CMSC389R

Spring 2018

COMPUTER SCIENCE
UNIVERSITY OF MARYLAND

your facilitators

Michael Reininger (michael@csec.umiacs.umd.edu)

William Woodruff (william@yossarian.net)

Joshua Fleming (secretary@csec.umiacs.umd.edu)

faculty advisor

Dr. Dave Levin

dml@cs.umd.edu

STICs

- Student Initiated Courses
- http://sticsumd.edu
- Please let us know how we’re doing

why

- Makes us better programmers
- Makes us better users
- Exercises a different way of thinking
- Field is constantly growing
- Plenty of jobs/internships

goals

- Learn the principles of ethical hacking
- Security techniques
- Improve Linux skills
- Explore Capture the Flag (CTF)
- Explore research and career options

warnings

- You will learn powerful skills in this class!
  - Governments and companies **do not mess around**
- We will be *practicing* ethical and legal hacking
  - Use approved resources (VMs, our VPSes)
  - *Always* ask for permission
- Violate the rules? You risk academic and/or legal punishment.

warnings

- Relevant statutes:
  - The Computer Fraud and Abuse Act of 1986
  - The Uniform Trade Secrets Act of 1985
  - The Economic Espionage Act of 1996
- Companies take break-ins seriously!
- The US Government takes them even more seriously!

rules

- Be respectful with computer usage in class
- Ask questions and start discussions
  - Try not to interrupt others during class
- Be respectful of your classmates and facilitators

admin

- Setup - bring laptops
- Install VirtualBox/VMware (recommended)
- Download Kali (recommended)
- DO NOT DO ASSIGNMENTS ON GRACE OR GLUE!

what

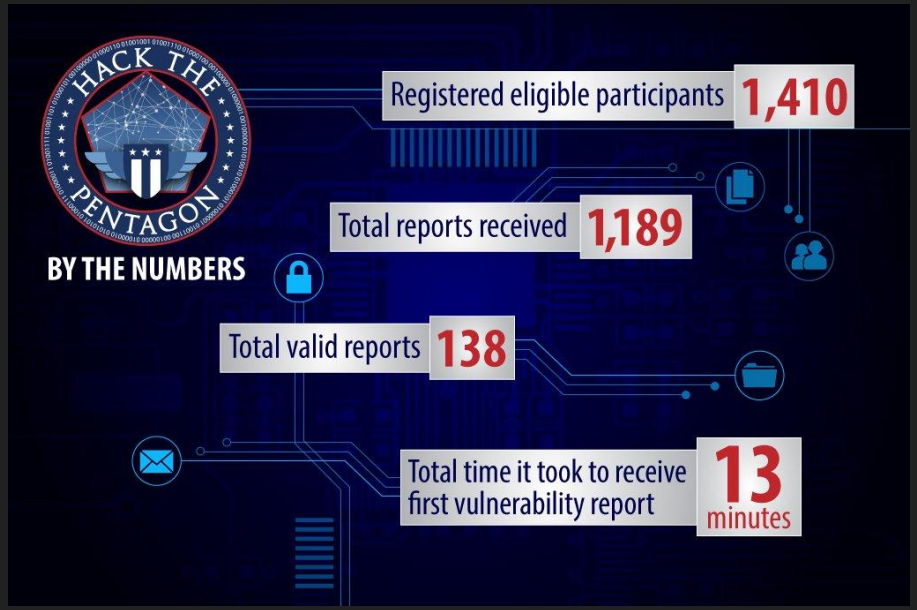
- Use an attacker’s mindset to evaluate the security of a system
  - Insiders/Outsiders/Physical/APTs/Hacktivists/Espionage/etc…
- Boils down to where organization will invest most in security
- Determine metric representing organization’s risk(s)

how

- Don’t just build - break!
- Constantly train (ie. CTFs, conferences, etc)
- Be alert and informed of new threats

really?

Yes! It works



Bounties

If you have discovered a security bug that meets the requirements, and you're the first eligible researcher to report it, we will gladly reward you for your efforts. Below is our bounty payout structure, which is based on the severity and impact of bugs.

Severity	Examples	Maximum payout in award miles
High	— Remote code execution	1,000,000
Medium	— Authentication bypass — Brute-force attacks — Potential for personally identifiable information (PII) disclosure — Timing attacks	250,000
Low	— Cross-site scripting — Cross-site request forgery — Third-party security bugs that affect United	50,000

methods

- Identify vulnerabilities
- Use (or develop) tools to exploit these vulnerabilities
- Backdoor, exfiltrate and cover your tracks

ethics

- What *is* ethics?
- Pertinence
- Difference between legality and ethicality
- Specific topics:
  - Responsible disclosure
  - Intelligence gathering and privacy
  - Whistleblowing

what *is* ethics?

- Ethics: The branch of philosophy concerned with *right* and *wrong* (*good* and *bad*, *permissible* and *impermissible*, etc)
  - Interchangeably: Morality, moral philosophy
- One of the oldest branches of philosophy, with many traditions (more on this later)
- Concerns *normative* statements: what *ought* to be, rather than what *is* (positive statements)

why should we care about ethics?

- In the world of cybersecurity (and programming in general!), we make ethical decisions:
  - About **what** *ought* to be done, i.e. what is *good* to do
  - About **who** (if anybody) should *benefit* from our work (governments? private companies?)
  - About **when** to disclose what we've learned, and **where** to disclose it

legality versus ethicality

- We will talk about both legality and ethicality in this class, but don’t confuse them!
- Legality and ethicality don’t always overlap:
  - Segregation was once law: was it ethical?
  - Is the CFAA a *good* law from an ethical perspective?
- Think about the legal/ethical distinction, but practice the law in this class!

syllabus

- 55% write-ups, 20% midterm, 25% final
- https://github.com/UMD-CS-STICs/389Rspring18

writeups

- These will be your HWs (250-500 words total)
- Publish your writeups (Medium, Wordpress, etc.)

Honor Pledge

Introduction

Problem

Explanation

Flag

for next class

- Piazza
- Gray Hat Hacking (Chapter 1)
- OSINT Handbook
- OPSEC Handbook