**IDs, Run Levels and Logs**

**IDs**

**Run the id cmd**

Uid

* UserID

Gid

* GroupID

Groups

* Actual full list of groups that the user is associated with
* Same as cat /etc/group | grep Brandon
  + Greps for all files containing Brandon in the groups directory
* Sudo -l will show the users sudo permissions

First commands to run on exploitation

* Id
* Sudo -l
* WhoAmI

**Run Levels**

A run level is a mode that the OS is in

When Linux starts up, the default run level is identified

A Linux OS will always be in some sort of run level whilst running

* Who -r, checks current run level

Level 0

* Tell the system to halt or shut down now
  + The off button

Level 1

* Single user mode, does not start any network services, daemons or allow any non-root logins.
* Mainly used for straight terminal access as a last resort
  + A sort of safe-mode
* Level 2
  + Multi-user mode, same as level 1 but with non-root logins
* Level 3
  + Multi-user mode with networking
  + Common run level for Linux with no GUI or installed in headless mode e.g., on a server
* Level 4
  + Undefined as it’s a custom start up mode
* Level 5
  + X11 is used here. Grub
  + Normal mode of operation with a GUI available by default
* Level 6
  + Tells machine to issue reboot
  + Same as reboot button

**Linux Logs**

Lfi – local file inclusion attack

Most logs stored in /var/log

Logs often hold valuable information about the system and who’s doing what

**HW - Named Pipes, lfi, log poisoning**