Muthu Kumar S

Ph. No.: +91 7548822001
Mail ID: muthukumars1720@gmail.com
LinkedIn ID: Muthu Kumar S
Portfolio: https://muthu1720.github.io
GitHub: Muthu1720

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.

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.

Technical Skills

Networking & Infrastructure: TCP/IP | DNS | DHCP | HTTP/HTTPS | SSL/TLS | VPN | Subnetting | VLANs | Routing and Switching | Firewalls | Active Directory
Operating Systems & Scripting & Cloud: Linux | Windows Administration | Kali Linux | Bash Scripting | PowerShell | Python | AWS | Azure | Cloud Workload Security | RHEL (7/8/9) | SUSE 15, AIX
Security Operations (SOC): SIEM | Splunk | Microsoft Sentinel | Log Analysis | Wireshark | Packet Capture | Nmap | Intrusion Detection System (IDS) | Intrusion Prevention System (IPS) | Endpoint Detection and Response (EDR)
Threat & Vulnerability Management: Vulnerability Assessment | Nessus | Qualys | Threat Intelligence | OWASP Top 10 | Metasploit | Ethical Hacking
Governance, Risk & Compliance (GRC): NIST Framework | MITRE ATT&CK | ISO 27001 | GDPR | SOC2
Identity and Access Management (IAM): Incident Response | Incident Handling | Root Cause Analysis | Digital Forensics | Malware Analysis | Disaster Recovery

Notable Achievements

- Engineered a Python-based automated vulnerability scanner, ReconnaissPro, which performed port scanning, service enumeration, and vulnerability identification, earning Best Project at a college technical expo.
- Supported SOC operations on a live environment using Splunk, performing continuous log monitoring, alert triage, and anomaly detection to assist in incident investigation and remediation tracking.
- Conducted network and web application vulnerability assessments and penetration testing, automating routine SOC tasks using Python and Bash scripts to improve operational efficiency.

Education

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

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.

Network & NFS Service Penetration Testing
- Performed end-to-end penetration testing covering reconnaissance, 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.

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.