Welcome Back - Spring 2021

Kyle Westhaus

January 12 2021

Reminders - Officers

- Kyle Westhaus, President
- Yu-Shiang Jeng, Vice President
- Andrew Haberlandt, Treasurer
- Jackson Leverett, CTF Captain
- Nick Kuhl, Outreach Coordinator
- Andrew Migot, Research Coordinator

Reminders - Communication/Links

- **Attendance** (because the College of Engineering and OSU make us): http://attend.osucyber.club
- **Mailing List:** http://mailinglist.osucyber.club
- **Slack:** http://slack.osucyber.club
- **Website:** http://osucyber.club
- **Wiki:** http://wiki.osucyber.club

Feedback Results

- CTF-specific survey, club survey
- People wanted:
  - Better cohesion between meetings
  - More hands-on experiences
  - Preparation for the competition, not just the competition itself

Our Past CTFs

- Weekend-long
- Range of challenge difficulty levels
- . . . but little background info about how to prepare an environment and begin competing

The Plan

- Floated idea of "Bootcamp" in winter break feedback - something other clubs have done before (Purdue)
- Series of meetings dedicated to teaching those with minimal CTF experience how to be successful
  - CTF background info
  - Technical knowledge for challenge categories
  - Wiki content about environment/tool setup
  - Challenges hosted all semester!

This Semester

- Tonight: background on CTFs
- Next week: more Bootcamp CTF specifics, start of actual bootcamp content
- Rest of semester: more technical education content for challenge categories, you participate and use what you learn in meeting to complete more and more challenges and get prizes along the way!

Capture the Flag

- "flags" = short snippets of identifiable text. Examples:
  - `osuctf{theflagincludesthestuffbeforethebraces}`
  - `osuctf{th15_15_n0t_a_r34l_flag}`
  - `osuctf{133tsp34k}`
- Not so much "find this text hidden somewhere on a computer", but rather "complete this technical challenge, the flag will be apparent at the end". Example:
  - "This ciphertext is weakly encoded, decode it to get the plaintext flag"

Why CTF?

Very popular for college clubs like our own because:

- Very effective way to learn
- Very effective way to demonstrate skills to future employers
- Fun competition

CTF Format

- Mostly jeopardy
  - Many problems, grouped by category, each has an associated number of points, available for a certain amount of time
  - Solve a challenge, submit flag, receive points
  - Team with most points at end of competition wins
  - Sometimes additional rules (e.g. only a few challenges unlocked at start, first team to solve gets to pick next unlocked challenge)
- King of the hill
- Red/blue team

CTF Interface

- Usually a website for registration, team creation, list of challenges, flag submission, scoreboard
- Extremely common software to run this part of a CTF is CTFd

Interfacing with Challenges

- Downloadable file in challenge description
  - Demo base64, open in text editor
  - Demo Somewhat Questionable LLC, open in browser
  - Demo speedrun3, view source, connect with netcat

Need for CTF Tools

When using any standard operating system, you can automatically do the following with challenges

- Downloadable
  - Look at file in file explorer, maybe extract, open in text editor
- Service URL
  - Open in web browser, something like netcat

. . . but often times you need to do more! Solution:

- Use recommended tools (see the wiki!)
- Do your own searching to find helpful tools
- Write your own code

Tool Examples

- Web tool (cryptii)
- Downloadable program with GUI (ghidra)
- Downloadable terminal program (urlbuster)
- Python library (pwntools)

How do I find CTFs?

- We are hosting a semester-long one!
- Other universities run them!
- Conferences run them!
- CTF teams host their own!

. . . and they are all on a list at https://ctftime.org/ (DEMO)

Other Content

- Livestreams/youtube videos of people solving CTFs
- CTF challenge solution writeups (github or blogs)

Wrap Up

- Questions for now
- Slack for questions later
- Come back next week!