Avery McCauley

720-878-2939 | avery.mccauley@colorado.edu | https://averymccauley.github.io/

EDUCATION:

University of Colorado Boulder Expected May 2023

Leeds School of Business, B.S. in Business Administration, emphasis in Information Management
College of Engineering and Applied Science, B.A. in Computer Science, emphasis in Cybersecurity

EXPERIENCE:

Leeds Technology Services March 2020 - Present

Lead IT Technician

- Assist faculty, staff, and PhD students with technical issues, including virus removal and data back-ups
- Use problem-solving skills to adjust to a dynamic technology environment
- Experience in supporting Windows and MacOS, Windows imaging for an organization, and effective communication to a non-technical audience

RELEVANT COURSEWORK:

Computer Systems

- Code Injection Attacks: Injected code to alter the execution flow of a program via a buffer overflow consisting of a string representation of a cookie
- Return-Oriented Programming: countered stack randomization and non-executable portions of the stack by identifying useful existing byte sequences
- Utilized a GNU debugger to view assembly, observe registers, memory states, and control flow to determine what the program achieved without the source code

Information Security

- Created targeted word lists using CeWL
- Implemented SQL injections, dictionary attacks, and hash-cracking using HashCat
- Practiced discovering and exploiting vulnerabilities using cybersecurity tools such as Metasploit, NMAP, Netflow, Squert, Wireshark, and Burp Suite to perform a comprehensive penetration test on a mock server

Cybersecurity Independent Study

- Reverse-engineered programs using Ghidra in a Kali Linux VM
- Solved various “crack-me” challenges using assembly knowledge
- Created function graphs using Ghidra to visually represent program control flows

Cybersecurity Fundamentals

- Length Extension Attack: Exploited the authentication capability of a server API by exploiting the length-extension vulnerability of hash functions in the MD5 and SHA family
- Hash Collision Attack: Created two Python scripts with identical MD5 hashes but different behaviors
- Discussed cryptographic functions and protocols, threat modeling, physical security, social engineering techniques, incident response, and computer forensics

TECHNICAL SKILLS:

Certifications: Adobe Photoshop Associate

Languages: C/C++, Python, SQL, JavaScript, HTML

Frameworks/Technologies: AWS, Git, Docker, VirtualBox, Google Cloud Platform

Cybersecurity Tools: Burp Suite, CeWL, HashCat, Kali Linux, Metasploit, NMAP, Nessus, Netflow, Parrot OS, Squert, and Wireshark