Cyber@UC Meeting 48

Docker for easy tool demos!

If You’re New!

- Join our Slack **ucyber.slack.com**
- **SIGN IN!**
- 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

- **April 12th CTF** at NKU
- **Labspace design** has been finalized
- Cincinnati B-Sides on **May 12th**, registration not open yet
- Tabling **this Tuesday** went great!

OC3 website

- Wrapping up by tomorrow
  - god have mercy on my soul
- Sneak peek: test.ohioc3.org

Public Affairs

- Please fill out Google form for **GroupMe** Numbers!
  https://goo.gl/forms/94i9kMJgtpDGXsC22

- Our brand new **YouTube** channel has just been made. We will be live streaming meetings, events, etc and posting relevant videos to the channel. Please subscribe!
  youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw

Follow us on our social media:

Facebook:	facebook.com/CyberAtUC/
Twitter:	twitter.com/UCyb3r
Instagram:	instagram.com/cyberatuc/
Website:	ucyber.github.io

Weekly Content

Atlanta held hostage

- Atlanta hit by ransomware, sent by SamSam hacking crew
  - SamSam believed to have sucessfully extorted >$1,000,000
  - Target hospitals, police, universities: have money, but can't afford to go offline
  - SamSam group is believed not to be native English speakers
- Ransom demand of $51,000
- Many major city systems tied up, critical systems like 911 were unaffected
- Courts can't validate warrants, police reports written by hand
- As of yesterday, many services are still not available, the wifi in airports is currently still off
- They don't think any confidential data was leaked
  - They are proceeding as if it has been

Atlanta ransomware(sources)

https://www.cnn.com/2018/03/27/us/atlanta-ransomware-computers/index.html

https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news&mtrref=www.nytimes.com

https://www.theatlantic.com/technology/archive/2018/03/atlantas-boring-ransomware-attack/556673/

State Department Bug Bounties

- A bill was introduced to congress that would setup a bug bounty program for vulnerabilities found in state department websites
- The secretary of State could decide what is included in the program and what types of vulnerabilities should be targeted, but there would be a requirement to report the # and severity of vulnerabilities found each year
- "We know that state-sponsored actors and black-hat hackers want to challenge and exploit our networks. We know that. What we didn't fully appreciate before this pilot was how many white-hat hackers there are who want to make a difference, who want to help keep our people and our nation safer," Secretary of Defense, Ash Carter

State Department Bug Bounties(continued)

- A pilot program from 2016: “Hack the Pentagon”
  - 1,400 hackers attempted to find vulnerabilities
  - 138/240 reported vulns were bounty eligible
  - $75,000 in prizes awarded, $150,000 total cost
  - Estimated using an outside firm would have cost $1 million

http://thehill.com/policy/cybersecurity/379283-house-lawmakers-introduce-state-department-bug-bounty-program

“Hack Back” Bill

- Would allow victims of attacks to attack back if the goal is to disrupt, monitor/attribute an attack, or destroy stolen files, beaconing
- Does not allow counterattackers to destroy anything other than their own stolen files and requires the FBI National Cyber Investigative Joint Task Force be notified
- Active defense: describes measures taken to slow attackers through deception or movement of files, not hacking an attacker
- Concern this bill could create more victims, and incite corporate wars

Hack Back sources

http://thehill.com/policy/cybersecurity/355305-hack-back-bill-hits-house

http://thehill.com/policy/cybersecurity/359526-controversial-hack-back-bill-gains-supporters-despite-critics

https://www.cyberscoop.com/tom-graves-active-defense-hack-back-bill-new-industry/

Part 9:
Enumeration Lab

Hack of the week:

GPS spoof your friends’ phones as they play Pokemon Go so they get banned and pay attention to your conversation

The Topics Today Go Something Exactly Like This

- VM & Container Theory / Comparison
- Installing Docker
- Playing with Docker
- OpenVAS Container Installation
- Look For Cool Containers

What is Docker?

- It’s a really really really small VM
- Doesn’t emulate hardware, only software
- ~~We're not shipping your machine~~
  - We are now shipping your machine as a text file
- Allows deployment of very large, complex software systems in a reproducible, simple way

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

Installing Docker

- Download: docker.com/community-edition
- Other containerizing softwares exist but Docker is the most mainstream one

Using Docker

- `docker` — Shows all Docker commands, there are quite a few
- `docker run` — Creates and starts a new container
- `docker start` — Starts an existing container
- `docker stop` — Stops a running container
  - Containers made with the ‘`--rm`’ flag will be deleted when stopped
- `docker ps -a` — Show all containers, running or stopped

OpenVAS Terminology

NVT: Network Vulnerability Test

CVE: Common Vulnerabilities and Exposures is a dictionary of publicly known information security vulnerabilities and exposures.

CVSS: The Common Vulnerability Scoring System (CVSS) is an open framework to characterize vulnerabilities.

Using the OpenVAS Container

```
docker run -d -p 443:443 --name openvas mikesplain/openvas
```

- Takes up to 5 minutes to start up the first time
  - Beats setup time for a host installation of OpenVAS (~15 minutes)
- Go to https://localhost when it’s ready
- Default credentials are admin/admin
- Play around with a scan on your local device

Using the OpenVAS Container Cont.

docker run -d -p 443:443 -e OV_PASSWORD=securepassword41 --name openvas mikesplain/openvas

- Changes the admin password

docker exec -it openvas bash

- Allows you to interact with the container via bash

- Update NVT’s and CVE’s via: **greenbone-nvt-sync**
- Then to finalize the changes: **openvasmd --rebuild --progress**