Michael Schultz

Alexandria, VA | 571 551 8409 | mschul6@gmu.edu | linkedin.com/in/themichaelaschultz/
github.com/raisschultz

Education

Bachelor of Applied Science (BAS), Cybersecurity *Expected May 2027*
George Mason University *Fairfax, VA*
Associate of Applied Science (AAS), Cybersecurity *December 2024*
Northern Virginia Community College *Alexandria, VA, USA*

Work Experience

Intern - Advancement Office, Leysin American School, Switzerland *June 2021 - August 2021*
>Updated and maintained alumni databases using Blackbaud and Raiser's Edge.
>Researched, verified, and documented alumni records from multiple sources.
>Improved alumni data accuracy through data reconciliation, record cross-indexing, and interviews.

Barista - Starbucks @ Virginia Square *April 2022 - January 2023*
- Memorized recipes and preparation standards *Arlington, VA, USA*
- Developed interpersonal communication skills and conflict resolution skills; "Make the Moment Right"
- Adhered to safety, cleanliness and food preparation hygiene standards.

Skills

Frameworks/Standards: familiar with NIST SP 800-53 and NIST SP 800-37; RMF process
Operating Systems: Linux - Unix, Kali, Windows Programming/Scripting: Python, Java
Security Tools: Familiar with the use of tools like Nmap, Wireshark, NetworkMiner, Nessus, Metasploit, VirusTotal, DynamiteLab
Networking & Administration: Experience working with and maintaining Windows Active Directory, and basic system and network configuration standards
Productivity: Proficiency in using Microsoft Office Suite and Google Workspace
Soft Skills: Strong technical and descriptive writing and documentation skills, research and analytical abilities, and effective communication and confident presentation and debate skills
Written and verbal fluency in French, conversational and basic written comprehension in German

Technical Experience

- Conducted vulnerability assessments with tools such as Nmap, Nessus, and Wireshark.
- Configured and tested industry level IT systems in lab environments, including Windows Active Directory and Kali Linux, according to federal assessment standards.
- Conducted capture the flag style penetration tests of vulnerable systems using Metasploit.
- Authored technical documentation of technical findings and testing results in lab projects.

Additional Information

- U.S. citizen, eligible for security clearance.
- Pursuing CompTIA Linux+ and Security+ certifications.