Muhammad Faisal Farooq

Penetration Tester

Islamabad, Pakistan | +92 313 5520012 | faisalfarooq17121@gmail.com
linkedin.com/in/muhammadfaisalfarooq | github.com/xor-1 | faisalfarooq.dev

Professional Summary

Penetration tester who assesses web applications, networks, and live production environments the way a real attacker would, then turns the findings into clear, actionable remediation guidance. Runs authorized assessments at PKCERT on government and public-sector systems, uncovering high- and critical-severity vulnerabilities and managing responsible disclosure from proof of concept to verified fix. Complemented by hands-on SOC experience with SIEM tools. Builds custom tooling in Python, C++, and C#, and designs Boot2Root machines for CTF competitions. Seeking to contribute offensive depth to penetration testing, security audit, and threat detection work, while growing further in Active Directory and enterprise security.

Technical Skills

Web Application Testing: Burp Suite, sqlmap, ffuf, Gobuster, Nuclei, Nikto, wfuzz

Network Testing & Exploitation: Nmap, Metasploit, Hydra, Netcat, Wireshark, Chisel

Password Attacks: Hashcat, John The Ripper, Hydra

Scripting & Tool Development: Python, Bash, C++, C#

Operating Systems & Lab Environments: Linux, Windows, macOS, Docker, VirtualBox, VMware, Git

Professional Experience

Penetration Testing Trainee *Jun 2026 – Present*
Pakistan Cyber Emergency Response Team (nCERT) *Islamabad, Pakistan*

- Test live production web applications under authorization, using manual techniques to find and exploit high- and critical-severity vulnerabilities, mostly leading to RCE, that automated scanners miss.
- Verify each finding with a working proof of concept, assess its real business impact, and coordinate responsible disclosure with the affected owners.
- Write clear technical reports with prioritized remediation steps so development teams can fix issues quickly and confidently.

Boot2Root Challenge Developer *Sep 2025 – Present*
SUDO FUZZERS *Islamabad, Pakistan*

- Design and build Boot2Root machines for university CTF competitions, from initial foothold through privilege escalation.
- Model each environment on realistic misconfigurations and attack chains so players practise the exploitation and post-exploitation steps used in real engagements.

SOC Analyst Intern *Jul 2025 – Sep 2025*
ITSOLERA PVT LTD *Pakistan*

- Deployed and configured a Wazuh SIEM for file integrity monitoring and centralized log analysis.
- Integrated pfSense firewall telemetry into Wazuh, improving visibility and threat detection coverage.
- Supported malware analysis, incident investigation, and day-to-day security monitoring.

Projects

Autonomous Web Penetration Testing Agent (Python, LangChain)

- Built an LLM-driven agent that plans and executes multi-step web attacks end to end: reconnaissance, payload generation, exploitation, and finding validation to filter false positives, benchmarked against enterprise-grade web targets.

Active Decoy – AD Deception & ITDR Framework (Python, Java)

- Engineered a framework that automatically deploys Active Directory honey-objects to detect and track lateral movement; **deployed in a live enterprise environment** for proactive threat detection.

Cyber Range

- Built an attack-and-defense platform where red teams exploit vulnerable machines while blue teams analyze the real telemetry those attacks generate.

Multi-Host Zero Trust Monitoring System (Multi-Agent AI)

- Designed a multi-agent system with endpoint agents that continuously assess OS security posture across multiple hosts and stream live data to dashboards.

Audit X Pro – Windows Compliance Auditor (C++)

- Wrote a native C++ auditor that checks Windows configurations against industry hardening best practices and generates compliance reports.

EDUCATION

Bachelor's Degree in Cyber Security — *2024 – 2028 (expected)*
National Cyber Security Academy, Air University — *Islamabad, Pakistan*

Intermediate in Computer Science (Higher Secondary) — *2022 – 2024*
Punjab Daanish School (Boys), Attock Campus — *Pakistan*

CERTIFICATIONS

Certified Network Security Practitioner (CNSP) – The SecOps Group — *2026*
Cisco Network Technician – Cisco — *2026*
Certified in Cybersecurity (CC) – ISC2 — *2025*
Google Cybersecurity Professional Certificate – Google — *2025*
ISO/IEC 27001:2022 Information Security Associate – SkillFront — *2025*

SECURITY LABS & TRAINING

TryHackMe — *Top 3% Globally*

- Ranked in the top 3% of users worldwide. Completed the Pre Security, Cyber Security 101, and Junior Penetration Tester paths.

PortSwigger Web Security Academy

- Exploited RCE-leading vulnerabilities in hands-on labs: OS command injection, server-side template injection (SSTI), unrestricted file upload, LFI/path traversal, SSRF, and SQL injection, plus access control and authentication bypass flaws.

Hack The Box

- Compromise vulnerable machines end to end, from enumeration and initial foothold to privilege escalation and post-exploitation.

AWARDS & ACHIEVEMENTS

- Zero-day vulnerability discovered in Grafana
- Best Intern of the Batch, PKCERT
- Cyber Patriot Award, PKCERT
- Letter of Appreciation for responsible disclosure, National Cyber Security Academy, Air University

REFERENCES

To be provided upon request.