Avery McCauley

avery.mccauley@colorado.edu | https://averymccauley.github.io/

EDUCATION:

University of Colorado Boulder May 2023

College of Engineering and Applied Science, B.A. in Computer Science, emphasis in Cybersecurity GPA: 3.77

Leeds School of Business, B.S. in Business Administration, emphasis in Information Management

EXPERIENCE:

PricewaterhouseCoopers June 2022 - August 2022

Advance Summer Intern

- Completed mock penetration test challenges, including exploiting insecure network protocols, analyzing LSASS process memory dumps, kerberoasting, navigating Active Directory, lateral movement, and privilege escalation
- Developed a custom Google App Script to automate a data entry process with the potential to save over 20 hours of manual labor

Leeds Technology Services March 2020 - Present

Lead IT Technician

- Support Windows and MacOS machines, including experience in virus removal and data back-ups
- Utilize troubleshooting skills to solve problems on the spot in a dynamic technology environment
- Developed effective communication skills regarding complex technical issues with non-technical target audiences

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 via HashCat, John the Ripper, and Mimikatz
- 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 corporate environment

Cybersecurity Independent Study: Ghidra

- 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 and different behaviors
- Completed a mock penetration test on a web apps, including SQL injections, CSRF, and XSS attacks
- Studied cryptographic functions and protocols, threat modeling, physical security, social engineering techniques, incident response, and computer forensics

TECHNICAL SKILLS:

Cybersecurity Tools: Burp Suite, CeWL, EyeWitness, Ghidra, HashCat, Hydra, Kali Linux, Metasploit, Nmap, Nessus, Netflow, Parrot OS, Responder, Rubeus, Squert, Wireshark

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

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