the CENTER for INTERNET SECURITY

# Center for Internet Security Benchmark for Xen 3.2

Version 1.0
May, 2008

Editor: Adam Cecchetti
Leviathan Security Group

cis-feedback@cisecurity.org

# Table of Contents

# Terms of Use

**Background**.

The Center for Internet Security ("**CIS**") provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems, and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

**No Representations, Warranties, or Covenants.**

CIS makes no representations, warranties, or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness, or completeness of the Products or the Recommendations. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties, or covenants of any kind.

**User Agreements.**

By using the Products and/or the Recommendations, I and/or my organization ("**We**") agree and acknowledge that:

1. No network, system, device, hardware, software, or component can be made fully secure;

2. We are using the Products and the Recommendations solely at our own risk;

3. We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;

4. We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades, or bug fixes; or to notify us of the need for any such corrections, updates, upgrades, or bug fixes; and

6. Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or

special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

**Grant of Limited Rights.**

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

1. Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

2. Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

**Retention of Intellectual Property Rights; Limitations on Distribution.**

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights."

Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend, and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development, or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs, and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

**Special Rules.**

The distribution of the NSA Security Recommendations is subject to the terms of the NSA Legal Notice and the terms contained in the NSA Security Recommendations themselves (http://nsa2.www.conxion.com/cisco/notice.htm).

CIS has created and will from time to time create, special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules.

CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

**Choice of Law; Jurisdiction; Venue**

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions.

Terms of Use Agreement Version 2.1 – 02/20/04

# Introduction

## *Explanation of This Document*

This document is a general guide for securing Xen Virtualization Server 3.2 hosted on the Red Hat Enterprise Linux 5 platform. The document contains sections on the configuration of Xen virtual networks, hosts and devices. These sets of rules constitute a benchmark. This benchmark represents an industry consensus of best practices, listing steps to be taken and the reasons for each recommendation.

## *Intended Audience*

While this document is intended for system administrators, it should be useful for anyone interested in the Xen server and virtual machine installation and configuration. We assume that the reader is a knowledgeable "system administrator." In the context of this document, a knowledgeable system administrator is defined as someone who can create and manage accounts and groups, set account policies and user rights, enable auditing and read audit logs, and who understands how operating systems perform access control. We further assume that the reader is familiar with Linux system administration. Consequently, no tutorial information is provided for Linux. Red Hat's web presence at http://www.redhat.com includes links an extensive array of Linux and Xen-related material.

## *Practical Application*

We encourage readers to compare this document to the security policies and procedures for their organization. This benchmark can be used to assess the security state of their Xen implementations.

## *Security Levels*

**Level 1** - The prudent level of minimum due care.

Settings are considered "safe" to apply to most systems. Using these configuration recommendations is unlikely to have a negative impact on performance or functionality unless indicated in the comments.

**Level 2** - Prudent security beyond the minimum level.

Settings provide a higher level of security, but may result in a negative impact to performance, functionality, or cost.

## *Precursor Technical Information*

Host Domain – The Host Domain refers to the operating system that hosts the Xen kernel extensions, Xen daemon (XenD), and Xen tools. Host Domain provides the Xen kernel extensions to the XenD that creates virtualized environments for the Guest Domains. Only administrators should be provided access to manage the Host Domain. Host Domain is often referred to as Domain0 or Dom0 in the Xen documentation.

Guest Domain – Refers to any guest host that is booted inside of a Host Domain virtualized environment. Guest Domain is often referred to by DomainU or DomU in the Xen documentation.

Direct Memory Access (DMA) – Direct memory access is an optimization mechanism used in nearly all modern computers. The DMA controller copies data from hardware to memory or from memory to memory without using the main CPU. The DMA controller has full unrestricted read and write access to all system memory, which provides a large performance increase. However the DMA provides no checks for writes performed by the DMA. These memory writes may include memory used by the Host Domain, Guest Domain, or other program on the host operating system. The Host Domain is responsible for ensuring that only approved writes are performed by the DMA controller , and uses kernel level access checks to do so. If a guest domain is allowed direct access to the DMA controller these checks are bypassed, an attacker can easily compromise the host domain or other guest domains.

Attack Surface – Attack Surface refers to the totality of the services running on a host and exposed to attack. Removing features or denying attackers access can both reduce the attack surface. Ideally attack surface should be as small as possible while allowing an organization to meet its business needs. By minimizing the attack surface complexity is reduced and time and resources can be dedicated to securing the remaining exposed services.

Open network and services are part of the attack surface for a networking interface. The fewer ports and services, the smaller the attack surface.

An exposed API and forms are part of the attack surface for a web application. The more forms and API calls available, the larger the attack surface.

In the Xen environment, attack surface is specific to each domain, with low level attacks generally affecting the Host Domain.

# 1. General Virtualization Guidance

The following sections provide general guides for Xen Host Domain, and Guest Domains.

## *1.1. Host Domain System Configuration*

Before any Xen virtual machines can be secure, the Host Domain of the host Linux operating system must be secure. A compromise of the Host Domain makes compromising the Guest Domains a simple task. Thus steps should be taken to reduce the attack surface of the Host Domain. These include but are not limited to:

- Remove unnecessary accounts and groups.
- Disable unnecessary services.
- Remove unnecessary binaries, libraries, and files.
- Firewall network access to the host.
- Install monitoring or Host Intrusion Detection Systems.
- Ensure that the Host Domain is not accessible from the Guest Domains.
- Ensure that monitoring or remote console interfaces for the Host Domain are not accessible via the Guest Domains.
- Ensure that the Guest Domains cannot directly affect any network storage or other resources that the Host Domain relies on for boot, configuration, or authentication.

The Host Domain host should only be used as a resource for virtualizing other operating environments. The Host Domain system should not host any other services or resources itself, including web, email and file servers. If such services are required, migrate the services to another system or consider creating a virtual machine to host them inside of a Guest Domain.

## *1.2. Xen Security Modules*

The Xen Security Module architecture adds pluggable security modules. These modules provide new forms of access control to the Xen Host Domain, Guest Domains, and hardware. Every Xen environment will differ in setup and policy requirements and this document only provides an overview of each module's functionality. For additional information see the documentation in the Xen software /tools/security and tools/Flask directories.

**Dummy**
The dummy security module is a placeholder module. It provides no additional security or access control mechanisms over Domains. It should not be used in a production environment.

**sHype**
The sHype security module enables Chinese Wall policies to be set for virtual machines. Chinese Wall policies prevent separate entities with strict conflicts of interest from accessing or influencing each other's information and resources. The policies are tunable for each environment, and allow the enforcement of which domains can run concurrently or share resources. It also controls which resources can be accessed on a per domain basis.

Consider an example with three domains labeled Accounting, Marketing, and R&D. An administrator can use sHype policy to specify that the Accounting and Marketing Domains can run concurrently on the same Xen server, unless an R&D domain is running. Labels are applied to each virtual machine for each department. When Xen attempts to boot an Accounting domain while an R&D Domain is already running, it is blocked by the sHype module. This allows for the isolation of sensitive information on the R&D Domain.

**Flask**
The Flask Xen Security Module utilizes the existing SELinux policy language and tools for policy generation and analysis. The Xen Flask policies are a reduced set of those provided by SELinux. These restrictions allow for setting fine grained custom policy to define which specific hardware, Guest Domains, Host Domain, and I/O resources a Domain can access. Set the following in `Config.mk` to enable Flask

```
XSM_ENABLE ?= y
FLASK_SECURITY ?= y
```

Recompile Xen:

```
$ make world
# make install
```

## *1.3. Virtualized vs. Non Virtualized Hosts*

Virtualization can bring many benefits to an infrastructure, however there are scenarios where it is better to consider dedicating a physical machine entirely to one host. These fall into two categories:

Guest Domains that require direct access to hardware

If a domain requires direct access to hardware resources for performance or compatibility with exotic hardware, it is best placed on a dedicated host. While Xen provides features for allowing an untrusted Guest Domain to directly access hardware, this creates a risk of attacks using Direct Memory Access (DMA), which could compromise the integrity and security of other Guest Domains on the same hardware.

Guest Domains that require strict security configurations

Physical hosts should be used instead of virtual ones where host security is of the utmost importance. Examples of such hosts are bastion management hosts and PKI Root servers. Virtualizing these hosts gives the Host Domain complete control over the Guest Domain. This increases the attack surface of the bastion host in the Guest Domain, as the compromise of either the Guest Domain or the Host Domain results in a successful attack.

# 2.Benchmark Summary Checklist

| Reference | Lv | Scr | Description | Default | Suggested |
|---|---|---|---|---|---|
| Disable Debugging Xen | L1 | Y | Disable debugging support for Xen at compile time. | `debug?= n` | `debug?= n` |
| Enable XSM, Flash, and ACM | L1 | Y | Enable Xen Security Modules and Access Control Module. | `XSM_ENABLE ?= n`<br>`FLASK_ENABLE ?= n`<br>`ACM_SECURITY ?= n` | `XSM_ENABLE ?= y`<br>`FLASK_ENABLE ?= y`<br>`ACM_SECURITY ?= y` |
| Use Absolute Path for Xend Log File | L1 | Y | The Xen logging path should be set as an absolute path and not a relative path or symbolic link. | `#(logfile /path)` | `(logfile /absolute/path)` |
| Disable Unnecessary Xen API Servers | L1 | N | Remove or disable non critical Xen API interfaces. | `#(xen-api-server)`<br>`#(xend-http-server no)`<br>`#(xend-api-server no)`<br>`#(xend-unix-server no)`<br>`#(xend-tcp-xmlrpc-server no)`<br>`#(xend-unix-xmlrpc-server no)` | `#(xen-api-server)`<br>`#(xend-http-server no)`<br>`#(xend-api-server no)`<br>`#(xend-unix-server no)`<br>`#(xend-tcp-xmlrpc-server no)`<br>`#(xend-unix-xmlrpc-server no)` |
| Disable Xen Relocation Server | L2 | Y | Remove or disable Xen relocation service. | *`(xend-relocation-server yes)`* | `#(xend-relocation-server yes)` |
| Use Absolute Path for `xend-unix-path` | L1 | Y | The `xend-unix-path` should be set as an absolute path and not a relative path or symbolic link. | `#(xend-unix-path /path/to/send-socket)` | `#(xend-unix-path /path/to/send-socket)` |
| Specify `xen-tcp-xmlrpc-server-address` Bind Address | L1 | Y | Ensure that only IP addresses on the `localhost` or management network are bound to the `xen-tcp-xmlrpc` server. | `(xen-tcp-xmlrpc-server-address ‘localhost’)` | `(xen-tcp-xmlrpc-server-address ‘localhost’)` |
| Specify `xend-address` Bind Address | L1 | Y | Ensure that only connections from the `localhost` or management network can access the HTTP API server. | `(xend-address ‘’)` | `(xend-address ‘localhost’)` |
| Specify `xend-relocation-address` Bind Address | L1 | Y | Ensure that only connections from the `localhost` or management network can access the Xen relocation server. | `(xend-relocation-address ‘’)` | `(xend-relocation-address ’localhost’)` |
| Filter Relocation and | L1 | N | Filter the relocation and management | `N/A` | `N/A` |

| | | | | | |
|---|---|---|---|---|---|
| Management Hosts and Ports | | | ports and hosts at the network segment level. | | |
| Specify Host List in Relocation Allow | L1 | N | Provide an approved list for relocation of Xen Domains. | N/A | N/A |
| Use SSL with `tcp-xmlrpc` | L1 | Y | Enable Secure Sockets with the `tcp-xmlrpc` API interface. | `#(xend-tcp-xmlrpc-server-ssl-keyfile /path/to/key)`<br>`#(xend-tcp-xmlrpc-server-ssl-certfile /path/to/cert)` | `(xend-tcp-xmlrpc-server-ssl-keyfile /path/to/key)`<br>`(xend-tcp-xmlrpc-server-ssl-certfile /path/to/cert)` |
| Disable Core Dumps | L1 | Y | Prevent Xen from creating a core dump on crash. | `(enable-dump yes)` | `(enable-dump no)` |
| Disable VNC Interface | L1 | Y | Disable the VNC interface for administration of Xen Domains. | `(vnc-listen )` | `#(vnc-listen)` |
| Specify VNC Bind Interface | L1 | Y | Ensure that the VNC interface can only listen on the localhost or management network interface. | `(vnc-listen ‘0.0.0.0’)` | `(vnc-listen ‘localhost’)` |
| Set VNC Password | L1 | Y | Ensure that the VNC password is set to and authentication is required. | `(vncpasswd ‘’)` | `(vncpasswd ‘5tr0ngP455w0rd!’)` |
| Use TLS For VNC | L1 | Y | Enable TLS for the VNC server. | `#(vnc-tls 1)` | `(vnc-tls 1)` |
| Set Absolute Path for VNC Cert Directory | L1 | Y | Ensure that the certificates directory is set to an absolute path and not a relative path or symbolic link. | `(vnc-x509-cert-dir /etc/xen/vnc)` | `(vnc-x509-cert-dir /etc/xen/vnc)` |
| Require User Client Certificate VNC Authentication | L2 | Y | Require a Client certificate for the TLS session. | `#(vnc-x509-verify 1)` | `(vnc-x509-verify 1)` |
| Set File Permissions on VNC Certificate and Key | L1 | Y | Ensure that proper file system permissions have been set on the VNC certificate and key file. | N/A | `755 certfile`<br>`400 keyfile` |
| Isolate Management Network | L2 | N | Isolate the Host Domain’s networking resources both physically and logically from the untrusted guest domains. | N/A | N/A |
| Disable PCI Permissive Devices | L1 | Y | Disable or remove entries from the PCI permissive list. | N/A | N/A |
| Restrict File System Permissions on Kernel and | L1 | N | Ensure that access rights are properly set for the kernel and ram disk files | N/A | `755 kernel`<br>`755 ramdisk` |

| | | | | | |
|---|---|---|---|---|---|
| Ramdisk Files | | | used in the Xen Guest Domain. | | |
| Inspect permissions on the virtual disk files | L1 | Y | Ensure the access rights to the virtual disks used in the Xen Guest Domain. | N/A | N/A |
| Use Absolute Path for Kernel and Ramdisk file | L1 | N | The kernel and initial ramdisk paths should be set as an absolute and not a relative path or symbolic link. | N/A | N/A |
| Use Absolute  Path to Virtual Disks | L1 | N | The virtual disk paths should be set as an absolute and not a relative path or symbolic link. | N/A | N/A |
| Bind VNC Server to Specific Interface | L1 | Y | Bind the VNC server to a specific network interface. | `vnclisten=”0.0.0.0”` | `vnclisten=”127.0.0.1”` |
| Set VNC Password | L1 | Y | Set a strong VNC password for administration and connecting to the Domain. | `vncpassword=’’` | `vncpassword=’5tr0ng!p455w0rd#’` |
| Disable or Restrict Root Login Via Console | L2 | N | Ensure root user is not allowed to log in via a serial console. | N/A | N/A |
| Disable Remote Root Login to SSH | L1 | Y | Restrict remote logins to non privileged users. | `#PermitRootLogin yes` | `PermitRootLogin no` |
| Configure SSH | L1 | Y | Configure the SSH server to be secure by default and disable legacy authentication mechanisms. | `#Banner /etc/banner`<br>`X11Forwarding yes`<br>`#RhostsAuthentication  yes`<br>`#HostbasedAuthentication yes`<br>`#PermitEmptyPasswords yes` | `Banner /etc/banner`<br>`X11Forwarding no`<br>`RhostsAuthentication  no`<br>`HostbasedAuthentication  no`<br>`PermitEmptyPasswords no` |
| Create a Non Privileged User for Management of Xen Server | L1 | Y | Create a regular user for login and administration of the Xen server. | N/A | N/A |
| Create a Management Group for Xen | L1 | Y | Create a group for the management of Xen and access to Xen binaries. | N/A | N/A |
| Create a Sudoers Command Alias for Xen | L1 | N | Create a command alias to separate Xen groups from the other administrative roles. | N/A | See detailed remediation |
| Assign the Xen Group to the Xen Command Alias | L1 | N | Assign the Xen command privileges to the Xen group. | N/A | `%xen ALL = XEN` |
| Enable Shadow Passwords | L1 | Y | Create shadow and gshadow files to be utilized by Xen server authentication systems. | N/A | `touch /etc/shadow`<br>`touch /etc/gshadow` |

| | | | | | |
|---|---|---|---|---|---|
| Change the Root Password | L1 | N | Rehash the root account password with the MD5 or stronger algorithm | N/A | N/A |
| Migrate All Existing Accounts to the Shadow and Gshadow Files | L1 | Y | Remove the user password hashes from the passwd file after the creation of the shadow files. Require all users to change their passwords on the Xen servers. | N/A | N/A |

# 3.General Configuration

## 3.1. Disable Debugging Xen

**Description:** Disable debugging support for Xen at compile time.

**Rationale:** Debugging support can leak sensitive Guest Domain information and may provide an attacker with additional information. Debugging support is disabled by default and should be left disabled unless a specific Xen issue is being traced. Administrators should recompile and reinstall Xen if debugging was initially enabled. Note: If you have removed the GCC package from your system per the RHEL 5 benchmark Xen will have to be recompiled on a different system and then copied over to the hardened host.

**Recommendation Level:** L1

**Scorable**: Yes

**Audit:** Inspect `Config.mk` for the following string:

```
debug ?= y
```

**Remediation:** Set the following in `Config.mk`

```
debug ?= n
```

## 3.2. Enable XSM, Flask, and ACM

**Description:** Enable Xen Security Modules and Access Control Module.

**Rationale:** Enabling the Xen Security Module options improves control of virtual machine access communications. The author recommends the usage of ACM or Flask for environments requiring strict security or privilege separation of Guest Domains. Enabling these features merely allows policy to be created and does not apply any additional security by default. By default ACM is enabled in the RHEL 5 Xen distributed binary package a recompile and install is only required if Flask is used or a or a custom installation of Xen is used.

**Note**: Only Flask or ACM can be enabled at the same time.

Note: If you have removed the GCC package from your system per the RHEL 5 benchmark Xen will have to be recompiled on a different system and then manually copied and installed to the hardened host.

**Recommendation Level:** L2

**Scorable**: Yes

**Audit:** Inspect `Config.mk` to ensure each of the following settings are set to 'n':

```
# grep XSM_ENABLE Config.mk
         XSM_ENABLE ?= n

# grep FLASH_ENABLE Config.mk
         FLASK_ENABLE ?= n

# grep ACM_SECURITY Config.mk
         ACM_SECURITY ?= n
```

**Remediation:** Edit `Config.mk` and set the following values:

```
XSM_ENABLE ?=y
FLASK_ENABLE ?=y
ACM_SECURITY ?= y
```

## 3.3. Use Absolute Path for Xend Log File

**Description:** The Xen logging path should be an absolute path and not a relative path or symbolic link.

**Rationale:** If an attacker can control the log file path, log information may be destroyed or replaced with content of the attacker's choice. Ensure that this path is absolute and has secure file permissions.

**Recommendation Level:** L1

**Scorable**: Yes

**Audit:** Inspect the `xend-config.sxp` file to ensure an absolute path is used for the `logfile` parameter.

```
$ grep logfile xend-config.sxp
      #(logfile /var/log/xen/xend.log)
```

**Remediation:**
Change the logfile entry to an absolute path. Delete the symbolic link if any, and create a file.

```
# rm  <logfile>
# touch <logfile>
```

## 3.4. Disable Unnecessary Xen API Servers

**Description:** Remove or disable non critical Xen API interfaces.

**Rationale:** Many of the Xen API services are legacy interfaces with little or no authentication. Disable the XenAPI interfaces if they are not required.

**Recommendation Level:** L1

**Scorable**: No

**Audit:** Inspect the `xend-config.sxp` file for any of the following set to yes:

```
# grep xen-api-server xend-config.sxp
      (xen-api-server )
# grep xen-http-server xend-config.sxp
      (xend-http-server no)
# grep xen-api-server xend-config.sxp
      (xend-api-server no)
# grep xen-unix-server xend-config.sxp
      (xend-unix-server no)
# grep xen-tcp-xmlrpc-server xend-config.sxp
      (xend-tcp-xmlrpc-server no)
# grep xen-unix-xmlrpc-server xend-config.sxp
      (xend-unix-xmlrpc-server no)
```

**Remediation:** Edit the `xend-config.sxp` file and **e**nsure that each of the xend servers is disabled.

```
#(xen-api-server)
#(xend-http-server no)
#(xend-api-server no)
#(xend-unix-server no)
#(xend-tcp-xmlrpc-server no)
#(xend-unix-xmlrpc-server no)
```

## *3.5. Disable Xen Relocation Server*

**Description:** Remove or disable Xen relocation service.

**Rationale:** Disabling this service reduces the number of services an attacker can target. Disable Xen relocation if it will not be used.

**Recommendation Level:** L2

**Scorable**: Yes

**Audit:** Inspect `xend-config.sxp` to ensure the `xend-relocation-server` parameter is set to 'yes'.

```
$ grep xend-relocation-server xend-config.sxp
    (xend-relocation-server yes)
```

**Remediation:**
Ensure that each of the xend servers are disabled in `xend-config.sxp`.

```
(xend-relocation-server no)
```

or comment out the entry

```
#(xend-relocation-server yes)
```

## *3.6. Use Absolute Path for xend-unix-path*

**Description:** The `xend-unix-path` should be set as an absolute path and not a relative path or symbolic link.

**Rationale:** If the Xen UNIX API will be used, ensure that the path is an absolute path. If an attacker can perform a file system attack to redirect the `xend-unix-path` to a resource they control, they will be able to attack or alter the socket resources for this API server. Ensure that this path is absolute and has secure file permissions.

**Recommendation Level:** L1

**Scorable**: Yes

**Audit:** Locate the `xend-unix-path` argument in `xend-config.sxp` and ensure the argument does not point to a symbolic link

```
$ grep xend-unix-path xend-config.sxp
   (xend-unix-path /path/to/send-socket)

$ ls –al /path/to/xend-socket
```

**Remediation:** Change the entry to an absolute path. Delete the symbolic link and create an appropriate directory.

## *3.7. Specify xen-tcp-xmlrpc-Server-Address Bind Address*

**Description:** Ensure that only IP addresses on the `localhost` or management network are bound to the `xen-tcp-xmlrpc` server.

**Rationale:** If the `tcp-xmlrpc-server` API interface will be used, ensure that only hosts on the management network are allowed to reach this interface. This will help reduce the attack surface from both the untrusted domains and the networking interface.

**Recommendation Level:** L1

**Scorable**: Yes

**Audit:** Inspect the `xend-config.sxp` file and ensure the relocation server is bound to `localhost`.

```
$ grep xen-tcp-xmlrpc-server-address xend-config.sxp
 (xen-tcp-xmlrpc-server-address ‘localhost’)
```

**Remediation:** Set the following in the `xend-config.sxp` file:

```
(xen-tcp-xmlrpc-server-address ‘localhost’)
```

## *3.8. Specify xend-address Bind Address*

**Description:** Ensure that only connections from the `localhost` or management network can access the HTTP API server.

**Rationale:** If the HTTP API interface must be used, ensure that only hosts on the management network are capable of reaching this interface. This will help reduce the attack surface from both the un-trusted domains and the networking interface.

**Recommendation Level:** 1

**Scorable**: Yes

**Audit:** Inspect the `xend-address` property and ensure it's bound to `localhost` or a management network address.

```
$ grep  xend-address xend-config.sxp
      (xend-address ‘0.0.0.0’)
```

**Remediation:** Set the `xend-address` to `localhost` in `xend-config.xsp`

```
(xend-address ’localhost’)
```

## 3.9. Specify xend-relocation-address Bind Address

**Description:** Ensure that only connections from the `localhost` or management network can access the Xen Relocation server.

**Rationale:** If the Xen relocation feature must be used, ensure that only hosts on the management network are capable of reaching this interface. This will help reduce the attack surface from both the untrusted domains and the networking interface.

**Recommendation Level:** 1

**Scorable**: Yes

**Audit:** Inspect the `xend-relocation-address` parameter in `xend-config.sxp` to ensure it is set to `localhost` or a management network address.

```
$ grep xend-relocation-address xend-config.sxp
      (xend-relocation-address ‘0.0.0.0’)
```

**Remediation:** Set the `xend-relocation-address` parameter in `xend-config.sxp` to `localhost`.

```
(xend-relocation-address ’localhost’)
```

## 3.10. Filter Relocation and Management Hosts and Ports

**Description:** Filter the relocation and management ports and hosts at the network segment level.

**Rationale:** Administrators should use additional network filters such as a firewall rules, access list, or a white list of Xen relocation and management hosts. This will help ensure that only approved Xen hosts can migrate or manage Guest Domain images.

**Recommendation Level:** L1

**Scorable**: No

**Audit:** N/A

**Remediation:** N/A

## *3.11. Specify Host List in Relocation Allow*

**Description:** Provide an approved list for relocation of Xen Domains.

**Rationale:** If the relocation feature is used, ensure that only approved Xen hosts can migrate Guest Domains to this host.

**Recommendation Level:** L1

**Scorable**: No

**Audit:** Inspect `xend-config.sxp` to ensure the `xend-relocation-hosts-allow` parameter is set to allow only authorized hosts.

```
$ grep xend-relocation-hosts-allow xend-config.sxp
      (xend-relocation-hosts-allow ‘’)
```

**Remediation:** Set the `xend-relocation-hosts-allow` parameter in `xend-config.sxp` to allow only authorized hosts.

```
(xend-relocation-hosts-allow ‘^localhost$ iplist domain.com’)
```

## *3.12. Use SSL with tcp-xmlrpc*

**Description:** Enable Secure Sockets with the `tcp-xmlrpc` API interface.

**Rationale:** SSL proves an additional layer of protection for the session and data passed to the `xmlrpc` API interface.

**Recommendation Level:** L1

**Scorable**: Yes

**Audit:** Inspect `xend-config.sxp` to ensure the `xend-tcp-xmlrpc-server-ssl-key-file` and `xend-tcp-xmlrpc-server-ssl-cert-file` points to the server's certificate and key files.

```
$ grep xend-tcp-xmlrpc-server-ssl-key-file xend-config.sxp
   #(xend-tcp-xmlrpc-server-ssl-key-file /path/to/key)

$ grep xend-tcp-xmlrpc-server-ssl-cert-file xend-config.sxp
   #(xend-tcp-xmlrpc-server-ssl-cert-file /path/to/cert)
```

**Remediation:** Enabling a certificate and key will require the `tcp-xmlrpc` server to use only SSL connections. Set the `xend-tcp-xmlrpc-server-ssl-key-file` and `xend-tcp-xmlrpc-server-ssl-cert-file` to point to the server's certificate and key files.

```
(xend-tcp-xmlrpc-server-ssl-key-file /path/to/key)
(xend-tcp-xmlrpc-server-ssl-cert-file /path/to/cert)
```

## *3.13. Disable Core Dumps*

**Description:** Prevent Xen from creating a core dump on crash.

**Rationale:** Core dumps can contain sensitive information or provide aid to an attacker. Unless a specific Xen issue is being debugged or traced, prevent debugging dumps from being created if Xen crashes.

**Recommendation Level:** L1

**Scorable**: Yes

**Audit:** Inspect the `xend-config.xsp` file to ensure the `enable-dump` parameter is set to 'no'.

```
$ grep enable-dump xend-config.sxp
      (enable-dump no)
```

**Remediation:** Edit `xend-config.sxp` and set the `enable-dump` parameter to ‘no’.

```
(enable-dump no)
```

## 3.14. Disable VNC Interface

**Description:** Disable the VNC interface for administration of Xen Domains.

**Rationale:** If the VNC interface will not be used for administration, disabling this feature will help reduce the attack surface of Xen.

**Recommendation Level:** L1

**Scorable**: Yes

**Audit:** Inspect `xend-config.sxp` to ensure the `vnc-listen` parameter is unset or commented out.

```
$ grep vnc-listen xend-config.sxp
         (vnc-listen )
```

**Remediation:** Ensure the `vnc-listen` parameter has no value or is commented out.

```
#(vnc-listen)
```

## 3.15. Specify VNC Bind Interface

**Description:** Ensure the VNC interface can only listen on the `localhost` or management network interface.

**Rationale:** The VNC interface should not be accessible to any networks other than those needed for management and the local host. Ensure that the VNC server can only accept connections originating from those network segments.

**Recommendation Level:** L1

**Scorable**: Yes

**Audit:** Inspect `xend-config.sxp` to ensure the `vnc-listen` parameter is set to `localhost` or a management network address:

```
$ grep vnc-listen xend-config.sxp
      (vnc-listen ‘localhost’)
```

**Remediation:** Set the `vnc-listen` property to ‘`localhost’`

```
(vnc-listen ‘localhost’)
```

## 3.16. *Set VNC Password*

**Description:** Ensure the VNC password is set to require authentication.

**Rationale:** Require the VNC server validate a password before allowing a session to be established. Requiring a password should be the minimum level of security for VNC authorization.

**Recommendation Level:** L1

**Scorable**: Yes

**Audit:** Inspect `xend-config.sxp` to ensure the *`vncpasswd`* parameter is set to a strong password.

```
$ grep vncpasswd xend-config.xsp
   (vncpasswd ‘’)
```

**Remediation:** Set the *`vncpasswd`* parameter in `xend-config.sxp` to a strong password.

```
(vncpasswd ‘5tr0ngP455w0rd!’)
```

## 3.17. *Use TLS for VNC*

**Description:** Enable TLS for the VNC server

**Rationale:** VNC sessions are sent across the network unencrypted. Without encryption, an attacker can intercept session information, including the VNC password used for authentication.

**Recommendation Level:** L1

**Scorable**: Yes

**Audit:** Inspect `xend-config.sxp` to ensure the `vnc-tls` parameter is set to ‘1’.

```
  $ grep vnc-tls xend-config.sxp
     #(vnc-tls 1)
```

**Remediation:** Set the `vnc-tls` parameter in `xend-config.sxp` to ‘1’.

```
   (vnc-tls 1)
```

## 3.18. Set Absolute Path for VNC Cert Directory

**Description:** Ensure that the certificates directory is set to an absolute path and not a relative path or symbolic link.

**Rationale:** If an attacker can alter the directory containing the certificate and key for the VNC server they can compromise the security of the TLS connection. Ensuing that an absolute path is used helps mitigate this risk.

**Recommendation Level:** L1

**Scorable**: Yes

**Audit:** Inspect `xend-config.sxp` to ensure the *`vnc-x609-cert-dir`* parameter points to a non-symbolic link absolute path.

```
  $ grep vnc-x609-cert-dir xend-config.sxp
        (vnc-x509-cert-dir /etc/xen/vnc)

  $ ls –al /etc/xen/vnc/*
```

**Remediation:** Change the directory to an absolute path and verify that the directory and certificate files are not symbolic links.

```
   (vnc-x509-cert-dir /etc/xen/vnc)
```

## 3.19. Require User Client Certificate for VNC Authentication

**Description:** Require a Client certificate for the TLS session.

**Rationale:** Requiring a client certificate for the VNC session provides considerably more security than a password alone. Use of client certificates also ensures the identity and integrity of both the client the VNC session.

**Recommendation Level:** L2

**Scorable**: Yes

**Audit:** Inspect `xend-config.sxp` to ensure the *`vnc-x509-verify-1`* parameter is set to ‘1’.

```
$ grep vnc-x509-verify-1 xend-config.sxp
   #(vnc-x509-verify 1)
```

**Remediation:** Set the *`vnc-x509-verify-1`* parameter in `xend-config.sxp` to ‘1’.

```
(vnc-x509-verify 1)
```

## 3.20. Set File Permissions for VNC Certificate and Key

**Description:** Ensure that secure file system permissions have been set on the VNC certificate and key file.

**Rationale:** A local user that has access to the certificate and key file could replace them with their own and compromise the security of the TLS session.

**Recommendation Level:** L1

**Scorable**: Yes

**Audit:** Inspect the permissions on the certificate and key files:

```
$ ls –al <certfile> <keyfile>
```

**Remediation:**

```
$ chmod 755 <certfile>
$ chmod 400 <keyfile>
```

## 3.21. Isolate Management Network

**Description:** Isolate the Host Domain's networking resources both physically and logically from the untrusted domains.

**Rationale:** If an untrusted domain successfully attacks Host Domain then the security of all the hosted Guest Domains is compromised. Place Host Domain hosts on a logically isolated networking segment for management and interface by the IT staff. This networking segment should not be accessible from the Guest Domains. Physically separate the Host Domain from the Guest Domains by assigning one networking interface card to the trusted Domains and one to the untrusted Domains.

**Recommendation Level:** L2

**Scorable**: No

**Audit:** N/A

**Remediation:** N/A

## 3.22. Disable PCI Permissive Devices

**Description:** Disable or remove entries from the PCI permissive list.

**Rationale:** The PCI permissive list allows direct access to hardware from an untrusted domain. Direct access from a Guest Domain could allow for a DMA write to be issued by an attacker inside of a Guest Domain, which could in turn allow a Guest Domain to overwrite or alter the memory contents of another Guest Domain or the Host Domain. This will quickly lead to system compromise. Consider dedicating an entire physical host if direct hardware access is required.

**Recommendation Level:** L1

**Scorable**: Yes

**Audit:** Ensure that the boot loader configuration file does not include the `pciback.permissive` kernel parameter setting.

```
    $ cat xend-pci-permissive.sxp
```

**Remediation:** Remove entries from the `xend-pci-permissive.sxp` and Grub configuration files. Migrate the virtual host to a physical resource.

# 4.Domain Configuration

## *4.1. Restrict File System Permissions on the Kernel and Ramdisk Files*

**Description:** Ensure that access rights are properly restricted for the kernel and ram disk files used in the Xen Guest Domain.

**Rationale:** A malicious user with access to the kernel or ramdisk files could replace them with their own or simply delete them, causing a Denial of Service to the Guest Domain. Verify that file system permissions are set to mitigate this risk.

**Recommendation Level:** L1

**Scorable**: No

**Audit:** Inspect the file permission on the kernel and ramdisk file:

```
$ ls –al /path/to/kernel /path/to/ramdisk
```

**Remediation:** Change to secure file system permissions

```
$ chmod 750 /path/to/kernel
$ chmod 750 /path/to/ramdisk
```

## *4.2. Inspect File Permissions on the Virtual Disk Files*

**Description:** Inspect access rights for the virtual disks used in the Xen Guest Domain.

**Rationale:** An attacker able to alter or replace the file systems used for the untrusted domains could easily compromise or Denial of Service (DoS) the system. Ensure that only proper administrators and owners have file system rights to their images.

If file systems are being mounted across a network special care must be taken to ensure the integrity and permissions of the virtual disks stored remotely.

**Recommendation Level:** L1

**Scorable**: Yes

**Audit:** Inspect the file permission on virtual disk files:

```
$ ls -al /path/to/virtualdiskfile
```

**Note:** Other audit features will be needed for remote file systems and will have to be evaluated on a case by case basis. The path to the virtualized disk file can be found in the `disk = ['file:/path/to/the/root/file, hdb1,w']` parameter in the Domain configuration file.

**Remediation:** Apply proper permissions for the UNIX user, group, or mount point.

```
$ chmod 760 /path/to/virtualdiskfile
```

## *4.3. Use Absolute Path for Kernel, Ramdisk file*

**Description:** The kernel and ramdisk paths should be set as an absolute and not a relative path or symbolic link.

**Rationale:** An attacker able to alter or replace the kernel files used for the untrusted domains could easily compromise or DoS the system.

**Recommendation Level:** L1

**Scorable**: No

**Audit:** Inspect the domain configuration file to ensure the `kernel` and `ramdisk` parameters point to absolute paths.

```
kernel = ‘/path/to/image’
ramdisk = ‘/path/to/ramdisk’
```

**Remediation:** Set `kernel` and `ramdisk` parameters to point to absolute paths.

```
kernel = ‘/path/to/image’
ramdisk = ‘/path/to/ramdisk’
```

## *4.4. Use Absolute Path for Virtual Disks*

**Description:** The virtual disk paths should be set as an absolute and not a relative path or symbolic link.

**Rationale:** An attacker able to alter or replace the disk images used for the untrusted domains could easily compromise or DoS the system.

**Recommendation Level:** L1

**Scorable**: No

**Audit:** Check the domain configuration file disk settings for each of the image files for the Xen hosts. The path for each disk will correspond to the entry in the domain confile file. Ex. `disk = ['file:/path/to/the/root/file, hdb1,w']`

```
$ grep disk domain_config_file
```

**Remediation:** Alter the path settings to be an absolute path.

## 4.5. Bind VNC Server to Specific Interface

**Description:** Bind the VNC server to a specific network interface.

**Rationale:** If the default setting from the Xend configuration file is modified, make sure that the VNC server is only available on the `localhost` or the intended administrative networking segment.

**Recommendation Level:** L1

**Scorable**: Yes

**Audit:** Inspect the domain file to ensure the `vnclisten` parameter is set to ‘`127.0.0.1`’.

```
$ grep vnclisten domainfile
   vnclisten=”127.0.0.1”
```

**Remediation:** Set the `vnclisten` parameter to ‘`127.0.0.1`’.

```
 vnclisten=”127.0.0.1”
```

## 4.6. Set VNC Password

**Description:** Set an appropriately strong VNC password for administration and connecting to the Domain.

**Rationale:** If the default setting from the Xend configuration file is modified, ensure that the VNC server password is set and uses a strong password for authentication.

**Recommendation Level:** L1

**Scorable**: Yes

**Audit:** Inspect the domain file to ensure the *`vncpasswd`* parameter is set to a strong password.

```
$ grep vncpasswd domainfile
      vncpassword=’’
```

**Remediation:** Set the `vncpasswd` parameter to a strong password.

```
vncpassword=’5tr0ng!p455w0rd#’
```

## 4.7. Disable or Restrict Root Login from Serial Console

**Description:** Ensure root user is not capable of logging in via a serial console.

**Rationale:** Audit and access controls are best maintained by requiring users to login and then escalate to root or Administrative privileges.

**Recommendation Level:** L2

**Scorable**: Yes

**Audit:** Inspect `/etc/securetty` for entries that allow root login via a Xen console device.

```
$ cat /etc/securetty
      tty0
      #tty1
      #tty2
```

**Remediation:** Remove the device entry from the `/etc/securetty` file.

```
#tty0
```

```
   #tty1
   #tty2
```

# 5. XenServer 4.0.1

## 5.1. Configure SSH

**Description:** Configure the SSH server to be secure by default and disable legacy authentication mechanisms.

**Rationale:** SSH is used to securely administer and update the Xen server. The configuration of the SSH daemon must be configured in the securest state while allowing for administrative tasks to be performed.

**Recommendation Level:** L2

**Scorable**: Yes

**Audit:**

```
grep PermitRootLogin /etc/ssh/sshd_config
grep Banner /etc/ssh/sshd_config
grep X11Forwarding /etc/ssh/sshd_config
grep IgnoreRhosts /etc/ssh/sshd_config
grep RhostsAuthentication /etc/ssh/sshd_config
grep HostbasedAuthentication /etc/ssh/sshd_config
grep PermitEmptyPasswords /etc/ssh/sshd_config
```

**Remediation:**
Create `/path/to/banner` file

Ensure the following are set in `/etc/ssh/sshd_config`:

```
Banner /path/to/file
X11Forwarding no
RhostsAuthentication no
HostbasedAuthentication no
PermitEmptyPasswords no
PermitRootLogin no
```

Restart `sshd` server `/etc/init.d/sshd restart`

## 5.2. Create a Non Privileged User for Management of Xen Server

**Description:** Create a regular user for login and administration of the Xen server.

**Rationale:** During installation only a root user is created for administration of the XenServer. The root user should not be used as a default login for the system. Proper account management and authentication should be utilized.

**Recommendation Level:** L2

**Scorable**: Yes

**Audit:** N/A

**Remediation:** Create a non privileged user account for Xen management and set a password for the account.

```
# useradd username
# passwd username
```

## *5.3. Create a Management Group for Xen*

**Description:** Create a group for the management of Xen and access to Xen binaries.

**Rationale:** Creating a group for Xen management maintains proper delegation of duties and roles on the host system.

**Recommendation Level:** L2

**Scorable**: Yes

**Audit:** Inspect *`/etc/group`* to ensure the existence of the *`'xen'`* group.

```
$ grep xen /etc/group
```

**Remediation:** Create a group for managing Xen and add all Xen administrators to this group.

```
# groupadd xen
# usermod -a -G xen <Xen administrator username>
```

## *5.4. Create a Sudoers Command Alias for Xen*

**Description:** Create a command alias to separate Xen groups from the other administrative roles.

**Rationale:** A sudoers role that is specific to the management and administration of Xen allows the owner of the Xen server to delegate specific responsibilities to administrators. This separation of roles reduces the number of individuals with need for root credentials.

**Recommendation Level:** L2

**Scorable**: No

**Audit:** Inspect */etc/sudoers* to ensure a XEN entry exists.

```
# grep XEN /etc/sudoers
```

**Remediation:** Add the following to /etc/sudoers

```
Cmnd_Alias XEN = /opt/xensource/bin/database-upgrade.sh,
/opt/xensource/bin/set-domain-uuid, /opt/xensource/bin/xe-mount-
iso-sr, /opt/xensource/bin/diskprep, /opt/xensource/bin/xapi,
/opt/xensource/bin/xe-set-iscsi-iqn,
/opt/xensource/bin/fix_firewall.sh, /opt/xensource/bin/xapi-
autostart-vms, /opt/xensource/bin/xe-toolstack-restart,
/opt/xensource/bin/list_domains, /opt/xensource/bin/xapi-wait-
init-complete, /opt/xensource/bin/metadata_upgrade,
/opt/xensource/bin/xe, /usr/bin/xencons, /usr/bin/xenstore-chmod,
/usr/bin/xenstore-ls, /usr/bin/xentrace, /usr/bin/xen-detect,
/usr/bin/xenstore-control, /usr/bin/xenstore-read,
/usr/bin/xentrace_format, /usr/bin/xeninfo, /usr/bin/xenstore-
exists, /usr/bin/xenstore-rm, /usr/bin/xentrace_setsize,
/usr/bin/xenperf, /usr/bin/xenstore-list, /usr/bin/xenstore-
write, /usr/sbin/xenbaked, /usr/sbin/xenmon.py,
/usr/sbin/xenperf, /usr/sbin/xentop, /usr/sbin/xen-bugtool,
/usr/sbin/xenmon.pyc, /usr/sbin/xen-python-path,
/usr/sbin/xentrace_setmask, /usr/sbin/xenconsoled,
/usr/sbin/xenmon.pyo, /usr/sbin/xenstored
```

## *5.5. Assign the Xen Group to the Xen Command Alias*

**Description:** Assign the Xen command privileges to the Xen group.

**Rationale:** This segments Xen administrated privileges to those assigned to the xen group. This further separates the Xen role from other system management privileges.

**Recommendation Level:** L2

**Scorable**: No

**Audit:** Inspect */etc/sudoers* to ensure `%xen` is set:

```
# grep /etc/sudoers %xen
```

**Remediation:** Add the following line to `/etc/sudoers`

```
%xen ALL = XEN
```

## 5.6. Enable Shadow Passwords

**Description:** Create `shadow` and `gshadow` files to be utilized by Xen server authentication systems.

**Rationale:** By default the Xen server does not ship with shadow password files. This prevents the authentication system from storing the password hash in the shadow file. As a result the hashes are stored in the `/etc/password` file which is world readable.

**Recommendation Level:** L2

**Scorable**: Yes

**Audit:** Inspect the file system to ensure */etc/shadow* and */etc/gshadow* exist:

```
$ ls /etc/shadow /etc/gshadow
```

**Remediation:** Create */etc/shadow* and */etc/gshadow* then set secure permissions on these files.

```
# touch /etc/shadow
# touch /etc/gshadow
# chmod 640 /etc/shadow
# chmod 640 /etc/gshadow
```

## 5.7. Change the Root Password

**Description:** Rehash the root account password with the MD5 or stronger algorithm.

**Rationale:** By default, the Xen root password is stored with the crypt function instead of the MD5 function. Calling `passwd` will store the root password using the MD5 algorithm.

**Recommendation Level:** L2

**Scorable**: No

**Audit:** Inspect `/etc/password` to ensure

```
$ grep -e '^root:' /etc/passwd
```

**Remediation:** Execute *`passwd`* as root.

```
# passwd
```

## 5.8. Migrate All Existing Accounts to the Shadow and Gshadow Files

**Description:** Remove the user password hashes from the `passwd` file after the creation of the shadow files. Require all users to change their passwords on the Xen servers.

**Rationale:** Migration and rotation of the user accounts and passwords will secure hashes that were exposed via the `passwd` file.

**Recommendation Level:** L2

**Scorable**: Yes

**Audit:** Inspect `/etc/passwd` for entries that are not shadowed:

```
$ grep -v -e '^.*\?:x' /etc/passwd
```

**Remediation:** Execute `passwd` for each user:

```
$ passwd <username>
```

Replace password hashes in `/etc/passwd` file with an 'x':

```
username:h45h0fp4ssw0rd:1:1:group:/home/dir:/bin/shell

becomes

username:x:1:1:group:/home/dir:/bin/shell
```

# Appendix A: sHype Example

## Enabling ACM

The sHype security module relies on an ACM enabled Xen hypervisor. These steps can be skipped if using the default RHEL5 Xen install.

Step 1: Download and unpack the Xen source tar ball from the Xen site.
Step 2: Edit the `Config.mk` file in the top level Xen directory and make the following modifications:

```
XSM_ENABLE ?= n to XSM_ENABLE ?= y

ACM_SECURITY?=n to ACM_SECURITY ?= y
```

**Note:** only one of ACM or FLASK can be enabled.

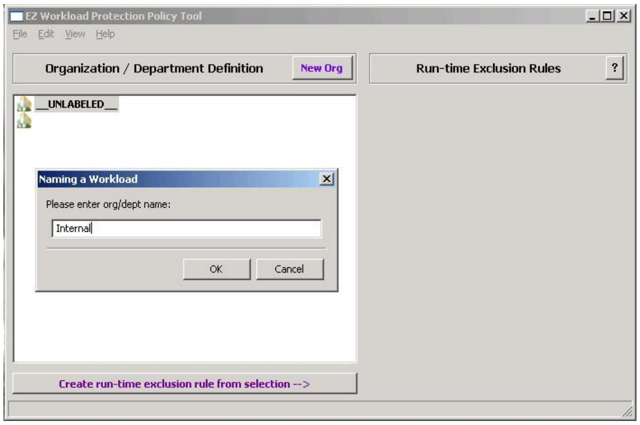
Step 3: Recompile Xen

```
# make world
# make install
# reboot
```

## Creating ACM Policy

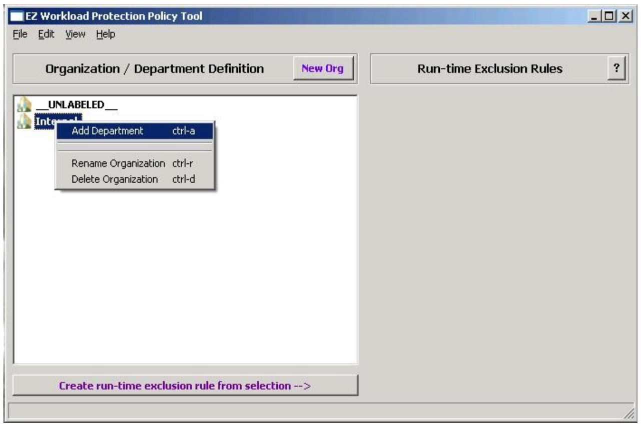
Using the `xensec_ezpolicy` editor including with the Xen tools is the easiest way to create a policy. Running this tool will require that both Python and the WxGTK framework are installed.

Step 1: Create a new workload by clicking the New Org button. This example will call the new org Internal.

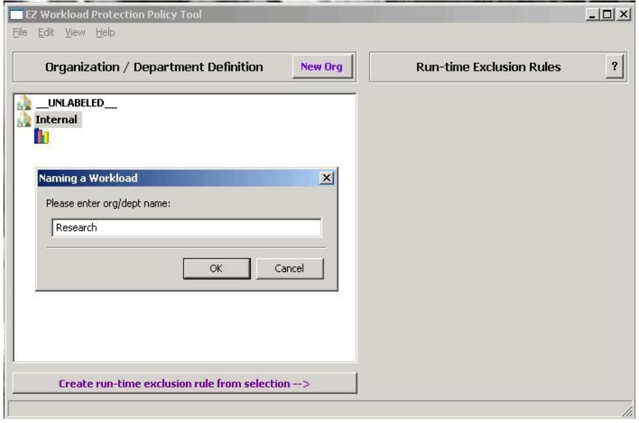

EZ Workload Protection Policy Tool
File Edit View Help
Organization / Department Definition
New Org
Run-time Exclusion Rules
?
__UNLABELED__
Naming a Workload
OK
Cancel
Create run-time exclusion rule from selection -->

Please enter org/dept name: Internal

Step 2: Right click on the organization that is created and select Add Department.

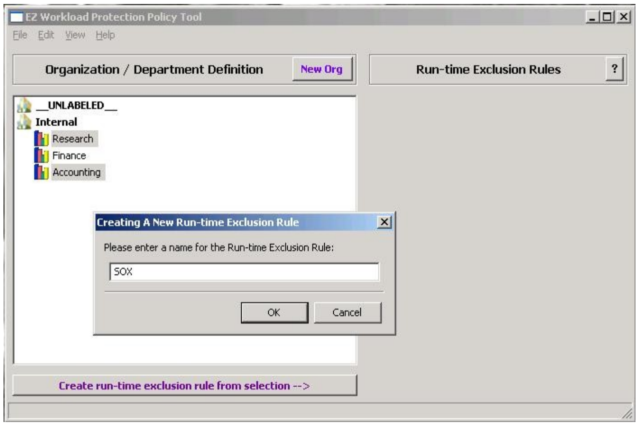

EZ Workload Protection Policy Tool
File Edit View Help
Organization / Department Definition
New Org
Run-time Exclusion Rules
?
__UNLABELED__
Add Department ctrl-a
Rename Organization ctrl-r
Delete Organization ctrl-d
Create run-time exclusion rule from selection -->

Step 3: Fill in a department name for each of the three examples. Research, Finance, and Accounting.


EZ Workload Protection Policy Tool
File Edit View Help
Organization / Department Definition
New Org
Run-time Exclusion Rules
?
__UNLABELED__
Internal
Naming a Workload
OK
Cancel
Create run-time exclusion rule from selection -->

Please enter org/dept name: Research

Step 4: Select the domains that will run mutually exclusive from each other and click "Create run-time exclusion rule from selection"

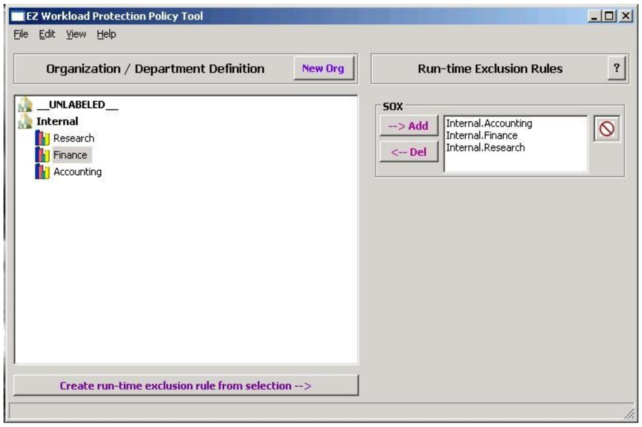


EZ Workload Protection Policy Tool
File Edit View Help
Organization / Department Definition
New Org
Run-time Exclusion Rules
?
__UNLABELED__
Internal
Research
Finance
Accounting
OK
Cancel
Create run-time exclusion rule from selection -->

Creating A New Run-time Exclusion Rule

Please enter a name for the Run-time Exclusion Rule:

SOX

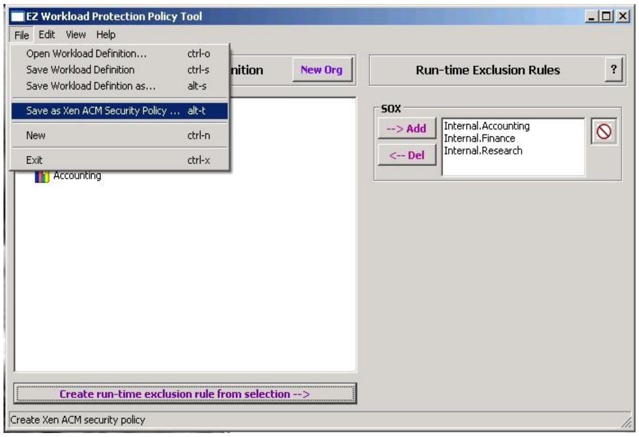


EZ Workload Protection Policy Tool
File Edit View Help
Organization / Department Definition
New Org
Run-time Exclusion Rules
?
__UNLABELED__
Internal
Research
Finance
Accounting
--> Add
<-- Del
Create run-time exclusion rule from selection -->

SOX

Internal.Accounting
Internal.Finance
Internal.Research

Step 5: Save the policy as a Xen ACM Security Policy. By default the policy file will be saved in the `/etc/xen/acm-security/policies` directory. Assign this policy the name `test-security_policy.xml`.



EZ Workload Protection Policy Tool
File Edit View Help
Open Workload Definition... ctrl-o
Save Workload Definition ctrl-s
Save Workload Defintion as... alt-s
Save as Xen ACM Security Policy ... alt-t
New ctrl-n
Exit ctrl-x
nition
New Org
Run-time Exclusion Rules
?
Accounting
--> Add
<-- Del
Create run-time exclusion rule from selection -->

SOX

Internal.Accounting
Internal.Finance
Internal.Research

Create Xen ACM security policy

Apply the policy using the xm command.

```
# xm setpolicy ACM test
```

The system must be rebooted for the changes to take effect.

```
  # reboot
```

Upon reboot check that the policy has been applied with:

```
  # xm getpolicy
```

Now that the ACM system has been enabled and the policy is set. The next step is to apply labels that map domains to policy.

List the current labels:

```
  # xm labels type=dom
```

Add a label to a domain:

```
  # xm  addlabel <label name> dom <domname>

 i.e.  xm add label Research dom Research_D1.xm
```

Boot the domain:

```
  # xm create <domain_name>
```

List the current domain label:

```
# xm list –label or xm getlabel <res|domain-id> <resource /configfile>
```

# Appendix B: Change History

| Version | Date | Changes |
|---|---|---|
| 1.0.0 | 5/2008 | Initial Public Release |