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



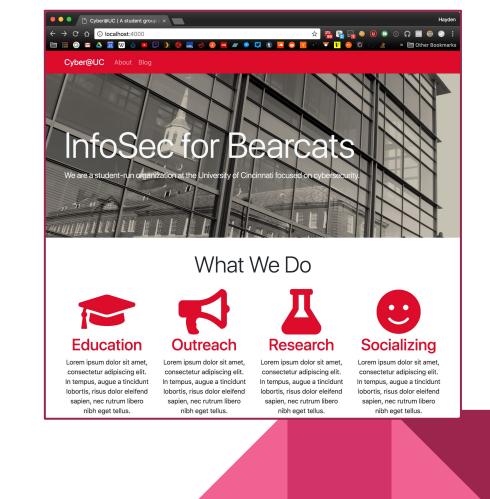
Announcements

- GOOD LUCK WITH EXAMS!
- Elections postponed to fall
- ThinkCyber Fellowship July 13–16 think-cyber.com
- Smart Cincy Conference, April 25–26 <u>smartcincy.org/uc-summit-registration</u>
- 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: <u>github.com/UCyber/cyberatuc.org</u>



New website

000	about.md — ~/Documents/cyberatuc.org		
Project	/ _config 5 header CI blog.md 5 blog.ht 5 default CI 2018-0	📕 🔍 🕛 About Us Cyber@UC 🛛 🗙	
		← → C ☆ ③ localhost:4000/about/	🖈 🐕 🖓 🖓 🐠 🔍 🗈 🙃 📾 🦃
5 foot.html	2 layout: page	🖷 🖿 🏭 🎯 🖬 🛆 🖻 🔍 👌 💷 💭 🔪 (🦓 🔜 🤌 😰 🐻 🖉 🔗 🔽 🕄 🦉 🚱 💟 👘 🔺 🗎 Other B
5 footer.html	3 title: About Us		
5 google-analytics.html	4 permalink: /about/	Cyber@UC About Us Blog	
5 head.html			
5 header.html	6 Cyber@UC is the official student led Information		
5 social.html	 Security OWASP Organization for the University of 	About Us	
∽ 🛅 _layouts	Cincinnati. We spread the knowledge and importance		
5 blog.html	of Information Security across all ages by doing outreaches or by collaboration with companies and	Cyber@UC is the official student le	ed Information Security OWASP Organization for the
5 content.html	organizations.	University of Cincinnati. We spread	d the knowledge and importance of Information Security
5 default.html	7	across all ages by doing outreache	es or by collaboration with companies and organizations.
5 page.html			
😇 post.html	9 * A.J. Cardarelli, President	The Team	
✓ im _posts	10 * Ryan O'Connor, Vice President	 A.J. Cardarelli, President 	
2018-04-18-welcome-to-jekyll.markdor	11 * Ryan Baas, Treasurer	Ryan O'Connor, Vice President	and the second se
> 💼 _sass	 * John Franco, Advisor * Cory Phillips, Content and Info Head 	Ryan Baas, Treasurer	
✓ ■ _site	14 * Alex Winkler, Outreach Head	 John Franco, Advisor 	
> 🛅 about	15 * Jai Singh, Public Affairs Head	Cory Phillips, Content and Int	felleed
🗸 🛅 assets	16 * Greg Barker, Recruitment Head	Alex Winkler, Outreach Head	
> 💼 font-awesome		Jai Singh, Public Affairs Head	
.sprockets-manifest-0c155769dea3		Greg Barker, Recruitment He	
1534739047_b31db3ed35_o-0df07d		- oreg barker, Recruitment he	sau
2689256367_12025d3b85_o-31f808			
main-6d10cef6e116972ecf47278b63		© 2018 Cyber@UC	A student group at the University of
JS main-a3e89b5b194c646bac1c1bc30		© 2010 Cyber@0C	Cincinnati dedicated to learning about and
🗃 main.css		H 🖸 🗡 🗖 🗘 🆤	educating others on all things cybersecurity.
> 📷 jekyll			caddalling others on an things cybersecurity.
5 blog.html			
<> feed.xml			
5 index.html			
> 🛅 .jekyll-cache			
> 🛅 .sass-cache			
🥖 _config.yml			
.gitignore			
m∎ about.md			
Mi blog.md			
🔫 Gemfile			
🔫 Gemfile.lock			
5 index.html			
about.md 8:9	LF UTF-8 GitHub Markdown 🖹 0 files 🗊 5 updal	s	

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

Hayden

0 n 🔤 🎯 . :

» 🛅 Other Bookmarks

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: @<u>CyberAtUC</u>
- Facebook: @<u>CyberAtUC</u>
- Instagram: @CyberAtUC

For more info: <u>ucyber.github.io</u>



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

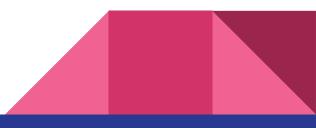
https://arxiv.org/pdf/1804.04014.pdf





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)

- <u>https://www.metasploit.com/</u>
- 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

