SUVAM BARUI

5852868666 ◇ sb9895@rit.edu ◇ suvam-barui(in) ◇ HTB

PROFESSIONAL SUMMARY

Versatile and certified cybersecurity professional with hands-on experience in offensive security, threat detection, and security automation across enterprise and simulated environments. Proven expertise in penetration testing, adversary emulation, and SOC operations, with strong proficiency in tools like Burp Suite, AlienVault, and SOAR platforms. Holds OSCP, HTB CPTS, CompTIA Security+, and AWS Cloud Practitioner certifications. Recognized for top-tier rankings on HackTheBox (Top 500) and TryHackMe (Top 1%), with a strong foundation in scripting, security orchestration, and continuous threat detection improvement.

EDUCATION

Rochester Institute of Technology — Rochester, NY
Master of Science in Computing Security — *Aug 2022 - Dec 2024*
Computer System Security, Cryptography & Authentication, Network Security, Web Application Security Audits, Social Engineering, Cyber Analytics & Machine Learning

Haldia Institute of Technology (MAKAUT) — Kolkata, India
Bachelor of Technology in Computer Science and Engineering — *Aug 2015 - May 2019*

CERTIFICATIONS

- Offensive Security Certified Professional OSCP+ | OSCP — Jul 2028
- HTB Certified Penetration Testing Specialist HTB CPTS — Jun 2025
- AWS Certified Cloud Practitioner AWS CCP — Feb 2028
- CompTIA Security+ SYO-601, COMP001021892318 — Jul 2027

WORK EXPERIENCE

Security Engineer Intern (Multiple Domains) — May 2025 - present
Securely Yours LLC — *(Bloomfield Hills, Michigan)*

- Conducted comprehensive web application penetration testing using tools like Burp Suite, ZAP Proxy, XSStrike, SQLMap and nuclei; identified and documented vulnerabilities with detailed reports outlining risk levels and remediation steps.
- Engineered a secure SOAR automation architecture using Shuffle workflows and USM Central APIs, fortifying incident response processes and ensuring alignment with industry security best practices.
- Automated security orchestration workflows by developing playbooks for incident response using USM Central and USM Anywhere APIs.
- Optimized firewall and network log management by analyzing, filtering, and suppressing redundant or low-value logs to enhance SIEM efficiency and reduce storage costs.
- Integrated Virus Total API to enrich security alerts and accelerate threat intelligence gathering. Generated client-ready OTX writeups, streamlining threat reporting and communication.

Security Operations Center (SOC) Intern — Feb 2025 - May 2025
Securely Managed LLC — *(Bloomfield Hills, Michigan)*

- Monitored security events and performed threat detection using AlienVault (LevelBlue), analyzing logs to identify and mitigate potential risks.
- Investigated security incidents and implemented incident response measures, implementing preventive actions, and generating detailed reports on threats and vulnerabilities.
- Researched emerging threats and provided monthly updates, improving security awareness, and strengthening overall security posture through continuous improvements.

Graduate Teaching Assistant, Hacking for Defense — Jan 2023 - Jul 2024
Simone Center for Innovation and Entrepreneurship, Rochester Institute of Technology — *Rochester, New York*

- Engage actively in classroom activities, fostering an environment conducive to student learning and engagement in solving real-world problems for government organizations, including the Department of State and the Department of Defense, leading to the adoption of some of the solutions by these agencies.
- Improved project efficiency through supervising and mentoring student groups on government problem statements, leading to successful project completion and stakeholder satisfaction.

Freelance Security Researcher/Penetration Tester at Fiverr (Remote) — March 2021 - Jun 2022

- Led a variety of projects for an international client base, with a primary emphasis on Vulnerability Assessment and Penetration Testing and Vulnerability Management.
- Demonstrated expertise in identifying, analyzing, and exploiting a wide range of vulnerabilities, both historical and current, ensuring comprehensive security threat awareness.

PROJECTS

Network Recon & Vulnerability Automation | Github Jan 2025

- Automated multi-stage Nmap reconnaissance: Developed a Bash script that seamlessly transitions from fast top-TCP and common-UDP scans to full-port sweeps and targeted vulnerability checks.
- Dynamic port extraction & targeting: Parsed full-port scan results to identify open services, then ran version detection and vulnerability scripts only against those ports to maximize efficiency.
- Comprehensive reporting: Consolidated outputs into human-readable text logs and XML files for easy review, integration with parsers, and archival.
- Efficiency-driven workflow: Structured scans from quickest to most thorough, enabling early prioritization of critical services while retaining deep analysis for later stages.
- Improved pentest consistency: Standardized Nmap usage across assessments, reducing manual errors and accelerating security audit cycles.

SOC Home Lab Design and Deployment Sep 2024

- Built a SOC home lab on VirtualBox with **Wazuh (SIEM/EDR)**, **ELK Stack**, **Suricata (IDS/IPS)**, and **Zeek**, simulating enterprise environments with Active Directory, Windows endpoints, and a **pfSense** firewall.
- Simulated real-world attacks using **Atomic Red Team** mapped to **MITRE ATT&CK**, validating detection for credential dumping, privilege escalation, and lateral movement while automating response with **Shuffle (SOAR)**, **MISP**, and **OpenVAS**.
- Managed incidents and reporting with TheHive, refining detection techniques, enhancing security automation, and continuously updating security tools to improve the lab's functionality.

Watering Hole Attack Simulation (Social Engineering) Sep 2024 - Dec 2024

- Designed a social engineering challenge mimicking the 2013 DoL watering hole attack, guiding users through stages of an attack.
- Utilized tools like **Maltego**, **Burp Suite**, **GoPhish**, and **Metasploit** to simulate a realistic attack flow, including website compromise and data exfiltration.

Deep Learning Security: Malware Classification Jan 2024 - May 2024

- Investigate methods to handle extreme multi-label classification tasks in the context of malware samples.
- Developed and optimized a multi-class malware classification system using PyTorch, integrating advanced machine learning techniques to process and classify malware signatures from LMDB and SQLite databases. The project involved creating custom data loaders, implementing neural network architectures, and conducting rigorous training and validation cycles with real-time performance analytics on GPU, significantly enhancing malware detection capabilities.

SKILLS AND INTERESTS

Interests: HackTheBox [R:569 Pro Hacker(Top 500)], TryHackMe Top 1%, Offensive Security, Security Operations, Enterprise Security, Application Security, Product Security
Languages: C, C++, Java, Python, SQL, Bash, Powershell **Operating Systems:** Microsoft Windows, Linux
Tools: Metasploit, Burp Suite, Nmap, Nessus, Snort, Wireshark, Splunk, Microsoft Office Suite
Core Competencies: Vulnerability Assessment and Management, Penetration Testing, Threat Modeling
Frameworks: MITRE ATT&CK, Cyber Kill Chain, NIST, SOC2
Soft Skills: Time Management, Critical Thinking, Presentation Skills, Communication, Adaptability, Resilience, Problem-solving skills, Teamwork, Work Ethic, Collaboration, Leadership skills, Self-Motivated, Interpersonal Skills

ACHIEVEMENTS AND AWARDS

- HackTheBox Global Ranking Top 500 (101 user+root)
- Part of HTB Team [REDACTED] ranked Top 10 Worldwide.
- Ranked 326/9300 Hack The Box Season 7 (VICE) Jan–Apr 2025
- Part of CTF Team RaptX placed 29/1528 IrisCTF 2025
- Ranked 81/7825 Hack The Box Season 5 (Anomalies) Apr-Jun 2024