Vansh Saini

Srinagar, India
+91 9103188243 | vansh.sainiwork@gmail.com | GitHub | LinkedIn | TryHackMe

Summary

3rd-year IT student (NIT Srinagar) with hands-on SOC tooling experience – built a log triage and alert-scoring tool mapped to MITRE ATT&CK, conducted a full VAPT engagement on a vulnerable web app, and ranked in the **Top 3% on TryHackMe**. Seeking a SOC Intern role to apply log analysis, detection engineering, and incident triage skills.

Education

National Institute of Technology (NIT) Srinagar — Srinagar, India
B.Tech in Information Technology — 2024 – 2028
CGPA: 8.01/10

Projects

Loghound – Security Log Triage Tool — GitHub
Python, Textual, MITRE ATT&CK, JSON
- Built a Python-based security log triage tool to analyze authentication and web access logs and prioritize suspicious activity for investigation.
- Implemented detection scoring, event aggregation, MITRE ATT&CK mapping, JSON reporting, and an interactive terminal interface for structured alert analysis.
-

VAPT Lab – Web Application VAPT on OWASP Juice Shop — GitHub
Kali Linux, Burp Suite, Nmap, OWASP Top 10, Web Security
- Conducted structured security testing of OWASP Juice Shop, identifying and validating 8 vulnerabilities across authentication, authorization, injection, XSS, sensitive data exposure, and security configuration.
- Documented vulnerability evidence, severity ratings using CVSS, proof-of-concept steps, impact, and remediation recommendations in a formal VAPT report.

Azure Secure Web Application — GitHub
Microsoft Azure, VNet, NSG, Application Gateway, WAF, Bastion
- Designed a segmented Azure network architecture and configured NSGs and Application Gateway WAF to restrict unauthorized traffic.
- Implemented Azure Bastion for secure VM administration without exposing SSH/RDP endpoints directly to the public internet.

Technical Skills

SOC & Security Operations: Security Monitoring, Log Analysis, Alert Triage, Detection Engineering, Incident Analysis, MITRE ATT&CK, Authentication Analysis
Security Tools: Splunk, Wireshark, Nmap, Burp Suite, Metasploit, Kali Linux, Git, GitHub
Networking & Security: TCP/IP, HTTP/HTTPS, DNS, Network Enumeration, Network Security, Web Security, OWASP Top 10
Cloud Security: Microsoft Azure, VNet, NSG, Application Gateway, WAF, Bastion
Programming: Python, Java, C, HTML, CSS
Core CS: Computer Networks, Operating Systems, DBMS, OOP, Data Structures & Algorithms

Experience

Team Lead – CodeSlayers 2K25 Hackathon — Nov 2025
NIT Delhi
- Led a 4-member team during a 36-hour hackathon, coordinating task allocation, technical execution, and project delivery.
- Designed and implemented a Solidity/Ethereum blockchain layer for tamper-resistant grievance records and auditability.

Caarya – NIT Srinagar Pod — Nov 2025 – May 2026
COO → Core Team Member — LOR
- Managed operational execution, documentation, and coordination across student teams within the NIT Srinagar Pod.
- Designed workflows using Notion, Google Drive, and Discord for onboarding, documentation, progress tracking, and team coordination.

Certifications

- **Certified Ethical Hacker (CEH v13) – EC-Council** — Certificate
- **Certified Network Security Practitioner (CNSP)** — Certificate
- **Defronix Ethical Hacking Essentials (DEHE)** — Certificate
- **TryHackMe AI Security Path – Completed** — TryHackMe

Achievements

- **Ranked in the Top 3% on TryHackMe** — Profile
- **CodeSlayers 2K25 (NIT Delhi) – Ranked 8th among 2600+ teams; Qualified for National Finals**