Hacking 300
CTF Cheat Sheet

We know, the other document has a lot of words. Here's a cheat sheet:

CTF LAB

- **PLEASE DO NOT DO THESE THINGS!**
  - Attacks outside of the lab environment
  - Attacks against any machines outside of the CTF approved target ranges below:
    - 192.168.2.200 – 192.168.2.220
    - 169.254.22.100 (NOT DIRECTLY ACCESSIBLE FROM AAR NETWORK)
    - 169.254.22.212 (NOT DIRECTLY ACCESSIBLE FROM AAR NETWORK)
  - Attacks against other students
  - Modify FLAGs, existing user accounts, files on shares, or anything else that looks like we set up for the CTF. (Please use good judgment and be considerate of other students.)
  - Install backdoors easily accessible by other students. Secure your stuff!
  - Deface the environment (We already did that for you!)
  - Banned attacks
    - DoS
    - ARP/DNS/DHCP Spoofing attacks / active MITM
    - If you are unsure, ASK US FIRST!
  - Share any information, FLAGs, or hints with other students. This is an individual exercise!
  - Depend on any files/data/settings saved on the CTF machines. CTF machines will be reset regularly throughout the CTF and any data added to them will be lost periodically.

- **PLEASE DO THESE THINGS!**
  - Start your CTF and Report work early
  - Keep detailed notes of everything you do, screenshots, logs, etc.
  - Turn in flags as soon as you find them
  - Report any suspected problems with the lab to us ASAP
  - If you install or copy software to a machine in the CTF lab, put it in a discrete location and if possible clean up after you are done.
  - Review the grading breakdown on the “Course Resources” page in Canvas to make sure you understand how your report will be evaluated!
  - Turn in your report by the due date specified on Assignment 6-9: CTF FINAL REPORT.
  - HAVE FUN HACKING!