Hello everyone! In this video, you will learn about password management in Linux OS.

Using a password with an associated user account is the primary method of authentication in Linux and most UNIX systems.
Shadow files are the encrypted user passwords which are kept in **/etc/shadow file**. This file is read-only directory and can be read only by root.
In the snapshot you can see that the **/etc/shadow** file contains nine columns separated by colons.
Starting from left to right, these nine columns contain username, encrypted password, last changed password day, number of days password must be left unchanged, password expiry day, warning number of days before password expiry, number of days after expiry before disabling the account, and the day account was disabled. Last column has no meaning yet.

login.defs is another important file placed generally in etc folder, in Linux which contains some default settings like password aging and length settings. You can view the password specific settings using the cat command and filtering the output with grep command, as shown in snapshot.

The chage command tracks the password management and stores all the events of password change and password characteristics. The -l option is used to list the information as shown here.

If a user on the machines is required to be disabled, without deleting it, Passwords in /etc/shadow file can be disabled by putting an exclamation mark **(!)**. If an exclamation mark is present in starting, then the password cannot be used. This process is called **locking, disabling**, and **suspending** a user account. It can be done in **vi** or with the **usermod** command, as shown here.

Thank You…