CMSC389R

Fall 2018

COMPUTER SCIENCE
UNIVERSITY OF MARYLAND

your facilitators

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

Wesley Weidenhamer (wesley@csec.umiacs.umd.edu)

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

faculty advisor

Dr. Dave Levin

dml@cs.umd.edu

http://bluepill.cs.umd.edu/~dml/hide/389r.html

STICs

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

admin

- Bring laptops to class and follow along
- Office hours held on Fridays from 3:50 - 5:00 PM and by appointment
- Install VBox/VMware/etc + Kali (recommended)
- * DO NOT DO ASSIGNMENTS ON GRACE OR GLUE! *

admin

- Be respectful with computer usage in class
  - Mute volume to prevent accidental distractions, etc.
- Ask questions and start discussions
  - Refrain from interrupting others during class
- Be respectful of your classmates and facilitators

writeups

- These will be your weekly HWs (250-500 words)
- Submit your writeups on ELMS

Name

Section

Honor Pledge

Problem

Solution(s) and Explanation(s)

Flags and/or Easter Eggs

grading

- 45% write-ups, 20% midterm, 25% final, 10% comp
  - Email us within 36 hours of HW grade release to request a regrade
  - We reserve the right to reject a regrade request
  - Assignments can be submitted up to 3 days late for a 5% penalty/day
- See syllabus for more info

goals

- Learn basic principles of ethical hacking
- Introduce offensive & defensive security
- Improve Unix/Linux skills
- Explore Capture the Flag (CTF) competitions
- Explore research and career options

warnings

- You will learn powerful skills in this class
  - Very **serious** repercussions if misused
- We will be *practicing* ethical and legal hacking
  - Use approved resources (VMs & our VPSes)
  - *Always* ask for permission from the **right** people/organizations/etc
- You risk academic and/or legal punishment if you violate the rules

(small set of) warnings

- Computer Fraud and Abuse Act of 1986
  - 18 USC 1030
  - “Prevents access to a computer w/o auth.”
- Wiretap Act of 1968
  - Criminalizes unauthorized interception, use, and disclosure of comms by government agencies and citizens
  - Otherwise, need warrant
- Prosecuting Cyber Crimes

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)
  - “Degrees of Insecurity”

how

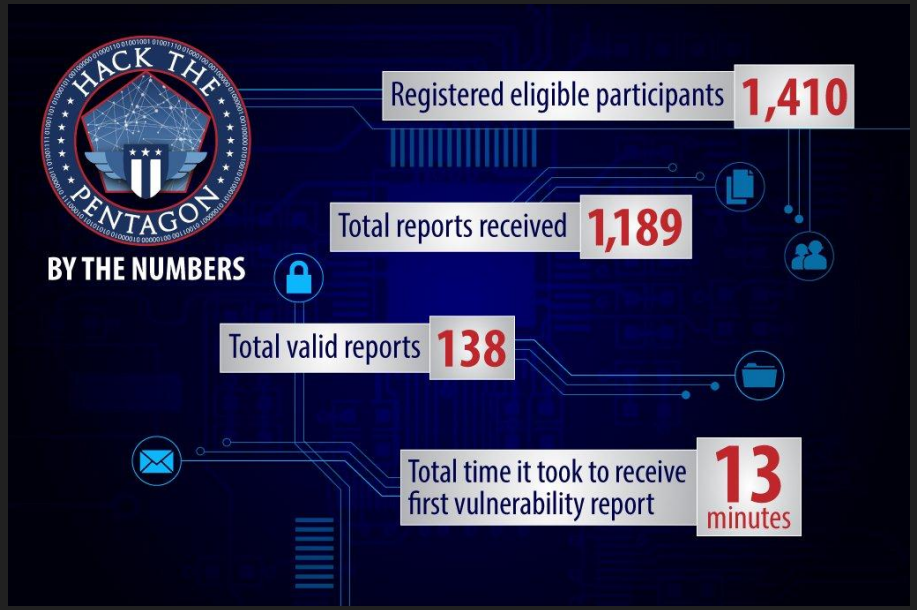
- Don’t just build - break!
- Constantly train (ie. CTFs, conferences, etc)
- Be alert and informed of new threats

conventional methods

- Identify vulnerabilities
  - (we'll cover this soon!)
- Use (or develop) tools to exploit these vulnerabilities
  - (aka your homework)
- Backdoor, exfiltrate and cover your tracks
  - (wait... is that a flag?)

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

experimenting

- We are teaching two sections!
  - We want to take advantage of this to do a bit of research...
- During the semester, we'll be trying different approaches to teaching the class
  - But you'll still be learning the same material across both sections
- Assessing the results via your weekly surveys + grades + specific feedback (ie. verbal, etc.)

ethics

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

- Ethics: The branch of philosophy concerned with *right* and *wrong* (*good* and *bad*, *permissible* and *impermissible*, etc)

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
- Think about the legal/ethical distinction, but always obey the law in (and outside) of this class!

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

guidelines for ethics

- Ethics is a field of active study and debate
  - You will not lose points for *disagreeing* about the ethics of something!
  - ...but you will lose points for not making ethical arguments.
  - Remember the principle of charity: assume the best possible interpretation of the position, and attack *that* interpretation

guidelines for doing ethics

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

ethical topics in csec

- Responsible disclosure
  - You’ve found a serious vulnerability. **When** do you disclose it, **where** (what platform), and to **whom**?
  - Even if your intentions are good, some businesses don’t like any disclosure (legal consequences)!
  - TWE do your interests outweigh society’s?

ethics on the job

- As an ethical hacker, you should
  - Understand the target - know what is off limits (IP/secrets/etc.)
  - Know the laws and target’s rules
  - Provide tons of feedback to target
  - Minimize leftover exposure
  - Non-disclosure agreements

for next class

- Register on the course Piazza
- Write-up #1 on Ethics
- OSINT Handbook
- OPSEC Handbook