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

Graphical user interface, text, application

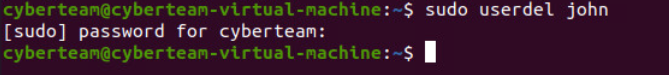
Description automatically generated

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 john needs to be removed so we can use the userdel command to delete the account.



We can also see that the users bob and steve are 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 frank is not an admin and should be and dennis is and should not be. This can be changed by clicking on the correct user and then using the administrator toggle.

Graphical user interface, application

Description automatically generated

The next step is to disable the guest account which can be done by editing the 40-enable-guest.conf file using nano to have the below text included.



Text

Description automatically generated

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

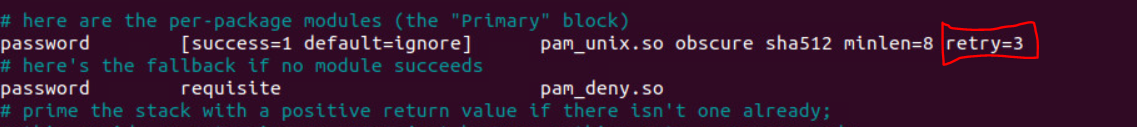


To set a minimum length requirement add the text in the red box.

Text

Description automatically generated

To set a number of times the user can try to enter a password before it aborts.



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



To set the amount of time before a password expires set add the line in the box.

Text

Description automatically generated

For the minimum length before the password can be changed add this line.

Text

Description automatically generated

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



When looking through the packages we can see that plex is installed as a media sharing server it is against policy and should be removed.



We can remove a package by using apt with the purge option.



To turn on the firewall use the command below.



Now we are going to secure some of the ssh configurations by editing the file below.

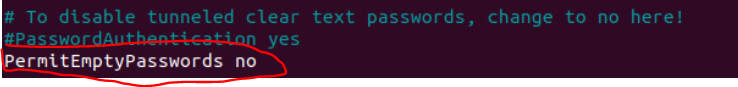


The below line sets the listening port that ssh uses by changing it from the default it can make it harder for unauthorized users to connect.

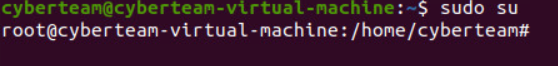
Text

Description automatically generated

Add the following line to the ssh configuration to make sure that ssh users must have a password set to be able to login.



Finally, you may have noticed that the unauthorized user keeps reappearing. To find how this is happening you can login as root using the command sudo su.



To list all of the crontabs use the command crontab -e which should show the following file. This cron job will run the commands in the script user.sh every 15 minutes. To remove it you can just delete that line.

A screenshot of a computer

Description automatically generated with low confidence

Lastly the script to add the user should be removed which can be done with the rm command.



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

Table

Description automatically generated