UNIX process hierarchy

- ssh b146-*
- pstree -p | less -S
- pstree -pu crandall
- lsof -p31009
- nc -l 20202 &
- lsof -p31626
- kill -9 31626
Sockets

- In UNIX systems, sockets typically come in two flavors
  - Datagram sockets: have a demarcated beginning and end, but no ordering guarantees between datagrams or anything like that
  - Stream sockets: whatever bytes the sender writes into it, the bytes can be read by the receiver in the same order (but no demarcations)
Network Sockets

• In *networked* UNIX systems, *network* sockets typically come in two flavors
  – UDP datagram sockets: have a demarcated beginning and end, but no ordering guarantees between datagrams or anything like that
    • Also, no guarantee that your datagram even gets there
  – TCP stream sockets: whatever bytes the sender writes into it, the bytes can be read by the receiver in the same order (but no demarcations)
    • Guaranteed delivery, which the kernel takes care of for you
An open TCP socket

ssh b146-*
netstat -tn
man lsof
Authentication in general

- Bishop: “Authentication is the binding of an identity to a principal. Network-based authentication mechanisms require a principal to authenticate to a single system, either local or remote. The authentication is then propagated.”
Authentication in general (continued)

● Bishop: “Authentication consists of an entity, the user, trying to convince a different entity, the verifier, of the user's identity. The user does so by claiming to know some information, to possess something, to have some particular set of physical characteristics, or to be in a specific location.”

● Informally: something you know, something you have, something you are
2FA = 2-Factor Authentication

• Two of these:
  – Something you know
  – Something you have
  – Something you are

• *E.g.*, bank card plus PIN

• For Internet services, typically the first two

• Helps protect against phishing, for example
SHA-512

password

Salt

username

/etc/passwd

/etc/shadow

Compare

hash

Match? Yes or no.
• First is special designations (symlink, directory)
• Next triplet is user (u)
• Triplet after is group (g)
• Last triplet is others (o)
• r = read, w = write, x = execute
• Sometimes you'll see other things, like s for Set UID
man ...

- ls (ls -l is a useful flag), cd, pwd, chown, chgrp, chmod, stat, id, w, who, last, kill, ps, pstree, netstat, cat, less, sudo, watch, screen, fuser
Some more things to read up on

- FIFO pipes (can be unnamed or named)
- The /proc/ filesystem
- Character devices (e.g., PTY, PTS, TTY)
Resources

- [http://www.cs.unm.edu/~crandall/linuxcommand cheatsheet.txt](http://www.cs.unm.edu/~crandall/linuxcommand cheatsheet.txt)
- Matt Bishop's *Computer Security: Art and Practice*, Chapter 12
- Any operating systems textbook, or Wikipedia