MUTHU KUMAR S

SOC Analyst | VAPT | Security Analyst
Bengaluru, Karnataka | +91 7548822001 | muthukumars1720@gmail.com | LinkedIn

PROFESSIONAL SUMMARY

Certified Ethical Hacker (CEH) and Cyber Security graduate with strong hands-on experience across **SOC operations, vulnerability assessment, and penetration testing**. Proven ability to monitor and analyze security events, perform **alert triage, log analysis, and incident investigation** using **Splunk and IBM QRadar**. Experienced in identifying, exploiting, and remediating **network and web application vulnerabilities** aligned with **OWASP Top 10 and MITRE ATT&CK**. Demonstrated practical exposure through internships, live environments, and real-world security engagements, making a strong fit for **entry-level SOC, VAPT, or Security Analyst roles**.

CORE SKILLS

- **Security Operations:** SIEM, Splunk, Microsoft Sentinel, SOC Operations, Log Analysis, Incident Handling, EDR (Endpoint Detection & Response).
- **Networking & Protocols:** TCP/IP, DNS, DHCP, HTTP/HTTPS, SSL/TLS, VPN, Routing & Switching, VLANs, Packet Analysis.
- **Vulnerability & Threat Management:** Vulnerability Assessment, Nessus, Qualys, Threat Intelligence, OWASP Top 10, Nmap, Metasploit.
- **Systems & Scripting:** Linux (Ubuntu/Kali), Windows Administration, Active Directory, Bash, PowerShell, Python.
- **Tools & Utilities:** Wireshark, Burp Suite, Snort, IDS/IPS, Firewall Configuration, Zap, etc.
- **Frameworks & Compliance:** NIST Cybersecurity Framework, MITRE ATT&CK, ISO 27001, IAM (Identity & Access Management), GDPR, PCI-DSS.
- **Technical Support:** bubble.io, Process Management, Onboarding Process, Following SOP's.

PROFESSIONAL EXPERIENCE

Technical Support Engineer – Training – Accura FMS Nov 2025
- Completed paid technical training focused on IT support and operational processes.
- Provided technical support for bubble.io and Slack platforms.
- Performed sanity testing after updates to ensure application stability.
- Supported client, vendor, and employee onboarding processes.

Cybersecurity Analyst Intern – The Coding Cult Mar 2025 – Jun 2025
- Supported SOC operations on a live environment using Splunk.
- Performed continuous log monitoring, alert triage, and anomaly detection.
- Assisted in incident investigation, evidence collection, and remediation tracking.
- Prepared incident documentation and security reports for senior analysts.

Cybersecurity Professional Intern – Cartel Software (Hacker School) Feb 2024 – Sep 2024
- Conducted network and web application vulnerability assessments and penetration testing.
- Automated routine SOC tasks using Python and Bash scripts.
- Investigated phishing attacks, malware indicators, and suspected botnet activity.
- Assisted in firewall rule tuning, IDS alerts review, and threat mitigation planning.

EDUCATION

B. Tech – Computer Science and Business Systems
Dhanalakshmi Srinivasan College of Engineering, Coimbatore | 2024 | CGPA: 8.1

CERTIFICATIONS

- Certified Ethical Hacker (CEH) – EC-Council (2025)
- Advanced Diploma in Cyber Security – Win in Life Academy (2025)
- HSCCSP – Hacker School Certified Cyber Security Professional (2024)

PROJECTS

ReconnaissPro – Network Vulnerability Scanner
- Designed and developed a Python-based automated vulnerability scanner.
- Performed port scanning, service enumeration, and vulnerability identification.
- Mapped findings to CVEs with severity assessment using CVSS.
- Generated structured reports with actionable remediation guidance.
- Awarded Best Project at college technical expo.

Network & NFS Service Penetration Testing
- Performed end-to-end penetration testing covering reconnaissance, exploitation, and post-exploitation.
- Identified critical service misconfigurations and privilege escalation risks.
- Validated attack paths and documented business impact.
- Delivered remediation recommendations aligned with secure configuration best practices.

FTP Service & Unauthorized Access Security Assessment
- Assessed FTP and file-sharing services for unauthorized access risks.
- Identified critical access control weaknesses and insecure file permissions.
- Validated exploitation scenarios in a controlled lab environment.
- Recommended hardening, monitoring, and patching strategies.

Web Application & Privilege Escalation Testing
- Conducted web application penetration testing covering directory traversal and file inclusion flaws.
- Achieved controlled remote code execution and user-level access.
- Performed local privilege escalation testing to assess system-level impact.
- Provided remediation guidance on secure coding and patch management.

Keylogger & Payload Generator (Lab Environment)
- Developed controlled forensic and payload simulation tools for Windows and Android.
- Used for behavioral analysis, attack simulation, and defensive detection testing.

Agro's Corner – Online Marketplace
- Developed a PHP-based online marketplace connecting farmers directly with buyers.
- Implemented backend logic, authentication flow, and user role management.
- Focused on secure data handling, optimized user flow, and application reliability.

Practical Exposure

- TryHackMe Labs: Firsthand threat detection and exploitation practice.
- VulnHub CTFs: Completed Beginner to Intermediate level challenges.
- Web Application Security: Extensive practice with PortSwigger Labs and OWASP Juice Shop.