# Rahil Vasa

+1 (404) 426-4988 rvasa7@gatech.edu linkedin.com/in/rahil-vasa-8b364a115/ github.com/rvasa01

## Objective

Last year Computer Engineering student skilled in malware reverse engineering, network security, and cyber threat detection, with hands-on experience in IDA Pro, Wireshark, Ghidra, Metasploit, Snort, and several CTF competitions. Seeking a full-time cybersecurity role starting summer 2025 to apply expertise in Security & Privacy.

## Education

**Georgia Institute of Technology, Atlanta, Georgia** **Aug 2023 – May 2025**
*Bachelor of Science in Computer Engineering* *GPA: 3.85/4.00*

- **Relevant Coursework:** Intro to Comp Security, Intro to Malware Reverse Engineering, Computer Communications
- **Relevant Skills:** IDA Pro, Wireshark, nping, Ghidra, Metasploit, Snort, CTFs
- **Relevant Programming Languages:** C++, C, Python, TypeScript, GoLang, Java, Intel x86 Assembly, Vue.js

**Emory University, Atlanta, Georgia** **August 2020 – May 2023**
*Bachelor of Arts in Computer Science and Minor in Physics* *GPA: 3.41/4.00*

- **Relevant Coursework:** Systems Programming with C, Advanced Computer Architecture, Data Structures and Algos

## Experience

**Honeypot Technologies,** Atlanta, Georgia | *Security Engineering Intern* **September 2024 - Present**

- Enhancing threat analytics platform to detect and mitigate malicious behaviors on client websites—including bots, harmful activities, anonymized traffic, and VPN users—flagging over 100,000 users fitting one or more of the above tags; contributing to a patent-pending cookieless 'handprint' tool to track malicious users across devices and networks.
- Utilizing TypeScript to efficiently execute code on Cloudflare Workers for rapid end-user engagement, proactively implementing countermeasures and achieving a 70% improvement in response time to malicious activity.
- Developing the front-end using Vue.js and TypeScript, integrating with back-end Python services; implemented AES-256 encryption to securely store critical customer and session data within cookies.

**Honeypot Technologies,** Atlanta, Georgia | *Security Engineering Intern* **May 2024 – August 2024**

- Leveraged the Open Canary library to deploy decoy online services (honeytokens) that mimic active services, attracting cyber threat actors scanning for open ports and services. Captured detailed attack telemetry to identify and assess malicious activities, contributing to early-stage detection in the incident response process.
- Developed a GoLang-based SaaS CLI to automate the deployment of honeypot VMs with honeytokens via AWS. Securely sent POST messages with attacker data and targeted ports to the server for real-time monitoring.
- Utilized AWS KMS to generate RSA key pairs and sign SaaS license data with secure hashing via SHA-256, ensuring encrypted communication between the client and Honeypot's server, and secure license validation at CLI execution.

**Cyberphysical Systems Lab,** Atlanta, Georgia | *Research Team Leader* **August 2023 – December 2023**

- Led a research team integrating Robot Operating Systems (ROS) and HELICS, improving simulation accuracy by 10x, effectively capturing both robotic and energy system dynamics.
- Collaborated with GTRI researchers using Agile methodologies, implementing C++ algorithms to replicate robot sensor environments, resulting in a 50% improvement in accuracy benchmarks.
- Managed task assignments and progress using Jira, aligned tasks with team members' skills, led Agile-style meetings, and documented outcomes in an IEEE-format research paper.

## Projects

**Penetration Testing and Exploitation** | *Wireshark, Snort, Metasploit, Nmap* **May 2024 - October 2024**

- **Penetration Testing using Metasploit in Kali Linux** | *Atlanta, Georgia*
  Conducted penetration testing on a vulnerable system using Metasploit tools and Nmap for service enumeration, exploiting rlogin, ingreslock, distccd, VSFtpd, Samba, and Postgres services to gain root access and display critical files.
- **Buffer Overflow Exploitation** | *Atlanta, Georgia*
  Developed an exploit to perform a buffer overflow attack, injecting shellcode to spawn a root shell by manipulating return addresses. Utilized GDB to analyze memory layouts, implement NOP sleds, and calculate target addresses for successful exploitation.
- **TCP/IP Vulnerabilities and Attack Simulation** | *Wireshark, nping, Telnet, SSH, Packet Spoofing*
  Conducted SYN flooding attacks, simulated TCP RST packets, performed session hijacking with sequence number prediction, and developed reverse shell backdoors using Nping, Wireshark, and Netcat.

**Reverse Engineering** | *IDA Pro, Ghidra, Intel x86 Assembly Programming* **January 2024 - February 2024**

- **Disassembly of SQL Slammer Worm using Ghidra** | *Atlanta, Georgia*
  Analyzed its propagation via SQL Server 2000's buffer overflow vulnerability, utilizing a 376-byte code that dispersed 10,000 packets within 10 minutes, deepening understanding of malware dissemination.