TIGERSCHEME™

Providing excellence in penetration testing

QSTM

1 day assessment

An intermediate qualification for penetration testing engineers, aimed at the CHECK Team Member level, and suitable for all those wishing to move into a recognised penetration testing position.

The assessment is based on a demonstration of both theoretical and practical skills, encompassing service delivery as well as technical knowledge.

The Tiger Scheme QSTM (Qualified Security Team Member) qualification is the intermediate qualification within the security assessment series, requiring both a practical and theoretical demonstration of security assessment skills.

The assessment comprises a two hour practical in which candidates are asked to achieve specific objectives on a dedicated test environment, which will be supplemented by a half hour viva exam, in which candidates will be asked to explain and discuss their methods, findings and recommendations. These components are backed up by a multiple-choice examination and a long question paper on networking and security theory. The assessment can be taken in isolation, although it is recommended that it be preceded by training available from Tiger Scheme's authorized training partners.

The assessment has been reviewed by CESG as the National Technical Authority in the UK, and has been accepted as meeting the technical requirements for a CHECK Team Member assault course. Candidates wishing to achieve eligibility for CHECK Team Member can opt to have their practical assessment overseen by a CHECK Team Leader. In all other respects, the assessment and standards are identical for all candidates and those not working for accredited CHECK companies are not eligible for CHECK Team Member status.

Objectives

To be successful, candidates will need to demonstrate a good understanding of:
- Information security in the corporate world
- Professionalism and communication skills, ethics and the law
- Network enumeration and network mapping
- Network device management and exploitation
- Service enumeration
- Service topology/dependency mapping
- Service management and exploitation
- Application enumeration and profiling
- Application and operating system management
- Application and operating system exploitation and manipulation

Key benefits

- Demonstrable theoretical knowledge of key security standards and issues
- Recognition of professional/ethical behaviour in the area of vulnerability testing
- Key communications skills and project management skills for vulnerability testing

Requirements

Candidates should possess knowledge of:
- IP, TCP, UDP and ICMP protocols, including IP-based routing and the TCP state chart
- Key network services including DNS
- How a TCP/IP network can be profiled and have its topology mapped
- How to configure and manage a network device
- How to subvert a network and bypass network based security mechanisms
- The role and function of service in a networked environment
- The techniques associated with service enumeration
- How critical service dependences within a network enabled environment can be enumerated and validated
- How services should be managed and can be manipulated and exploited
- How applications and operating systems should be configured and managed
- The ways in which applications and operating systems can be subverted

TIGERSCHEME™

For more information visit **www.TigerScheme.org**

Providing excellence in penetration testing