MUHAMMAD ZUBAIR

Offensive Security / Red Team Professional

(+92) 320 9564941

Personal Portfolio Details
zubair@arcanixsecurity.com
bericontraster.github.io
linkedin.com/in/mhamd-zubair
medium.com/@bericontraster

CERTIFICATIONS

Offensive Security Certified Professional (OSCP) ↗	Oct 2024
Certified Penetration Testing Specialist (CPTS) ↗	Feb 2024

WORK EXPERIENCE

Information Security Engineer (Tranchulas) ↗

London, UK (Remote)

Dec 2024 - Present

- Conducted full-scope penetration tests (external, internal, web applications, APIs, Android, Active Directory, cloud, and AI-enabled systems), simulating real attacker workflows from initial access to post-exploitation.
- Conducted security assessments for high-impact and regulated environments, including healthcare systems and large-scale consumer applications, under strict confidentiality requirements.
- Identified and validated critical and high-risk vulnerabilities by chaining authentication, authorization, and configuration flaws to demonstrate realistic end-to-end compromise scenarios and attacker impact.
- Delivered enterprise-grade reports aligned with industry standards, translating technical findings into risk-prioritized remediation guidance for both engineering teams and non-technical stakeholders.
- Designed and led offensive security training programs aligned with standards published by NCSC, CREST, and APMG International, mentoring 50+ students globally and evaluating performance through final practical exams.
- Led administration and migration of security infrastructure across AWS and on-prem Proxmox environments, hosting vulnerable labs, VPNs, and training platforms; reduced operational costs by 20%+ while improving performance and administrative control.

IT Support Assistant (11ven Tech Yards)

Islamabad, PAK (Hybrid)

May 2023 - Aug 2024

- Independently handled and resolved a high volume of remote technical support issues, building strong system-level troubleshooting and root-cause analysis skills.
- Automated system administration tasks using PowerShell and batch scripting (log rotation, temp cleanup, directory management), reducing manual workload by 25%.
- Applied scripting and systems knowledge to develop a deeper understanding of Windows internals later leveraged in offensive security and post-exploitation workflows.
- Collaborated with technical teams to identify recurring issues, contributing to improved documentation and preventive security measures.

PROJECTS

Enterprise-Grade Offensive Security Courses

Designed and delivered two enterprise-grade offensive security training programs aligned with standards published by NCSC, CREST, and APMG International. Incorporated hands-on labs and final practical exams, awarding certifications to students upon successful completion.

Offensive Security CTF Development

Engineered multiple vulnerable lab environments used by clients and public communities, featuring realistic attack surfaces including Active Directory, privilege escalation, and web exploitation.

SKILLS

Operating Systems: Linux, Microsoft Windows (internals, privilege escalation, post-exploitation)
Offensive Security: Penetration Testing, Vulnerability Assessment, Security Architecture Review
Domains: Web Applications, APIs, Active Directory, Cloud & AI-enabled Applications
Scripting & Development: Python, PowerShell, Bash, JavaScript, C, C++ (secure coding, automation)
Analysis & Problem Solving: Threat analysis, exploitation logic, risk prioritization
Communication: Technical & executive reporting, client-facing communication
Security Mindset: Emerging threats, modern security controls, continuous learning
Governance, Risk & Compliance (GRC): ISO/IEC 27001 (ISMS concepts), risk assessment, control mapping, security controls, business impact awareness