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.

Classes will be held in JEB 006, RADICL, at (time?).

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.

We reserve the right to select teams based on criteria including but not limited to: skill, area of skill, experience, attendance, team cohesion, etc.

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. Attendance is also an important factor in team selection, although you can miss up to three classes before it starts affecting your eligibility to compete. Also, attending Cyber Defense Club (CDC@UI) can be done to make up for absences.

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)

Please bring a printed summary of the news event you're planning to discuss.

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`
...	...

Tutorials should be submitted at least two days prior to the presenation date. ?A student will be assigned to read through the tutorial and prepare five or more questions on the material.? The student presenting will then create a writeup afterwards to be submitted within five days.

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
- Git (for template, syllabus, etc, for next class and hold previous classes also, persistence over time)
- ...

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

Presentations for beginning of class (by class leadership).
Quarter 2: Windows fundamentals

Quarter 3: Linux fundamentals

Quarter 4: Networks and domains?

In more detail: 15 weeks, 30 classes:

Week 1, Day 1: Syllabus, time, expectations, overview of course (emphasis on quality over quantity)
What is the competition, expectations of tema members, etc
Intro to course and competition

Week 1, Day 2: Understanding a virtual environment and how to set up responsibly at home
Assign first presentations
Explain terminology (ISO, checksum, etc.)

1st half of semester: 2 news per day (10 min), 2 tutorials (35 min per)
30 slides, 1 min for each
Two people per presentation first round

2nd half: 1 tutorial
One person presents

Week 2:
Intro Windows
Intro Linux
Networking/OSI Model