

Cyber@UC Meeting 44

Indirect 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

- We will be **running a CTF** at the **RevUC Hackathon**, this weekend!
- **We do not have a sport team :(**
- **Lakota East outreach** next **Monday March 5th**
- We have been asked to help with **OC3's website**



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.

Research Experience for Undergraduates Summer 2018

Cyber Security Research May 14 – July 20



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

It Was Russia All Along

- Remember Olympic Destroyer?
- Turns out it was the Russians getting revenge on the olympic committee
- Russia also tried to frame North Korea
 - The only thing surprising about this is that North Korea didn't also try to hack the olympics, but had their packets lost about a hundred miles off the coast
- This act of making an attack while trying to frame another country is known as false flag operation
- Hacked hundreds of computers and routers
 - Router malware is very expensive to develop
- This is believed to be the same group involved in NotPetya, connected to GRU
 - Fancy bear, a Russian APT released a set of emails, stolen from Olympic officials earlier this month

Olympic hack sources

https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html?utm_term=.a5a4aade487


<https://www.vanityfair.com/news/2018/02/russia-hacked-pyeongchang-olympics-doping>

<http://securityaffairs.co/wordpress/69568/hacking/pyeongchang-olympics-computers-hack.html>

NSA Requires White House Authorization

- NSA director Michael Rogers testified that he does not have the “day-to-day authority” to counter attempts by Russia to influence elections
- Such authorization would have to come from the president, which has not happened as of yet
- Russia continues to attempt to target the US election process because they haven’t paid a price for it yet
- Following links contains footage of the testimony at the end:

<https://www.darkreading.com/threat-intelligence/nsas-rogers-no-white-house-request-for-action-against-russian-hacking/d/d-id/1331147>



Domain Theft Strands Thousands of Web Sites

- Newtek Business Services Corp. is a web services conglomerate
- Operate the websites of over 100k businesses
- Had several of their core domains stolen
- Newtek sent an email to clients that domains were being changed due to “increased” security, no mention of a breach, a link to the email is in the article
- A vietnamese hacker replaced the login page of Newtek’s web site management portal webcontrolcenter[dot]com with a live web chat service
- 10 hours after the incident, Newtek acknowledged the incident was because of a dispute over three domains. It was advised that customers not go to those domains

Domain theft (continued)

- Speaking with the attacker via his web chat
 - Claimed to have notified Newtek five days earlier of a bug found in their online operations, but received no response
- Newtek customers are outraged/dissatisfied at Newtek's handling of this attack

<https://krebsonsecurity.com/2018/02/domain-theft-strands-thousands-of-web-sites/>





Reconz

Part 4: Indirect Recon

Hackathon is this weekend





The Topics Today Go Something Exactly Like This

- Steps of Ethical Hacking
- Information Gathering
 - What is / Types?
 - Why do? / Goals
 - Information Type and Sources
 - Threats of Finger Printing (put on our white hats)
 - Process and Tools
- Tool Overviews
 - Search Engines
 - Social Networks
 - DNS Records
 - Public Records
- 127.0.0.1 on the range
 -
- Practice CEH questions

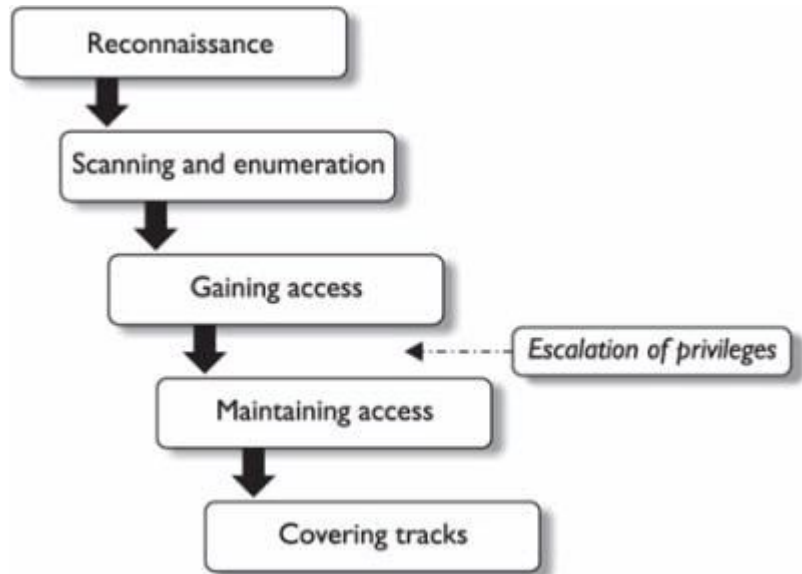


Put on your ~~3D glasses~~ **Linux Distro**
now



Steps of Ethical Hacking: Reconnaissance

- This marks our first real content on the Ethical Hacking process
- 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
- **Direct**
 - Directly gathering information from the target through site visits, social engineering, etc.



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



Indirect Sources of Information

- **Public Records**
 - Are they filling for building permits or buying property?
- **Job Postings**
 - What are they looking for in Management and IT?
 - What are the skills of people they have recently hired?
 - Who connects with them on LinkedIn that they don't employ?
- **News Articles**
- **Target Website**
 - If they sell things on their website what can you infer from changes in prices?
- **Technical Records**
 - What DNS addresses do they have?
 - Which addresses have they recently acquired?
 - What does a large increase of registered addresses say?



Goals of Information Gathering

- Find potential gaps or loopholes in security that we can exploit later
- Know what protective measures we may need to evade
- Give us a competitive advantage (Business Intelligence)



Threats of Information Gathering

- **Business Intelligence / Competitive Analysis**
 - Our competition know knows what we're selling, buying, and planning on doing
- **Revealing of Network Architecture**
 - Someone knows what we have running on our network and can exploit it



Tool Overview: Search Engines

- **Google Like Search Engines**
 - Search for web content (FTP/HTTP) and apply lots of filters
 - Google has about 100 different search filters you can use in unexpected ways
 - **filetype:pdf** will only show pdf results
- **Shodan Like Search Engines**
 - Search for open services on the web (ei look for any open database on the internet)



Tool Overview: Social Networks

- **Companies** put what they are looking for on hiring sites
- **Employees** put what they do on social and hiring sites
- **We** can read between the lines and infer business secrets
 - We can also combine social and job sites with our search engines using some of the special filters available



Tool Overview: DNS Records

- Can show us communications (email servers)
- Can show us what products they may be releasing soon (new domains)
- Can show us where their servers are (IP addresses corresponding to records)



Tool Overview: Public Records

- Can show us what is going on inside the building
 - Are they SKIF rooms for classified materials?
 - Are they upgrading a network system?
- Can show us future business plans
 - Are they planning on building anywhere?
 - Are they planning on acquiring any existing properties?
- Can show us current business issues
 - If the business is a poultry supply and their own website shows that they are out of chicken we can infer that they have a supplier issue
 - If we are selling the same products but they are selling at lower prices and appear to still be making a profit then we can infer that they have a better supplier
 - Most profits on commercial items around 10-15% (soft goods) or 50-60% (hard goods)



Google Dork Search Terms

Check out <https://www.exploit-db.com/google-hacking-database/>

intitle:

- will search for matching text in html title
- ex. intitle:"login"
- **allintitle:** is a broader search

inurl:

- Searches for string in URL
- ex. inurl:"login.php"

filetype:

- Searches for specific file types
- ex. Filetype:pdf
- **ext:pdf** will also find pdf extensions

intext:

- searches for text in websites
- ex. intext:"index of/"
- **allintext:** is another version

site:

- Searches only specific site
- ex. site:kroger.com

Modifiers:

- + requires term to match exactly
- - avoid results that match term
- * Wildcard
- "" search for specific phrase



WHOIS Information

whois.domaintools.com

- Who **registered a domain**
- **Time** of registration
- **Address** of registrant
- **IP address** of domain
- **Phone numbers** of registrant
- **Who is hosting** the domain



Cool Resources

[Google Hacking Database](#)

[Google Dorking](#)

[Null-Byte Google Dorking](#)



127.0.0.1 on the Range

This week's Activities:

- **Google Hacking**
 - Let's find some open cameras and user manuals, etc.
- **Public Records**
 - Who voted on campus in 2016?



Notes/Additional Content

You're Leaking Trade Secrets - defcon presentation

I know where your cat lives - website that uses machine intelligence to scrape pictures of cats posted on social media

Hacking cameras like a hollywood hacker - blackhat presentation that touches google hacking of unsecured cameras