

Cyber@UC Meeting 50

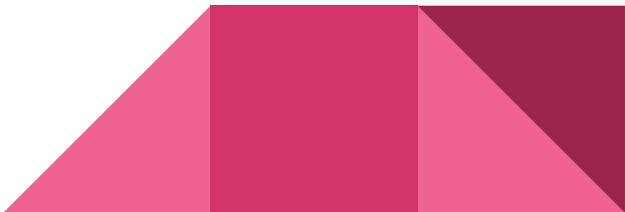
Systems Exploitation with Metasploit

If You're New!

- Join our Slack: ucyber.slack.com
- **SIGN IN!** (*Slackbot will post the link in #general*)
- Feel free to get involved with one of our committees:
Content Finance Public Affairs Outreach Recruitment
- Ongoing Projects:
 - Malware Sandboxing Lab
 - Cyber Range
 - RAPIDS Cyber Op Center

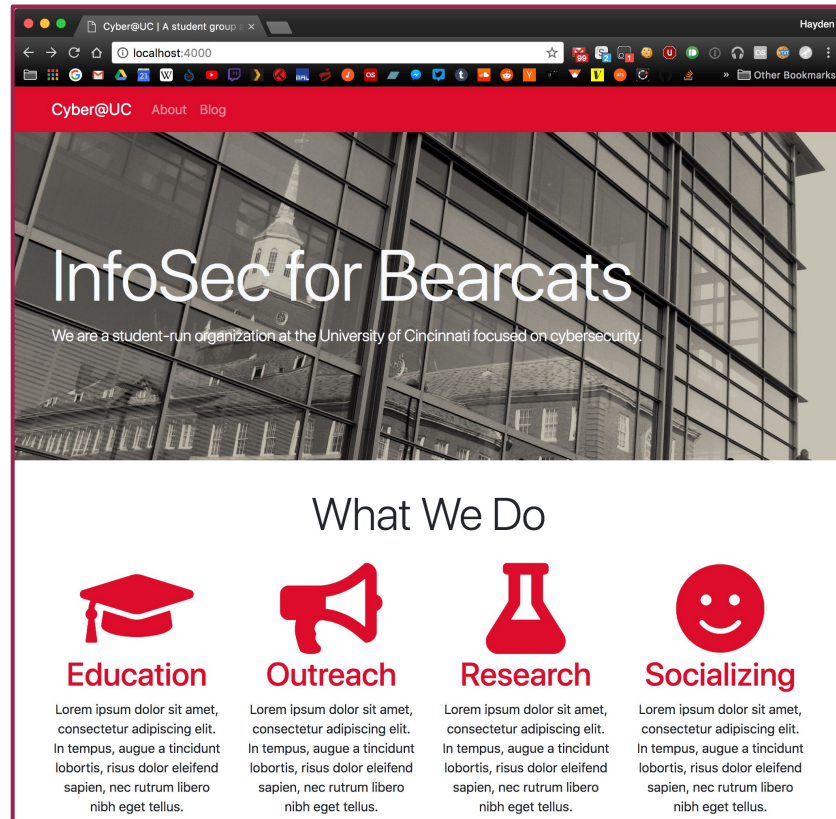


Announcements

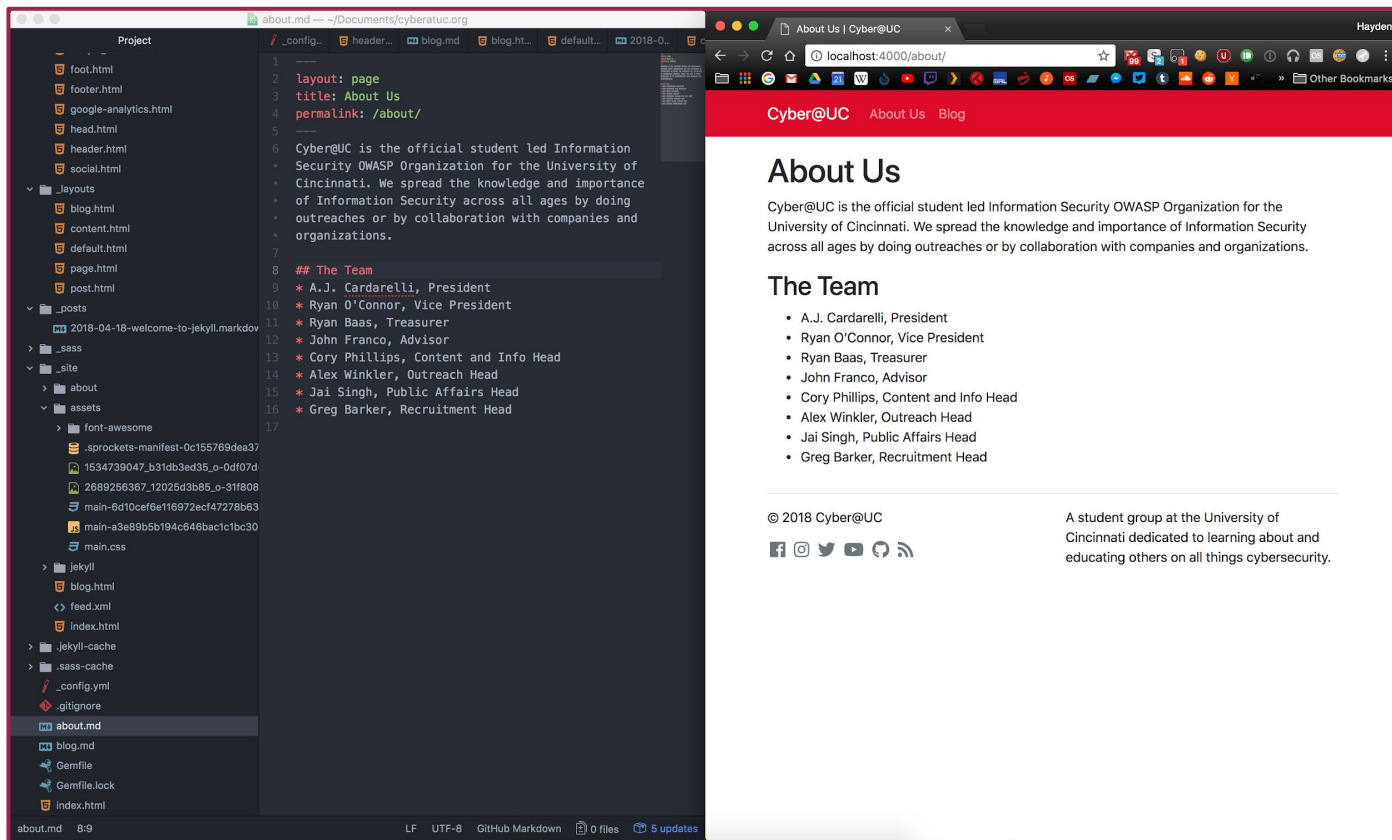
- **GOOD LUCK WITH EXAMS!**
 - Elections postponed to fall
 - **ThinkCyber Fellowship** July 13–16 think-cyber.com
 - **Smart Cincy** Conference, April 25–26 smartcincy.org/uc-summit-registration
 - Partnership with **Galois** in the works
 - **BSides** Saturday May 12
 - Outreach: **Next Tuesday** to **Lakota East**
- 

New website

- Progress finally being made!
- Using Jekyll, Bootstrap
- Check it out: cyberatuc.ox3.in
- Code on GitHub:
github.com/UCyber/cyberatuc.org



New website



If you can use
Markdown and
GitHub, you can
edit this site.

Public Affairs

Useful videos and weekly livestreams (except this week 🐼) on **YouTube**:

youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw

Follow us for club updates and cybersecurity news:

- **Twitter:** [@CyberAtUC](https://twitter.com/CyberAtUC)
- **Facebook:** [@CyberAtUC](https://facebook.com/CyberAtUC)
- **Instagram:** [@CyberAtUC](https://instagram.com/CyberAtUC)

For more info: ucyber.github.io



Weekly Content

Power Hammer

- Malware used to exfiltrate data through powerlines
- Manipulates the CPU to regulate power utilization
- Data is then transmitted over the current flow
- An attacker then measures the emissions
- Can be exfiltrated at a rate of 10 or 1000 bits/sec depending on where the emission is being read from



<https://arxiv.org/pdf/1804.04014.pdf>

Intel Threat Detection

- Threat Detection Technology and Security Essentials
- Offer hardware-based built in security and improve threat detection without compromising performance
- TDT allows accelerated memory scanning and advanced platform telemetry
- Accelerated memory scanning allows av programs to use intel's integrated GPU to scan and detect memory-based malware attacks while reducing impact on performance and power consumption
- In testing, using the built in GPU reduced CPU utilization from 20% to 2%



Intel Threat Detection (continued)

- Advanced Platform Telemetry incorporates cloud-based learning and endpoint data collection to better identify potential security threats and reduce false positives and minimize performance impact
- Will be available in 6,7, and 8th gen intel processors but needs to be used by av vendors
- Microsoft and Cisco are already making use of it

<https://thehackernews.com/2018/04/intel-threat-detection.html>





Part 10: Exploitation w/ Metasploit

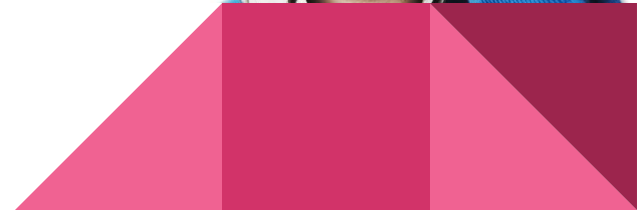
Witty jokes return

The Topics Today Go Something Exactly Like This

- MSF Setup
- Target Setup
- Metasploitation



Put on your ~~3D glasses~~ Linux Distro now



Forewarning, Metasploit is live ammunition

- Do not play with live tools outside of a controlled environment
- Do not try and exploit other person's computers without permission
- Failure to follow the above advice may result in the Computer Fraud and Abuse Act being thrown at you



Tool Overview: Metasploit Framework (MSF)

- <https://www.metasploit.com/>
- Open source tool sponsored by **Rapid7**
- Widely used
- Ties together so many things (exploits, scanners, tools, etc) that one slide will never be able to explain it
- Holds 1700+ exploits and ~500 payloads to unload on a target



Metasploit looks like this



We'll make it look more like this



Setup

Kali:

- Already installed

Docker:

- `docker run -i -t --name MSF metasploitframework/metasploit-framework`

Anything Else:

- Use premade installer or install docker



Usage Overview

1. Configure Exploit
2. Check Target Susceptibility (Should probably be #1)
3. Configure Payload
4. Obfuscate via Encoding (Hides from firewalls & IDS)
5. Execute



Commands to start with

Start Metasploit backend with **service postgresql start** if on kali

Search <keyword> - Look for tools related to keywords

Throw

Set - Sets a exploit variable

Sessions - Play with the shells you've opened on remote hosts

