RAJA M

CYBER SECURITY ENGINEER

9176220725 | raja.madhavann@gmail.com | Chennai, India | rajam.vercel.app | M-Raja | Raja M

PROFESSIONAL SUMMARY

Detail-oriented Cyber Security Engineer with practical experience in ethical hacking, vulnerability assessment, and web application security. Possesses a strong foundation in Linux, networking, and cloud computing, transitioning from an Associate Technical Engineer role focused on Linux, cloud, and network operations. Proficient in penetration testing tools including Burp Suite, Nmap, Metasploit, and Wireshark. Seeking to leverage technical expertise to identify, analyze, and mitigate cybersecurity threats effectively.

EXPERIENCE

Associate Technical Engineer

Kyndryl India | August 2023–June 2025

- Managed and secured Linux servers, Mainframe systems, cloud infrastructure and enterprise network operations, ensuring 99.9% uptime and high availability.
- Automated operational workflows with Bash, Python, and JCL scripting, reducing manual tasks by 30% and improving efficiency across Linux and Mainframe environments.
- Troubleshot and optimized system and network performance, implementing security hardening, patch management, and access control reviews to strengthen the security posture.
- Supported incident response activities, identifying root causes of security events and implementing proactive remediation measures.
- Collaborated with cross-functional teams to align with security compliance frameworks , contributing to faster incident response and improved infrastructure resilience.

CERTIFICATIONS

- AWS Certified Cloud Practitioner (Ongoing)
- Ethical Hacking Essentials – EC-Council
- Cybersecurity & Ethical Hacking (Advanced) – Guvi
- Operating System Fundamentals (Windows & Linux) – Cybrary
- Network Fundamentals (TCP/IP, VPN, Wireshark, Nmap) – Cybrary
- Scripting & Programming Fundamentals (Bash, PowerShell, Python) – Cybrary
- (Artificial Intelligence) AI Fundamentals - Cybrary

TECHNICAL SKILLS

- **Programming /Scripting language :** Python , Java , Bash , PowerShell scripting
- **Pentesting:** Web Application , Network , Vulnerability Management, Social Engineering , Manual & Automated Security Testing , Exploit Development
- **Tools:** Burp Suite, SonarQube , Nessus/Qualys , OWASP ZAP , Jenkins/GitLab CI Kubernetes Security , Docker Security
- **OS:** Kali Linux , Windows, Ubuntu , Debian , Mac
- **Cloud:** AWS, Azure Cloud
- **Networking:** TCP/IP, VPNs , Firewalls ,Active Directory security , IDS/IPS
- **Security Standards:** OWASP Top 10 , MITRE ATT&CK, NIST , Cyber Kill Chain ISO 27001/27002

EDUCATION

Bachelor's in Computer Application

SRM Institute of Science and Technology | August 2020 - March 2023

- CGPA: 8.71
- Proficient in Python , Web Technology , and DBMS.
- Strong understanding of Cyber security , Computer Networks, Cloud Computing , and AI .
- Passionate about problem-solving and practical applications of technology.

PROJECTS

WebShield Scanner – Web Security Testing Platform

Python | Node.js | FAST API | OWASP ZAP | Nmap | GitHub Actions

- Built and deployed a web-based vulnerability scanner capable of performing OWASP Top 10 testing | SSL/TLS certificate validation | HTTP security header analysis | server fingerprinting, enhancing web application security assessment.
- Automated deep scans using OWASP ZAP | Nmap, enabling detection of common vulnerabilities like XSS | SQL Injection | CSRF | directory traversal, and generated structured security reports (HTML | PDF | DOCX) with remediation steps.
- Developed secure REST endpoints for scan initiation | scan history retrieval | report export, allowing seamless integration with CI/CD pipelines and external security workflows.
- Implemented GitHub Actions workflows for automated builds | vulnerability scan execution | cloud deployment, ensuring continuous security testing and faster release cycles.
- **Live Demo :** webshield-demo.com

Network Vulnerability Scanner & Assessment – Security Automation Project

Python | Nmap Integration | Port Scanning | Vulnerability Assessment | Reporting

- Designed and developed a custom Python-based network vulnerability scanner for security assessments in a controlled lab environment.
- Implemented automated host discovery, port scanning, and service enumeration using Python sockets and Nmap integration.
- Built custom vulnerability checks to detect misconfigurations, outdated services, and weak protocols across scanned systems.
- Generated automated security reports summarizing open ports, identified services, and potential security issues.
- Tested tool extensively in VirtualBox/VMware lab networks (Kali Linux, Windows, Metasploitable) to simulate real-world attack surfaces.
- Strengthened skills in penetration testing, vulnerability management, and security reporting aligned with SOC/Red Team practices.
- Gained practical experience in ethical hacking workflows, combining open-source tools with custom scripting for network defense and offense.
- **GitHub :** cybersec-network-scanner

SecureAware – Cybersecurity Awareness & Phishing Simulation Platform

GoPhish | Python | Flask | HTML/CSS | SMTP/IMAP | SQLite

- Developed and deployed a phishing & awareness simulation platform for offensive phishing campaign testing, credential harvesting scenarios, and employee susceptibility measurement.
- Built real-time dashboards and reports to track campaign success rates, click-through rates, and credential submissions, supporting penetration testing deliverables.
- Automated phishing scenarios with customizable templates, landing pages, and email workflows to simulate real-world social engineering attacks for red team exercises.
- **Live Demo :** threatacademy.vercel.app