SIDDHANT MANDAL

Nagpur, India | +91-8329084769 | siddhantmandal31415@gmail.com | linkedin.com/in/sigmandal | github.com/SkaiWkr

Summary

Computer Science (Cyber Security) student specializing in Linux security, malware analysis, and detection engineering. Designs and builds system-level security tools — including a behavioral shellcode analysis framework and a Linux privilege-drift monitoring system — to detect and analyze security-relevant system behavior.

Technical Skills

- **Programming:** Python, Java, C, C++, Bash, SQL
- **Security Tools:** Burp Suite, Wireshark, Nmap, Autopsy
- **Security Frameworks:** Unicorn Engine, Capstone, Scikit-learn
- **Operating Systems:** Arch Linux, BlackArch Linux, Windows
- **Platforms:** TryHackMe, Hack The Box
- **Domains:** Linux Security, Malware Analysis, Threat Detection, Detection Engineering, Behavioral Analysis, Privilege Escalation, Digital Forensics, Reverse Engineering, Cryptography, Security Research, Security Automation, Network Security

Projects

MorphShell — Sandboxed Shellcode Behavioral Analysis Framework GitHub ↑

Python • Unicorn Engine • Capstone • Scikit-learn

- Designed a Python framework for sandboxed shellcode behavioral analysis, safely emulating raw shellcode with Unicorn Engine and disassembling instructions via Capstone instead of executing samples natively.
- Engineered a feature-extraction pipeline capturing instruction flow, memory writes, Linux `int 0x80` syscalls, loops, NOP sleds, and write-then-execute behavior, then trained a Random Forest classifier (scikit-learn) to generate JSON reports with classification confidence.

PrivDrift — Linux Privilege Drift Monitoring Framework GitHub ↑

Python • Linux • HTML • JSON

- Designed and implemented a lightweight, zero-dependency Linux framework that captures trusted system baselines and performs deterministic snapshot comparison to detect drift across SUID/SGID bits, sudo rules, privileged groups, UID 0 accounts, and cron entries.
- Structured the system as a Collector-Baseline-Detector-Reporter pipeline with rule-based risk scoring, producing JSON reports and an HTML dashboard for reviewing detected changes.

Experience

OWASP Nagpur May 2026 – Present

Core Team Member

- Coordinate chapter operations and technical programming as part of the core organizing team for a local OWASP chapter.
- Collaborate on planning and delivery of security-focused sessions and community initiatives within the chapter.

BharatCares® Jun 2026 – Jul 2026 (120 Hours)

Cyber Security Intern

- Performed malware and shellcode analysis using controlled execution and behavioral analysis techniques to examine sample activity.
- Applied reverse engineering methods to support analysis and built internal security tooling to strengthen detection workflows.

SkillCraft Technology Jun 2025 – Jul 2025

Cyber Security Intern

- Performed vulnerability assessments and penetration testing to identify security weaknesses and attack vectors.
- Applied attack-simulation techniques to evaluate system security posture under controlled conditions.

The Hacker's Meetup — Nagpur Chapter Nov 2025 – Present

Management Lead

- Lead end-to-end planning and execution of cybersecurity meetups as chapter head, coordinating speakers, logistics, and technical session delivery.

Phoenix Cybersecurity Aug 2025 – Present

Technical Team Member

- Assist in organizing cybersecurity workshops and national-level events, co-coordinating *Hacker's Heist* (Cyberpunk 3.0) and hosting *EncipherX 4.0* at SVPCET.

Education

St. Vincent Pallotti College of Engineering & Technology Aug 2024 – Present

B.Tech in Computer Science & Engineering (Cyber Security) — CGPA: 9.29 / 10 *Nagpur, India*

Certifications

IBM Cybersecurity Fundamentals | Security Operations Center in Practice | NPTEL Cyber Security and Privacy (Elite) | EC-Council Ethical Hacking

Achievements

- 1st Place — HackFusion 3.0 (National Hackathon)
- 2nd Place — Signal CTF, YCCE
- 15th Rank — ACN CTF, Amrita Vishwa Vidyapeetham
- 2nd Runner-Up — Gigagen, AI Verse 2.0