Chapter 0

- Documentation
  - What is appropriate documentation (common knowledge)
    - Forum
    - Slack
    - The internet (in general)
  - What is not common knowledge
    - Getting a specific answer from a classmate
    - A specific blog / writeup of a machine
    - Direct copying
- IPs
  - Students - 10.11.0.0/16 except 10.11.1.0/24 (do not scan)
  - Public Labs - 10.11.1.x/24
  - Megacorpone.com
- Hints
  - Student Control Panel
    - Crackpot!
  - Forum
  - IRC (minimally useful)
  - Eachother (20 minutes stuck on exercises, 40 minutes on labs)
- Kali
  - Do no update until after complete exercises (Java)
  - SNAPSHOT!
- Lab Behavior
  - Shared VMs - be polite
- Notes
  - Keepnote is great.
  - Shutter (apt-get install shutter) is kali version of sniping tool
  - Use google drive to more back and forth

Chapter 1 (RTFM pages 5-9 [linux], 15-17 [windows])

- Help
  - Tab complete!
  - Man <command>
  - <command> --h, --help
- Find, locate, which (your path $PATH), updatedb
  - Find based on group? User? Permissions?
  - Find -name, find -user, find -group, find -perm, find -exec
  - `find directory -user root -perm -4000 -exec ls -ldb {} \; >/tmp/filename`
- Systemctl, service
  - SSH (copy files via scp)
  - Simple python http (python -m SimpleHTTPServer 8000)
- Wget, curl, curl -X “Post”

- Grep, grep -r, cut, awk, sort, unique
    - Grep -r, grep -v (not does contain), grep -A -B or -N (lines above, below, both)
    - Zgrep for compressed
- What does > or >> or < or | mean?
    - Stdin v stdout v sterr
    - 2>/dev/null
- Bash scripting
    - What is $url?
    - What is for url in $(cat list.txt)
    - Can do similar with `command `
- Cat, head, tail
- Chmod, useradd
- Networking
    - Ss vs netstat
    - Ip add v. ifconfig v. ipconfig

Chapter 2-2.2

Nc.

- nvlp (what does each do
- -K
- Notice the command are different on windows then linux
- -e

Reverse vs Bind shells

- which is better based on firewalls and acl

Alternative callbacks

- http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet