26572 - Penetration Tester

Location: Braine L'Alleud, Belgium.

Period: 697 (start on 15 Oct. 2026)

Deadline: 16 Sep. 2026

Duties/Roles:

- Lead and/or be part of the Red/Blue Team during NATO military exercises;
- Provide Web, infrastructure and application level penetration testing;
- Provide security design reviews to ensure compliance with NATO policies and directives;
- Provide security consultancy and advice to projects, plans, and other entities;
- Build and sustain effective communications with different stakeholders; specifically, the NCIA Configuration Control Board, Security Accreditation Boards, NATO Security Accreditation Authorities, and NCI Agency organization units supporting accreditation processes.
- Brief at both executive and technical levels on security reports and testing outcome, including at flag officer level;
- In co-ordination with the Head of the Penetration testing Cell, ensure proactive collaboration and coordination with internal and external stakeholders.

Skills, Knowledge, Experience Required:

Mandatory:

- The candidate must have a currently active NATO SECRET security clearance
- Extensive knowledge and experience (more than 3 years) in web application penetration testing;
- Extensive knowledge and experience (more than 3 years) in IT infrastructure penetration testing;
- Extensive knowledge and experience (more than 3 years) in network security architecture design;
- Extensive knowledge and experience (more than 3 years) in assessing security vulnerabilities within OS, software, protocols & networks;
- Extensive knowledge and experience (more than 3 years) in researching and evaluating security products & technologies;

- Knowledge in system and network administration of UNIX and Windows systems;

- Extensive knowledge and experience (more than 3 years) in the use of penetration testing tools, techniques, and recognized testing methodologies;

- Scripting skills in at least one of the following: Perl, Python, Ruby, shell (bash, ksh, csh);

- Technical knowledge in system and network security, authentication and security protocols, cryptography, application security, as well as, malware infection techniques and protection technologies.

- Ability to evaluate risks and formulate mitigation plans;

- Proven ability to write clear and structured technical reports including executive summary, technical findings and remediation plan for several different audiences.

Required Level of Security Clearance:

NATO SECRET.