Escaping chroot jails

Why?

- Chroot jails come up in writing exploits, CtF competitions, *etc.*
- In the context of this class, a good intro to basic UNIX concepts

UNIX 101

- “man man”
- “man 2 chroot”
- Users (UID 0 is root)
- Tree of processes, with owners
  - pstree, ps, top
- Tree of files and directories, with owners and permissions
  - ls, tree

Explore in the shell a little bit...


insmod part_msdos
insmod ext2
linux16
inspiron

After you boot

- Authentication
  - Ties a person to a process
  - Typically involves entering username and password

chroot jail

- Intended to keep a process in its own root directory
  - *E.g.*, to keep them out of /home directory
- Not intended to keep a superuser who can run arbitrary code contained, but people try to use it for that
  - FreeBSD has a stronger jail concept, or use Linux Containers

Putting ourselves in a chroot jail...

Breaking out of it...

- Build a new jail inside the one you're in
- Request that the new jail be your jail
  - Okay because it's smaller and inside the one you're currently in
- Ask to go anywhere you want in the system
  - Not a problem, because you're not in your jail anyway so you're not getting let out

Explore both versions of the C code...

References

- https://filippo.io/escaping-a-chroot-jail-slash-1/