Password Management

The password management in Linux system. So first we will learn about the shadow file shadow file files store the encrypted user password which is capped in /etc/shadow.

This file is the read-only directory that can only read by the root user. So, let's try to read the shadow. File by typing cat. Shadow and you can see it is not readable by a normal user right now that it. CDAC and we can read it by using pseudo privilege. and you can see here, we can see.

All the password that has been stored for the various users like CDAC. For the user one and for the demo user. these are the encrypted password. That you can see here. Now there is a file that is /etc/login.def.devs.

That contains some default settings like password aging and the land setting. Let's try to open it using sudo. Let's try to see what settings are there in this dev file. So, I will grab here only the string path. So, I have to use the cat to read this file. So, you can see here we can see the various settings like password maximum days.

Maximum number of days is password may be used pass mean days. Minimum number of days allowed between password changes.

And you can see that has been set as five time nine for the maximum days that a user can use this password and minimum days is zero. and password is number of days warning given a password expire, it will expire in seven days. So now we will come to the next. That is the change command. Change command is used by a user.

To know the information about their password. For example, I will use pseudo change. Then I will type minus l. Options. To list the information of a user. That is demo and we can see.

The last password change of the demo user is 13th June 2022 password expired never for this user password is inactive. That is never for this user. Account will never expire for this user. And the warning that will be shown.

For this user for the seven days. Now we can enable and disable password for a particular user also. So, let's try to show the shadow file again and here you can see. That for the user CDAC there is. Encrypted password and for the user one.

Also, and you can see first it will give the username, then the Encrypted password similar for another user. And please note that there is.

Please note that there is not an exclamation mark. An exclamation mark is present in starting. If an exclamation mark is present in.

Starting then the password cannot be used. So, let's try to use an exclamation. Mark for a user to disable the password. So, I will use the user one. To disable the password. There is not an exclamation mark for. The user one so I will type sudo. The command is user mode.

Type the Username in which the password that we want to disable. Before that, after user mode, give space hyphen l space, then the username and press Enter.

Now the password has been disabled for the user one. So, let's again open the shadow file. and try to see whether the password has been disabled or not.

And I will filter the output and you can see there is an exclamation mark. That means password has been disabled for this user. Now, if I want to enable it.
Again, for the user one, enable the password. So, the command for that is pseudo user mode hyphen capital view and provide the user for which the password has been disabled. And when we press Enter, the password will be enabled again.

So again, open the shadow file to verify whether the exclamation mark has been removed or not. It has been removed. That means the password has been enabled for the user one.

So that's all about the password management.

Thank you for watching this video.