Advanced Users & Groups (Administrative Tasks)
LinuxAcademy.com

/etc/passwd – This file contains the list of users on the system.
Format: username:password:UID:Primary GUID:comment:homedir:default shell

User id's under 1000 are reserved for system users. Some systems vary and user accounts will be 500 or less.

Can directly edit the passwd file to add,remove or modify users

Changing the shell section of the format to /bin/false will prevent the user shell login

/etc/passwd permissions must be readable by all, but /etc/shadow only should be readable by the superuser.

Pwck – Verifies the integrity of the users and authentication information. Checks entries for /etc/passwd and ./etc/shadow for proper format.

/etc/skel – Skeleton file used when creating new users. It allows you to set what files and settings need to be configured as default for every user added.

Useradd/Adduser – Creates a user on the system. Some distributions such as slackware use adduser instead of useradd. Note: both username and password are case-sensitive.

- -c Comment, can be used as a comment but is currently used for users full name

- -d Set the user home dir. By default it is /home/user if this is used you can set the location to anything you would like.

- -e expire-date Set the users expiration date. On this date the account password will “expire” and the user will no longer have access. YYYY-MM-DD

- -p Set your own encrypted password and not let the system do it. This is not advised. The

- pre-encrypted password is added as is to your /etc/passwd and /etc/shadow files.

- -M Do not create the home directory. Even if the /etc/login.defs has the default set to yes.

- -m Create a home directory /home/username if it does not exist. Files contained in the /etc/skel directory will be copied into the new users home directory. Useradd creates a user home directory by default.

- -G Defines all the other groups that the member belongs to. Separate each group by a comma .

- -g Sets the default group that is the users group when the user first logs in

- -f INACTIVE defines the number of days after a password expires that an account is permanently disabled. Value of 0 disables immediately after the password expires and -1 disables the entire inactive feature.

- -k skel_dir : says what skel dir for the useradd command to use when creating a user. Allows you to have different default settings for different users you might want to add. If the option is not set it uses /etc/skel by default.

/etc/default/useradd - Location for default settings for the useradd command

/etc/shadow – Contains the encrypted password for the user accounts on the system. This and the

/etc/passwd file can be directly modified. The useradd and usermod commands are an interface to automatically modify these files.
Format
username:password:days_until_change_allowed:days_before_change_required:days_of_warning_before_expiration:days_between_expiration_activation:expiration_date:special_flag

Flag names are self-explanatory. However, a value of -1 or 99999 will indicate that the feature is disabled for that user.

Chage – Changes and manages users expiry information. Changes the number of days between required password changes. Force password changes for users after x number days

- -E set the date that the users password will expire

- -I set the number of days of inactivity after a password has expired before locking account

- -m Set minimum number of days between password changes

- -M Set maximum number of days which a password is valid

groupdel – Groupdel groupname if any user has this group as their primary group then the group cannot be removed until the user not longer has this as their primary group.

groupmod - Modify group name or group id

- -g: specify a new group id (returns error if group already exists)
- -o: When used with -g it allows two groups to share the same group id
- -n: Specify a new group name

userdel – Deletes users accounts and associated files.• -f Forces the removal of the user account even if the user is still logged in. It will also delete the user home directory and mail. This is not typically recommended. You can use kill to boot a user from your system and then remove the user account.

- -r This will remove the users home directory, files located in the users home directory and the users mail. This does not remove files owned by the user outside of the user home directory. Use the find command to find files based off owner.

Usermod – Modify a user account

- -d set the users home directory to a new directory
- -e set date on which user account will expire yyyy-mm-dd
- -f number of days after a password expires until account is permanently disabled
- -g group id/name of the users new default login group
- -G list of extra groups the member is also a member of
- -l change the login name of the user
- -L lock the users account

/etc/group – This file contains a list of groups and all the members associated to the groupexample of /etc/group: groupName:Password:GUID:userlist

groupadd – Adds a group to the system

- -g: Specify a group idea. If not specified it will auto select one for you

- -r: instructs groupadd to pick a group id less than 500 used for system groups

- -f: forces group creation even if another group already exists

passwd – Change user password. For root account you do not need existing password. Root can change another users password by adding the username after passwd command.

- -x number of days a password remains valid.

- -n minimum number of days between password changes

- -i make account inactive after password has been expired for x days.