Ditikrushna Routray

SOC Analyst

ditikrushnaroutray@gmail.com Cuttack,Odisha ditikrushnaroutray.netlify.app
linkedin.com/in/ditikrushnaroutray github.com/ditikrushnaroutray

PROFILE

SOC Analyst with **3+ years** of freelance experience in **network forensics**, **log analysis**, **Linux hardening**, and **incident triage** through self-built labs. Skilled in **packet analysis**, **auth log investigation**, and **security automation** using **Python** and **Bash**. Strong foundation in **threat detection** and **blue team operations**.

SKILLS

Security Tools - Wireshark - Nmap - Hydra - Fail2Ban
Operating Systems - Linux Mint - Ubuntu - Kali Linux - Windows Security Basics
Scripting & Development - Python - Bash - Git - GitHub - C++
Networking - TCP/IP - DNS - HTTP/HTTPS - SSH - DHCP
Security Concepts - Incident Response - IOC Analysis - MITRE ATT&CK
Authentication Security - File Integrity Monitoring

PROJECTS

Project Nighthawk-SSH | SSH Attack Detection & Hardening Lab 04/2026 – 04/2026
Executed **500+ SSH login attempts** using **Hydra** against Ubuntu 24.04 test VM in isolated lab- Investigated **50+ failed authentication events** in `/var/log/auth.log` using source IP and timeline analysis- Hardened SSH access using **ED25519 key-based authentication**- Configured **Fail2Ban + iptables** to automatically block repeated brute-force attempts- Documented **attack path, indicators, and remediation process**

CyberDefenders HawkEye Lab | Malware Traffic Investigation 04/2026 – 04/2026
Analyzed **4,000+ packets** involving malware infection and exfiltration traffic
Identified compromised Windows host using **MAC address** and **DHCP evidence**
Extracted malicious executable from **HTTP stream** for analysis
Generated **MD5 IOC hash** for malware identification
Decoded **Base64 SMTP credentials** to trace attacker communication
Reconstructed attacker exfiltration workflow and documented findings

SECURITY TOOL DEVELOPMENT 03/2026 – 03/2026
Sentinel-FIM | Linux File Integrity Monitor |
Built Python-based **file integrity monitor** using watchdog API
Monitored 100+ files/directories for changes and permission abuse
Generated timestamped alerts for suspicious tampering
Ironclad Relay | Secure Messaging Prototype |
Developed encrypted messaging prototype using Python and C++
Implemented **RSA-2048** identity verification
Added secure **deletion for temporary sensitive data**

CERTIFICATES

- Google CyberSecurity

EDUCATION

B.Sc. Computer Science | Utkal University | 2023 – 2026
Class 12 (Science) | ***CHSE Odisha*** | *2021 – 2023*