**E-MAIL:** [ryancmower1@gmail.com](mailto:ryancmower1@gmail.com)

**CELL:** 651-283-9492

**ADDRESS:** 3720 Sumter Ave S, Saint Louis Park, MN 55426

**GitHub:** <https://github.com/RyanMower/>

**LinkedIn:** <https://www.linkedin.com/in/ryan-mower-25b269191/>

**Ryan Mower**

**OBJECTIVE:**

A current information security engineer seeking an opportunity to learn and assist with Red Team operations, develop payloads and exploits, and drive process automation.

**EDUCATION:**

College

* University of Minnesota, Twin-Cities, College of Science and Engineering 2019-2023
* Bachelor | Master of Science in Computer Science
* North Dakota State University 2018-2019
* GPA: 4.00

Coursework

Computer Networks I, II, III

Advanced Programing

Secure Software Systems I, II, III

Parallel/Distributed Computing

2020-2023

* Operating Systems I, II
* Machine Architecture

**ACCOMPLISHMENTS:**

* First author on *Graphics Card Based Fuzzing* – IEEE Computer Society
* Dean’s List 2019-2023

**TECHNICAL SKILLS AND COMPUTER SCIENCE KNOWLEDGE:**

* BurpSuite, Ghidra, AFL Fuzzer, Metasploit, Nmap, LLVM
* C/C++, Java, Python, SQL, Git, Docker, JavaScript
* 5G Network, 5Greplay, VIM, PwnTools, Virtualization
* Microsoft Office, Google Suite, Domo, Power Apps

**WORK EXPERIENCE:**

**Associate Information Security Engineer** Summer of 2023-Present

* Retested discovered vulnerabilities, developed proof-of-concept exploits
* Coordinated penetration tests between application teams and penetration testers
* Automated processes, conveyed remediation techniques to application teams

**Network and Security Research Assistant** 2022-2023

* Compiled 5G network infrastructure with CFI enabled via the LLVM framework
* Reverse engineered IoT devices, fuzzed 5G network protocols and discovered vulnerabilities
* Captured and sanitized egress data from IoT devices with fake information to the cloud

**Optum Software Security Engineer** Summers of 2021-2022

* Developed web portal, performed agile development with DevSecOps
* Interacted with: REST API’s, LDAP, MySQL, Kubernetes, Docker, Express, React
* Scanned applications with Fortify, pentested web portal, fixed vulnerabilities
* Collaborated with teammates and peers, practiced daily scrums, presented project

**INDEPENDENT WORK:**

**Enterprise Hack the Box** Summer of 2023-Present

* Participating in penetration testing course Optum penetration testers developed
* Learn penetration testing techniques, actively use various pentest tools

**NetSPI Dark Side Ops II - Adversary Simulation Training** Fall of 2023-Present

* Implement defensive bypasses, public research, and modify existing toolkits

**NetSPI Dark Side Ops I - Malware Dev Training** Fall of 2023

* Learned several execution vectors, payload generation, automation, staging,

command and control, and data exfiltration.

* Hands-on experience with Throwback C2 and modern antivirus bypassing techniques

**Actively Compete in Hack the Box** 2020-Present

* Pentest boxes gaining both user and root level access in a CTF fashion
* Common tools include Nmap, Gobuster, Metasploit, BurpSuite, Hashcat, and many others