Yash Suhas Shinde

+1 607-624-9047 | shindeyash28@gmail.com | linkedin.com/in/shindeyash28

EDUCATION

SUNY Binghamton **May 2024**
Masters in Computer Science
University of Mumbai **May 2022**
Bachelor of Engineering in Information Technology

CERTIFICATIONS

OffSec OSCP — Ongoing
ISC2 Certified in Cybersecurity (ISC2) — Dec 2024
CompTIA Security+ SY0-701 (CompTIA) — Aug 2024
Google Cybersecurity Professional Certificate (Coursera) — May 2024

TECHNICAL ACTIVITIES

JerseyCTF – Participant **New Jersey, USA**
- Solved 10+ forensic and exploitation challenges, capturing flags from memory dumps, disk images, and log files using Autopsy/ FTK.
- Uncovered encoded payloads and demonstrated techniques such as metadata manipulation.

Homelab – Personal Cybersecurity Lab **New York, USA**
- Created and managed a virtual SOC environment with pfSense, Suricata, and Kali Linux, generating 200+ IDS events per week for simulated intrusion detection testing.
- Planning to expand this to create a custom NAS solution for personal use.

CTF Club @ SUNY Binghamton – Active Member **New York, USA**
- Solved 30+ cryptography and reverse engineering problems, using Ghidra and Python scripting to analyze compiled binaries and recover hidden messages.
- Ranked in the top 20% of the total members in terms of successful flag captures.

WORK EXPERIENCE

Trace Labs – Volunteer Coach **Remote | Nov 2024 – Present**
- Coached 15+ OSINT teams in real-time CTF investigations, validating over 100 pieces of intelligence and ensuring highest accuracy in submissions during global Search Party events.
- Utilized OSINT tools like Wayback Machine, Google Dorking, and TruePeopleSearch to validate 100+ submissions and uncover digital footprints.

Syndicate Services LLC – Junior Information Security Analyst **Remote | July 2025 – Present**
- Monitored network and system activity through centralized logging, assisting in investigations and refining alert workflows to improve detection accuracy.
- Supported deployment of defensive technologies, access reviews, and documentation efforts, enhancing policy compliance and audit.

SUNY Binghamton – Research Intern **New York, USA | July 2024 – July 2025**
- Deployed Passbolt on AWS with SSL/TLS, RBAC, and automated backups; built a custom firewall to segment traffic and began developing a VPN solution for secure inter-environment communication.
- Collaborated with a cybersecurity professor to assess IAM practices, network segmentation, and policy adherence across the university's infrastructure, identifying and documenting key security gaps.

TCRInnovation – Junior SOC Analyst **Mumbai, India | Apr 2022 – Aug 2022**
- Monitored and triaged over 500+ security alerts using Chronicle and Suricata, identifying patterns of DNS tunneling and brute-force attacks across enterprise logs.
- Tuned SIEM alerts by analyzing recurring false positives and writing basic rule logic to improve detection accuracy, reducing average alert noise and response time by 15%.

PROJECTS

Secure Election Booth **Sep 2023 – Mar 2024**
- Developed a Python-based online voting platform with SSL/TLS encryption and one-time session tokens to protect ballot integrity and prevent vote duplication.
- Implemented authentication logic and access controls to simulate secure voting workflows for academic evaluation of confidentiality and non-repudiation principles.

Web Proxy Server **Aug 2022 – Nov 2022**
- Developed a multithreaded proxy server in Python implementing caching to handle concurrent HTTP requests efficiently.
- Incorporated socket reuse and response validation to manage request redundancy and ensure handling of client-server communication.

Enterprise Network Design for College **Aug 2022 – Nov 2022**
- Designed a scalable network for 500+ users using CPT, incorporating VLANs, ACLs tailored to the college's infrastructure needs.
- Collaborated with the college IT team to optimize the design for improved efficiency and cost-effectiveness, balancing performance.

SKILLS

Security Tools: Suricata, Google Chronicle, Splunk, FTK Imager, Autopsy, Wireshark, Burp Suite, Powershell
Platforms: Kali Linux, pfSense, AWS, Azure, VMware, Docker, VirtualBox, Python, Bash, ServiceNow
Security Domains: Incident Response, SIEM, Log Analysis, Digital Forensics, Firewall Config, OSINT