Samrat Dey

+91-9382919726 samratdey.career@gmail.com github.com/3rr0r-505 linkedin.com/in/samratd3y

B.Tech — Computer Science Engineering • *Penetration Testing & Red Team Enthusiast*

Professional Summary

B.Tech Computer Science graduate with hands-on experience in cybersecurity, penetration testing, and vulnerability analysis across lab, academic, and cloud environments. Proficient in Linux security, network protocols (TCP/IP, DNS, HTTP), Python-based security scripting, and SIEM-based threat monitoring using Wazuh. Seeking an entry-level role in red teaming, security auditing, or enterprise security assessment.

Technical Skills

Offensive Security Tools: Metasploit, Nmap, Burp Suite, Nikto, WPScan, Searchsploit, Trivy, Bandit, Safety-CLI, msfvenom, Sherlock

Security & Monitoring: Wazuh SIEM, Wireshark, log analysis, threat detection, MITRE ATT&CK

Programming & Scripting: Python (security scripting, automation), C/C++, Bash

Cloud & Platforms: AWS EC2, Docker, Git/GitHub, VMware, VirtualBox, VS Code

Databases: MongoDB (Atlas, Compass), MySQL **OS:** Kali Linux, Ubuntu, Windows

Experience

Cyber Security & Ethical Hacking Intern *Jul. 2024 – Aug. 2024*
NIELIT Haridwar, India Certificate

- Performed vulnerability assessment and exploitation using Metasploit, Nmap, Searchsploit, and Sherlock against lab environments (Metasploitable, EternalBlue/DoublePulsar).
- Conducted adversary simulation on Android targets (msfvenom, AndroRAT, StromBreaker); deployed and monitored Wazuh SIEM for threat detection and log correlation.
- Analyzed landmark malware campaigns (WannaCry, NotPetya, Stuxnet) to extract TTPs and map to MITRE ATT&CK; completed structured CTF challenges on TryHackMe.

Projects

HoneyPott3r — Honeypot Vulnerability Assessment Framework GitHub
Systematic security analysis framework targeting honeypot infrastructure (Docker, AWS EC2).

- Executed simulated attack scenarios (detection evasion, privilege escalation, reverse exploitation, DoS) against Cowrie, Conpot, and Wordpot honeypots; conducted multi-vector scanning using Trivy, Bandit, Nmap, Nikto, and WPScan.
- Identified critical configuration weaknesses; stored telemetry in MongoDB with interactive dashboard for reporting. Findings published as peer-reviewed paper in IJPREMS (Mar. 2025).

KeySpy — Endpoint Monitoring & Keystroke Security Research Tool GitHub
Python-based endpoint risk analysis tool for keylogger and remote payload execution (RPE) research.

- Simulated USB-based payload delivery and RPE scenarios to evaluate EDR gaps; implemented AES encryption for secure data storage and built a real-time web interface for event visualization.

HawkPro — Linux System Monitor for Process & Resource Analysis GitHub
Terminal-based real-time monitoring tool in C++ with ncurses — relevant to process injection detection.

- Parsed Linux `/proc` filesystem for CPU, memory, and process-level statistics; modular CMake architecture with optimized polling for minimal overhead.

Education

Adamas University, Kolkata *2021 – 2025*
B.Tech in Computer Science and Engineering *CGPA: 8.77*

Publications

HONEYPOTT3R: An Open-Source Multi-Layered Security Analysis Framework for Honeypot Vulnerability Assessment
IJPREMS, vol. 5, issue 3, pp. 1723–1730, Mar. 2025 DOI: 10.58257/IJPREMS39220

Certifications

TryHackMe: CompTIA Pentest+, Jr. Penetration Tester, Advent of Cyber 2024, Intro to Cyber Security, Web Fundamentals

AWS Educate: Introduction to Cloud 101, Cloud Semester 1