Tiger Scheme

QST/CTM Standard

Title	**Tiger Scheme Qualified Security Tester Team Member Standard**
Version	1.2
Status	Public Release
Date	21st June 2011
Author	Professor Andrew Blyth (Tiger Technical Panel)
Review Date	1st July 2012

Version	Date	Author	Changes and Comments
1.0	01/02/2010	Professor Andrew Blyth	DRAFT
1.1	10/04/2010	Professor Andrew Blyth	FINAL VERSION
1.2	21/06/2011	Professor Andrew Blyth	FINAL VERSION

Table of Contents

1. Introduction

1.1 Aims and Objectives

1.1.1 This document is intended to define the base-line technical standards for the TIGER Scheme *Qualified Security Tester Member* (QSTM) level. This level is technically equivalent to a CHECK Team Member

1.1.2 The Qualified Security Tester Member is expected to possess and have the ability to demonstrate a wide range of skills and knowledge associated with security testing and assessment.

1.1.3 The nature of the assessment for a Qualified Security Tester Member is that of an assault course whereby the candidate is expected to discuss numerous aspects of security testing and subsequently to demonstrate technical capability on specially designed and maintained assault course networks.

1.1.4 The objective of the assault course is to evaluate the candidate in an environment that mimics a typical real-world security-testing scenario as much as possible.

1.1.5 The areas of expertise that are to be assessed at the TIGER Qualified Security Tester Member level consist of three overall aspects categorised as follows:

- **Management, Ethics & Compliance:** Demonstration of knowledge and capability in areas such as legal knowledge, understanding customer requirements, the scoping of security assessments, the planning and management of engagements, risk management throughout engagements and the use of a suitable security testing platform.

- **Technical Expertise:** Demonstration of knowledge and capability in areas including design and architecture security assessments, security testing of infrastructure and applications, the classification of technical risk and the ability to provide coherent remediation recommendations for identified security vulnerabilities and exposures.

- **Deliverables**: Demonstration of capability in the preparation and presentation of security testing results to both non-technical and technical audiences. In both instances the results will be documented providing a summary of the issue, the impact and risk along with relevant recommendations

1.1.6 These aspects have been chosen in an attempt to ensure that the security testing requirements and concerns of industry are incorporated into the individual candidate evaluation process.

1.1.7 The assessment for a Tiger Qualified Security Tester Member consists of four parts:

- A multiple choice assessment (30 Minutes)
- A written examination (2 Hours)
- A practical assessment via an assault course (3 Hours)
- A viva (30 Minutes)

1.1.8 The Qualified Security Tester Member assault course is an assessment of technical skill and is designed to evaluate the candidate as a whole and their capabilities across the security-testing spectrum.

1.1.9 The pass marks for each element of the QSTM/CTM assessment is 60% and a successful candidate must pass all components of assessment.

1. The Standard

2.1 Understand Requirements

Demonstrate the ability to understand customer requirements and set customer expectations for a given security-testing scenario.

ID	Description
A1	The candidate MUST liaise effectively with the assessor who will provide a list of requirements and constraints for the security-testing scenario.
A2	Typical requirements that MAY be requested include: • Internal security testing of a LAN; • Application security testing of a web application server; and • External penetration test of an organisation's Internet gateway.
A3	Typical constraints that MAY be placed on testing include: • Exclusion of sensitive or critical systems; • Exclusion of particular techniques such as account password guessing; and • No intrusive testing or exploitation of

	vulnerabilities. • The use of black and white listing of IP addresses.

2.2 Defining Scope

Demonstrate the ability to define a scope of testing given certain customer requirements, timeframes and any constraints.

ID	Description
B1	The Candidate MUST demonstrate: • An understanding of scope restrictions on test practice. • A comprehensive understanding of the requirements for testing safety critical or other designated high-risk systems. • A comprehensive understanding of the practical issues regarding permission to test, especially in production and hosted environments. • An understanding of how to apply a consistent methodology during test execution. • A comprehensive understanding of test errors, including false-positive and false-negative results and confirmation methods. • A comprehensive understanding of record keeping.

2.3 Legal Issues

Demonstrate an appropriate knowledge of law potentially relevant to security testing in a variety of situations in the country and region of certification.

ID	Description
C1	The Candidate SHOULD demonstrate • An understanding of the general international legal environment with regards to penetration testing. • An understanding of major international

	personal & corporate data protection regimes. • An understanding of the legal regime regarding destructive testing applying to the jurisdiction within which they are taking the examination. • An understanding of the e-crime legal regime applying to the jurisdiction within which they are taking the examination. • A comprehensive understanding of the TigerScheme Code of Conduct.

2.4 Planning and Management

Demonstrate the ability to develop a project plan for a given security testing requirement and defined scope.

ID	Description
D1	The candidate MUST be able to demonstrate awareness of the • Requirement for suitable system access, • Requirement for testing authority documents to have been signed by all relevant parties including any third party hosting company or service providers; • Requirement for physical access and escorts in a timely fashion.

2.5 Managing risk

Demonstrate the ability to follow risk reduction procedures and liaise with the customer and other relevant parties to reduce the likelihood or impact of any unwanted issues arising from security testing.

ID	Description
E1	The candidate MUST demonstrate awareness of the risks associated with security testing that can impact on customer systems.
E5	The candidate MAY demonstrate the ability to suggest strategies aimed at reducing risk throughout the test, these would be expected to include ensuring that both the testing team and the customer have established point of contact for

	emergencies.

2.5 Testing Methodology

Demonstrate understanding of and adherence to a stated methodology for a given testing requirement and defined scope.

ID	Description
F1	The Candidate MUST demonstrate: • An understanding of scope restrictions on test practice. • An understanding of the requirements for testing safety critical or other designated high-risk systems. • An understanding of the practical issues regarding permission to test, especially in production and hosted environments. • An understanding of how to apply a methodology during test execution. • An understanding of test errors, including false-positive and false-negative results and confirmation methods. • An understanding of record keeping.

2.6 Testing platform

Demonstrate possession and use of a suitable well-maintained and configured testing platform.

ID	Description
G1	The candidate MUST be in possession of a laptop system that is suitable for performing a security test. The system may be configured with any choice of software and operating system(s) however the following conditions must be met: • All commercial software MUST be suitably licensed • Anti-virus software SHOULD be installed and configured in such a way so as to not disrupt the security testing tools

3.0 Technical Expertise

3.1 Technology and Vulnerabilities

Demonstrate awareness of existing and emerging security technologies likely to have relevance to security testing. Demonstrate knowledge of existing and emerging threats and vulnerabilities.

ID	Description
H1	The Candidate MUST demonstrate: • A comprehensive understanding of basic networking protocols. • An understanding of common Internet encryption protocols (e.g. SSL/TLS, SSH) including encryption protocol negotiation and key exchange. • An understanding of authentication protocols and techniques and their common weaknesses. • An understanding of common computer hardware architectures. • An understanding of operating systems in common commercial use. • Possession and use vulnerability information.
H2	The Candidate SHOULD demonstrate • An understanding of Internet Routing. • An understanding of security issues related to multi-protocol operations. • An understanding of security issues related to communications protocol interfaces (e.g. LAN / WAN transitions). • An appreciation of the security strengths and weaknesses of common networking protocols. • An understanding of the appropriate use of encryption and the varying requirements for data (or link), end-to-end and storage

	encryption. • A practical understanding of encryption key lengths, negotiation and entropy. • An understanding of the security strengths and weaknesses of common operating systems both in principle and as commonly implemented.
H3	The Candidate SHOULD demonstrate: • An understanding of the concepts of randomness and entropy as applied to encryption methods and keys. • A detailed understanding of asymmetric encryption as applied to common Internet protocols. • A detailed understanding of hybrid encryption as applied to common Internet protocols. • A detailed understanding of symmetric encryption as applied to common Internet protocols.

3.2 Assessing Network Design

Demonstrate the ability to assess network designs with regard to security and identify potential areas of risk. This will include aspects of network security such as network protocols, perimeter security, monitoring and general architecture.

ID	Description
I1	The Candidate MUST demonstrate: • A detailed understanding of Internet and network segment addressing, including CIDR, unassigned and invalid addresses RFC1918, NAT / PAT and ASNs. • A detailed understanding of the use of active network tools to enumerate or confirm a network or infrastructure diagram. • An understanding of the use and limitations of multi-homed and bridging devices. • An understanding of Network Perimeter

	devices and their effects on scanning. • An understanding of the use and limitations of active network tools to determine the operating system(s) running on a target.
I2	The Candidate SHOULD demonstrate: • An understanding of the use of passive network tools to enumerate or confirm a network or infrastructure diagram. • An understanding of port scanning and OS fingerprinting techniques along with their strengths and weaknesses.
I3	The Candidate MAY demonstrate: • An understanding of the differences between IP V4 and IP V6 addressing. • An understanding of the roles of the Regional Internet Registries. • An understanding of the effects and limitations of address spoofing.

3.3 Assessing Application Design

Demonstrate the ability to assess an application design with regard to security and identify potential areas of risk.

ID	Description
J1	The candidate MUST be able to demonstrate the ability to assess application architecture on paper and identify potential weaknesses and security issues. The candidate would also be expected to suggest generic recommendations for addressing any issues

3.4 Security Testing – Enumeration

Demonstrate a high level of proficiency in enumeration techniques employed during security tests on both network infrastructure and applications.

ID	Description
K1	The candidate MUST demonstrate and discuss using open sources for gathering information

	related to the target systems.
K2	The candidate MUST demonstrate being able to use and explain active techniques for network topology identification.
K3	The candidate MUST demonstrate and explain active techniques for discovery of nodes on a network.
K4	The candidate MUST demonstrate and explain the use of service detection and identification tools to determine network services presented by a variety of systems including version numbers and vendors where appropriate.
K5	The candidate MUST demonstrate and explain the enumeration of data from a variety of common network services on various platforms including: • File-systems shared remotely • User account information • Service or system configuration and management

3.5 Security Testing – Identification and Proof of Issues

Demonstrate a high level of proficiency in the identification and subsequent analysis and subsequent proof of security issues on a range of networks, devices, operating systems and applications.

ID	Description
L1	The candidate MUST demonstrate the ability to identify, the existence of various types of network infrastructure vulnerabilities such as Network protocol weaknesses and insecurities at all network layers
L2	The candidate MUST demonstrate the ability to identify, explain and prove the existence of the following types of Operating System vulnerabilities and exposures: • Known software vulnerabilities • Inadequate access control of services • Authentication Mechanisms

	• Management mechanism insecurities • Remote and Local user access control insecurities
L3	The candidate MUST demonstrate the ability to perform a security build review of common Operating Systems.
L4	The candidate MUST be able to discuss current vulnerabilities in a variety of common Operating Systems.

3.6 Security Testing – Classifying Risk

Demonstrate a reasonable level of proficiency in the suitable classification and analysis of technical risk posed by various technical security vulnerabilities and exposures. This will include understanding of impact and the identification of any mitigating factors or controls.

ID	Description
M1	The candidate MUST be able to describe and understand the following aspects of a given security vulnerability/issue and how they relate to classifying an issue with regard to the risk that is posed: • The nature of the vulnerability • How the vulnerability might be exploited • The type of attacker capable of exploiting the vulnerability • Any pre-requisites that an attacker would need to exploit the vulnerability • The likelihood of a successful exploitation • The presence of mitigating factors that prevent the exploitation or reduce the likelihood of a successful exploitation • The technical impact to the target with regard to confidentiality, integrity and availability if the vulnerability is exploited
M2	The candidate SHOULD be able to classify a number of given security issues with regard to risk posed and communicate this by attaching a quantity to the risk (e.g. High, Medium, Low or

	5,4,3,2,1 etc.)

3.7 Remediation

Demonstrate knowledge of the strategies and technology that can be used to counter a security threat.

ID	Description
N1	The candidate MUST demonstrate some knowledge and understanding of remediation strategies and steps suitable for addressing a variety of identified security risks and vulnerabilities.

4 Deliverables

4.1 Management Presentation of Results

Demonstrate the ability to produce a written and verbal summary of security testing results to a non-technical audience.

ID	Description
O1	The candidate MUST be able to provide both a verbal and written summary of a security test to their line management.

4.2 Technical Presentation of Results

Demonstrate the ability to document and explain identified security issues identifying the issue, impact, risk and suitable recommendations.

ID	Description
P1	The candidate MUST be able to provide detailed information on identified security issues to their line management.