Ali Nawaz Malik

☎ +92 325 3969391 ✉ ali.malik9545@gmail.com in linkedin.com/in/ali-malik-76212a253

Profile

Cyber Security undergraduate specializing in vulnerability assessment, SIEM/XDR solutions, OSINT investigations, and network defense. Proficient with leading security tools, penetration testing techniques, and incident response workflows. Experienced in building and testing secure applications, configuring security infrastructure, and conducting digital forensics. Adept at translating technical findings into actionable recommendations, with a strong focus on improving organizational security posture. Seeking opportunities to apply hands-on expertise in SOC operations, threat detection, and security engineering.

Education

Air University Islamabad **2022 – 2026**
B.S. in Cyber Security *Islamabad, Pakistan*

Experience

Codistan **July 2025 – Oct 2025**
Cybersecurity Intern *OnSite / Islamabad*

- Performed web vulnerability scans (**Nikto**, **WPScan**, **ZAP**); documented missing headers, mixed content, outdated components.
- Built vulnerable Flask app to demonstrate **SQLi** and **XSS** for developer security training.
- Conducted OSINT on suspicious IPs/domains (**Shodan**, **Nmap**, **AbuseIPDB**), WHOIS/DNS, subdomain enum, spoofed-domain checks; compiled reports.
- Installed/evaluated **Wazuh**, **Security Onion** (Suricata, Zeek) for SOC2-aligned SIEM/XDR.
- Set up **pfSense** lab; simulated **SYN flood** attacks, wrote firewall rules, verified in Wireshark/pfSense logs.
- Ran **Nessus**/**Nmap** scans; analyzed findings; created remediation plan (protocol hardening, credentialed scans).
- Reverse-engineered Android/iOS apps (**MobSF**, **JADX**); found hardcoded secrets, risky logging, sensitive permissions.
- Investigated **OneDrive**/**AggregatorHost** deletion; paused sync, restored data, hardened endpoints, collected artefacts.

Yellow World Tech (UAE) **Jul 2024 – Aug 2024**
Cyber Security Intern *Remote*

- Assisted with log review, vulnerability checks, and documentation; gained exposure to SOC workflows.

Projects

PhishDetect – ML-based URL Classifier **Python, Flask, scikit-learn**

- Analyzes URL features to classify **Phishing vs Legitimate**; provides confidence score and reasons in a clean UI.

ILA-SOC – Intelligent Log Analysis & Incident Response (FYP) **Python**

- Lightweight, ML-powered log analysis platform with threat intel and dashboards for affordable SOC/SIEM use.

Skills

- **Security Tools:** Nikto, Nessus, ZAP, WPScan, Burp, Nmap, SQLMap
- **SOC/Monitoring:** Wazuh, Security Onion, Wireshark, pfSense, Linux tooling
- **OSINT/DFIR:** Shodan, AbuseIPDB, WHOIS/DNS, subdomain enum, Windows Event Viewer
- **Programming:** Python (Flask), Bash, SQLite, HTML/CSS/JS, Git

Certifications

Red Team Infra Dev (CRT-ID)
Cyberwarfare Labs | 68c6df8b806f169445f605d8

Red Team Analyst (CRTA)
Cyberwarfare Labs | 68bea692806f169445f45ed7

Junior Pen-Tester (PT1)
TryHackMe | 689cd19ed14e090d4155c915

Google Cybersecurity Proffesional Cert (v2).
Credential ID: A936C54ZGW7R

Web Dev (HTML/CSS/JS)
JHU | 62V6R24N317U

Cryptography
ISC2 | OVOIEWQBMFJO

Intro to Networking
NVIDIA | 9DEUZFA1WPW9