



2 day assessment

Certify your ability to plan, execute and summarize vulnerability testing and make appropriate recommendations.

Recommended for Tiger Scheme Qualified Testers with hands-on experience; those with significant practical experience in vulnerability/penetration testing.

SST

Those with considerable security testing experience and a detailed understanding can move to the higher level of certification, the Tiger Scheme Senior Tester qualification awarded by the Tiger Scheme Examining Body, The University of Glamorgan, by passing this advanced theoretical & practical assessment. Tiger Scheme SST has been recognised by CESG as technically equivalent to the CHECK Team Leader assault course.

The test consists of a multiple choice paper, a long question paper, a practical element and an interview, requiring the candidate to plan, execute and summarise a vulnerability assessment ("penetration test") on an example mixed Unix and Windows™ network, and make recommendations for eradication or mitigation of the vulnerabilities found.

Objectives

Please note that this is not a training course and no new material is taught. Candidates should already have successfully completed a course leading to the award of Tiger Scheme Qualified Security Team Member (QSTM) and have a number of years of hands-on experience, or should have significant practical experience in this field. The Tiger Scheme Senior Tester assessment is a challenging undertaking, demanding industry-leading abilities.

The example network used in the assessment may contain any or all of the following operating systems: Microsoft™ Windows 2000 with and without SP1, Windows 2003, Redhat™ 7.2, Microsoft NT SP3 and SP6, Windows XP SP2, Cisco™ 2801 and Cisco PIX 515E.

Key points

To complete the assessment successfully the candidate will need to:

- demonstrate a thorough understanding of the theory behind the tools and techniques used in vulnerability testing
- provide a detailed explanation and analysis of the results obtained and conclusions drawn
- perform a technical penetration test within the criteria set out in the SST Technical Standard
- identify and explain vulnerabilities including their limitations and default behaviour
- understand the mechanism for remote detection and validation of vulnerabilities
- explain the protection measures that could be implemented and assured
- understand how a penetration test is scoped via stakeholder involvement
- understand and explain protective network technologies and architectures
- detect and validate weaknesses/vulnerabilities within the following standard TCP/IP environments:
 - network TCP/IP data capture and analysis using standard network tools
 - network weaving via ARP spoofing and poisoning
 - TCP/UDP service identification and validation
 - port forwarding and port redirection
 - access control lists on network perimeter devices
 - network topology mapping
 - routing identification and verification
 - identification and exploitation of RIP and OSPF
 - information retrieval from DNS servers and understanding of the DNS record
 - DNS server identification and DNS poisoning

Course details continued on reverse >



For more information visit www.TigerScheme.org

Providing excellence in penetration testing

Tiger Scheme™ is a trademark of Tiger Scheme Ltd. This information may not be reproduced without written permission



SST

Course details continued:

Candidates will also be expected to demonstrate an appropriate level of knowledge and expertise in the following key areas:

- Detect and validate weaknesses/vulnerabilities with the following standard Windows/UNIX environments:
 - Password security and brute forcing
 - Windows trust relationships
 - NetBIOS information enumeration
 - Domain and site information
 - Sirectory services and active directories
 - LDAP and SNMP servers
 - Default installations of the SQL databases
 - Terminal services such as VNC
- Detect and validate weaknesses/vulnerabilities within the following standard services:
 - Common web servers, such as IIS and Apache
 - Web services such as SOAP and WSDL
 - Misconfigured servers such as FTP, Telnet and SSH
 - Samba shares and services
 - Insecure X servers
 - Mail services such as SMTP and POP
 - Understanding of the SNMP MIB structure
 - Understanding of the structure of LDAP
 - NFS servers and clients
 - SQL Injection and cross-site scripting
 - Information leakage via HTML
- Understand and carry out information retrieval and analysis from UNIX SNMP servers

Tiger Scheme is a not-for profit organisation working in co-operation with The University of Glamorgan to provide an independent, University recognised assessment of the technical, legal and ethical capabilities of penetration testers within the UK. Buyers of penetration testing are vocal of the shortage of certified skill in the UK, and the negative impact this has on project timescales and costs. Tiger Scheme bridges this gap between buyers and suppliers of assessment services. Whilst many UK based certification concentrate purely on commercial service providers, Tiger Scheme offers certification to both professional penetration testers and IT professionals working within internal IT teams. This allows organisations to have leading edge expertise within their own teams, offering greater flexibility and cost effectiveness.



For more information visit www.TigerScheme.org

Providing excellence in penetration testing