The Chartered Institute for IT

Enabling the information society

Penetration Testing

Definition: Penetration testing is a method for evaluating computer and network security by simulating an attack on a computer system or network. The objective is to find security flaws and configuration errors, and to provide the organisation with remediation advice in order to minimise the risk of a successful attack. It primarily concerns itself with governance, confidentiality, integrity, availability, risk management and compliance.

Context: Today, real and credible threats to cyber security are diverse, complex and at an unprecedented scale. Examples of determined and successful efforts include: stealing intellectual property, stealing commercially sensitive data; exploiting information security weaknesses through the targeting of partners, subsidiaries and supply chains at home and abroad. Organisations have a poor history of developing, implementing and supporting systems which are secure against attack. Penetration testing, coupled with post-test remediation, provides the CISO/CIO/CTO with evidence that their infrastructure and applications are adequately secure.

Key issues:

- *Acquisition and Implementation*
- *Confidentiality*
- *Integrity*
- *Availability*
- *Compliance*
- *Maintenance*
- *Risk*
- *Scope and Engagement*

Acquisition and Implementation

BCS believes that understanding cyber-security threats and ensuring that corporate governance and risk management are focused on reducing cyber-security risks at the design or acquisition stage will minimise an organisation's vulnerability to cyber-threats, whether existing or emerging. Penetration testing is an essential component in achieving this objective. This should extend into the supply chain to an equal degree particularly where significant levels of the solution rely on out-sourced implementation and/or support resources. The on-going penetration testing of the solution should be considered during the design, or acquisition phase.

Confidentiality

Penetration testing for unauthorised access to systems and data should be conducted as early as possible and throughout the design or acquisition phase, together with an on-going testing programme once a system is live. Tests should reference ISO 27001 and good practice guidance offered by manufacturers, the Open Web Application Security Project (OWASP) and other appropriate guidance.

Integrity

Penetration testing for the ability to execute unauthorised changes to systems and data should be scheduled as early as possible, together with an on-going testing programme once a system is live. Tests should reference ISO 27001 and good practice guidance offered by manufacturers, OWASP and other appropriate guidance.

Availability
Penetration testing the resilience of systems to 'denial of service' attacks should be conducted as early as possible, together with an on-going testing programme once a system is live. Tests should reference ISO 27001 and good practice guidance offered by manufacturers, OWASP and other appropriate guidance.

Compliance
Penetration testing itself should comply with all statutory and regulatory requirements, such as the Data Protection Act and the Computer Misuse Act. This should be extended to suppliers through contractual arrangements and rigorous assessment of suppliers at appropriate time intervals.

Maintenance
Systems subject to on-going maintenance and changes to software and configurations should be penetration tested on a regular basis and after every major change.

Scope and Engagement
The scope of any penetration test should be discussed in detail with the penetration testing supplier and, where possible, based on an initial threat and risk analysis to ensure all possible threat agents and vectors have been considered. Reference should be made to the British Government's HMG IA Standard No. 1, Technical Risk Assessment.

The type of test, from both a technical and procedural perspective, should be clearly defined and contractually agreed between all relevant parties before any work begins. The scope of works should include the parameters of the test, exactly what needs to be tested and to what level the tests should be conducted, what constraints should be in place and how the test will be conducted. The scope should also explicitly exclude any adjoining systems which are not to be tested. Reference should be made to the Open Source Security Testing Methodology Manual (OSSTMM).

Consent forms should be used to ensure that the testing supplier has permission from the system owner(s) and any relevant third parties to conduct the test without contravening any legislation, such as the Computer Misuse Act.