AKHIL RAJ

SECURITY ANALYST

Phone: +91 9207557099 **Location**: Kerala, India **Email**: akhilrj103@gmail.com

ABOUT ME

Cybersecurity professional with experience in penetration testing, vulnerability assessment, and network security. Skilled in threat detection, Security Information and Event Management (SIEM) using Splunk, Intrusion Detection/Prevention Systems (IDS/IPS), and ethical hacking. Focused on securing digital assets and mitigating cyber threats. Seeking a cybersecurity analyst position to apply expertise in network defense

EXPERIENCE

SECURITY ANALYST - Cybersquare

2024 JUN- PRESENT

- Conducted vulnerability assessments of web applications, networks, and systems.
- Performed penetration testing using Nmap, Burp Suite, Hydra, and SQLMap to evaluate system security.
- Investigated cybersecurity incidents, documented findings, and proposed mitigation strategies.
- Assisted in configuring and securing Linux and Windows systems to minimize attack surfaces.
- Created detailed technical reports outlining vulnerabilities, risk levels, and mitigation strategies.
- Provided security awareness training on phishing attacks, password security, and safe browsing.
- Stayed updated with the latest cybersecurity threats, attack techniques, and security tools.

TECHNICAL SKILLS

Network Security & Infrastructure

- Proficient in network scanning and troubleshooting using Wireshark, Nmap, Netstat, Ping, and Traceroute.
- Skilled in switching and routing concepts, including VLANs, STP, OSPF, BGP, and NAT.
- Strong understanding of network protocols – TCP/IP Model, OSI Model, TCP, UDP, and their security implications
- Hands-on experience in configuring and managing firewalls (Sophos) and VPNs (IPSec, SSL, OpenVPN)
- Knowledge of intrusion detection/prevention systems (IDS/IPS: Snort, Suricata) and firewall rule optimization
- Experience in network segmentation and secure architecture design to prevent lateral movement in attacks

Identity & Access Management (IAM)

- Experience with Active Directory (AD) for user management, authentication, and access control.
- Knowledge of Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and Least Privilege models.

SIEM & Log Analysis

- SIEM tools: Splunk; Splunk Search Processing Language (SPL) for log analysis and threat detection.
- Experienced in real-time monitoring, security event correlation, and incident response using SIEM solutions

Security Testing & Vulnerability Assessment

- Skilled in penetration testing using Burp Suite, OWASP ZAP, Nikto, and Metasploit.
- Experience with manual security testing for XSS, SQL Injection, authentication flaws, and OWASP Top 10 vulnerabilities.
- Proficient in vulnerability scanning tools like Nessus, OpenVAS, and Qualys for security assessments.
- Familiar with password auditing using John the Ripper, Hashcat, and Hydra.

System & Server Security

- Hands-on experience in securing Windows Server, Active Directory, and Linux (Ubuntu, Kali, Parrot OS).
- Skilled in hardening web servers (Apache, Nginx) against security threats

Programming & Cloud Security

- Basic knowledge of Python for scripting, automation, and security tool development.
- Familiar with cloud security concepts and basic configurations in AWS, Azure, and Google Cloud

Security Compliance & Risk Management

- Knowledge of ISO 27001, GDPR, NIST, PCI-DSS, and HIPAA compliance frameworks.
- Assisted in security audits, compliance checks, and risk assessments.
- Understanding of data protection laws & regulatory security requirements.

PROJECT: WEB APPLICATION SECURITY TESTING & VULNERABILITY ASSESSMENT

Description

Conducted a comprehensive security assessment of a web application to identify vulnerabilities and evaluate its security posture. Performed a structured security assessment to ensure compliance with security best practices through scanning, testing, and reporting

Tools Used

- Nmap – Network scanning and enumeration
- Burp Suite & OWASP ZAP – Web application security testing
- SQLMap – SQL Injection testing
- Nessus/OpenVAS – Vulnerability scanning
- Wireshark – Packet analysis
- Splunk – Log analysis and threat detection

Key Tasks

- Performed network and web application scanning to detect potential security flaws.
- Conducted manual security testing for XSS, SQL Injection, authentication bypass, and CSRF vulnerabilities.
- Used Nmap & Nessus to identify open ports, misconfigurations, and vulnerabilities.
- Analyzed HTTP requests & responses using Burp Suite & OWASP ZAP.
- Investigated logs and security alerts using Splunk to detect suspicious activities.
- Provided detailed vulnerability reports, risk levels, and recommended security fixes.

Outcome

- Identified and reported critical vulnerabilities that could be exploited by attackers.
- Helped improve security configurations of the application.
- Created a technical report outlining vulnerabilities, risk impact, and mitigation strategies.

EDUCATION

Bachelor of Commerce (B.Com), - 2017 - 2020 - University of Calicut
Higher Secondary Education Commerce - 2015 - 2017 - Chinmaya Vidyalaya
High School Education - 2015 - Chinmaya Vidyalaya

CERTIFICATIONS

- Cisco Certified Network Associate (CCNA)
- EC-Council Certified Ethical Hacking Essentials (EHE)
- Certified IT Infrastructure & Cyber SOC Analyst
- Splunk Core Certified User
- Network Defense Essentials (NDE) – EC-Council

SOFT SKILLS

- Time Management & Multitasking
- Analytical Thinking
- Communication Skills
- Attention to Detail
- Troubleshooting & Problem-Solving

LANGUAGES

- English
- Malayalam
- Hindi
- Tamil