Syed Muhammad Asad Abbas

Lahore, Pakistan · +92 322 3805454 · syedasadabbas.1815@gmail.com · linkedin.com/in/syedasadabbas1815

PROFILE

BSIT (Specialization in Cybersecurity) student with hands-on experience in malware analysis, network defense, digital forensics, and SOC automation. Skilled in building and securing systems within controlled lab environments. Seeking an entry-level SOC or Incident Response role to apply technical and analytical skills in real-world security operations.

EDUCATION

BSIT (Specialization in Cybersecurity) — Bahria University, Lahore · Expected 2026

CERTIFICATIONS

• Mastercard — Cybersecurity Job Simulation (Forage)

TECHNICAL SKILLS

Core Competencies: Network Security · Incident Response · Malware Analysis · Digital Forensics · Web Application Security (OWASP) · DDoS Mitigation · Threat Intelligence · OSINT

Tools & Platforms: Kali Linux · Wireshark · Burp Suite · Nmap · Suricata/Zeek · Splunk · ELK Stack · LimaCharlie · Metasploit (defensive)

Programming & Automation: Python · Bash · Linux Administration · Windows Security · SIEM Rule Writing · Log Correlation

HANDS-ON LAB EXPERIENCE (HOME LABS & ETHICAL FOCUS)

• Honeypot Deployment & Monitoring: Deployed and monitored a controlled honeypot to capture attacker telemetry, extract IP/time vectors, and automate log pipelines for analysis.

• Global Attack Mapping: Processed honeypot logs to geolocate attacker IPs and visualize patterns, prioritizing mitigation strategies based on temporal spikes.

• Digital Forensics: Performed forensic triage on captured artifacts, extracted indicators of compromise (IOCs), and compiled structured incident reports.

• Malware Analysis & Detection: Conducted sandboxed analysis of suspicious binaries, focusing on behavior profiling, IOC extraction, and detection rule creation.

• Network Monitoring & Packet Analysis: Used Wireshark, Suricata/Zeek, and tcpdump for anomaly detection and network event correlation.

• Web Security & Reconnaissance: Conducted OWASP-based testing (XSS, SQLi, auth flaws) and ethical reconnaissance to identify and report vulnerabilities.

PROJECTS

• SOC Automation Using LimaCharlie — Automated alert enrichment and triage workflows for simulated SOC operations; integrated endpoint telemetry and rule-based alerts for faster investigations.

• Phishing Detection Prototype — Built a detection model combining visual webpage analysis and DOM-based features to identify phishing attempts and generate real-time alerts.

STRENGTHS

Analytical problem-solver · Strong ethical discipline · Clear technical writing · Fast learner · Committed to continuous improvement and teamwork.

REFERENCES

Available upon request.