Harshit Garg

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

Education

Georgia State University

Bachelor of Science in Computer Science — *Atlanta, GA*

- Relevant Coursework: Data Structures, Computer Org, System Levels & Programming, CYB 101 (Intro to Cybersecurity), CYB 102 (Intermediate Cybersecurity), Ethical & Social Issues in Computing.
- GPA: 3.71, Microsoft Scholar 2024.

Certifications & Skills

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

Tools: OSINT, John-the-ripper, SIEM, Wireshark, Virustotal, nmap, Cyberchef, Shodan, msfvenom

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

Work Experience

Mission Omega — **September 2024 - Present**

IT & Security Intern — *Remote*

- Reviewed security policies and recommended improvements to meet compliance requirements, ensuring alignment with organizational standards.
- Replaced manual Excel-based tracking of software licenses and costs by importing vendor and license data into HaloITSM, mapping licenses to users, and automating monthly cost reporting with SQL queries, significantly improving efficiency and accuracy in cost management.

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.

Projects

GSU Technology Immersion Challenge (CTF) sponsored by Truist | *OSINT, CyberChef, Wireshark, Docker* — **Novemeber 2024**

- Led Cipher Soldiers as team captain to a top 10 finish (10th of 27 teams) in the CTF challenge, by solving 8 of 10 challenges and earning 4,525 points.
- Enhanced cybersecurity skills across reverse engineering, forensics, cryptography, and pwn categories through strategic problem-solving and collaboration.

Level Effect CTF Challenge | *OSINT, Virus Total, Wireshark* — **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.

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.