This is what the scoring screen should show at the start.

Graphical user interface, text, application, email

Description automatically generated

Use the tail command to view the last 15 lines of the passwd file to see the user accounts on the machine.

Text

Description automatically generated

Comparing the list of users with the list of allowed users we can see that vicious needs to be removed so we can use the userdel command to delete the account.



We can also see that the user ed is missing and needs to be create which can be done with the adduser command.

Text

Description automatically generated

Next, we are going to look at the administrator accounts to make sure that only the correct accounts are admins. This can be done by clicking the dropdown menu in the top right corner and opening the settings.

Graphical user interface, text, application

Description automatically generated

Once we have the settings open, we will need to unlock it by clicking the button in the top right and entering the password.

Graphical user interface, text, application

Description automatically generated

When looking through the user accounts we can see that jet is not an admin and should, this can be changed by clicking on the correct user and then using the administrator toggle.

Graphical user interface, text, application

Description automatically generated

To set password age policies we need to edit the login.defs file.



To set the amount of time a user is warned before their password expires add the line below.

Text

Description automatically generated

Now we are going to set password requirements by editing the common-password file.



By adding the reject username and enforce for root options we are making it so that users cannot set their password to their username and the all password policies are also applied to the root account.

Text

Description automatically generated

Now we are going to audit the installed packages, to list the installed packages use the following command.



We can find that the hacking tool netcat is installed and should be removed.



This can be done using apt with the purge option.



To turn on the firewall use the command ufw enable.



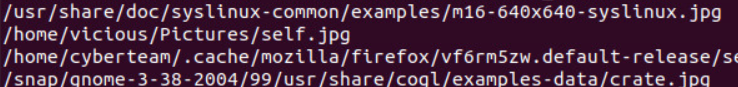
Now we are going to solve the forensic question which asks about media file download by the unauthorized user. The answer can be seen below.

A picture containing table

Description automatically generated

To find that answer you can either look through the user that was deleted files or use the find command to look for files with certain extensions. By trying a few different media extensions, you can eventually fine an image file named self.jpg in vicious picture folder.





Then delete the image with the rm command.



Now looking at the readme the service ssh is required and needs to be installed which can be done with the following command.



Then the ssh configuration needs to be secured.



The below line sets the listening port that ssh uses by changing it from the default it can make it harder for unauthorized users to connect.

Text

Description automatically generated

To permit the root account to login remotely you should add the line below.

Text

Description automatically generated

This is what the score report should look like after all scored vulnerabilities have been properly addressed.

Graphical user interface, application, table

Description automatically generated