MUHAMMAD ZUBAIR

Offensive Security / Red Team Professional

(+92) 320 9564941 — (Relocating to KSA, Riyadh)

Site: bericontraster.com
Mail: contact@bericontraster.com
LinkedIn: linkedin.com/in/mhamd-zubair
Blog: 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

- Co-developed a vishing (voice-phishing) platform using ElevenLabs, Twilio, and AI models to simulate realistic social engineering attacks and execute automated campaigns that enhanced client security awareness.
- Identified and exploited ~50 vulnerabilities across Web, Cloud, and Active Directory environments, strategically chaining flaws to demonstrate maximum real-world impact for enterprise clients in the healthcare and transportation sectors. I managed the end-to-end remediation process, providing technical support for patch implementation and performing rigorous post-remediation revalidations to ensure total risk closure.
- Authored high-fidelity security reports that prioritize vulnerabilities based on specific business infrastructure, providing clear, step-by-step remediation plans and immediate "Quick-Win" actions to neutralize critical risks.
- Developed two industry-standard offensive security courses comparable to PNPT, encompassing Web, Active Directory, and AI exploitation vectors. I architected the final practical examinations, managed global certification issuance, and personally trained over 50 students and corporate professionals on real-world adversary TTPs.
- Built and handled most of the development and security architecture of a large-scale backend application with admin and user dashboards to automate Essential Eight (ACSC) compliance for enterprise clients.
- Managed production-grade AWS environments with zero downtime while concurrently architecting a custom Proxmox infrastructure hosting ~20 vulnerable lab environments and proprietary VPN servers for advanced offensive training.

IT Support Assistant (11ven Tech Yards)

Islamabad, PAK (Hybrid)

May 2023 - Aug 2024

- Managed high-availability web services and databases with zero downtime, while hardening Linux environments for the secure deployment and administration of Nextcloud instances.
- Developed PowerShell and Python automation tools to resolve complex system-level issues, building a deep foundation in Windows internals and root-cause analysis currently used in post-exploitation workflows.
- Partnered with technical teams to identify recurring systemic vulnerabilities, contributing to improved documentation and the implementation of preventive security measures

PROJECTS

AI Prompt Security Gateway (Early Development)

Designing an application-layer security filter to prevent sensitive data (secrets, credentials, internal information) from being submitted to AI systems. Currently defining detection logic, policy controls, and safe-handling workflows with a focus on reducing data leakage risk in enterprise AI usage.

Web Vulnerability Scanner (In Progress)

Designing and building a web vulnerability scanner aimed at reducing attack surface and enabling teams to identify and fix security issues independently. Focused on clear, AI-generated reports that translate findings into actionable, business-relevant remediation guidance.

SKILLS

Offensive Security & Red Teaming: Full-scope Red Team Operations, Adversary Emulation (MITRE ATT&CK Framework), TIBER-EU-based threat-led testing, and Advanced Persistent Threat (APT) simulation.

Active Directory & Internal Exploitation: Expertise in advanced AD exploitation, including Kerberoasting, AS-REP roasting, DCSync attacks, and lateral movement within complex enterprise environments.

Infrastructure & Cloud Operations: Hands-on experience managing and hardening cloud and virtualized environments (AWS, Proxmox), including deployment and security of custom OpenVPN infrastructure for controlled remote access to complex, vulnerable lab environments.

GRC & Regulatory Alignment: Proficient in mapping technical vulnerabilities to NCA ECC/CSCC (KSA). Focused on risk-based control implementation and ISO/IEC 27001 standards for regulated industries.