Vinay Menon

Schedule Meeting | +1-(315)886-4655 | Github | vimenon@syr.edu | LinkedIn | E-Portfolio

EDUCATION

Syracuse University (GPA: 3.5 / 4.0) **Master of Science in Cybersecurity, May 2025**

- Digital Forensics, Internet of Things: Security and Privacy, Internet Security.

SRM Institute of Science and Technology **Bachelor of Technology in Computer Science, June 2021**

- Computer Networks, Cryptography, Artificial Intelligence, and MIS.

WORK EXPERIENCE

Bank of America, Software Engineer **March 2022 - July 2023**

- Designed and implemented scalable Python applications using Django and Flask, collaborating closely with cross-functional teams to align on project requirements and achieve a 30% improvement in application performance.
- Developed and maintained RESTful APIs, coordinating with front-end developers and third-party services to ensure seamless integration and a 25% reduction in response times.
- Resolved 100+ software incident tickets through code reviews and integration testing, leading to improved code quality.
- Planned automated testing using pytest and unittest, increasing test coverage to 90% and reducing bug-related issues.
- Mentored 5 interns, guiding the development of 75+ RAFT automation scripts, which reduced manual testing time by 60%.

Wipro LTD, Project Engineer (Security Team) **June 2021 - March 2022**

- Utilized Splunk to collect and analyze security logs from diverse sources, enhancing real-time threat detection and response accuracy, and achieving a 25% reduction in incident response time.
- Documented and reported on 100+ incidents with ServiceNow, ensuring accurate and detailed records that supported a 20% increase in incident resolution.
- Leveraged Python scripting to automate routine security tasks, saving approximately 5 hours of manual work per week and enhancing the efficiency of security operations.
- Designed and executed phishing simulations in collaboration with IT security team, creating realistic scenarios with GoPhish to test 1000+ workstation responses and improve training programs.
- Led and organized cybersecurity awareness training sessions for over 100 employees.

PROJECT EXPERIENCE

Virtual Private Network **May 2024**

- Developed a TUN/TAP interface with Python for TCP/IP packet handling and interface configuration, ensuring reliable operation with 100% uptime and effective network traffic management.
- Established a UDP tunnel supporting up to 2048 bytes per packet, enabling efficient bidirectional communication.

Data Encryption for Medical Images **February 2024**

- Collaborated on a group project to develop a data encryption system for medical images using AES and steganography LSB algorithms, enhancing data security and confidentiality.
- Integrated encryption and steganography techniques in Python, resulting in a 50% increase in protection against unauthorized access to sensitive medical data.

Defense against Data poisoning on SVM **December 2023**

- Created and evaluated an SVM classifier on 10,000 MNIST samples, achieving over 95% accuracy.
- Simulated label flipping and data injection attacks, devised anomaly detection using techniques like PCA and Isolation Forest, resulting in a 25% improvement in model accuracy under attack conditions.

SKILLS

- **Programming:** Python (Intermediate), Java (Intermediate), C# (Basic), JavaScript (Basic), Shell/Bash scripting.
- **Penetration Testing:** Nmap, Kali Linux, Metasploit, Burp Suite, Aircrack-ng, OWASP ZAP.
- **Security Tools:** Wireshark, Active Directory, Splunk, Nessus, Snort, OpenVAS, Qualys.
- **Additional Skills:** MITRE ATT&CK Framework, SIEM, SOAR, Cloud Security, Firewalls, VPN, IDS/IPS, Microsoft Excel.
- **Certifications:** CompTIA Security+ (2024).

PROFESSIONAL DEVELOPMENT

- Completed over 50 rooms on TryHackMe, demonstrating advanced cybersecurity skills and ranking in the top 5% of users.
- Created mini projects such as a Remote Access tool and Morris Worm simulation, highlighting hands-on experience in network security and malware analysis.
- Participated in Capture the Flag (CTF) events, including NCL, where I used password cracking tools and various CTF-specific techniques to solve security challenges and vulnerabilities.