additionally, it would be prudent to allow access via physical key through only one door in order to guard against failures in the electronic system. The physical key should be unique to that door and held only by two or three senior computer center and physical plant staff. FAST further recommends that all exits from the room also be logged with an audible alarm triggered locally and at the central security guard console whenever anyone exits without using a badge.

6.2 Boot and System Console Configuration

FAST has examined the system BIOS and boot settings in use on the farm nodes. The following tables summarize the important security-related BIOS

settings. Nodes of type 1, 3 and 4 are represented. No type 2 nodes were available for the BIOS testing; the boot settings, however, were checked.

FAST does not recommend upgrading the BIOS on the type 1 nodes. Although the version is relatively old (4.x, while the latest is 8.x) the BIOS manufacturer, Phoenix Technologies, recommends against upgrading unless required by the addition of new hardware[12]. Since this is not the case, we will follow the vendor and not recommend an upgrade.

We do recommend several changes to the type 1 BIOS configuration, however. First, the BIOS is flash upgradeable, which may allow a successful attacker to overwrite the BIOS. Unless actively involved in performing a BIOS upgrade, FAST recommends always disabling this capability. Further, the floppy drive should not be included in the boot sequence unless the system is actually being upgraded by an administrator. Any user with physical access to the machine (and there are many, as shown in section 6.1) can boot the machine from a floppy and obtain full control over all local data. This includes adding backdoor root accounts for later remote access. Similarly, attackers with physical access should be prevented from modifying the BIOS settings which control all these values by setting a BIOS password and changing the "Security Option" parameter to "Setup" (which will prompt for the password whenever entering the BIOS setup program).

Setting	Recommended Value	Actual Value
BIOS Flash Update	Disabled	**Enabled**
Boot Sequence	C	**A, C**
Security Option	Setup	**System**
Boot Sector Virus Protection	Disabled	Disabled
BIOS Password	Set	**Not Set**

Table 2: Type 1 Node BIOS Settings: Award BIOS v4.51PG (rev 1009)

The BIOS settings of type 3 and 4 nodes are identical, and in better shape. FAST recommends setting BIOS passwords on these as well, and changing the boot device priority as explained above.

Setting	Recommended Value	Actual Value
Event Logging	Enabled	Enabled

ECC Event Logging	Disabled	Disabled
Remote Console Access Feature	Disabled	Disabled
Boot Sector Virus Protection	Disabled	Disabled
Boot Device Priority	LAN	**LAN, Floppy, HD, CDROM**
BIOS Password	Set	**Not Set**

Table 3: Types 3 & 4 Node BIOS Settings: AMIBIOS 7.00.xx (Build 6/13/01)

The BIOS settings are only part of proper boot time security, however. The systems all use lilo, the Linux boot loader. Lilo is responsible for booting the Linux kernel, which controls the entire operating system. The kernel is the core of the OS and as such, it controls the security of the running system. If the kernel is to be considered secure, then the boot time parameters passed to the kernel by lilo must also be secure. Lilo is configured with a standard set of kernel options to use when booting, but anyone with access to the system console can override these, which can lead to system compromise. FAST recommends the use of a lilo boot loader password (the *password* and *restrict* options) [4], which effectively removes this capability from unauthorized users. The following sample */etc/lilo.conf* file is similar to that in use on the farm nodes. Lines in **bold** have been added to effect the recommended changes.

```
prompt
timeout=50
default=linux
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
message=/boot/message
linear
password=ShouldB_h4rd2Gess

image=/boot/vmlinux-2.4.18-lkpc-4
        label=linux
        read-only
        root=/dev/hda3
```

restricted

In addition to boot loader settings, FAST recommends configuring the OS to require a password before entering single user mode[4]. Even if an attacker were successfully denied access to the boot loader flags that normally cause the system to boot into single user mode, there are still other ways of forcing the system to boot into this state. For example, repeatedly turning the system on and off may cause file system errors that will put the machine into maintenance mode. In this mode, the attacker would again have complete access to the entire machine and would be free to steal data, leave backdoors for later, etc. To accomplish this, edit the */etc/inittab* file and replacing the single user line:

I1:Ss1single:wait:/sbin/login

with

I1:Ss1single:wait:/sbin/sulogin

6.3 Operating System Configuration

FAST finds the system's basic OS configuration to be adequate for the security classification of these machines. RedHat Linux 7.2 is still fully supported by the vendor, though an eventual upgrade to 7.3 may be prudent. The system build process includes a basic configuration and hardening script that provides a certain minimum level of security applied throughout the enterprise. All cleartext login methods (telnet, rlogin, rsh, and ftp) have been disabled in favor of SSH and its related utilities. The system default resource limits for number of child processes (1024) and the maximum size of a core file (2MB) are adequate. Other limits such as maximum memory size and CPU time are either inappropriate for the type of computation performed on these systems or handled by the batch queuing environment automatically. The time on all nodes is tightly synched to GIAC Enterprises' enterprise NTP infrastructure.

6.4 Software

Other than jobs submitted by users, there are two main sources of software installed on the machine. Most software is part of the OS install and is managed by the typical RPM package management commands. Some third party software is also available via an NFS mounted partition containing packages compiled from source by GIAC staff (a few pieces of commercial software are also present in this directory). In general, there is a lot of software on the farm that probably should be removed. An important principle of secure system management is "the more software installed on the system, the greater the chance that some vulnerability will be found and exploited."[4] In other words, administrators should try to provide only the tools necessary to do the job and nothing more. This section examines what is necessary and what might be safely removed.

6.4.1 OS Software

Most nodes have exactly the same list of installed RPMs. In our test of 12 randomly selected nodes, only two nodes had any differences in the installed RPMs, one of which was a single extra package. A typical node has 1075 different RPMs installed, a full list of which is included in *Appendix B: Installed RPMs*. The list of installed software includes many packages which should be considered somewhat "dangerous", including the libpcap (network packet sniffing library), tcpdump and ethereal (network packet sniffers using libpcap) and nmap (port scanner and general purpose reconnaissance tool). There are also a large number of other, less immediately dangerous packages for which there is probably no legitimate reason to use, such as XFree86 (a windowing system is not appropriate for a batch farm), compilers, office applications and many others.

FAST strongly recommends reviewing the list of available RPMs to see which could be removed. Our recommendations for which packages to remove can also be found in Appendix B: . If all of our recommendations were followed, the 1075 RPMs currently installed on each node could be reduced to as few as 177 packages, greatly decreasing the risk of having a vulnerable package available.

6.4.2 Third Party Software

Third-party software in the NFS-mounted applications area accounts for approximately another 180 packages available on the system. Most applications in this area are intended solely for interactive users. Applications such as Star Office, EMACS and ImageMagick are not appropriate for farm users. Although some important technical computing libraries do exist there, (maple, matlab) the majority of the software is not needed. FAST recommends that GIAC establish a separate application area just for the farm nodes, which can be stripped of all non-essential software.

6.5 Account and Password Security

User account information for the farm nodes is controlled via GIAC's enterprise-wide NIS domain. Numerous vulnerabilities have been noted in NIS over the years[1], largely due to the lack of a built-in security model. Although there are definite security concerns relating to the use of NIS[9], an analysis of the security of GIAC's NIS infrastructure is outside the scope of this document.

System account information is stored locally in each node's */etc/passwd* file. Shadow passwords are not used, though FAST recommends them highly. Placing the root password hash in a publicly readable file like */etc/passwd* exposes the system to attack via automated password cracking software[11]. FAST strongly recommends using shadow passwords in order to avoid this exposure.

Interactive login access to these machines is controlled via membership in the "giaccc" NIS netgroup. This group contains all members of GIAC's IT staff, not just the administrators of these machines. Further, it includes student interns, system accounts assigned to specific pieces of software and a small number of

unidentified accounts which seem to belong to employees no longer affiliated with the computer center. FAST also strongly recommends that the membership of the giaccc group be updated to include only those with legitimate need to access these machines.

In terms of password security, GIAC Enterprises is nearly above reproach. They have implemented an enterprise wide password change system that employs multiple levels of security, from a rule-based front end that enforces their password re-use and quality policies to a weekly automated attempt to crack all system passwords (this serves as an audit of the effectiveness of the front end). They have even automated the process of password expiration and expiration warnings. FAST finds no improvement necessary in GIAC's password policies or their implementation.

6.6 Services and Daemons

The farm nodes run a minimal set of daemons at boot time, including cron, the NFS automounter and the SSH server, all of which are necessary for proper operation and administration of the system. There are only two daemons, the line printer daemon (lpd) and the mail-processing daemon (sendmail) that should be disabled. Since the systems are not used for interactive processing, there should be no need to print anything from them, nor do they host any printers themselves. Likewise, they do not host email services. Email generated by system processes should be queued and a cron job should be established to run sendmail in queue processing mode (sendmail –q) once every hour, just like the rest of GIAC Enterprises' systems. Both systems are high profile targets for UNIX attackers, so leaving these daemons running when they are not in use could open them up to possible attack.

Xinetd, the newer version of the traditional inetd service manager, is installed on the system. Typically, xinetd monitors specific service ports for incoming connection requests and starts the appropriate processes to service them. These systems, however, do not support the typical services (telnet, rlogin, rsh, echo and others) offered by xinetd. Although xinetd is not started when the system boots, it is possible that a future upgrade, patch or administrative slip could accidentally re-enable it, and consequently offer these forbidden services. Since xinetd is not used anyway, and is never expected to be used on these machines, it should be removed to avoid the possibility of accidentally enabling these services in the future.

Probably the most important recommendation for this section is that the TCP wrappers[9] included with Linux should be configured to allow system access from only a limited number of other hosts on the local network. TCP wrapper support is integrated into many of the services and daemons used on these machines, including the SSH server. By editing */etc/hosts.deny* and */etc/hosts.allow*, the administrators can implement a "deny by default" policy that will be implemented automatically in many of the machines' running services. This will also provide an additional layer of protection in the event that new services are enabled in the future, either accidentally or intentionally.

6.7 Network and Firewall Configuration

All farm nodes connect to one of 8 24 port 10/100 Ethernet switches, which are in turn connected to each other by a gigabyte Ethernet switch. GIAC's central fileservers are directly attached to the gigabyte switch via dedicated gigabyte Ethernet interfaces.

The central gigabyte switch has gigabyte Ethernet connections to GIAC's central site router, and thus to the rest of the LAN and Internet. Unfortunately, there are no firewalls protecting the farm from access via the GIAC LAN. At a minimum, the routers should block all communications between the farm nodes and other parts of the GIAC network. Specifically, the nodes should be allowed access to ports 111 and 733 (the statically configured NIS server port) on the NIS master and slaves. Port 22 (SSH) should also be allowed from a select few management stations as should the ports associated with the batch submission system (listen in Table 4: Nmap Scan Summary). All other ports should be denied access (NFS will still work, since it's got a dedicated connection to the switch). In addition, the router should aggressively filter access from these machines to the Internet, with the exception a few service ports needed to run the grid protocols (the port numbers have not yet been finalized at the time of this audit, so cannot be included here specifically).

FAST also recommends the use of host-based firewalling techniques[16] based on iptables, especially if a hardware firewall or router port blocking is not feasible at this time. At a minimum, this capability would provide a free, flexible firewalling capability that would achieve an effect similar to having a perimeter firewall. Used in conjunction with a real firewall, it provides important defense-in-depth. It would also help the individual nodes resist attacks from other nodes in the event of a partial compromise. In such an event, both parties to a network communication would be behind the hardware firewall and the host-based firewall would be the only level of network security which could be brought to bear.

Finally, there are some minor network stack configuration tweaks that would also provide enhanced security. The most important of these is to disable ICMP ECHO REPLY packets to broadcast pings. With a large number of systems connected to a small LAN, the farm would be an ideal amplifier for a Smurf attack. *Appendix A: Network Tuning Parameters* contains some recommended settings for each system's */etc/sysctl.conf* file which will implement these tuning suggestions.

6.8 Device Security

Security of data on disk or tape is only as good as the security of the device files used by the OS to control access to the data. During this portion of the audit, FAST examined the entire file system for device special files (either block or character type). As expected, all files were in the */dev* hierarchy. FAST also examined the owner, group and permission bits associated with each disk file, and found them all to be owned by root and free of world read, write and execute

access. One puzzling finding was that they were all owned by group "mail". This seems to be an install time default. FAST strongly recommends changing them to be owned by group "root" instead. Other system processes run with group mail permissions, so compromise of one of them could lead to compromise of any data on the system, since the device files all have mode read and write enabled for the group.

6.9 Logging and Monitoring

Logging and monitoring are almost non-existent on these nodes. Although each node has syslog enabled, they all use the standard RedHat syslog.conf file. These log a variety of information, including system logins and logouts, boot time and kernel messages. Unfortunately, they are logged only to the local disk, and not to GIAC's central syslog server. This means that not only are they archived past the system default of 1 month, but also they are also not easily available for system staff to review. No automated reporting or alerting is ever done on these logs, nor do any system administrators ever review them unless there is some specific reason (i.e. e., troubleshooting on a particular node or the suspicion of a security incident). Although the individual availability of each node is monitored on a periodic basis via ping, there is a large opportunity for a clever attacker to remain undetected on these nodes for quite a long time. FAST strongly recommends integrating the logs from these machines into the site's central syslog server and that the administrators review the log reports on a regular basis.

6.10 Host-based IDS and Vulnerability Assessment

Host-based Intrusion Detection System (HIDS) and a routine program of vulnerability assessment are important methods of improving system security. Vulnerability assessments help uncover new ways for attackers to exploit a system, and help system administrators keep current with the most recent threats. HIDS systems are equally important, as they allow administrators to know when their systems are actually under attack. Both are considered important parts of the security cycle, but none are being done on the farm. FAST strongly recommends the use of Tripwire or a similar tool to track changes to important system files. FAST further recommends that these systems be included in GIAC's existing CyberCop vulnerability scans and that the results of these scans be provided to the farm administrators on a regular basis.

6.11 Configuration and Patch Management

GIAC Enterprises has a strong patch management solution in place for RedHat Linux, based on AutoRPM[9], and the farm nodes seem to be configured to participate in this. Our audit showed, however, that several of the latest patches (e.g. OpenSSL) had not yet been applied to any of these nodes, though other non-farm machines using the same AutoRPM configuration had updated themselves long ago. The reason for this discrepancy should be determined and corrected.

Third party software patches are handled on a much more *ad hoc* basis. The major source of third party software on these machines is an NFS mounted application area shared with other Linux workstations and servers on the GIAC LAN. Some commercial applications are installed here, but most are Open Source packages compiled by GIAC staff. They are typically only updated when new functionality is needed or significant security bulletins are issued for any of the included packages. Many of the releases here are old, out of date, or even obsolete according to their maintainers. GIAC staff should periodically review the contents of this application area and verify that the included packages are up to date. This review should happen at least every 6 months.

Although GIAC Enterprises has deployed a configuration management scheme for the majority of its other UNIX systems, no configuration management is in place for the farm nodes. Nodes are built using a standardized, automatic install process so they start out being configured properly. The operational life of a node might be 2 years or more, though, and significant configuration drift can occur. FAST strongly recommends integrating these nodes into the site-wide configuration management system. This will ensure that critical system services stay running, unauthorized services stay shut down, system configuration files are always in a known state and that the farm nodes can easily be included in mass configuration updates when necessary (such as when the root password changes).

7 Automated Scan Results

Fast chose 5 nodes at random on which to run a suite of automated tests. First, we used nmap to gather information about listening ports and services on each hosts. Next, we used the Nessus vulnerability scanner to do a simple network-based vulnerability analysis on the machines. Finally, we used the Center for Internet Security's CISscan tool, which provides a score based upon how closely a system corresponds to various security best practices. In this section, we discuss the results of these scans. The complete reports can be found in the appendices to this document.

7.1 Running Services

Nmap[12] is probably the world's most popular port scanner. It scans a system and reports which TCP ports are open. It also has the option of identifying RPC-based services. Knowing the port numbers that are listening isn't a very reliable indicator about what service is available there, since many services can be offered on arbitrary ports. Also, even knowing the service (i.e. e., an HTTP server) doesn't tell you what software is used to provide that service, or what version number it is. FAST used the *rpcinfo* and *lsof* commands to determine which ports were used by which processes.

Note: By default, most modern Linux systems are resistant to UDP port scans, since they implement ICMP response throttling which slows down the response packets upon which the scanning tools rely. In the interests

of time, FAST has scanned only the TCP ports. Listening UDP ports were properly detected by the rpcinfo and lsof commands.

Port	Service
22	SSH Server
111	portmap
912	ypbind
3878	Batch System
3882	Batch System
32768	rpc.statd
32769	nlockmgr
32770	nlockmgr
32771	Batch System
32772	Batch System

Table 4: Nmap Scan Summary

Table 4 summarizes the output of the Nmap scan. There were minor variations between the hosts tested, but in general they were each very similar to this profile. 6 of the 10 ports belong to easily identifiable, standard UNIX services. Of course, port 22 is used for the SSH server, which is mandatory. The systems all use NIS and NFS, so portmap, ypbind, rpc.statd and nlockmgr are all required. The other ports all belong to the batch system used to manage jobs submitted to the farm. In short, no unusual TCP services were found listening on any of the hosts. All UDP services listed in the lsof and rpcinfo command output were likewise found to belong to legitimate UNIX or batch services required for the farm to operate.

7.2 CIS Security Score

The Center for Internet Security (CIS), a non-profit group of more than 150 companies, government agencies, universities and other organizations publishes a benchmark for minimum security standards[2]. The standards are derived from consensus of best security practices among the member organizations, and have gained much credibility in the security community. CIS also publishes a benchmark-scanning tool, CISscan, which can evaluate a system for compliance with the benchmark and produce a detailed compliance report.

FAST ran this tool on a sampling of 5 farm nodes, and achieved virtually identical results on all of them. All nodes scored a 5.89 out of a possible 10, though this score should not be taken at face value, since the tool flagged several items which FAST believes are not problems in the current configuration. Appendix D: shows the detailed output of this scan for a typical host. In this section, we will analyze the output and make recommendations based on it.

Negative 1.1: System appears not to have been patched within the last month

This seems to be related to the AutoRPM patching problem noted in section 6.11. FAST believes that solving that problem will remove this item from the benchmark report and increase the score.

Negative: 2.2 No Authorized Only banner for telnet in file /etc/xinetd.d/krb5-telnet.

Negative: 2.2 No Authorized Only banner for ftp in file /etc/xinetd.d/gssftp.

Negative: 2.2 No Authorized Only banner for login in file /etc/xinetd.d/rlogin.

Telnet, rlogin and FTP services are disabled on the farm nodes, so no "Authorized Users Only" banner is not necessary, since it would never be displayed anyway.

Negative: 2.7 xinetd either requires global 'only-from' statement or one for each service.

Although xinetd is disabled on the farm nodes, it is possible that it could one day become accidentally re-enabled due to system administrator error or by applying a patch. FAST recommends adding a line like the following to */etc/xinetd.conf* :

only_from=127.0.0.1

This will prevent other hosts from accessing any xinetd services in the event that it is accidentally re-enabled in the future.

Negative: 3.3 NFS script nfslock not deactivated.

Negative: 3.3 NFS script autofs not deactivated.

Negative: 3.4 NIS Client processes (ypbind rc script) not deactivated.

Negative: 3.6 portmapper not deactivated.

Negative: 3.8 netfs rc script not deactivated.

The farm systems rely upon both NFS and NIS in order to function, so all these processes and scripts are necessary.

Negative: 3.9 lpd (line printer daemon) not deactivated.

Since these systems do not host printers, the LPD service should be deactivated as noted in section 6.6.

Negative: 4.1 Coredumps aren't deactivated.

The users who submit batch jobs often require core dumps to analyze program faults, since there is no possibility of interactive debugging access. In addition, the large datasets they process generate large core dumps, so limits on the ability to generate dumps or caps on the maximum size would be inappropriate given the system's intended use.

Negative: 4.3 /proc/sys/net/ipv4/tcp_max_syn_backlog should be at least 4096 to handle SYN floods.

The use of SYN cookies (see section 6.7 and Appendix A:) makes this unnecessary. Filling the connection buffer will have no effect on these machines, since all connection state information can be dynamically recomputed if the client returns the proper cookie.

Negative: 6.1 Removable filesystem /mnt/floppy is not mounted nosuid.

Negative: 6.2 PAM allows users to mount CD-ROMS. (/etc/security/console.perms)

Negative: 6.2 PAM allows users to mount floppies. (/etc/security/console.perms)

There is no reason to allow normal users to mount removable media, since these are batch systems. Furthermore, removable media should not be allowed to contain setuid/setgid files, since anyone using the media should be an administrator and would not require that feature.

FAST recommends adding *nosuid* to the /mnt/floppy line in */etc/fstab*, like so:

```
/dev/fd0/mnt/floppy     auto    noauto,owner,kudzu,nosuid    0       0
```

Furthermore, a normal user's ability to mount floppy or cdrom media should be removed by deleting the following lines from the */etc/security/console.perms* file:

```
<console>   0600  <floppy>      0600  root.floppy
<console>   0600  <cdrom>       0600  root.disk
```

Negative: 7.1 rhosts authentication not deactivated in /etc/pam.d/rlogin.

Negative: 7.1 rhosts authentication not deactivated in /etc/pam.d/rsh.

The .rhosts authentication method allows any user to specify which users on which other machines can log into his or her local account without being prompted for a password. This is dangerous, as a compromise of another trusted machine can lead directly to a compromise of the local machine. Although all services which are known to offer .rhosts authentication have either been disabled or had the .rhosts method turned off, it is a good idea to explicitly disable this authentication mechanism system-wide, in the event that such .rhosts-aware services are accidentally re-enabled in the future.

To accomplish this, remove the lines that end in "pam_rhosts_auth.so" from all files in the */etc/pam.d* directory.

Negative: 7.3 User nscd is not present in /etc/ftpusers

Negative: 7.3 User ident is not present in /etc/ftpusers

Negative: 7.3 User gdm is not present in /etc/ftpusers

Negative: 7.3 User gopher is not present in /etc/ftpusers

Negative: 7.3 User rpc is not present in /etc/ftpusers

Negative: 7.3 User squid is not present in /etc/ftpusers

Negative: 7.3 User apache is not present in /etc/ftpusers

Negative: 7.3 User rpcuser is not present in /etc/ftpusers

Negative: 7.3 User named is not present in /etc/ftpusers

Negative: 7.3 User xfs is not present in /etc/ftpusers

Negative: 7.3 User mailnull is not present in /etc/ftpusers

These users are present in the system password file, which could potentially allow them to authenticate to the system via FTP. However, FTP services are disabled on all the farm nodes. Furthermore, the accounts all have locked passwords and invalid shells, which would prevent them from logging in to FTP in any case. It is prudent to add these names (as well as all other system accounts) to the */etc/ftpusers* file, but this is of low priority since there are three other safeguards in place already which prevent these accounts from logging on through FTP.

Negative: 7.4 Couldn't open cron.allow

Negative: 7.4 Couldn't open at.allow

Only the root account needs to be able to run cron jobs on the farm nodes. Users should never be permitted to use either cron or at to run jobs, since they would not be managed by the batch system's process accounting. Both the */etc/cron.allow* and */etc/at.allow* files should exist, and contain the single line "root". This will prevent non-root users from using cron or at to schedule jobs on the farm nodes.

Negative: 7.5 The permissions on /etc/crontab are not sufficiently restrictive.

The master system crontab file */etc/crontab*, as well as the ancillary crontab files in */etc/cron.d, /etc/cron.hourly, /etc/cron.daily, /etc/cron.weekly and /etc/cron.monthly* are world readable. The named directories are also world readable and listable. This allows any user on the system to have detailed knowledge of which programs are called by root's cron entries and their schedule, which provides a list of high-value targets for attack. FAST recommends executing the following command as root on each node to correct this defect.

chmod –R go-rwx /etc/cron*

Negative: 7.7 /etc/securetty has a non tty1-12 line: tty10.

This is a spurious error message, probably due to a bug in the scanning tool. No action need be taken.

Negative: 7.8 lilo isn't password-protected.

As discussed in section 6.2, the lilo boot loader should be configured to require a password in order to boot the system with alternate kernel options.

Negative: 8.1 news has a valid shell of /bin/sh. Remember, an empty shell field in /etc/passwd signifies /bin/sh.

Even with a locked password, the *news* account should never have a valid shell associated with it, especially on machines that are not news servers. The problem originated because the news server RPMs were installed, which created a server account. These RPMs (inn and inn-devel) should be removed and the account deleted from /etc/passwd.

Negative: 8.2 /etc/passwd contained +: in it!

Negative: 8.3 User +@ccc has no password in /etc/passwd!

Negative: 8.3 User +@ccc has no password in /etc/shadow!

Negative: 8.3 User + has no password in /etc/passwd!

Negative: 8.3 User + has no password in /etc/shadow!

Negative: 8.4 A non-root UID 0 account (named +@ccc) was found.

Negative: 8.4 A non-root UID 0 account (named +) was found.

These are incorrectly flagged. The + and +@ constructs in */etc/passwd* are part of the NIS support, and are meant to include NIS password map entries into the local password file. In particular, the + entry applies to all accounts, and the +@giaccc entry applies to a subset of accounts belonging to GIAC computer center staff. The + entry maps every user's account to the shell */bin/false* which prevents them from logging in, so this is required. Also, the +@giaccc entry is required because it overrides the */bin/false* shell for the system staff so they can continue to access the system. Given that removing NIS is not an option for the farm machines, these warnings can be ignored.

Negative: 8.3 User root has no password in /etc/shadow!

These systems do not use the shadow password facility, which protects an account's password hash string from being viewed by normal user accounts. FAST strongly recommends that root's account use the shadow password facility. Any user on the farm (including batch jobs) can copy root's password hash and try to crack it. Since gaining the root password would mean total system compromise of over 100 machines, this string should be well protected. See the man page for *pwconv(8)*[5] for more details on converting to a shadow password file.

Negative: 8.3 User bin has no password in /etc/shadow!

Negative: 8.3 User daemon has no password in /etc/shadow!

Negative: 8.3 User adm has no password in /etc/shadow!
Negative: 8.3 User lp has no password in /etc/shadow!
Negative: 8.3 User sync has no password in /etc/shadow!
Negative: 8.3 User shutdown has no password in /etc/shadow!
Negative: 8.3 User halt has no password in /etc/shadow!
Negative: 8.3 User mail has no password in /etc/shadow!
Negative: 8.3 User news has no password in /etc/shadow!
Negative: 8.3 User uucp has no password in /etc/shadow!
Negative: 8.3 User operator has no password in /etc/shadow!
Negative: 8.3 User games has no password in /etc/shadow!
Negative: 8.3 User gopher has no password in /etc/shadow!
Negative: 8.3 User ftp has no password in /etc/shadow!
Negative: 8.3 User nobody has no password in /etc/shadow!
Negative: 8.3 User mailnull has no password in /etc/shadow!
Negative: 8.3 User rpm has no password in /etc/shadow!
Negative: 8.3 User xfs has no password in /etc/shadow!
Negative: 8.3 User ntp has no password in /etc/shadow!
Negative: 8.3 User rpc has no password in /etc/shadow!
Negative: 8.3 User gdm has no password in /etc/shadow!
Negative: 8.3 User rpcuser has no password in /etc/shadow!
Negative: 8.3 User nfsnobody has no password in /etc/shadow!
Negative: 8.3 User nscd has no password in /etc/shadow!
Negative: 8.3 User ident has no password in /etc/shadow!
Negative: 8.3 User radvd has no password in /etc/shadow!
Negative: 8.3 User apache has no password in /etc/shadow!
Negative: 8.3 User squid has no password in /etc/shadow!
Negative: 8.3 User named has no password in /etc/shadow!
Negative: 8.3 User pcap has no password in /etc/shadow!
Negative: 8.3 User amanda has no password in /etc/shadow!
Negative: 8.3 User junkbust has no password in /etc/shadow!
Negative: 8.3 User mailman has no password in /etc/shadow!
Negative: 8.3 User mysql has no password in /etc/shadow!
Negative: 8.3 User ldap has no password in /etc/shadow!

Negative: 8.3 User pvm has no password in /etc/shadow!

None of these users have password hash strings in the system password file, so there is no immediate reason for them to be included in the shadow file. These warnings can be ignored for now. Note that in the future, if real passwords are set, they should be set in the shadow password file. It would be prudent to add the entries to the shadow file anyway, to avoid accidentally enabling these accounts in the future.

Negative: 8.10 Default umask may not block world-writable. Check /etc/profile.

Negative: 8.10 Default umask may not block group-writable. Check /etc/profile.

Negative: 8.10 Default umask may not block world-writable. Check /etc/csh.login.

Negative: 8.10 Default umask may not block group-writable. Check /etc/csh.login.

Negative: 8.10 Default umask may not block group-writable. Check /etc/csh.cshrc.

These warnings are couched in "may not" terms because the tool does not check the default umask directly. Rather, it looks to see if a umask is set explicitly in the system default files for Bourne and C Shell users. A umask value of 022, which removes group and world writable bits, is highly recommended, This is the default on these machines according to our tests, even though the umask is not explicitly set. FAST recommends setting the umask explicitly in these files, by including a "umask 022" line at the beginning of each.

Negative: 6.5 Non-standard SUID program /usr/bin/rnews

Negative: 6.5 Non-standard SUID program /usr/bin/sperl5.6.1

Negative: 6.5 Non-standard SUID program /usr/bin/nwsfind

Negative: 6.5 Non-standard SUID program /usr/bin/rlpq

Negative: 6.5 Non-standard SUID program /usr/bin/rlpr

Negative: 6.5 Non-standard SUID program /usr/bin/rlprd

Negative: 6.5 Non-standard SUID program /usr/bin/rlprm

Negative: 6.5 Non-standard SUID program /usr/lib/sendmail

Negative: 6.5 Non-standard SUID program /usr/lib/amanda/calcsize

Negative: 6.5 Non-standard SUID program /usr/lib/amanda/killpgrp

Negative: 6.5 Non-standard SUID program /usr/lib/amanda/rundump

Negative: 6.5 Non-standard SUID program /usr/lib/amanda/runtar

Negative: 6.5 Non-standard SUID program /usr/lib/amanda/dumper

Negative: 6.5 Non-standard SUID program /usr/lib/amanda/planner

Negative: 6.5 Non-standard SUID program /usr/sbin/mailq

Negative: 6.5 Non-standard SUID program /usr/sbin/amcheck

Negative: 6.5 Non-standard SGID program /usr/bin/slrnpull

Setuid programs allow anyone who executes them to run with the temporary privilege of another user. This can open the system to attack if the program is poorly designed. Buffer overflows, race conditions and format string vulnerabilities are just a few of the ways and attacker could trick a setuid program into executing commands on his behalf. Setuid programs should be disabled wherever possible. GIAC Enterprises should review this list to determine which commands can safely be removed (most of them), and which can still operate after removing the setuid bit.

7.3 Vulnerability Analysis

Finally, to conclude the automated portion of the audit, FAST ran the Open Source vulnerability scanner Nessus[6] against 5 of the farm nodes. The results in each case were identical. Although the full scan report can be found in Appendix E: , this section provides more detailed advice for each of the notes, warnings and security holes reported.

Warning found on port general/icmp: The remote host answers to an ICMP timestamp request

The ICMP protocol used by ping can also be used to carry other types of messages. One built-in message is the TIMESTAMP REQUEST message, asking a remote host for its local time. The message indicates that the host replied to one of these requests with a TIMESTAMP REPLY packet. Although this is a relatively low threat level, knowing the value of a system's clock could make it easier for a remote attacker to perpetrate a successful replay attack or predict random numbers using the system's clock as a seed value.

FAST recommends disabling ICMP TIMESTAMP REQUEST messages via *iptables* with the following command, used in conjuction with the host-based firewalling recommendation in section 6.7:

```
iptables –A INPUT –protocol icmp –icmp-type timestamp-request –j DROP
```

Alternatively, the following command could be used to disable all ICMP support, though blocking ECHO REQUEST/ECHO RESPONSE packets may have unintentional side effects, so more testing should be performed before deploying this in a production environment.

```
iptables –A INPUT –protocol icmp –j DROP
```

Warning found on port 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

The farm nodes run NTP version 4.1.0-4, while the latest RPM RedHat offers is 4.1.1-1. This can be corrected by fixing the AutoRPM implementation on these machines, as noted in section 6.11.

Information found on port ntp (123/udp): It is possible to determine a lot of information about the remote host by querying the NTP variables

Although these machines function solely as NTP clients, they still must run the NTP server code, which by default will allow any host to request a wide variety of time-related information from the host. In theory, this could allow an attacker to infer information about the rest of your network by locating other time servers or the IP addresses of the machine's peers. It also allows other clients to use the NTP protocol to determine the system's time, which can lead to exposure as outlined earlier in this section.

To combat this, FAST recommends including NTP access control in the */etc/ntp.conf* file which will deny query rights to all other hosts, like so:

restrict default ignore

Note that this restriction only applies when the machine is acting as a server (which it should never do anyway). Client operation is unaffected by this change.

Warning found on port general/tcp: The remote host uses non-random IP IDs

Each IP datagram generated by a host should contain a unique ID field used in fragment reassembly. Many TCP/IP implementations simply start by assigning the first packet they send an IPID of 0 and then incrementing this ID by 1 for each packet thereafter. Unfortunately, this makes the IPID predictable and exposes to the system to a port scanning technique known as *idle scanning*[12]. This technique involves reading the IPID from a system, causing a third party system to probe a port on the host, then reading the next IPID. If the connection was successful, the IPID would have incremented and the attacker would know that the port was listening. The real attacker, however, would never have scanned the target host directly, and thus they hide more effectively.

FAST believes there is no exposure here. The Linux kernel routinely sets the IPID field of its packets to 0x00 unless fragmentation is expected, so Nessus believes that the IPID is predictable when, in fact, it is not so easy to predict when the IPID is actually being used.

Warning found on port unknown (32770/udp): The nlockmgr RPC service is running.

Warning found on port unknown (32768/udp): The statd RPC service is running.

Warning found on port unknown (909/udp): The ypbind RPC service is running.

These services are all required for normal NFS and NIS operation. No action is required to correct these situations.

8 Issues and Recommendations

This section summarizes the recommendations FAST has made based on this audit. Entries are sorted first by their severity, and then by their location in this report.

This table is intended only as a quick reference. In cases where more information on a specific topic is needed, please refer to the indicated section.

Severity	Section	Issue
HIGH	4.3	Develop and maintain system administration documentation.
HIGH	6.1	Remove combination lock on computer room door. Restrict access via physical key to one door and issue key to only two or three key staff. Require all other users to use electronic badge system to enter and exit the room.
HIGH	6.4.1	Review list of installed RPMs and determine which can be safely removed.
HIGH	6.5	Use shadow passwords for root's account
HIGH	6.5	Update giaccc netgroup membership
HIGH	6.6	Configure TCP Wrappers
HIGH	6.7	Use a firewall between farm and the other networks, including the Internet
HIGH	6.7	Establish host-based firewalls on each node
HIGH	6.9	Integrate syslogs into site-wide collection and review reports on a regular basis.
HIGH	6.10	Use Tripwire or other host-based IDS to help monitor changes to the local file system on each node.
HIGH	6.11	Fix problem which keeps AutoRPM from running regularly.
HIGH	6.11	Integrate nodes into the site-wide configuration management scheme.
HIGH	7.2	Remove news-related RPMs
HIGH	7.2	Disable non-standard setuid programs
Medium	4.1	Farm security policy should be updated for use with the grid.
Medium	4.1	Logical error in security policy mis-classifies farm nodes as "General Interactive Systems."
Medium	4.4	Update disaster recovery policy to include plans for long-term farm outages.

Medium	6.1	Require visitors to badge out of the computer room.
Medium	6.2	Update BIOS settings on all nodes.
Medium	6.2	Require use of a boot loader password
Medium	6.2	Require a password to enter single user mode
Medium	6.4.2	Establish separate, stripped-down third party application area for farm nodes.
Medium	6.6	Disable lpd and sendmail in system startup.
Medium	6.6	Remove xinetd from the system entirely
Medium	6.8	Change group ownership of all disk devices from *mail* to *root*.
Medium	6.11	Periodically review contents of third party application directory and update as necessary.
Medium	7.2	Turn off .rhosts authentication in PAM config files
Medium	7.2	Restrict normal users from accessing cron
Medium	7.2	Change permissions on system crontab files to prevent users from looking at them
Low	6.7	Modify network stack parameters
Low	7.2	Restrict default access to xinetd applications
Low	7.2	Disallow setuid/setgid programs on removable media
Low	7.2	Do not allow users to mount removable media
Low	7.2	Prevent system accounts from logging in via FTP
Low	7.2	Add system accounts to shadow password file, even though they currently have no actual passwords defined
Low	7.2	Set explicit umask in */etc/profile* and */etc/csh.login*
Low	7.3	Disable ICMP TIMESTAMP REQUEST packets
Low	7.3	Restrict access to each node's NTP server

Table 5: List of Recommendations

9 References

1. *Cert Coordination Center*, 26 September 2002. URL: http://www.cert.org (27 September 2002)

2. *CIS Level-1 Benchmark and Scoring Tool for Linux*. URL: http://www.cisecurity.org/bench_linux.html (3 October 2002)
3. *Linux Kernel Patch Collection*, 5 March 2002. URL: http://freshmeat.net/projects/lkpc (25 September, 2002).
4. *Linux Man Page for LILO.CONF(5)*. URL: http://nodevice.com/sections/ManIndex/man0709.html (2 October 2002)
5. *Linux Man Page for PWCONV(8)*. URL: http://nodevice.com/sections/ManIndex/man1255.html. (3 October 2002)
6. *Nessus Web Site*. 26 August 2002. URL: http://www.nessus.org. (3 October 2002)
7. *Securing Linux Step-By-Step Version 2.0 (Advance Copy)*, The SANS Institute. 2002
8. Avian, Robert. *"GIAC Enterprises E-Security Program Plan v3.2"*. Confidential internal document. 29 May 2002.
9. Bauer, Kirk. *AutoRPM*. 4 March 2002. URL: http://www.autorpm.org/ (2 October 2002)
10. Dunne, Paul. *Securing Your Network: An Introduction to TCP Wrappers*. ITWorld.com. 30 June 2000. URL: http://www.itworld.com/AppDev/1076/UIR000630tcp (27 September 2002)
11. Dunne, Paul. *Illuminating Shadow Passwords*. LinuxWorld.com. URL: http://www.linuxworld.com/linuxworld/lw-2000-07/lw-07-shadowpasswords.html (27 September 2002)
12. Fyodor, *Idle Scanning and related IPID games*. URL: http://www.nmap.org/nmap/idlescan.html. (3 October 2002)
13. Fyodor, *Nmap – Free Stealth Scanner For Netowrk Exploration & Security Audits*. URL: http://www.nmap.org/nmap/index.html (2 October 2002)
14. Phoenix Technologies. *BIOS FAQS*. URL: http://www.phoenix.com/en/support/bios+support/awardbios/bios+faqs.htm#Q13 (2 October 2002)
15. Scambray, Joel; McClure, Stuart; Kurtz, George. *Hacking Exposed (Third Ed)*. Berkeley, CA: Osborne/McGraw-Hill, 2002. pp 106 – 107, pg 326.
16. Ziegler, Robert L. *Linux Firewalls (2nd Edition)*. New Riders Publishing. 24 October 2001.

Appendix A: Network Tuning Parameters

The following lines should be added to each system's */etc/sysctl.conf* file to implement some important network security tuning[4]. Comments are included directly into the snippet.

```
# Disallow source routing
net.ipv4.conf.all.accept_source_route=0
# Don't forward packets between interfaces
net.ipv4.conf.all.forwarding=0
# Don't do multicast routing
net.ipv4.conf.all.mc_forwarding=0
# Drop incoming packets if the responses would travel out
# on a different network interface (spoofing protection)
net.ipv4.conf.all.rp_filter=1
# Drop ICMP redirect messages
net.ipv4.conf.all.accept_redirects=0
# Don't send ICMP redirect messages
net.ipv4.conf.all.send_redirects=0
# Disallow Smurf attacks (don't respond to broadcast pings)
net.ipv4.icmp_echo_ignore_broadcasts=1
# Increase resources to mitigate SYN floods
net.ipv4.tcp_max_syn_backlock=1280
# Enable TCP syncookies to fight TCP synflood attacks
net.ipv4.tcp_syncookies=1
```

Appendix B: Installed RPMs

The following is a list of RPM packages installed on the systems. Entries in **bold** are packages which FAST recommends be reviewed by the administration staff to determine whether or not they can be safely removed.

4Suite-0.11-2
a2ps-4.13b-15
adjtimex-1.11-5
alchemist-1.0.18-1
alchemist-devel-1.0.18-1
alien-7.24-3
amanda-2.4.2p2-4
amanda-client-2.4.2p2-4
amanda-devel-2.4.2p2-4
amanda-server-2.4.2p2-4
am-utils-6.0.6-3
anaconda-7.2-7
anaconda-runtime-7.2-7
anacron-2.3-17
anonftp-4.0-9
apache-devel-1.3.22-6
apache-manual-1.3.22-6
apmd-3.0final-34
arpwatch-2.1a11-11.7.2.0
arts-2.2.2-2
ash-0.3.7-2
asp2php-0.75.17-1
asp2php-gtk-0.75.17-1
aspell-0.33.7-1
aspell-devel-0.33.7-1
at-3.1.8-23
audiofile-0.2.1-2
audiofile-devel-0.2.1-2
aumix-2.7-5
aumix-X11-2.7-5
authconfig-4.1.19.2-1
autoconf-2.13-14
autofs-3.1.7-21
automake-1.4p5-2
autorun-2.7-1
awesfx-0.4.3a-8
balsa-1.2.3-1
basesystem-7.0-2
bash-2.05-8
bash-doc-2.05-8
bc-1.06-5
bcm5820-1.17-6
bdflush-1.5-17
bind-9.2.1-0.7x
bindconf-1.6.1-1
bind-devel-9.2.1-0.7x
bind-utils-9.2.1-0.7x
binutils-2.11.90.0.8-12
bison-1.28-7
blas-3.0-12
blas-man-3.0-12
blt-2.4u-7
bonobo-1.0.7-2
bonobo-devel-1.0.7-2
bootparamd-0.17-7
bug-buddy-2.0.6-4
busybox-0.51.062801-3
busybox-anaconda-0.51.062801-3
byacc-1.9-19
bzip2-1.0.1-4
bzip2-devel-1.0.1-4
bzip2-libs-1.0.1-4
caching-nameserver-7.2-1
cadaver-0.17.0-2
Canna-devel-3.5b2-50
Canna-libs-3.5b2-50
cdda2wav-1.10-4
cdecl-2.5-20
cdlabelgen-1.5.0-9
cdp-0.33-21
cdparanoia-alpha9.8-2
cdparanoia-devel-alpha9.8-2
cdrdao-1.1.3-10
cdrecord-1.10-4
cdrecord-devel-1.10-4
cervisia-1.4.1-2
chkconfig-1.2.24-1
chkfontpath-1.9.5-2
chromium-0.9.12-5
cipe-1.4.5-6
cleanfeed-0.95.7b-12
compat-egcs-6.2-1.1.2.16
compat-egcs-c++-6.2-1.1.2.16
compat-egcs-g77-6.2-1.1.2.16
compat-egcs-objc-6.2-1.1.2.16
compat-glibc-6.2-2.1.3.2
compat-libs-6.2-3
compat-libstdc++-6.2-2.9.0.16
comsat-0.17-3
console-tools-19990829-36
control-center-1.4.0.1-18
control-center-devel-1.4.0.1-18
cpio-2.4.2-23
cpp-2.96-98
cproto-4.6-9
cracklib-2.7-12
cracklib-dicts-2.7-12
crontabs-1.10-1
ctags-5.0.1-2
curl-7.8-1
curl-devel-7.8-1
cvs-1.11.1p1-7
cWnn-devel-1.11-19
cyrus-sasl-1.5.24-23
cyrus-sasl-devel-1.5.24-23
cyrus-sasl-gssapi-1.5.24-23
cyrus-sasl-md5-1.5.24-23
cyrus-sasl-plain-1.5.24-23
dateconfig-0.7.4-6
db1-1.85-7
db1-devel-1.85-7

db2-2.4.14-7
db2-devel-2.4.14-7
db31-3.1.17-1
db3-3.2.9-4
db3-devel-3.2.9-4
db3-utils-3.2.9-4
dbskkd-cdb-1.01-9
ddd-3.3.1-5
dejagnu-1.4.1-2
desktop-backgrounds-1.1-4
dev-3.2-5
dev86-0.15.5-1
dhcp-2.0pl5-8
dhcpcd-1.3.18pl8-13
dia-0.88.1-3
dialog-0.9a-5
diffstat-1.28-1
diffutils-2.7.2-2
dip-3.3.7o-23
diskcheck-1.1-1
Distutils-1.0.2-2
dmalloc-4.8.1-6
docbook-dtd30-sgml-1.0-10
docbook-dtd31-sgml-1.0-10
docbook-dtd40-sgml-1.0-11
docbook-dtd412-xml-1.0-1
docbook-dtd41-sgml-1.0-10
docbook-dtd41-xml-1.0-7
docbook-style-dsssl-1.64-3
docbook-utils-0.6.9-2.1
docbook-utils-pdf-0.6.9-2.1
dos2unix-3.1-7
dosfstools-2.7-1
doxygen-1.2.8.1-1
doxygen-doxywizard-1.2.8.1-1
dump-0.4b25-1.72.0
e2fsprogs-1.26-1.72
e2fsprogs-devel-1.26-1.72
ed-0.2-21
ee-0.3.12-5
eel-1.0.2-2
eel-devel-1.0.2-2
efax-0.9-9
eject-2.0.9-2
ElectricFence-2.2.2-8
elm-2.5.6-1
emacs-20.7-41
emacs-el-20.7-41
emacs-nox-20.7-41
emacs-X11-20.7-41
enlightenment-0.16.4-11
enscript-1.6.1-16.2
eruby-0.1.2-1
esound-0.2.22-5
esound-devel-0.2.22-5
ethereal-0.9.4-0.7.2.0
ethereal-gnome-0.9.4-0.7.2.0
ethtool-1.2-1
exmh-2.4-2
expat-1.95.1-7
expat-devel-1.95.1-7
expect-5.32.2-65
ext2ed-0.1-26
extace-1.5.1-3
fam-2.6.4-11
fam-devel-2.6.4-11
fbset-2.1-8
fetchmail-5.9.0-11
fetchmailconf-5.9.0-11
file-3.35-2
filesystem-2.1.6-2
fileutils-4.1-4
findutils-4.1.7-1
finger-0.17-9
finger-server-0.17-9
firewall-config-0.95-4
flex-2.5.4a-15
fnlib-0.5-9
fnlib-devel-0.5-9
foomatic-1.1-0.20011218.3
fortune-mod-1.0-16
freecdb-0.62-4
freeciv-1.12.0-1
freetype-2.0.3-7
freetype-devel-2.0.3-7
freetype-utils-2.0.3-7
FreeWnn-devel-1.11-19
FreeWnn-libs-1.11-19
ftp-0.17-12
ftpcopy-0.3.9-1
fvwm2-2.2.5-4
fvwm2-icons-2.2.5-4
gaim-0.11.0pre4-5
gal-0.8-6
gal-devel-0.8-6
galeon-1.2.0-4
gated-3.6-12
gawk-3.1.0-3
gcc-2.96-98
gcc3-3.0.4-1
gcc3-c++-3.0.4-1
gcc3-g77-3.0.4-1
gcc3-java-3.0.4-1
gcc3-objc-3.0.4-1
gcc-c++-2.96-98
gcc-chill-2.96-98
gcc-g77-2.96-98
gcc-java-2.96-98
gcc-objc-2.96-98
GConf-1.0.4-3
GConf-devel-1.0.4-3
gd-1.8.4-4
gdb-5.1-1
gdbm-1.8.0-10
gdbm-devel-1.8.0-10
gd-devel-1.8.4-4
gdk-pixbuf-0.11.0-8
gdk-pixbuf-devel-0.11.0-8
gdk-pixbuf-gnome-0.11.0-8
gdm-2.2.3.1-20
gd-progs-1.8.4-4
gedit-0.9.4-6
genromfs-0.3-9
gettext-0.10.38-7
gftp-2.0.8-2
ggv-1.0.1-4
ghostscript-6.51-16.2
ghostscript-fonts-5.50-3
giftrans-1.12.2-9
gimp-1.2.1-7
gimp-data-extras-1.2.0-2
gimp-devel-1.2.1-7
gimp-perl-1.2.1-7
gkermit-1.0-9
gkrellm-1.0.8-5
glade-0.6.2-3
glib10-1.0.6-10
glib-1.2.10-5

glibc-2.2.4-24
glibc-common-2.2.4-24
glibc-devel-2.2.4-24
glibc-profile-2.2.4-24
glib-devel-1.2.10-5
glms-1.03-11
gmp-3.1.1-4
gmp-devel-3.1.1-4
gnome-applets-1.4.0.1-6
gnome-audio-1.0.0-12
gnome-audio-extra-1.0.0-12
gnome-core-1.4.0.4-38
gnome-core-devel-1.4.0.4-38
gnome-games-1.4.0.1-4
gnome-games-devel-1.4.0.1-4
gnomeicu-0.96.1-3
gnome-kerberos-0.2.2-4
gnome-libs-1.2.13-16
gnome-libs-devel-1.2.13-16
gnome-linuxconf-0.67.1-1
gnome-lokkit-0.50-6
gnome-media-1.2.3-4
gnome-pim-1.2.0-13
gnome-pim-devel-1.2.0-13
gnome-print-0.29-6
gnome-print-devel-0.29-6
gnome-user-docs-1.4.1-1
gnome-utils-1.4.0-4
gnome-vfs-1.0.1-17
gnome-vfs-devel-1.0.1-17
gnome-vfs-extras-0.1.3-1
gnorpm-0.96-12.7x
gnucash-1.6.2-1
gnuchess-4.0.pl80-8
gnumeric-0.67-10
gnumeric-devel-0.67-10
gnupg-1.0.6-3
gnuplot-3.7.1-13
gperf-2.7.2-1
gphoto-0.4.3-13
gpm-1.19.3-20
gpm-devel-1.19.3-20
gq-0.4.0-3
gqview-0.8.1-5
grep-2.4.2-7
grip-2.96-1
groff-1.17.2-7.0.2
groff-gxditview-1.17.2-7.0.2
groff-perl-1.17.2-7.0.2
grub-0.90-11
gsl-0.9-1
gsm-1.0.10-3
gsm-devel-1.0.10-3
gtk+10-1.0.6-10
gtk+-1.2.10-11
gtk+-devel-1.2.10-11
gtk-doc-0.5.9-1
gtk-engines-0.11-3
gtkglarea-1.2.2-10
gtkhtml-0.9.2-9
gtkhtml-devel-0.9.2-9
Gtk-Perl-0.7008-3
gtoaster-1.0beta2-3
gtop-1.0.13-4
guile-1.3.4-16
guile-devel-1.3.4-16
Guppi-0.35.5-7
Guppi-devel-0.35.5-7
gv-3.5.8-13
g-wrap-1.1.10-5
g-wrap-devel-1.1.10-5
gzip-1.3-15
hdparm-4.1-2
hexedit-1.2.1-3
hotplug-2001_04_24-11
hotplug-gtk-2001_04_24-11
htdig-3.2.0-2.011302
htdig-web-3.2.0-2.011302
htmlview-1.2.0-1
hwbrowser-0.3.5-2
ical-2.2-25
ImageMagick-5.3.8-3
ImageMagick-c++-5.3.8-3
ImageMagick-c++-devel-5.3.8-3
ImageMagick-devel-5.3.8-3
ImageMagick-perl-5.3.8-3
imap-2001a-1.72.0
imap-devel-2001a-1.72.0
imlib-1.9.13-3.7.x
imlib-cfgeditor-1.9.13-3.7.x
imlib-devel-1.9.13-3.7.x
indent-2.2.6-2
indexhtml-7.2-1
inews-2.3.2-5
info-4.0b-3
initscripts-6.43-1
inn-2.3.2-5
inn-devel-2.3.2-5
ipchains-1.3.10-10
iproute-2.2.4-14
iptables-1.2.4-2
iptables-ipv6-1.2.4-2
iptraf-2.4.0-5
iputils-20001110-6
ipxutils-2.2.0.18-6
irb-1.6.4-2
ircii-4.4Z-7
irda-utils-0.9.14-2
isapnptools-1.22-5
iscsi-2.0.1.8-2
isdn4k-utils-3.1-46
isdn4k-utils-vboxgetty-3.1-46
isicom-1.0-8
itcl-3.2-65
jadetex-3.11-4
jed-0.99.14-2
jed-common-0.99.14-2
jed-xjed-0.99.14-2
jikes-1.14-1
joe-2.9.6-2
joystick-1.2.15-9
jpilot-0.99-7
junkbuster-2.0.2-28
kaffe-1.0.6-6
kakasi-dict-2.3.2-4
kbdconfig-1.9.14-1
kdbg-1.2.1-5
kde1-compat-1.1.2-11

kde1-compat-devel-1.1.2-11
kdeaddons-kate-2.2.2-1
kdeaddons-kicker-2.2.2-1
kdeaddons-knewsticker-2.2.2-1
kdeaddons-konqueror-2.2.2-1
kdeaddons-noatun-2.2.2-1
kdeadmin-2.2.2-3
kdeartwork-2.2.2-1
kdeartwork-locolor-2.2.2-1
kdebase-2.2.2-1
kdebase-devel-2.2.2-1
kdebindings-2.2.2-1
kdebindings-devel-2.2.2-1
kdebindings-kmozilla-2.2.2-1
kdebindings-perl-2.2.2-1
kdebindings-python-2.2.2-1
kdegames-2.2.2-1
kdegraphics-2.2.2-1
kdegraphics-devel-2.2.2-1
kde-i18n-Bulgarian-2.2.2-2
kde-i18n-Chinese-Big5-2.2.2-8
kde-i18n-Hebrew-2.2.2-2
kde-i18n-Lithuanian-2.2.2-2
kde-i18n-Polish-2.2.2-2
kdelibs-2.2.2-2
kdelibs-devel-2.2.2-2
kdelibs-sound-2.2.2-2
kdelibs-sound-devel-2.2.2-2
kdemultimedia-2.2.2-2
kdemultimedia-devel-2.2.2-2
kdenetwork-2.2.2-1
kdenetwork-ppp-2.2.2-1
kdepim-2.2.2-3
kdepim-cellphone-2.2.2-3
kdepim-devel-2.2.2-3
kdepim-pilot-2.2.2-3
kdesdk-2.2.2-1
kdesdk-devel-2.2.2-1
kdetoys-2.2.2-1
kdeutils-2.2.2-1
kdevelop-2.0.2-2
kdoc-2.2.2-1
kernel-2.4.7-10
kernel-2.4.9-34
kernel-debug-2.4.7-10
kernel-doc-2.4.9-34
kernel-headers-2.4.9-34
kernel-pcmcia-cs-3.1.27-10
kernel-smp-2.4.7-10
kernel-smp-2.4.9-34
kernel-source-2.4.9-34
koffice-1.1.1-2
koffice-devel-1.1.1-2
kpppload-1.04-29
krb5-devel-1.2.2-13
krb5-libs-1.2.2-13
krb5-server-1.2.2-13
krb5-workstation-1.2.2-13
krbafs-1.0.9-2
krbafs-devel-1.0.9-2
krbafs-utils-1.0.9-2
ksconfig-1.9.8-4
ksymoops-2.4.1-1
kudzu-0.99.23-1
kudzu-devel-0.99.23-1
kWnn-devel-1.11-19
lam-6.5.4-1
lapack-3.0-12
lapack-man-3.0-12
lclint-2.5q-4
less-358-21
lesstif-0.92.32-6
lesstif-devel-0.92.32-6
lftp-2.4.0-2
lha-1.00-17
libao-0.8.0-1
libao-devel-0.8.0-1
libcap-1.10-5
libcap-devel-1.10-5
libelf-0.7.0-1
libesmtp-0.8.4-2
libesmtp-devel-0.8.4-2
libgal7-0.8-6
libgcc-3.0.4-1
libgcj-2.96-28
libgcj3-3.0.4-1
libgcj3-devel-3.0.4-1
libgcj-devel-2.96-28
libghttp-1.0.9-2
libghttp-devel-1.0.9-2
libglade-0.16-4
libglade-devel-0.16-4
libgnomeprint15-0.29-6
libgtop-1.0.12-4
libgtop-devel-1.0.12-4
libgtop-examples-1.0.12-4
libjpeg6a-6a-8
libjpeg-6b-16
libjpeg-devel-6b-16
libmng-1.0.2-1
libmng-devel-1.0.2-1
libmng-static-1.0.2-1
libodbc++-0.2.2pre4-12
libodbc++-devel-0.2.2pre4-12
libodbc++-qt-0.2.2pre4-12
libogg-1.0rc2-1
libogg-devel-1.0rc2-1
libole2-0.2.3-1
libole2-devel-0.2.3-1
libpcap-0.6.2-11.7.2.0
libpng-1.0.12-2
libpng-devel-1.0.12-2
libPropList-0.10.1-8
librep-0.13.6-5

librep-devel-0.13.6-5
librsvg-1.0.0-7
librsvg-devel-1.0.0-7
libsigc++-1.0.3-5
libsigc++-devel-1.0.3-5
libstdc++-2.96-98
libstdc++3-3.0.4-1
libstdc++3-devel-3.0.4-1
libstdc++-devel-2.96-98
libtermcap-2.0.8-28
libtermcap-devel-2.0.8-28
libtiff-3.5.5-13
libtiff-devel-3.5.5-13
libtool-1.4-8
libtool-libs13-1.3.5-2
libtool-libs-1.4-8
libungif-4.1.0-9
libungif-devel-4.1.0-9
libungif-progs-4.1.0-9
libunicode-0.4-6
libunicode-devel-0.4-6
libuser-0.32-1
libuser-devel-0.32-1
libvorbis-1.0rc2-2
libvorbis-devel-1.0rc2-2
libxml10-1.0.0-8
libxml-1.8.14-2
libxml2-2.4.10-0.7x.2
libxml2-devel-2.4.10-0.7x.2
libxml-devel-1.8.14-2
libxslt-1.0.7-2
libxslt-devel-1.0.7-2
licq-1.0.3-7
licq-gnome-1.0.3-7
licq-kde-1.0.3-7
licq-qt-1.0.3-7
licq-text-1.0.3-7
lilo-21.4.4-14
links-0.96-2
linuxconf-1.25r7-3
linuxconf-devel-1.25r7-3
lm_sensors-2.5.5-6
lm_sensors-devel-2.5.5-6
locale_config-0.3.2-1
lockdev-1.0.0-14
lockdev-devel-1.0.0-14
logrotate-3.5.9-1
lokkit-0.50-6
losetup-2.11g-5
lout-3.17-9
lout-doc-3.17-9
LPRng-3.7.4-28.1
lrzsz-0.12.20-10
lslk-1.28-1
lsof-4.51-2
ltrace-0.3.10-7
lv-4.49.4-3
lynx-2.8.4-17
m2crypto-0.05_snap4-2
m4-1.4.1-5
macutils-2.0b3-17
Maelstrom-3.0.1-17
magicdev-0.3.6-2
MagicPoint-1.08a-4
mailcap-2.1.6-1
mailx-8.1.1-22
make-3.79.1-8
MAKEDEV-3.2-5
man-1.5i2-6
man-pages-1.39-2
mars-nwe-0.99pl20-6
mawk-1.3.3-7
mc-4.5.51-36
mcserv-4.5.51-36
memprof-0.4.1-5
Mesa-3.4.2-10
Mesa-demos-3.4.2-10
Mesa-devel-3.4.2-10
metamail-2.7-28
mgetty-1.1.26-6
mgetty-sendfax-1.1.26-6
mgetty-viewfax-1.1.26-6
mgetty-voice-1.1.26-6
micq-0.4.6.p1-2
mikmod-3.1.6-12
mingetty-0.9.4-18
minicom-1.83.1-16
mkbootdisk-1.4.2-3
mkinitrd-3.2.6-1
mkisofs-1.10-4
mkkickstart-2.4-1
mktemp-1.5-11
mkxauth-1.7-16
mm-1.1.3-1
mm-devel-1.1.3-1
modutils-2.4.13-0.7.1
mount-2.11g-5
mouseconfig-4.23-1
mozilla-0.9.9-12.7.2
mozilla-chat-0.9.9-12.7.2
mozilla-devel-0.9.9-12.7.2
mozilla-mail-0.9.9-12.7.2
mozilla-psm-0.9.9-12.7.2
mpage-2.5.1-7
mpg321-0.2.9-2.5
mrtg-2.9.6-6
mtools-3.9.8-2
mtr-0.44-1
mtr-gtk-0.44-1
mt-st-0.6-1
mtx-1.2.13-1
mutt-1.2.5.1-1
mx-2.0.1-1
MyODBC-2.50.37-2
mysql-3.23.41-1
mysqlclient9-3.23.22-6
mysql-devel-3.23.41-1
MySQL-python-0.9.0-2
mysql-server-3.23.41-1
nasm-0.98-8
nasm-doc-0.98-8
nasm-rdoff-0.98-8
nautilus-1.0.4-47
nautilus-devel-1.0.4-47
nautilus-mozilla-1.0.4-47
nc-1.10-11
ncftp-3.0.3-6
ncompress-4.2.4-24
ncpfs-2.2.0.18-6
ncurses4-5.0-5
ncurses-5.2-12
ncurses-devel-5.2-12
nedit-5.1.1-10

netconfig-0.8.11-7
netpbm-9.14-2
netpbm-devel-9.14-2
netpbm-progs-9.14-2
netscape-common-4.78-2
netscape-communicator-4.78-2
netscape-navigator-4.78-2
net-tools-1.60-3
newt-0.50.33-1
newt-devel-0.50.33-1
nfs-utils-0.3.1-13.7.2.1
njamd-0.8.1-2
nkf-1.92-6
nmap-2.54BETA22-3
nmap-frontend-2.54BETA22-3
nmh-1.0.4-9
nscd-2.2.4-24
nss_db-2.2-6
nss_db-compat-2.2-6
nss_ldap-189-2
ntp-4.1.0-4
ntsysv-1.2.24-1
nut-0.45.0-3
nut-client-0.45.0-3
nvi-m17n-nocanna-1.79-19991117.9
oaf-0.6.5-10
oaf-devel-0.6.5-10
octave-2.1.34-3
open-1.4-12
openjade-1.3-17
openldap12-1.2.12-4
openldap-2.0.21-1
openldap-clients-2.0.21-1
openldap-devel-2.0.21-1
openldap-servers-2.0.21-1
openssh-3.1p1-6
openssh-askpass-3.1p1-6
openssh-askpass-**gnome-3.1p1-6**
openssh-clients-3.1p1-6
openssh-server-3.1p1-6
openssl095a-0.9.5a-11
openssl096-0.9.6-6
openssl-0.9.6b-8
openssl-devel-0.9.6b-8
openssl-perl-0.9.6b-8
ORBit-0.5.8-4
ORBit-devel-0.5.8-4
p2c-1.22-10
pam-0.75-19
pam-devel-0.75-19
pam_krb5-1.46-1
pam_smb-1.1.6-2
pan-0.9.7-2
parted-1.4.16-8
parted-devel-1.4.16-8
passwd-0.64.1-7
patch-2.5.4-10
pax-1.5-4
pccts-1.33mr22-5
pciutils-2.1.8-23
pciutils-devel-2.1.8-23
pcre-3.4-2
pcre-devel-3.4-2
pdksh-5.2.14-13
perl-5.6.1-26.72.3
perl-DateManip-5.39-5
perl-DBD-MySQL-1.2216-4
perl-DBD-Pg-1.01-1
perl-DBI-1.18-1
perl-Digest-MD5-2.13-1
perl-HTML-Parser-3.25-2
perl-HTML-Tagset-3.03-3
perl-libnet-1.0703-6
perl-libwww-perl-5.53-3
perl-libxml-enno-1.02-5
perl-libxml-perl-0.07-5
perl-MIME-Base64-2.12-6
perl-Parse-Yapp-1.04-3
perl-SGMLSpm-1.03ii-4
perl-Storable-0.6.11-6
perl-URI-1.12-5
perl-XML-Dumper-0.4-5
perl-XML-Encoding-1.01-2
perl-XML-Grove-0.46alpha-3
perl-XML-Parser-2.30-7
perl-XML-Twig-2.02-2
pidentd-3.0.14-1
pilot-link-0.9.5-8
pilot-link-devel-0.9.5-8
pine-4.44-1.72.0
pinfo-0.6.1-2
pkgconfig-0.7.0-3
playmidi-2.4-16
playmidi-X11-2.4-16
plugger-3.3-4
pmake-1.45-4
pnm2ppa-1.04-2
popt-1.6.4-7x
portmap-4.0-38
postgresql-docs-7.1.3-2
postgresql-jdbc-7.1.3-2
postgresql-libs-7.1.3-2
postgresql-odbc-7.1.3-2
postgresql-perl-7.1.3-2
postgresql-python-7.1.3-2
postgresql-tcl-7.1.3-2
postgresql-tk-7.1.3-2
ppp-2.4.1-3
printconf-0.3.61-4.1
printconf-gui-0.3.61-4.1
procinfo-18-2
procmail-3.21-1
procps-2.0.7-11
procps-X11-2.0.7-11
psacct-6.3.2-9
psgml-1.2.1-13
psmisc-20.1-2
pspell-0.12.2-3
pspell-devel-0.12.2-3
psutils-1.17-13
pump-0.8.11-7

pump-devel-0.8.11-7
pvm-3.4.3-28
pvm-gui-3.4.3-28
pwdb-0.61.1-3
pxe-0.1-23
pychecker-0.7.5-1
pygnome-1.4.1-3
pygnome-applet-1.4.1-3
pygnome-capplet-1.4.1-3
pygnome-devel-1.4.1-3
pygnome-gtkhtml-1.4.1-3
pygnome-libglade-1.4.1-3
pygtk-0.6.8-3
pygtk-devel-0.6.8-3
pygtk-glarea-0.6.8-3
pygtk-libglade-0.6.8-3
PyQt-2.4-1
PyQt-devel-2.4-1
PyQt-examples-2.4-1
python-1.5.2-35
python2-2.1.1-2
python2-devel-2.1.1-2
python-devel-1.5.2-35
python-docs-1.5.2-35
python-tools-1.5.2-35
python-xmlrpc-1.5.1-7.x.3
PyXML-0.6.5-4
qt1x-1.45-16
qt1x-devel-1.45-16
qt1x-GL-1.45-16
qt-2.3.1-5
qt-designer-2.3.1-5
qt-devel-2.3.1-5
qt-static-2.3.1-5
qt-Xt-2.3.1-5
quanta-2.0-0.cvs20010724.2
quota-3.01pre9-3
radvd-0.6.2pl4-1
raidtools-0.90-24
rarpd-ss981107-9
rcs-5.7-15
rdate-1.0-8
rdist-6.1.5-16
readline2.2.1-2.2.1-4
readline41-4.1-10
readline-4.2-2
readline-devel-4.2-2
redhat-config-network-0.9.10-2
redhat-config-users-0.9.2-6
redhat-logos-1.1.3-1
redhat-release-7.2-1
reiserfs-utils-3.x.0j-2
rep-gtk-0.15-6
rep-gtk-gnome-0.15-6
rep-gtk-libglade-0.15-6
rhmask-1.0-10
rhn_register-2.7.9-7.x.2
rhn_register-gnome-2.7.9-7.x.2
rlpr-2.04-1
rmt-0.4b25-1.72.0
rootfiles-7.2-1
routed-0.17-8
rp3-1.1.10-3
rpm2html-1.7-3.7x
rpm-4.0.4-7x
rpm-build-4.0.4-7x
rpmdb-redhat-7.2-0.20010924
rpm-devel-4.0.4-7x
rpmfind-1.7-4.7x
rpmlint-0.32-4
rpm-perl-4.0.4-7x
rpm-python-4.0.4-7x
rp-pppoe-3.2-3
rsh-0.17-5
rsh-server-0.17-5
rsync-2.4.6-13
ruby-1.6.4-2
ruby-devel-1.6.4-2
ruby-docs-1.6.4-2
ruby-libs-1.6.4-2
ruby-tcltk-1.6.4-2
rusers-0.17-12
rusers-server-0.17-12
rwall-0.17-10
rwall-server-0.17-10
rwho-0.17-11
rxvt-2.7.6-4
samba-2.2.1a-4
samba-client-2.2.1a-4
samba-common-2.2.1a-4
samba-swat-2.2.1a-4
sane-backends-1.0.5-4.1
sane-backends-devel-1.0.5-4.1
sane-frontends-1.0.5-2
sash-3.4-11
sawfish-0.38-11
sawfish-themer-0.38-11
screen-3.9.9-3
scrollkeeper-0.2-6
SDL-1.2.2-3
SDL-devel-1.2.2-3
SDL_image-1.2.0-3
SDL_image-devel-1.2.0-3
SDL_mixer-1.2.0-4
SDL_mixer-devel-1.2.0-4
SDL_net-1.2.2-1
SDL_net-devel-1.2.2-1
sed-3.02-10
semi-xemacs-1.14.3-8
sendmail-8.11.6-3
sendmail-cf-8.11.6-3
sendmail-doc-8.11.6-3
serviceconf-0.6.6-1
setserial-2.17-4
setup-2.5.7-1
setuptool-1.8-2
sgml-common-0.5-7
sgml-tools-1.0.9-12
shadow-utils-20000902-4
shapecfg-2.2.12-7
sharutils-4.2.1-8.7.x
sh-utils-2.0.11-5
sip-2.4-3
sip-devel-2.4-3
slang-1.4.4-4
slang-devel-1.4.4-4
sliplogin-2.1.1-12
slocate-2.6-1
slrn-0.9.7.1-3

slrn-pull-0.9.7.1-3
smpeg-0.4.4-3
smpeg-devel-0.4.4-3
smpeg-xmms-0.3.4-3
snavigator-5.0-4
sndconfig-0.65.2-1
sox-12.17.1-4
sox-devel-12.17.1-4
specspo-7.2-1
squid-2.4.STABLE6-6.7.3
stat-2.5-2
statserial-1.1-23
strace-4.3-2
stunnel-3.22-1
swig-1.1p5-10
switchdesk-3.9.7-1
switchdesk-gnome-3.9.7-1
switchdesk-kde-3.9.7-1
sylpheed-0.5.0-3
symlinks-1.2-13
sysctlconfig-0.14-1
sysklogd-1.4.1-4
syslinux-1.52-2
sysreport-1.2-1
sysstat-4.0.1-2
SysVinit-2.78-19
talk-0.17-12
talk-server-0.17-12
tamago-4.0.6-5
taper-6.9b-4
tar-1.13.19-6
tcl-8.3.3-65
tcllib-1.0-65
tclx-8.3-65
tcpdump-3.6.2-11.7.2.0
tcp_wrappers-7.6-19
tcsh-6.10-6
telnet-0.17-20
telnet-server-0.17-20
termcap-11.0.1-10
tetex-1.0.7-38.2
tetex-afm-1.0.7-38.2
tetex-doc-1.0.7-38.2
tetex-dvilj-1.0.7-38.2
tetex-dvips-1.0.7-38.2
tetex-fonts-1.0.7-38.2
tetex-latex-1.0.7-38.2
tetex-xdvi-1.0.7-38.2
texinfo-4.0b-3
textutils-2.0.14-2
tftp-0.17-14
tftp-server-0.17-14
time-1.7-14
timeconfig-3.2.2-1
timidity++-2.10.4-2
tix-8.2.0b1-65
tk-8.3.3-65
tkinter-1.5.2-35
tmake-1.7-3
tmpwatch-2.8.1-1
traceroute-1.4a12-1
transfig-3.2.3d-2
tree-1.2-13
tripwire-2.3.1-5
ttcp-1.12-2
ttfm-0.9.1-8
ttfonts-1.0-4
ttfonts-ja-1.0-7
tux-2.2.0-1
tuxracer-0.61-5
ucd-snmp-4.2.5-7.72.0
ucd-snmp-devel-4.2.5-7.72.0
ucd-snmp-utils-4.2.5-7.72.0
umb-scheme-3.2-21
unarj-2.43-8
units-1.55-10
unix2dos-2.2-12
unixODBC-2.0.7-3
unixODBC-devel-2.0.7-3
unixODBC-kde-2.0.7-3
unzip-5.42-1
up2date-2.7.61-7.x.2
up2date-gnome-2.7.61-7.x.2
urw-fonts-2.0-12
usbview-1.0-2
usermode-1.46-1
utempter-0.5.2-6
util-linux-2.11f-17
VFlib2-2.25.1-20
VFlib2-devel-2.25.1-20
VFlib2-VFjfm-2.25.1-20
vim-common-6.0-7.13
vim-enhanced-6.0-7.13
vim-minimal-6.0-7.13
vim-X11-6.0-7.13
vixie-cron-3.0.1-63
vlock-1.3-8
vnc-3.3.3r2-18.4
vnc-doc-3.3.3r2-18.4
vnc-server-3.3.3r2-18.4
vorbis-1.0rc2-1
w3c-libwww-5.2.8-10
w3c-libwww-apps-5.2.8-10
w3c-libwww-devel-5.2.8-10
w3m-0.2.1-11
w3m-el-1.0-4
watanabe-vf-1.0-5
wget-1.7-3
which-2.12-3
whois-1.0.9-1
WindowMaker-0.65.1-3
WindowMaker-libs-0.65.1-3
wine-20010822-1
wine-devel-20010822-1
wireless-tools-21-3
wl-xemacs-2.4.1-6
wmakerconf-2.8.1-2
Wnn6-SDK-1.0-14
Wnn6-SDK-devel-1.0-14
words-2-17
wu-ftpd-2.6.1-20
wvdial-1.41-15
x3270-3.2.16-4
x3270-tcl-3.2.16-4
x3270-text-3.2.16-4
x3270-x11-3.2.16-4
xalf-0.11-4
Xaw3d-1.5-10
Xaw3d-devel-1.5-10
xawtv-3.54-5
xbill-2.0-15
xbl-1.0j-7
xboard-4.2.3-2
xcdroast-0.98a9-2
xchat-1.8.9-1.72.0
Xconfigurator-4.9.39-2
xcpustate-2.5-11
xdaliclock-2.18-8

xdelta-1.1.1-11
xdelta-devel-1.1.1-11
Xdialog-2.0.2-1
xemacs-21.1.14-23.7.2
xemacs-el-21.1.14-23.7.2
xemacs-info-21.1.14-23.7.2
xfig-3.2.3d-3
XFree86-100dpi-fonts-4.1.0-25
XFree86-4.1.0-25
XFree86-75dpi-fonts-4.1.0-25
XFree86-compat-libs-4.0.3-2
XFree86-compat-modules-3.3.6-42
XFree86-devel-4.1.0-25
XFree86-doc-4.1.0-25
XFree86-FBDev-3.3.6-42
XFree86-ISO8859-15-100dpi-fonts-4.1.0-25
XFree86-ISO8859-15-75dpi-fonts-4.1.0-25
XFree86-ISO8859-7-100dpi-fonts-1.0-10
XFree86-ISO8859-7-1.0-10
XFree86-ISO8859-7-75dpi-fonts-1.0-10
XFree86-ISO8859-7-Type1-fonts-1.0-10
XFree86-KOI8-R-100dpi-fonts-1.0-6
XFree86-libs-4.1.0-25
XFree86-tools-4.1.0-25
XFree86-twm-4.1.0-25
XFree86-xdm-4.1.0-25
XFree86-xf86cfg-4.1.0-25
XFree86-xfs-4.1.0-25
XFree86-Xnest-4.1.0-25
XFree86-Xvfb-4.1.0-25
xinetd-2.3.3-1
xinitrc-3.20-1
xisdnload-1.38-46
xloadimage-4.1-21
xlockmore-4.17.2-4
xmailbox-2.5-14
xml-i18n-tools-0.9-2
xmms-1.2.5-7
xmms-devel-1.2.5-7
xmms-gnome-1.2.5-7
xmms-skins-1.2.5-7
xmorph-2001.02.22-2
xosview-1.7.3-5
xpdf-0.92-5
xpilot-4.3.2-2
xrn-9.02-10
xsane-0.82-3.1
xsane-gimp-0.82-3.1
xscreensaver-3.33-4
xsnow-1.40-14
xsri-2.0.3-1
xsysinfo-1.7-4
xtoolwait-1.3-1
xtraceroute-0.9.0-3
ypbind-1.8-1
ypserv-1.3.12-2
yp-tools-2.5-1
ytalk-3.1.1-7
zebra-0.91a-6
zip-2.3-10
zlib-1.1.3-25.7
zlib-devel-1.1.3-25.7
zsh-4.0.2-2

Appendix C: Port Scan Output

The following is the output of the Nmap scan, followed by samples of the outputs from the lsof and rpcinfo commands performed on each host.

NMAP

```
# nmap (V. 2.54BETA31) scan initiated Wed Oct  2 16:09:18 2002 as: nmap
-sT -sR -O -I -v -oA /tmp/nmap-scan -iL /tmp/hosts.scan -p 1-65535 -T
Aggressive
Interesting ports on fnode166.giac.org (192.168.17.8):
(The 65525 ports scanned but not shown below are in state: closed)
Port       State       Service (RPC)           Owner
22/tcp     open        ssh
111/tcp    open        sunrpc
912/tcp    open        unknown
3878/tcp   open        unknown
3882/tcp   open        unknown
32768/tcp  open        unknown
32769/tcp  open        unknown
32770/tcp  open        sometimes-rpc3
32771/tcp  open        sometimes-rpc5
32772/tcp  open        sometimes-rpc7

Remote operating system guess: Linux Kernel 2.4.0 - 2.4.17 (X86)
Uptime 0.090 days (since Wed Oct  2 13:59:48 2002)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=3646782 (Good luck!)
IPID Sequence Generation: All zeros
Interesting ports on fnode55.giac.org (192.168.16.124):
(The 65525 ports scanned but not shown below are in state: closed)
Port       State       Service (RPC)           Owner
22/tcp     open        ssh
111/tcp    open        sunrpc
922/tcp    open        unknown
3878/tcp   open        unknown
3882/tcp   open        unknown
32768/tcp  open        unknown
32769/tcp  open        unknown
32770/tcp  open        sometimes-rpc3
32771/tcp  open        sometimes-rpc5
32772/tcp  open        sometimes-rpc7

Remote operating system guess: Linux Kernel 2.4.0 - 2.4.17 (X86)
Uptime 0.085 days (since Wed Oct  2 14:07:32 2002)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=1619281 (Good luck!)
IPID Sequence Generation: All zeros
Interesting ports on fnode70.giac.org (192.168.16.139):
(The 65525 ports scanned but not shown below are in state: closed)
Port       State       Service (RPC)           Owner
22/tcp     open        ssh
111/tcp    open        sunrpc
923/tcp    open        unknown
3878/tcp   open        unknown
3882/tcp   open        unknown
```

```
32768/tcp  open        unknown
32769/tcp  open        unknown
32770/tcp  open        sometimes-rpc3
32771/tcp  open        sometimes-rpc5
32772/tcp  open        sometimes-rpc7

Remote operating system guess: Linux Kernel 2.4.0 - 2.4.17 (X86)
Uptime 0.083 days (since Wed Oct  2 14:10:12 2002)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=2248302 (Good luck!)
IPID Sequence Generation: All zeros
Interesting ports on fnode74.giac.org (192.168.16.143):
(The 65526 ports scanned but not shown below are in state: closed)
Port       State       Service (RPC)           Owner
22/tcp     open        ssh
111/tcp    open        sunrpc
925/tcp    open        unknown
3878/tcp   open        unknown
3882/tcp   open        unknown
32768/tcp  open        unknown
32769/tcp  open        unknown
32770/tcp  open        sometimes-rpc3
32771/tcp  open        sometimes-rpc5

Remote operating system guess: Linux Kernel 2.4.0 - 2.4.17 (X86)
Uptime 0.074 days (since Wed Oct  2 14:22:46 2002)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=3010951 (Good luck!)
IPID Sequence Generation: All zeros
Interesting ports on fnode66.giac.org (192.168.16.135):
(The 65528 ports scanned but not shown below are in state: closed)
Port       State       Service (RPC)           Owner
22/tcp     open        ssh
111/tcp    open        sunrpc
922/tcp    open        unknown
3878/tcp   open        unknown
32768/tcp  open        unknown
32769/tcp  open        unknown
32770/tcp  open        sometimes-rpc3

Remote operating system guess: Linux Kernel 2.4.0 - 2.4.17 (X86)
Uptime 0.076 days (since Wed Oct  2 14:20:50 2002)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=4436290 (Good luck!)
IPID Sequence Generation: All zeros

# Nmap run completed at Wed Oct  2 16:09:41 2002 -- 5 IP addresses (5
hosts up) scanned in 22 seconds
```

LSOF

```
COMMAND     PID USER   FD   TYPE DEVICE SIZE NODE NAME
portmap     570 root    3u  IPv4    819       UDP *:sunrpc
portmap     570 root    4u  IPv4    823       TCP *:sunrpc (LISTEN)
rpc.statd   598 root    4u  IPv4    847       UDP *:774
rpc.statd   598 root    5u  IPv4    878       UDP *:32768
```

```
rpc.statd   598 root    6u  IPv4    881       TCP *:32768 (LISTEN)
ntpd        708 root    4u  IPv4    982       UDP *:ntp
ntpd        708 root    5u  IPv4    983       UDP fnode166.giac.org:ntp
ntpd        708 root    6u  IPv4    984       UDP fnode166:ntp
ypbind      731 root    6u  IPv4    996       UDP *:909
ypbind      731 root    7u  IPv4   1001       TCP *:912 (LISTEN)
ypbind      731 root    9u  IPv4 129529       UDP *:924
ypbind      734 root    6u  IPv4    996       UDP *:909
ypbind      734 root    7u  IPv4   1001       TCP *:912 (LISTEN)
ypbind      734 root    9u  IPv4 129529       UDP *:924
ypbind      735 root    6u  IPv4    996       UDP *:909
ypbind      735 root    7u  IPv4   1001       TCP *:912 (LISTEN)
ypbind      735 root    9u  IPv4 129529       UDP *:924
ypbind      736 root    6u  IPv4    996       UDP *:909
ypbind      736 root    7u  IPv4   1001       TCP *:912 (LISTEN)
ypbind      736 root    9u  IPv4 129529       UDP *:924
sshd        912 root    3u  IPv4   1185       TCP *:ssh (LISTEN)
lim        1149 root    3u  IPv4   2643       UDP *:lim
lim        1149 root    4u  IPv4   2644       TCP *:32771 (LISTEN)
res        1151 root    3u  IPv4   2426       TCP *:res (LISTEN)
res        1151 root    4u  IPv4   2433       TCP *:32770 (LISTEN)
res        1151 root    5u  IPv4  37104       UDP *:1018
res        1151 root    6u  IPv4   2806       UDP *:1021
res        1151 root    7u  IPv4   2807       UDP *:1020
sbatchd    1153 root    3u  IPv4   2592       UDP *:1022
sbatchd    1153 root    4u  IPv4   2974       UDP *:1019
sbatchd    1153 root    5u  IPv4   2982       TCP *:sbatchd (LISTEN)
sbatchd    1153 root    6u  IPv4   2983       UDP *:1017
pim        1172 root    3u  IPv4   2719       TCP *:32772 (LISTEN)
sshd      12089 root    6u  IPv4 145463       TCP
fnode166.giac.org:x11-ssh-offset (LISTEN)
```

RPCINFO

```
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  32768  status
    100024    1   tcp  32768  status
    100007    2   udp    909  ypbind
    100007    1   udp    909  ypbind
    100007    2   tcp    912  ypbind
    100007    1   tcp    912  ypbind
    100021    1   udp  32770  nlockmgr
    100021    3   udp  32770  nlockmgr
    100021    4   udp  32770  nlockmgr
    100021    1   tcp  32769  nlockmgr
    100021    3   tcp  32769  nlockmgr
    100021    4   tcp  32769  nlockmgr
```

Appendix D: CIS Benchmark Scan Output

```
*** CIS Ruler Run ***
Starting at time 20021003-08:37:25

Negative: 1.1 System appears not to have been patched within the last
month.
Negative: 2.2 No Authorized Only banner for telnet in file
/etc/xinetd.d/krb5-telnet.
Negative: 2.2 No Authorized Only banner for ftp in file
/etc/xinetd.d/gssftp.
Negative: 2.2 No Authorized Only banner for login in file
/etc/xinetd.d/rlogin.
Positive: 2.3 telnet is deactivated.
Positive: 2.4 ftp is deactivated.
Positive: 2.5 rsh, rcp and rlogin are deactivated.
Positive: 2.6 tftp is deactivated.
Negative: 2.7 xinetd either requires global 'only-from' statement or
one for each service.
Positive: 3.1 Miscellaneous scripts are all turned off.
Positive: 3.2 NFS Server script nfs is deactivated.
Negative: 3.3 NFS script nfslock not deactivated.
Negative: 3.3 NFS script autofs not deactivated.
Negative: 3.4 NIS Client processes (ypbind rc script) not deactivated.
Positive: 3.5 NIS Server processes are deactivated.
Negative: 3.6 portmapper not deactivated.
Positive: 3.7 samba windows filesharing daemons are deactivated.
Negative: 3.8 netfs rc script not deactivated.
Negative: 3.9 lpd (line printer daemon) not deactivated.
Positive: 3.10 Graphical login is deactivated.
Positive: 3.11 Mail daemon is not listening on TCP 25.
Positive: 3.12 Web server is deactivated.
Positive: 3.13 snmp daemon is deactivated.
Positive: 3.14 DNS server is deactivated.
Positive: 3.15 postgresql (SQL) database server is deactivated.
Positive: 3.16 routing daemons are deactivated.
Positive: 3.17 Webmin GUI-based system administration daemon
deactivated.
Positive: 3.18 Squid web cache daemon deactivated.
Positive: 3.19 inetd/xinetd not activated.
Positive: 3.20 Found a good daemon umask.
Negative: 4.1 Coredumps aren't deactivated.
Positive: 4.2 NFS server restricts clients to privileged ports.
Negative: 4.3 /proc/sys/net/ipv4/tcp_max_syn_backlog should be at least
4096 to handle SYN floods.
Positive: 4.4 All 'additional' network parameters set correctly.
Positive: 5.1 syslog captures auth and authpriv messages.
Negative: 6.1 Removable filesystem /mnt/floppy is not mounted nosuid.
Negative: 6.2 PAM allows users to mount CD-ROMS.
(/etc/security/console.perms)
Negative: 6.2 PAM allows users to mount floppies.
(/etc/security/console.perms)
Positive: 6.3 password and group files have right permissions and
owners.
Positive: 6.4 all temporary directories have sticky bits set.
```

```
Negative: 7.1 rhosts authentication not deactivated in
/etc/pam.d/rlogin.
Negative: 7.1 rhosts authentication not deactivated in /etc/pam.d/rsh.
Positive: 7.2 /etc/hosts.equiv file not present or has size zero.
Negative: 7.3 User nscd is not present in /etc/ftpusers
Negative: 7.3 User ident is not present in /etc/ftpusers
Negative: 7.3 User gdm is not present in /etc/ftpusers
Negative: 7.3 User gopher is not present in /etc/ftpusers
Negative: 7.3 User rpc is not present in /etc/ftpusers
Negative: 7.3 User squid is not present in /etc/ftpusers
Negative: 7.3 User apache is not present in /etc/ftpusers
Negative: 7.3 User rpcuser is not present in /etc/ftpusers
Negative: 7.3 User named is not present in /etc/ftpusers
Negative: 7.3 User xfs is not present in /etc/ftpusers
Negative: 7.3 User mailnull is not present in /etc/ftpusers
Negative: 7.4 Couldn't open cron.allow
Negative: 7.4 Couldn't open at.allow
Negative: 7.5 The permissions on /etc/crontab are not sufficiently
restrictive.
Positive: 7.6 All authorized-use-only warning banners are in place.
Negative: 7.7 /etc/securetty has a non tty1-12 line: tty10.
Negative: 7.8 lilo isn't password-protected.
Negative: 8.1 news has a valid shell of /bin/sh.  Remember, an empty
shell field in /etc/passwd signifies /bin/sh.
Negative: 8.2 /etc/passwd contained +: in it!
Negative: 8.3 User root has no password in /etc/shadow!
Negative: 8.3 User bin has no password in /etc/shadow!
Negative: 8.3 User daemon has no password in /etc/shadow!
Negative: 8.3 User adm has no password in /etc/shadow!
Negative: 8.3 User lp has no password in /etc/shadow!
Negative: 8.3 User sync has no password in /etc/shadow!
Negative: 8.3 User shutdown has no password in /etc/shadow!
Negative: 8.3 User halt has no password in /etc/shadow!
Negative: 8.3 User mail has no password in /etc/shadow!
Negative: 8.3 User news has no password in /etc/shadow!
Negative: 8.3 User uucp has no password in /etc/shadow!
Negative: 8.3 User operator has no password in /etc/shadow!
Negative: 8.3 User games has no password in /etc/shadow!
Negative: 8.3 User gopher has no password in /etc/shadow!
Negative: 8.3 User ftp has no password in /etc/shadow!
Negative: 8.3 User nobody has no password in /etc/shadow!
Negative: 8.3 User mailnull has no password in /etc/shadow!
Negative: 8.3 User rpm has no password in /etc/shadow!
Negative: 8.3 User xfs has no password in /etc/shadow!
Negative: 8.3 User ntp has no password in /etc/shadow!
Negative: 8.3 User rpc has no password in /etc/shadow!
Negative: 8.3 User gdm has no password in /etc/shadow!
Negative: 8.3 User rpcuser has no password in /etc/shadow!
Negative: 8.3 User nfsnobody has no password in /etc/shadow!
Negative: 8.3 User nscd has no password in /etc/shadow!
Negative: 8.3 User ident has no password in /etc/shadow!
Negative: 8.3 User radvd has no password in /etc/shadow!
Negative: 8.3 User apache has no password in /etc/shadow!
Negative: 8.3 User squid has no password in /etc/shadow!
Negative: 8.3 User named has no password in /etc/shadow!
Negative: 8.3 User pcap has no password in /etc/shadow!
Negative: 8.3 User amanda has no password in /etc/shadow!
```

```
Negative: 8.3 User junkbust has no password in /etc/shadow!
Negative: 8.3 User mailman has no password in /etc/shadow!
Negative: 8.3 User mysql has no password in /etc/shadow!
Negative: 8.3 User ldap has no password in /etc/shadow!
Negative: 8.3 User pvm has no password in /etc/shadow!
Negative: 8.3 User +@ccc has no password in /etc/passwd!
Negative: 8.3 User +@ccc has no password in /etc/shadow!
Negative: 8.3 User + has no password in /etc/passwd!
Negative: 8.3 User + has no password in /etc/shadow!
Negative: 8.4 A non-root UID 0 account (named +@ccc) was found.
Negative: 8.4 A non-root UID 0 account (named +) was found.
Positive: 8.5 root's PATH is clean of group/world writable directories
or the current-directory link.
Positive: 8.6 root account has no dangerous rhosts, shosts, or netrc
files.
Positive: 8.7 No user's home directory is world or group writable.
Positive: 8.8 No group or world-writable dotfiles!
Positive: 8.9 No user has a .netrc or .rhosts file.
Negative: 8.10 Default umask may not block world-writable.  Check
/etc/profile.
Negative: 8.10 Default umask may not block group-writable.  Check
/etc/profile.
Negative: 8.10 Default umask may not block world-writable.  Check
/etc/csh.login.
Negative: 8.10 Default umask may not block group-writable.  Check
/etc/csh.login.
Negative: 8.10 Default umask may not block group-writable.  Check
/etc/csh.cshrc.
Positive: 9.1 System is running sshd.
Positive: 9.2 This machine is synced with ntp.
Preliminary rating given at time: Thu Oct  3 08:37:36 2002

      Preliminary rating = 5.89 / 10.00

Negative: 6.5 Non-standard SUID program /usr/bin/rnews
Negative: 6.5 Non-standard SUID program /usr/bin/sperl5.6.1
Negative: 6.5 Non-standard SUID program /usr/bin/nwsfind
Negative: 6.5 Non-standard SUID program /usr/bin/rlpq
Negative: 6.5 Non-standard SUID program /usr/bin/rlpr
Negative: 6.5 Non-standard SUID program /usr/bin/rlprd
Negative: 6.5 Non-standard SUID program /usr/bin/rlprm
Negative: 6.5 Non-standard SUID program /usr/lib/sendmail
Negative: 6.5 Non-standard SUID program /usr/lib/amanda/calcsize
Negative: 6.5 Non-standard SUID program /usr/lib/amanda/killpgrp
Negative: 6.5 Non-standard SUID program /usr/lib/amanda/rundump
Negative: 6.5 Non-standard SUID program /usr/lib/amanda/runtar
Negative: 6.5 Non-standard SUID program /usr/lib/amanda/dumper
Negative: 6.5 Non-standard SUID program /usr/lib/amanda/planner
Negative: 6.5 Non-standard SUID program /usr/sbin/mailq
Negative: 6.5 Non-standard SUID program /usr/sbin/amcheck
Negative: 6.5 Non-standard SGID program /usr/bin/slrnpull
Ending run at time: Thu Oct  3 08:37:52 2002

      Final rating = 5.89 / 10.00
```

Appendix E: Nessus Vulnerability Scan Output

```
Nessus Scan Report
------------------


SUMMARY

 - Number of hosts which were alive during the test : 5
 - Number of security holes found : 5
 - Number of security warnings found : 30
 - Number of security notes found : 10



TESTED HOSTS

 fnode166 (Security holes found)
 fnode70 (Security holes found)
 fnode74 (Security holes found)
 fnode66 (Security holes found)
 fnode55 (Security holes found)



DETAILS

+ fnode166 :
 . List of open ports :
   o general/icmp (Security warnings found)
   o ntp (123/udp) (Security warnings found)
   o general/tcp (Security warnings found)
   o unknown (32770/udp) (Security warnings found)
   o unknown (32768/udp) (Security hole found)
   o unknown (909/udp) (Security warnings found)
   o general/udp (Security notes found)

 . 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 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 found on port 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

. Information found on port 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


. 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


. Warning found on port unknown (32770/udp)
```

```
   The nlockmgr 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 : CVE-2000-0508

. Vulnerability found on port unknown (32768/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 found on port unknown (32768/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-1999-0493

. Warning found on port unknown (909/udp)


   The ypbind 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 : CVE-1999-0312

  . Information found on port general/udp


    For your information, here is the traceroute to 192.168.17.8 :
    192.168.40.1
    192.168.1.9
    192.168.1.50
    192.168.17.8

+ fnode70 :
  . List of open ports :
    o general/icmp (Security warnings found)
    o ntp (123/udp) (Security warnings found)
    o general/tcp (Security warnings found)
    o unknown (32770/udp) (Security warnings found)
    o unknown (32768/udp) (Security hole found)
    o unknown (920/udp) (Security warnings found)
    o general/udp (Security notes found)

  . 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 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 found on port 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

 . Information found on port 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


 . 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


 . Warning found on port unknown (32770/udp)



    The nlockmgr 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 : CVE-2000-0508

 . Vulnerability found on port unknown (32768/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 found on port unknown (32768/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-1999-0493

. Warning found on port unknown (920/udp)


   The ypbind 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 : CVE-1999-0312

. Information found on port general/udp


   For your information, here is the traceroute to 192.168.16.139 :
   192.168.40.1
   192.168.1.9
```

```
    192.168.1.50
    192.168.16.139

+ fnode74 :
 . List of open ports :
   o general/icmp (Security warnings found)
   o ntp (123/udp) (Security warnings found)
   o general/tcp (Security warnings found)
   o unknown (32770/udp) (Security warnings found)
   o unknown (32768/udp) (Security hole found)
   o unknown (922/udp) (Security warnings found)
   o general/udp (Security notes found)

 . 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 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 found on port 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

 . Information found on port 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


 . 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

 . Warning found on port unknown (32770/udp)



    The nlockmgr 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 : CVE-2000-0508

 . Vulnerability found on port unknown (32768/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 found on port unknown (32768/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-1999-0493

  . Warning found on port unknown (922/udp)


    The ypbind 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 : CVE-1999-0312

  . Information found on port general/udp


    For your information, here is the traceroute to 192.168.16.143 :
    192.168.40.1
    192.168.1.9
    192.168.1.50
    192.168.16.143

+ fnode66 :
  . List of open ports :
    o general/icmp (Security warnings found)
    o ntp (123/udp) (Security warnings found)
    o general/tcp (Security warnings found)
    o unknown (32770/udp) (Security warnings found)
    o unknown (32768/udp) (Security hole found)
    o unknown (919/udp) (Security warnings found)
    o general/udp (Security notes found)

  . 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 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 found on port 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

. Information found on port 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


. 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


. Warning found on port unknown (32770/udp)



   The nlockmgr 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 : CVE-2000-0508

. Vulnerability found on port unknown (32768/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 found on port unknown (32768/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-1999-0493

  . Warning found on port unknown (919/udp)



    The ypbind 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 : CVE-1999-0312

  . Information found on port general/udp


    For your information, here is the traceroute to 192.168.16.135 :
    192.168.40.1
    192.168.1.9
    192.168.1.50
    192.168.16.135

+ fnode55 :
  . List of open ports :
    o general/icmp (Security warnings found)
    o ntp (123/udp) (Security warnings found)
    o general/tcp (Security warnings found)
    o unknown (32770/udp) (Security warnings found)
    o unknown (32768/udp) (Security hole found)
    o unknown (919/udp) (Security warnings found)
    o general/udp (Security notes found)

  . 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 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 found on port 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

. Information found on port 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


. 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
```

```
. Warning found on port unknown (32770/udp)


   The nlockmgr 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 : CVE-2000-0508

. Vulnerability found on port unknown (32768/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 found on port unknown (32768/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-1999-0493

. Warning found on port unknown (919/udp)
```

```
    The ypbind 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 : CVE-1999-0312

 . Information found on port general/udp


    For your information, here is the traceroute to 192.168.16.124 :
    192.168.40.1
    192.168.1.9
    192.168.1.50
    192.168.16.124



------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

Last Updated: July 24th, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**