
Linux Academy
Red Hat Certificate of Expertise in Server Hardening
Introduction

## Introduction

- About Linux Academy
- Let’s see the features available to you as a member

## Prerequisites

- What do you need before taking this course or the exam?
- Red Hat Certified System Administrator or comparable work experience and skills.
- Experience with server hardening and concepts will help.
- If you intend to do the exam, also review the exam objectives on the Red Hat exam page: https://www.redhat.com/en/services/training/ex413-red-hat-certificate-expertise-server-hardening-exam
- At the time of course creation, the exam is based on Red Hat Enterprise 6.

## Red Hat Documentation

- In the downloads section of the course are several Red Hat documents:
  - Red Hat Enterprise Linux 6 Security guide.
  - Red Hat Enterprise Linux 7 Security guide.
  - Red Hat Enterprise Linux 6 SE Linux guide.
  - Red Hat Enterprise Linux 7 SE Linux guide.
- The most updated versions of these guides can be found on the Red Hat website by clicking the links above or by going to the Red Hat website directly.
- Use of Red Hat Documentation is provided as a courtesy.
  The Linux Academy is in no away affiliated with Red Hat, Inc., and this course is not provided or reviewed by Red Hat, Inc.

## Why Server Hardening?

- The internet wasn't designed for security. Any security features have all been added later.
- Within a very short time of a new server being available on the internet it will be scanned for vulnerabilities. It’s best not to have any.
- You have a duty of care for your organization to ensure its as secure as you can make it from unauthorized access.
- There have been well-publicized breaches to systems at large and small organizations.
- So even small companies, non profits, and home systems are targets.
- Attack tools are easy to obtain and easy to use.
- Controls - Physical, Technical, Administrative.


Linux Academy
Red Hat Certificate of Expertise in Server Hardening
Identify Red Hat Common Vulnerabilities and Exposures

## Standard Security Model

- There is a Standard Security Model. It's called the CIA Security Model.
- **C**onfidentiality. Provide sensitive info to only predefined individuals
- **I**ntegrity. Unauthorized users are unable to change or destroy data.
- **A**vailability. Should be accessible to authorized users whenever needed.
- SELinux, which is an enhancement to the Linux kernel.

## Online tools - CVE & RHSA

- Red Hat Common Vulnerabilities and Exposures (CVEs)
- Red Hat Security Advisories (RHSA)
- Red Hat URL for security advisories: https://access.redhat.com/security/security-updates/#/security-advisories
- Mitre CVE - http://cve.mitre.org
- NIST NVD, which is built upon and fed by the CVE list: https://nvd.nist.gov/general/nvd-dashboard

## Alerts on Vulnerabilities

- On the Red Hat portal, you can set up alerts
- Log in to the Red Hat Portal
- Navigate to this URL and enter your details: https://access.redhat.com/security/security-updates/#/security-advisories

## Checking with yum

- yum install yum-plugin-security
- yum updateinfo
- yum updateinfo list
- yum updateinfo list --sec-severity=Critical
- yum updateinfo list --sec-severity=Moderate
- Let’s have a look at this on a server


Linux Academy
Red Hat Certificate of Expertise in Server Hardening
Verify package security and validity

## yum Security Features

- Download software from trusted sources
- Verify signed packages
- Red Hat packages are signed with GPG keys
- You can import GPG keys
- You can display GPG keys


Linux Academy
Red Hat Certificate of Expertise in Server Hardening
Identify and Employ Standards-based Practices

## Common Standards

- Physical protection - People having physical access to the servers.
  - Secured datacenters - no unauthorized access.
  - BIOS password.
  - No booting from alternate methods - e.g CD-ROM.
- Virtual or server based protections
  - Latest version of OS
  - Separated partitions
    - /var
    - /var/log
    - /var/audit
    - /home
    - /tmp

## Common Standards

- Firewall installed (network and/or server) and configured.
- Sticky bit on world writeable directories.
- Register servers with Red Hat Satellite (patch updates)
- Ensure you have Red Hat GPG key and it’s enabled.
- Remove legacy services where possible.
- Disable services that wont be used.
- Set SSH protocol to 2.
- Set SSH loglevel to info.
- Disable root login from remote.
- Set SSH permit empty passwords to no.
- Use software such as AIDE or OSSEC

## Encrypted file systems

- Data at rest.
- Full disk encryption.
  - Red Hat uses LUKS (Linux Unified Key Setup-on-disk-format).
  - Natively supported.
  - Bulk encrypts your drive.
  - Data is protected when computer is off or drive unmounted.
  - Default cipher is aes-cbc-essiv:sha256 - 256bits by default
  - Anaconda, by default, uses AES cipher in XTS mode, aes-xts-plain64.
  - Anaconda default LUKS key size is 512 bits.
- File based encryption can be used.

## Btrfs

- Creating file systems
- Btrfs - designed by oracle.
- Uses B-tree file system.
- B-tree is optimized for systems that read and write large blocks of data. B-trees are a good example of a data structure for external memory. It is commonly used in databases and filesystems.
- Access to data in a file is quick.
- Uses copy-on-write.
- Some features.
  - Cloning (as mentioned).
  - Snapshots.
  - Subvolume (like a folder but can be mounted separately).
  - Quota groups.

## Ext4

- Next step up from ext3.
- Backward compatible with ext3.
- Unlimited number of folders.
- Better performance than ext3.
- Larger storage limits - 1 Exabyte.

## XFS

- Default FS for RHEL 7.
- High performance.
- Also a journaled file system like ext4
- 64-bit (8 Exabyte)

## Security Properties for Mounting Filesystems

- There are several things to be aware of when mounting filesystems that could affect security and stability of your servers.
- These are some of the properties that would be used when mounting a drive, whether through the mount command or the /etc/fstab
- async/sync - How data is stored when a write is made.
- atime/noatime - File accessed timestamp.
- dev/nodev - whether to allow a device file on the drive.
- rw/ro – Read/write or read only.
- suid/nosuid - Allow a user to run a program as root.
- exec/noexec - turn off executable files on the file system.
- The defaults when you mount are:
  - rw, suid, dev, exec, auto, nouser, async.

## Ext4

- ext4 is a journaling file system.
- The mount options go in the /etc/fstab or on the mount command.
- Let's discuss some ext4 mount options to think about:
  - journal_checksum - enables check summing of the journal transactions.
  - barrier=0 | barrier = 1 - Enable or disable write barriers.
  - delalloc | nodelalloc - How disk blocks are allocated.

## XFS

- XFS is the now the default file system for RHEL 7.
- The mount options go in the /etc/fstab or on the mount command.
- attr2 | no attr2 - Extended attributes available for XFS.
- Quota journaling - No need for quota consistency checks after crash.
- Project/directory quotas - Quota restrictions over a directory tree.
- Sub second timestamps - This allows timestamps to go to the subsecond.
- barrier | nobarrier - Enable or disable write barriers.
- discard | nodiscard - How free space is reclaimed.
- grpid | no grpid - Similar to SGID (set group id).
- Large disk support for inodes - inode64.
- XFS quotas can be enabled at mount time.
    - includes a noenforce option.

## SUID

- setuid allows a user to run an executable file with the permissions of the files owner.
- Often used to temporarily elevate privileges, but doesn't have to be.
- Is needed for proper system use.
- Normal users who can execute the file gain the privileges associated with the file.
- Useful but can be dangerous.
- Some filesystems can be set to ignore the setuid attribute.
- Search filesystems for suid programs.
- Disable unnecessary suid programs.
- Audit the filesystem regularly.
- chmod u+s file & chmod u-s file to remove it.
- chmod 4750 file & chmod 0750 file to remove it.

## SGID

- sgid is similar to suid.
- sgid in directories.
  - Files ownership is normally based on who creates a file.
  - In sgid directory, files are owned by the group owner instead.
- chmod 2775 file to add & chmod 0775 file to remove
- chmod g+s file to add & chmod g-s file to remove.

## Sticky Bit

- A sticky bit is used on folders to avoid file deletion by users who don't own the file.
- When a sticky bit is enabled:
  - Owner of file can delete it.
  - Owner of directory can delete it.
  - The root use can delete it.
- It modifies the meaning of the write permission.
- chmod o+t directory or remove with chmod o-t directory.
- chmod 1xxx directory or remove with 0xxx directory.

## File Access Control List

- File access control lists or FACL.
- Control access to an individual level for folders or files.
- Normally enabled for new installations of Red Hat or CentOS.
- May need to enable the option in /etc/fstab or mount if new filesystem.
- Support is in the kernel.
- To set or remove use setfacl.
- To look at the FACL use getfacl.
- There is a mask option to set maximum permissions.
- The mask option can quickly change effective permissions.
- Better to use mask than delete individual permissions.

## setfacl

- Command format is - setfacl -m ACL file|directory.
- The ACL looks like the following.
  - [d[efault]:}] [u[ser]:] uid [:perms]
  - [d[efault]:}] [g[roup]:] gid [:perms]
  - [d[efault]:}] [o[ther][:] [:perms].
    You don't need to use an ACL for other, as normal permissions work instead
  - [d[efault]:}] [m[ask][:] [:perms]
- Examples to set rw- perms on a file as follows:
  - setfacl -m user:sue:rw- file.txt
  - setfacl -m u:sue:rw- file.txt
  - setfacl -m u:sue:6 file.txt
- The getfacl command works as shown below:
  - getfacl file.txt

## setfacl - mask

- The mask setting.
- Allows for quick changes to settings as it sets maximum permissions.
- The mask does not affect the owner or 'others' settings.
- Preferred over deleting all ACLs

## setfacl - default

- The default option sets the defaults for new items.
- If set on a folder, all new files from user or group inherit the 'default' permissions.
- Enabled by using d or default on the setacl command.
- Some examples that set permissions for the user sue in the folder payroll:
  - setfacl -m d:user:sue:rw- payroll
  - setfacl -m d:u:sue:rw- payroll
  - setfacl -m default:u:sue:6 payroll
- Any new files created by sue inherits the permissions shown above.

## setfacl - delete

- It’s simply to delete a FACL.
- Use the -x option.
- setfacl -x :u:sue:rw- file.txt


Linux Academy
Red Hat Certificate of Expertise in Server Hardening
Install and Use Intrusion Detection

## Intrusion Detection - AIDE

- Intrusion detection, detect (possibly also respond) to system breach.
- Better to not be breached, but if you have an intruder, know about it.
- AIDE - Advanced intrusion detection environment.
- It is a file and directory integrity checker.
- AIDE creates a database from rules (regular expression).
- Database needs to be initialized.
- AIDE can verify the integrity of files.
- Uses digest algorithms to check file integrity.
- File attributes can be checked for inconsistencies.

## AIDE - cont.

- Install with **yum install aide**
- The files to be monitored are in /etc/aide.conf
- Build the baseline database.
  - /usr/sbin/aide --init
  - Creates db at /var/lib/aide/aide.db.new.gz
- Now the baseline is built. Copy it to where you can check it regularly.
- copy /var/lib/aide/aide.db.new.gz to /var/lib/aide/aide.db.gz
- Integrity checking as follows:
  - /usr/sbin/aide --check
- Put it into your cron file. You can edit the /etc/crontab and change the MAILTO: root to be your email address so email from cron goes to you. Save that and exit.
- Add a daily job to run everyday. Put the following into the root crontab.
- 0 1 * * * /usr/sbin/aide --check

## Intrusion Detection - OSSEC

- OSSEC - Open source intrusion detection.
- Scalable multi-platform.
- Server and client available.
  - Can use a central server and have the clients report back.
- Runs on Linux, OpenBSD, FreeBSD, MacOS, Solaris, Windows.
- Download from https://ossec.github.io/
- Source install or via yum.
- Yum install via the atomic repository.
  - **wget -q -O - http://www.atomicorp.com/installers/atomic | sh**
  - Should also have the epel repository installed.
  - yum install ossec-hids ossec-hids-server
- Adjust the config file - /var/ossec/etc/ossec.conf for:
  - your email & your email server & send from.
- Start the service


# Red Hat Certificate of Expertise in Server Hardening

## Account and Group Security

## User Accounts

- Note:  Expected that users have experience with user management.
- User accounts have 3 types of files associated with them:
  - /etc/passwd
  - /etc/shadow
  - /etc/group
- Manage users with:
  - useradd
  - usermod
  - userdel

## Password Ageing

- Password ageing is setting passwords to expire after certain criteria are met.
- Corporate policy, makes sense.
- Force users to change passwords.
- Files used for password ageing policies:
  - /etc/default/useradd
  - /etc/login.defs
  - Can use PAM (Pluggable Authentication Modules).

## Group Account Security

- Regular permissions set onto files and folders.
- Use the chown or chgrp commands to change group.
- Use groupadd to create new group.
- SGID - discussed under configure default permissions section.
  - chmod g+s FOLDER
  - Note:  s means x+s and S means just setgid no x permissions set.
- Group passwords.
  - /etc/gshadow
  - group - log in to new group
  - gpasswd - administer group users.
- Can add users as group administrators.
  - gpasswd [option] GROUP
  - Only sysadmin (root) can add group admins.


# Red Hat Certificate of Expertise in Server Hardening

## Manage System Login Security Using Pluggable Authentication Modules (PAM)

## PAM

- Pluggable Authentication Modules.
- Provides a common framework for authentication and security.
- Central authorization and authentication.
- The /etc/pam.d contains pam configuration files.
- Each PAM-aware application or *service* has a file in the **/etc/pam.d/** directory. Each file in this directory has the same name as the service to which it controls access.
- Modules/Libraries are located in /usr/lib64/security.
- Docs can be found under /usr/share/doc/pam-x.x.x  (x.x.x=version)

## Modules

- PAM config files contain directives which define the modules.
- Directives are as follows:
  - *module_interface*
  - *control_flag*
  - *module_name*
  - *module_arguments*
- Module interfaces are defined as follows:
  - **auth** — This module interface authenticates use.
  - **account** — This module interface verifies that access is allowed.
  - **password** — This module interface is for changing user passwords.
  - **session** — This module interface configures and manages user sessions.
- Module interfaces are the first field defined.
- Second field is the Control field.
- Third field is the module and arguments.

## Control Flags

- Control flags tell PAM what to do with a success or failure of the PAM module.
  - **required -** Must be successful for authentication to continue.
  - **requisite -** Must be successful for authentication to continue.
  - **sufficient -** Ignored if it fails.
  - **optional -** Result is ignored.
  - **include -** This flag calls lines in the configuration file which match the given parameter and appends them as an argument to the module.
- Order of required flags not important.  Sufficient and requisites flags are.


Linux Academy
Red Hat Certificate of Expertise in Server Hardening
Console Security

## Console Security

- A Linux console is the main terminal used for the server.
- A Linux console provides a way for the kernel and other processes to send text output to the user, and to receive text input from the user.
- Also referred to as the system console.
- It is the console used when a system is brought to a single user mode.
- One of the first features of the kernel.
- Originally written by Linus Torvalds.
- Its an optional kernel feature, most servers have it enabled.
- Most embedded Linux systems do not enable it.
- In Linux, several devices can be used as system console:
  - A virtual terminal
  - Serial port
  - USB serial port
  - VGA in text-mode (monitor plugged into a server).
- VGA in text mode is what we will discuss here.

## Disable Ctrl-Alt-Del

- On CentOS 6, there was a software update that changed the method to disable Ctrl-Alt-Del. The file that causes init to handle it is /etc/init/control-alt-delete.conf.
- Note: If upstart package is prior to upstart-0.6.5-12 then the file to modify is /etc/init/control-alt-delete.conf.
- Note: Upstart > upstart-0.6.5-12 was enhanced to parse /etc/init/*.override files.
- File the version of upstart with **rpm -q upstart**

## Disable Ctrl-Alt-Del, cont.

- This is for **Red Hat 6 or CentOS 6**.
- For upstart **prior to upstart-0.6.5-12**.
- Directly modify the /etc/init/control-alt-delete.conf file.
- Note: future updates to the upstart may require you to make changes again.
- Comment out the line that says the following:
  - exec /sbin/shutdown -r now "Control-Alt-Delete pressed"
- Add a new line that says the following:
  - exec /usr/bin/logger -p authpriv.notice -t init "Ctrl-Alt-Del was pressed and ignored"
- This change will generate a log entry when crtl-alt-del is pressed but will not reboot the server.
- You should reboot the server to ensure this works properly.

## Disable Ctrl-Alt-Del, cont.

- This is for **Red Hat 6 or CentOS 6**.
- For upstart **newer than upstart-0.6.5-12**.
- Create /etc/init/control-alt-delete.override (which will not be affected by any package updates) and making desired changes there.
- cp -v /etc/init/control-alt-delete.conf /etc/init/control-alt-delete.override
- Comment out the line that says the following:
  - exec /sbin/shutdown -r now "Control-Alt-Delete pressed"
- Add a new line that says the following:
  - exec /usr/bin/logger -p authpriv.notice -t init "Ctrl-Alt-Del was pressed and ignored"
- This change will generate a log entry when crtl-alt-del is pressed but will not reboot the server.
- You should reboot the server to ensure this works properly.

## Disable Ctrl-Alt-Del, cont.

- This is for **Red Hat 7 or Centos 7**.
- You need to mask (disable) the service.
- systemctl mask ctrl-alt-del.target
- Note: The above steps will not disable the ctrl + alt + delete key combination in GUI mode. To disable it in GUI you change the keyboard settings.
- In GUI mode:
  - Navigate to Applications -> System Tools -> Settings -> Keyboard -> Shortcuts -> System Set value of “Logout” as Disabled.

## Console Security, cont.

- Configure the **BIOS** to disable booting from **CD/DVD**, **External Devices**
- Set GRUB password to protect server.
  - Stops someone from entering parameters on the boot line that could compromise security.
  - Stops access to single user mode.
  - Prevents access to insecure OS's that may also be installed.
- First create a password hash with grub-md5-crypt.
- Copy the MD5 hash.
- Edit /boot/grub/grub.conf and add the following line.
- password --md5 *<password-hash>*
- Replace *<password-hash>* with the value returned by **/sbin/grub-md5-crypt.**
- The next time the system boots, the GRUB menu prevents access to the editor or command interface without first pressing **p** followed by the GRUB password.


Linux Academy
Red Hat Certificate of Expertise in Server Hardening
Red Hat Identity Management

## Identity Management

- Red Hat Identity Management.
- A way to create identity stores, centralized authentication, domain control for Kerberos and DNS services, and authorization policies
- Identity Management provides a unifying skin for standards-defined, common network services, including PAM, LDAP, Kerberos, DNS, NTP, and certificate services, and it allows Red Hat Enterprise Linux systems to serve as the domain controllers.
- Identity Management defines a domain, with servers and clients that share centrally-managed services, like Kerberos and DNS.
- IdM server and an IdM replicas.
- Once an IdM server is set up, its configuration can be copied and used as the basis for another IdM server. When an IdM server is copied, that copy is called a *replica*.

## IM, cont.

- Clients are configured to interact with the IdM servers.
- A client is simply any machine which is configured to operate within the IdM domain, using its Kerberos and DNS services, NTP settings, and certificate services.
- Recommended prerequisites:
  - Red Hat enterprise 6.
  - For 10,000 users & 100 groups at least 2GB of RAM, 1GB swap space.
  - hostname must be a fully-qualified domain name. For example, **ipaserver.example.com**
- *yum install ipa-server bind bind-dyndb-ldap*


Linux Academy
Red Hat Certificate of Expertise in Server Hardening
Configure Remote System Logging

## Remote Logging

- Sending logs to a different server.
- Why do this?
  - A remote copy of server logs elsewhere.
  - If logs were to be changed would need to be changed elsewhere.
  - Allows a central log repository for reporting instead of connecting to each server and pulling the logs.
- rsyslog is a method to transfer logs from one server to another.
- Simple and quick to set up.
- Can be set to send all logs or only certain log types.
- Available on multiple operating systems.

## System Logging

- System logging is controlled by the rsyslog daemon.
- Already installed and setup on most Red Hat 6 or CentOS 6 servers
- Log files are at /var/log
- **rsyslog** offers various ways to filter syslog messages. The most used and well-known way to filter syslog messages is to use the facility/priority-based filters which filter syslog messages based on two conditions: *facility* and *priority* separated by a dot.
  - *FACILITY.PRIORITY*
  - kern.*
  - mail.crit
  - cron.!info,!debug - This selects all cron except info or debug.
- /etc/rsyslog.conf is the rsyslog config file.
- You can filter messages and specify where to save them.
  - cron.* /var/log/cron.log
- More about logging in Red Hat Enterprise Linux 6 Deployment Guide.

## Log Management

- Managing system logs.
- Logs will grow in size over time.
- We must manage that growth sustainably.
- Get rid of old logs that are no longer useful.
- We can rotate logs.  Close the old log, open up a new one.
- We can compress these old logs so they take less space.
- /etc/logrotate.conf & /etc/logrotate.d/
- Options are:
  - **rotate**:  No of logs to keep for example - rotate 5
  - **compress**: Compress old log files to save disk space.
  - **daily**, **weekly**, **monthly** or **yearly**: Specified periodicity.
  - **size**: Size of log file. For example "size 500M".
  - **minsize**: Like size but monthly, weekly etc. Rotate log files if period reached and log file larger than the minsize.
  - **prerotate**, **postrotate**: commands run before and after log rotation.


Linux Academy
Red Hat Certificate of Expertise in Server Hardening
Configure System Audit Services

## System Audit Services

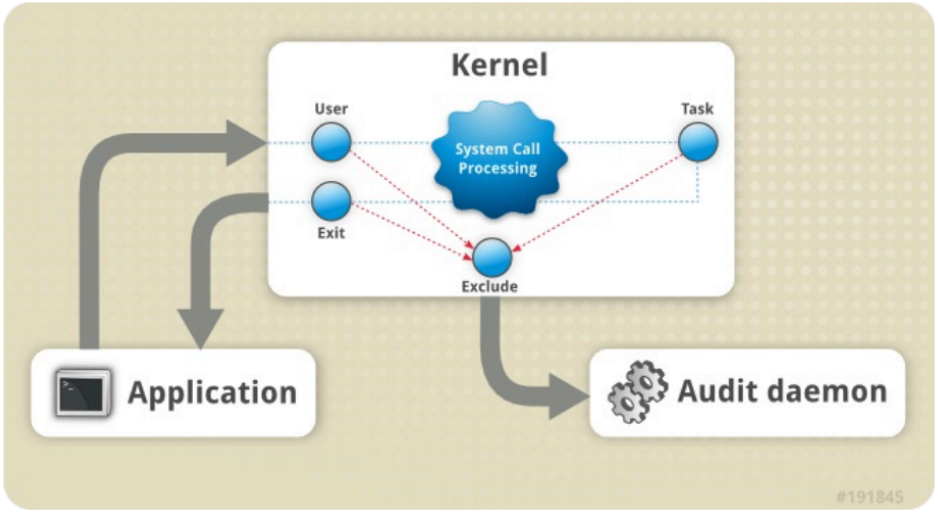
- Linux Audit system tracks security-relevant information on your system.
- Audit generates log entries about events happening on your system.
- The extra security provided is being able to discover violations of policy.
- Information audit can provide:
  - Date and time, type, and outcome of an event.
  - Sensitivity labels of subjects and objects.
  - Associate an event with identity of user who triggered the event.
  - Modifications to audit config and attempts to access audit log files.
  - Uses of authentication mechanisms such as SSH, Kerberos and others.
  - Changes to any trusted database, such as **/etc/passwd**.
  - Attempts to import/export information into/from the system.
  - Include/exclude events based on user identity, subject and object labels, and other attributes.

## Use Cases

- Watching file access.
- Monitor system calls.
- Record commands run by a user.
- Record security events.
- Searching for events.
- Running summary reports.
- Monitoring network access.

## Audit System

- The user-space audit daemon collects the information from the kernel and creates log file entries in a log file. Other audit user-space utilities interact with the audit daemon, the kernel audit component, or the audit log files:



## Install and Configure

- yum install audit
- Config file is /etc/audit/auditd.conf
- Default configuration should be suitable for most environments.
- service auditd start
- chkconfig auditd on


Linux Academy
Red Hat Certificate of Expertise in Server Hardening
Network Scanning Tools

## System Scanning Tools

- Software that is installed can have vulnerabilities.
- There are tools available to check your systems.
- Both commercial and open source.
- Port scanning - nmap.
  - Scans your server for open ports.
- System scanning - nessus.
  - Scan's your server for vulnerabilities.
- Both these tools are open source.
- Install nmap:
  - yum install nmap
- Install nessus:
  - https://www.tenable.com/products/nessus

## IPTables

- IPTables is the firewall used for Red Hat Enterprise 6 and CentOS 6.
- The Linux kernel features a powerful network subsystem called netfilter.
- Provides stateful or stateless packet filtering as well as NAT and IP masquerading services.
- Netfilter is implemented using the **iptables** administration tool.
- In Red Hat Enterprise 7 or Centos 7 the firewall used is firewalld.
- Why a firewall?
- You don't need to be an expert. There are command line tools or a file to edit.
- By default it may be disabled.
- File that holds the firewall info is /etc/sysconfig/iptables
- Graphical application also. **System** → **Administration** → **Firewall**
  - **system-config-firewall**


# Red Hat Certificate of Expertise in Server Hardening

## Conclusion

## Conclusion

- Thank you.
- What we talked about during this course.
- Identify common vulnerabilities.
- Verify package security.
- Configure default permissions.
- Install and use intrusion detection.
- Manage user account security and user password security.
- Manage system login security.
- Configure console security.
- Configure system wide acceptable use notifications.

## Conclusion

- Worked with identity management services.
- Configured remote logging.
- Configured system auditing.
- Used network scanning tools for network ports.

## Conclusion

- Read the study guide, it's there to help you.
- Follow the labs and complete the tasks required.
- Answer the quiz questions.

## Where to Go from Here

- Have a look at the Red Hat manuals available in the downloads section.
- Often they can go into deeper depth for any subject if your interested.
- Have a look at some of the other courses we provide.
  - Linux Academy Red Hat Certified Systems Administrator Prep Course
  - Linux Academy Red Hat Certified Engineer Prep Course


Linux Academy
Red Hat Certificate of Expertise in Server Hardening
Thank you.