STUTI SAXENA

stutisaxena337@gmail.com | +91 9407446913 | www.linkedin.com/in/stuti-19-saxena |
https://github.com/stuti-19

PROFESSIONAL SUMMARY

Cybersecurity professional with expertise in Security Operations, Digital Forensics, VAPT, and Threat Intelligence. Skilled in incident response, malware analysis, network traffic analysis, and automating threat workflows using Python and ML. Experience in SOC operations, penetration testing, offensive security research, and MITRE ATT&CK mapping.

TECHNICAL SKILLS

Security Operations: SIEM (QRadar), Alert Triage, Log Analysis, Incident Response, Threat Intelligence, IOC Correlation, CVE/CVSS Analysis, MITRE ATT&CK Mapping
Offensive Security: Vulnerability Assessment, Network Scanning, Service Enumeration, Web Application Testing, Penetration Testing, Red Team Operations
Digital Forensics: Disk Imaging, Memory Forensics, Network Forensics, Malware Analysis, Email Forensics, OSINT, Chain of Custody
Programming: Python, Bash, SQL, SQLite, NLP, Machine Learning (Random Forest, SVM)
Tools: Nmap, Nessus, Burp Suite, Metasploit, Suricata, Wireshark, Autopsy, FTK Imager, Kibana, ELK Stack, Docker, Tor
Technologies: IBM watsonx.ai, REST APIs, Docker Compose, STIX/TAXII

PROFESSIONAL EXPERIENCE

Digital Forensics and Cyber Crime Investigation Intern September 2, 2025 – October 4, 2025
Slytherin EduTech Pvt. Ltd *Bhopal, India*

- Analyzed malware traffic, email headers, and network artifacts to identify attack vectors and indicators of compromise
- Applied MITRE ATT&CK techniques during incident response simulations and threat-hunting exercises
- Built Python and SQLite automation to classify digital evidence, reducing analysis time by 40%
- Created investigation-ready documentation including IOCs, timelines, and threat intelligence reports

Cyber Security and Digital Forensics Intern July 2025
Madhya Pradesh (HQ) Cyber Cell *Bhopal, India*

- Supported active cybercrime investigations through log correlation, system imaging, and artifact identification
- Conducted forensic analysis using Autopsy and FTK Imager to extract and document digital evidence
- Prepared structured forensic reports following strict chain-of-custody and evidence preservation procedures

AI & Cloud Technologies Intern July 2025 – August 2025
IBM SkillsBuild *Bhopal, India*

- Implemented secure AI/ML workflows and APIs using IBM watsonx.ai with cloud security best practices
- Built NLP-based automation for classification tasks and model lifecycle management
- Developed secure API integrations and cloud infrastructure protection strategies

PROJECTS

Red Team Recon & CVSS-Based Exploitation Mapper 2025
Python, Nmap, MITRE ATT&CK, CVSS, Metasploit

- Developed automated Red Team reconnaissance tool using Python and Nmap to enumerate network services and support VAPT assessments
- Implemented CVE correlation with CVSS v3 severity scoring to prioritize vulnerabilities based on risk and exploitability

- Mapped attack vectors to MITRE ATT&CK techniques and integrated Metasploit exploit guidance for ethical penetration testing
- Generated structured, report-ready output for vulnerability prioritization and executive-level security decision support

Adaptive Deception & Threat-Intelligence Honeypot Platform (ADTIP) 2025
Python, Suricata, Docker, ELK Stack, MITRE ATT&CK, Machine Learning

- Architected distributed honeypot infrastructure with Suricata IDS detecting 500+ simulated attack attempts
- Developed automated threat correlation pipeline using Python and ELK stack with ML classifiers achieving 92% accuracy
- Mapped captured TTPs to MITRE ATT&CK framework and generated STIX/TAXII-compliant threat intelligence feeds
- Containerized microservices architecture using Docker Compose for scalable multi-tenant deployment

Dark Web Marketplace Monitor (OSINT Prototype) 2024
Python, Selenium, BeautifulSoup, NLP, SQLite, Tor

- Engineered Tor-proxied web scraping framework for automated .onion domain reconnaissance
- Implemented NLP pipeline with TF-IDF vectorization to extract PII, CVE references, and malware indicators
- Built pattern matching engine for cryptocurrency wallet detection with automated alert generation
- Designed SQLite schema with indexed full-text search for rapid querying of 10,000+ scraped entries

EDUCATION

Bachelor of Technology in Information Technology Expected July 2026
University Institute of Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya Bhopal, India
Higher Secondary Education (PCM with Python) 2022
Carmel Convent Senior Secondary School, B.H.E.L. Bhopal, India

CERTIFICATIONS

Certified Ethical Hacker (CEH) v13 AI-integrated – EC-Council
Google Cybersecurity Professional Certificate – Google
Android Bug Bounty – EC-Council
Introduction to Dark Web, Anonymity, and Cryptocurrency – EC-Council

ACHIEVEMENTS

- Captured all flags in Indian Army Terrier Cyber Quest CTF demonstrating exploitation and forensics skills
- Assisted MP Cyber Cell with threat classification through dark web monitoring and forensic analysis workflows
- Developed honeypot platform detecting and analyzing 500+ simulated attacks with automated threat intelligence reporting