RANBIR MISHRA

Cybersecurity Analyst | SOC Analyst | SIEM & Threat Detection | Vulnerability Management (VAPT)

Jajpur, Odisha, India | +91-7205873191 | ranbirmishra2004@gmail.com |
LinkedIn: linkedin.com/in/ranbir-mishra-b5794a294 **| GitHub:** github.com/ranbirmishra2004

Portfolio: ranbirmishra2004.github.io

PROFESSIONAL SUMMARY

Entry-Level SOC & Cybersecurity Analyst | MCA Graduate with hands-on experience in SIEM monitoring, security log analysis, threat detection, and incident triage. Proficient in Splunk Enterprise and SPL for analyzing and correlating Windows security telemetry, including Event IDs 4624, 4625, and 4740, along with PowerShell and Sysmon logs to identify suspicious authentication and credential-abuse activity. Experienced in network traffic analysis with Wireshark and Nmap, vulnerability assessment using Burp Suite and Nessus, and web security testing aligned with the OWASP Top 10. Skilled in Linux administration, Bash scripting, TCP/IP networking, IoC investigation, MITRE ATT&CK mapping, and security documentation, with practical exposure to EDR-based threat detection and incident response using LimaCharlie.

TECHNICAL SKILLS

SIEM & SOC OPERATIONS: Splunk Enterprise, SPL, Universal Forwarder, Log Ingestion & Centralized Logging, Security Monitoring, Alert Triage, Threat Detection, Incident Investigation, Windows Event Log Analysis (4624, 4625, 4672, 4740), Sysmon, PowerShell Logging

THREAT DETECTION & INCIDENT RESPONSE: MITRE ATT&CK, NIST Incident Response Lifecycle, Cyber Kill Chain, IoC Identification & Analysis, Incident Triage, Root Cause Analysis, Evidence Collection, Threat Investigation, Incident Documentation, Detection Engineering

VULNERABILITY & WEB SECURITY: VAPT, OWASP Top 10, SQL Injection, XSS, Command Injection, Broken Access Control, API Security Testing, Vulnerability Validation, Remediation Tracking, Burp Suite, Nessus, OpenVAS, OWASP ZAP, Nikto

NETWORK SECURITY & ANALYSIS: TCP/IP, DNS, SSH, Network Traffic Analysis, Packet Analysis, Wireshark, Nmap, Port Scanning & Service Enumeration, Firewall Fundamentals, Netcat, Metasploit

EDR & ENDPOINT SECURITY: LimaCharlie EDR, Windows Endpoint Monitoring, Endpoint Telemetry Analysis, Process & Command-Line Analysis, PowerShell Monitoring, Detection Rules, Process Tree Investigation, MITRE ATT&CK Mapping

LINUX & WINDOWS ADMINISTRATION: Kali Linux, Ubuntu, Windows 10/11/Server, Linux CLI, User & Permission Management, chmod, chown, sudoers, Process Management, ps, top, systemctl, journalctl, Syslog, Cron

SCRIPTING & DEVELOPMENT: Python, Bash Scripting, SQL, MySQL, MongoDB, Git, GitHub, VS Code

EXPERIENCE

Cybersecurity & SOC Operations Trainee | Self-Directed Security Operations Lab
Practical SOC Monitoring, Threat Detection & Incident Response | 3 Months

- Monitored Windows and Linux security logs, analyzing authentication events, process activity, and network traffic to identify suspicious behavior.
- Performed Tier-1 SOC alert triage, IOC investigation, and threat analysis using Splunk, Windows Event Logs, Sysmon, and MITRE ATT&CK.
- Conducted network analysis and vulnerability assessments using Wireshark, Nmap, Nessus, Burp Suite, and OWASP ZAP.
- Investigated Linux security events and documented incident findings, evidence, threat analysis, and remediation recommendations using Bash, journalctl, and systemctl.

PROJECTS

PROJECTS

1. SIEM-Based SOC Monitoring, Threat Detection & Incident Investigation

Technologies: Splunk Enterprise, Universal Forwarder, SPL, Windows Event Logs, Sysmon, Ubuntu

- Built a centralized SOC lab using Splunk Universal Forwarder to collect and analyze Windows Security, System, and PowerShell logs.
- Developed SPL queries and detection searches for suspicious authentication activity, brute-force attempts, and account lockouts using Windows Event IDs 4624, 4625, 4648, 4672, and 4740.
- Created security dashboards and threshold-based alerts, performing incident investigation, event correlation, and evidence documentation.

2. Windows EDR Threat Detection & Incident Response Using LimaCharlie

Technologies: LimaCharlie EDR, Windows, MITRE ATT&CK, PowerShell

- Developed a Windows endpoint monitoring lab using LimaCharlie to detect suspicious process execution, PowerShell activity, scheduled tasks, and network behavior.
- Created custom detection rules and investigated endpoint telemetry, process trees, and suspicious activities.
- Mapped detected behaviors to MITRE ATT&CK and documented alert triage, investigation, response, and reporting workflows.

3. AI-Assisted SOC Analyst Platform – Automated Log Analysis & Incident Investigation

Technologies: Python, Flask, SQLite, Ollama, Llama 3.2, REST API

- Developed a Flask-based SOC platform to analyze uploaded authentication logs and identify suspicious login patterns and brute-force activity.
- Implemented IOC extraction, rule-based threat classification, MITRE ATT&CK mapping, and AI-assisted incident analysis using Ollama (Llama 3.2).
- Integrated incident management, SQLite storage, and downloadable investigation reports to support security analysis and documentation.

4. Network Security Monitoring, Packet Forensics & Traffic Analysis Lab

Technologies: Wireshark, Nmap, hping3, TCP/IP, Kali Linux

- Performed network reconnaissance, service enumeration, port scanning, and OS fingerprinting using Nmap.
- Analyzed TCP/IP traffic using Wireshark to investigate suspicious connections, handshake anomalies, and plaintext communication.
- Simulated abnormal packet traffic using hping3 and documented network findings, potential indicators of compromise, and investigation results.

5. Web Application Vulnerability Assessment & Mitigation (DVWA)

Technologies: Burp Suite, Nessus, OWASP ZAP, Nikto, OpenVAS, Kali Linux

- Conducted black-box and gray-box vulnerability assessments against DVWA, testing SQL Injection, XSS, OS Command Injection, and Broken Access Control.
- Used Burp Suite and automated vulnerability scanners to identify, validate, and investigate web application security weaknesses.
- Prepared VAPT reports documenting proof-of-concept findings, CVSS severity ratings, false-positive validation, and remediation recommendations.

EDUCATION

Master of Computer Applications (MCA) **2024–2026**
Dr. Harisingh Gour Central University, Sagar, Madhya Pradesh | **8.67 CGPA**

Bachelor of Science in Computer Science **2021–2024**
Utkal University, Bhubaneswar, Odisha | **81.72% | 8.4 CGPA**

Higher Secondary Education (+2 Science) **2019–2021**
Fakir Mohan Higher Secondary School, Balasore, Odisha | **85%**

CERTIFICATIONS & TRAINING

- **Google Cybersecurity Professional Certificate (Version 2)** — Google, Coursera (9 Courses Completed) | October 2026
- **Ethical Hacker** — Cisco Networking Academy
- **Introduction to Cybersecurity** — Cisco Networking Academy
- **Cybersecurity Fundamentals** — IBM SkillsBuild
- **Cybersecurity Analyst Job Simulation** — Deloitte, Forage

ACHIEVEMENT

- **Selected for IDEATHON – Smart India Hackathon 2025 (Internal Round)**; collaborated with a cross-functional team to develop and present the **"Discover Delight"** project.
- **TryHackMe — Top 4% Global Ranking:** Demonstrated hands-on cybersecurity skills through practical labs covering **SOC Operations, Threat Detection, Network Security, Linux, Web Security, and Incident Response**.

LANGUAGES

English: Proficient | **Hindi:** Fluent | **Odia:** Native