Course Overview

This course is intended for students who are interested in cybersecurity and especially for those who are preparing for PRCCDC (the Pacfic Rim Collegiate Cyber Defense Comptetition). Students taking this course are expected to be self-motivated and interested in learning, with the ability to research a given topic and share their knowledge with others. Class this semester will involve hands-on tutorials involving basic hardening, attack, and defense skills on Windows and *Nix based operating systems.

Course Objective

Over the semester, students will have an opportunity to practice researching and presenting on assigned topics that are relevant to PRCCDC, with the highly encouraged option to include more information as they find it useful and interesting. This is a student directed course with the purpose of competing well at PRCCDC, but prior knowledge is not necessary as this semester is targeted at raising every student's knowledge to the level at which we hope to compete.

Grading

Attendance	60%
Discussion	10%
Tutorials	30%

Attendance at 80% of classes or more is required if you are taking this class for two credits. Understanding that students have many priorities, the expectation is that if you make a reasonable effort to attend every class and communicate if you have a conflicting commitment.

Discussion will involve sharing current events at the beginning of class. Good sources for news are:

YCombinator Hacker News	`https://news.ycombinator.com/news?p=1`
ArsTechnica	`https://arstechnica.com/information-technology/`
Wired	`https://www.wired.com/category/security/`
Twitter	(depending on who you follow)

Tutorials will be assigned and chosen at the beginning of the semester. A template with specific expectations will be given, which you are expected to follow in order to receive full credit. In the process of preparing for tutorials, you may find the following resources helpful:

Cyberdefense Github	`https://github.com/GhostofGoes/ui-prccdc`
...	...

Topics

- How to research and find good resources
- Presenting effectively
- Commonly used acronyms
- Nmap and making a network map
- Persistence (sticky keys, scheduled tasks)
- Windows firewall (basic rules that should & shouldn't be there, not locking yourself out by denying RDP)
- Windows command line
- Powershell
- Windows task manager and common tasks (detecting an intruder)
- Sysinternals (autoruns, process explorer)
- Group policy and active directory
- Layer 7 firewalls (Palo Alto)
- Layer 3 firewalls (VyOS, pfSense)
- Bash fundamentals
- Bash scripting
- *nix variants and how they differ: FreeBSD, Solaris, Linux, etc.
- Linux directory structure and contents
- Cron
- Networking & the OSI model
- IPv4 addressing
- NAT rules
- ...

Schedule

Quarter 1: Introduction, common acronyms and terminology, overview of PRCCDC and motivation for why and how we're preparing, expectations such as presentation templates, grading, goals, how to ask *good* questions and precisely articulate problems, review of previous competitions, resources that are available, and overview of semester schedule

Quarter 2: Windows fundamentals

Quarter 3: Linux fundamentals

Quarter 4: Networks and domains?