Linux Academy

Study Guide

Linux Academy Red Hat Certificate of Expertise in Server Hardening (EX413)

Contents

Prerequisites

Linux

- The server the exam uses at the time of course creation is Red Hat Enterprise 6. Many of the items we cover in this course will translate to Red Hat Enterprise 7, so will still be useable in the future.
- All of the course material also applies to CentOS 6. The servers used to make this course are almost exclusively CentOS 6.

Experience

- This course will help you if you are interested in sitting the EX413 exam but will also be useful to fill in any gaps in your knowledge about server hardening.
- Red Hat Certified System Administrator or Red Hat Certified System Engineer would be helpful with this exam but is not required.
- Experience with server hardening and experience with managing Linux servers will help if you choose to sit the exam.
- If you are intending to sit the exam you should review the exam objectives which (at time of writing) can be found at this location: 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.

Overview

Why Server Hardening?

- The internet wasn't designed for security. Any security features were added after it had been used for many years.
- Within a very short time of a new server being available on the internet, it will be scanned for vulnerabilities. This can be seen in the logs showing login attempts. This can occur within minutes of a server coming online.
- Even small companies, nonprofits, and home systems are targets. Any system that can be taken over and used as a 'bot' or that may have information of interest will be a target.
- Unfortunately, attack tools are easy to obtain and use, as we show in portions of this course.

Common Vulnerabilities and Exposures

Standard Security Model

- There is a standard security model used call CIA. This stands for:
  - **Confidentiality** - You should only provide sensitive info to predefined and authorized individuals.
  - **Integrity** - Unauthorized users are unable to change or destroy data.
  - **Availability** - Resources should be accessible to authorized users whenever needed, so system availability is important.
- SELinux is an enhancement to the Linux kernel and is not covered in this course since SELinux is not a part of this exam. There are documents relating to SELinux in the download section of this course.

Online Tools

- Red Hat has several online tools for checking the vulnerabilities of your server and the installed software.
- Red Hat URL for security advisories: https://access.redhat.com/security/security-updates/#/security-advisories
- **Mitre CVE** - Common vulnerabilities and exposures - http://cve.mitre.org
- **NIST NVD** - National Vulnerability Database, which is built upon and fed by the CVE list - https://nvd.nist.gov/general/nvd-dashboard - This site is maintained by the U.S. Department of Commerce and the National Institute of Standards and Technology.
- On the Red Hat website you can set up alerts. Log in to the Red Hat website with your customer details. (Note: Only current customers are able to set up alerts. Non-customers can, however, view the information.) Navigate to this URL and enter your details: https://access.redhat.com/security/security-updates/#/security-advisories

Using Yum

- There are several tools, including yum, that can be used to check for security related updates to your servers.
- First you need to install a plugin called `yum-plugin-security`. You install this via `yum install yum-plugin-security`
- Once that is installed, you can use the following commands to check for specific types of updates:
  - `yum updateinfo`
  - `yum updateinfo list`

- `yum updateinfo list --sec-severity=Critical`
- `yum updateinfo list --sec-severity=Moderate`

Verify Package Security and Validity

- Software can easily compromise your systems, so only download software from trusted sources.
- Verify signed packages. Red Hat packages are signed with GPG keys, so can be trusted. Ensure what software is being installed is from a trusted source. Ensure that you have the GPG keys installed for that source.
- You can import GPG keys and you can display GPG keys and see information about them.
  - `rpm --import KEY-FILE` to import a key
- To display the GPG keys installed, use:
  - `rpm -qa gpg-pubkey*`
- To obtain details about a specific key, use:
  - `rpm -qi gpg-pubkey-KEYVALUE`
- Verify a signature on a package with the following:
  - `rpm -K rpm-file`

Identify and Employ Standards-based Practices

Common Standards

- Physical protection - Stop unauthorized people having physical access to the servers.
  - Secure your datacenters or Server locations; no unauthorized access.
  - Set up BIOS passwords on your servers.
  - Remove the ability to boot a server from alternate methods - e.g. CD-ROM.
- Server-based protection
  - Latest version of operating system.
  - Latest patch level.
  - Separate Partitions, so problems with one will minimize problems with other data. Some examples below:
    - `/var`

    - `/var/log`
    - `/var/audit`
    - `/home`
    - `/tmp`
  - Server-based firewall installed.
  - Sticky bit on world writeable directories.
  - Use and register servers with Red Hat Satellite for updates.
  - Ensure you have the Red Hat GPG key and its enabled in the repositories.
  - Remove legacy services where possible.
  - Disable services that wont be used and can't be removed.
  - Set SSH protocol to 2.
  - Set SSH loglevel to info or higher.
  - Disable the root user login from remote.
  - Set SSH permit empty passwords to no.
  - Use software such as AIDE or OSSEC to monitor the installed software and system changes.
- Encrypted file systems can be used to encrypt data 'at rest.' There is full disk encryption available for use. You can either enable encryption on server build, or you can add it later to new drives you mount.

File Systems

- There are several different file systems available for RHEL 6 and RHEL 7. And you can use these when you mount a new drive.
- **Btrfs** - Sometimes called butterfs. Designed by Oracle.
  - Uses B-tree file system.
  - 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 file systems.
  - Access to data is quick.
  - Uses copy-on-write. This means that if you have a file and you make a copy of it, unchanged, then it creates a clone of the file but doesn't actually create the file, so no extra space is used. If either file changes, then a new file is created.

    - Snapshots are available.
    - SubVolume (similar to a folder but can be mounted separately)
    - Quota groups.
- **Ext4** - Similar to ext3 and backwards compatible but with new features.
    - Next step up from ext3.
    - Backwards compatible with ext3.
    - Unlimited number of folders.
    - Better performance than ext3.
    - Journaled file system.
    - Larger storage limits - 1 Exabyte.
- XFS
    - Default for RHEL 7.
    - High performance.
    - Journaled file system.
    - 64 bit (8 Exabyte)

Security Properties for Mounting File Systems

- There are several settings to be aware of when mounting file systems to your server.
- These properties are common across btrfs, ext4 and XFS:
    - `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 mount options available are as follows:
    - `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 mount options available are as follows:
    - `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.
    - Subsecond 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 and includes a `noenforce` option.

File Properties

- `setuid` allows a user to run an executable file with the permissions of the file's 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 if care not taken.
    - Some file systems can be set to ignore the `setuid` attribute.
- You should search your file systems for suid programs, and, if they are unnecessary, disable or delete them. Care must be taken in case they are needed for proper system operation.
- You should audit the file system regularly.
    - You enable it with `chmod u+s FILE` (or `chmod 4xxx FILE`)
    - Disable it with `chmod u-s FILE` (or `chmod 0xxx FILE`)
- sgid is similar to suid but acts on folders.
    - File ownership is normally based on who creates a file, but in an sgid directory, files are owned by the group owner instead.
    - `chmod 2775 file` to add and `chmod 0775 file` to remove.

    - `chmod g+s file` to add and `chmod g-s file` to remove.
- 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 the file can delete it.
    - Owner of the directory can delete it.
    - The root user can delete it.
    - It modifies the meaning of the write permission.
    - To enable use `chmod o+t directory` or remove with `chmod o-t directory`.
    - To enable use `chmod 1xxx directory` or remove with `chmod 0xxx directory`.
- **FACL** or **file access control list**.
    - 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 mounted, if new file system.
    - Support is built into the kernel.
    - To set or remove use the `setfacl` command.
    - To examine use the `getfacl` command.
    - 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.
    - 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]`
        - `[d[efault]:}] [m[ask][:] [:perms]`
    - Examples to set rw permissions 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`

Install and Use Intrusion Detection

- Intrusion detection is used to check and watch a system to ensure there are no breaches to security. It's designed to detect any issues.
- **AIDE** - Advanced Intrusion Detection is open-source software freely available that can be installed with `yum`.
    - It is a file and directory integrity checker.
    - AIDE creates a database from rules (regular expression).
    - When first installed and when changes to files are made, its database needs to be initialized.
    - AIDE verifies the integrity of files.
    - File attributes can be checked for consistency.
    - Install with `yum install aide`.
    - The files to be monitored are in `/etc/aide.conf`.
    - You have to build the baseline database.
        - `/usr/sbin/aide --init`
        - This creates a database 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 `MAILTO: root` to be your email address, so email from cron goes to you. Save and exit.
    - Add a daily job to run. Put the following into the root crontab:
        - `0 1 * * * /usr/sbin/aide --check`
- **OSSEC** - Open source Intrusion Detection. It's scalable and multiplatform.
    - Server and client is 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.
- You can then install with:
    - `yum install ossec-hids ossec-hids-server`
- Adjust the config file, `/var/ossec/etc/ossec.conf`, for:
    - Your email, your email server, and send from.
- Start the service with `service ossec-hids start`

Account and Group Security

User Accounts

- User accounts have 3 types of files associated with them:
    - `/etc/passwd`
    - `/etc/shadow`
    - `/etc/group`
- Users are managed with:
    - `useradd`
    - `usermod`
    - `userdel`

Password Ageing

- Password ageing is setting passwords to expire after certain criteria are met. Normally, this is set as a policy for a company and is company-wide, not just on servers.
- It's forcing users to change their password, based upon certain criteria, like how old a password is, its length, etc.

- Files used for password ageing policies:
  - `/etc/default/useradd`
  - `/etc/login.defs`
- You can also use PAM (Pluggable Authentication Modules).

Group Account Security

- You can control group permissions with regular permissions that are set on files and folders, but there are other methods.
- **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.

Pluggable Authentication Modules (PAM)

- Pluggable Authentication Modules provides a common framework for authentication and security.
- Allows for central authorization and authentication.
- The `/etc/pam.d` direction 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)
- 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 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.
- The order of required flags is not important. Sufficient and requisites flags are.

Console and Physical Access to Server 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.

- The console is one of the first features of the kernel that was originally written by Linus Torvalds.
- It's 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).
- The VGA in text mode is what we will discuss here.

Disable Ctrl-Alt-Delete

- Note: 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.
- Note: 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.
- 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.

Other Security Options to Consider

- 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 OSes 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.

Red Hat Identity Management

IPA Server (IdM)

- Red Hat Identity Management is 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 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.
- You can have IdM server and a 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.
- 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 and 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`

Configure System Logging

Remote Logging of Messages

- With remote logging we are talking about sending logs to a different server.
- Why do this?
    - Keeps a copy of server logs elsewhere.
    - If logs were to be changed, they would need to be changed elsewhere.
    - Allows a central log repository for reporting instead of connecting to each server and pulling the logs. Could use with logstash or other software for reporting.

- rsyslog is a method to transfer logs from one server to another.
  - It is 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. It is already installed and set up on most Red Hat 6 or CentOS 6 servers, so nothing should be needed unless you wish to make changes.
- 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 can be found in the Red Hat Enterprise Linux 6 Deployment Guide.

System Audit Services

System Audit Service

- 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

- Some of the use cases for system auditing:
  - Watching file access.
  - Monitor system calls.
  - Record commands run by a user.
  - Record security events.
  - Searching for events.
  - Running summary reports.
  - Monitoring network access.

Installation

- In most cases, the audit systems should already be installed. If they are not then you can install them with the following:
  - `yum install audit`
- The config file is `/etc/audit/auditd.conf`
- Default configuration should be suitable for most environments.
- You may need to enable the service. In CentOS 6 or RHEL 6:
  - `service auditd start`
  - `chkconfig auditd on`

Network Scanning Tools and Local Firewall

Why Network Scanning?

- Software that is installed can have vulnerabilities, but there are tools available to check your systems that are either free or low to no cost.
- There are both commercial and open source tools available but we will only discuss 2 of them here.
- Port scanning - `nmap`.
- System scanning - `nessus`.

nmap

- Scans your server for open ports.
- To install `nmap`:
  - `yum install nmap`

Nessus

- Scans your servers for vulnerabilities.
- To install Nessus you must go to their website and download the software, Then register for a license key. Follow the install process to install the software. It will use a web server as the tool to schedule or perform scans.
- The website for Nessus is https://www.tenable.com/products/nessus

Local firewall

- 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? While your network firewall may protect your servers from the internet or other network segments, there is no protection from possible threats that are inside your network. This could be rogue employees, temp workers, or someone who has found an open network port or poorly protected wireless access point.
- With IPTables, you don't need to be an expert. There are command line tools or a file to edit.

- By default it may be disabled.
- The file that holds the firewall info is `/etc/sysconfig/iptables`
- There is a graphical application also: **System** > **Administration** > **Firewall**
- `system-config-firewall`

Resources

- There are several guides available in the downloads section for this course. While they are not necessary for this course, I have added them for your convenience. The most updated versions of these guides can be found on the Red Hat website.
- Note: Linux Academy is in no way affiliated with Red Hat, Inc. This course is not provided or reviewed by Red Hat, Inc.