

Penetration Test

In today's increasingly interconnected business world, vulnerabilities present in an organisation's technical infrastructure can lead to serious problems – the loss of trade secrets, damage to reputation or even breach of legal obligations to protect confidential information.

A penetration test is designed to emulate real life attack motivations and techniques in order to provide a comprehensive register of vulnerabilities, weaknesses and exposures based on a specific scenario or threat, or focused on a subset of technical infrastructure.

The service can be tailored to meet the particular requirements of your organisation. In the most straightforward case a penetration test will take the form of a focused attack against a defined localised target such as a specific network. Our tests can also be modified to emulate a specific scenario, such as assessing the damage that a disgruntled employee could cause within your corporate network or determining the extent of access a completely anonymous attacker might be able to obtain without any prior knowledge of the target. Options such as social engineering, where appropriate, add the important human factor into the assessment and may also be incorporated.

Whichever scenario is adopted, the methodology followed is likely to contain the following phases:

- **Network Mapping and Target Discovery**

IRM will gather information about the deployment of the target network, identifying systems present and any intermediate network devices that might be of interest.

- **Target Identification and Service Discovery**

Operating systems and services are enumerated to form a picture of the functionality available that might be abused by an attacker.

- **Vulnerability Identification and Analysis**

Identified hosts and services will be assessed for the presence of both known software vulnerabilities and incidences of poor configuration. Both automated tools and manual techniques will be used to ensure maximum coverage.

- **Exploitation and Further Access**

IRM will attempt to exploit any vulnerabilities or weaknesses uncovered, both to verify their presence and to gain an understanding of the business impact a particular issue might have for the organisation. At this stage, our consultants will attempt to access any information or systems specified by the client as ultimate targets for the penetration test (such as critical servers or company confidential data).

- **Deliverables**

IRM will deliver a formal report including an executive summary, a risks and recommendations table detailing the high level results of the assessment and a detailed description of each issue discovered including remediation advice.

About IRM

Information Risk Management Plc (IRM) is a vendor-independent information security consultancy. Founded in 1998 to work alongside global enterprises in understanding the security risks inherent in an increasingly interconnected business environment, IRM has become a leader in penetration testing, risk assessment and security auditing.