**Privilege Tree:**

Diagram

Description automatically generated

**There are two main privilege escalation variants:**

**Horizontal privilege escalation:** This is where you expand your reach over the compromised system by taking over a different user who is on the same privilege level as you. For instance, a normal user hijacking another normal user (rather than elevating to super user). This allows you to inherit whatever files and access that user has. This can be used, for example, to gain access to another normal privilege user, that happens to have an SUID file attached to their home directory (more on these later) which can then be used to get super user access. [Travel sideways on the tree]

**Vertical privilege escalation (privilege elevation):**This is where you attempt to gain higher privileges or access, with an existing account that you have already compromised. For local privilege escalation attacks this might mean hijacking an account with administrator privileges or root privileges. [Travel up on the tree]