Muhammad Talha

Cybersecurity Practitioner | Vulnerability Assessment | Threat Analysis
+92 307 195 5559 | infosectalha@gmail.com | LinkedIn | GitHub | Portfolio: infosectalha.github.io

Education

NUML University Faisalabad, Pakistan
Bachelor of Business Administration (BBA) *In Progress*

- Elected Class Representative (CR), demonstrating leadership and advocacy skills.
- Focusing on strategic planning and organizational leadership relevant to GRC and Project Management.

Experience

SOC Analyst Intern Remote
Cyborts *1 Month*

- Deployed and configured **Wazuh SIEM** manager and agents across Windows and Ubuntu endpoints.
- Implemented File Integrity Monitoring (FIM) and configured **Snort IDS** for network traffic analysis.
- Simulated brute-force (Hydra) and malware payload attacks (Metasploit) to validate detection rules.
- performed threat intelligence correlation using the **VirusTotal API** within the Wazuh dashboard.
- Authored weekly technical reports documenting incident analysis, logs, and remediation steps.

Associate Project Manager Intern Remote
Excelerate *1 Month*

- Managed full project lifecycle for a virtual team, overseeing task delegation and progress tracking.
- Recruited and onboarded team members, ensuring alignment with strategic project goals.
- Applied agile methodologies to coordinate deliverables in a remote environment.

Receptionist Intern Faisalabad, Pakistan
American Lyceum School *1 Month*

- Managed multi-line communication and front-facing inquiries in a fast-paced environment.
- Streamlined office operations and maintained organizational records.

Security Projects

Mitre Att&ck Framework Analysis | *Threat Modeling, SIEM, EDR*

- Executed a simulation project mapping TTPs for 3 distinct organizational case studies.
- Mapped attacker paths from Initial Access to Impact using Mitre IDs.
- Defined specific detection rules and mitigation strategies using SIEM and EDR concepts.

Web App Vulnerability Assessment (DVWA & bWAPP) | *Burp Suite, Owasp ZAP*

- Conducted structured assessments on vulnerable web apps in a Kali Linux lab.
- Exploited OWASP Top 10 flaws including SQL Injection, XSS, and OS Command Injection.
- Documented findings with severity ratings, PoC screenshots, and remediation guidance.

Cryptography & Secret Retrieval Lab | *Docker, OpenSSL, Linux*

- Solved crypto-analysis challenges involving Base64, XOR, RSA keys, and AES-256-CBC decryption.
- Extracted sensitive data from Docker containers to authorized decryption.

Network VAPT (Metasploitable) | *Nessus Essentials, CVE Analysis*

- Executed authenticated vulnerability scans using Nessus Essentials on a Metasploitable target.
- Analyzed critical vulnerabilities, correlated CVEs, and produced professional remediation reports.

Technical Skills

Defensive Security: Wazuh SIEM, Snort IDS/IPS, Log Analysis, Incident Response, Firewall Config, Phishing Analysis
Offensive Security: Nessus, Burp Suite, Metasploit, Nmap, OWASP ZAP, SQL Injection, XSS, Wireshark
Systems & Tools: Kali Linux, Docker, Git/GitHub, Python (Scripting), OpenSSL, Microsoft Azure
Soft Skills: Leadership, Project Management, Technical Writing, Critical Thinking, Team Collaboration

Certifications & Badges

Microsoft Certified: Azure Fundamentals (Microsoft)

(ISC)^2 Candidate – Official Member Status

Linux Fundamentals 100 (TCM Security)

Vulnerability Assessment & Pentesting (Udemy)

Critical Infrastructure Protection (ICIP) (OPSWAT)

SOC Analyst Internship Certificate (Cyborts)

Windows Password Cracking & Recovery (Udemy)

Certified Reproduction Tester (Test IO)

Fundamentals of Darkweb (SOCRadar)

Mastering Vulnerability Assessment (Tech Hierarchy)

Basics of Python (Uniathena)

Google Soft Skills Program (PAFLA)

Languages

English (Professional) | **German** (A1 - Basic)