

RABYA HASSAN

Chasing Threats, Defending Networks · SOC Analyst in Training

Islamabad, Pakistan | hassanrabya90@gmail.com | linkedin.com/in/rabya-hassan | github.com/hassanrabya
hassanrabya.github.io | TryHackMe: 30+ Rooms

PROFESSIONAL SUMMARY

2nd-year Cybersecurity student (Air University, Kamra) with hands-on SOC experience in threat monitoring, incident triage, vulnerability assessment, and network intrusion detection. Currently completing an onsite SOC L1 internship at ZTBL (through Aug 2026), with a self-built home SOC lab and hands-on practice across OWASP Top 10 vulnerabilities, phishing/email investigation, and OSINT reconnaissance. Pursuing TryHackMe SOC Level 1 and ISC2 CC (expected Dec 2026). Seeking a SOC/Blue Team internship or entry-level analyst role.

EXPERIENCE

SOC L1 Intern (Onsite) | ZTBL (Zarai Taraqiati Bank Limited)

Jul 2026 – Aug 2026

- Monitor security events and alerts across SIEM/IDS platforms including Wazuh and Elastic, triaging daily alerts and escalating confirmed incidents per SOC playbooks.
- Document and track vulnerability findings and incidents in Jira through remediation, improving average ticket turnaround time.
- Collaborate with a blue team shift to investigate suspicious network activity and produce incident reports for stakeholders.

PROJECTS

SOC Home Lab | Wazuh · Elastic · VirtualBox

2025

- Built a virtualized SOC environment with HIDS detection pipelines, correlating Wazuh/Elastic alerts for end-to-end incident analysis.

Network Scanning & Traffic Analysis | Nmap · hping3 · Wireshark · TryHackMe

2025

- Performed network reconnaissance and simulated DoS traffic, analyzing traffic patterns and mapping findings to MITRE ATT&CK techniques.

Vulnerability Management & Cloud IAM | OpenVAS · Nessus · AWS IAM · Jira

2025

- Performed CVSS-based vulnerability assessments and implemented least-privilege AWS IAM policies with Jira-tracked remediation.

Email Investigation & Phishing Analysis | Email Headers · MXToolbox · PhishTool

2026

- Analyzed email headers, SPF/DKIM/DMARC records, and attachments to trace spoofed senders and identify phishing indicators.

Reconnaissance – Passive & Active | Nmap · theHarvester · Shodan · Maltego

2026

- Performed passive OSINT/WHOIS/DNS recon and active Nmap scanning to profile target infrastructure and document attack surface.

OWASP Top 10 – Hands-On Vulnerability Labs | DVWA · Juice Shop · Burp Suite

2026

- Practiced labs covering Cryptographic Failures, Insecure Design, Security Misconfiguration, SQL Injection, and XSS, with remediation write-ups.

TECHNICAL SKILLS

SIEM & Security Tools: Wazuh, Elastic, OpenVAS, Nessus, Burp Suite, Wireshark

Recon & OSINT: Nmap, theHarvester, Shodan, Maltego, WHOIS, Sublist3r, OSINT Framework

Scripting & Cloud: Python, Bash, AWS IAM, MITRE ATT&CK, Jira

CERTIFICATIONS

In Progress: TryHackMe SOC Level 1 (Expected Oct 2026) · ISC2 Certified in Cybersecurity (CC) (Expected Dec 2026)

EDUCATION

BS Cybersecurity | Air University, Kamra — Semester 4

2024 – 2028

- Coursework: Network Security, OS Security, Cryptography, Information Assurance, Computer Networks