Hacking Legally

Ethics and Laws

Ethics

- What is this “ethics” thing?

- You must understand ethics to be able to take on ethical hacking
  - White Hat Hacking == Ethical Hacking

Ethical Hacking

- Ethical hacking is an activity where a computer and network security expert attacks a system on behalf of its owners.
  - Utilizing the same/similar tools and techniques as malicious hackers
  - Looking for the same vulnerabilities that a malicious hacker looks for
  - Attempts to gain the same accesses into a network that a malicious hacker would gain

  - BUT – ethical hackers report the problems to the owners for remediation, rather than maliciously taking advantage of them.

When in Doubt, ASK!

- Most people have a good sense of right or wrong. Most.
  - Follow your gut!
  - If you’re not sure, ask someone BEFORE proceeding!!!

- Don’t start down a path you don’t want to be on
  - Illegally downloaded a $0.99 song?
  - What’s next?

Wanna Get a Sweet Fed Job?

- Thousands of people are probably applying for the same job
- You're smart. They're smart.
  - It's going to come down to something else – lawfulness.

- Mary, Bob, and Jim – all super smart on paper, same degree, same qualifications.
  - Mary downloaded a song illegally once.
  - Bob hacked into the local radio station's website once.
    - Does this mean Bob is smart and has proven his l33t hacking abilities?
  - Jim finds himself driving a few mph over the speed limit occasionally.

TL;DR;

- Do the right thing.
- If it’s not yours, don’t touch it.
- Stay legal.

- Speaking of legal…

Cyber Law

Is Anyone Here a Lawyer?

- I am not a lawyer.
- I am not an expert in law.
- I’m not a lawyer.
- These laws are complicated.
- I’m not a lawyer.
- Computer laws are changing all the time
- I’m not a lawyer.

Laws Are Complex

- Many of these laws are somewhat “behind the times”
  - But some change rapidly along with technology.
  - Drones?
- Laws vary from place to place.
  - Your state might have their own laws.
  - Important to know what affects you, what’s legal for you locally.
    - Be aware of location
      - Your location
      - Location of the company/equipment you’re testing (Do you really know?)
      - What if your packets are routed through a different state? (I’m still not a lawyer)

What are Weapons?

- Some tools we'll use in class are weapons
  - Metasploit, and others
  - "hacking tools are like guns"
    - Not illegal to have, unless you shoot someone

Laws Can Be Strict

- German Law Section 202
  - Adopted in 2007
  - 10 years in prison, and be held liable for monetary damages

  - “Manufacturing, programming, installing, or spreading software that has the primary goal of circumventing security measures is *verboten*, which means that some security scanning tools might become illegal. In theory, this applies only to illicit programs like trojans, but some groups worry about how the new criteria will be applied.” https://arstechnica.com/information-technology/2007/05/germany-adopts-anti-hacker-law-critics-say-it-breeds-insecurity/

Some Laws that Apply to You

- http://www.sans.org/reading_room/whitepapers/legal/federal-computer-crime-laws_1446
- Federal Laws
  - Computer Fraud and Abuse Act (CFAA)
  - Electronic Communications Privacy Act (ECPA)
  - Cyber Security Enhancement Act (CSEA)
  - Patriot Act
  - …others…

CFAA

- Oldest computer crime law – 1984
- Most important computer crime statute in the U.S.
  - Most other statutes modify the CFAA
- CFAA criminalizes seven types of computer activities
  - First 4 unauthorized access

Electronic Communications Privacy Act (ECPA)

- Passed in 1986
  - Amendment to the federal wiretap law
- Makes it illegal to intercept stored or transmitted electronic communication without authorization
- Defines provisions for access, use, disclosure, interception, and privacy protections of electronic communications

Cyber Security Enhancement Act

- Passed along with the Homeland Security Act in 2002
- Grants sweeping powers to law enforcement organizations
- Increases penalties that were set in the CFAA

Digital Millennium Copyright Act (DMCA)

- Signed into law by Clinton in 1998
- Provides legal protection to copyright and intellectual property owners
- Working around DMCA protections to share/copy property
  - Music, Movies, Software, anything copyrighted or any IP
- When we are reverse engineering software or firmware… Does that violate DMCA?

IoT Cybersecurity Improvement Act of 2017

- **NOTE: This is not law…yet. Just a proposed bill at this point.**
- The Fed buys IoT things, and they want IoT things to have better security.
- Two major components
  - Procurement requirements on the government.
  - Adds a research exemption to existing statutes, including DMCA and CFAA

CFAA Exemption

"(k) This section shall not apply to a person who—

"(1) in good faith, engaged in researching the cybersecurity of an Internet-connected device of the class, model, or type provided by a contractor to a department or agency of the United States; and

"(2) acted in compliance with the guidelines required to be issued by the National Protection and Programs Directorate, and adopted by the contractor described in paragraph (1), under section 3(b) of the Internet of Things (IoT) Cybersecurity Improvement Act of 2017.".

Those are all Federal, what about State?

- http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx

The work we do is legally difficult. People often operate in a gray area legally, which is bad.

Marcus Hutchins - MalwareTech

- Security Researcher
- Clearly a white hat (at least sometimes)
  - Stopped WannaCry from spreading

- Allegedly…
  - Some code he wrote years ago ended up in the Kronos Banking Trojan
  - The FBI didn't like that
    - So they arrested him
  - Currently faces 6 charges of creating and selling malware (Kronos)
    - If proven guilty, could be in a US jail for 40 years.

Tennessee Man Sentenced for Unauthorized Access of Former Employer's Networks

- An Arlington, Tennessee man was sentenced today to 18 months in prison and two years of supervised release for intentionally accessing a competing engineering firm's computer network without authorization in order to obtain proprietary information.
- In addition to his prison term, Needham was ordered to pay $172,393.71 in restitution to Allen & Hoshall.
- According to admissions made in connection with his guilty plea, Needham admitted to repeatedly accessing, over a nearly two-year period, Allen & Hoshall's servers to download digitally rendered engineering schematics and more than 100 PDF documents containing project proposals and budgetary documents.

What You Cannot Do Legally

- Access a computer without permission
- Installing worms or viruses
- Denial of Service attacks
- Denying access to network resources
  - Be careful that you don’t prevent customers from doing their jobs.

- * without permission

Scope

- In addition to laws, the scope of a test must be clearly defined to determine what you can and cannot do.
- Which computers you can touch, which you cannot.

WhiteHat Agreement

- Let’s read it.

- You’ll sign it.

Red Team? Pentest? Vuln Assessment?

- Vulnerability Assessment (VA)
  - Typically credentialed
  - Given full access knowledge of the network, search for misconfigurations and vulnerabilities
- Penetration Test (PT)
  - Legal attempt to break into a company's network to find vulnerabilities
  - Findings are reported for remediation.
- Red Teaming
  - Test the organization's detection and response capabilities
  - Proving you can get in
  - More closely mimics a real threat.

What Do I Need?

- Well, knowledge. Good thing you're here. ☺
- The major knowledge point that will be useful to you but not covered in class… PROGRAMMING
  - Script kiddies always, always rely on someone else's tool
  - Learn to write your own
  - Learn to reverse software
  - Learn to write exploits
    - Much of this is going to get very low level
      - Assembly, C, C++… Sure there's some Python and Perl in there as well.

Other Tools

- Dedicated machine if possible
  - Collection of OSs and tools
- Old cheap laptop/desktop
- Or a VM
- In this class…
  - Local copy of a Kali VM
  - VMs in the IA Lab

Using Kali…

- Be careful, this contains weapons.
- You could jo to jail
- Network Settings for your Kali VM
  - Host Only = best
  - NAT = ok, but turn off wireless and unplug Ethernet

- If you start attacking someone else's machine or network, purposefully or otherwise, you're going to have a bad time.
- You could jo to jail`

Ben Ten (0xA) @Ben0xA · 51m

Any offensive consultant that isn't "also" a defensive consultant is missing a critical part of their skill-set. Red must learn blue!

5 4 17

Ben Ten (0xA) @Ben0xA · 34m

Replying to @Ben0xA

Also, anyone who says "We only break things." is not helping your organization. You need breakers and fixers. They should not be exclusive.

2 5

Who Else Did Bad?

- Find some more cases of cyber crime on your own.
- What did they do?
- What was the result?
  - Jail?
  - Fines?