

Managing Unix Users and Groups

- Users and Groups are identified by number
 - Typically 0 .. 65536 (16-bit)
 - Newer Linux allows 32-bit
 - UID = User ID
 - UID zero is the “root” or super user
 - The super user never sees a “permission denied” error
 - Low numbered UIDs (and GIDs) are *somewhat* standardized
 - GID = group ID
 - Groups allow resources to be shared among member users
- Text configuration files map between user and group names and numeric ids
 - /etc/passwd associates text info with each UID
 - /etc/group associates group names with GIDs and lists member users
 - /etc/shadow associates encrypted passwords and expiry with user names
 - <http://www.slackbook.org/html/essential-sysadmin-hardusers.html>
 - Names are just for convenience, UIDs and GIDs really matter
 - To rename a user, just change text files
 - NFS requires that UIDs and GIDs match across machines
- Processes normally inherit the UID and GID of their creator
 - Root User processes can masquerade as any other user
 - Special permission on binary executables allow them to do the same
 - Even when invoked by “normal” users
 - This is how the su command works



File permissions

- Everything in Unix is a file
 - Serial ports, disk drives, shared memory, etc.
 - All these resources have file permissions
 - Processes must pass a security check to open any file
- Permissions are a bit mask
 - http://www.comptechdoc.org/os/linux/usersguide/linux_ugfilesp.html
 - <http://www.perfect.com/articles/chmod.shtml>

