# Avery McCauley

## 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**

*Associate* August 2023 - Present

- Conduct comprehensive penetration tests across various platforms, including APIs, web, mobile, and desktop applications, as well as PCAP analysis, AWS resource configuration reviews, and internal network assessments for multiple Fortune 500 clients, ensuring robust security and risk mitigation
- Assumed a project management role in a comprehensive assessment of 170+ applications, overseeing the entire workflow from initial kickoff meetings and logistical coordination to access validation and final report submission, ensuring timely and efficient delivery of high-quality results
- Lead and facilitate detailed penetration test report readout meetings, collaborating with client development teams to clearly communicate findings, prioritize vulnerabilities, and provide actionable recommendations for improving security posture

*Advance Summer Intern* June 2022 - August 2022

- Completed mock penetration test challenges, including exploiting insecure network protocols, analyzing LSASS process memory dumps, kerberoasting, navigating Active Directory, lateral movement, and privilege escalation
- Designed and developed a custom Google App Script to automate a data entry process, streamlining workflow efficiency and reducing manual input errors

**University of Colorado Boulder - Leeds Technology Services** March 2020 - August 2023

*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**

- 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 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

## TECHNICAL SKILLS:

**Cybersecurity Tools:** Burp Suite, CeWL, EyeWitness, Ghidra, HashCat, Hydra, Kali Linux, Metasploit, Nmap, Nessus, Responder, Rubeus, Wireshark

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

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