Cyber and Fraud Centre Scotland

Job Description

Job title: Penetration Tester

The Role

You will deliver high-quality, ethical penetration testing engagements aligned with CREST standards. A hands-on technical role with opportunities to grow and develop your skills as part of a social enterprise contributing to Scotland's wider cyber resilience ecosystem.

A hands-on technical role with opportunities to grow and develop your skills as part of a social enterprise contributing to Scotland's wider cyber resilience ecosystem.

Key Responsibilities

Deliver CREST-aligned penetration testing engagements, including:

- Infrastructure and network testing.
- Web and application testing.
- Cloud and hybrid environments.
- Execute tests in line with agreed methodologies and best practice.
- Produce clear, high-quality technical and executive-level reports.
- Communicate findings and risk in a clear, constructive manner to a range of stakeholders.
- Support remediation discussions and re-testing where required.
- Maintain accurate records and testing artefacts in line with governance and assurance requirements.
- Contribute to continuous improvement of tools, methodologies, and internal knowledge sharing.
- Stay informed about emerging cyber threats, fraud trends, and regulatory changes affecting organisations.
- Achieve and maintain CREST accreditation.

About You

You will be joining a caring and committed team with a strong sense of purpose.

It is essential that you have:

- 1-2 years of proven experience delivering penetration testing in professional or client-facing environments.
- Understanding of common vulnerabilities and attack techniques (e.g. OWASP Top 10, MITRE ATT&CK).
- Experience with industry-standard tools (e.g. Burp Suite, Nmap, Metasploit, Nessus or equivalents).
- Ability to write clear, high-quality technical reports.
- Strong ethical mindset and commitment to responsible disclosure.

Desirable:

- CREST penetration testing certifications, such as CPSA or CRT.
- Experience in cloud security testing (AWS, Azure, GCP).
- Knowledge of secure architecture or defensive controls.
- Additional certifications (e.g. OSCP, CHECK, CISSP, cloud security certs).

About Us

- Meaningful work with real-world impact across Scotland's cyber ecosystem.
- Flexible and hybrid working arrangements.
- Support for continued professional development and certification.
- A collaborative, mission-driven culture.
- Competitive salary and benefits package (commensurate with experience).
- Location: 19 Rutland Square, Edinburgh, with flexible/hybrid working options.
- Environment: Employee-first culture operating a 4-day work week.
- Impact: Direct contribution to the social enterprise's mission to reinvest funds into the Scottish cyber community.

You must have the right to work in the UK.

More Information

Send an up-to-date CV and cover letter setting out your suitability for the role to Kara.McLaughlin@cyberfraudcentre.com. Application deadline: 5pm Friday 11th September 2026.