

ANKESH KUMAR YADAV

Pune, Maharashtra, India

+91-9905455312

ankesh.yadav0700@gmail.com

LinkedIn

GitHub

Portfolio



Professional Summary

Cybersecurity-focused Computer Engineering Graduate with hands-on experience in SIEM, log analysis, and endpoint monitoring. Skilled in alert triage and basic incident response, with knowledge of malware, phishing, and ransomware. Familiar with SOC operations, MITRE ATT&CK, and Windows/Linux. Seeking an entry-level Cybersecurity role.

Education

B.Tech – Computer Engineering

2022 – 2026

Pimpri Chinchwad College of Engineering, Pune

Cybersecurity Skills

- SIEM (Splunk Basics), Log Analysis, Event Correlation, Alert Triage
- Incident Response (Basics), Threat Detection, Threat Intelligence
- Malware Analysis (Basics), Phishing Analysis, Ransomware Concepts
- MITRE ATT&CK Framework (Basics), OWASP Top 10
- Vulnerability Assessment and Basic Risk Analysis
- Network Security Monitoring, Endpoint Security (Windows Defender Basics)
- TCP/IP, DNS, HTTP/HTTPS Protocol Analysis, IP Routing and Subnetting

Security Tools

- Splunk (Basics)
- Wireshark
- Nmap
- Kali Linux

Cybersecurity Projects

SIEM Log Analysis and Threat Detection (Splunk)

- Monitored and analyzed security logs to detect suspicious activities and anti-malware alerts
- Performed initial alert triage to identify false positives and potential threats
- Created dashboards and alerts for real-time security monitoring and reporting
- Identified brute-force attacks and unauthorized access attempts through log correlation

Network Traffic Analysis (Wireshark)

- Captured and analyzed network packets to detect anomalies and malicious traffic patterns
- Investigated DNS and HTTP traffic to detect indicators of compromise (IOCs)
- Identified suspicious connections and abnormal behavior

Network Design and Routing Simulation (Cisco Packet Tracer)

- Designed and simulated network topologies using Cisco Packet Tracer
- Configured IP addressing, subnetting, and routing protocols (static and dynamic routing)
- Implemented network segmentation and basic security controls (ACL concepts)

Certifications

-  Certified SOC Analyst (CSA) – EC-Council
- Cyber Security: SOC and SIEM (Splunk) for Beginners – Udemy
- Master SIEM, Log Analysis, Threat Intelligence & Incident Response – Udemy
- CCNA Training – WebAsha Technologies, Pune
- NPTEL Ethical Hacking – Elite

Additional Skills

- Linux (Ubuntu, Kali Linux), Windows
- Basic System Administration
- Security Monitoring and Troubleshooting