Global Information Assurance Certification Paper

Building a Secured OS for a Root Certificate Authority

Don Murdoch, CISSP
GCIA, GCIH,
MCSD, MCSE

Graduate Program in
Information Security
Mary Washington College

SANS GCUX
Version 1.9
Option 1

Table of Contents

Table of Figures

Executive Summary

This paper discusses the procedures necessary for securing an installation of Red Hat Enterprise Server 2.1 in support of a root certificate authority that will eventually function in the Higher Education Bridge Certificate Authority. As a basis of evaluation, the Federal Bridge Certificate Authority requirements will be used to provide guidance for assembling the certificate authority, as published by the Higher Education Public Key Infrastructure Policy Activities Group[1].

The computer system described in this paper will be the Root Certificate Authority (CA) - the highest server in the organizations' Public Key Infrastructure (PKI) architecture. Practically, a Root CA is used rarely; it is hardened to the point that it will support only authorized access with strong physical, technical, and administrative controls. The Root CA must support PKI operations such as cross certification with other Root CA's and signing certificates for issuing CA's.

This document is intended to be an artifact document for the certificate authority that will be assembled for an actual University and is part of the Security Policy[2] for the Certificate Authority as part of the evaluation process for participating in the HEBCA.

Important Terms

There are a few important terms, acronyms, and phrases that are used extensively in this paper. They are briefly explained here:

- PKI: Public Key Infrastructure
- CA: Certificate Authority. This is a server that can issue an X.509 V3 digital certificate which will match a person's digital identify to a proper name. The proper name corresponds to a person at a particular organization, such as "DonMurdoch@University.EDU".
- Root CA: The Root Certificate Authority. A Root CA is the "highest" server in a PKI - all other CA's are subordinate to a Root CA. This document discussed configuring a Root CA.
- CPS: Certificate Practice Statement. This document (usually more than 100 pages) that describes how certificates are issued and managed by an organization. This document describes certificate management and usage - it is operating system and certificate authority product agnostic.
- FBCA: Federal Bridge Certificate Authority. This is an existing US Government program which is designed to provide a framework for government agencies to

[1] HEBCA PAG Meeting Minutes, Dec 7, 2000. URL: http://www.educause.edu/hepki/pag_minutes/2000-12-07.asp
[2] As required by the current HEBCA draft document, from: http://middleware.internet2.edu/certpolicies/.

build and deploy PKI's that allow one agency to assert and prove the digital identity of its staff.

- HEBCA: Higher Education Bridge Certificate Authority. The HEBCA is an application of the FBCA designed to support the needs of Higher Education. Practically, the FBCA and HEBCA are almost the same. The current draft document is posted at: http://middleware.internet2.edu/certpolicies/.
- HEPKI : Higher Education Public Key Infrastructure, which is sponsored by Educause, and Internet[2].
- RHES: Red Hat Enterprise Server, Ver. 2.1. Throughout this document "RHES" refers to the operating system being hardened for participating in the HEBCA.

Higher Education and HEPKI Overview[3]

Higher educational institutions are interested in implementing a Public Key Infrastructure (PKI) that can provide for trust amongst participating institutions of higher learning (.edu's). There are a number of Internet[2] initiatives that require distributed trust, meaning that one institution must be able to provide a method where its members can interact with other institutions.

As a practical example, one such initiative is to build a network of high performance computing (HPC) systems known as "The Grid". Many institutions have HPC systems like Sun Enterprise 10000 systems - 32 processors, 1 Terabyte of storage, and 4 GB of main memory. Other examples include Linux based multiprocessor clusters. The Grid is implemented using GLOBUS technologies. GLOBUS relies on certificate based authentication, whereby a user is identified by their X.509 V3 certificate. Specifically, a person may be "dmurdoch@cs.university.edu", and this user may be granted permissions to submit jobs on a Grid system. GLUBUS authenticates a user based on the digital identity in the certificate, and checks with the issuing CA to make sure that the certificate is current. Systems administrators must be able securely exchange email with one another in managing the Grid. With these requirements in mind, PKI is an ideal solution to digitally sign and exchange email and to provide a framework for identifying a user via a digital certificate.

There are three groups that are at the forefront of the Higher Education Public Key Infrastructure (HEPKI) -Educause and Internet[2]. There are two primary working groups. First, there is the Policy Activities Group (HEPKI-PAG). This group is concerned with procedure, policy, and the issues surrounding implementation of PKI. Second, there is the Technical Activities Group (HEPKI-TAG) which is focused on the technology issues in implementing PKI.

[3] The majority of this information is derived from various reports, presentations, meeting minutes, and documents posted on the Internet2 middleware website: http://middleware.internet2.edu/. GLOBUS is documented at the website: http://www.globus.org/.

For participating in the HEPKI, an institution must follow the guidance as established by the Internet[2] Middleware Initiative group[4]:

> "PKI Activities. I2-MI is working with the federal government in both PKI and PKI-for-NGI developments. We are also working with our partners (Educause, CREN[5], and CNI) to establish a coherent vision for a PKI for higher education. In order to catalyze research and establish testbeds for interoperability, I2-MI is also beginning to define higher-education-specific research issues within PKI."

There are many concerns in participating in a PKI. The one that continually percolates to the top of the list is being assured that the person presenting the certificate really is the person, and that they were issued that certificate from a PKI that is trusted. There are a wide variety of issues involved in this statement. For the purposes of this document, focus is on building a secured operating system that can support the strict audit requirements of a root Certificate Authority in the HEBCA.

Description of the System

The system is the root certificate authority for a major University network. It will be infrequently used, as it will primarily be used to secure issuing certificate authorities and issuing certificates to the staff who will be managing the system. Regardless of how much it will be used there are a detailed set of auditing requirements that must be met for the life of the server.

A Root CA actually consists of four distinct components:

- Server Platform
- Hardware Security Module which will protect the private keys of the CA[6].
- Secured Operating System
- Certificate Authority Software

The components are more fully described in the table below:

System Component	Notes
Operating System Software	RedHat Enterprise Server, 2.1 (required by Netscape)
Certificate Authority Software	Netscape CMS 6.2 configured at a Root CA

[4] This quote is from the Internet2 Middleware Areas of Activity page. http://middleware.internet2.edu/overview/areas-of-activity.html

[5] CREN was the Corporation for Research and Educational Networking, which was dissolved on Jan 7, 2003. It existed and functioned for more than 20 years.

[6] Unfortunately, the nCipher hardware will not be available by the time this assignment is due to SANS/MWC

System Component	Notes
Server Platform	Dell 2650 with external SCSI interfaces for connection to an external DLT tape drive as needed.
Server Processor	Single Pentium 2.4 GHz -
Server Disk	Mirrored 36 GB UW SCSI - hardware based mirroring provided by onboard RAID controller.
Server Removable Media	CD-RW/DVD drive
Server Network	Onboard Dual Ethernet (not used)
Hardware Security Module	The nCipher NForce HSM is the preferred device. This device supports both Solaris and RHES, and provides a secured environment to protect the private keys of the Root CA by using smart cards to lock and unlock the keys.

Additional Notes

It is not necessary to have super processor, or a dual processor based on system function. The server will be single purpose, with the most difficult processing being the occasional signing of a Certificate Services Request (CSR).

Backup and recovery will be done with a local tape drive as needed - which won't be that often. As needed, some logs will be archived onto CD using the CD-RW drive. This has a distinct advantage - CD has a much longer shelf life than tape. Note that media (tapes, CD, DVD) produced as part of normal system backup must be strictly controlled and custody must be maintained at all times.

With respect to the disk drives, the system was ordered with the option to "Keep your disk". This option allows the University to keep the hard drive and still receive warranty support should the drive fail. This purchasing option is critical - the University needs to show, for audit purposes, that no private key data (particularly the private keys for the CA) ever left the site in a way that can violate the Certificate Practices Statement (CPS).

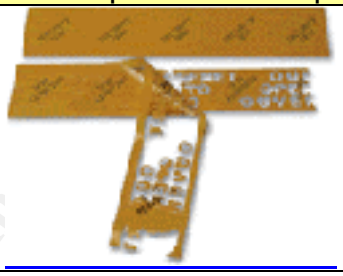
When the system is finally installed into production, it must meet operational characteristics that stipulate a high degree of auditing in order to participate in the HEBCA.

Physical Seals

One of the physical security issues involved in managing a Root CA is providing a physical evidence trail that shows the system's integrity hasn't been violated. In practice, this is accomplished in one of two ways. First, the server can be put into a safe - an impractical solution. Second, tamper evident tape can be used to provide a

seal on the system. The University prefers this approach, as it will be using a locked cabinet for the server. Tape is applied to the system covering the disk drives, securing the power cord, the chassis, and network cables. If the seal is broken, the tape will provide a trail that can be viewed externally without powering the system on.

Examples of tamper evident sealing tape are shown in the accompanying table.

Nova Vision[7]	TapeLine's Tamper Evident Tape[8]
	

Risk Analysis

Steps in Risk Analysis

There are a variety of ways to perform risk analysis. Here, the five step quantitative processes as expressed by Shon Harris are used[9]. These steps are:

1. Assign a value to the assets (usually dollars).
2. Estimate potential loss per risk.
3. Perform a threat analysis.
4. Derive an overall loss potential per threat.
5. Reduce, assign, or accept the risk.

Normally, the end goal of a risk analysis is to determine the Annualized Loss Expectancy (ALE), which measures or estimates the frequency (an actual percentage) of a given threat in a single year. The ALE equation is:

(AV x EF) x ARO = ALE

[7] This tape is described at the Nova Vision website: http://www.novavisioninc.com/pages/prod_tampevidtape.html

[8] This tape is described at the TapeLine website: http://www.tapeline.com/stockprints/tamper-evident/tamper-evident.html

[9] Shon Harris has written one of the most highly respected Common Body of Knowledge (CBK) review guides for the ISC2's CISSP credential. In Chapter 3, "Security Management Practices", she explains the five step risk analysis process that is used here.

Where:

- AV = Asset Value (how much the asset is worth)
- EF = Exposure Factor (a percentage of loss
- ARO = Annualized Rate of Occurrence (how often a threat is realized during a one year period)

Step One: Value of the Root CA

The asset value of the Root CA is derived from several factors. These factors include cost of hardware, labor, installed software, recovery, and costs associated with deploying every subordinate issuing certificate authority and cross signed certificate authority that participates in the HEBCA over the life of the CA. Why so many costs? Since the Root CA is the starting point for the validity of the certificates issued by the organization, its asset value will increase over its lifespan.

Initial Costs (Tangible)

Hardware (server, HSM, keycards, rack components)	$16,000
Software (OS, CA)	$3,500
Labor (160 hrs for setup at $60/hr)	$9,600
Procedural Development Labor (480 at $60/hr)	$28,800
Total of measurable asset costs at initial deployment of the Root CA:	$57,900

From the above numbers the tangible value of the Root CA, as an asset is about $58,000 at the time of installation. Remember that this is only a single real cost - the intangible costs of the integrity of the overall system over a 20 year lifecycle would be much more difficult to calculate and much larger. The table below shows some measurement of value, based solely on tangible deployment and maintenance costs, of the cost of the total system at its life cycle midpoint (10 years of deployment):

Midpoint Lifecycle costs (10 year point for the Root CA)

Hardware (Root and Issuing CA server, HSM, keycards, rack components) - this number is based on estimated similar hardware costs of lifecycle replacement and recurring costs incurred for the HSM, and integration with backup/recovery.	$96,200
Software (OS, CA, 2500 certificates issued at any one time)	$18,500
Ongoing Labor (monthly audit)	$115.200
Certificate issuance, assuming that 25% certificate holders have hardware tokens there is 10% turnover in certificate holders, and "issuance" costs 25.00/certificate (labor)	$562,200

Total of measurable asset costs at initial deployment of the Root CA:	$792,100

Once again - these are the tangible costs that can be estimated. There are likely to be real hidden costs (turnover, changing enterprise backup/recovery, integration with site DRP/BCP[10], etc) that are not recorded here. But it can be seen that there are real costs which would be forfeited if the Root CA were seriously compromised - a lifecycle investment of about $792,000 would be lost at the point of compromise, as the certificates would no longer be "trusted".

So what's the measurable value of the Root CA? Quantitatively, the value of the CA is about $58,000 at initial deployment and about $792,000 at its 10 year midpoint.

Step Two: Potential Loss

The potential loss of the Root CA is determined by the physical loss, lost productivity, information value, and recovery costs.

As above - the actual cost of assets times the exposure factor. Based on the CPS and the operational procedures that are in place at the site and the most likely threat (water damage from hurricane), the Single Loss Expectancy of the Root CA in the data center is $29,100. Here, the tangible costs are replacement equipment, operating system, software, and rebuild. Since backups and recovery keys will be preserved offsite, the CA can be reassembled. It is assumed that water penetration would damage all three components beyond economical repair. Therefore, the Single Loss Expectancy is $29,100. Note that the Procedural Development item listed above is required to put the CA into operation, but is strictly a labor item.

29,100 x 100% = 29,100

At the system's 10 year midpoint in its lifecycle, the potential loss is $394,050.

Step Three: Threat Analysis

What are the threats to the Root CA? Essentially, the primary threat is a violation of the integrity, confidentiality, and availability of the digital certificates provided by the Root CA. Primarily this is its ability to authorize subordinate certificate authorities in a manner that assures an authorized CA received signed certificate request following the Certificate Practices Statement (CPS) for the organization.

[10] Disaster Recovery Planning / Business Continuity Processing.

For the scope of the Root CA as a component of an overall certificate services architecture, the Root CA needs to be protected from:

- Physical Compromise - theft, destruction, life cycle loss, improper use.
- Invalid CSR - Improper PKI operation, such as signing a Certificate Service.
- Request (CSR) for an Issuing Certificate Authority which is not authorized according to the CPS.
- Issuing a Certificate - Actually issuing a certificate to an unauthorized person.
- Theft - Of the Root CA's private keys.
- Network Access - a Root CA, by definition, is offline (not connected to a network).
- Unauthorized login - only a small select group of persons can access the Root CA.
- Unaudited operations - Both the FBCA and the HEBCA require that all operations be audited that relate to system security and system availability.
- Disaster recovery - Should the hardware or the data center "fail" to the point that the operating system cannot be booted or used, the certificate hierarchy will have limited life and cannot be expanded.
- Damage of audit logs - there are stringent requirements for audit logging on the platform and on the certificate authority product.
- Possession of the private key - In order to have assurance that the CA is operating properly, and that has been protected over its life cycle, the CA must prove possession of its private key (accomplished by using an HSM).

Step Four: Overall Loss Potential

Natural Disaster: Here, the most likely natural disaster threat is a hurricane. The likelihood that this physical threat being directed against the facility would be realized if a Class III hurricane visiting the location caused a building breach. For the region, this occurs every 12 (or so) years. Therefore, the Annualized Rate of Occurrence (ARO) of the most likely natural disaster is is 8.33% and the Annualized Loss Expectancy is 2,424.

$$29{,}100 \times 8.33\% = \$2{,}424.03$$

Human Induced Compromise: The second category of loss potential is much more serious - an operator or system administrator in a trusted position either a) stealing the keys or b) issuing a certificate to an unauthorized subordinate CA. This would be catastrophic - and depending on the skill level or collusion potential, might take up to a month to detect (FBCA audit requirements stipulate monthly audits). Due to the controls on the system, the likelihood of a trusted person violating the integrity of the system is remote - but there is potential, which will be set at 2% in order to have a

number to work with. Therefore, the Annualized Rate of Occurrence (ARO) is 2% and the Annualized Loss Expectancy is $582 at the time of installation.

29,100 x 2% = $582.00

Step Five: Risk Mitigation

In order to reduce the risk exposure - to mitigate the risks - there are three actions that can be taken. They are risk reduction, risk acceptance, and risk transference.

Risk Reduction: Here, the HEBCA audit requirements (discussed next) go a long way to reducing risk because they stipulate that the system must be audited frequently. Also, strong physical controls (data center operations, seals, locked rack, policy) greatly reduce the risk of system compromise. Because the system will use an HSM to manage the private keys for the Certificate Authority software (Netscape CMS), the private keys of the Root CA will be protected by a FIPS 140 Level 2[11] high security device. Such devices are standard in the Identrus financial trust network, so the most respected international banking institutions (who are inherently risk adverse) have put their stamp of "de facto" approval on using them to protect private keys. The University is also investing in a state of the art data center to protect is computing assets.

Data Center: The Root CA is located in a secured data center. This data center has these characteristics:

- Located on an upper floor of a limited access brick ergonomic (green) building.
- Monitoring is enabled for the environment (temperature, humidity).
- Air is scrubbed by modern HVAC systems.
- Building has motion activated cameras with notification to local law enforcement if an exterior door is found open after hours.
- Building has proximity card protection, with only four people having supervisory rights to the access control server. Complete audit trails are maintained.
- Elevator requires card access after hours.
- The center is manned 7x24x365.
- Fire detection is installed using optical and ionization sensors.
- UPS and generator can provide power for at least 48 hours based on local fuel supply and full up system load. Onsite fuel storage is expected to provide power for 12 days with current reserves. The UPS is tested weekly, and frequently used in the hot summer months.
- The root server is located in a locked cabinet. Only four people have keys to the cabinet (two in operations, two in security). The computer system itself is locked with front / rear access, and keys to the server are only held by the security staff.

[11] FIPS: Federal Information Processing Standard. Level 2 is a very high level of protection for private key storage.

- Following HEBCA audit guidelines, the Root CA is booted and audited on a monthly basis. All access to the server is logged in a tamper evident log book.
- The system has tamper evident seals installed.

Risk Acceptance: The organization has accepted the risk of operating a PKI - and in order to reduce the risks there are strong policies and procedures in place to manage the system (described later).

Risk Transference: The site is insured against many forms of loss, including theft, vandalism, and electrical damage.

Business Risks and HEBCA Audit Requirements

There is significant business risk in building the operating systems that the Root CA (and thus the PKI) depends on - being able to show an audit trail of the actions taken on the operating system from its inception. Here, if a site assembles a CA and doesn't take the necessary steps to ensure that the system and the certificate authority software can be audited properly, they will have wasted countless hours and prevented their CA from participating in the bridge. Therefore, from a business risk analysis point of view, the proper procedures must be followed from the beginning and throughout the life of the CA.

The audit requirements for a HEBCA Entity CA are documented in the "X.509 Certificate Policy for the Higher Education Bridge Certificate Authority", dated 10/27/02 and available from the middleware.Internet2.edu website[12]. Requirements are listed below are cited from section "4.5 Security Audit Procedure", with criteria for this Root CA based on the "BASIC" certificate assurance level, pp. 28 - 33 as they pertain to the operating system. Below are some highlights from this section. The entirety of Section 4.5 is presented in Appendix B.

- PKI operations must be fully logged - who performed what tasks, what CSR was used, etc.
- Operating system backup/recovery must be logged.
- Supervisory actions taken by staff must be logged.
- Only authenticated logon is allowed (logons associated to an individual).

Security Controls

There are three broad classes of controls that are addressed by the installation and ongoing management of the Root CA. In the information security world there is a common illustration for describing how security controls work (see figure). Physical controls protect the system (the Root CA) itself from unauthorized access. Technical

[12] URL: http://middleware.internet2.edu/certpolicies/

controls provide a layered defense; govern who can login and how the audit logs are protected. Administrative controls guide and enforce behaviors by the people who have access to the system.

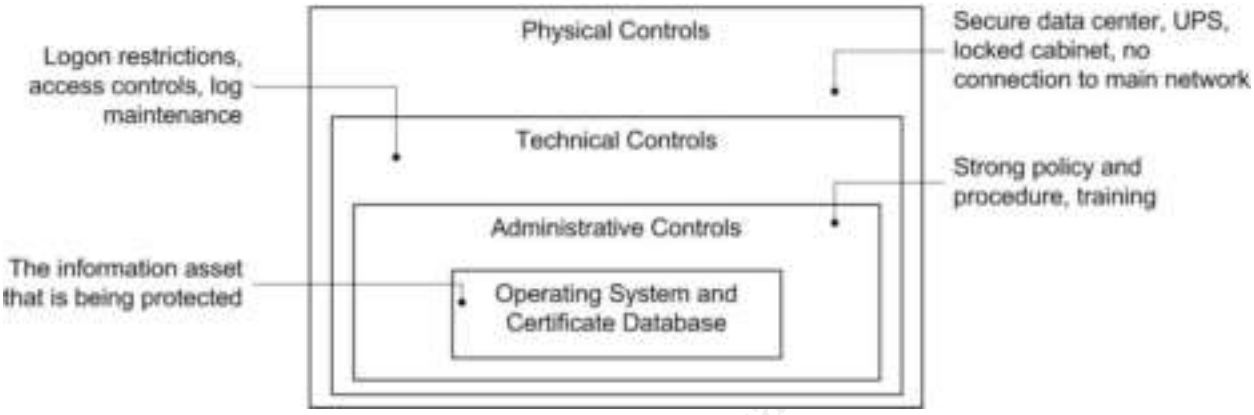


Figure 1: Controls Model.[13]

Physical Installation Considerations

HEBCA CP Sections:

- 5.1 PHYSICAL CONTROLS FOR THE HEBCA OR INSTITUTION CA

Location: The system is installed in a limited access data center (described above). Based on organizational policy, the only personnel who have access to the data center computer room are people who have job responsibilities within the data center itself. Based on the site Certificate Practices statement, the only people who have keys to the security cabinet are the Information Systems Security Officer, the Data Security Administrator, and the Assistant Director of Enterprise Systems. Two of the three people must be present to allow access to the cabinet securing the PKI hardware. Each time that the cabinet is accessed an entry is made in a log book.

There is building level UPS and onsite diesel generator power with sufficient onsite fuel reserve for 72 hour operations of the data center during summer (the HVAC system is sized for running air conditioning for the data center in August, the hottest time of the year for the geographical location).

HSM Access: Access to the Hardware Security Module (the HSM) which protects the private keys of the CA is governed by the "N+1 of X" rule. This rule states that a simple majority of key holders must be present with smart cards in order to enable access to the private keys of the CA which are held in the HSM. For this site, there are

[13] This model is from Shon Harris's book, "CISSP All in One Guide, 2nd Ed.", Chapter 3, Security Management Practices, p. 52.

five (5) sets of smart cards issued (the X) and three (3) people must be present to access the HSM (the N+1 model).

Inventory: Initially, an inventory of system components is made. Serial numbers of each item that can be considered a "component" will be recorded and logged. This includes the chassis, power supplies (if numbered), and disk drives. Next, the system will be installed in its rack. The network adapter(s) will be plugged into a 4 port hub so that the system will have an Ethernet link without being connected to a real network. The remaining two connection points will have a blank RJ45 connector installed so that no other network cables can be plugged into the hub. So - at this point the server is inventoried, in its rack, and secured from other network devices.

Rack Security: The rack has lockable half doors on the front and rear - meaning that the doors are about 1/3 of the height of the rack. A fixed shelf is installed at the top of the doors, which prevents entry into the space where the server(s) are. At this point the server(s) are physically protected from access, essentially being "caged", as illustrated below.

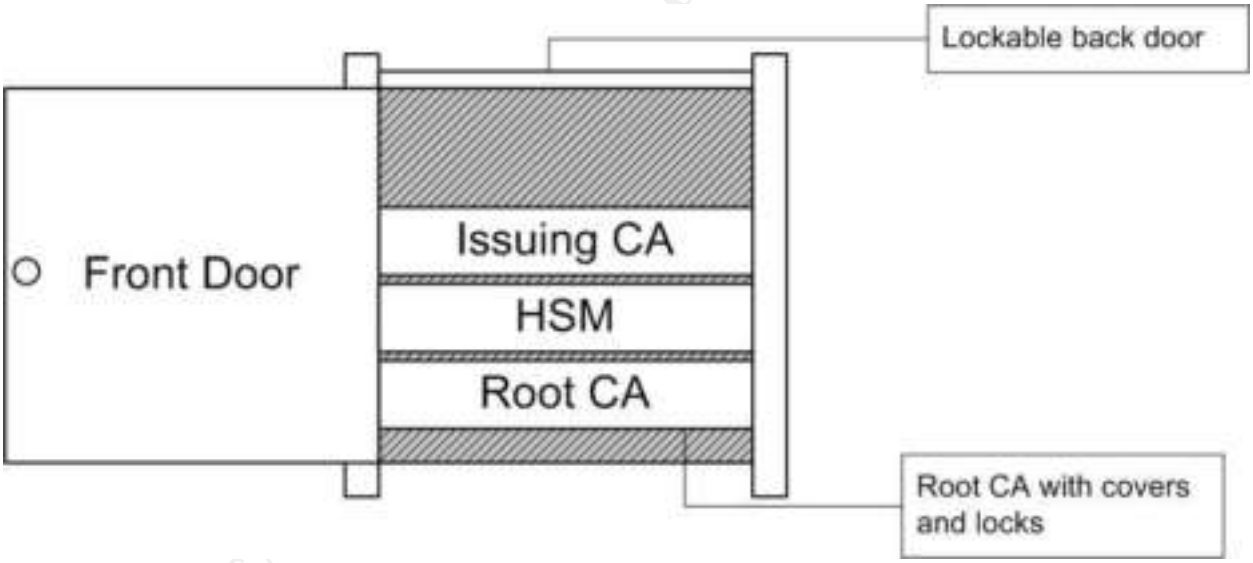


Figure 2: Rack Illustration

Administrative Controls

HEBCA CP Sections:

- 5.2 PROCEDURAL CONTROLS FOR THE HEBCA AND INSTITUTION CA
- 5.3 PERSONNEL CONTROLS

There are four identified roles for the CA. They are[14]:
1. Administrator – authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.
2. Officer – authorized to request or approve certificates or certificate revocations.
3. Auditor – authorized to view and maintain audit logs.
4. Operator – authorized to perform system backup and recovery.

These roles are formalized through site operational policy, and the appropriate staff are identified elsewhere. As part of the annual review cycle, a confidentiality statement is signed by each person. The group of people identified by these roles received training on the CPS and the strict management policy of the Root CA. Since the University is a state agency as per state policy each of the people filling an identified role has had a criminal background check. Lastly, the Root CA is only managed by local staff - there are no vendors who work with the Root CA.

Step by Step OS Installation

Checklist

This section will work through a checklist of steps to perform when installing RedHat Enterprise Server 2.1 as a secured system supporting Netscape Certificate Management Server 6.2 and the HEBCA. For reference, the checklist is provided below. As each aspect of the checklist is discussed, relevant sections of the draft HEBCA are identified for further study.

1. Install in a physically secure environment which will protect the Root CA.
2. Use valid RedHat media and updates.
3. Install the minimal OS components for the environment.
4. Use a disk layout that will support the high degree of auditing required.
5. Preserve initial OS files in order to show before and after state.
6. Protect the system from its network connection - cabled to a local hub.
7. Remove unnecessary software / system packages.
8. Configure the system to support Netscape CMS (application users) and the four operational roles (4 users).
9. Remove unnecessary local and network services (use chkconfig).
10. Increase the amount of system logging to support audit requirements.
11. Assess the system by using the CIS tool.
12. Assess the system externally with a scanning tool and improve security based on results provided by the tool.

[14] This text is taken directly from the CP document itself, p. 52. For reference the FBCA document defines the same roles with the same text.

13. Perform an initial assessment of open files and processes, establishing a baseline for later analysis and auditing.
14. Insure that the system can support the HEBCA CP audit requirements, as outlined in section 4.5 of the current HEBCA CA CP draft.
15. Install a file integrity tool (Tripwire).

Initial RHES Installation

First and foremost, the installer system administrator will use genuine manufacturer CD media. Note the actual media used will be preserved/retained for the life of the Root CA. For the purposes of installation, a separate written log will be kept (using a notebook PC) that will record installation options and choices while the system is installed.

Installation Process

1. Insert RHES 2.1 CD 1 into the drive and power up the system. Log the start time.
2. The initial greeting screen should appear. At the prompt, choose text based installation by typing in "linux text".
   Note: Text mode installation is a matter of preference - others may prefer the GUI mode.
3. When the "Language Selection" screen is displayed, choose "English" and then OK to continue.
4. When the "Keyboard Configuration" screen is displayed, choose "us" and then OK to continue.
5. When prompted, perform tests of all four media (RedHat CD1 - CD4). Log the results of each media test and the time.
6. When the "Mouse Configuration" screen is displayed, choose an appropriate mouse. For instance, "Generic - 3 Button Mouse (PS/2)" and then OK to continue.
7. On the "Red Hat Enterprise Linux ES" screen, choose OK to continue.
8. On the "Installation Type" screen, use the arrow keys to select "Custom" and then choose OK to continue.
   Explanation: Due to the sensitive nature of the system that is being built, the maximum degree of control needs to be applied to the system install process. The "Server" option makes many decisions and relies on several assumptions.
9. On the "Disk Partitioning Setup" screen, use the arrow keys to select "Disk Druid" and press Enter to continue.
   Explanation: specific disk layouts are needed for the system, and they will be described next.
10. On the disk partitioning screen, individual partitions are added. Note that as partitions are added the correct file system type needs to be selected. The partition scheme is as follows:

a. Screen capture of Partitioning details.

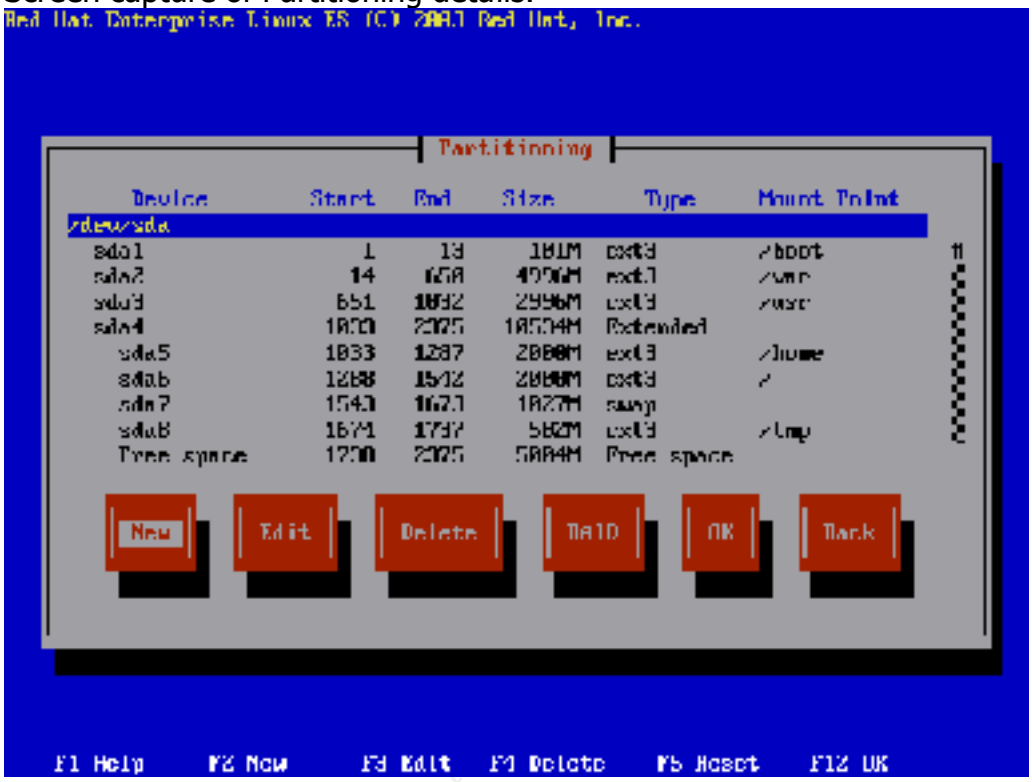


Figure 3: Disk Layout

b. Explanation. The /boot partition contains necessary booting files, and RedHat recommends it be 100 MB in size. The /var partition is where log files are kept - as logging is a mission critical aspect of the system, this file system should be separated out and of adequate size. The / partition contains all files during setup, and various operating system directories (therefore it must be a little larger). The /usr file system contains runtime binaries, man pages and libraries. The swap file system is generally recommended to be twice that of physical memory. The /tmp file system is separated out so that it may be managed. Also, should something occur that writes data to /tmp, there should be a cap on space so that a process cannot fill up the / file system (/tmp is normally a directory under /).

c. After editing the disk layout, choose OK to continue.

11. On the (first) "Boot Loader Configuration" screen, leave the default of "GRUB[15]" selected. Choose OK to continue.
12. On the (second) "Boot Loader Configuration" screen make sure that the option "/dev/sda Master Boot Record" is selected. The boot loader needs to be on the disk so that the system will start. Next, choose OK. There are no additional parameters

[15] GRUB: GRand Unified Bootloader.

to enter as the operating system supports the network adapters and the SCSI adapters in the system.

13. On the (third) "Boot Loader Configuration" screen, choose OK to continue (the system knows about the SCSI controller).
14. On the (forth) "Boot Loader Configuration" screen, there should be only one option for the boot loader - this is a new installation. Choose OK to continue.
15. On the GRUB password screen, use the tab key to check "Use GRUB Password". Then tab to the "Boot Loader" password fields, and enter the GRUB password for this server. Tab to the "Confirm" field and enter in the same password.
    Note and Explanation: the boot loader password will protect the operating system during boot up as it is required to perform non-standard booting procedures.
    a. Screenshot of the GRUB password entry.

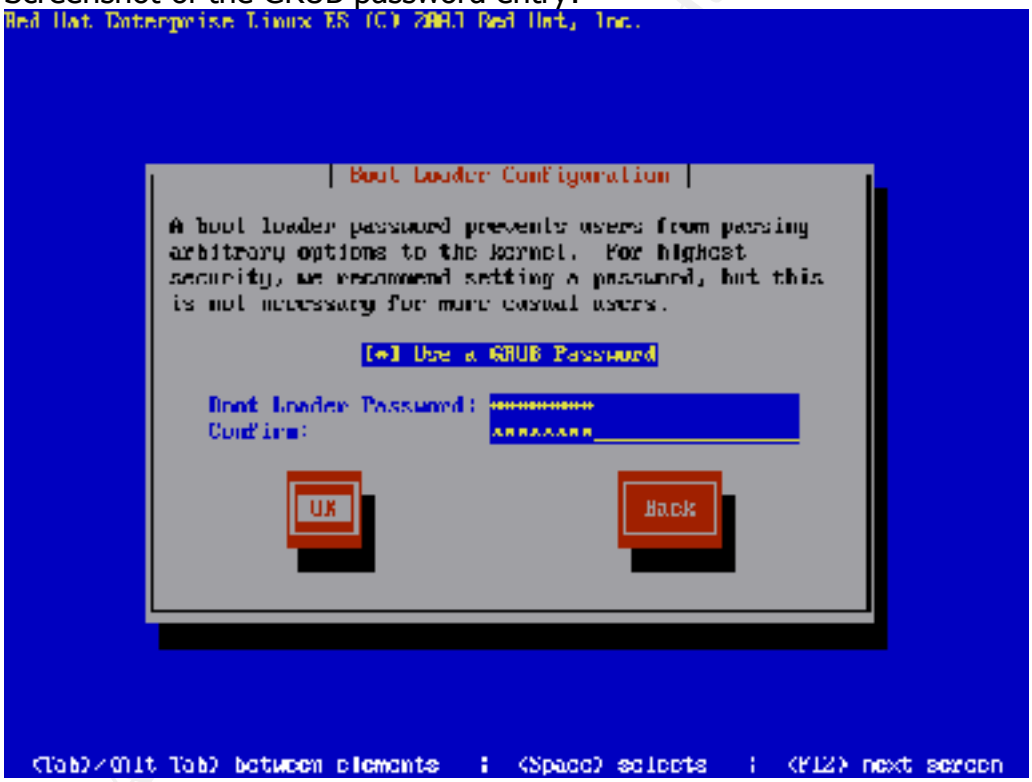


Figure 4: GRUB Password Entry

    b. Explanation: In order to help properly protect the system from possible physical compromise, a password is entered on the boot loader.
16. On the "Network Configuration" screen, deselect "Use bootp/dhcp". The Root CA will have a network interface configured, even though it will not connect to a network (Netscape CMS needs to be installed to a real IP address). Enter in appropriate network options.
    Example:

    IP Address: 192.168.1.17

Netmask: 255.255.255.0
Default Gateway: 192.168.1.17
Primary nameserver: 192.168.1.17 (the system will point to itself)

Choose OK to continue.

17. On the "Hostname Configuration" screen, type in "rootca.university.edu" as the host name. Choose OK to continue.
18. On the "Firewall" screen, select "High" and then choose OK to continue.
    Note: the firewall configuration will be changed later, but a minimal firewall needs to be "on" during the early configuration setup. RHES uses IPChains by default, and this will be changed to IPTables by hand, later.
19. On the "Time Zone Selection" screen, leave the default of "American/New York" (presuming this is the proper timezone). Do not check the "System clock uses UTC". The BIOS level clock will be set to the local time at the data center. Choose OK to continue.
20. On the "Root Password" screen, enter and confirm the agreed upon root password. Choose OK to continue.
21. On the "Add User" screen, do NOT enter any data. User creation needs to be fully logged as a matter of proper audit - users will be created later. Choose OK to continue.
22. On the "Authentication and Configuration" screen, leave the defaults of "Use Shadow Password" and "Enable MD5 Passwords". Choose OK to continue.
23. On the "Language Support" screen leave the default of "English" and choose OK to continue.
24. Next, package selection begins. On the "Workstation Defaults" screen, tab to check the "Customize software selection" option. Choose OK to continue.
25. On the "Package Group Selection", several package groups will be selected and then detailed options will be set by selecting "Select Individual Packages". Choosing packages is a three part process. First, the major groups. Second, individual components of the groups. And third, letting the installer figure out that some of the selected packages have deselected (or not selected) dependencies, so what is chosen will be over ridden somewhat. The goal in specifying groups and individual packages is to have the maximum degree of control. When the package groups are selected as outlined below, choose OK to continue.

    Select these package groups:

Package Group	Explanation
Printing Support	At various times reports and documents will be generated from the Root CA (a local printer will be attached as needed).
Classic X Windows	Deselect.
X Window System	Select

Package Group	Explanation
GNOME	Select. Users will need a window manager. Users may prefer GNOME over KDE.
KDE	Select.
Sound and Multimedia	Deselect - This is a server, and not an end user workstation.
Network Support	Basic networking for local operations will be needed; most of these options will be deselected later.
Dialup Support	Deselect. A modem attached to a Root CA would be in clear violation of best practice PKI principles, plus it would allow an avenue of attack.
Messaging and Web Tools	Select. Most of the options will be deselected. A browser is necessary for managing Netscape CMS (and not supplied with the CA software).
Graphics and Image Manipulation	Deselect. During installation, if there are necessary packages the installer will figure out what is necessary.
News Server	Deselect.
NFS File Server.	Deselect.
Windows File Server.	Deselect.
Anonymous FTP Server	Deselect.
SQL Database Server.	Deselect.
Web Server.	Deselect. Netscape CMS will install its own as needed.
Router / Firewall	Select. Firewall software will be a necessary component later.
DNS Name Server	Deselect.
Network Managed Workstation.	Deselect.
Authoring and Publishing.	Deselect.
Emacs.	Select. Editors will be needed on the system, and Emacs is a great editor.
Utilities.	Select. This will open up sub options that will allow for more granular control of packages installed.
Legacy Application Support	Deselect.
Software Development	Select. A C Compiler is needed for installing optional software, and if there is any need later on for compiling any of the sample code with Netscape CMS a compiler will be necessary.
Kernel	Deselect. Netscape CMS depends on the specific kernel being

Package Group	Explanation
Development	installed - it should not be possible to change the kernel on the system.
Windows Compatibility / Interoperability	Deselect. Some reports may be needed from the system, but there are sufficiently powerful applications available on the Windows platform to deal with file format compatibility issues. Also, no Windows applications will be installed.
Server	Select. Basic server functionality is needed.
Everything	Deselect, as selecting everything is self-defeating.

26. On the "Individual Package Selection" screen, the specific packages need to be tailored. Remember that this part of package selection is designed to pair down the list of installed software - the installer will determine what is actually needed and will adjust the list of installed packages when done. For each major group, either "Remove" or "Add" options based on the table below. An asterisk indicates that there are several packages beginning with a name.

Package Name	Notes
Amusements/ Games	Remove All.
Amusements/ Graphics	Keep only "xscreensaver" (users will configure a screen saver).
Applications/ Archiving	Add: cdrecord, dump, sharutils Remove: rmt (Network backups will not be used).
Applications/ Communications	Deselect everything.
Applications/ Databases	Deselect everything.
Applications/ Editors	Add: various "emacs" packages and the "vim" packages. (emacs is a matter of preference - vi would suffice).
Applications/ Engineering	Deselect everything.
Applications/ File	No change.
Applications/ Internet	Remove: ftp, gftp, htdig, htmlview, kdenetwork, kdenetwork-ppp, kpppload, micq, mtr, mtr-gtk, ncftp, openldap*, openssh*, rsh, stunnel, talk, telnet, wget, xchat Add: Mozilla, mozilla-mail, mutt, netscape*
Applications/ Multimedia	Deselect everything.
Applications/ Publishing	Defaults are acceptable.

Package Name	Notes
Applications/ System	Remove: ipvsadm, isdn*, mkxauth, rdate, rdist, samba*, xisdnload Add: nmap*, redhat-config*, tripwire,
Applications/ Text	Defaults are acceptable.
Development/ Debuggers	Deselect everything.
Development/ Languages	Add: compat-egcs-c++ (Netscape CMS requires some compat libraries), gcc (will compile an application later), Remove: py* (python), rep*,
Development/ Libraries	Add: compat* (Netscape CMS requires some compat libraries), lam, less*, libpcap Remove: python*
Development/ System	Deselect everything.
Documentation	Add: man-pages, sendmail-doc
System Environment/ Base	Remove: alchemist, ksconfig, pam_krb5, rhn*, up2date*, yp*
System Environment/ Daemons	Remove: ORB*, autofs, cipe, esound, finger-server, nfs*, openssh*, pidentd, portmap, ppp, radvd, rp-pppoe, rsh*, rusers*, rwall*, rwho, samba*, talk-server, telnet-server, ucd-snmp, wvdial, yp*
System Environment/ Libraries	Add: ncurses4 (Netscape CMS required support) Remove: bonobo, arts, *audio*, eel*
System Environment/ Shells	Defaults are acceptable.
System/ Libraries	Defaults are acceptable.
User Interface / Desktop	Remove: vnc (remote control is highly unadvisable)
User Interface/ X	Remove: vnc* (as above, remote control is not advisable)
User Interface/ X Hardware Support	Add: If known, the specific library set for installed video card (ATI in this case).

27. On the "Package Dependencies" screen, select "Install packages to satisfy dependencies". If is check is made through the list, there are several packages that depend on packages that really won't hamper system security. Choose OK to continue.

28. On the "Video Card Configuration" screen, confirm that the installed video card is selected. Choose OK to continue.
29. On the "Installation to begin" screen, note the log location of the installation - /root/install.log. Once the installation is finished, this log file must be captured and preserved (as it documents the installation of the CA's OS). Choose OK to continue (and begin installation).
30. Once the packages are installed, the installer will prompt to create a boot disk on the "Boot Disk" screen. There is no floppy in the system, so select "No" to continue.
31. The last screen should confirm that RHES is installed. Choose OK to reboot.

A Note about RHES 3.0: Choosing RHES 2.1 begs the question, "Why not use a more recent OS?" In preparing this paper, that very idea was attempted. Through repeated attempts to install Netscape CMS 6.2, several libraries were missing on the system. Even after libraries were added, the setup program still failed to properly install Netscape CMS and attempting to start parts of Netscape CMS that appeared to install failed. Examples of dependant libraries include: libdb.so.3, ibnsres31.so[16], and libstdc++ libc6.2-2.so.3.

Preliminarily Post Installation Tasks

A Note on Documentation: There are some general tasks that need to be performed once the system is initially installed - but more importantly, the tasks must be documented. Tasks in configuring the system fall under following the "principle of due care". This principle states that professionals must conduct themselves with competence, diligence, and take every reasonable measure to prevent possible security breaches[17]. As part of properly installing and securing a Root CA, the systems administration staff must be able to demonstrate and prove what they did.

One of the better methods for documenting tasks performed is to use the UNIX/Linux "script" command. System administrators must run a command like "`script ~/admin_tasks/20031217_1103`" in a terminal window, or on the console. This command will record everything that the system administrator types in using the "`20031217_1103`" (date + time) file located in the "`~/admin_tasks`" directory (the ~ means the logged in users' HOME directory). If you are implementing steps outlined in this guide use the script command to document your work.

Preserve Initial Install Information: On the first reboot, the install log should be preserved. Copy the `/tmp/install.log` file a directory in root's home directory and query the RPM list.

```
Commands to preserve install details:
```

[16] Related RedHat bug: http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=91180
[17] This is paraphrased from Harris, p. 614.

```
Commands to preserve install details:
# cp /tmp/install.log ~/install_log
# rpm -qa | sort > ~/install_log/initial_rpm_list
```

Enable logging for bad logons: By default, the operating system will not log bad logon attempts. Support for this is critical to insuring the integrity of the Root CA and HEBCA audit. If there are any failed logon attempts the site needs to know about it, and it needs to be logged.

Check to make sure that there is a `/var/log/wtmp` file - there should be one. To enable logging for bad logon attempts, use the command to create the "btmp" file (a companion file to wtmp):

```
touch /var/log/btmp
```

Edit grub.conf: RHES 2.1 installs two kernels. The SMP kernel may not boot correctly on the particular system. By default, the SMP kernel is listed first in the `/boot/grub/grub.conf` file. Edit this file so that the "default" line reads "`default=1`", which will boot the single processor kernel as listed in the `grub.conf` file below.

```
grub.conf file
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sda5
#          initrd /initrd-version.img
#boot=/dev/sda

# boot the '1' kernel (the second in the list below - counting starts at 0)

default=1
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz

# below is the MD5 encrypted password from the install process
password --md5 $1$àóþ1æp.8$ISDBedwD5huzC4fXi7hfy0
title Red Hat Enterprise Linux ES (2.4.9-e.12smp)
       root (hd0,0)
       kernel /vmlinuz-2.4.9-e.12smp ro root=/dev/sda5
       initrd /initrd-2.4.9-e.12smp.img
title Red Hat Enterprise Linux ES-up (2.4.9-e.12)
       root (hd0,0)
       kernel /vmlinuz-2.4.9-e.12 ro root=/dev/sda5
       initrd /initrd-2.4.9-e.12.img
```

Edit hosts file: The hosts file needs to be configured for local name resolution of the server. Here, the Root CA will be setup to use 192.168.1.17 for the name of the system. In order to support name resolution, the system needs to be able to resolve the IP address to names. Below is the hosts file for the Root CA with the Fully Qualified Domain Name (FQDN) and the short name on the last line.

hosts file
```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1           localhost.localdomain localhost

192.168.1.17  rootca.university.edu rootca
```

Review/Edit the network file: The `/etc/sysconfig/network` file controls whether networking is enabled and the hostname of the system. Here, the name of the system must be changed from "`localhost.localdomain`" to the proper name.

/etc/sysconfig/network file
```
NETWORKING=yes
HOSTNAME=rootca.university.edu
```

Review/Edit the ifcfg-eth0 file: The `/etc/sysconfig/networking/devices/ifcfg-eth0` file contains the details about the local Ethernet configuration. It should be edited to have the proper IP address (192.168.1.17, in this case).

/etc/sysconfig/networking/devices/ifcfg-eth0
```
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
IPADDR=192.168.1.17
GATEWAY=192.168.1.17
TYPE=Ethernet
USERCTL=no
NETMASK=255.255.255.0
NETWORK=192.168.1.0
BROADCAST=192.168.1.255
PEERDNS=no
```

Review/Edit the resolv.conf file: The `/etc/resolv.conf` file needs to be configured with the domain suffix name for the system. Edit the `resolv.conf` file so it has a "domain" entry as shown below.

/etc/resolv.conf
```
domain university.edu
```

Configure X11: By default, X11 will listen on TCP port 6000 for remote connections. X11 should be configured not to accept any connections over the network. Even though this system will not be connected to a network, connectivity should be disabled. This measure is an example of "defense in depth", which means that extra measures of security are added in order to provide stronger defense. Also, the level of auditing that the X server does needs to be increased above the default (1) so that all successful connections and disconnects are reported.

Edit `/usr/lib/X11/xdm/usr/lib/X11/xdm/Xservers` and change the configuration line so it reads as follows:

```
:0 local /usr/X11R6/bin/X -nolisten tcp -audit 2
```

Next, edit the `/etc/X11/gdm/gdm.conf` file and change the configuration line at the bottom of the file to read:

```
0=/usr/bin/X11/X -nolisten tcp -audit 2
```

Continue editing the `gdm.conf` file, and every line that says " `command=/usr/X11R6/bin/X`" should read "`command=/usr/X11R6/bin/X -nolisten tcp -audit 2`".[18]

As will be mentioned later, X11 actually needs to be updated so as to not actually listen to incoming requests on 6000/TCP.

Test with reboot: Once these changes are made (startup kernel and network), reboot the system with the "`reboot`" command, login, and ping the system by name with the command "`ping rootca.university.edu`". At this point the system should be configured for "local networking". Remember that this system is not to be attached to a production network - the Ethernet interface(s) should be connected to a local hub with no other connections.[19]

Enable Script Capturing: Once the initial configuration is done, the `/etc/profile` script is updated to support running a "script" command (as discussed earlier) for every login session. By putting commands to run the script command every time someone logs in, automatic tracking of commands occurs. Modify the file as shown below:

Additions to `/etc/profile`

```
...
for i in /etc/profile.d/*.sh ; do
    if [ -r $i ]; then
        . $i
    fi
done

unset i

# add the following IF test and script command

if [ ! -d $HOME/activity ]; then
   mkdir $HOME/activity
fi
script $HOME/activity/`date+%Y%m%d.%H%M%s`.${USER}.$$
```

[18] This additional fact was confirmed by Carlo Aureus in RedHat Technical support.

[19] It is worth pointing out that there is an alternative. A crossover cable can be plugged into both of the Ethernet interfaces on the system, and sealed with tape. However, this would mean that the tape would need to be removed during monthly audit (discussed later). Using an external device as described here would, hopefully, keep things "cleaner" (literally).

Script Capture Explanation: The script command at the end of the /etc/profile file will create a file in the logging in users' home directory that is stamped with the data, time, username, and process ID.

Script Capture Risks: There is a risk in using this method of command documentation. First, someone might type in "exit" or press Control-D, and then run more commands. Second, if an Xterm isn't invoked with a shell as a "login" shell, command logging can become confused (commands intermixed in the log file). Third, if someone cat's the script command file, it will log what its displaying - and quickly consume disk space by logging what it is displaying. Each of these risks it outweighed by the benefit of command logging, because the HEBCA requires that system tasks be audited, using the script command in this manner documents what people did on the system. Making sure that staff follows good rules solves these problems and takes advantage of the script command. Example rules are "exit", and really exit when one logs off, always 'login' with shells and don't read the script file, especially since the history command shows what commands were executed.

Package Review and Removal

Many of the installed packages are not necessary - meaning that they do not provide for system administration or functionality which relates to running Netscape CMS 6.2. Ultimately, that is the primary decision criterion on which packages should be removed is whether they support the systems primary function - being a Root CA. Remember that part of being a Root CA is producing audit reports, so there are packages that should be on the system such as an editor and printing support. The list of packages (RPM's) that were initially is listed in Appendix A. Packages that were removed are underlined in the Appendix.

At the command line the command "`rpm -q --info --all`" is used to see all of the installed packages and several details about the package.

Example output of "rpm -q --info --all"

```
Name        : glibc                         Relocations: (not relocateable)
Version     : 2.2.4                              Vendor: Red Hat, Inc.
Release     : 31.7                           Build Date: Thu 12 Dec 2002 10:35:06 AM EST
Install date: Thu 18 Dec 2003 11:19:47 PM EST      Build Host: stripples.devel.redhat.com
Group       : System Environment/Libraries   Source RPM: glibc-2.2.4-31.7.src.rpm
Size        : 18101928                          License: LGPL
Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
Summary     : The GNU libc libraries.
Description :
The glibc package contains standard libraries which are used by
multiple programs on the system. In order to save disk space and
memory, as well as to make upgrading easier, common system code is
kept in one place and shared between programs. This particular package
contains the most important sets of shared libraries: the standard C
library and the standard math library. Without these two libraries, a
Linux system will not function.

...

Name        : perl-NDBM_File                Relocations: (not relocateable)
Version     : 1.75                               Vendor: Red Hat, Inc.
```

Example output of "rpm -q --info --all"

```
Release     : 26.72.4                       Build Date: Tue 26 Mar 2002 02:30:47 PM EST
Install date: Thu 18 Dec 2003 11:20:11 PM EST      Build Host: daffy.perf.redhat.com
Group       : Development/Languages         Source RPM: perl-5.6.1-26.72.4.src.rpm
Size        : 24835                            License: Artistic
Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
Summary     : NDBM_File module for Perl
Description :
NDBM_File modules for Perl

...
Name        : XFree86-doc                   Relocations: (not relocateable)
Version     : 4.1.0                              Vendor: Red Hat, Inc.
Release     : 44                            Build Date: Sun 05 Jan 2003 05:48:28 PM EST
Install date: Thu 18 Dec 2003 11:55:55 PM EST      Build Host: stripples.devel.redhat.com
Group       : Documentation                 Source RPM: XFree86-4.1.0-44.src.rpm
Size        : 10106753                         License: MIT
Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
Summary     : Documentation on various X11 programming interfaces.
Description :
XFree86-doc provides a great deal of documentation, in PostScript
format, on the various X APIs, libraries, and other interfaces.  If
you need low level X documentation, you will find it here.  Topics
include the X protocol, the ICCCM window manager standard, ICE
```

There are two methods to remove packages. The RPM command can be used or the graphical GNOME RPM tool. Either method is satisfactory - but there is an advantage in using the GUI tool. As can be seen in the screenshot, the package details list shows package name, version, release, and a summary of the packages.

Command Line Example: To remove the thee parts of VNC[20], which are "`vnc-server`", "`vnc-doc`", and "`vnc`" packages with the command line RPM tool, for example, issue the commands below. The first three commands remove a specific package, and the last command checks to make sure that VNC is no longer in the RPM database (and off of the system).

Commands to remove VNC:

```
rpm -e vnc-server
rpm -e vnc-doc
rpm -e vnc
rpm -qa | grep vnc
```

GUI Application Example: In the next figure is a screenshot of the Gnome RPM graphical package manager. In the figure, the "Games" group is selected and the "fortune-mod" package is then selected. For reference, the Package Info dialogue is also shown, so that the details of the package are visible. In order to remove this package, press the "Uninstall" button.

[20] VNC stands for "Virtual Network Computing".

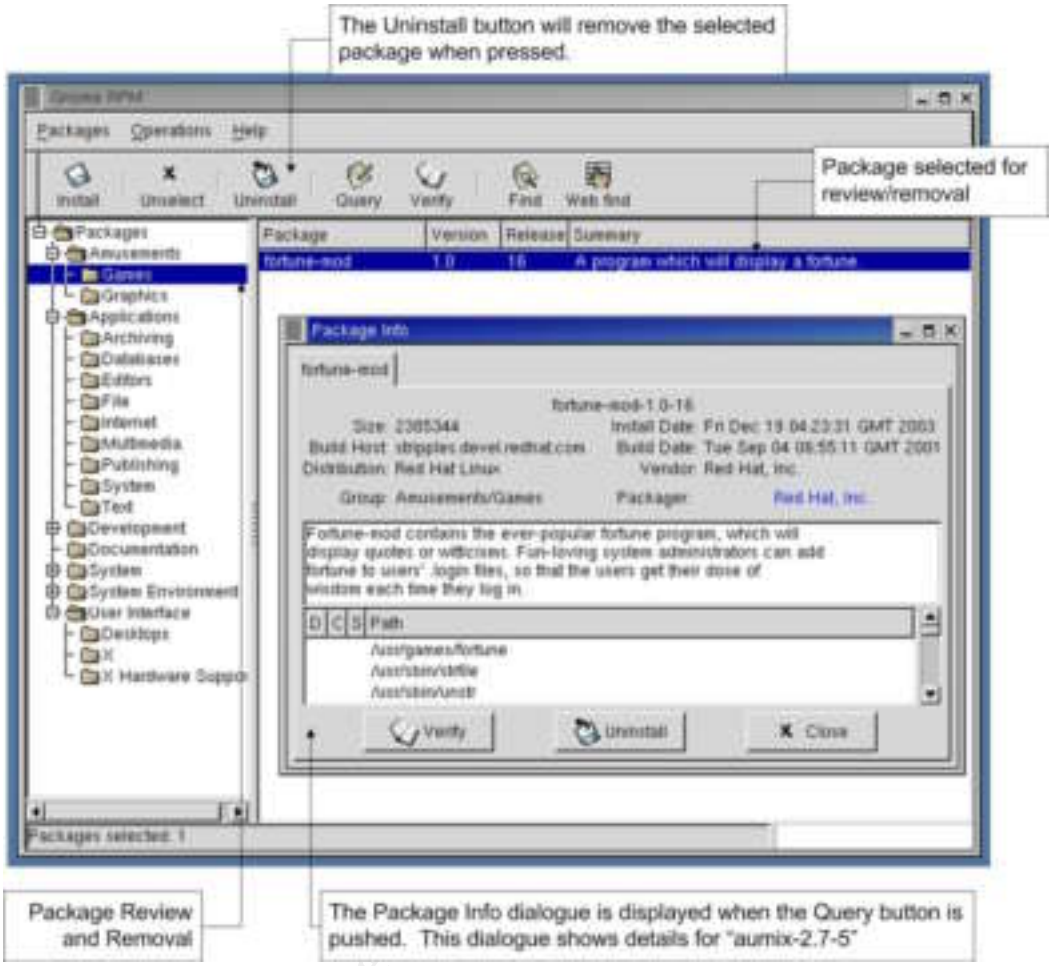


Figure 5: Gnome RPM Manager

Update System Software

Currently, RedHat expects customers to use the RedHat Network local client (up2date) in order to automate the installation of patches on the system. Since it is not possible to update patches from a system disconnected from the network using a network based update client (even in offline mode[21]), the only way that software updates can be applied is by downloading the "Update 3[22]" CD sets from RedHat and going through the RPM directories by hand - a tedious process at best.

What should be updated? Software that relates to system security, either as an enhancement or a fix is what should be updated. However, the kernel patches should not be installed because Netscape CMS is only supported on kernel 2.4.9-e.12.

[21] This fact was verified using Red Hat's Web based support process. A ticket was started, the situation explained, and technical support confirmed that the only way to update patches was to download the CD's and search through them by hand.
[22] Update 3 supercedes Update 2, as confirmed with RedHat technical support.

Security Packages that the Root CA depends on include:

- sudo
- IPTables
- Tripwire
- syslog
- X11 (discussed below)

Checking the RPM's on each of the four Update 3 CD's from RedHat, these updates are found:

- CD 1 - iptables-1.2.5-3.i386.rpm - same as on system
- CD 1 - sudo-1.6.5p2-1.7x.1.rpm - same as on system
- CD 1 - sysklogd-1.4.1-4.i386.rpm - same as on system
- CD 2 - tripwire-2.3.1-5.i386.rpm - same as on system

Since there are no necessary updates (at this time) for the system on the Update CD's from RedHat, no packages need to be updated. If there were a package that needed to be updated, it should be copied to a common directory like `/opt/update` and then the "`rpm -Fvh PACKAGE`" command run on the update. The -F option "freshens" the system with the update, -v means verbose output, and -h means to show hash marks as the package is unpacked (indicates progress).

Upgrading X11: In order for X11 to properly avoid listening to port 6000/TCP, several X11 packages need to be upgraded. The corresponding RPM's for these packages are on CD1 and CD2 of the RHES Update 3 CD's:

- XFree86-libs-4.1.0-50.EL
- XFree86-100dpi-fonts-4.1.0-50.EL
- XFree86-75dpi-fonts-4.1.0-50.EL
- XFree86-ISO8859-15-75dpi-fonts-4.1.0-50.EL
- XFree86-twm-4.1.0-50.EL
- XFree86-xfs-4.1.0-50.EL
- XFree86-4.1.0-50.EL
- XFree86-ISO8859-15-100dpi-fonts-4.1.0-50.EL
- XFree86-tools-4.1.0-50.EL
- XFree86-xdm-4.1.0-50.EL

In order to upgrade these packages, the individual RPM file needs to be copied from the CD to the system (into the `/opt/X11updates` directory) and the command "`rpm -Fvh *.rpm`" issued.

Logon Banners

HEBCA CP Sections:

- 5.2 PROCEDURAL CONTROLS FOR THE HEBCA AND INSTITUTION CA
- 5.3 PERSONNEL CONTROLS

Logon Banners are essential component of system security. There must be a warning banner which a user must see whenever the system is left at a logon prompt. Also, in order to address Federal wiretap requirements, there is existing organizational policy that requires system logon banners that allows for wiretap by consent in conformance with established Federal law (related law includes 18 U.S.C. §§ 2510-22, 18 U.S.C. §§ 2701-12, and 18 U.S.C. §§ 3121-27).

Logon banners must address five points:[23]

1. Access to the system is limited to authorized activity.
2. Unauthorized access and modification is prohibited.
3. Unauthorized use may face criminal or civil penalties.
4. Use of the system may be monitored and recorded.
5. Law enforcement may be notified if monitoring reveals criminal activity.

These points are very good - and they would apply well to most computer systems operated by a given organization. However, they do not specifically address a particular requirement unique to a Root CA- that being that the use and management of the system must be conducted in accordance with the policies set forth in the Certificate Practices Statement (CPS) for the organization. With that in mind, the following warning banner must be installed on the system:

> "This University owned and operated Certificate Authority Server must be used in accordance with the Certificate Practices (CP) Statement, the CP Policy, and the CP Procedures as established by the University. Only properly authorized staff may access this system. Access to this system must be logged in the logbook. Unauthorized use of this system may result in criminal or civil penalties. Use of this system will be monitored and recorded, and may not be circumvented in any way. Use of this system implies consent in conformance with Federal law (including 18 U.S.C. §§ 2510-22, 18 U.S.C. §§ 2701-12, and 18 U.S.C. §§ 3121-27)."

This logon banner must be put in every banner file (meaning edit these files and add in the text) associated with every access point to the system, including:

`/etc/issue` - this file contains the logon banner which is displayed at system startup.

[23] These five points are taken from the SANS GCIH curriculum, Track 4, Day 1.

`/etc/issue.net` - network equivalent of `/etc/issue`.
`/etc/motd` - this file is displayed after login before the login shell is executed.

After these files are edited, log out and log back in to make sure that the banners are functioning.

Create Necessary Accounts

HEBCA CP Sections:

- 5.2.1 Trusted Roles - this section defines the actual tasks for a role and is quoted below for reference.

To quote the current HEBCA CP, trusted roles are defined as:[24]

> "A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the HEBCA or an Institution CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion."

Role	Function	Staff and login name[25]
Administrator	• installation, configuration, and maintenance of the CA; • establishing and maintaining CA system accounts; • configuring certificate profiles or templates and audit parameters, and; • generating and backing up CA keys.	C. Elwes / celwes M. Patinkin / mpatink
Officer	• registering new subscribers and requesting the issuance of certificates; • verifying the identity of subscribers and accuracy of information included in certificates; • approving the issuance of certificates;	I. Montoya / imontoya M. Max / mmax

[24] This text is taken directly from the CP document itself, p. 52-54. For reference the FBCA document defines the same roles with the same text.
[25] Note: These names are fictitious. They are used here as placeholders.

Role	Function	Staff and login name[25]
	• requesting or approving the revocation of certificates.	
Auditor	• reviewing, maintaining, and archiving audit logs; • performing or overseeing internal compliance audits to ensure that the HEBCA or institution CA is operating in accordance with its CPS;	B. Crystal / bcrystal W. Shawn / wshawn
Operator	• The operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media;	C. Sarandon / csarando R. Wright / rwright

Operating system groups must be created for these roles. Then, the users can be created in the proper groups. Later, these groups will be used when configuring sudo so that group members can perform job tasks without requiring the root password. Below is a script that is used to create users and groups for this system. Note that the default "operator" account in the RHES password file is not reused -there should be no carryover from the initial operating system install, as operators have specifically defined roles for this system based on the HEBCA.

Script file to create groups and users:

```
#!/bin/sh
/usr/sbin/groupadd caadmin
/usr/sbin/groupadd officer
/usr/sbin/groupadd auditor
/usr/sbin/groupadd ops
/usr/sbin/useradd -g caadmin celwes -c "C. Elwes Server Admin"
/usr/sbin/useradd -g caadmin mpatink -c "M. Patinkin Server Admin"
/usr/sbin/useradd -g officer imontoya -c "I. Montoya Sec Officer"
/usr/sbin/useradd -g officer mmax -c "M. Max Sec Officer"
/usr/sbin/useradd -g auditor bcrystal -c "B. Crystal Auditor"
/usr/sbin/useradd -g auditor wshawn -c "W. Shawn Autidor"
/usr/sbin/useradd -g ops csarando -c "C. Sarandon Operator"
/usr/sbin/useradd -g ops rwright -c "R. Wright Operator"
```

Once the accounts are created, individual passwords must be assigned. Many organizations create a default password amongst trusted staff - this practice may suffice for a typical commercial group, but not for a Root CA. Individual passwords must be created by each person - a default password can allow for one person to assume another's login identity.

Protect Files and File Systems

Now that the properly authorized users and groups are created, and unnecessary users and groups are deleted, the user password and user group files need to be protected

with the `chattr` command. Note that after this next change, file attributes will need to be reset in order to change users and passwords.

Comands to protect password and group files

```
chattr +i /etc/passwd
chattr +i /etc/group
chattr +i /etc/shadow
```

Configure/Enable sudo Access[26]

HEBCA CP Sections:

- 5.2 PROCEDURAL CONTROLS FOR THE HEBCA AND INSTITUTION CA
- 5.3 PERSONNEL CONTROLS

The `sudo` program is designed to allow authorized users to perform supervisory or enhanced privilege operations without giving them the root (or super user) password. UNIX/Linux suffers from an architectural security issue in the sense that it follows the "all or nothing" security model - Root CAn do any and everything. Access with `sudo` must map to the operational roles as defined above, as defined under "Administrative Controls". `sudo` needs to be configured to a) audit and b) provide proper access based on the staff members operational (or functional) role on the system.

Below is a commented `/etc/sudoers` file - each comment explains what is occurring and how the settings map to an operational role for the Root CA as defined in the HEBCA. Note that this file is incomplete. Commands will need to be added for working with the HSM, which hasn't been purchased as of this document.

/etc/sudoers file

```
# sudoers file.
# This file MUST be edited with the 'visudo' command as root.
# See the sudoers man page for the details on how to write a sudoers file.

# the name of the machine - specified for completeness
Host_Alias      ROOTCA=rootca.university.edu

# Specific command groups for groups.
# The auditor group needs to be able to read and search various log files.
# reading files can be accomplished in several ways - this should cover the bases
Cmnd_Alias      READ=/bin/more, /usr/bin/less, /bin/grep, /bin/cat

# operators will need to do backup and recovery, system startup and shutdown
Cmnd_Alias      BACKUP = /sbin/dump, /bin/tar, /bin/cpio, /sbin/restore
Cmnd_Alias      SHUTDOWN = /sbin/shutdown, /sbin/reboot

# the four groups, and their membership
User_Alias      ADMINS=celwes,mpatink                   # Administrator role
User_Alias      OPER=csarando,rwright                   # Operator role
User_Alias      CA=imontoya,mmax                        # Officer role
User_Alias      AUDIT=bcrystal,wshawn                   # Auditor role

# Default entries - actions taken must be logged to syslog and to their own file
# for audit trail purposes.  Mail should be generated to the lead auditor of errors
```

[26] For complete reference to sudo, see: http://www.courtesan.com/sudo/man/sudoers.html.

/etc/sudoers file

```
# in usage
Defaults        syslog=auth, logfile=/var/log/sudolog, \
                mail_no_user, mail_no_perms, \
                mailto=bcrystal

# system administrators don't need a "lecture" and the auditor should be informed
# of any bad password attempts
Defaults:ADMINS !lecture, mail_badpass

# User privilege specification
root    ALL=(ALL) ALL

# allow the auditors to read files on the system
AUDIT   ROOTCA = READ

# the actual administrators need to be able to run normal root commands
%caadmin                ALL=(ALL)       ALL
```

This configuration needs to be tested. Some example tests are:

- Login as bcrystal and issue the command "`sudo more /var/log/messages`". Presuming that bcrystal is in the proper group, the messages file should be viewable, as it is root owned and only root readable/writeable.
- Login as rwright and issue the command "`/usr/sbin/reboot`". The results should be quite obvious, as the system reboots.

Other tests should be performed as appropriate by the person(s) who are the respective account holders.

Disable Root Logins[27]

Now that there are authorized accounts on the system, and now that at least two of those accounts can perform supervisory functions, it is time to disable root (or super user) access at the system console. Note that there is a specific order in these operations - root access should not be disabled until there are people that can perform supervisory functions with `sudo`. This also means that, henceforth, actions taken by the two system administrators will be performed by the appropriate staff using the `sudo` command.

There are two tasks involved in disabling root login. First, root's shell is set to `/sbin/nolgin`. This will prevent root from actually logging in when shell access is required. Second, the valid list of devices for root login can be entered in the `/etc/securetty` file. If the file is empty, Root CAnnot login on any device. In order to

[27] The procedures in this section are based on the RedHat knowledge base. URL: http://kbase.redhat.com/faq/dml_fetch.pl?CompanyID=842&ContentID=680&FaqID=587&word=/etc/passwd&faq_template=http://kbase.redhat.com/faq/searchfaq.shtm&topic=38&back_refr=http://kbase.redhat.com/faq/&topicname=Red%20Hat%20Linux%209/8.0/7.x&Id=&Instance=&Shared=

create an empty `securetty` file, edit the file and delete each of the lines. Once done, root won't be able to interactively login.

Disable Extra Gettys

The Root CA needs to provide an environment where a single console - a single entry point - is allowed into the system. By default, RHES (and many other Linuxes) run additional getty processes that can be accessed from the system keyboard. Accessing additional getty's is done by pressing ALT-F1 to ALT-F6 - there are six possible login points on the system. This action is important because the system, should in essence, only be allowed to be used by a single authorized person at a time - the system admin for SA tasks, the auditor for auditing tasks, etc. By controlling the network (discussed elsewhere) and extra getty processes we guarantee that one user can functionally use the system at a time.

To disable extra gettys, edit the `/etc/inittab` file and comment out (or delete) the five mingetty lines that start as shown in the next table.

Partial entry of the `/etc/inittab` file.

```
...
# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
# 2:2345:respawn:/sbin/mingetty tty2
# 3:2345:respawn:/sbin/mingetty tty3
# 4:2345:respawn:/sbin/mingetty tty4
# 5:2345:respawn:/sbin/mingetty tty5
# 6:2345:respawn:/sbin/mingetty tty6
...
```

Improve Default Syslog Operations

Syslog is the UNIX/Linux system logging facility. While the default configuration may be acceptable for many environments, for a system like a Root CA a higher degree of logging and more granular/verbose logging required. There are two important concepts to understand about syslog - facilities and priorities. A facility is a category of messages. Currently, the supported facilities in Linux are auth, auth-priv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, uucp, and local0 through local7. Facilities are independent of one another. Priorities are hierarchical (from lowest to highest). Currently, the defined priorities are debug, info, notice, warning, err, crit, alert, emerg and panic. For syslog to work more responsibly for the Root CA, there should be more logging than the default and logs should separated out a little more to represent what is being logged.

Edited Syslog.conf file:

```
# Log all kernel messages to the a log file for later use.
# log higher priority messages to the screen
kern.*                                                  /var/log/kernel
kern.warn                                               /dev/console
```

Edited Syslog.conf file:

```
# enable logging that is sent / split out by priority, grouping all "level" messages
# together in a single file - by priority
*.debug                 /var/log/1debug
*.info                  /var/log/2info
*.notice                /var/log/3notice
*.warning               /var/log/4warning
*.error                 /var/log/5error
*.critical              /var/log/6critical
*.alert                 /var/log/7alert
*.panic                 /var/log/8panic

# enable marking
mark.*                  /var/log/messages

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info                  /var/log/messages
# All mail messages from warn and above are logged to "messages" (default is 'none')
mail.warn               /var/log/messages
# all authpriv facility messages are logged to "messages" (default is 'none')
authpriv.*              /var/log/messages
# All cron messages from warn and above are logged to "messages" (default is 'none')
cron.warn               /var/log/messages

# The authpriv file has restricted access.
# log both auth and authpriv to the secure file - this file contains security
# related events (this is non-standard)
auth.*                          /var/log/secure
authpriv.*                      /var/log/secure

# Log all the mail messages in one place.
mail.*                          /var/log/maillog

# Log cron stuff
cron.*                          /var/log/cron

# Everybody gets emergency messages
*.emerg                         *

# Save news errors of level crit and higher in a special file.
uucp,news.crit                  /var/log/spooler

# Save boot messages also to boot.log
local7.*                        /var/log/boot.log
```

Once the `/etc/syslog.conf` file is adjusted, the startup for syslog is adjusted. Edit the `/etc/init.d/syslog` file, and change the `$OPTIONS` variable to be "`-m 30`" instead of "`-m 0`". This setting will cause syslog to write a MARK line to the messages file. For the Root CA, these messages will help to document how long the system was up and the relative activity during its operations - a critical auditing element as this shows the period of activity for the system.

Install Supplemental Software

Additional programs need to be installed on the system as listed in the table below.

Package Name	Package Source
lsof	http://www-rcd.cc.purdue.edu/~abe/
CI Security Level 1 Assessment tool	http://www.cisecurity.org

Descriptions:

- lsof: This program is used to "list open files for running processes" and it is used as a great diagnostic tool.
- CI Security: This is an analysis tool that is designed to aid and assist in reducing information security threats. The benchmarks are designed by a consensus of security professionals and organizations. This tool audits - it does not fix the system.[28]

A Matter of Trust: In order to trust the site VIC.CC.PURDUE.EDU, its IP address (128.210.7.20) was looked up with `nslookup` and at whois.arin.net, to make sure that the IP address really belonged to Purdue University (it did), and a direct ftp connection was done to that IP with a command line FTP client (not on the Root CA- an office PC). The same tests were done for cisecurity.org. For each of the packages source code is available and can be reviewed as needed. Note that from an auditing perspective, a CD is made with each additional package and stored with the original media used to install the system (forming a record).

CIS Rationale: It is worth mentioning that there are other tools that can be used to audit and harden a system - an obvious choice is Bastille Linux. The CIS benchmark was chosen over other tools because the author's provide an MD5 sum which can be used to mathematically verify the integrity of the downloaded package.

Next, the packages were copied to a CD for installation on the system even though, collectively, they will fit on a floppy. CD's are expected to have a shelf life of 16 to 20 years.

Once the CIS tool is copied on the system (in an appropriate directory, like `/opt/CIS`) an md5 sum must be verified on the package file against the md5 sum from the www.cisecurity.org web site. Creating a local md5 sum is designed to insure that the tool available for download is the tool that we actually downloaded and the tool that was actually posted (no bits changed in transit and at the other end). Below is a sequence of commands that shows the process of verifying the md5 sum of the CIS tool (as one of the approved administrators, celwes):

Commands for verifying CIS package integrity:

```
[celwes@rootca CIS]$ ls -la
total 508
drwxr-xr-x    2 celwes   caadmin      4096 Dec 27 01:15 .
drwx------   13 celwes   caadmin      4096 Dec 27 01:14 ..
-rwxr-xr-x    1 celwes   caadmin    503516 Dec 27 01:14 cis-linux.tar.gz
-rwxr-xr-x    1 celwes   caadmin        51 Dec 27 01:14 cis-linux.tgz.md5
[celwes@rootca CIS]$ md5sum cis-linux.tar.gz
624304dcfcfd238723d40606209f502c  cis-linux.tar.gz
```

[28] From the website: URL: http://www.cisecurity.org/bench.html.

```
[celwes@rootca CIS]$ cat cis-linux.tgz.md5
624304dcfcfd238723d40606209f502c  cis-linux.tar.gz
```

There are several steps to installing the CIS benchmark tool, as shown below. Note that the `sudo` command must be used to install the package (root privileges are required to write to the install directory).

Commands for installing the CIS benchmark tool:

```
gunzip cis-linux.tar.gz
tar xvf cis-linux.tar
cd cis
sudo rpm -i CISscan-1.4.2-1.0.i386.rpm
```

In order to run the tool, use the command "`/usr/local/CIS/cis-scan`" (this will be done later on).

Compiling and installing `lsof` takes several steps. First, gunzip and then untar the `lsof.tar.gz` file, and then untar the source file. Next, the configure command needs to be run which will take an "inventory" of the system and then customize the `machine.h` file. While running Configure, answer "y" to the question "Enable HASSECURITY" which prevents anyone from running the command and seeing all open files. Also answer "y" to the "Enable HASNOSOCKSECURITY" question. Answer "n" to the "Disable WARNINGSTATE" question as one would want to see any warning messages generated by lsof. Answer "n" to the "Enable HASKERNIDCK" question as the software is being built on the target system where it will be executed. Answer "y" to the question about renaming the `machine.h` file. Once done, copy `lsof` to the `/sbin` directory (as it is a system binary).

Commands to compile lsof

```
tar xvf lsof.tar.gz
gunzip lsof.tar
tar xvf lsof.tar
cd lsof_4.69
tar xvf lsof_4.69_src.tar
cd lsof_4.69_src
./Configure linux                (answer y,y,n.n,y)
make
sudo cp lsof /sbin
```

Install Netscape CA

Prerequisites

Before Netscape CMS 6.2 is installed, there needs to be a user and a group created. The CMS documentation suggests running as user "nobody", but that user is not particularly self documenting. For this system a normal group and user named "`netscape`" is created using the `groupadd` and `useradd` commands, as shown in the next table.

Create group/user
`groupadd netscape` `useradd -g netscape netscape -c "Netscape Server"`

Netscape Installation Checklist[29]

There are several installation considerations and decisions that need to be made before Netscape CMS is installed. They are documented in the checklist, along with details on how Netscape is installed.

Item	Installation Notes
Create user account	Created an account "netscape"
Install Location	/usr/netscape/servers
Subsystems to install: • Certificate Manager Server & console • Java Classes, Console • Directory Server & Console • Administration Server & Console	Each will be installed (using setup). Since the server will function as a stand alone CA, it will need to be fully functional.
Directory Server LDAP port	The default port of 389 is used.
Computer Name	rootca.university.edu
LDAP Distinguished name for the Directory Manager.	cn=Directory Manager.
Configuration Directory administrator username and password	Use the default of "admin". The password will be set by one of the "administrators".
Administration Server administrator username and password	Since this will not be a custom installation (one that works with an existing Netscape hierarchy), this is not needed.
Directory Suffix	dc=university, dc=edu. As part of the CPS, the formal name must be used to properly identify the site.
Administration port	The setup program will randomly generate the port number during installation. 49267 was the port number generated.
Log file directory:	During installation, the log file directory will be /usr/netscape/servers/cert_rootca/logs.

Remove Unnecessary Accounts and Groups

There are several accounts on the system which are not needed. On a Root CA the only accounts that should be active are authorized accounts. Here, "active" means that

[29] This list of tasks is derived from Chapter 2, "Installation", of the Netscape Certificate Management System Administration Guide, p. 70 - 84.

either a process or a user can login with the account. The original password file is copied in order to preserve the User ID field (a number that matches an account name) because there may be files which were owned by an account that will be deleted.

In order to get an idea of what account correlates with what service, review the `/usr/share/doc/setup-2.5.27/uidgid` file[30]. This file shows the User ID (UID), Group ID, (GID), home directory, shell, and packages that are associated with the system account.

Once these tasks are done (add netscape user and approved users), groups that are not necessary on the system need to be removed. For instance, the "gopher" user is associated with the "gopher" service (not installed on this system, and hasn't had widespread use over recent years).

The following script can be used to preserve and then delete accounts:

Script to delete unnecessary accounts and groups

```
#!/bin/sh
cp /etc/passwd ~/initial_password_file
cp /etc/group ~/initial_group_file
for usr in adm shutdown halt news uucp operator games gopher ftp xfs ntp rpc gdm
rpcuser ncsd pcap apache
do
    /usr/sbin/userdel $usr
done
for grp in adm news uucp games dip users lock nfsnobody
do
    /usr/sbin/groupdel $grp
done
```

For the remaining accounts on the system, the password field in the `/etc/shadow` file needs to be changed to "!!" which will prevent these system accounts from logging in (file below). Here, by setting the password field to "!!" means that we are documenting the fact that there is no password - this option doesn't mean "No Password" to the system; rather, it locks the account[31]. Because these characters are an improper md5 hash, no password can actually match the field, so a user can't falsely login. When you edit the `/etc/shadow` file be careful not to change the order of the lines. In the shadow file example below, five users and root have passwords properly assigned to them.

`/etc/shadow` file with locked users:[32]

```
root:$1$XMKs.lK4$0g6Y9Kq6laEkAQrghh1eo/:12418:0:99999:7:::
bin:!!:12405:0:99999:7:::
daemon:!!:12405:0:99999:7:::
```

[30] This detail was provided by RedHat Technical support via a support request.
[31] The use of "!!" isn't in the useradd(8) or shadow(5) man pages; rather, it is in the RedHat knowledge base, article titled "How does the useradd command work on a system that has shadow passwords enabled?".
[32] Note that the MD5 hashes were altered - these are not real MD5 hashes from a production system.

/etc/shadow file with locked users:[32]

```
lp:!!:12405:0:99999:7:::
sync:!!:12405:0:99999:7:::
mail:!!:12405:0:99999:7:::
nobody:!!:12405:0:99999:7:::
mailnull:!!:12405:0:99999:7:::
rpm:!!:12405:0:99999:7:::
pvm:!!:12405:0:99999:7:::
nscd:!!:12405:0:99999:7:::
ident:!!:12405:0:99999:7:::
netdump:!!:12405:0:99999:7:::
mysql:!!:12405:0:99999:7:::
dmurdoch:$1$éòÕËSreû$1tlIrRiB2rcyPggCwR8FD/:12405:0:99999:7:::
netscape:!!:12408:0:99999:7:::
celwes:$1$vSg371iB$fk1Xp.9tbwThu1phwpC7m/:12410:0:99999:7:::
mpatink:!!:12410:0:99999:7:::
imontoya:!!:12410:0:99999:7:::
mmax:$1$Wyukjc1B$V2OdXTmQRuirJvWFV5V37/:12410:0:99999:7:::
bcrystal:$1$EQsMBizh$NKX.123MSM3x0rkysrTig0:12410:0:99999:7:::
wshawn:!!:12410:0:99999:7:::
csarando:!!:12410:0:99999:7:::
rwright:$1$oNiFZ57T$ScDZpPabcQlbxUpG3zlQUcG/:12410:0:99999:7:::
```

Disable Unnecessary Services

There are a variety of processes and services running on the system which are not necessary for a Root CA to function properly. Removing unnecessary services does two things - it prevents an avenue of possible compromise and it helps to insure that the server is running only what it needs to be running. At a command prompt, not running under X11/Gnone (from a straight non-graphical login!), run the command "`ps -aux > init_processes`". This command will get a process table and will write it to the file "init_prcesses" - documenting the initial set of processes on the system after Netscape CMS is installed.

Output of the ps -aux command:

```
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.2   1416   472 ?        S    04:26   0:04 init
root         2  0.0  0.0      0     0 ?        SW   04:26   0:00 [keventd]
root         3  0.0  0.0      0     0 ?        SW   04:26   0:00 [kapm-idled]
root         4  0.0  0.0      0     0 ?        SWN  04:26   0:00 [ksoftirqd_CPU0]
root         5  0.0  0.0      0     0 ?        SW   04:26   0:01 [kswapd]
root         6  0.0  0.0      0     0 ?        SW   04:26   0:00 [kreclaimd]
root         7  0.0  0.0      0     0 ?        SW   04:26   0:00 [bdflush]
root         8  0.0  0.0      0     0 ?        SW   04:26   0:00 [kupdated]
root         9  0.0  0.0      0     0 ?        SW   04:26   0:00 [mdrecoveryd]
root        17  0.0  0.0      0     0 ?        SW   04:26   0:00 [kjournald]
root        95  0.0  0.0      0     0 ?        SW   04:26   0:00 [khubd]
root       192  0.0  0.0      0     0 ?        SW   04:26   0:00 [kjournald]
root       193  0.0  0.0      0     0 ?        SW   04:26   0:00 [kjournald]
root       194  0.0  0.0      0     0 ?        SW   04:26   0:00 [kjournald]
root       195  0.0  0.0      0     0 ?        SW   04:26   0:00 [kjournald]
root       196  0.0  0.0      0     0 ?        SW   04:26   0:00 [kjournald]
root       667  0.0  0.2   1476   532 ?        S    04:27   0:00 syslogd -m 0
root       672  0.0  0.2   2072   444 ?        S    04:27   0:00 klogd -2
rpc        692  0.0  0.2   1568   492 ?        S    04:27   0:00 portmap
rpcuser    720  0.0  0.3   1612   652 ?        S    04:27   0:00 rpc.statd
root       833  0.0  0.2   1400   452 ?        S    04:27   0:00 /usr/sbin/apmd -p
root       905  0.0  0.5   2676  1064 ?        S    04:27   0:00 /usr/sbin/sshd
root       938  0.0  0.4   2280   840 ?        S    04:27   0:00 xinetd -stayalive
root       979  0.0  0.8   5448  1580 ?        S    04:27   0:00 sendmail: accepti
root      1007  0.0  0.0      0     0 ?        SW   04:27   0:00 [scsi_eh_1]
```

Output of the ps -aux command:

```
root       1026  0.0  0.2  1444  468 ?        S    04:27   0:00 gpm -t imps2 -m /
bin        1045  0.0  0.3  1944  620 ?        S    04:27   0:00 cannaserver -sysl
root       1063  0.0  0.3  1596  604 ?        S    04:27   0:00 crond
xfs        1111  0.0  0.4  4512  940 ?        S    04:27   0:00 xfs -droppriv -da
daemon     1147  0.0  0.2  1452  492 ?        S    04:27   0:00 /usr/sbin/atd
root       1157  0.0  0.1  1388  380 tty2     S    04:27   0:00 /sbin/mingetty tt
root       1158  0.0  0.1  1388  380 tty3     S    04:27   0:00 /sbin/mingetty tt
root       1159  0.0  0.1  1388  380 tty4     S    04:27   0:00 /sbin/mingetty tt
root       1160  0.0  0.1  1388  380 tty5     S    04:27   0:00 /sbin/mingetty tt
root       1161  0.0  0.1  1388  380 tty6     S    04:27   0:00 /sbin/mingetty tt
root       2035  0.0  0.5  2560  960 ?        S    08:47   0:00 ./uxwdog -d /usr/
root       2036  0.0  3.7 14984 7148 ?        S    08:47   0:01 ns-httpd -d /usr/
root       2038  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2040  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2041  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2042  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2043  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2043  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2044  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2046  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2047  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2048  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2049  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2050  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2051  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2052  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2053  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2054  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2055  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2056  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2057  0.0 14.5 349956 27668 ?      S    08:47   0:01 ns-httpd -d /usr/
root       2058  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2059  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2060  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2061  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2062  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2063  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2064  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2065  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2066  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2066  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2067  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2068  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2069  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2070  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2071  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2072  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2073  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2074  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2075  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2076  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2077  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2078  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2079  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2080  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2081  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2082  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2083  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2084  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2085  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2086  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2087  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2088  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2088  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2089  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2090  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
root       2091  0.0 14.5 349956 27668 ?      S    08:47   0:00 ns-httpd -d /usr/
```

Output of the ps -aux command:

```
root      2092  0.0 14.5 349956 27668 ?        S    08:47   0:00 ns-httpd -d /usr/
root      2093  0.0 14.5 349956 27668 ?        S    08:47   0:00 ns-httpd -d /usr/
root      2094  0.0 14.5 349956 27668 ?        S    08:47   0:00 ns-httpd -d /usr/
root      2095  0.0 14.5 349956 27668 ?        S    08:47   0:00 ns-httpd -d /usr/
root      2096  0.0 14.5 349956 27668 ?        S    08:47   0:00 ns-httpd -d /usr/
root      2097  0.0 14.5 349956 27668 ?        S    08:47   0:00 ns-httpd -d /usr/
root      2098  0.0 14.5 349956 27668 ?        S    08:47   0:00 ns-httpd -d /usr/
root      2099  0.0 14.5 349956 27668 ?        S    08:47   0:00 ns-httpd -d /usr/
root      2100  0.0 14.5 349956 27668 ?        S    08:47   0:00 ns-httpd -d /usr/
root      2101  0.0 14.5 349956 27668 ?        S    08:47   0:00 ns-httpd -d /usr/
root      2102  0.0 14.5 349956 27668 ?        S    08:47   0:00 ns-httpd -d /usr/
root      2103  0.0 14.5 349956 27668 ?        S    08:47   0:00 ns-httpd -d /usr/
root      2104  0.0 14.5 349956 27668 ?        S    08:47   0:00 ns-httpd -d /usr/
root      2105  0.0 14.5 349956 27668 ?        S    08:47   0:00 ns-httpd -d /usr/
root      2106  0.0 14.5 349956 27668 ?        S    08:47   0:00 ns-httpd -d /usr/
root      2107  0.0 14.5 349956 27668 ?        S    08:47   0:00 ns-httpd -d /usr/
root      2108  0.0 14.5 349956 27668 ?        S    08:47   0:00 ns-httpd -d /usr/
root      2113  0.0 14.5 349956 27668 ?        S    08:48   0:00 ns-httpd -d /usr/
root      2236  0.0  1.1  3896 2204 ?         S    09:40   0:00 oafd --ac-activat
root      2241  0.0  0.5  2340 1080 ?         S    09:40   0:00 login -- root
root      2242  0.0  0.6  2452 1268 tty1      S    09:41   0:00 -bash
root      2298  0.0  0.5  3012 1020 tty1      R    09:46   0:00 ps -aux
```

As can be seen from the listing there are several processes that do not need to be running. There are two steps in disabling unnecessary services. First, the service must be stopped. Second, the `chkconfig` command must be run so that it disables the service from starting. `chkconfig` manages the symbolic links in the various `/etc/rc[0-6].d` directories. When the system boots it checks the run level from the `/etc/initab` file, and runs all of the scripts associated with the run level and lower[33]. With the process list in hand, the various scripts in `/etc/init.d` need to be reviewed. In other words, use the process list in conjunction with the system init files to determine what should be "turned off".

These services can safely be disabled on the system:

- `apmd`: The "Advanced Power Management Daemon"[34] (process ID 833).
- `atd`: This service can be disabled as it is for "running jobs queued for later execution" (process ID 1147).
- `autofs`: This is the "control script for the automounter". According to the online Linux manual, automount will "automatically mount file systems with the base mount-point when they are accessed in any way". The Root CA will not be mounting directories across the network, so this service is not needed[35].
- `cannaserver`: This server is run from the 'canna' script (process ID 1045). The script says it is "Canna Japanese Conversion Engine". This type of service is not needed on a Root CA.

[33] This description comes from the chkconfig man page.
[34] apmd is described in the apmd man page.
[35] This information comes from the automount and the autofs man pages.

- `gpm`: This is "a cut and paste utility and mouse server for virtual consoles"[36] (process ID 1026) and, since on this system a user should only be logging to one tty (the real console), this service can be disabled.
- `kudzu`: This is the hardware configuration tool - it detects changes and updates the system at boot time. Since a change in the hardware is not likely on the system, this service isn't needed.
- `ip6tables`: This service is the "IPV6 packet filter administration" (firewall) service[37]. This system will not connect to a production network using IP V6; this service is not needed.
- `netfs`: According to the startup script, this script "Mounts and unmounts all Network File System (NFS), SMB (LAN Manager/Windows), and NCP (NetWare) mount points"[38]. Therefore, since the Root CA will not connect to network file shares, this service can be disabled.
- `nfslock`: According to the startup script, this script "NFS is a popular protocol for file sharing across TCP/IP networks. This service provides NFS file locking functionality"[39]. Therefore, since the Root CA will not connect to network file shares, this service can be disabled.
- `pcmcia`: There are no PCMCIA cards in the system, so this is not needed.
- `portmap`: RPC connections are managed by the portmap service (process ID 692). Since there are not supposed to be network services offered over the network, this service should be disabled.
- `inetd/xinetd`: These services respond to TCP/IP connections and direct the traffic to the proper process, often invoking the processes as needed. Since a Root CA won't be connected to a network and won't be responding to dynamic requests, these services are not needed. Further, Netscape CMS (the primary application on the system) can't be configured to run under inetd/xinetd.
- `rhnsd`: The RedHat network is a service offered by RedHat to allow users to better manage and update their system, or more specifically `rhnsd` is "a program for quering the Red Hat Network for updates and information."[40]. A Root CA is offline, and a connection to the Internet - no matter how well managed - opens up the possibility for attack. Updates will be performed by hand on this system.
- `sshd`: This is the "OpenSSH Secure Shell Daemon"[41] (process id 905). Since there are not supposed to be interactive logins over the network, this service should be disabled.

In order to disable these services, the following script can be used[42]:

[36] According to the gpm man page.
[37] According to the ip6tables man page.
[38] From the /etc/init.d/netfs script on the system.
[39] From the /etc/init/d/nfslock script on the system.
[40] From the rhnsd man page.
[41] OpenSSH is described in the sshd man page.

Script to disable services:

```
#!/bin/sh

for service in apmd portmap sshd canna atd gpm kudzu sendmail netfs pcmcia xfs nfslock
rhnsd ip6tables autofs xinetd
do
        /etc/init.d/$service stop
        /sbin/chkconfig --level 12345 $service off
done
```

Services Disable script output

```
Shutting down APM daemon:                                  [  OK  ]
Stopping portmapper:                                       [  OK  ]
Stopping sshd:                                             [  OK  ]
Stopping cannaserver:                                      [  OK  ]
Stopping atd:                                              [  OK  ]
Shutting down console mouse services:                      [  OK  ]
Shutting down sendmail:                                    [  OK  ]
Shutting down xfs:                                         [  OK  ]
Shutting down NFS file locking services:
Shutting down NFS statd:                                   [  OK  ]
```

Once this script has completed, run the "`chkconfig --list`" command and review the results. There should be very few services running at this point on the system. Also in the process list there are several Netscape threads listed, from process ID 2036 to process ID 2113. These threads are "normal", meaning that the Netscape CMS services startup of dozens of threads to manage certificate requests.

Output of the "chkconfig --list" command:

```
keytable        0:off   1:on    2:on    3:on    4:on    5:on    6:off
atd             0:off   1:off   2:off   3:off   4:off   5:off   6:off
canna           0:off   1:off   2:off   3:off   4:off   5:off   6:off
sendmail        0:off   1:off   2:off   3:off   4:off   5:off   6:off
syslog          0:off   1:off   2:on    3:on    4:on    5:on    6:off
gpm             0:off   1:off   2:off   3:off   4:off   5:off   6:off
microcode_ctl   0:off   1:off   2:off   3:off   4:off   5:off   6:off
kudzu           0:off   1:off   2:off   3:off   4:off   5:off   6:off
netfs           0:off   1:off   2:off   3:off   4:off   5:off   6:off
network         0:off   1:off   2:on    3:on    4:on    5:on    6:off
random          0:off   1:off   2:on    3:on    4:on    5:on    6:off
rawdevices      0:off   1:off   2:off   3:on    4:on    5:on    6:off
pcmcia          0:off   1:off   2:off   3:off   4:off   5:off   6:off
apmd            0:off   1:off   2:off   3:off   4:off   5:off   6:off
ipchains        0:off   1:off   2:on    3:on    4:on    5:on    6:off
iptables        0:off   1:off   2:on    3:on    4:on    5:on    6:off
crond           0:off   1:off   2:on    3:on    4:on    5:on    6:off
anacron         0:off   1:off   2:on    3:on    4:on    5:on    6:off
xinetd          0:off   1:off   2:off   3:off   4:off   5:off   6:off
lpd             0:off   1:off   2:on    3:on    4:on    5:on    6:off
xfs             0:off   1:off   2:off   3:off   4:off   5:off   6:off
ntpd            0:off   1:off   2:off   3:off   4:off   5:off   6:off
portmap         0:off   1:off   2:off   3:off   4:off   5:off   6:off
autofs          0:off   1:off   2:off   3:off   4:off   5:off   6:off
nfs             0:off   1:off   2:off   3:off   4:off   5:off   6:off
nfslock         0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

[42] This script is nearly identical to the script presented in the SANS GCUX curricula, Day 5, "Disabling RedHat Services".

Output of the "chkconfig --list" command:

```
netdump         0:off   1:off   2:off   3:off   4:off   5:off   6:off
identd          0:off   1:off   2:off   3:off   4:off   5:off   6:off
snmpd           0:off   1:off   2:off   3:off   4:off   5:off   6:off
snmptrapd       0:off   1:off   2:off   3:off   4:off   5:off   6:off
netdump-server  0:off   1:off   2:off   3:off   4:off   5:off   6:off
smartd          0:off   1:off   2:off   3:off   4:off   5:off   6:off
rhnsd           0:off   1:off   2:off   3:off   4:off   5:off   6:off
sshd            0:off   1:off   2:off   3:off   4:off   5:off   6:off
httpd           0:off   1:off   2:off   3:off   4:off   5:off   6:off
tux             0:off   1:off   2:off   3:off   4:off   5:off   6:off
ip6tables       0:off   1:off   2:off   3:off   4:off   5:off   6:off
iscsi           0:off   1:off   2:on    3:on    4:off   5:on    6:off
mysqld          0:off   1:off   2:off   3:off   4:off   5:off   6:off
xinetd based services:
        chargen-udp:    off
        chargen:        off
        daytime-udp:    off
        daytime:        off
        echo-udp:       off
        echo:   off
        time-udp:       off
        time:   off
        krb5-telnet:    off
        telnet: off
        sgi_fam:        on
        finger: off
        eklogin:        off
        gssftp: off
        klogin: off
        kshell: off
```

Local Firewall

If a system isn't going to be connected to a network, why install a local firewall? This is a "Defense in Depth" measure, meaning that an extra added layer of security is being added to make a potential compromise that much more difficult.

There are two firewall types that are available to choose from on RHES 2.1 - IPChains and IPTables. IPChains is an older firewall product, and if IPTables is available it is the preferred firewall tool to use. As can be seen from the output of "chkconfig" earlier, both are running on the system. IPChains needs to be disabled and IPTables needs to be set to run on the system. In order to disable IPChains, use the commands below:

```
sudo /etc/init.d/ipchains stop
sudo /sbin/chkconfig --level 12345 ipchains off
```

These commands should produce similar output as shown in the table. Note that the `sudo` command was used, and `celwes` is the system administrator who performed the task.

Output of commands to disable ipchains

```
[celwes@rootca servers]$  sudo /etc/init.d/ipchains stop
Password:
Flushing all chains:                                       [  OK  ]
Removing user defined chains:                              [  OK  ]
Resetting built-in chains to the default ACCEPT policy:    [  OK  ]
[celwes@rootca servers]$ sudo /sbin/chkconfig --level 12345 ipchains off
```

In order to enable IPTables and to build up rule sets that allow the system to communicate only with itself, these commands are used:

```
sudo /sbin/iptables -A INPUT -s 127.0.0.1 -j ACCEPT
sudo /sbin/iptables -A INPUT -s 192.168.1.17 -j ACCEPT
sudo /sbin/iptables -A INPUT -i eth0 -p tcp -j REJECT --reject-with tcp-reset
sudo /sbin/iptables -A INPUT -i eth0 -p udp -j REJECT --reject-with icmp-port-
unreachable
```

The first two IPTables commands tell the kernel's packet filtering system to accept packets that come from the system itself. The localhsot address is 127.0.0.1, and the actual local IP address is 192.168.1.17. The second two rules tell the system to reject any TCP or UDP data. Since there is an "accept" rule before a "reject" rule, the system effectively communicates with itself. The firewall's configuration can (and should) be verified as shown below (and will be further verified by using nmap later in this document).

Commands to verify the iptables firewall:

```
[celwes@rootca celwes]$ sudo /sbin/iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  localhost.localdomain  anywhere
ACCEPT     all  --  rootca.university.edu  anywhere
REJECT     tcp  --  anywhere              anywhere           reject-with tcp-reset
REJECT     udp  --  anywhere              anywhere           reject-with icmp-port-
unreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

After the table configuration is reviewed, it must be saved to the default IPTables configuration file. The system administrator should make a copy of the configuration in the process - the two commands below accomplish this, and properly log (to the sudo log), this administrative action.

```
sudo /sbin/iptables-save > ~/iptables
sudo cp ~/iptables /etc/sysconfig/iptables
```

As an added measure of security, the `/etc/ethers` file will be updated to include the hardware addresses of the system. This file controls the arp[43] database. Use the `/sbin/ifconfig` command to get the hardware address, and put it into the ethers file. This task mitigates the possibility of an attacker pretending to be the system (assuming

[43] ARP: Address Resolution Protocol. ARP is used to let a system ask the question "What is the hardware address of IP address X.X.X.X?", and get a MAC (Media Access Control) address from the system with the corresponding IP.

that physical security was violated) and spoofing the IP of the system, bypassing IPTables (only one Ethernet interface is configured).

```
/sbin/ifconfig | grep HWaddr
```

Example `/etc/ethers` file (a single line)

```
00:50:56:40:65:83 192.168.1.17
```

Once these tasks are completed, test the system by rebooting and then using nmap. See the Network Accessibility section under Configuration Checks for details on how to do this.

Perform a Preliminary CIS Scan

By default as delivered from the Center for Internet Security (CIS, at www.cisecurity.org), the CIS benchmark tool will not run for RHES Linux version 2.1. Three changes need to be made to the distribution. First, three of the configuration files need to be copied over from a source version for Linux to a destination that will match. Since RHES 2.1 is closest to RH 7.2[44], copies of the scripts can be made as shown in the commands below.

```
[celwes@rootca CIS]$ sudo cp cis_ruler_suid_programs_redhat_7.2
cis_ruler_suid_programs_redhat_2.1
 [celwes@rootca CIS]$ sudo cp cis_ruler_sgid_programs_redhat_7.2
cis_ruler_sgid_programs_redhat_2.1
[celwes@rootca CIS]$ sudo cp cis_ruler_world_writable_files_redht_7.2
cis_ruler_world_writable_files_redhat_2.1
```

After there are configuration files for the benchmark, the script needs to be modified at about line 232. An additional test needs to be added for RHES 2.1. Example code is shown below for reference.

Excerpt from /usr/local/CIS/tester.sub.

```
    elsif ($release_line =~ /^Red Hat Linux Advanced Server release (\d+\.\w+)\s+/) {
       $DISTRIBUTION = "RH";
       $DISTRIBUTION_VERSION = $1;
    }
# added line for RHES below:
    elsif ($release_line =~ /^Red Hat Enterprise Linux ES release (\d+\.\w+)\s+/) {
       $DISTRIBUTION = "RH";
       $DISTRIBUTION_VERSION = $1;
    }
    elsif ($release_line =~ /^Linux Mandrake release (\d\.\d)/) {
       $DISTRIBUTION = "MD";
       $DISTRIBUTION_VERSION = $1;
    }
```

Run the command: "`/usr/local/CIS/cis-scan`". The output of the command instructs that the system administrator review the file "`cis-ruler-log.20031231-14:22:34.1267`",

[44] This fact was confirmed with RedHat Technical Support.

which is the output from this particular run (your file time suffix will be different; output is in Appendix C).

Log Rollover

The default log rollover in RedHat Linux will not suffice, as the HEBCA audit requirements state that log information must be maintained for the life of the CA. To that end, the default log handling scripts need to be disabled on the system. By default, the RedHat logrotate package will rotate logs weekly and only keep four (4) weeks worth of logs. In order to fully disable the logrotate function without removing the package, use the commands:

```
sudo mv /etc/cron.daily/logrotate ~/initial
sudo mv /etc/logrotate.conf ~/initial
```

One might ask the question, "Why not delete the logrotate package?". the command session below explains that removing the logrotate package would break a dependency on the sysklog package.

Commands verifying that logrotate should not be removed:

```
[celwes@rootca celwes]$ rpm -qa | grep logro
logrotate-3.5.9-1
[celwes@rootca celwes]$ sudo rpm -e logrotate
Password:
error: removing these packages would break dependencies:
        logrotate >= 3.5.2 is needed by sysklogd-1.4.1-4
```

These commands will move the default log roll over script into the SA's directory where original RedHat scripts and configuration data are being kept. Other cron based scripts won't be affected. Below is a replacement `logrotate` script that keeps all log files in an "archive" directory, organized by year/month and then by date. The comments in the script explain how it functions. Copy this script into `/etc/cron.daily` and name it `loghandler` - this name is deliberate, as this script should not be confused with `logrotate`. Make sure to monitor the system for a few days so that it is functioning properly.

Replacement logrotate script[45]

```
#!/bin/sh

# on this system, the log directory is '/var/log'
#
cd /var/log

# get the year/month date combo (2003.12)
# and then the year/month/day combo (2003.12.30)
DIRDATE=`date +%Y.%m`
```

[45] Note: This script isn't my own creation - it was originally written by David Dandar, GCIH and I modified it for this practical.

Replacement logrotate script[45]

```
DAYDATE=`date +%Y.%m.%d`

# this is the list of log files that are either a) in the directory
# by default or b) may appear over time (don't want to miss something later)

# The beginning set of files match the syslog configuration.
#

FILES="1debug 2info 3notice 4warning 5error 6critical 7alert 8panic \
cron lastlog maillog rzlog secure szlog kernel rpmklogs sudolog messages \
ftmp xferlog local0 local1 local2 local3 local4 local5 local6 local7"

# create the log target directory for archival purposes
OLD=/var/log/archive/${DIRDATE}
mkdir $OLD

# Note: this should keep the file descriptors that syslog is using intact --
# it doesn't destroy them - syslog will write to the "hold" files while
# they are open

for lfile in $FILES
do
    if [ -e $lfile ] ; then
      mv $lfile ${lfile}.hold
      touch $lfile
    fi
done

# the kill command tells syslogd to reinitialize itself by closing / opening
# log files and rereading the configuration file
kill -SIGHUP `cat /var/run/syslogd.pid`

echo "Compressing..."
for lfile in $FILES
do
   if [ -e ${lfile}.hold ]; then
      nice gzip -9vc ${lfile}.hold >> ${OLD}/${DAYDATE}.${lfile}.gz && rm
${lfile}.hold
   fi
done
```

File Integrity with Tripwire[46]

Once the base system is initially hardened and the primary application is installed, the next major task is to install the file integrity tool, Tripwire. Tripwire is a good, well respected tool that is designed to check and report on the overall integrity of the files on the system. Tripwire performs a mathematical analysis on files as well as their directory attributes (time, ownership, permissions, I-Node, etc) and will alert if files

[46] These instructions follow the discussion on using Tripwire in the SANS GIAC Certification: Security Essentials Toolkit (GSEC), pp. 66 to 73 very closely.

and/or attributes change. The command "`rpm -qa | grep trip`" confirms that `tripwire-2.3.1-5` is installed on the system. There are several steps in installing and configuring Tripwire are outlined next.

Step One: Run the configuration script. Use the command below - note that it uses "sudo" - actions will be properly logged.

```
sudo /etc/tripwire/twinstall.sh
```

This script will prompt for two key pieces of information as outlined in the table:

Tripwire Install Information	Example (not used on the system)
Site keyfile pass phrase:	"RootCA site"
Local keyfile pass phrase:	"Root CA local"

Step Two: Install the policy file. By installing the policy file, Tripwire will understand what to check on the system by building an encrypted file from the plain text file. Use the command below - note that it uses "sudo".

```
sudo /usr/sbin/twadmin -m P /etc/tripwire/twpol.txt
```

Step Three: Create the initial checksum database (this process may take a while). The checksum database provides the repository of file integrity information.

```
sudo /usr/sbin/tripwire -m i
```

Step Four: Adjust the policy file. First, create a list of files to delete and in a second window open the "`files_to_delete`" file in an editor. Next, open the "`twpol.txt`" and edit out the files listed in delete file list.

```
sudo /usr/sbin/tripwire -m c | grep Filename > files_to_delete
vi /etc/tripwire/twpol.txt
```

In the twpol.txt file, change the "HOSTNAME" to "rootca.university.edu". Next, put a # sign in front of the "/var/lock" files, and every file listed in the delete files.

Step Five: Tripwire doesn't know about Netscape CMS. The perl script below can be used to generate a function that can be added to the Tripwire configuration file. This script builds a list of files in the directory, and ignores several files and directories that don't need to be analyzed. Netscape has about 6,000 files in its installation - this script generates about 3,600 file entries that Tripwire will examine.

Perl script to generate Tripwire rule section.

```
#!/usr/bin/perl
use File::Find;
```

Perl script to generate Tripwire rule section.

```
print '
# Netscape Files

(
  rulename = "Netscape Files",
  severity = $(SIG_HI)
)
{
';

find sub {
    #print $File::Find::name, -d && '/', "\n"
# }, @ARGV;
    $f = $File::Find::name;

    next if ( -d );
    next if ( $f =~ /\.gif$/ );                 # image files for web site
    next if ( $f =~ /\.txt$/ );                 # doc's
    next if ( $f =~ /\.icon$/ );                # image files for web sites
    next if ( $f =~ /\/examples\// );           # source code and script examples
    next if ( $f =~ /\/manual\// );             # directories with PDF's, HTML
    next if ( $f =~ /\/graphics\// );           # whole directories of graphics
    next if ( $f =~ /\/include\// );            # sample source code C header files
    next if ( $f =~ /\/javadocs\// );           # from the Java Runtime
    next if ( $f =~ /\/man\/man\//);            # man pages

# log files are constantly changing - the type of tripwire
# checking is different
    if ( $f =~ "\/cert-rootca\/logs" ) {
        print "\t" . $f . "\t" . '-> $(SEC_LOG) ;' . "\n";
    } else {
        print "\t" . $f . "\t" . '-> $(SEC_BIN) ;' . "\n";
    }
}, "/usr/netscape/servers" ;
print "}\n";
```

In order to run this script, use the command:

```
sudo ./netscape_tw.pl > ~/tw_ns.out
```

Once executed, edit the `twpol.txt` file, navigate almost to the end and right above the last comment block add the output of the script to the policy file[47].

Establish a new Tripwire policy file with the command:

```
sudo /usr/sbin/twadmin --update-policy twpol.txt
```

Step Six: Test the installation of Tripwire by modifying some of the files that Tripwire is monitoring.

```
sudo chattr -i /etc/passwd
sudo touch /usr/netscape/servers/start-admin
sudo /usr/sbin/tripwire -m c > ~/twreport.txt
```

[47] If you are using this guide in order to configure your system and don't know how to do this, the Emacs "Control - x i" command is suggested.

Review the `twreport.txt` file and make sure that Tripwire detected changes to these two files. A sample of the twreport.txt file is shown below for reference.

When finished with the `twpol.txt` file, delete it. Plain text descriptions of files that Tripwire is configured to monitor should not be left on the system

Part of the Tripwire report:

```
--------------------------------------------------------------------------------
Rule Name: Netscape Files (/usr/netscape/servers/start-admin)
Severity Level: 100
--------------------------------------------------------------------------------

Modified:
"/usr/netscape/servers/start-admin"
```

Step Seven: There are instructions under the section titled "System Backups" on making an ISO image, and putting that ISO onto a CD. The Tripwire database, which is located in /var/lib/tripwire, should be copied to a CD-R (or CD-RW) using multiple sub directories - one per date - so that there can be a history of when Tripwire was updated.

Establish Baseline

Once the operating system is installed, hardened, and Netscape is installed, a set of data needs to be collected in order to establish an auditable baseline. In other words, the system needs to be examined to see what it should be running and what resources are in use so that its state can be assessed during the normal audit process. Several commands are executed on the system with their results recorded and preserved so that system integrity can be checked during the normal audit cycle. Below is a list of commands with explanations of what task they perform and why they are relevant to the system state audit process. As a caveat, these commands need to be executed in a non X11 login window session - the GUI will generate extra information that will change from time to time.

Command	Explanation
`netstat -anp48 > netstat_anp_baseline`	This command shows network connections. -a: -n: Shows numerical IP address output (not names) -p: Shows the Process ID and name of the program for each socket.
`ps -aux49 > ps_aux_baseline`	This is one of two process lists. The first list is more abridged and easier to read.

[48] The details in the explanation section come from the netstat man page.

Command	Explanation
`ps -auxeww > ps_auxeww_baseline`	This is the second of two process lists. This list contains a higher degree of detail,
`lsof -i > lsof_i_baseline`	This command will show all processes who are listening of all Internet and X.25 network files.
`lsof -d rtd > lsof_d_baseline`	This command is normally used with a list of file descriptors - here, it shows basic file descriptor information for processes who have files open from the root (/) directory (this should only be trusted system processes).
`nmap -sT -O localhost > nmap_localhost_baseline`	This command will show what ports are open on the local system that are listening for a TCP connection.
`rpm -Va > rpm_va_baseline`	This command validates all of the installed RPM's in the RPM database.

Server Platform Hardening

Once the operating system has been hardened, the next step is to harden the server itself. There are several actions which are necessary to harden the server platform. These steps are designed to prevent accidental power up as well as detecting if the system was compromised at the physical level during its "normal down time".
Enable a system password:[50] In order to access the Dell Server BIOS screen, press F2 when the system starts. In the "System Security" screen, check the "Password Status" field to make sure that it says "Unlocked". Next, the system password can be set. Once the password is entered twice, properly, the "System Password" setting will change to say "Enabled".

At this point the hardware based system password must be entered when the system boots.

Ongoing Maintenance

There are several aspects to maintaining the Root CA over its life cycle. This system will be relatively static, meaning that its basic configuration of a current operating system and a supported version of Netscape CMS will need to be maintained. To that end, several tasks must be performed. These include:

[49] The details in the explanation section come from the ps man page.
[50] These instructions are based on the the Dell Server Users Guide, which can be downloaded from: http://premiersupport.dell.com/docs/systems/pe650/en/index.htm.

- Effective change control and appropriate updates
- System and Netscape CMS backups which support the CPS
- Audits which conform to the CPS and the HEBCA
- System validation that its integrity has been maintained which includes physical security maintenance
- Certificate issuance in accordance with the CPS

Effective Change Control and Appropriate Updates

Over time, vendors will require that the software and hardware must be updated over time. Recently, a new practice in the software industry has started, called "End Of Life" announcements. This practice occurs when a manufacturer makes a declaration that they will no longer support a particular operating system or product, usually with quite a bit of notice. In order to keep informed about vendor change control practices, the four primary components in this system will be under annual vendor maintenance (paid support). This does have an ongoing financial cost, but that cost is offset by the benefit of paid technical support. Staff who is involved in system administration (people with the four roles previously defined) will keep informed about changes from the primary vendors (RedHat, Dell, Netscape, and nCipher) by subscribing to mailing lists for the products installed (each vendor has a list service). Further, RedHat has a quarterly CD update program for the operating system - this will help insure that updates are applied as necessary.

Next, a policy needs to be established on what updates to perform. As above, the kernel on the system cannot be updated (as of Jan 2004). The specific version of the installed kernel is required for Netscape CMS. Since this is the primary application on the system, updates must be made based on the requirements of this application. Therefore, the policy in supporting the system is that changes will be made in accordance with Netscape CMS requirements - updates to the operating system and platform shall not jeopardize functioning of the Root CA.

When a change is suggested, these procedures will be followed:

1. Staff will consult with Netscape to see if the update has specific operating system configuration, version, or package. Continue if there are no contraindications.
2. Staff will consult with nCipher to see if the update has specific operating system configuration, version, or package. Continue if there are no contraindications.
3. A backup of the system will be made using a local tape drive.
4. The update will be applied.
5. The system will be reviewed to make sure that it is still functioning by a reboot, login, open up the various Netscape consoles and make sure that information is still visible.
6. The change process will be logged in the change control log.

System Backups

For the majority of its life, the Root CAis powered off. Therefore, it does not normally perform backups according to traditional schedules (incremental backups at night, full backup over the weekend) .System backups occur on at least a monthly basis for Netscape - meaning that its directory, logs, and certificate database must be backed up to reliable media monthly (as outlined in Section 4.6, Records Archival, in Appendix A). Because of the time mandates for records retention (10 1/2 years at the Medium level, and 20 1/2 years at High) backups of the Netscape CMS database will be done to CD or DVD media (650MB to 4.3 GB of data) as needed or on a monthly basis, which ever comes first.

The commands to create a CD of image of the Netscape directory are explained next[51].

Step One: Create a tar archive of the `/usr/netscape/servers` directory.

```
cd /usr/netscape/servers
tar cvzf ~/cms20031229.tar.gz ./*
```

Note: If this archive is unpacked, be sure to use the -p option of the tar command to preserve permissions.

Explanation: These commands change directory to the Netscape directory. Then a compressed tar archive is created in the users HOME directory, named "cms20031229.tar.gz". The files that are backed up in the archive are location relative - meaning that they begin with "./", so they may be restored as needed without having to be restored to the original path.

Step Two: Create an ISO image of the tar file.

```
cd ~
mkisofs -r -N -l -allow-lowercase -iso-level 3 -relaxed-filenames -no-iso-translate -A
"CMS20031229" -V "NetscapeCMS" -P "Rootca.University.edu" -p "C. Elwes" -o
~/cms20031229.iso cms20031229.tar.gz
```

These command line options mean[52]:

- -r: This option sets the UID and GID of the files in the ISO image to 0.
- -N: Omit the file version numbers in the ISO image.
- -l: allow for file names that are 31 characters long (many of the files in the Netscape directory are longer than 11 characters).
- -allow-lowercase: Lowercase letters can appear in ISO file names - this is important to the UNIX/Linux system as the majority of files and directories are in lower case.

[51] For further information on CD recording, there are several Linux CD RW howto's on the Internet. One such is from the Linux Documentation Project, at: http://www.tldp.org/HOWTO/CD-Writing-HOWTO.html
[52] These details are taken from the mkisofs man page.

- -iso-level 3: sets the ISO conformance level (3 means that no restrictions apply).
- -relaxed-filenames
- -no-iso-translate
- -A "CMS20031229": specifies the volume ID for the ISO image. Here, the letters "CMS" mean "Certificate Management Server" and "20031229" are the date that the ISO was made.
- -V "NetscapeCMS"
- -P "Rootca.University.edu": Here, the publisher ID field is being used to identify the name of the system.
- -p "C. Elwes": Here, the preparer ID field is used to identify who made the ISO image.
- -o ~/cms20031229.iso: This is the output file name.

Step Three: Test the image by mounting it as a loopback device:

```
mount -t iso9660 -o ro,loop=/dev/loop0 cms20031229.iso /mnt/cdrom
```

Explanation: This command mounts the image file as an ISO (-t iso9660) read only file system on the loopback device (loop=/dev/loop0) onto the /mnt/cdrom mount point.

Step Four: Use the cdrecord program to write the image file to the CD-RW device[53].

```
cdrecord -v dev=0,3,0 cms20031229.iso
```

Explanation: This command will record the ISO image to the SCSI CD RW device located at device 0,3,0 (SCSI bus, SCSI device ID, SCSI logical unit number) with verbose output (-v).

System Audits

As required by the HEBCA document (see Appendix B), various aspects of the system will be audited over time. Auditing (reviewing logfiles) will be done by someone with the "auditor" role. Auditing consists of reviewing the various operating system logs in /var/log for anomolies, errors, sudo access, and reboots. These actions will be checked with the system administrators to make sure that if an action occurred it was warranted. By implementing this two person process (one to check, one to do tasks) the principle of "separation of duties" is followed by the site.

[53] If you are implementing these steps in your own environment and need to determine the target address of your CD recorder, use the command "`cdrecord -scanbus`" to determine device information

Filesystem Integrity Maintenance

Whenever the system is booted, a Tripwire analysis will be done. In the first command listed below, the word "DATE" needs to be the date in YYYYMMDD format when the analysis ran. Whenever an update is applied to the system, Tripwire's file integrity database will be updated.

Analyze: Generally, to analyze the system the following Tripwire command can be used:

```
sudo /usr/sbin/tripwire -m c > ~/DATE.txt
```

Updates: To update, first perform an analysis with the command:

```
sudo /usr/sbin/tripwire -m c
```

From this command, Tripwire will produce an output report file which ill be in `/var/lib/tripwire/report` (by default). This report file needs to be used in the update process with the command (an example -report numbers change over time):

```
sudo /usr/sbin/tripwire -m u   -r /var/lib/tripwire/report/rootca.university.edu-
20031231-153905.twr
```

When the report file is reviewed by searching for the "[x]" symbol and appropriate changes are made to the report, upon quitting the editor Tripwire will prompt for the local pass phrase and update the database file.

Certificate Issuance

Over time the Root CAwill issue certificates to users who have one of the four CA roles, to subordinate CA's, and to cross certified CA's. Netscape CMS has a user interface for reviewing issued CA's. These will be matched with a paper trail of certificate requests - since this is not a general purpose issuing CA but rather a special purpose, tightly controlled CA, there must be a paper trail for certificates that are issued from the system.

Configuration Check

HEBCA CP:

- 2.7 COMPLIANCE AUDIT

Following the requirements set forth in the HEBCA CP, section 2.7, on a monthly basis the system must be audited. To quote from section 2.7.4,

> "2.7.4 Topics Covered by Compliance Audit
> The purpose of a compliance audit shall be to verify that an entity subject to the requirements of this CP, a MOA, or an Institution CP is complying with the requirements of those documents."

Here, the HEBCA states that the system integrity and confidentiality are maintained. An auditor should check several characteristics about the CA and its operation. This section will outline how several of those checks are made at the operating system level - checks within Netscape CMS are not germane to the operating system.

1. The system is not accessible from the network (check by connecting a notebook equipped with scanning tools to the hub).
2. Only authorized users have logged on (review log files).
3. Assess the file system integrity with Tripwire.
4. Assess the system state by reviewing open files list (with lsof), process table (with ps), and network connections (with netstat).
5. Verify login is not possible for root, and is only possible for authorized accounts.
6. Check system time from external source.

Network Accessibility

In order to see if the system can be accessed from the network hub, the security group's incident response laptop will be used to perform an nmap scan against the system. Remove one of the blocker RJ45 connectors and connect a network cable from the laptop. Reconfigure the laptop to use IP address 192.168.1.20/24, so it will be on the same Class C network as the Root CA. Then run nmap using this local command line:

```
sudo nmap -sS -p1-65535 192.168.1.17
```

The output of this command (below) shows that there are only two services running on the system that are actually listening for network connections - the LDAP server on port 389 and the administration server on port 49267.

nmap information

```
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on rootca.university.edu (192.168.1.17):
(The 65533 ports scanned but not shown below are in state: closed)
Port       State       Service
389/tcp    open        ldap
49267/tcp  open        unknown
```

Off network Accessibility: A notebook PC can be plugged into the hub and an analysis performed with nmap in order to determine if the system is listening for network connections on any ports. Below is the same command running from the Security Services notebook PC, plugged into the hub for this test.

nmap information

```
[root@localhost root]# nmap -sS -p1-65535 192.168.1.17

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
```

```
All 65535 scanned ports on  (192.168.1.17) are: closed

Nmap run completed -- 1 IP address (1 host up) scanned in 25 seconds
```

Login Review

Many logs need to be reviewed on the system during the audit cycle. Procedurally, according to the CPS, these tasks are performed by one of the people with the auditor role.

Bad Logins: There are two commands to view bad login records shown below. These commands will show the history of last logged in users:

```
lastb -aidx
lastb
```

Below is the output of these commands. They show that two users had problems logging on Jan 1, in different formats (these records were produced as part of testing and creating configuration checks for the "Configuration Checks" section).

```
Output of lastb -aidx
celews                   Thu Jan  1 10:11 - 10:11  (00:00)     0.0.0.0
celews                   Thu Jan  1 10:10 - 10:10  (00:00)     0.0.0.0
root                     Thu Jan  1 10:02 - 10:02  (00:00)     0.0.0.0
root                     Thu Jan  1 10:02 - 10:02  (00:00)     0.0.0.0
root                     Thu Jan  1 08:27 - 08:27  (00:00)     0.0.0.0
root                     Thu Jan  1 08:27 - 08:27  (00:00)     0.0.0.0
root                     Thu Jan  1 08:27 - 08:27  (00:00)     0.0.0.0
```

```
Output of lastb
celews   tty1                     Thu Jan  1 10:11 - 10:11  (00:00)
celews   tty1                     Thu Jan  1 10:10 - 10:10  (00:00)
root     tty1                     Thu Jan  1 10:02 - 10:02  (00:00)
root     tty1                     Thu Jan  1 10:02 - 10:02  (00:00)
root     tty1                     Thu Jan  1 08:27 - 08:27  (00:00)
root     tty1                     Thu Jan  1 08:27 - 08:27  (00:00)
root     tty1                     Thu Jan  1 08:27 - 08:27  (00:00)
```

Good Logins: The commands to check good login history are nearly identical, as shown next along with a sample of output.

```
last -aidx | more
last | more
```

Below is the output of these commands. They show that the system was rebooted on Jan 1 and that a system administrator was logged in at that time (these records were produced as part of testing and creating configuration checks for the "Configuration Checks" section).

```
Output of last -aidx
celwes                   Tue Jan  6 20:56   still logged in    0.0.0.0
runlevel                 Thu Jan  1 10:01 - 21:29 (5+11:28)    0.0.0.0
reboot                   Thu Jan  1 10:01         (5+11:28)    0.0.0.0
runlevel                 Thu Jan  1 09:59 - 10:01  (00:01)     0.0.0.0
reboot                   Thu Jan  1 09:59         (5+11:30)    0.0.0.0
shutdown                 Thu Jan  1 09:58 - 21:29 (5+11:31)    0.0.0.0
```

```
runlevel             Thu Jan  1 09:58 - 09:58  (00:00)     0.0.0.0
celwes               Thu Jan  1 08:27 - down   (01:30)     0.0.0.0
```

Output of last

```
celwes   tty1                          Thu Jan  1 10:12   still logged in
reboot   system boot  2.4.9-e.12       Thu Jan  1 10:01         (5+11:32)
reboot   system boot  2.4.9-e.12       Thu Jan  1 09:59         (5+11:33)
celwes   tty1                          Thu Jan  1 08:27 - down   (01:30)
```

Log Rotation

The log rotation process needs to be checked in order to see that the `anacron` service is rotating logs on a daily basis. This service doesn't necessarily run at a specific time; rather it monitors the system to make sure that the process is run at least every day (in this case, as the `loghandler` script is in `/etc/cron.daily`).

Supporting details are shown next.

Example archived logs - Jan 6 (in `/var/log/archive/2004.01`)

```
-rw-r--r--    1 root     root         4913 Jan  6 20:58 2004.01.06.cron.gz
-rw-r--r--    1 root     root         8128 Jan  6 20:58 2004.01.06.kernel.gz
-rw-r--r--    1 root     root        18659 Jan  6 20:58 2004.01.06.lastlog.gz
-rw-r--r--    1 root     root        30075 Jan  6 20:58 2004.01.06.lastlog.gz
-rw-r--r--    1 root     root          946 Jan  6 20:58 2004.01.06.maillog.gz
-rw-r--r--    1 root     root         4359 Jan  6 20:58 2004.01.06.secure.gz
-rw-r--r--    1 root     root         3482 Jan  6 20:58 2004.01.06.sudolog.gz
```

These files match the current log files (by name) from the /var/log directory.

Rotated logs - Jan 6 (in `/var/log`)

```
drwxr-xr-x    3 root     root         4096 Jan  6 20:58 archive
-rw-------    1 root     root        13836 Jan  1 10:01 boot.log
-rw-r--r--    1 root     root         2688 Jan  1 10:11 btmp
drwxr-xr-x    2 bin      bin          4096 Nov 11  2002 canna
-rw-r--r--    1 root     root          287 Jan  6 21:20 cron
-rw-r--r--    1 root     root         8063 Jan  1 10:01 dmesg
drwxr-xr-x    2 root     root         4096 Sep  4  2001 gdm
drwxr-xr-x    2 root     root         4096 Oct 23  2002 httpd
-rw-r--r--    1 root     root          340 Jan  1 10:01 iscsi.log
-rw-r--r--    1 root     root            0 Jan  6 20:58 kernel
-rw-r--r--    1 root     root            0 Jan  6 20:58 lastlog
-rw-r--r--    1 root     root            0 Jan  6 20:58 maillog
-rw-------    1 root     root            0 Jan  6 21:22 messages
-rw-r-----    1 mysql    mysql           0 Dec 21 01:33 mysqld.log
-rw-r--r--    1 root     root        13477 Dec 27 04:02 rpmpkgs
drwxr-xr-x    2 root     root         4096 Jan  6 16:40 sa
-rw-r--r--    1 root     root          526 Jan  6 21:22 secure
-rw-------    1 root     root            0 Dec 21 01:33 spooler
-rw-r--r--    1 root     root          494 Jan  6 21:22 sudolog
-rw-------    1 root     root          703 Dec 24 03:14 syslog
-rw-rw-r--    1 root     utmp       172800 Jan  6 20:56 wtmp
```

Sudo Review

What type of commands have staff with sudo permission been running lately? User "bcrystal", a staff member with the "auditor" role, reviews the sudo log history.

Through this process, it is shown that bcrystal attempted the tail command (3,4) - an oversight on the part of the initial sudo configuration. After the attempt to use tail, the system administrator used visudo (7,8) to give the auditor sufficient privilege in order to use this command (11,12) (line numbers added).

```
 1: [bcrystal@rootca log]$ sudo tail sudolog
 2:   COMMAND=/usr/bin/nmap -sS -p1-65535 192.168.1.17
 3: Jan  1 08:47:48 : celwes : TTY=pts/1 ; PWD=/var/log ; USER=root ;
 4:   COMMAND=/usr/bin/tail sudolog
 5: Jan  1 08:49:17 : bcrystal : command not allowed ; TTY=pts/3 ; PWD=/var/log ;
 6:    USER=root ; COMMAND=/usr/bin/tail sydolog
 7: Jan  1 08:50:01 : celwes : TTY=pts/1 ; PWD=/var/log ; USER=root ;
 8:  COMMAND=/usr/sbin/visudo
 9: Jan  1 08:50:42 : bcrystal : TTY=pts/3 ; PWD=/var/log ; USER=root ;
10:    COMMAND=/usr/bin/tail sydolog
11: Jan  1 08:50:53 : bcrystal : TTY=pts/3 ; PWD=/var/log ; USER=root ;
12:    COMMAND=/usr/bin/tail sudolog
```

System Integrity and Tripwire

The tape seals on the system need to be inspected to make sure that the system has maintained physical integrity. Also, the handwritten access log needs to be reviewed on a monthly basis.

As discussed under the "File Integrity with Tripwire" section, there are specific commands that can be run in order to check the system against the Tripwire database. Specifically, the command:

```
sudo /usr/sbin/tripwire -m c > ~/twreport.txt
```

can be used to check and see if there has been an integrity issue with files on the system. Note that a prior Tripwire database can be copied off of CD (as discussed in Step Seven under "File Integrity with Tripwire") and used to check system integrity against a particular point in history.

System State

Over time, the system state will be assessed with commands that are designed to show running processes, disk utilization, open files, and listening services. The output of these commands needs to be checked over time to make sure that proper processes are running and that the system is behaving as expected. Below are commands and sample output that can be used to determine system state, captured from an administrator login session.

The same set of commands discussed under "Establish Baseline" should be executed and their results compared with the baseline results. There will likely be differences in process ID numbers, but by and large the same set of commands should yield nearly identical results. Differences in current state and baseline state warrant some investigation.

Disk utilization also needs to be checked on an ongoing basis. The amount of disk space used will only grow slightly over time - issuing certificates and cross certifying with other CA's takes up hardly any room. In order to see a summary of disk space usage, use the "df" command below.

Command to get summary disk informaiton:

```
[celwes@rootca /]$ sudo df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda5             1.9G  183M  1.6G  10% /
/dev/sda1             106M   22M   79M  22% /boot
/dev/sda6             1.9G  218M  1.6G  12% /home
none                   93M     0   93M   0% /dev/shm
/dev/sda7             980M   17M  913M   2% /tmp
/dev/sda2             3.8G  1.4G  2.2G  39% /usr
/dev/sda3             2.9G   71M  2.6G   3% /var
```

Login Checks

The root user should not be allowed to login. An example test was performed on Jan 1, and the results below demonstrate that a bad logon attempt was made for "root". These records correspond to the Jan 1 logon attempts cited above where "root" tried to login (testing the security measures designed to prevent root login) and then one of the system administrators (celwes) logged in.

Records from the "messages" file:

```
Jan  1 08:27:04 rootca login(pam_unix)[764]: authentication failure; logname=LOGIN
uid=0 euid=0 tty=tty1 ruser= rhost=  user=root
Jan  1 08:27:07 rootca login[764]: FAILED LOGIN 1 FROM (null) FOR root, Authentication
failure
Jan  1 08:27:13 rootca login[764]: FAILED LOGIN 2 FROM (null) FOR root, Authentication
failure
Jan  1 08:27:20 rootca login[764]: FAILED LOGIN 3 FROM (null) FOR root, Authentication
failure
Jan  1 08:27:27 rootca login(pam_unix)[764]: session opened for user celwes by
LOGIN(uid=0)
Jan  1 08:27:27 rootca  -- celwes[764]: LOGIN ON tty1 BY celwes
```

System Time

When the system is powered up its BIOS clock needs to be checked against a different time source in the data center. Practically, a second console on any given system is acceptable - ideally, it would be a console on a Network Time Protocol server, or a stand alone chronometer. The correct time needs to be entered on the system before the operating system boots - time is rather sensitive in the PKI process.

References

SANS GCUX Practical Papers

These papers were of great guidance and practical value in preparing this document. In fact, Scott McGee's paper is a next logical step for the CA, as the basis for his paper is in securing an LDAP server. Netscape CMS ships with a directory server that is slightly newer that the directory server discussed in his paper.

McGee, Scott: "Secure LDAP Server", Aug 24, 2003. URL: http://www.giac.org/practical/GCUX/Scott_McGee_GCUX.pdf (Dec 29, 2003)

Chau, Jackqui: "Hardening a Red Hat Linux Apache Web Server with Snort Installed" (19 Dec 2003). URL: http://www.giac.org/practical/GCUX/Jacqui_Chau_GCUX.pdf (Dec 29, 2003).

Wald, Rickey. "Securing Red Hat Linux 9 as an Apache Web Server, VSFTP Server and MySQL server ", Dec 5, 2003. URL: http://www.giac.org/practical/GCUX/Ricky_Wald_GCUX.pdf (Dec 29, 2003).

Websites and other References

www.nist.gov, National Institute of Standards, URL: http://csrc.nist.gov/pki/fbca/ (Jan 11, 2003).

Adams, Carlisle, Lloyd, Steve. Understanding PKI: Concepts, Standards, and Deployment Considerations, Second Edition. Addison Wesley. Nov 6, 2002. Chapter 12.

Cole, Eric; Newfield, Mathew; Millican, John M. Northcutt, Stephen. SANS GIAC Certification: Security Essentials Toolkit (GSEC). Que Publishing, Indianapolis, March 2002. pp. 66 to 73.

Harris, Shon. CISSP Certification All In One Exam Guide, Second Edition. McGraw Hill Osborne, New York. 2003. Pp. 58 - 59, 68 to 72, 614.

Prosise, Chris; Manda, Kevin; Pepe, Matt. Incident Response Second Edition: Computer Forensics, McGraw Hill Osborne, Ch. 3, 4, 6, 8, 9, and 13. July 2003.

enterprise.netscape.com, Product Documentation for Certificate Management System; (Jun 12, 2003). URL: http://enterprise.netscape.com/docs/cms/index.html (Jan 12, 2004)

enterprise.netscape.com, Product Documentation for Certificate Management System: Chapter 2, Installation, (Jun 12, 2003), URL enterprise.netscape.com, Product Documentation for Certificate Management System, Jan 2004, URL: http://enterprise.netscape.com/docs/cms/62/cert/admin/install.htm#17691 (Jan 12, 2004) (print version, Pp. 70-84)

middleware.internet2.org. Areas of Activity. (Dec 22, 2003) http://middleware.internet2.edu/overview/areas-of-activity.html (Dec 22, 2003)

premiersupport.dell.com. "Dell PowerEdge 650 Systems". Oct 2, 2003. URL: http://premiersupport.dell.com/docs/systems/pe650/en/index.htm (Dec 24, 2003).

SANS Institute, GIAC Certified Incident Handler Curriculum, 2003.

SANS Institute, GIAC Certified Unix Security Administrator, 2003.

www.cisecurity.org. "What are the benchmarks" (2003). URL: khttp://www.cisecurity.org/bench.html (Dec 27, 2003).

www.courtesan.com. Miller, Todd; Jepeway, Chris. " FAQ and Troubleshooting Tips", May 8, 2003.URL: http://www.courtesan.com/sudo/troubleshooting.html and http://www.courtesan.com/sudo/man/sudoers.html (Dec 2 9, 2003)

www.globus.org. "The Globus Alliance" (Dec 22, 2003). URL: http://www.globus.org. (Dec 22, 2003).

Abell, Vic; www-rcd.cc.purdue.edu, LSOF, URL: http://www-rcd.cc.purdue.edu/~abe/ (Jan 12, 2004)

www.redhat.com, Knowledge Base (2003). URL's:

- http://kbase.redhat.com/faq/dml_fetch.pl?CompanyID=842&ContentID=680&FaqID=587&word=/etc/passwd&faq_template=http://kbase.redhat.com/faq/searchfaq.shtm&topic=38&back_refr=http://kbase.redhat.com/faq/&topicname=Red%20Hat%20Linux%209/8.0/7.x&Id=&Instance=&Shared=

www.tldp.org. Trumpier, Winfried. "CD-Writing Howto" (23 July 2000). URL: http://www.tldp.org/HOWTO/CD-Writing-HOWTO.html (Dec 29, 2003).

Appendix A: Complete Package List

This package list is the list of software on the system after updates.

indexhtml-7.2-1
redhat-logos-1.1.3-1
filesystem-2.1.6-2
glibc-2.2.4-31.7
bzip2-libs-1.0.1-4
cracklib-2.7-12
db2-2.4.14-9
dosfstools-2.7-1
eject-2.0.9-2
gdbm-1.8.0-11
hdparm-4.1-2
ksymoops-2.4.1-2
mailx-8.1.1-22
mktemp-1.5-11
parted-1.4.16-8
perl-5.6.1-26.72.4
perl-CPAN-1.59_54-26.72.4
perl-NDBM_File-1.75-26.72.4
pwdb-0.62-1
rsh-0.17-5
shadow-utils-20000902-9.7
newt-0.50.33-1
ntsysv-1.3.5-3
syslinux-1.52-2
db3x-3.2.9-3
libtermcap-2.0.8-28
bzip2-1.0.1-4
hotplug-2001_04_24-11
libstdc2.96-116.7.2
logrotate-3.5.9-1
ncurses-5.2-12
cpio-2.4.2-23
ed-0.2-21
at-3.1.8-23
gawk-3.1.0-3
ash-0.3.7-2
grub-0.90-11
less-358-21
openssl-0.9.6b-28
procps-2.0.7-11
raidtools-1.00.2-1.2
redhat-release-es-2.1ES-7
sed-3.02-10
kbdconfig-1.9.14-1
sysklogd-1.4.1-4
tcsh-6.10-6
dev-3.3-1
mouseconfig-4.23-1
tmpwatch-2.8.1-1
vim-common-6.0-7.15
which-2.12-3
cracklib-dicts-2.7-12
authconfig-4.1.19.2-1
cyrus-sasl-md5-1.5.24-24
gpm-1.19.3-20
passwd-0.68-1.2.1
sendmail-8.11.6-9.72.4
krb5-libs-1.2.2-16
kudzu-0.99.42.3-3
lilo-21.4.4-14
SysVinit-2.78-19
rpm-4.0.4-7x.20
initscripts-6.47.2-1.1
apmd-3.0final-34
iptables-1.2.5-3
libaio-0.3.13-3
pciutils-2.1.8-25
quota-3.01pre9-3
vixie-cron-3.0.1-63
xinetd-2.3.3-1
freetype-2.0.3-7
gmp-3.1.1-4
libpng-1.0.14-0.7x.4
libxslt-1.0.15-2
m4-1.4.1-5
nkf-1.92-6
perl-DateManip-5.39-5
perl-HTML-Tagset-3.03-3
perl-libnet-1.0703-6
perl-Parse-Yapp-1.04-3
perl-URI-1.12-5
perl-XML-Encoding-1.01-2
perl-XML-Parser-2.30-7
perl-libxml-enno-1.02-5
perl-XML-Twig-2.02-2
Omni-foomatic-0.5.0-4
psutils-1.17-13
python-1.5.2-43.72
PyXML-0.6.5-4
ttfonts-ja-1.0-8
ghostscript-6.51-16.2
fortune-mod-1.0-16
libjpeg-6b-16
gdk-pixbuf-0.14.0-0.2.1
tk-8.3.3-65
ttfonts-1.0-4
audiofile-0.2.1-2
esound-0.2.22-5
libmng-1.0.2-1
imlib-1.9.13-3.7.x
libxml-1.8.14-2
ntp-4.1.0b-2.AS21.4
ORBit-0.5.8-4
libglade-0.16-4
pygnome-1.4.1-3
pygnome-libglade-1.4.1-3
tix-8.2.0b1-65
usermode-1.46-1
hwbrowser-0.3.5-2
printconf-gui-0.3.61-4.1
serviceconf-0.6.6-1
libtool-libs-1.4-8
aspell-0.33.7-1
gal-0.8-6
gnome-pim-1.2.0-13
gqview-0.8.1-5
imlib-cfgeditor-1.9.13-3.7.x
gnorpm-0.96-12.7x
gnome-print-0.29-6
libgtop-1.0.12-5
libole2-0.2.3-1
librsvg-1.0.0-7
mozilla-nspr-1.0.1-2.2.1
mozilla-nss-1.0.1-2.2.1
oaf-0.6.5-10
GConf-1.0.4-3
bug-buddy-2.0.6-4
gnome-vfs-extras-0.1.3-1
fam-2.6.4-11
rep-gtk-gnome-0.15-6
gdm-2.2.3.1-20
umb-scheme-3.2-21
xscreensaver-3.33-4
gtkhtml-0.9.2-9
gnome-core-1.4.0.4-39
gnome-utils-1.4.0-4
nautilus-mozilla-1.0.4-46.1
kdelibs-2.2.2-6
kdeartwork-2.2.2-1
kdepim-2.2.2-4
libogg-1.0rc2-1
lm_sensors-2.5.5-6
kdeaddons-kate-2.2.2-1
kdeaddons-konqueror-2.2.2-1
efax-0.9-9
switchdesk-kde-3.9.7-1
zip-2.3-10
bind-utils-9.2.1-1.7x.2
finger-0.17-9
gq-0.4.0-3
firewall-config-0.95-4
libpcap-0.6.2-12.2.1AS.1
nmap-2.54BETA22-3
nscd-2.2.4-31.7
openssh-3.1p1-6
netdump-0.6.6-1
redhat-config-network-1.0.4-0.AS21.1
sendmail-cf-8.11.6-9.72.4

traceroute-1.4a12-1
whois-1.0.9-1
lrzsz-0.12.20-10
statserial-1.1-23
netscape-common-4.79-2
openssh-server-3.1p1-6
sysstat-4.0.1-2
gnome-lokkit-0.50-6
rarpd-ss981107-9
compat-glibc-6.2-2.1.3.2
binutils-2.11.90.0.8-12
gcc-2.96-116.7.2
gcc-c2.96-116.7.2
compat-libs-6.2-3
XFree86-libs-4.1.0-50.EL
XFree86-100dpi-fonts-4.1.0-50.EL
XFree86-75dpi-fonts-4.1.0-50.EL
XFree86-ISO8859-15-75dpi-fonts-4.1.0-50.EL
XFree86-twm-4.1.0-50.EL
Xconfigurator-4.9.41-1
glibc-common-2.2.4-31.7
mailcap-2.1.6-1
setup-2.5.7-1
basesystem-7.0-2
bdflush-1.5-17
chkconfig-1.3.5-3
db1-1.85-7
db3-3.3.11-5
e2fsprogs-1.26-1.72
file-3.35-2
glib-1.2.10-5
iputils-20001110-6.AS21.2
losetup-2.11g-6
mingetty-0.9.4-18
net-tools-1.60-3
pcre-3.4-2
perl-CGI-2.752-26.72.4
perl-DB_File-1.75-26.72.4
popt-1.6.4-7x.20
reiserfs-utils-3.x.0j-3
setserial-2.17-4
slang-1.4.4-4
netconfig-0.8.11-7
setuptool-1.8-2
tcl-8.3.3-65
termcap-11.0.1-10
bash-2.05-8
crontabs-1.10-1
iproute-2.2.4-14
groff-1.17.2-7.0.2
MAKEDEV-3.3-1
info-4.0b-3
diffutils-2.7.2-2
fileutils-4.1-10.1
findutils-4.1.7-1
grep-2.4.2-7
dhcpcd-1.3.18pl8-13
gzip-1.3-15
man-1.5i2-6
procmail-3.21-1
psmisc-20.1-2
readline-4.2-2
rootfiles-7.2-1
console-tools-19990829-36
slocate-2.6-1
tar-1.13.25-4.AS21.0
textutils-2.0.14-2
mount-2.11g-6
time-1.7-14
utempter-0.5.2-6
vim-minimal-6.0-7.15
words-2-17
pam-0.75-29
cyrus-sasl-1.5.24-24
cyrus-sasl-plain-1.5.24-24
openldap-2.0.27-2.7.3
ppp-2.4.1-3
sh-utils-2.0.11-5
modutils-2.4.13-13
mkinitrd-3.2.6-1
mkbootdisk-1.4.2-3
zlib-1.1.3-25.7
util-linux-2.11f-20
kernel-headers-2.4.9-e.12
ipchains-1.3.10-10
kernel-2.4.9-e.12
lokkit-0.50-6
pvm-3.4.3-28
timeconfig-3.2.2-1
anacron-2.3-17
expat-1.95.1-7
ghostscript-fonts-5.50-3
groff-perl-1.17.2-7.0.2
libxml2-2.4.19-2
LPRng-3.7.4-28.1
mpage-2.5.1-9
Omni-0.5.0-4
perl-Digest-MD5-2.13-1
perl-HTML-Parser-3.25-2
perl-MIME-Base64-2.12-6
perl-Storable-0.6.11-6
perl-libwww-perl-5.53-3
perl-XML-Grove-0.46alpha-3
perl-libxml-perl-0.07-5
perl-XML-Dumper-0.4-5
foomatic-1.1-0.20011218.3
pnm2ppa-1.04-2
a2ps-4.13b-15
alchemist-1.0.18-1
watanabe-vf-1.0-5
VFlib2-2.25.1-20
chkfontpath-1.9.5-2
urw-fonts-2.0-12
printconf-0.3.61-4.1
gtk+1.2.10-11
libtiff-3.5.5-13
switchdesk-3.9.7-1
pvm-gui-3.4.3-28
Xaw3d-1.5-10
Mesa-3.4.2-10
xinitrc-3.20-1
xloadimage-4.1-21
arts-2.2.2-6
libcap-1.10-6
libungif-4.1.0-9.1
libuser-0.32-1
netpbm-9.14-2
openmotif-2.1.30-11
gnome-libs-1.2.13-16
pygtk-0.6.8-3
pygtk-libglade-0.6.8-3
qt-2.3.1-5
tkinter-1.5.2-43.72
dateconfig-0.7.4-7
locale_config-0.3.2-1
redhat-config-users-0.9.2-6
xsri-2.0.3-1
pspell-0.12.2-3
aumix-2.7-5
gdk-pixbuf-gnome-0.14.0-0.2.1
gnome-user-docs-1.4.1-1
gtk-engines-0.11-3
libghttp-1.0.9-2
libgnomeprint15-0.29-6
gedit-0.9.4-6
libgal7-0.8-6
gtop-1.0.13-4
librep-0.13.6-5
libunicode-0.4-6
mozilla-1.0.1-2.2.1
mozilla-psm-1.0.1-2.2.1
bonobo-1.0.7-2
gnome-vfs-1.0.1-18
eel-1.0.2-2
portmap-4.0-38
rep-gtk-0.15-6
scrollkeeper-0.2-6
switchdesk-gnome-3.9.7-1
xchat-1.8.9-1.21as.1
control-center-1.4.0.1-18
sawfish-0.38-11
gnome-applets-1.4.0.1-6
nautilus-1.0.4-46.1
kdeartwork-locolor-2.2.2-1
kdeadmin-2.2.2-4
kdelibs-sound-2.2.2-6
koffice-1.1.1-2
libvorbis-1.0rc2-2.1
kdebase-2.2.2-6
kdeaddons-kicker-2.2.2-1
make-3.79.1-8
pilot-link-0.9.5-10
unzip-5.50-2
kdeutils-2.2.2-2

```
compat-libstdc6.2-
2.9.0.16
gnupg-1.0.6-3
htmlview-1.2.0-1
krbafs-1.0.9-2
logwatch-2.6-1
nmap-frontend-
2.54BETA22-3
nss_ldap-189-4
openssh-clients-3.1p1-
6
radvd-0.6.2pl4-1
rmt-0.4b25-1.72.0
tcp_wrappers-7.6-19
wget-1.8.2-4.72
lockdev-1.0.0-14
minicom-1.83.1-16
mutt-1.2.5.1-1
netscape-communicator-
4.79-2
netdump-server-0.6.6-1
cpp-2.96-116.7.2
iptables-ipv6-1.2.5-3
tripwire-2.3.1-5
ncurses4-5.0-5
glibc-devel-2.2.4-31.7
libstdcdevel-2.96-
116.7.2
man-pages-1.39-2
netscape-navigator-
4.79-2
XFree86-xfs-4.1.0-
50.EL
XFree86-4.1.0-50.EL
XFree86-ISO8859-15-
100dpi-fonts-4.1.0-
50.EL
XFree86-tools-4.1.0-
50.EL
XFree86-xdm-4.1.0-
50.EL
```

Appendix B: HEBCA Audit Requirements (Section 4.5)

This section is taken directly from the Higher Education Certificate Bridge Authority draft document, which is available at the Internet2 website at thus URL: http://middleware.internet2.edu/certpolicies/. Note that this document is not expressly copyrighted, and is almost the same as the Federal Bridge Certificate Authority document from NIST.

4.5 SECURITY AUDIT PROCEDURE

Audit log files shall be generated for all events relating to the security of the HEBCA or Institution CAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall maintained in accordance with Retention period for archive, Section 4.6.2.

Types of Events Recorded

All security auditing capabilities of the HEBCA or Institution CA operating system and PKI CA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. (Note: the table below may be replaced in future releases of this CP with a reference to the Certificate Issuance and Management Components (CIMC) Protection Profile being developed by NIST.) Auditing capabilities relevant to Test Assurance level shall be set forth in the MOA, and thus are not described below. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event
- The date and time the event occurred
- A success or failure indicator when executing the HEBCA or Institution CA's s igning process
- A success or failure indicator when performing certificate revocation
- Identity of the entity and/or operator (of the HEBCA or Institution CA) that caused the event.

- Message from any source requesting an action by the HEBCA or Institution CA is an auditable event. The message must include message date and time, source, destination and contents.

Auditable Event	Rudimentary	Basic	Medium	High
SECURITY AUDIT				
Any changes to the Audit parameters, e.g., audit frequency, type of event audited		X	X	X
Any attempt to delete or modify the Audit logs		X	X	X
Obtaining a third-party time-stamp		X	X	X
IDENTIFICATION AND AUTHENTICATION				
Successful and unsuccessful attempts to assume a role		X	X	X
The value of maximum authentication attempts is changed		X	X	X
Maximum authentication attempts unsuccessful authentication attempts occur during user login		X	X	X
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts		X	X	X
An Administrator changes the type of authenticator, e.g., from password to biometrics		X	X	X

Auditable Event	Rudimentary	Basic	Medium	High
LOCAL DATA ENTRY				
All security-relevant data that is entered in the system		X	X	X
REMOTE DATA ENTRY				
All security-relevant messages that are received by the system		X	X	X
DATA EXPORT AND OUTPUT				
All successful and unsuccessful requests for confidential and security-relevant information		X	X	X
KEY GENERATION				
Whenever the HEBCA or Institution CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X	X	X
PRIVATE KEY LOAD AND STORAGE				
The loading of Component private keys	X	X	X	X
All access to certificate subject private keys retained within the HEBCA or Institution CA for key	X	X	X	X

Auditable Event	Rudimentary	Basic	Medium	High
recovery purposes				
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE				
All changes to the trusted public keys, including additions and deletions	X	X	X	X
SECRET KEY STORAGE				
The manual entry of secret keys used for authentication			X	X
PRIVATE AND SECRET KEY EXPORT				
The export of private and secret keys (keys used for a single session or message are excluded)	X	X	X	X
CERTIFICATE REGISTRATION				
All certificate requests	X	X	X	X
CERTIFICATE REVOCATION				
All certificate revocation requests		X	X	X
CERTIFICATE STATUS CHANGE APPROVAL				

Auditable Event	Rudimentary	Basic	Medium	High
APPROVAL				
The approval or rejection of a certificate status change request		X	X	X
HEBCA OR AGENCY CA CONFIGURATION				
Any security-relevant changes to the configuration of the HEBCA or Institution CA		X	X	X
ACCOUNT ADMINISTRATION				
Roles and users are added or deleted	X	X	X	X
The access control privileges of a user account or a role are modified	X	X	X	X
CERTIFICATE PROFILE MANAGEMENT				
All changes to the certificate profile	X	X	X	X
REVOCATION PROFILE MANAGEMENT				
All changes to the revocation profile		X	X	X
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT				

Auditable Event	Rudimentary	Basic	Medium	High
PROFILE MANAGEMENT				
All changes to the certificate revocation list profile		X	X	X
MISCELLANEOUS				
Installation of the Operating System		X	X	X
Installation of the HEBCA or Institution CA		X	X	X
Installing hardware cryptographic modules			X	X
Removing hardware cryptographic modules			X	X
Destruction of cryptographic modules		X	X	X
System Startup		X	X	X
Logon Attempts to HEBCA or Institution CA Apps		X	X	X
Receipt of Hardware / Software			X	X
Attempts to set passwords		X	X	X
Attempts to modify passwords		X	X	X
Backing up HEBCA or Institution CA internal database		X	X	X
Restoring HEBCA or Institution CA internal database		X	X	X
File manipulation (e.g., creation, renaming, moving)			X	X

Auditable Event	Rudimentary	Basic	Medium	High
Posting of any material to a repository			X	X
Access to HEBCA or Institution CA internal database			X	X
All certificate compromise notification requests		X	X	X
Loading tokens with certificates			X	X
Shipment of Tokens			X	X
Zeroizing tokens		X	X	X
Rekey of the HEBCA or Institution CA	X	X	X	X
Configuration changes to the CA server involving:				
Hardware		X	X	X
Software		X	X	X
Operating System		X	X	X
Patches		X	X	X
Security Profiles			X	X
PHYSICAL ACCESS / SITE SECURITY				
Personnel Access to location of HEBCA or Institution CA			X	X
Access to the HEBCA or Institution CA server			X	X
Known or suspected violations of		X	X	X

Auditable Event	Rudimentary	Basic	Medium	High
physical security				
ANOMALIES				
Software Error conditions		X	X	X
Software check integrity failures		X	X	X
Receipt of improper messages			X	X
Misrouted messages			X	X
Network attacks (suspected or confirmed)		X	X	X
Equipment failure	X	X	X	X
Electrical power outages			X	X
Uninterruptible Power Supply (UPS) failure			X	X
Obvious and significant network service or access failures			X	X
Violations of Certificate Policy	X	X	X	X
Violations of Certification Practice Statement	X	X	X	X
Resetting Operating System clock		X	X	X

Frequency of processing data

Audit logs shall be reviewed in accordance to the table below. All significant events shall be explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

Assurance Level	Review Audit Log
Test	As set forth in the MOA
Rudimentary	Only required for cause
Basic	Only required for cause
Medium	At least once every two months Statistically significant set of security audit data generated by institution CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity
High	At least once per month Statistically significant set of security audit data generated by institution CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity

For the HEBCA, 100% of security audit data generated by the HEBCA since the last review shall be examined.

Retention period for security audit data

Audit logs shall be retained onsite for at least two months as well as being retained in the manner described below. The individual who removes audit logs from the HEBCA or Institution CA system shall be an official different from the individuals who, in combination, command the HEBCA or an Institution CA signature key.

Protection of security audit data

Institution CA and HEBCA system configuration and procedures must be implemented together to ensure that:

- only authorized people have read access to the logs;
- only authorized people may archive or delete audit logs; and ,

- audit logs are not modified.

The entity performing audit log archive need not have modify access, but procedures must be implemented to protect archived data from deletion or destruction prior to the end of the audit log retention period (note that deletion requires modification access). Audit logs shall be moved to a safe, secure storage location separate from the HEBCA equipment.

Security Audit data backup procedures

Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit log shall be sent off-site in accordance with the CPS on a monthly basis.

Security Audit collection system (internal vs. external)

The audit log collection system may or may not be external to the HEBCA or Institution CA system. The audit process shall not be done by or under the control of the HEBCA OA (or comparable authority for an Institution CA). Audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the HEBCA OA Administrator (or comparable Institution authority) shall determine whether to suspend HEBCA operation (or Institution CA operation respectively) until the problem is remedied.

Notification to event-causing subject

This CP imposes no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

Vulnerability Assessments

No stipulation.

Appendix C: Results from Initial CI Security Benchmark Scan

```
*** CIS Ruler Run ***
Starting at time 20031231-14:47:22

Positive: 1.1 System appears to have been patched within the last
month.
Negative: 1.2 System isn't running sshd.
Negative: 2.1 xinetd service sgi_fam requires full deactivation -- you
should set 'disable=yes' in sgi_fam.
Positive: 2.2 telnet is deactivated.
Positive: 2.3 ftp is deactivated.
Positive: 2.4 rsh, rcp and rlogin are deactivated.
Positive: 2.5 tftp is deactivated.
Positive: 2.6 imap is deactivated.
Positive: 2.7 POP server is deactivated.
Positive: 3.1 Found a good daemon umask of 022 in
/etc/rc.d/init.d/functions.
Negative: 3.2 xinetd is still active.
Positive: 3.3 Mail daemon is not listening on TCP 25.
Positive: 3.4 Graphical login is deactivated.
Positive: 3.5 X Font Server (xfs) script has been deactivated
Positive: 3.6 Miscellaneous scripts are all turned off.
Positive: 3.7 Windows compatibility servers (samba) have been
deactivated.
Positive: 3.8 NFS Server script nfs is deactivated.
Positive: 3.9 This machine isn't being used as an NFS client.
Positive: 3.10 NIS Client processes are deactivated.
Positive: 3.11 NIS Server processes are deactivated.
Positive: 3.12 RPC rc-script has been deactivated.
Positive: 3.13 netfs rc script is deactivated.
Negative: 3.14 lpd (line printer daemon) not deactivated.
Positive: 3.15 Web server is deactivated.
Positive: 3.16 SNMP daemon is deactivated.
Positive: 3.17 DNS server is deactivated.
Positive: 3.18 SQL database server is deactivated.
Positive: 3.19 Webmin GUI-based system administration daemon
deactivated.
Positive: 3.20 Squid web cache daemon deactivated.
Positive: 3.21 Kudzu hardware detection program has been deactivated.
Negative: 4.1 /proc/sys/net/ipv4/conf/eth0/accept_source_route should
be set to 0.
Negative: 4.1 /proc/sys/net/ipv4/conf/lo/accept_source_route should be
set to 0.
Negative: 4.1 /proc/sys/net/ipv4/conf/eth0/accept_redirects should be
set to 0.
Negative: 4.1 /proc/sys/net/ipv4/conf/lo/accept_redirects should be set
to 0.
Negative: 4.1 /proc/sys/net/ipv4/conf/eth0/secure_redirects should be
set to 0.
Negative: 4.1 /proc/sys/net/ipv4/conf/lo/secure_redirects should be set
to 0.
Negative: 4.1 /proc/sys/net/ipv4/tcp_max_syn_backlog should be at least
4096 to handle SYN floods.
```

```
Negative: 4.2 /proc/sys/net/ipv4/conf/eth0/send_redirects should be set
to 0.
Negative: 4.2 /proc/sys/net/ipv4/conf/lo/send_redirects should be set
to 0.
Positive: 5.1 syslog captures authpriv messages.
Positive: 5.2 FTP server is configured to do full logging.
Positive: 5.3 All logfile permissions and owners match benchmark
recommendations.
Negative: 6.1 /boot is not mounted nodev.
Negative: 6.1 /var is not mounted nodev.
Negative: 6.1 /home is not mounted nodev.
Negative: 6.1 /tmp is not mounted nodev.
Negative: 6.1 /usr is not mounted nodev.
Negative: 6.2 Removable filesystem /mnt/floppy is not mounted nosuid.
Negative: 6.2 Removable filesystem /mnt/floppy is not mounted nodev.
Negative: 6.2 Removable filesystem /mnt/cdrom is not mounted nosuid.
Negative: 6.2 Removable filesystem /mnt/cdrom is not mounted nodev.
Negative: 6.3 PAM allows users to mount removable media: <floppy>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <cdrom>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <pilot>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <jaz>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <zip>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <ls120>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <camera>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <memstick>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <flash>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <diskonkey>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <rem_ide>.
(/etc/security/console.perms)
Negative: 6.3 PAM allows users to mount removable media: <rio500>.
(/etc/security/console.perms)
Positive: 6.4 password and group files have right permissions and
owners.
Positive: 6.5 all temporary directories have sticky bits set.
Positive: 7.1 rhosts authentication totally deactivated in PAM.
Positive: 7.2 /etc/hosts.equiv and root's .rhosts/.shosts files either
don't exist, are zero size or are links to /dev/null.
Positive: 7.3 FTP daemons do not permit system users to use FTP.
Negative: 7.4 X is listening on TCP port 6000.
Negative: 7.5 Couldn't open cron.allow
Negative: 7.5 Couldn't open at.allow
Negative: 7.6 The permissions on /etc/crontab are not sufficiently
restrictive.
Negative: 7.7 No Authorized Only message in Gnome's
/etc/X11/gdm/gdm.conf.
```

```
Negative: 7.7 No Authorized Only banner for telnet in file
/etc/xinetd.d/telnet.
Negative: 7.7 No Authorized Only banner for krb5-telnet in file
/etc/xinetd.d/krb5-telnet.
Negative: 7.7 No Authorized Only banner for klogin in file
/etc/xinetd.d/klogin.
Negative: 7.7 No Authorized Only banner for eklogin in file
/etc/xinetd.d/eklogin.
Negative: 7.7 No Authorized Only banner for gssftp in file
/etc/xinetd.d/gssftp.
Negative: 7.7 No Authorized Only banner for kshell in file
/etc/xinetd.d/kshell.
Negative: 7.8 xinetd either requires global 'only-from' statement or
one for each service.
Positive: 7.9 System is set to only allow root login on console.
Positive: 7.10 GRUB is password-protected.
Positive: 7.10 GRUB is password-protected.
Negative: 7.11 /etc/inittab needs a /sbin/sulogin line for single user
mode.
Positive: 7.12 /etc/exports is empty or doesn't exist, so it doesn't
need to be tuned for privports.
Negative: 8.1 rpm has a valid shell of /bin/bash.
Negative: 8.1 pvm has a valid shell of /bin/bash.
Negative: 8.1 netdump has a valid shell of /bin/bash.
Negative: 8.1 mysql has a valid shell of /bin/bash.
Positive: 8.2 All users have passwords
Negative: 8.3 User dmurdoch should have a minimum password life of at
least 7 days.
Negative: 8.3 User dmurdoch should have a maximum password life of
between 1 and 90 days.
Negative: 8.3 User netscape should have a minimum password life of at
least 7 days.
Negative: 8.3 User netscape should have a maximum password life of
between 1 and 90 days.
Negative: 8.3 User celwes should have a minimum password life of at
least 7 days.
Negative: 8.3 User celwes should have a maximum password life of
between 1 and 90 days.
Negative: 8.3 User mpatink should have a minimum password life of at
least 7 days.
Negative: 8.3 User mpatink should have a maximum password life of
between 1 and 90 days.
Negative: 8.3 User imontoya should have a minimum password life of at
least 7 days.
Negative: 8.3 User imontoya should have a maximum password life of
between 1 and 90 days.
Negative: 8.3 User mmax should have a minimum password life of at least
7 days.
Negative: 8.3 User mmax should have a maximum password life of between
1 and 90 days.
Negative: 8.3 User bcrystal should have a minimum password life of at
least 7 days.
Negative: 8.3 User bcrystal should have a maximum password life of
between 1 and 90 days.
```

```
Negative: 8.3 User wshawn should have a minimum password life of at
least 7 days.
Negative: 8.3 User wshawn should have a maximum password life of
between 1 and 90 days.
Negative: 8.3 User csarando should have a minimum password life of at
least 7 days.
Negative: 8.3 User csarando should have a maximum password life of
between 1 and 90 days.
Negative: 8.3 User rwright should have a minimum password life of at
least 7 days.
Negative: 8.3 User rwright should have a maximum password life of
between 1 and 90 days.
Negative: 8.3 /etc/login.defs value PASS_MAX_DAYS = 99999, but should
not exceed 90.
Negative: 8.3 /etc/login.defs value PASS_MIN_DAYS = 0, but should not
be less than 7.
Negative: 8.3 /etc/login.defs value PASS_MIN_LEN = 5, but should be at
least 6.
Positive: 8.4 There were no +: entries in passwd, shadow or group maps.
Positive: 8.5 Only one UID 0 account AND it is named root.
Negative: 8.6 Couldn't find root's shell among our list so as to check
PATH variable.  List includes: sh,csh,ksh,tcsh,bash,ash,zsh,bsh
Positive: 8.7 No user's home directory is world or group writable.
Positive: 8.8 No group or world-writable dotfiles in user home
directories!
Positive: 8.9 No user has a .netrc file.
Negative: 8.10 Current umask setting in file /etc/profile is 000 -- it
should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/profile is 000 -- it
should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/csh.login is 000 --
it should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/csh.login is 000 --
it should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/bashrc is 022 -- it
should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/bashrc is 022 -- it
should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/csh.cshrc is 002 --
it should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /etc/csh.cshrc is 002 --
it should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.bash_profile is 000
-- it should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.bash_profile is 000
-- it should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.bashrc is 000 -- it
should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.bashrc is 000 -- it
should be stronger to block group-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.cshrc is 000 -- it
should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.cshrc is 000 -- it
should be stronger to block group-read/write/execute.
```

```
Negative: 8.10 Current umask setting in file /root/.tcshrc is 000 -- it
should be stronger to block world-read/write/execute.
Negative: 8.10 Current umask setting in file /root/.tcshrc is 000 -- it
should be stronger to block group-read/write/execute.
Negative: 8.11 Coredumps aren't deactivated.
Preliminary rating given at time: Wed Dec 31 14:47:24 2003

      Preliminary rating = 6.62 / 10.00

Negative: 6.6 Non-standard world-writable file:
/usr/netscape/servers/java/.java/.systemPrefs/.system.lock
Negative: 6.6 Non-standard world-writable file:
/usr/netscape/servers/java/.java/.systemPrefs/.systemRootModFile
Negative: 6.7 Non-standard SUID program /usr/X11R6/bin/Xwrapper
Negative: 6.7 Non-standard SUID program /usr/sbin/sendmail
Ending run at time: Wed Dec 31 14:47:33 2003

      Final rating = 6.62 / 10.00
```