SYED IRFAAN S J

Chennai, Tamil Nadu

✉ Syedirfaan643@gmail.com in www.linkedin.com/in/syedirfaan GitHub

PROFILE SUMMARY

Cybersecurity professional with hands-on experience in penetration testing, vulnerability analysis, and security automation. Skilled in web, network, cloud, and enterprise security including Google Workspace and Active Directory. Focused on improving organizational security posture through practical and scalable solutions.

EXPERIENCE

Research Security Intern – DigiAlert July 2025 – September 2025

- Conducted web application and network penetration testing using Burp Suite, Nmap, and Postman.
- Assisted in red team assessments, vulnerability analysis, and remediation validation.
- Developed Google Workspace security monitoring solution to analyze configurations and improve cloud security posture.

Cyber Security Specialist Intern – Intrainz Innovation May 2024 – July 2024

- Conducted vulnerability scans and assisted in penetration testing activities.
- Identified and reported security flaws in internal web applications and network endpoints, gained hands-on experience with Kali Linux, Burp Suite, and penetration testing tools.

PROJECTS

AI-Integrated Active Directory Security Monitoring and Response System

Technologies: Windows Server, Active Directory, Python, ML, LLM, Linux

- Built an Active Directory lab environment to simulate enterprise authentication, user behaviour, and security events. Collected and processed Windows security logs using Winlogbeat and Logstash for centralized analysis.
- Integrated an MCP server to orchestrate ML-based anomaly detection and LLM-assisted log analysis, enabling SOC-style investigation, alert triage, and automated response recommendations through a dashboard.

Google Workspace Security Automation Tool

Technologies: React, Node.js, Google Admin SDK, OAuth 2.0, Tailwind CSS

- Developed a centralized dashboard to monitor configurations, MFA compliance, phishing alerts, and email security settings across Google Workspace.
- Integrated Google Admin SDK and Gmail API to analyse user configurations and improve security visibility.

Honeypot Integrated with SIEM

Technologies: Cowrie, Splunk, Linux, Python

- Deployed Cowrie honeypot to capture attacker activity.
- Forwarded logs into Splunk SIEM for centralized monitoring and analysis.

TECHNICAL SKILLS

Security Tools: Nmap, Burp Suite, Postman, FFUF, Metasploit, Wireshark, DirBuster, Splunk.

Cloud & Enterprise: Google Workspace Security, Microsoft 365 Security, Active Directory, AWS & Azure Basics.

Operating Systems: Linux (Kali, Debian), Windows.

Programming: Python, Shell Scripting.

Domains: Vulnerability Assessment and Penetration Testing (VAPT), OWASP Top 10, SOC Operations, SIEM, Log Analysis, Incident Detection and Response (Basics), Networking Fundamentals.

EDUCATION

Bachelor of Technology in Cybersecurity 2022 – 2026 (Present)

B.S. Abdur Rahaman Crescent Institute of Science and Technology

CERTIFICATIONS

- Certified Penetration Tester – Red Team Hacker Academy
- Network Basics – Cisco Networking Academy