NIRAKARA MISHRA

Aspiring SOC Analyst | Cybersecurity Analyst

📍 Odisha, India | 📧 nirakaramishra.cse@gmail.com | 📞 +91-958-390-9109 | 🔗 Linkedin | 🌐 Portfolio

Professional Summary

Cybersecurity graduate with hands-on experience in security monitoring, threat detection, and vulnerability assessment. Developed practical security solutions including an AI-based Intrusion Detection and Prevention System and a Web Application Security Scanner aligned with OWASP Top 10. Skilled in network traffic analysis, Linux environments, SIEM fundamentals, and Python-based security automation. Seeking an entry-level SOC Analyst or Cybersecurity Analyst role to contribute to threat monitoring, incident investigation, and security operations.

Key Security Tools

- Wireshark
- Splunk, QRadar (Basic SIEM Monitoring)
- Nmap
- Nessus
- Burp Suite
- CyberChef
- Metasploit

Technical Skills

Security Operations & Analysis

- Security Monitoring
- Alert Analysis & Investigation
- Incident Response Lifecycle
- Log Analysis
- Threat Detection

Networking

- TCP/IP
- Firewalls
- VPNs
- Routing & Switching
- Wireless Security Fundamentals

Operating Systems

- Linux (Kali Linux, Ubuntu)
- Windows Security Fundamentals

Programming & Automation

- Python
- Bash
- SQL

Security Frameworks & Knowledge

- MITRE ATT&CK Framework
- OWASP Top 10
- NIST Cybersecurity Framework

Virtualization & Platforms

- VirtualBox
- Docker
- GitHub

SOC Analyst Skills

- Alert triage and investigation
- Network traffic analysis using packet inspection
- Log monitoring and security event analysis
- Threat detection and incident documentation
- Basic SIEM monitoring and log correlation

Projects

Advanced Intrusion Detection and Prevention System (AI/ML)

- Developed a Flask-based IDS using a machine learning model trained on the NSL-KDD dataset to classify malicious network traffic.
- Implemented centralized logging with IP address and timestamp to simulate SOC-style incident records.
- Built real-time dashboards for monitoring detected attacks and analyzing threat patterns.
- Added filtering and Excel export functionality to support incident reporting and analysis.

Technologies: Python, Flask, Pandas, Scikit-learn, Matplotlib

Advanced Web Application Security Scanner

- Developed a Python-based vulnerability scanner capable of detecting common OWASP Top 10 vulnerabilities including SQL Injection and Cross-Site Scripting (XSS).
- Automated vulnerability detection and generated structured scan reports.
- Implemented scan history tracking and reporting dashboards for security auditing.

Technologies: Python, Flask, Pandas, Nmap, BeautifulSoup

IP Allowlist Security Automation

- Developed a Python-based automation tool to manage and enforce IP allowlisting for secure system access.
- Implemented logic to dynamically update allowlists and restrict unauthorized IP addresses.
- Simulated real-world access control scenarios to enhance system security.
- Automated monitoring and filtering of IP addresses to prevent unauthorized access attempts.

Technologies: Python, Networking Concepts

Certifications

- **Google Cybersecurity** Professional Certificate
- **IBM Cybersecurity Analyst** Professional Certificate
- Cyber Threat Management — Cisco Networking Academy
- Network Defense — Cisco Networking Academy
- Advent of Cyber 2025 — TryHackMe

Education

Bachelor of Technology (B.Tech) — **Computer Science & Engineering**

Biju Patnaik University of Technology (BPUT), Odisha — Graduation: 2025

Security Lab Experience

- Completed **TryHackMe's 24-day Advent of Cyber** challenge featuring realistic Blue Team and SOC investigation scenarios focused on threat detection, incident analysis, and defensive security
- Practiced attack detection, privilege escalation, and vulnerability exploitation using **TryHackMe security labs**
- Performed vulnerability scanning and enumeration exercises in controlled lab environments
- Analyzed network packet captures using Wireshark to identify suspicious activity
- Conducted web security testing aligned with OWASP Top 10
- Performed log monitoring and basic security event analysis using Splunk in lab environments