Panuganti Siva Aditya

sivaaditya456@gmail.com — +91 9391092669 — Rangampeta, India
https://github.com/sivaadityacoder

Professional Summary

Cybersecurity professional specializing in red team operations, penetration testing, and vulnerability assessment. Experienced in simulating adversary tactics, identifying security gaps, and recommending remediation. Proficient in scripting, security tools, and incident response.

Education

B.Tech in CSE-IoT, Aditya College of Engineering and Technology
2023–2026 CGPA: 6.55

Diploma, Aditya College of Engineering
2021–2023 Grade: 60%

Skills

Red Team Operations
- Penetration Testing (Web, Network, Cloud)
- Vulnerability Assessment
- Social Engineering
- Python, Bash, PowerShell
- Kali Linux, Metasploit, Burp Suite, Nmap, Cobalt Strike
- Security Reporting
- Incident Response

Experience

Intern – AGRATAS EDUTECH, Hyderbad (Feb 2025 – May 2025)
Project: Malware Analysis
- Conducted static and dynamic analysis on various malware samples to identify behavior patterns, system modifications, and persistence mechanisms.

- Reverse-engineered executable files and monitored system-level activities (file system, registry, network traffic) using tools like Ghidra, Wireshark, and Process Monitor.

- Documented malware functionality and propagation techniques, Including Trojans, ransomware, and worms, to develop detailed behavioral reports and detection signatures.

Freelance Security Researcher - Remote — 2024-Present
- Discovered and disclosed vulnerabilities via bug bounty programs.
- Built and maintained a personal attack simulation lab.

Projects

Active Directory Attack Lab - Designed a virtual lab for privilege escalation and lateral movement practice.
Phishing Simulation Campaign - Executed a phishing awareness campaign, reducing click rates by 60

Web Application Penetration Testing - Performed end-to-end penetration testing on a mock e-commerce platform.
- Identified and exploited vulnerabilities such as SQL injection, XSS, and insecure authentication.
- Documented findings and provided remediation steps.

Network Security Monitoring with SIEM - Deployed and configured a Security Information and Event Management (SIEM) solution using open-source tools.
- Monitored network traffic, detected suspicious activities, and generated incident reports.

Custom Exploit Development - Developed custom scripts in Python to automate vulnerability scanning and exploitation.
- Created proof-of-concept exploits for known CVEs in a controlled lab environment.

CTF (Capture The Flag) Participation - Participated in online CTF competitions (Hack The Box, TryHackMe).
- Solved challenges in web exploitation, cryptography, and reverse engineering.

Password Cracking Automation - Built a tool to automate password attacks using wordlists and hashcat.
- Demonstrated the importance of strong password policies to peers.

Certifications

- TryHackMe Red Team Path (Completed 2024)
- TryHackMe Junior Penetration Tester (Completed 2024)

Extracurriculars

Conducted Ethical Hacking on Own Lab Infrastructure - Set up local and cloud-based vulnerable machines (DVWA, Metasploitable, VulnHub VMs) to practice exploits and post-exploitation techniques.