# Cybersecurity

## Activity 3.1.2 Access Control

Copy and paste screenshots and/or answer questions from the activity.

#4

|  |  |  |
| --- | --- | --- |
|  | message.sh | welcome.txt |
| Owner | can read, write, and execute | Read and write |
| Group | Read, execute | Read |
| Other | none | read |

#5 Who owns message.sh? What do you think the color of the filename tells you?

Alpha, green means its an executable or script

#6 Now that you know that message.sh is executable, use the cat command to look at its contents and try to determine what it does.

It shows the contents of welcome.txt

#11 To change the extension, move the file to message.doc and rerun the file command. Record what the file command reports each time you run it.

Graphical user interface, text

Description automatically generated

#13 What are the types of files in alpha’s home directory? In the Pictures directory?

Text

Description automatically generated



#22 Confirm that the remaining file is the one that was generated by gpg. What is the file

extension?

Text

Description automatically generated

File extensions is .gpg

#23 Use the cat command to try to view the encrypted email\_addresses.gpg file. Describe

what you see.



Absolute garbage

#26 How would you complete Step 26? What would the commands look like?

* Move the files
  + mv year1 business/financials
  + mv year2 business/financials
  + mv year3 business/financials
* Go to the target directory
  + Cd business/financials
* Confirm the files were moved correctly
  + ls
* Hide the files
  + mv year1 .year1
  + mv year2 .year2
  + mv year3 .year3
* Encrypt the files
  + gpg -c .year1 && rm .year1
  + gpg -c .year2 && rm .year2
  + gpg -c .year3 && rm .year3