Harshit Garg

Atlanta, GA | +1 (404)-259-0501 | iharshit.garg.cs@gmail.com | Linkedin: //harshitgarg-cs | Github: //harshitgarg-cs

Education

Georgia State University **Expected May 2026**

Bachelor of Science in Computer Science *Atlanta, GA*

- Relevant Coursework: Principles of Computer Science, Calculus I, CYB 101 (Intro to Cybersecurity), CYB 102 (Intermediate Cybersecurity).
- GPA: 3.48, Microsoft Scholar 2024.

Certifications & Skills

Certifications: ISC2: Certified in Cybersecurity, Microsoft Cybersecurity Analyst Professional Certificate

Tools: OSINT, John-the-ripper, SIEM, Splunk, Wireshark, Virustotal, Metasploit, MISP, nmap

Technical Skills: Python, Kali Linux, VMware Workstation, Password Hashing, Ethical Hacking, Network Security, Threat Detection & Mitigation, Identity & Access Management (IAM), Malware Analysis, Incident Response & Investigation

Work Experience

Mission Omega **September 2024 - Present**

IT & Security Intern *Remote*

- Assisting in the design and implementation of IT and security operations using Microsoft 365 and Azure platforms, focusing on streamlining processes through Power Automate and enhancing security monitoring with Azure Sentinel.
- Collaborating with the IT team to integrate Microsoft SharePoint and Power BI into operational workflows, working towards improved data analysis and reporting for enhanced decision-making.

Datacom **August 2024**

Job Simulation *Remote*

- Conducted a comprehensive threat analysis on APT34 using OSINT tools, leading to the identification of key Tactics, Techniques, and Procedures (TTPs) and the development of a defense strategy that enhanced the client's network security against future cyber threats.
- Applied the MITRE ATT&CK Framework to categorize cyber threats, successfully devising and recommending specific security measures such as multi-factor authentication (MFA), system patching, and network segmentation, resulting in improved protection for critical industries targeted by APT34.

TATA **July 2024**

Security Analyst Job Simulation *Remote*

- Acquired expertise in identity and access management (IAM) by collaborating with the Cybersecurity Consulting team to strategically align security measures with business objectives.
- Delivered comprehensive documentation and presented complex technical concepts in an accessible format to clients, enhancing understanding of cybersecurity best practices.
- Performed IAM assessments that resulted in stronger access controls and improved security policies for clients.

Projects

Level Effect CTF Challenge | *OSINT, Virus Total, Wireshark, Cryptography* **July 2024**

- Participated in a national cybersecurity Capture The Flag (CTF) competition focused on real-world scenarios.
- Analyzed and solved challenges related to cryptography, web security, incident response, and OSINT.
- Achieved a 360th rank out of all participants with a score of 2400 points, demonstrating proficiency in critical cybersecurity skills.

Incident Response Simulation | *SIEM, Virus Total, Wireshark, Splunk* **April 2024**

- Accomplished a simulated incident response by orchestrating and executing an investigation utilizing a range of cybersecurity tools, including Wireshark, Splunk, and SIEM to identify and mitigate security incidents.
- Analyzed traffic logs and extracted relevant threat intelligence to detect anomalies, utilizing Splunk dashboards to create insightful visualizations of threat events.
- Investigated indicators of compromise (IoCs) and used VirusTotal to assess potential malware threats, improving response efficiency by 15% compared to previous exercises.

Password Cracking Using John | *John-the-ripper* **October 2023**

- Cracked hashed passwords of different salts from a simulated data breach using John the Ripper, employing multiple wordlists and custom-made rules to test password strength.

Penetration Testing | *nmap, Wireshark, Virus Total, vsftpd* **October 2023**

- Utilized nmap to conduct a comprehensive scan for open ports and potential vulnerabilities.
- Leveraged the Metasploit Framework to execute pre-made exploits, specifically demonstrating the vsftpd backdoor exploit. This involved running msfconsole, loading, and executing the exploit to gain access to the target system.