CMSC388U

ITROS + ETHICS 1

COMPUTER SCIENCE
UNIVERSITY OF MARYLAND

(This lecture is being recorded)

user@388:~$ whoami

Course Facilitators!

John (Vanya) Gorbachev →

← Alden Schmidt

user@388:~$ sudo whoami

Dave Levin - Assistant Professor in CS
www.cs.umd.edu/~dml

I do network & systems security research
censorship.ai
irs.gov-login.pw (really)

I am passionate about getting undergrads into security!
breakerspace.cs.umd.edu

Come to me for:

- Medical extensions and such
- Any concerns about the class
- Interest in research

STICs

- STudent Initiated Courses
- Allows students to teach topics that wouldn’t necessarily be covered in their Major Curriculum
- https://stics.umd.edu/

CSEC

- CSEC @ UMD
- https://csec.umd.edu/
- We have talks/workshops
- Open to all and very loving <3

Administrative things

- Lectures will be held live over Zoom during class time
- Homeworks are due before the next lecture on Friday
    - There are no late submissions as the homeworks may be covered during lecture
- We want to know what you think!

Grading

- How grading is going to work
  - Turn in the homeworks by the lecture
    - No late credit (sorry)
  - Per-HW rubrics will be posted on ELMS
  - Midterm and Final Hack/Exam big %’s

Writeups

- Header w/ Name, UID#, Honor pledge
- Follow the rubric
  - Partial credit will be described (if possible)
- Formatting & pictures strongly recommended
  - We recommend using markdown
  - Export to PDF to make life simple
- Goal is to show the process, not just the solution(s)
  - Examples from last UMDCTF: https://ctftime.org/event/1040/tasks/

`snap install typora`

Course Goals

- To get everyone excited about hacking, CTFs, and infosec as a whole!
    - We want to share our passion in this area
- Show how ethical hacking in real life works
    - Various aspects, careers, hobbies, etc.
- Help prep for CMSC414 + other security courses
- “How do I get into hacking?”
    - We want to help be the initial push

Course overview

- Topics are listed on the syllabus, but this course is very much breadth versus depth
- At a surface level we are going to cover
    - Web hacking
    - Reverse engineering / Binary Exploitation
    - Forensics and Steganography
    - Cryptography
    - Penetration Testing
    - OSINT and Reconnaissance
    - Linux
    - And more!

What is ethical hacking?

- Common terminology:
    - Whitehat
    - Greyhat
    - Blackhat

- There isn’t one answer! But generally ethical hacking is:

“Legally breaking into computer systems with the express purpose of fixing the vulnerability”

How to hacker?

- Only kidding, but there are tons of ways! And taking this class is a great way to start!
- Try stuff! Break stuff! ~~Cause Chaos!~~
  - The whole hacker mantra is to make stuff behave in ways it isn’t supposed to
  - No “right way” to do things!
- Train!
  - CTF competitions, conferences, labs, etc…
- Keep up to date
  - New vulns/exploits are always being discovered, if you see one just came out, read!
  - Blogs, videos, writeups, Twitter(!) all have great info

Ethical hacking IRL

- Do people actually do this IRL?
    - YES!
        - For fun and for profit
- How?
    - Bug bounty platforms
    - Penetration testers
    - Red Teamers
    - Exploit Devs
    - You name it!

bugcrowd

hackerone

ZERO DAY
INITIATIVE

!!WARNING!!

- You’re gonna learn some very powerful things in this class
  - **MISUSING THEM WILL GET YOU INTO TROUBLE**
- We are teaching you **ETHICAL** hacking (it’s literally in the name)
  - Use approved resources (VMs and targets with permission)
  - **ALWAYS** ask for permission from the **RIGHT** people before attacking anything
- If you don’t **you will face both legal and academic consequences**

- **Note:** We aren’t lawyers - read from multiple sources and use your best judgement.
  - Best way to stay out of trouble is not get yourself in troubling circumstances!

SERIOUSLY

!!WARNING: The Sequel!!

- Computer Fraud and Abuse Act of 1986
  - 18 USC 1030
  - “Prevents access to a computer without authorization”
- Digital Millennium Copyright Act of 1988
  - Exclusions for some “Good faith security research”
- Wiretap Act of 1968
  - Criminalizes unauthorized interception, use, and disclosure of communications by government organizations and citizens
  - Get a warrant!
- Cyber Crime Prosecution
  - 200 Pages of how the government will come after you if you violate the law
  - So just, **don’t**

SERIOUSLY

Let's get Ethical!

(ethical! I wanna get ethical! Lets do ethics yea.)

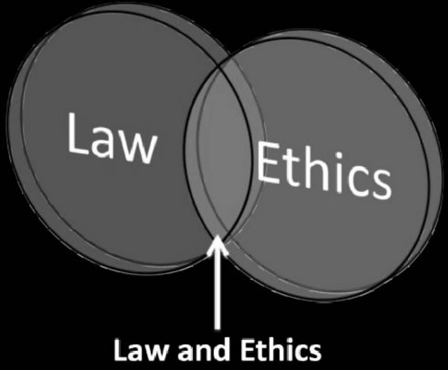
Ethics

- What even is *ethics?*
- Pertinence
- Difference between legality and ethicality

Ethics: the discipline dealing with what is good and bad and with *moral duty and obligation*

Legality vs. Ethicality

- We will talk about both in this class, but they aren't the same thing!
- They don't always overlap
- Think about the difference between legality vs. ethicality
    - Examples?
- Always follow the LAW in (and outside) of this class



Why care about ethics?

- In the world of cybersecurity (and computer science generally) we make lots of ethical decisions
    - What *ought* to be done, or what is *good* to do
    - Who (if anyone) will benefit from our work (Govs? Private companies? The public?)
    - When to disclose *what* we've discovered, and *where* to disclose it

Disclosure

- Disclosure
  - You find a serious vuln, When, where, and to whom do you disclose?
  - How do you disclose? Many common types such as responsible/full/etc.
  - Even if your intentions are good, how will businesses respond? (sometimes poorly)
  - Anonymity?

- Where do you go for help?

CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY

Ethics on the job

- As an ethical hacker you should…
  - Understand the target - know what is and what is not in scope (IP addr, URLs, etc)
  - Know the laws and the target's rules
  - Provide tons of feedback to target
  - Minimize leftover exposure
  - Act responsibly and carefully (demo/"PoC" instead of exploit)
    - Do just enough to prove, and check about every next step
- Non-disclosure agreements (NDA's)

Guidelines for doing ethics

- Build an ethical argument:
    - State the claim
    - Substantiate the claim (give the argument)
    - Consider counterclaims / opposing arguments
    - Explain how the counterclaims/arguments fail
- Do this (roughly) linearly, and your argument will be easy to follow!
- Most important: **be straightforward**

For next class...

- We are going to post a small homework assignment sometime this weekend on ethics
    - Don’t go too crazy, 250-500 words max
- Will be posting 2 videos on setting up Kali Linux in either VMWare or VirtualBox (either is fine!)
- Please setup Kali for next class, not strictly needed but will be helpful
- Will also be posting some OSINT related links, explore a little bit!

HAVE FUN

DON’T BE DUMB

CITE YOUR SOURCES