HOOR UL EIN SOOMRO

231315@students.au.edu.pk | +923110040058
GitHub: hurrainjhl | LinkedIn: hoor-ul-ein-soomro

SUMMARY

Cybersecurity student with hands-on internship exposure in Red Teaming, SIEM dashboard development, and DLP solution training. Proficient in vulnerability assessment, threat analysis, and security automation using Python, Kali Linux, and Wazuh. Eager to apply technical expertise in penetration testing and incident response to strengthen organizational security posture.

EXPERIENCE

Red Team Intern **Jun 2025 – Aug 2025**
ITSOLERA PVT LTD (Remote)

- Conducted external and internal penetration testing on client web applications, identifying critical vulnerabilities (SQLi, XSS).
- Developed custom exploitation scripts using Python and Bash to automate reconnaissance and privilege escalation.
- Documented security findings with remediation steps, delivering technical reports to development teams.

Information Security Intern (DLP & Solution Team) **May 2025 – Jul 2025**
Trillium Information Security Systems (Hybrid)

- Successfully completed the CompTIA Security+ training certification track as part of the internship program.
- Learned and explored Forcepoint DLP operations, including data classification, policy enforcement, and endpoint monitoring configurations.

SIEM Intern **Jun 2024 – Sep 2024**
NCCS (Remote)

- Developed a working SIEM dashboard using Wazuh for real-time security event visualization, log correlation, and incident monitoring.
- Correlated firewall, endpoint, and network logs to identify malicious activity patterns and configured custom alerting rules.
- Designed interactive dashboards to present security metrics and operational trends for analysis.

EDUCATION

BS in Cybersecurity **2023 – 2027**
Air University, Islamabad, Pakistan

FSc (Pre-Engineering) **2020 – 2022**
Global Science College, Larkana, Pakistan

PROJECTS

- **PayloadGen** — Universal payload generator for XSS, SQL Injection, and Command Injection testing with WAF evasion techniques.
- **FEAS (Forensic Evidence Acquisition System)** — Digital forensic acquisition platform with SHA-256 hashing and chain-of-custody reporting.
- **Fizzup-recon-toolkit** — Advanced reconnaissance toolkit for passive & active scanning.
- **CortexCLI** — Cybersecurity command-line toolkit for automation and security-focused operations.
- **Distributed DNS System** — Implementation-focused project for understanding scalable DNS architectures.
- **ReconX & RedHawkx** — Custom reconnaissance CLI for passive/active information gathering and banner grabbing.
- **Voice Assistant Project** — Python-based voice assistant using speech recognition and TTS automation.
- **ThreadSleuth** — High-performance forensic tool using C++ multithreading to analyze disk images in parallel.
- **Zentryx** — PostgreSQL security middleware and SOC dashboard. Inspects SQL queries pre-execution, blocks dangerous commands, fingerprints approved query templates, and visualizes query risk context for analysts.
- **CipherGraph (CTI Knowledge Graph)** — Cyber Threat Intelligence platform that transforms unstructured OSINT reports into interactive knowledge graphs. Extracts threat actors, tools, and victims using LLMs (OpenRouter), resolves aliases, and maps relationships via Neo4j for visual investigation.

SKILLS

- **Security Domains:** Penetration Testing, Digital Forensics, Malware Analysis, Incident Response, Vulnerability Assessment, DLP (Forcepoint), SIEM (Wazuh).
- **Frameworks & Methodologies:** MITRE ATT&CK, NIST, Cyber Kill Chain.
- **Digital Forensics Tools:** Autopsy, FTK Imager, Wireshark, SHA-256 Hashing, Chain-of-Custody Procedures.
- **Penetration Testing & OS:** Kali Linux, Burp Suite, Nmap, Metasploit, John the Ripper, FlareVM, Remnux.
- **Development & Databases:** Python (Multi-threading, Sockets, Tkinter), Bash, C++, SQL, PostgreSQL, Neo4j.
- **Soft Skills:** Analytical Thinking, Technical Writing, Team Collaboration.

ACHIEVEMENTS

- FAST CyberFest Hackathon Participant — IoT & Cybersecurity Track (2024).
- 3rd Place — Scavenger Hunt Competition | Air University Cyber Skills Club (Team TrillBuzz).

CERTIFICATIONS

- Certified Threat Intelligence Analyst (Foundation Level) — arcX (May 2026)
- OSINT'10 Workshop & Capture The Flag (CTF) — Blistorm (Aug 2024)
- GitHub & Version Control Workshop — Dr. Coders (Aug 2024)
- Ethical Hacking MasterClass — Hacker Utd (Jul 2025)
- SOFTEC Cybersecurity Competition Participant (Feb 2024)
- CompTIA Security+ (Training Completed) — TISS Internship Program (2024)
- TISS DLP & SOC Security Training — Trillium Information Security Systems (2024)
- Tryna Bootcamp — 48-Hour AI Security Hackathon (2024)
- Digital Pakistan Cybersecurity Hackathon Participant (Oct–Nov 2023)
- ByteBotSec Capture The Flag (CTF) Participant (Sep 2025)

PROFESSIONAL INTERESTS

- Actively developing open-source security tools and conducting research in Red Teaming tradecraft, Digital Forensics, and Penetration Testing methodologies.