# Capturing Their Attention

Utilizing Capture-The-Flag (CTF) Competitions In The Classroom

# Josh Stroschein - @jstrosch

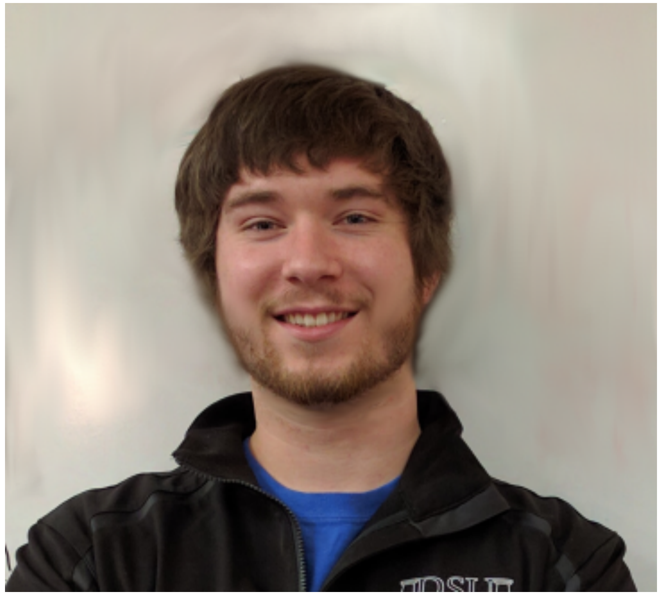
- Dakota State University
  - Assistant Professor Cyber Operations
- VDA Labs
  - IR / AppSec / MA / (Red/Purple/Blue) Team
- Bromium
  - MA
- IA ANG: Cyber Protection Team (CPT)
  - Director of Training
- PluralSight Author
  - MA

joshua.stroschein@dsu.edu

DSU
DAKOTA STATE

# Andrew Kramer

- Dakota State University
  - Instructor of Computer Science and Cyber Security
- Johns Hopkins Applied Physics Lab
  - Cyber Security Intern
- Experienced penetration test engineer
- Master of all things CTF



Andrew.Kramer@dsu.edu

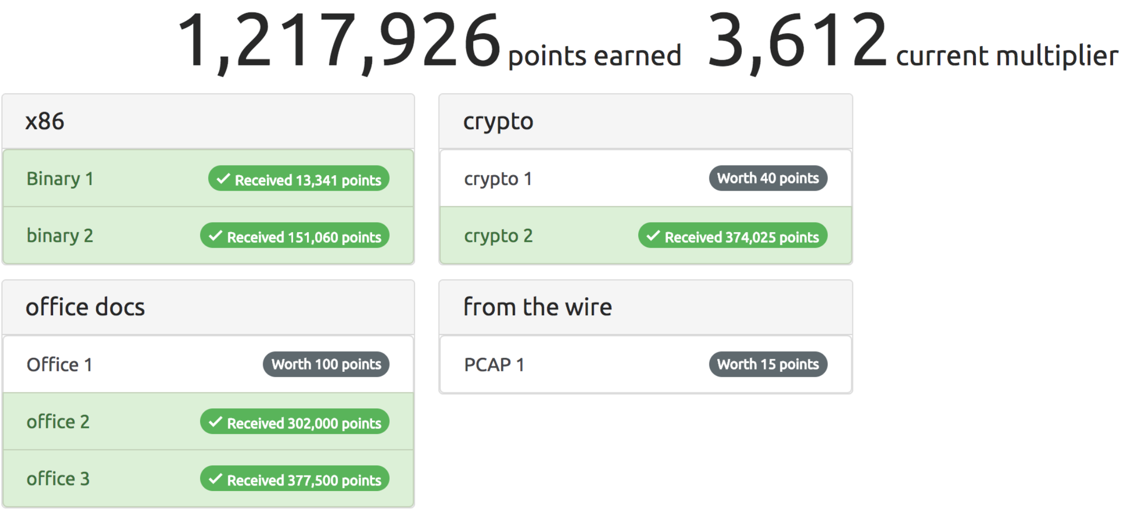
# Capture the Flag (CTF)

- Attack-Defend
  - Blue team / Red team (What about purple?)
  - Typically more logistics in setup, technical know how, on-site presence
  - Example: Collegiate Cyber Defense Competition (CCDC)

- Jeopardy-Style
  - Jeopardy style game board, typically consists of categories and challenges
  - Designed for solo or team effort
  - Generally easier to setup – participants can be remote
  - Example: Flare-On (by Mandiant/FireEye)

# CTF

- Attack/Defend: CCDC @ DSU
- Jeopardy: 0xEvilC0de.com CTF



1,217,926 points earned 3,612 current multiplier

x86

- Binary 1 ✓ Received 13,341 points
- binary 2 ✓ Received 151,060 points

crypto

- crypto 1 Worth 40 points
- crypto 2 ✓ Received 374,025 points

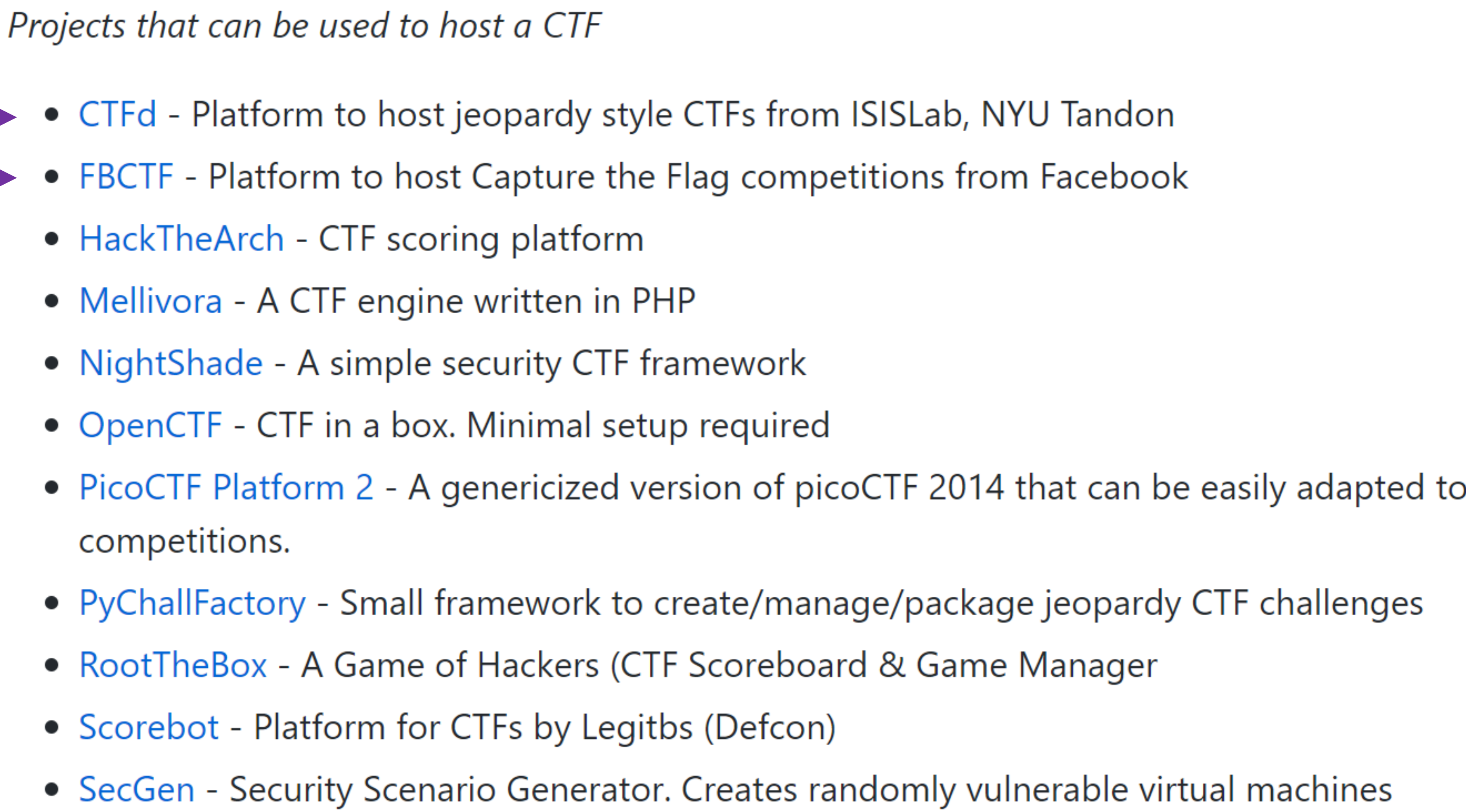
office docs

- Office 1 Worth 100 points
- office 2 ✓ Received 302,000 points
- office 3 ✓ Received 377,500 points

from the wire

- PCAP 1 Worth 15 points

# Popular CTF Platforms



*Projects that can be used to host a CTF*

- CTFd - Platform to host jeopardy style CTFs from ISISLab, NYU Tandon
- FBCTF - Platform to host Capture the Flag competitions from Facebook
- HackTheArch - CTF scoring platform
- Mellivora - A CTF engine written in PHP
- NightShade - A simple security CTF framework
- OpenCTF - CTF in a box. Minimal setup required
- PicoCTF Platform 2 - A genericized version of picoCTF 2014 that can be easily adapted to competitions.
- PyChallFactory - Small framework to create/manage/package jeopardy CTF challenges
- RootTheBox - A Game of Hackers (CTF Scoreboard & Game Manager
- Scorebot - Platform for CTFs by Legitbs (Defcon)
- SecGen - Security Scenario Generator. Creates randomly vulnerable virtual machines

Source: https://github.com/apsdehal/awesome-ctf

# Complications

- Varying levels of technical know-how to setup the framework
  - Many host their code on Github
  - May provide Docker (or similar) images for easier deployment

- Need infrastructure to host
  - Ensure students don’t hack the infrastructure, just the challenges

- Hint/help system
  - What if students get stuck? Is this another opportunity to educate?

# Complications

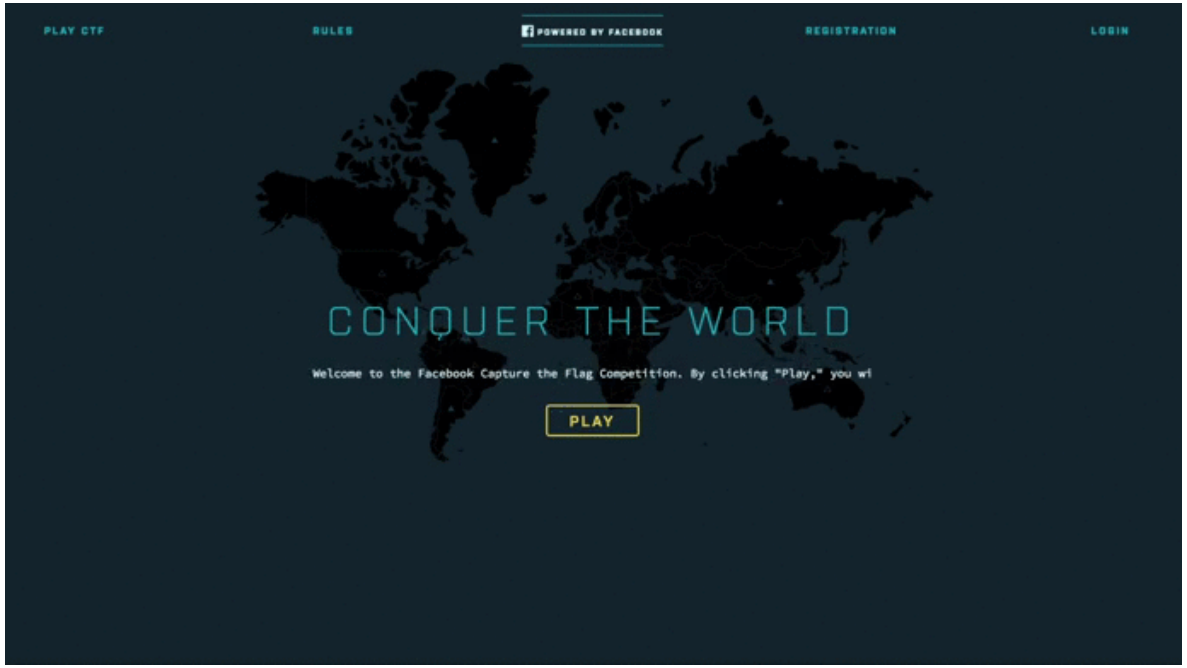
- Challenges, challenges, challenges!
  - Need to create challenges of varying categories and difficulties
  - Goal is generally to educate and engage

- Grading options?
  - Integration with LMS/Grading platform? None that I’m aware of but probably some export options
  - How do you grade teams? How do you grade based on performance?

# Facebook CTF

- On Github - [https://github.com/facebook/fbctf](https://github.com/facebook/fbctf)

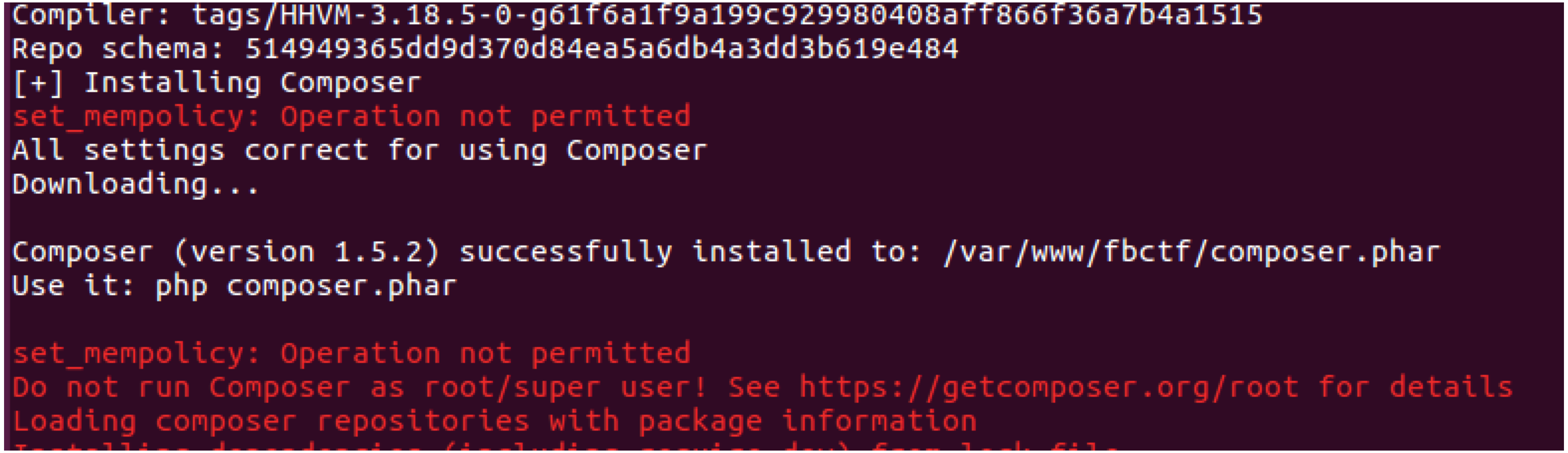
- Installation and Setup
  - Development or Production mode
  - Quick Setup Options
    - Direct Installation
    - Multi-Server Direct Installation
    - Standard Docker Startup
    - Multi-Container Docker Startup
    - Standard Vagrant Startup
    - Multi-Container Vagrant Startup



CONQUER THE WORLD

Welcome to the Facebook Capture the Flag Competition. By clicking "Play," you wi

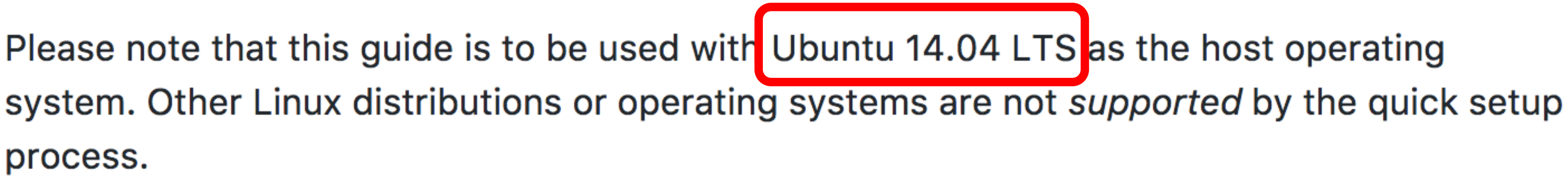
# Facebook CTF



```
Compiler: tags/HHVM-3.18.5-0-g61f6a1f9a199c929980408aff866f36a7b4a1515
Repo schema: 514949365dd9d370d84ea5a6db4a3dd3b619e484
[+] Installing Composer
set_mempolicy: Operation not permitted
All settings correct for using Composer
Downloading...

Composer (version 1.5.2) successfully installed to: /var/www/fbctf/composer.phar
Use it: php composer.phar

set_mempolicy: Operation not permitted
Do not run Composer as root/super user! See https://getcomposer.org/root for details
Loading composer repositories with package information
Installing dependencies (including require-dev) from lock file
```



Please note that this guide is to be used with Ubuntu 14.04 LTS as the host operating system. Other Linux distributions or operating systems are not *supported* by the quick setup process.

# Facebook CTF Levels

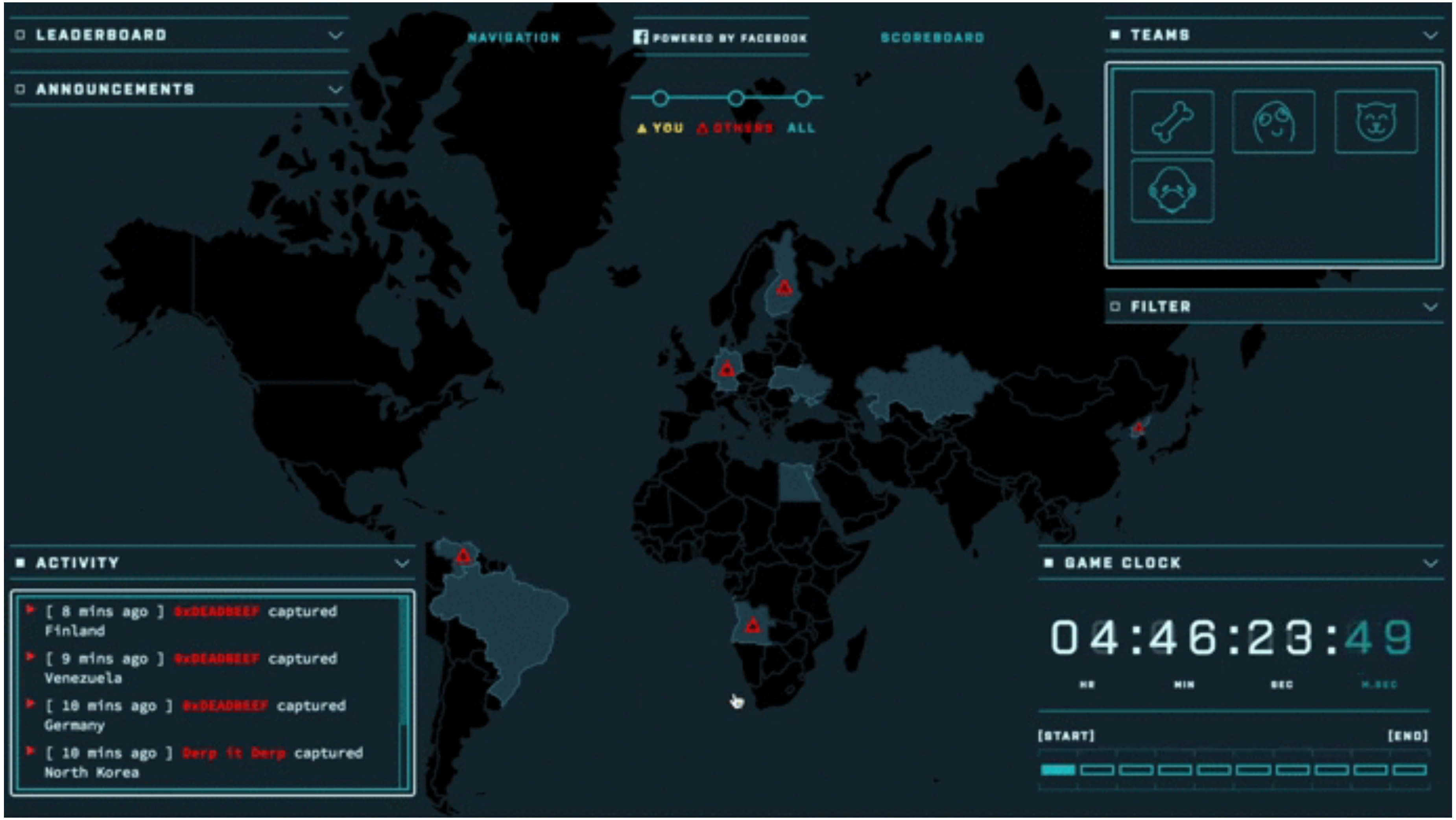
- Quizzes
  - Question and answer format

- Flags
  - Interactive and can include attachments and links
  - Bonus options for point values

- Bases
  - Represent a target system which must be compromised by team to capture points
  - King of the Hill game
  - Must install an agent on the target system(s)

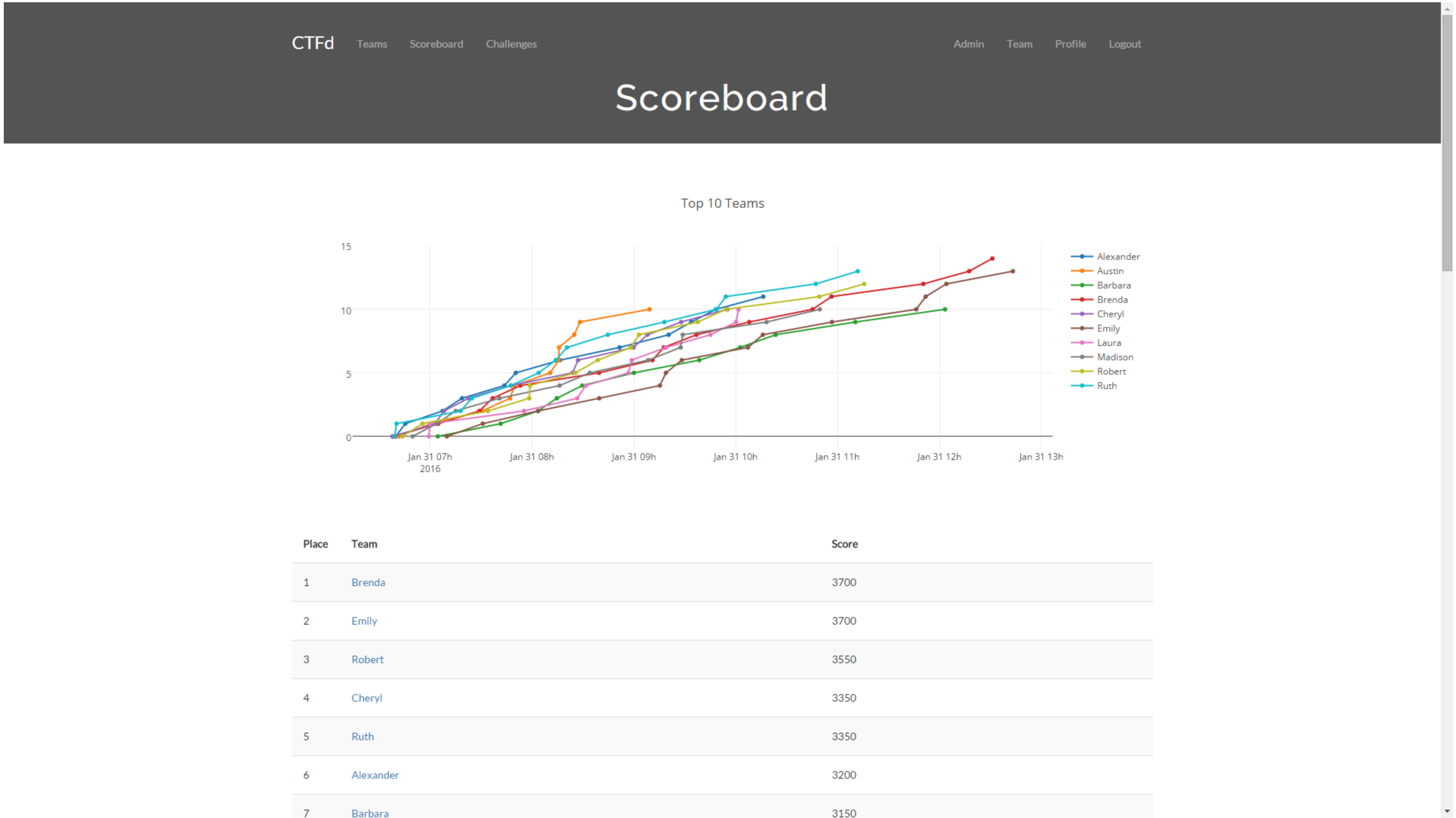
- All allow for hints w/ optional penalty

# Facebook CTF



```
[ 8 mins ago ] 0xDEADBEEF captured
Finland
[ 9 mins ago ] 0xDEADBEEF captured
Venezuela
[ 10 mins ago ] 0xDEADBEEF captured
Germany
[ 10 mins ago ] Derp it Derp captured
North Korea
```

# CTFd



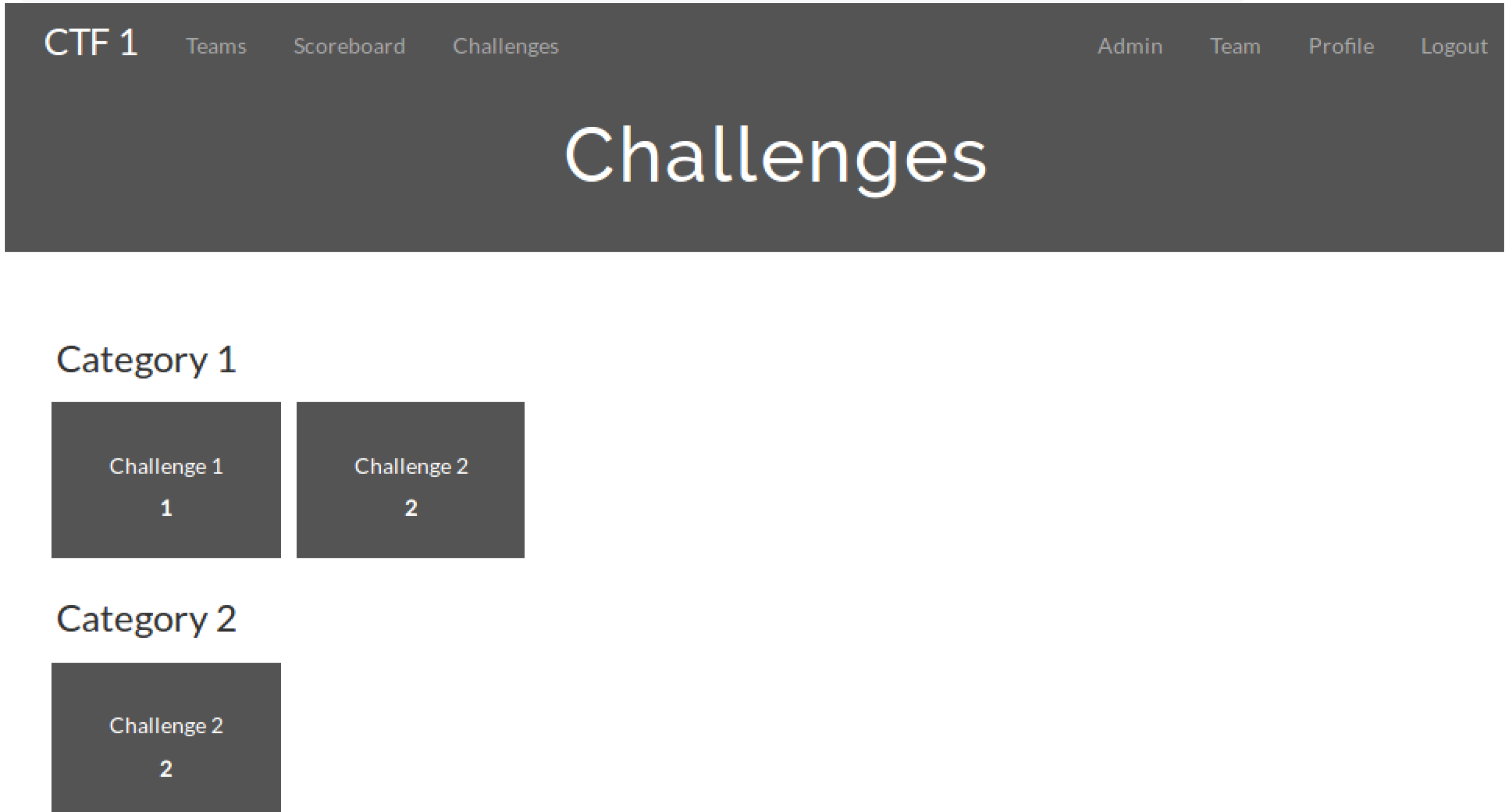
## Scoreboard

| Place | Team | Score |
|---|---|---|
| 1 | Brenda | 3700 |
| 2 | Emily | 3700 |
| 3 | Robert | 3550 |
| 4 | Cheryl | 3350 |
| 5 | Ruth | 3350 |
| 6 | Alexander | 3200 |
| 7 | Barbara | 3150 |

DSU
DAKOTA STATE

# CTFd

- Setting up your own CTFd instance – fairly straight-forward

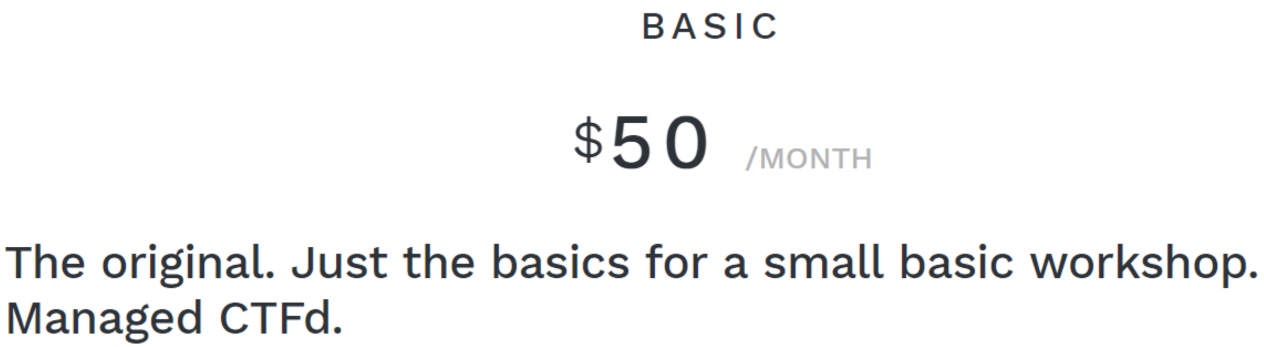


# CTFd

- Not as feature-rich as FBCTF
  - No hint system
  - Jeopardy-style only

- Scoring and statistics

- Offers a managed solution



BASIC

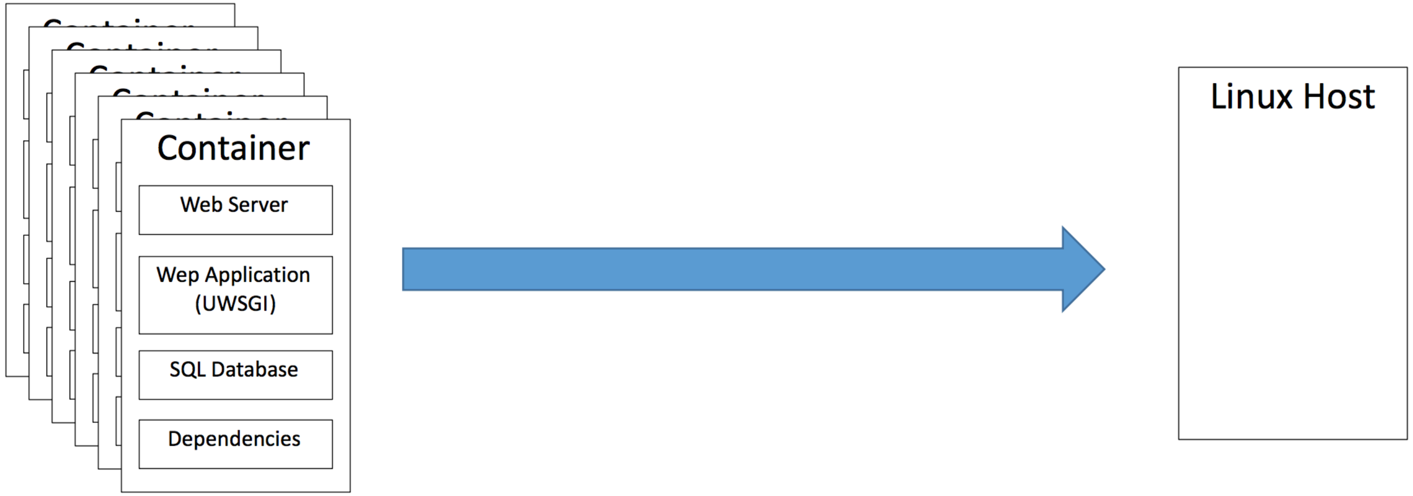
$50 /MONTH

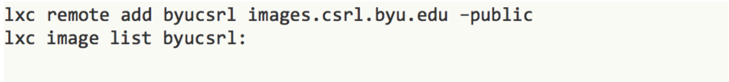
The original. Just the basics for a small basic workshop. Managed CTFd.

# CTF Workshop using LXD Containers

- Presented at 2016 CAE Community Meeting
  - [http://cpsid.et.byu.edu/doku.php?id=ctf:containers](http://cpsid.et.byu.edu/doku.php?id=ctf:containers)

- Goal is to ease the deployment of CTF platforms





```
lxc remote add byucsrl images.csrl.byu.edu –public
lxc image list byucsrl:
```

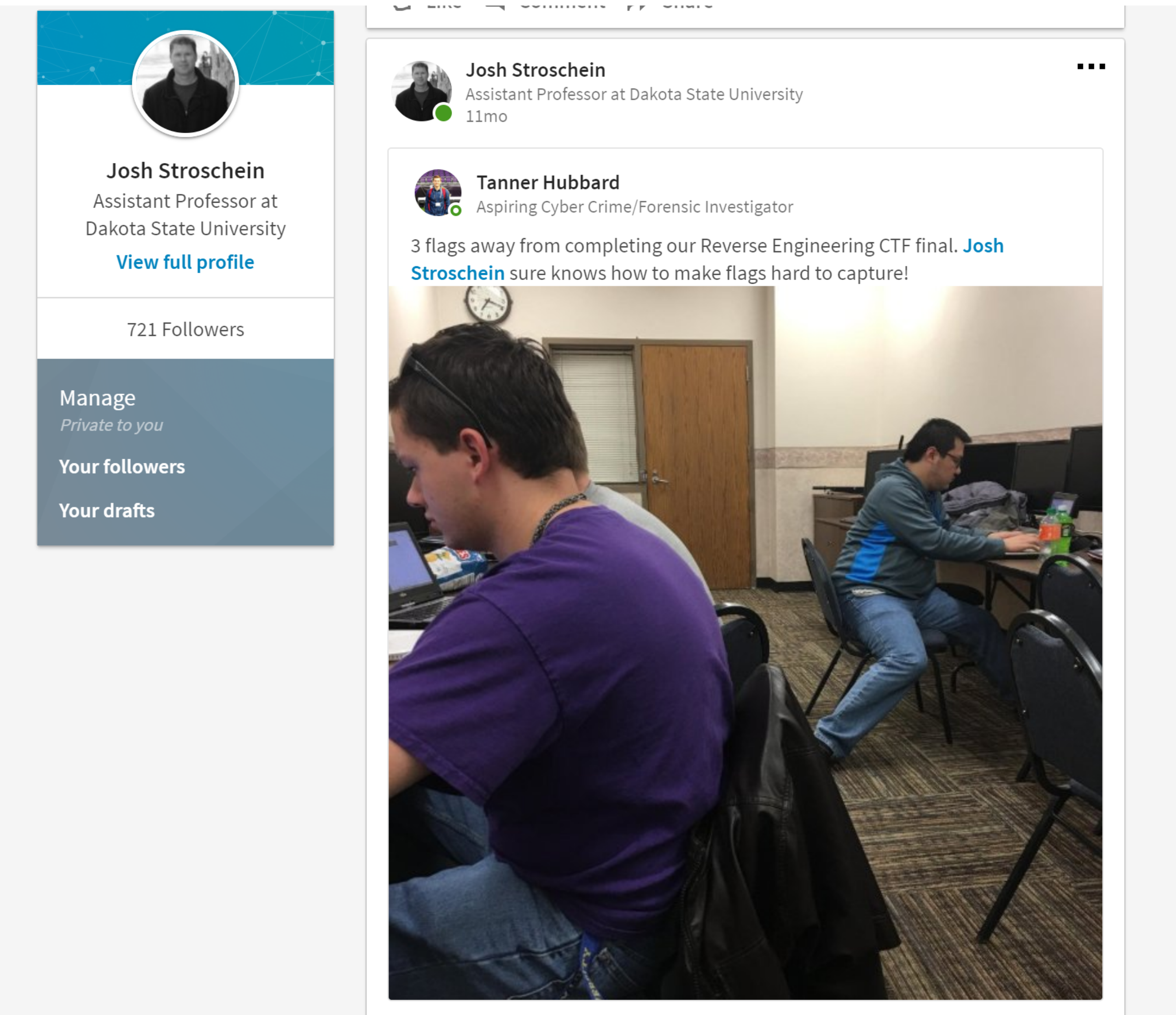
# Successes

- Increase awareness and interest in cyber security
  - Host annual CTF challenge for CAE community
  - ”Advertise” through social media and NSA Tech Talk community

- Use CTF platforms in the classroom
  - Engages both online and on-campus students
  - Experiment with teams versus solo effort – both have pros and cons
  - Often first time students have seen/competed in a CTF
  - Increase exposure to techniques, topics, tools, etc

- Engage undergraduate students in developing the CTF framework
  - Software development experience ++

# Successes



Like Comment Share

Josh Stroschein
Assistant Professor at Dakota State University
View full profile

721 Followers

Manage
*Private to you*
Your followers
Your drafts

Josh Stroschein
Assistant Professor at Dakota State University
11mo

Tanner Hubbard
Aspiring Cyber Crime/Forensic Investigator

3 flags away from completing our Reverse Engineering CTF final. Josh Stroschein sure knows how to make flags hard to capture!

# Failures

- Grading/measurement difficulties
  - Run outside of classroom?
  - Team vs Solo (is collaboration good or bad)

- Run into configuration issues
  - Wrong flags
  - Wrong binaries/files
  - Platform availability issues

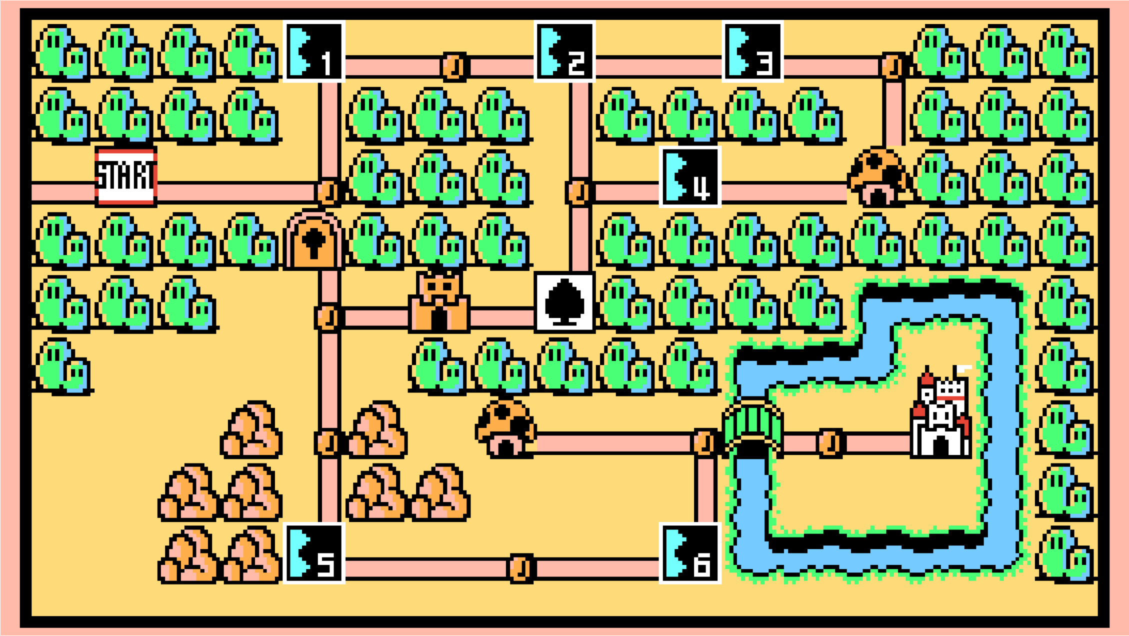
- Time-based element may not be for everyone

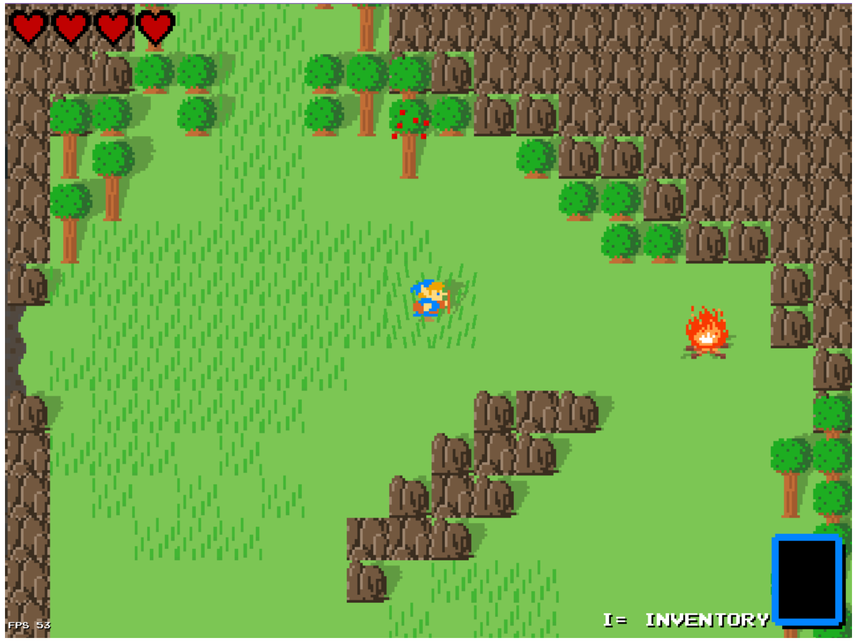
# Introducing 0xEvilCode(.com)

- https://beta.0xevilc0de.com

# Future Work

- Continue gamification of the platform
  - Allow for creation of an RPG-style game board
  - NES Mario 3 graphics + NES Zelda Exploration
  - Expand into K12





# Future Work

- Repository of challenges
  - Created by faculty and students – plan to crowd-source
  - Organized by tags – category, difficulty, requirements, etc to be able to search and discover
  - Record statistics – number of uses, number of solves, user feedback/rating

- Restricted access to org admins

- Quickly create a robust CTF with minimal overhead

- Include detail solutions – understand the challenge and optionally create hints

# Interested?

- To create a CTF you need to have an organization created and be the admin
  - If you want me to create an org for you – send me an email
  - Once you are an org admin, you can create CTFs

- You can sign-up to your mailing list to receive important updates as well as announcements for future events
  - http://eepurl.com/c9RWf5

Joshua.Stroschein@dsu.edu