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



Now to look at group membership use the following command

Text

Description automatically generated

Looking at the /etc/group file we can see that there is a group called Primes that should not exist.

Text

Description automatically generated

To remove the group, you can use the following command.



Next, we are going to see logging policies for user logons by editing the following file.



To log successful logins add the following line to the file.

Text

Description automatically generated

Then make sure that both the options below are set to yes to log su behavior.

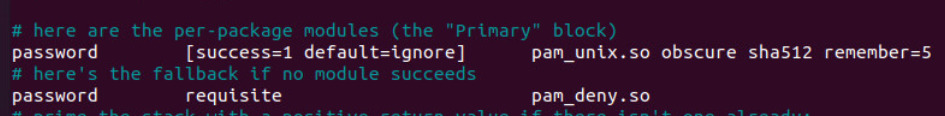
Text

Description automatically generated

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



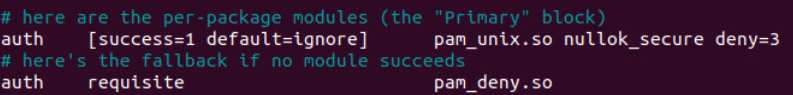
To set the number of passwords that are remembered to prevent password reuse add the remember options as shown below.



Now to set account lockout policies we are going to edit the file below.



Then add the deny option to set how many attempts a user has before their account is locked.



Now we are going to configure ssh to be more secure by editing the config file.



Scroll down until you see this section and make sure the following line is added.

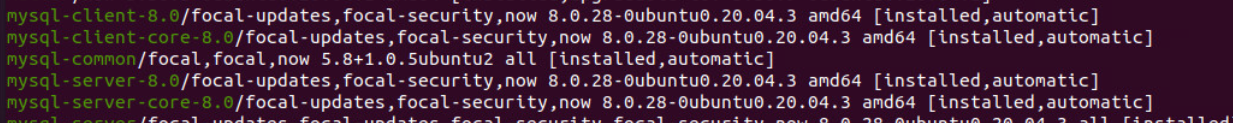
Text

Description automatically generated

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



Looking at the results we can see that mysql is installed and is not needed and should thus be removed.



That can be done by using the following command to remove all packages that start with mysql.



Looking at the first forensics question we can see that there was an unauthorized group which if you remember was the group Primes that was removed earlier.

Graphical user interface, application, Word

Description automatically generated

The second forensics question involves decoding some cipher text.

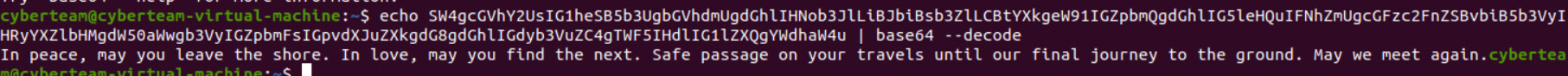
Graphical user interface, text, application, email

Description automatically generated

You may recognize that this encoded using a base64 conversion but if not, you can use a tool like the one found at [https://www.boxentriq.com/code-breaking/cipher-identifier.Graphical user interface

Description automatically generated with medium confidence](https://www.boxentriq.com/code-breaking/cipher-identifier.#)

To decode base64 text you can use the following command then to get the answer take that output and remove all of the whitespace.



Finally, the readme requests that notepadqq be made available and can be installed with the following command.



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