

# Cyber@UC Meeting 32

Setting up a VM Lab

# If You're New!

- Join our Slack **ucyber.slack.com**
- Follow us on **Twitter @UCyb3r** and Facebook UC.yber; University of Cincinnati OWASP Chapter
- 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

*Happy late Halloween*

- **October 27/28th** was the **ACM** programming challenge
- **CharitEweek** from Nov. 13th-Nov. 17th
- **Red team** against Franco's Class! *Nov. 30th - 1st Dec.*
- Reached out to **P&G** again for a tour of their **cybersecurity operations center**
- **Logo Design** Competition




The background is a solid pink color. In the top right corner, there are several overlapping geometric shapes: a dark pink square, a medium pink square, and a light pink square, all partially cut off by the edge of the frame.

# Weekly Info Session

# Firefox 58 will block fingerprinting by default

- HTML 5 Canvas allows dynamically drawn graphics on web pages
- Being used to track and potentially identify users across websites by secretly fingerprinting their web browser
- The Canvas' ability to draw unique images lets each user's device to be assigned a number to identify it
- This works, even if cookies are turned off
- Also used in identify theft and credit card fraud detection
- The fingerprints are used to detect when a specific user visits websites to create a profile of their browsing habits and the info is shared with advertisers
- Users have previously been forced to use third party plug-ins
- This feature is already available in Firefox's prerelease version

# Reaper (update)


- IoT malware using exploits in cameras and recording devices to create a botnet
  - An additional 2 million potential hosts have been identified that haven't been added to the botnet yet, likely because the spread was slowed by the coders to keep under the radar
  - They believe that the botnet will be used as an attack for hire service, known as a booter or stresser service, like the Chinese DDoS for hire market
  - They believe reaper to be a product of the criminal Chinese underground
- 

# Reaper (update continued)

- They know a certain number of devices in the networks they had access to were infected, therefore they can make an estimate on the total number of devices infected
- Between Check Point and Netlab360, they have found over 58k infected devices



# Gaza cybergang a rising threat

- Politically motivated, arabic-language based cybercriminal group
  - Operating since 2012
  - Target MENA(Middle East North Africa)
  - Targets include oil/gas, media, activists, politicians, government embassies
  - Primarily intelligence seeking
  - Previously relied on remote access trojan's RATs like Cobalstrike payloads
  - Send malware as compressed email attachment
  - Have recently moved to their first zero-day exploit
  - Focus on humanitarian and political causes in their social engineering
  - Show signs of moving to mobile malware
- 



# Sources

<https://thehackernews.com/2017/10/canvas-browser-fingerprint-blocker.html>

[https://en.wikipedia.org/wiki/Device\\_fingerprint](https://en.wikipedia.org/wiki/Device_fingerprint)

<https://krebsonsecurity.com/2017/10/fear-the-reaper-or-reaper-madness/#more-41321>

<https://securelist.com/gaza-cybergang-updated-2017-activity/82765/>





# Setting up a VM

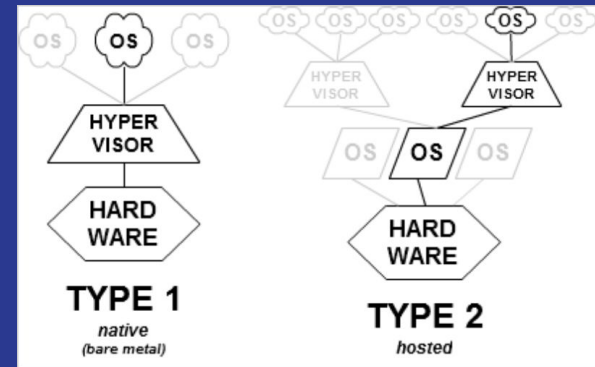
## *Breakout Session*

# 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