Tiger Scheme
SST Standards

Title	**Tiger Scheme Senior Security Tester Standards**
Version	3.2
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	15/05/07	Mr Greg Jones	-
1.1	15/05/07	Mr Greg Jones	-
2.0	04/06/07	Mr Greg Jones	-
3.0	31/10/08	Professor Andrew Blyth	-
3.1	19/12/08	Professor Andrew Blyth	-
3.2	21/06/11	Professor Andrew Blyth	-

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 *Senior Security Tester* (SST) level.

1.1.2 The Senior Security Tester 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 Senior Security Tester 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 Senior Security Tester 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. The Senior Security Tester assault course is more than s simple assessment of technical

skill and is designed to evaluate the candidate as a whole and their capabilities across the security-testing spectrum.

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

- A multiple choice assessment (1 Hour)
- A written examination (3 Hours)
- A practical assessment via an assault course (6 Hours)
- A viva (30 Minutes)

1.1.8 The Senior Security Tester 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 SST/CTL assessment is 60% and a successful candidate must pass all components of assessment.

1.1.10 1.2 Summary of TIGER Scheme Senior Tester Requirements

Area	Skill-set	Skills Requirement Summary
Management, Ethics & Compliance	Understanding requirements	Demonstrate the ability to understand customer requirements and set customer expectations for a given testing scenario.
	Defining scope	Demonstrate the ability to define a scope of testing given customer requirements, timeframes and any constraints.
	Legal issues	Demonstrate an appropriate knowledge of UK law potentially relevant to security testing in a variety of situations.
	Planning and Management	Demonstrate the ability to develop a project plan for a given security testing requirement and defined scope. Demonstrate an understanding of engagement management issues such as customer and supplier liaison, arranging access to facilities, secure storage of customer data and contingency planning.
	Managing risk	Demonstrate the ability to enforce procedures and liaise with the customer and other relevant parties to reduce the likelihood or impact of any unwanted issues arising from security testing such as disruption to service.
	Testing methodology	Demonstrate the adherence to a stated methodology for a given testing requirement and defined scope.
	Testing platform	Demonstrate possession and use of a suitably well maintained and configured testing platform.
Technical Expertise	Technology and Vulnerabilities	Demonstrate awareness of existing and emerging security technologies. Demonstrate up-to-date knowledge of existing and emerging threats and vulnerabilities.
	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 intrusion detection, network segregation and general architecture.
	Assessing application design	Demonstrate the ability to assess an application design with regard to security and identify potential areas of risk. Such an assessment is expected to demonstrate an understanding of areas including application authentication and access control, database security and application communications.
	Security testing - enumeration	Demonstrate a high level of proficiency in enumeration techniques employed during security tests on both network infrastructure and applications. This will include open source enumeration, network topology mapping, network node identification, network service enumeration, application service enumeration and web application mapping and enumeration.
	Security testing – identification and proof of issues	Demonstrate a high level of proficiency in the identification and subsequent analysis and proving of security issues on a range of networks, devices, operating systems and applications. This will require the ability to identify both false positives and false negatives and operate within the constraints of the scope of testing whilst keeping risk of disruption to an acceptable level.
	Security testing – classifying risk	Demonstrate a adequate 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.
	Remediation	Demonstrate a reasonable knowledge and understanding of suitable remediation strategies and steps suitable for addressing a variety of identified security risks and vulnerabilities. This will include design and architectural issues and technical configuration flaws in a range of devices and operating systems and application software security issues.
Deliverables	Management presentation of results	Demonstrate the ability to produce a written and verbal summary of security testing results to a non-technical audience.
	Technical presentation of results	Demonstrate the ability to document and explain identified security issues identifying the issue, impact, risk and suitable recommendations.

2 Management, Ethics and Compliance

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 large WAN; • 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 be able to produce a suitable scope for the testing based on the requirements and constraints provided by the assessor during the 'understanding requirements' phase of the assault course.
B2	The candidate MUST be able to discuss with the assessor the benefits and disadvantages of particular approaches and how the requirements will or will not be met by the proposed scope.

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 MUST be able to demonstrate an understanding of the relevance of the local and national laws and the requirement for a letter of authorisation prior to the commencement of testing. The candidate SHOULD also demonstrate awareness of the need to inform and obtain permission from third parties in certain situations.

2.4 Planning and Management

Demonstrate the ability to develop a project plan for a given security testing requirement and defined scope. Demonstrate an understanding of engagement management issues such as customer and supplier liaison, arranging access to facilities; secure storage of customer data and contingency planning.

ID	Description
D1	The candidate MUST be able to demonstrate awareness of the requirement for suitable system access (e.g. network addresses, switch ports, account credentials etc.)
D2	The candidate MUST be able to demonstrate awareness of requirement for testing authority documents to have been signed by all relevant parties including any third party hosting company or service providers
D3	The candidate MUST be able to demonstrate awareness of the requirement for physical access and escorts in a timely fashion.
D4	The candidate MUST be able to demonstrate awareness of the availability of key customer staff for specific elements of the security assessment (e.g. interview with Firewall administrator).
D5	The candidate MUST be able to demonstrate awareness of the agreements on any status update process throughout the security assessment (e.g. daily wash up meetings, immediate notification of high risk issues.)
D6	The candidate MUST be able to demonstrate awareness of the agreements with regard to delivery of the draft and final reports.

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 such as disruption to service.

ID	Description
E1	The candidate MUST demonstrate awareness of the risks associated with security testing that can impact on customer systems, these may include unintentional disruption to network devices and links through bandwidth consumption.
E2	The candidate MUST demonstrate awareness of the risks associated with security testing that can impact on customer systems, these may include unintentional disruption to systems and applications through the unintentional triggering of error conditions
E3	The candidate MUST demonstrate awareness of the risks associated with security testing that can impact on customer systems, these may include disruption to user access through the lockout of user and application accounts.
E4	The candidate MUST demonstrate awareness of the risks associated with security testing that can impact on customer systems, these may include disruption to audit and monitoring functions due to excessive security event recording
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.
E6	The candidate MAY demonstrate the ability to suggest strategies aimed at reducing risk throughout the test, these would be expected to include ensuring that the customer has operational backup/restore procedure in place in the event of unintended data or system corruption.
E7	The candidate MAY demonstrate the ability to suggest strategies aimed at reducing risk throughout the test, these would be expected to include ensuring that the customer is aware of the potential for generating large amounts of audit logs and IDS alerts.
E8	The candidate MAY demonstrate the ability to suggest strategies aimed at reducing risk throughout the test, these would be expected to include ensuring that critical applications or systems are identified before testing starts and potentially avoided or assessed using other means.

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, when asked throughout the assault course; show how any activities performed or tools used are supported directly by their chosen methodology.

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 an up-to-date knowledge of existing and emerging threats and vulnerabilities.

ID	Description
H1	The candidate MUST understand the operation and role of the following security technologies and controls: • Firewalls • Proxy servers • Intrusion Detection Systems • Virtual Private Networks • Public Key encryption • Symmetric Key encryption • File Access Control Lists • Operating System hardening principles • Link encryption devices • Two Factor authentication • Digital Certificates
H2	The candidate MUST be expected to demonstrate possession and use of up-to-date and comprehensive sources of vulnerability information.
H3	The candidate SHOULD be able to discuss recent significant vulnerability announcements making reference to the availability of exploit code where appropriate and the potential impact of the vulnerability.

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 intrusion detection, and network segregation and general architecture.

ID	Description
I1	The candidate MUST be able to demonstrate the ability to assess a network design or network map on paper and identify potential weaknesses and security issues. The candidate would also be expected to suggest generic recommendations for addressing any issues.
I2	The candidate will be provided a network design

	for an organisation or network and SHOULD identify: • The actual network perimeter • Perimeter security gateways • Perimeter security weaknesses with suggestions for improvement • Internet secure networks and associated gateways • Network areas where monitoring should be deployed • Network areas where additional access controls should be deployed • Strategies for network segregation and access control • Strategies for protecting against a variety of given 'internal threats.'

3.3 Assessing Application Design

Demonstrate the ability to assess an application design with regard to security and identify potential areas of risk. Such an assessment is expected to demonstrate an understanding of areas including application authentication and access control, database security and application communications.

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
J2	The candidate will be provided an architecture design chart for an application and SHOULD to identify or discuss: • Effectiveness of application authentication • Effectiveness of application auditing • Effectiveness of segregation of user systems from application database(s) • Application communication security • Exposure of application infrastructure to 'external' attack • Types of vulnerability that may be present in various components of the application architecture. • Areas of application software that may be suitable for limited application security testing

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	It is anticipated that misleading and incorrect information will be presented to the candidate intentionally by certain components of the assault course network during the enumeration process. The candidate MAY be expected to identify such instances of inaccurate or incorrect information.
K2	The candidate MUST demonstrate and discuss using open sources for gathering information related to the target systems. These would include: • Web search engines and third-party Web sites; • The target's own web site • Network Registration databases; • Target mail and name services that are incorrectly configured; • Newsgroups; and • Vendor manuals and documentation
K3	The candidate MUST demonstrate being able to use and explain passive and active techniques for network topology identification.
K4	The candidate MUST demonstrate and explain active and passive techniques for discovery of nodes on a network.
K5	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.
K6	The candidate MUST understand and discuss methods for the identification and analysis of unknown services.
K7	The candidate MAY demonstrate understanding of advanced analysis techniques for unknown services and protocols.
K8	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 • System resources presented remotely • User account information • Service or system configuration/management

K9	The candidate MUST demonstrate the following techniques and explain how they are used to map out and enumerate web applications: • Utilisation of man-in-middle proxy to capture site structure; • Hyperlink analysis and brute force resource identification; • Analysis and inspection of available page source code; • Identification of the session control mechanism used within the application; and • Identification of relevant scripts, applications and associated parameters.
K10	The candidate MUST demonstrate understanding of the potential limitations of using automated software on some web applications. E.g.: • Sites that feature heavy use of dynamic client side scripting • Sites that use client side executable components; and • Sites which generate incorrect server responses.

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 both false positives and false negatives and operate within the constraints of the scope of testing whilst keeping risk of disruption to an acceptable level. For each action performed the candidate should demonstrate an awareness of any risks involved, for example ARP poisoning attacks on an internal LAN carry with them a high risk of local network disruption.
L2	The candidate MAY suggest further techniques for proving issues, which may fall outside of the constraints and scope in place during the assault course.
L3	The candidate MUST demonstrate the ability to identify, explain and prove the existence of the following types of network infrastructure vulnerabilities and exposures: • Physical network weaknesses • Network protocol weaknesses and insecurities at all network layers

	• Network device issues:
	  o Known software vulnerabilities
	  o Inadequate access control of network services
	  o Trust relationship insecurities
	  o Management mechanism insecurities
	• Network access control and segregation vulnerabilities

L4	The candidate MUST be able to discuss current and existing vulnerabilities in a variety of common network devices; the candidate should have an awareness of the likelihood of exploitation and the likely impact of recently announced vulnerabilities.
L5	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 • Trust relationship insecurities • Management mechanism insecurities • Remote and Local user access control insecurities
L6	The candidate MUST demonstrate the ability to perform a security build review of common Operating Systems.
L7	The candidate MUST be able to discuss current and existing vulnerabilities in a variety of common Operating Systems and 3rd Party Software, the candidate should have an awareness of the likelihood of exploitation and the likely impact of recently announced vulnerabilities.
L8	The candidate MAY demonstrate knowledge of a number of more advanced operating system vulnerabilities and identification methods including: • Use of tools and techniques to identify new OS software vulnerabilities • Use of techniques to develop exploits / code for existing and new vulnerabilities.
L9	The candidate MUST demonstrate the ability to identify, explain and prove the existence of the following types of web application vulnerabilities and exposures: • Input data validation vulnerabilities • Session control mechanism vulnerabilities • Authentication mechanism vulnerabilities • Functional logic and function access control • Application server hardening flaws

L10	The candidate MUST also be able to discuss current and existing vulnerabilities in web applications. The candidate should have an awareness of the likelihood of exploitation and the likely impact of recently announced vulnerabilities.

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 • How to reference further information with respect to vulnerabilities (e.g. CVE/BID/CVSS)
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 a sound knowledge and understanding of suitable remediation strategies and steps suitable for addressing a variety of identified security risks and

	vulnerabilities. This will include design and architecture issues, technical configuration issues in a range of devices and operating systems and application software security issues although extensive knowledge of specific platforms and applications is not required.
N2	Detailed recommendation sometimes require extensive product knowledge and if a candidate is not in possession of this knowledge then they SHOULD, in the least, suggest an overview recommendation.
N3	The candidate MUST be able to provide a summary of how each issue identified or discussed during the assault course may ideally be solved (e.g. 'ensure XYZ service performs adequate authentication and access control for remote users'.) The candidate MAY then further suggest specific details of how to achieve the recommended action.

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 customers who are non-technical. Whilst it is appreciated that many security issues and vulnerabilities are by definition technical, it is always possible to relay concepts such as probability of exploitation and impact to information systems and associated data.
O2	For each given issue, or group of issues if appropriate, the candidate SHOULD convey the following information: • The cause of the issue (e.g. mis-configuration, human error, software vulnerability) • Which type of attacker would most likely exploit the issue (e.g. authorised internal user, external Internet connected anonymous user, attacker with physical access etc.) • The difficulty and likelihood of a successful exploit • The potential impact to the customer's information systems and data preferably in terms of confidentiality, integrity and availability.

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 technical or technical security customers. Such information is likely to include a list of affected components, details of the issue, technical impact and recommended action(s) for remediation.
P2	For each given issue the candidate, or group of issues if appropriate, the candidate SHOULD convey the following information: • A detailed description of the problem

	• A list of affected components (if relevant) • A description of the risk posed referencing the type of attack that can occur and what the impact of the attack would be with regard to the confidentiality, integrity and availability of the target system and other dependent systems. • A qualitative assessment of the risk posed (on a scale of High-Low or 5-1 etc.) • Possible sources of further information • A recommendation or series of recommendations which may extend beyond the technical arena, to mitigate the identified risk.