Cyber@UC Meeting 45

Direct Recon

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

- **CTF** at **RevolutionUC** went great!
- **Lab space has been approved**, equipment has been ordered
- **Lakota East outreach** was awesome

Announcements: OC3 website

- They liked our demo site!
- We found some security issues in their CMS platform

WRIGHT STATE UNIVERSITY | COMPUTER SCIENCE AND ENGINEERING

Research Experience for Undergraduates Summer 2018

Cyber Security Research

May 14 – July 20

Eligibility:

Applicants must be citizens or permanent residents of the United States. Preference will be given to students whose home institutions have very limited or no research program in cyber security. Women and minorities are strongly encouraged to apply.

Research Topics:

- Network Security
- Intrusion Detection
- Wireless Sensor Network Security
- Internet Malware Detection, Analysis, and Mitigation
- Software Reverse Engineering Vulnerability Discovery
- Privacy-Preserving Data Mining

Support:

- $5,000 stipend for 10 weeks
- Housing provided at no charge
- $1,200 food allowance for 10 weeks
- Travel funds up to $700 from/to the program

Review:

The review of applications will begin **March 7, 2018** and will continue until all positions are filled.

For more information, please visit reu.cs.wright.edu **or** contact Dr. Junjie Zhang junjie.zhang@wright.edu 937-775-5015.

ASME E-FEST


An engineering festival is coming to Penn State this spring!
+ THREE DAYS
+ ENGINEERING COMPETITIONS
+ CAREER ADVICE & MENTORING
+ INTERACTIVE EXPERIENCES & NETWORKING
+ WORKSHOPS & SESSIONS
+ ENTERTAINMENT & FUN
First 50 students to register get a FREE ticket! Book using code EFTEAST50


ASME E-Fests™
Brought to you by ASME Engineering Festivals™.
E-FEST EAST
April 13th - 15th, 2018
Penn State

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: gauss.ececs.uc.edu/UC.yber/

Weekly Content

Kali now available on Windows 10

- There is an existing feature in Windows 10 called, Windows Subsystem for Linux (WSL)
- Kali is just the most recent of several available Linux distributions
  - Ubuntu, OpenSUSE, SUSE Enterprise
- You can also get the kali desktop environment running, instructions in the link below
- Unfortunately, this Kali does not come with the typical pre-installed tools

https://thehackernews.com/2018/03/kali-linux-hacking-windows.html

BotNet Roundup: Avalanche, Kronos

- This article is giving updates on three different botnets
  - Avalanche, Kronos, NanoCore
- Avalanche: leader of Avalanche gang, Gennady Kapkanov, has been on the run since a cybercrime crackdown in Ukraine
  - Fired on officers with Kalashnikov, released on an arrest technicality
  - Re-arrested this past Monday because his passport was fake
- Kronos: Marcus “MalwareTech” Hutchins, helped stop WannaCry, but is now on trial for Kronos botnet, currently claims innocence
  - Prosecutors expect a quick trial: Business records, statements, malware samples, Jabber chats, audio recordings of interrogations

BotNet Roundup: NanoCore

- NanoCore was developed by Taylor Huddleston
- Sold a RAT on hackforums[dot]net advertised to allow remote administration of one or many computers, claimed RAT was meant to be remote administration tool
- Defense argued that Mr. Huddleston was not guilty for what his clients did with the software he developed
- Sentencing suggests that where you choose to sell something online says a lot about what you think of your product and who is likely to buy it

https://krebsonsecurity.com/2018/02/bot-roundup-avalanche-kronos-nanocore/

Memcached DDoS Attacks

- In the last week, we've seen two new record breaking DDoS attacks
  - 1.35 Tbps and 1.7 Tbps
- These attacks relied on amplification/reflection to amplify the bandwidth of the DDoS by a factor of 51,000
- Memcached is an open source distributed memory caching system
- Exploit works by sending a forged request to the targeted Memcached server on port 11211 using a spoofed IP address that matches the victim's IP
- These few bytes sent to the memcached server triggers tens of thousands of times bigger response against the target IP

Sources

https://thehackernews.com/2018/03/memcached-ddos-exploit-code.html

https://thehackernews.com/2018/02/memcached-amplification-ddos.html

https://thehackernews.com/2018/03/ddos-attack-memcached.html

https://thehackernews.com/2018/03/biggest-ddos-attack-github.html

Exposed servers: https://pastebin.com/raw/eSCHTTVu

Exploit code: https://pastebin.com/raw/ZiUeinae

Part 4:
Direct Recon

Spring Break is not for COOP students

The Topics Today Go Something Exactly Like This

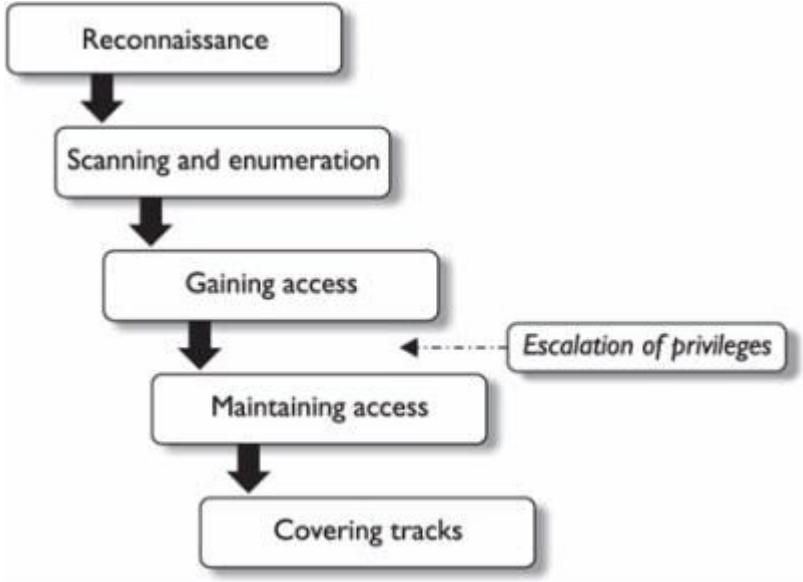
- Steps of Ethical Hacking
- Information Gathering
  - What is / Types?
  - Why do? / Goals
  - Information Type and Sources
  - Social Engineering
  - Direct Contact
- Tool Overviews
  - Maltego
  - Social Engineering Toolkit
  - Target Websites and Servers
- 127.0.0.1 on the range
  - Stay Out (or don’t)

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

KALI

Steps of Ethical Hacking: Reconnaissance

- Reconnaissance helps us know what systems, software, and data our targets may hold



What is Information Gathering?

- Gathering of useful information on target(s) that can be used to create an advantage later
- This can include anything from the fact that a manager is out of town to knowing what payroll software a target uses

Types of Information Gathering

- **Indirect**
  - Using publicly available information
  - Google
  - Facebook
  - Job Sites
- **Direct**
  - Directly gathering information from the target through site visits, social engineering, etc.
  - Use tools like Maltego and the Social Engineer's Toolkit to grab data from targets directly
  - Dumpster Diving is also valid

Types of Information

- Network/Systems
  - What systems are they using
  - What tools are they using
  - What is running on the network
- Organizational
  - Employee information
  - Business Goals
  - Supplier Information
  - Client Information
- Security
  - What systems are in place

Direct Sources of Information

- **Social Engineering**
  - Job Interviews
  - Emails
- **Site Casing**
  - Reveal Private Web Apps / Menus
  - Find Top Level Network Information
  - Enumerate through subdomains

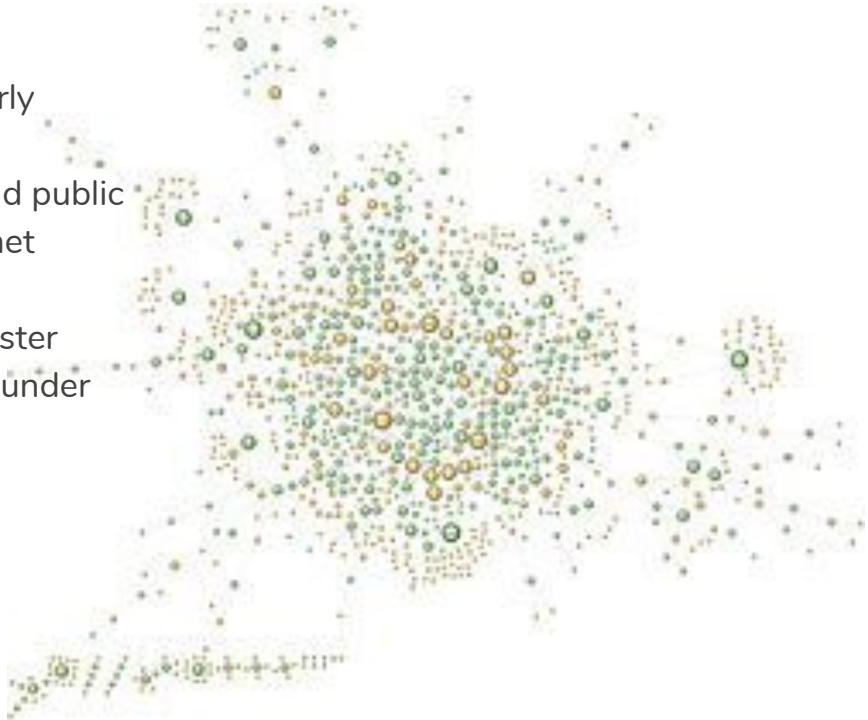
Tool Warning

- The tools we are starting to cover can be abused very easily
- Some people don’t take kindly to you gathering a very large amount of personal information on them
- If anyone abuses a tool we cover, they may ruin it for all of us

Tool Overview: Maltego

MALTEGO

- Basically an intelligence agency with a yearly subscription fee
- Maltego correlates personal information and public records to graph out a target entity's internet footprint
- Offers a free, community edition if you register
- Maltego's cheapest paid version costs just under $800 for the first year
- Used every day to find criminals by law enforcement



Tool Overview: Social Engineer's Toolkit

- Made by the same people who make the **Penetration Tester's Framework**
- Focuses on creating digital social engineering attacks such as malicious emails and scripts embedded in documents
- Does a whole lot more too

127.0.0.1 on the Range

This week's Activities:

- **Maltego**
  - Graph yourself
- **SEC**
  - Make a USB with reverse shell that attempts to autorun
- **Robots.txt**
  - Find something that should not be available to you on a website but someone forgot to require authentication for