

Cyber@UC Meeting 47

POC CVEs and Scanning

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

- **\$1000** should be handed over soon
- **Labspace design** has been finalized
- Cincinnati B-Sides on **May 12th**, registration not open yet
- **Static IP** for our server should be coming soon
- Tabling **this Tuesday** in Baldwin



OC3 website

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



Tabling in Baldwin

- When?
 - April 3rd (Tuesday), 9am - 2pm
- What?
 - We are going to have a table for people to stop at to talk to us to learn more about what we do and who we are.
- Why would people approach us?
 - Well we plan to have drink and some **BILL'S DONUTS!** Plus AJ is helping put together a demo!
- Where?
 - Baldwin lobby
- We ask that you please tell people you may think could be interested to come by, and at a minimum get a donut. Also we need some volunteers to be there who can talk to people and tell them about our chapter.





Public Affairs

- Please fill out Google form for **GroupMe** Numbers!
<https://goo.gl/forms/94i9kMJgtpDGXsC22>
- Our brand new **YouTub**e 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

Hacker Conventions, Why attend?

- Networking
- Competitions
- Technical talks
- Lots of fun!!!




Bsides

- InfoSec conference focused on presenting and participating in talks and collaborations
- Lots of bsides conferences around the world
- A calendar of BSides conference dates and locations can be found on their website <http://www.securitybsides.com>
- Originally started due to the # of rejections to the CFP for Black Hat in 2009, due to lack of space and time
- Local BSides: BSides Columbus, BSides Indy, BSides Cincinnati May 12

<http://bsidescincy.org/>



2600

- Origin of 2600 comes from the discovery in the 60s that transmitting a tone at 2600 hertz, easily produced by a Cap'n Crunch cereal toy, gave access to “operator mode” allowing elevated phone privileges like free long distance calls: https://en.wikipedia.org/wiki/2600:_The_Hacker_Quarterly
 - Here is an awesome documentary on the topic: <https://www.youtube.com/watch?v=SQ5H01axILs>
 - Meet every first Friday at “The Brew House” here in Cincinnati
 - <https://cinci2600.org/>
 - Nearby 2600 groups: Cincinnati, Dayton, Columbus
- 

Cincinnati SMBA

- SMBA: Security Masters of Beer Appreciation
- Allows security professionals to meet and discuss current info sec topics
- Free adult beverage of choice, networking, certification credits
- Meet monthly to drink beer, usually for free, and discuss topics
- Next meeting is April 16th, sponsored by Phantom at 2910 Wasson Rd, register on their website: <https://sites.google.com/view/cincysmba/home>



Central Ohio InfoSec Summit

- 5/14-5/15 2018, Hyatt Regency Columbus
- \$225 ticket for both days
- 9am - 5pm
- Brian Krebs will be there
- <https://www.infosecsummit.com/ehome/2018cbusinfosec/611667/>



CircleCityCon

- They have a really cool website: <http://circlecitycon.com/>
- Yearly conference in Indianapolis
- Focused on training classes, events, and contests
- June 1-3, in westin Indianapolis
- Student tickets \$100



SecureWV

- Offer talks, classes, and events, like CTFs
- 3 days long, this year Nov 30-Dec 2, 2018
- Occurs in Charleston West Virginia
- About 200 attendees
- Lots of classes on Forensics
- <http://securewv.com/index.html>



DC850

- Meet monthly, have to check their site for dates and locations, < 1 year old
- Very focused around red team activities and penetration testing
- <https://dc859blog.wordpress.com/>



DerbyCon

- Running for eight years, even sold out tickets within a few minutes last year
- Run out of Louisville
- October 3 - 7 2018
- Advertise themselves as good for beginners or experts
- <https://www.derbycon.com/>



Day-Con

- Running for over 10 years
- Their website kind of sucks right now: <http://www.day-con.org/>
- Run out of Dayton near the end of September



ShmooCon

- Hosted by some pretty smart people, including developers of Linux Apache, PGP, [OpenSSL](#) and [Snort](#)
- Run out of D.C., January 18-20 2019
- Sell out every year
- \$150 per person
- <http://shmoocon.org/>



BlackHat

- August 4-9 2018, Las Vegas, started in 1997
- Advertise themselves as the most technical security conference
- Offer briefings and trainings
- \$2195-2795 for briefing prices, recommend you go to the site to determine which pass type you want
- <https://www.blackhat.com/us-18/registration.html>



DefCon

- DefCon comes from Defense Condition
- DefCon 26 August 9-12 2018 Caesar's Palace Las Vegas
- About \$250 per ticket
- <https://www.defcon.org/index.html>



Honorable Mentions

- OWASP AppSec Conference: <https://2018.appsecusa.org/>
- RSA Conference: <https://www.rsaconference.com/events/us18>
- ToorCon: <https://toorcon.net/>
- Usenix Security Symposium:
<https://www.usenix.org/conference/usenixsecurity18>
- Infosec World: <https://infosecworld.misti.com/>



Other sources to find events in the area

- <http://infosecevents.net/2010/10/21/cincinnati-security-community/>
- <http://hackermaps.org/>
- https://en.wikipedia.org/wiki/Category:Hacker_conventions
- <https://infosec-conferences.com/events/conferences-top-ten-must-go-to/>



Part 7: Scanning

Get your cat up front for a cat scan

The Topics Today Go **Something** Exactly Like This

- Going From Intelligence Gathering to Scanning
- What is Scanning
- What is Gained from Scanning
- Types of Scans
- Vulnerabilities and Proof of Concepts
- Common Scanning Tools
- Example?



From Intelligence Gathering to Scanning

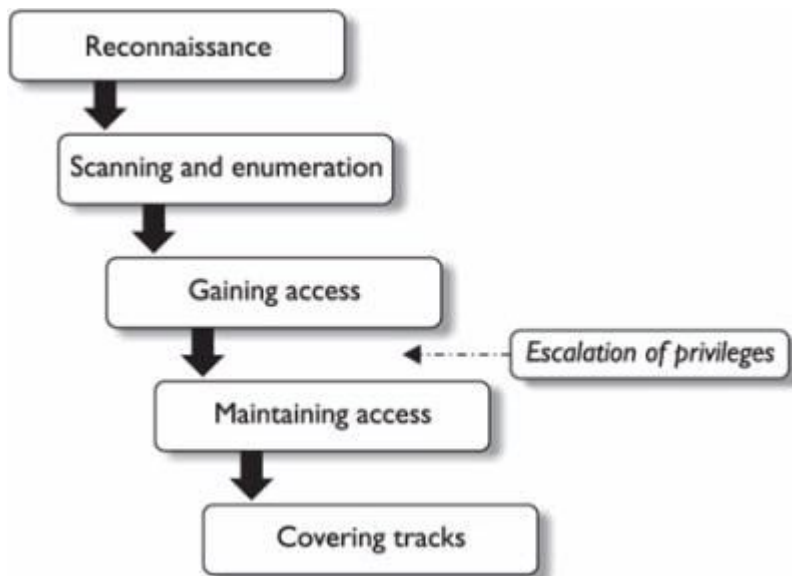
In our intelligence gathering and reconnaissance activities we were able to figure out what systems our target may be running and where they are running from.

Logically we should now start looking close at what we have found to try to find our way into the target systems.



What is Scanning

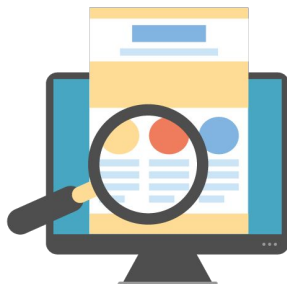
Scanning is taking a better look at the system and finding exploitable targets



What is Gained from Scanning?

Scanning can reveal:

- Internal Network Topology
- Network Services, down to the version number in some cases
- Machines on the network and what OS's they may be running
- Vulnerabilities that affect any of the previous three items that we can use to gain access into the system(s)



The Types of Scans

PDF Scan - Digitizes a document in PDF format

Network Scan - Map out the network terrain

Port Scan - Find open services on target machines

Vulnerability Scan - Find Vulnerabilities on targets




Vulnerabilities and Proof of Concepts

If scanning is done to find vulnerabilities, what is a vulnerability?

- **Common Vulnerabilities and Exposures (CVE's)** are documents published by researchers that detail where errors are in systems and how those errors can be used maliciously against the system
- **Proof of Concepts (PoC's)** are examples that utilize known CVE's to exploit a system in a demonstrative capacity

CVE's are uniquely numbered and usually tagged with corresponding PoC's when published.



Vulnerabilities and Proof of Concepts (cont.)

Where are these CVE's?

- cve.mitre.org is the central CVE list and is both downloadable and web searchable
- Vulnerability scans may give an exact CVE # which can be searched on Google to find PoC's or even canned exploits



Common Scanning Tools

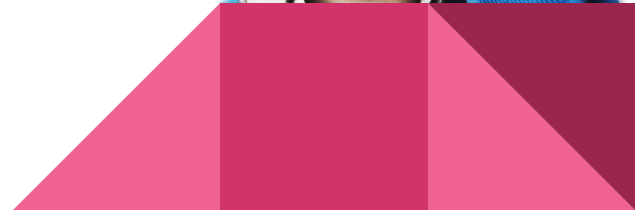
Network Scan - Map out the network terrain

Port Scan - Find open services on target machines

Vulnerability Scan - Find Vulnerabilities on targets



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



Common Scanning Tools

Network Scanners	Nmap, masscan, dnmap
Port Scanners	Nmap, masscan, dnmap
Vulnerability Scanners	OpenVAS, BBQSQL, BED, Nessus, Lynis



OpenVAS

- For Kali Linux: *apt install openvas*
- Then run: *openvas-setup*
- Then: *openvas-start*
- Navigate to **127.0.0.1:9392** and log in with the generated password



SearchSploit

- Install: *apt install exploitdb*
- Update the database: *searchsploit -u*
- Use: *searchsploit "ftp"*
- ???
- Profit

