Divakar K

divakar.k2023@gmail.com | +91 93420 06729

SUMMARY

SOC and SecOps-focused cybersecurity engineer with hands-on experience detecting endpoint and network-based attacks including suspicious PowerShell execution, brute-force authentication attempts, and web application attacks using Sysmon, SIEM, and log correlation techniques.

EXPERIENCE

Internship
Aug 2025 - Sep 2025 | Elevate Labs

Conducted penetration testing and vulnerability assessments on web and mobile applications using OWASP Top 10 methodologies, identifying critical flaws including XSS, SQL injection, and authentication bypass vulnerabilities.

Applied networking and cybersecurity fundamentals in lab-based tasks, including network security monitoring, incident simulation, and building real-world security projects to demonstrate practical threat detection and mitigation skills.

Performed vulnerability scanning and service enumeration with Nmap and Burp Suite, followed by post-remediation validation to ensure security controls were effectively patched and critical vulnerabilities eliminated.

PROJECTS

WINDOWS SYSMON DETECTION LAB | SOC PROJECT

2025 -- 2026 | Self Project

Built a Windows Sysmon-based detection lab to identify suspicious process creation, PowerShell abuse, registry persistence, and unauthorized network connections, mapping detections to MITRE ATT&CK techniques.

GitHub: WINDOWS ENDPOINT MONITORING AND DETECTION LAB

TOR GUARD NODE PREDICTOR | NETWORK FORENSICS PROJECT

2025 -- 2026 | Team Project

Built a machine learning–based system to predict Tor guard nodes using synthetic Tor traffic data by analyzing exit node IP behavior for network forensic analysis.

GitHub: TOR-DEANONYMIZATION-FORENSICS-SYSTEM

SQL INJECTION DETECTION | WEB SECURITY PROJECT

2025 -- 2026 | Personal Project

Developed a SQL Injection detection lab capable of identifying malicious query patterns, logging attack payloads in real time, and differentiating between vulnerable and secure database interactions for forensic analysis.

GitHub: SQL-INJECTION-DETECTION

EDUCATION

RAJALAKSHMI INSTITUTE OF TECHNOLOGY

Bachelor of Computer and Communication Engineering
Expected: Current | Chennai - 600010

SKILLS

PROGRAMMING

Python • Java • MySQL

SECURITY - TOOLS

Nmap • Burp Suite • Metasploit Framework • Wireshark • Splunk • OWASP ZAP • Gobuster • Hydra • Tenable Nessus • Git/GitHub • Zeek • ELK Stack

PLATFORMS | OS

Windows • Kali Linux • Docker

SECURITY CAPABILITIES

Endpoint attack detection using Sysmon telemetry.
Suspicious PowerShell activity detection and analysis.
Brute-force authentication attack detection.
Web application attack detection (SQL Injection, XSS)
SIEM-based log correlation and alert investigation.
MITRE ATT&CK-aligned threat analysis.

CERTIFICATIONS

CCEP – Red Team Leader

AWS Cloud Certification

AWS Security Encryption

Cisco Cybersecurity Essentials

GRC | Mindset, Methods, Skills

ISO/IEC 27001:2022 | Information Security Associate

LINKS

Github: **Divakar-K**
LinkedIn: **Divakar-K**
Portfolio: **Divakar-K-Portfolio**