

## CERTIFICATIONS

Offensive Security Certified Professional (OSCP) [↗](#)  
Certified Penetration Testing Specialist (CPTS) [↗](#)

Oct 2024  
Feb 2024

## WORK EXPERIENCE

### Information Security Engineer (Tranchulas) [↗](#)

London, UK (Remote)

Dec 2024 - Present

- Performed 30+ penetration tests, uncovering 80+ vulnerabilities across web, API, Android, AD, and external environments, and delivering enterprise-grade reports aligned with industry standards.
- Designed and delivered enterprise-grade offensive security programs aligned with standards published by NCSC, CREST, and APMG International. Trained and mentored 50+ students globally, with certifications awarded upon passing final practical exams.
- Developed 30+ custom vulnerable labs on Proxmox, designed to support complete attack-and-defense workflows.
- Migrated infrastructure from AWS to Proxmox, cutting cloud operating costs by 60%+ while improving system performance and administrative control.
- Owned large-scale projects and course development, reducing team workload and accelerating delivery timelines, directly increasing revenue by 20% through on-time project completion.

### IT Support Assistant (11ven Tech Yards)

Islamabad, PAK (Hybrid)

May 2023 - Aug 2024

- Delivered remote technical support with a 95%+ resolution rate, strengthening troubleshooting skills and developing a security-first approach across email, cloud storage, and enterprise software environments.
- Safeguarded sensitive client and business data through strict confidentiality and secure digital practices, laying the foundation for a career in security-focused operations.
- Developed PowerShell and batch scripts to automate system administration tasks (log rotation, temp file management, directory structuring), reducing manual workload by 30% and building practical skills later applied in offensive security scripting.
- Collaborated with technical teams to identify recurring issues, contributing to improved documentation, root-cause analysis, 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

- Extensive experience working with operating systems (Linux, Microsoft Windows)
- Experience with penetration testing, architecture assessments, and vulnerability assessments
- Strong analytical and problem-solving capabilities
- Desire to learn more, stay ahead
- Proficient in secure programming principles and languages (C, C++, Javascript, PowerShell, Bash, Python)
- Excellent written and verbal communication skills
- Advanced knowledge of emerging technology security solutions and trends