Cybersecurity Club

at FLORIDA STATE UNIVERSITY

# All About Capture The Flag

# What are CTFs?

- Hacking Competitions!
- Safe way to learn security
- Training Grounds

CTF TIME https://ctftime.org/ctf-wtf

# Who Organizes them?

- Tons of people, companies, universities
- NYU Poly (CSAW)
- DEFCON
- Security Firms (SANS)

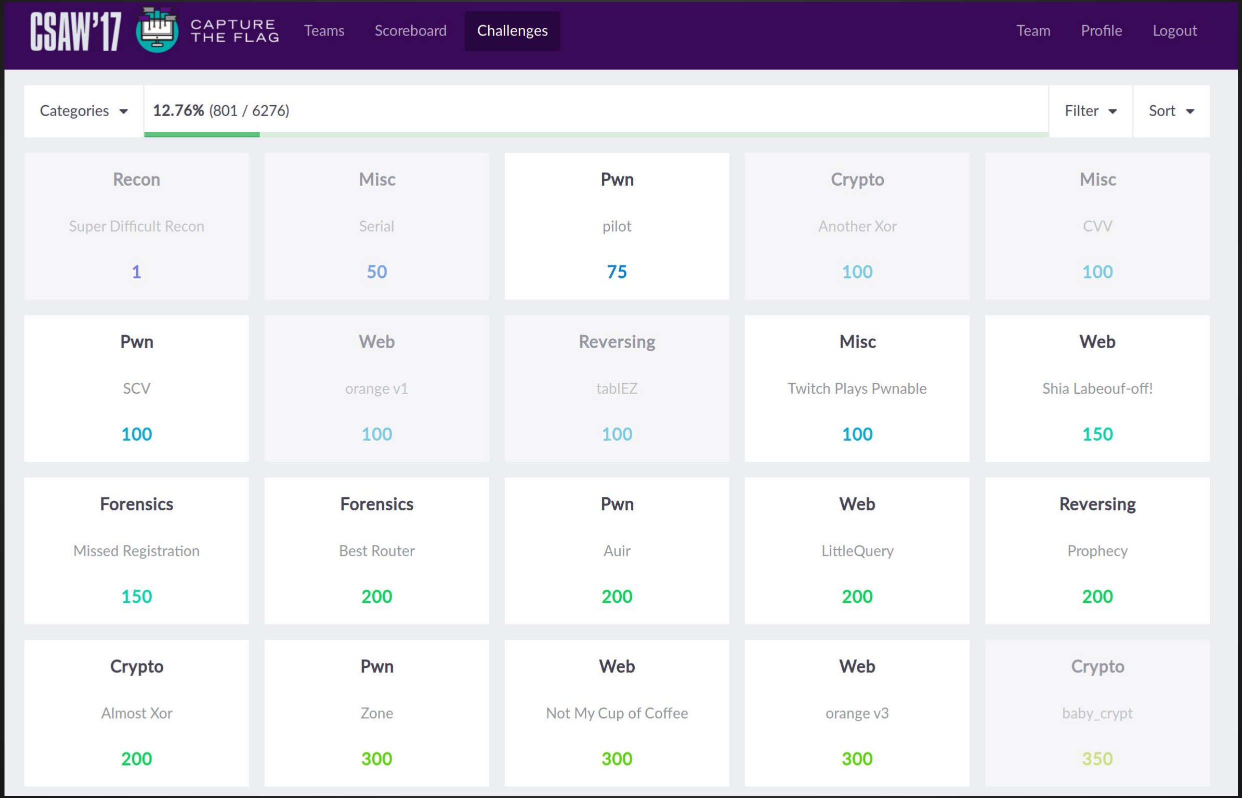
# Styles - Onsite or Remote

- Onsite
  - Typically held during a conference (but not necessarily)
  - DEFCON http://youtu.be/1UT3qXHduts
- Remote
  - Email-based (No cON Name CTF Quals)
  - Web
  - Snail Mail (USB Drive, Raspberry Pi)

# Styles - Attack / Defend

- Attack (Red Team), Defend (Blue Team)
- Defend
  - Servers with services to maintain and protect. Points for uptime or business injections/tasks.
- Attack
  - Exploits need to be developed/discovered to attack other teams. Points deducted from other teams, or gained for the attacker.

# Styles - Jeopardy



**12.76%** (801 / 6276)

| | | | | |
|---|---|---|---|---|
| Recon<br>Super Difficult Recon<br>1 | Misc<br>Serial<br>50 | Pwn<br>pilot<br>75 | Crypto<br>Another Xor<br>100 | Misc<br>CVV<br>100 |
| Pwn<br>SCV<br>100 | Web<br>orange v1<br>100 | Reversing<br>tablEZ<br>100 | Misc<br>Twitch Plays Pwnable<br>100 | Web<br>Shia Labeouf-off!<br>150 |
| Forensics<br>Missed Registration<br>150 | Forensics<br>Best Router<br>200 | Pwn<br>Auir<br>200 | Web<br>LittleQuery<br>200 | Reversing<br>Prophecy<br>200 |
| Crypto<br>Almost Xor<br>200 | Pwn<br>Zone<br>300 | Web<br>Not My Cup of Coffee<br>300 | Web<br>orange v3<br>300 | Crypto<br>baby_crypt<br>350 |

# Common Categories

- Recon
- Forensics
- Networking
- Programming
- Exploitation
- Mobile Security

- Reversing
- Cryptography
- Web
- Trivia
- Miscellaneous
- Steganography

# Trivia

- Google Searches
- Hacker Culture
- “Hack The Planet”

# Recon

- Find everything you can about a target
- Fuzyll Challenge - Dota Replay
- Julian Cohen - OKCupid profile
- Kevin Chung - High School photo

# Web

- SQLi
- XSS
- API Information Disclosure
- Command Injection / Escapes

# Exploit

- Strings / File / Tricks
- Memory Exploitation
- Sandbox Escapes
- Information Leakage

# Reversing

- Strings / File / Tricks
- Compressed Files
- Obscure Systems

# Forensics / Networking

- PCAP Files
- Log Files
- File Systems / Obscure things

# Programming / Scripting

- Python
- Netcat
- Ex: Answer a math problem correctly 1000 times in a minute.

# Steganography

- Hiding data in media. (Picture/Audio files)
- Gimp
- Audacity

# Resources

# Events & Meetings

- CTF Competitions
- Cybersecurity Club meetings Thursdays 5:00pm in Shores 206 (Goldstein Library)
- Weekend Hacking Meetings (Variable times/location)

# n0l3ptr (Who to ask??)

- Mitch Schmidt: Crypto, Exploitation, Python
- Nathan Nye: Web, Linux
- Shawn Stone: Reversing, Exploitation, Forensics
- Brandon Everhart: Reversing, Beginner Questions, Team Questions

# Write Ups

- https://github.com/n0l3ptr
- https://ctftime.org
- http://cybersecurity.fsu.edu/club/

# Team Communication

- https://n0l3ptr.slack.com
  - Join channel: “ctfgroup”
- Club Email List
- Facebook: Cybersecurity Club @ FSU

# Books

- Hacking The Art Of Exploitation
  - Jon Erickson