**Working with File Permissions**

Graphical user interface, application, Word

Description automatically generated

-/d

* Refers to file or directory

r/w/x

* Read/write/execute

Graphical user interface, application

Description automatically generated

**Binary Permissions**

A binary representation of permissions

Common way to change permissions on a file or directory

* Read = 4
* Write = 2
* Execute = 1
* Chmod 770
  + -rwxrwx---

Usually want to assign as low permissions as necessary

**Sticky Bit**

Allows executable to be ran in the context of the owner

If vi on a file, owned by root, had a sticky bit on it and you ran vi as a standard user

* A shell could be spawned off of vi with root permissions from your standard user