Basics of Exploitation, proposed for Winter 2025

Will be co-taught with John Berry,[1] winner and organizer of the world-leading Defcon Capture-the-Flag cyber competition, as a Hacker in Residence at Dartmouth

Goals: Understanding the nature of unintended, unexpected computation emergent in today's most popular computing environments. Exposing the students to state-of-the-art cyber attack and exploit analysis techniques. Exposing the students to the national cybersecurity challenges arising from exploitation of computing systems and orienting them for careers in cybersecurity research and technical leadership.

Guest Lectures: Distinguished cybersecurity industry and academic researchers will be invited as guest speakers, to share real-world experiences, cover advanced topics, and offer ideas for the students to get involved in the development of the state-of-the-art tools and internships with the industry leading cybersecurity companies.

Materials: The use and enhancement of the DARPA-sponsored "pwn.college" interactive environment developed at the Arizona State University (ASU) is anticipated.

Homework Assignments: Weekly homework assignments to reinforce the concepts covered in class.

Graduate credit: The course will serve M.S. and Ph.D. students interested in cybersecurity, and will offer paths to M.S. theses and exposure to potential Ph.D. research topics.

Reading Materials: State-of-the-art papers published in first and second tier cybersecurity conferences will be assigned as required reading to graduate students and optional reading to undergraduates. Optional course projects, Senior Honors Thesis topics, and M.S. thesis topics will be offered to the respective groups of students.

Pre-requisites: COSC 51 or equivalent knowledge of a CPU instruction set or assembly. For example, a COSC 69 HackLab or Basics of Reverse Engineering is sufficient.

This course deals with technology and offers multiple labs on computing subjects. We believe it will be appropriate for TLA or TAS distribution requirements.

Approximate course timeline:

Week 1: Introduction to Binary Exploitation / RE Crash Course

- * Topics Covered:
  - Overview of binary exploitation and its significance in cybersecurity.
  - Introduction to the tools and environments (e.g., gdb, Ghidra, Binary Ninja, IDA Pro, etc.).
  - Setting up the environment: Linux basics, necessary software, and security settings.
  - Introduction to reverse engineering and its tools.
  - Basic static and dynamic analysis techniques.
  - Recognizing C constructs in assembly (loops, conditionals, functions).
- * Lab/Activity:
  - Environment setup and first steps with binary analysis tools.
  - Write and analyze simple assembly programs.
  - Reverse a simple binary and identify its functionality.

[1] John holds an M.S. in Computer Science from Dartmouth, 2022

Week 2: Memory Corruption Vulnerabilities
* Topics Covered:
  - Understanding memory layout (stack, heap, BSS, data, text).
  - Introduction to buffer overflows, stack overflows, and heap overflows, etc.
* Lab/Activity:
  - Exploit a simple stack buffer overflow vulnerability.

Week 3: Shellcoding Basics
* Topics Covered:
  - What is shellcode and how is it used in exploits.
  - Writing basic shellcode.
  - Null byte avoidance and other encoding techniques.
* Lab/Activity:
  - Write and test basic shellcode in a controlled environment.

Week 4: Exploitation Techniques and Defenses
* Topics Covered:
  - Return-to-libc attacks.
  - Introduction to defenses: ASLR, NX, Stack Canaries, and how to bypass them.
* Lab/Activity:
  - Bypass a stack canary and execute a return-to-libc attack.

Week 5: Heap Exploitation
* Topics Covered:
  - Basics of heap management and vulnerabilities (use-after-free, heap overflow).
  - Heap spraying fundamentals.
* Lab/Activity:
  - Exploit a simple heap-based vulnerability.

Week 6: Exploit Primitives & Weird Machines
* Topics Covered:
  - Discuss ASU's primitive taxonomy and how they can be used to classify exploits.
  - Discuss the concept of Weird Machines (formulated at Dartmouth).
* Lab/Activity
  - Exploit additional vulnerability types, integer overflow, uninitialized data, etc.

Week 7: Advanced Exploitation Techniques
* Topics Covered:
  - Return Oriented Programming (ROP) basics.
  - Finding and chaining ROP gadgets.
  - Heap Feng-shui (a.k.a. memory massaging).
  - Other Advanced topics TBD
* Lab/Activity:
  - Develop a simple ROP chain to bypass non-executable memory protections (NX, DEP, etc.)
  - Use heap massaging techniques

Week 8: Real-World Applications and Case Studies
* Topics Covered:
  - Analyze real-world exploits (e.g., famous bugs and vulnerabilities).
  - Mitigation techniques and secure coding practices.
* Lab/Activity:
  - Analyze and discuss a real-world exploit from recent years.

Week 9: Capture The Flag (CTF) Challenge

* Topics Covered:
  - Apply knowledge from the course in a mini-CTF style competition.
  - Challenges will include a mix of reverse engineering, shellcoding, and other exploit tasks.
* Lab/Activity:
  - Participate in the CTF, followed by a review of solutions and techniques.

The following statements are required in all syllabi:

Academic Honor Principle

Academic Honor Policy for the Undergraduate Students in Arts and Sciences

Religious Observances

Dartmouth has a deep commitment to support students' religious observances and diverse faith practices. Some students may wish to take part in religious observances that occur during this academic term. If you have a religious observance that conflicts with your participation in the course, please meet with me as soon as possible—before the end of the second week of the term at the latest—to discuss appropriate course adjustments.

Student Accessibility and Accommodations

Students requesting disability-related accommodations and services for this course are required to register with Student Accessibility Services (SAS; Apply for Services webpage; student.accessibility.services@dartmouth.edu; 1-603-646-9900) and to request that an accommodation email be sent to me in advance of the need for an accommodation. Then, students should schedule a follow-up meeting with me to determine relevant details such as what role SAS or its Testing Center may play in accommodation implementation. This process works best for everyone when completed as early in the quarter as possible. If students have questions about whether they are eligible for accommodations or have concerns about the implementation of their accommodations, they should contact the SAS office. All inquiries and discussions will remain confidential.