Vedika Sunil Bang

+1-8437431326 vedikabang@gatech.edu LinkedIn GitHub vedikabang.com Atlanta, GA (Open to Relocation)

Education

Georgia Institute of Technology **Aug 2022 – Dec 2023**
MS in Cybersecurity (GPA: 3.63/4.0)(Highest Honors) *Atlanta, GA*

- Relevant Coursework: Information Security Policies, Applied Cryptography, Intro to Malware Reverse Engineering, Advanced Network Security, Secure Computing Systems, Defense Lab, Cyber Practicum

Graduate Teaching Assistant – CS 6725 [Fall'23] Introduction to Information Security Policies

Pune Institute of Computer Technology **Aug 2016 – Nov 2020**
BE Electronic and Telecommunications (First Class with Distinction) *Pune, India*

Experience

Georgia Tech **March 2024 – Present**
Cybersecurity Research Associate *Atlanta, GA*

- Reverse engineering password-stealing trojans against open-source password managers - Bitwarden & KeePass, focusing on MITRE ATT&CK's TTP, TA0006 Credential Access to identify vulnerabilities and improve detection and prevention strategies

Stroz Friedberg, an Aon company **Jun 2023 – Aug 2023**
Cyber Summer Associate *Washington, DC*

- Led the identification and documentation of tactics, techniques, and procedures (TTPs) by analyzing MSP tools such as RMMs - ScreenConnect, and AnyDesk, integrating over 40 unique Indicators of Compromise (IoCs) into Aon's SIEM , enhancing threat intelligence capabilities and incident response efficiency by 20%
- Performed comprehensive host-based analysis on over 70 digital forensic images using tools like X-ways, EnCase, and FTKImager, while performing log analysis on firewall logs, VPN logs, network traffic, O365 and AWS, Azure environments' logs for a Business Email Compromise (BEC) and a Threat hunt to identify potential Adversarial TTPs
- Developed Python and PowerShell scripts to automate routine security tasks, reducing manual workload by 10% and enhancing the overall efficiency of security operations

Information Sharing and Analysis Center **Dec 2021 – May 2022**
Computer Forensics Engineer *Delhi, India*

- Performed malware analysis using Volatility3, Wireshark, IDA-Pro & LAMP for memory analysis, identifying critical vulnerabilities in live engagements.
- Conducted detailed code reviews and developed 3 critical exploits for Windows, contributing significantly to threat modeling and the evaluation of new security controls.
- Dockerized, and tested 200+ specialized labs for virtual Capture The Flag (CTF) event, covering a diverse range of OWASP Top 10 challenges, simulating real-world red teaming exercises

Wattlecorp Cybersecurity Labs **Aug 2021 – Dec 2021**
Vulnerability and Penetration testing Intern *Remote, India*

- Performed vulnerability assessments, and analyzed code for OWASP vulnerabilities on 6 assigned systems, utilizing both SAST (Static Application Security Testing) and DAST (Dynamic Application Security Testing) methodologies - Reported Documented DOM-XSS, CSRF

Projects

Living off The Land Attacks: Application IoC Generator **Aug 2023 – Present**

- Developed a python-based tool for automating the generation of high-fidelity 75+ IoCs and detection rules for dual-use tools, achieving a 60% acceptance rate from leading open source SIEMs & Threat-Intel feed

Mini Coursework Projects **Jan 2023 – Dec 2023**

- Development of Host based and Network based IDS: CS 6264 Defense labs
- Implemented PoC for exploits involving XSS, CSRF, SQL Injection: CS 6035 Intro to Information Security
- Implemented Zero Trust Model for CS 6038 Secure computing system

Sending Email from a Residential ISP, CS 8803-EMS **Sep 2022 – Dec 2022**

- Led an experimental study with **Prof. Paul Pearce** to explore the individual impacts of removing email security protocols (SPF, DKIM, DMARC) on the deliverability and security of emails sent from residential IP addresses; providing insights into email server performance and reliability in home internet setups

Malware HomeLab *Tech stack: IDA Pro, Ghidra, Olly-dbg, C, x86_64/32* **Jan 2023 – Present**

- Engaged in solving complex CTF challenges on platforms like Root Me, CrackMes.one, and OverTheWire. Gained practical experience in reverse engineering malware such as Michelangelo.1, DOS-7, Harulf, SQLSlammer, Lucius by manual and dynamic code review

Technical Skills

Operating System: Linux/Unix (Pentesting), Windows (Malware Analysis)
Languages: Python, C, php, MySQL, Bash, PowerShell, Javascript, Java
Security Tools/Protocols: Volatility3, Wireshark, IDA Pro, Ghidra, GDB, Splunk, Xways, FTKImager, SQLite, Nmap, Metasploit, Burp Suite, YARA, Semgrep playground, OpenSSL, Snort3, Sigma, Suricata, Autopsy, ELK, Velociraptor
Frameworks: SOC2, Okta, Service Now, Docker, MITRE ATT&CK, AWS, ISO 27001, PCAP analysis, TCP/IP, TLS, DNS

Certifications & CTFs

Google Cybersecurity Professional Certificate	Google (Coursera)
OSCP	Targeted by August'24
NSA Codebreaker 2022 and 2023	6 out of 9 & 5 out of 8
TheDFIRReport CTF	15th rank