MOHAMMED ABDULRAHMAN

CYBERSECURITY ENGINEER

Riyadh, Saudi Arabia | +91 9908750289 | mr.mdabdulrahman@gmail.com | LinkedIn & GitHub Verified | Languages: English, Arabic, Urdu, Hindi

PROFESSIONAL SUMMARY

Cybersecurity Engineer based in Riyadh, Saudi Arabia, holding a Bachelor of Engineering in Computer Science and Engineering (Data Science). Hands-on technical background in network security architecture, vulnerability assessment and penetration testing (VAPT), security operations center (SOC) monitoring, and defensive automation. Experienced in building enterprise-grade security detection pipelines, designing isolated network lab topologies, conducting adversary simulation, and engineering automated vulnerability scanners.

TECHNICAL SKILLS & CORE COMPETENCIES

- **Security Domains:** Network Security, SIEM & Log Analysis, Vulnerability Assessment & Penetration Testing (VAPT), Cloud Security (AWS/Azure), Incident Response
- **Network & Defense:** TCP/IP Suite, OSI Model, Subnetting, Firewalls, VPNs, IDS/IPS (Suricata/Snort), Wireshark, Zeek, Nmap, Packet Analysis
- **SIEM & Operations:** Splunk Core Certified User, Microsoft Sentinel, Wazuh SIEM, Alert Triage, Log Correlation, Threat Hunting, MITRE ATT&CK; Framework
- **Offensive & Labs:** Burp Suite Professional, Metasploit, Nessus, SQLMap, Kali Linux, AD Security, Active Reconnaissance, OOB Callback Validation
- **Programming & Cloud:** Python (Advanced Automation, Scikit-learn), Bash, REST APIs, Git, Docker, AWS (IAM, VPC, CloudTrail), Microsoft Azure Fundamentals

PROFESSIONAL & INTERNSHIP EXPERIENCE

Cybersecurity & SOC Analyst Intern | Full Stack Academy (Aug 2025 – Nov 2025)

- Monitored live security telemetry and performed alert triage using Wazuh SIEM and Splunk across virtualized enterprise network environments.
- Investigated authentication anomalies, brute-force patterns, and malware staging; mapped threat techniques to MITRE ATT&CK; enterprise tactics.
- Conducted packet-level traffic inspection using Wireshark and Zeek to identify rogue DNS beacons, unencrypted credentials, and lateral movement.
- Authored structured incident triage documentation and remediation recommendations in accordance with standard operating procedures.

Python Developer Intern | Soulax Software Pvt. Ltd. (May 2025 – Aug 2025)

- Engineered scalable automation scripts and structured data ingestion pipelines using Python, Pandas, and asynchronous network libraries.
- Built statistical modeling scripts to profile anomalous operational data, optimizing throughput and parsing efficiency by 35%.

TECHNICAL SECURITY PROJECTS & EMPIRICAL LABS

Wazuh & Suricata Enterprise SIEM Lab [Wazuh, Suricata, Docker, Linux, MITRE ATT&CK;]

- Deployed and configured a multi-node SIEM and NIDS architecture in Docker; ingested host telemetry and raw network packets for continuous monitoring.
- Simulated adversary behaviors (port scans, Hydra brute-force, web attacks) and authored custom Wazuh detection rules with automated active response.

VulnScan Pro — Enterprise Security Scanner [Python, WAF Fingerprinting, OOB Validation, CVE Correlation]

- Engineered a production-ready vulnerability scanner implementing a 10-phase pipeline: port scanning, service enumeration, header audits, and CVE matching.
- Built an out-of-band DNS/HTTP callback listener via Interactsh and heuristic WAF fingerprinting across 11 major enterprise vendors to eliminate false positives.

EDUCATION & CERTIFICATIONS

B.E. in Computer Science & Engineering (Data Science) — First Class with Distinction | Lords Institute of Engineering & Technology, Osmania University (2021 – 2025)

Verified Credentials: Introduction to Cybersecurity (Cisco / NSDC Skill India, Oct 2025) • SOC Analysis Program (Full Stack Academy, Nov 2025) • Microsoft MCRA (2025) • Data Science with AI (Full Stack Academy, Feb 2025)
Active Preparation Tracks: CompTIA Security+ (SY0-701, Q1 2027) • AWS Certified Cloud Practitioner (CLF-C02, Q1 2027)