Cyber@UC Meeting 37

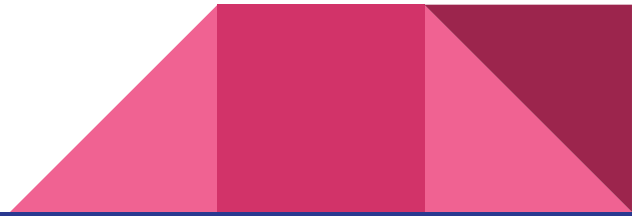
Welcome Back!

If You’re New!

- Join our Slack **ucyber.slack.com**
- Follow us on **Twitter @UCyb3r**
- Feel free to get involved with one of our committees: **Content, Finance, Public Affairs, Outreach, Recruitment**
- Stay updated through our weekly emails and **SLACK**

Announcements

- **P&G visit set for Jan 22nd 2-3pm**
- **ERC Lab** should be open this semester
- Work on **Malware Sandboxing System** to begin soon (Thursday)
- Logo designs welcome!

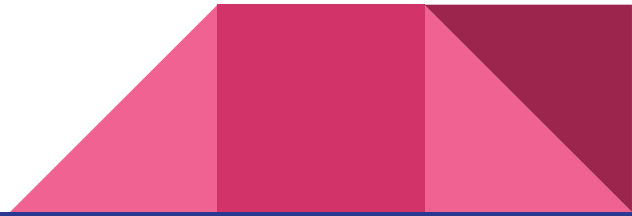


Meet the Exec’s

Semester Goals

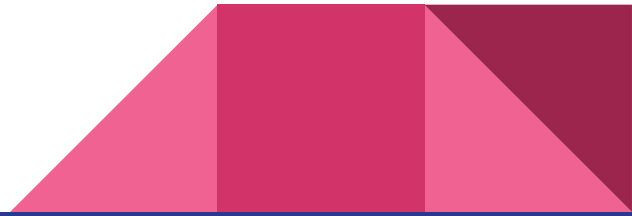
Certified Ethical Hacker

- https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
- Great certification to have in the field.
- We will attempt to get funding to cover test costs
- School of IT to provide materials



School Outreach

- Highly encourage all members to reach out to there HS CS teachers for us to visit!
- Topics we can cover range from basic bash, networking, to more complex cyber concepts



Advice/Ideas?

P&G Visit

- January 22nd
- 2pm

P&G Corporate Engineering Technologies Laboratory

8256 Union Centre Blvd

West Chester, OH 45069

Weekly Content

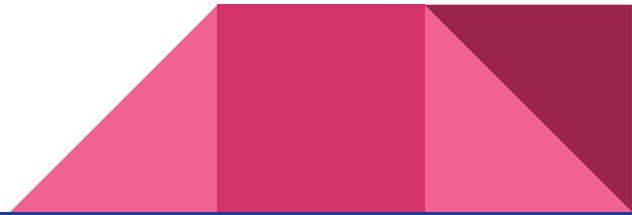
Meltdown & Spectre

- What is it?
  - Meltdown (CVE-2017-5754)
  - Spectre (CVE-2017-5753 and CVE-2017-5715)
  - Vulnerability that “could allow attackers to steal sensitive data which is currently processed on the computer.”
  - Larger threat to servers
  - Both processor based
  - No processor safe

https://thehackernews.com/2018/01/meltdown-spectre-vulnerability.html

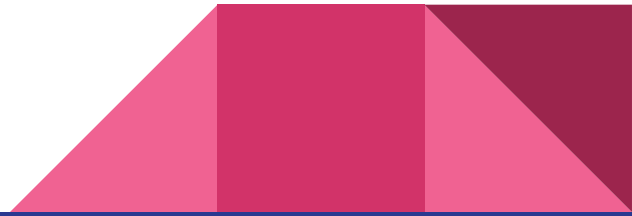
Meltdown

- Uses Out of Order Execution to break Isolation
- Out of order Execution
  - found in multithreading (processor level)
  - Predicted branch will leave data in cache
- Patch Already made (but it SUCKS)
  - KAISER patch
  - Isolating Page Tables, so user and kernel don’t work together
  - 40% performance drop
  - Circumvents much of the effects of Branch prediction



Spectre

- Forces targeted programs to access memory that it doesn’t need, then reads those programs through a side channel
- Can work across VM’s and onto hypervisors
  - Works below the level of the hypervisor
- Patches currently coming out
  - Really hard to patch since it is a HW issue



Turning an AV into a perfect spy

- AV softwares actually have a lot in common with some of the best malware out there
  - Persistence, scanning, automatic updates, upload capability, self-defense, anti-analysis
- One example of how these protectors can be turned into an enemy is that they can be easily changed to scan for classified files on a computer, like the example I found using Kaspersky
- Within /Library/Application Support/Kaspersky Lab/KAV/Binaries/kav the core of the anti-virus scanning and detection code can be found
- US government documents that contain “sensitive” information are marked TS/SCI

https://objective-see.com/blog/blog_0x22.html

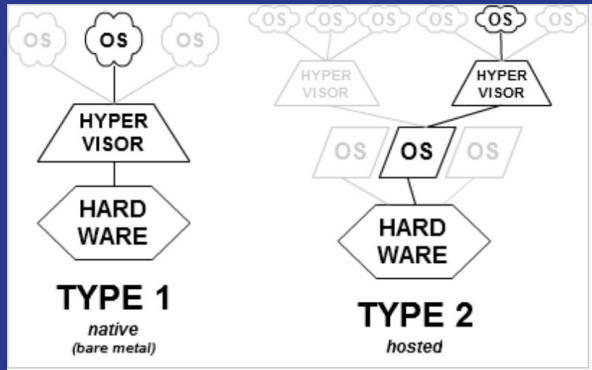
Setting up a VM
Breakout Session

How Does it Work?

Shares computer resources

https://en.wikipedia.org/wiki/Hypervisor

- VM Player and VirtualBox are *HOSTED* hypervisors
- A VM is considered a *GUEST* machine
- Your computer is the *HOST* machine



VM Workstation Player or VirtualBox

VM Workstation Player

- Only supports Linux and Windows
- 64bit OS’s only
- Pay for full feature set
- Single VM per window at a time
- Widely used at the enterprise level

VirtualBox

- Supports all OS’s
- Open Source and FREE
- Multiple VM’s per window
- Can configure by command line
- Support for many open source projects (Cuckoo)

*Might need to go into bios and turn on virtualization