



# Penetration Test

## What is a penetration test?

A penetration test is the process of actively evaluating security measures of your information assets. There are a number of ways that this can be undertaken. The most common procedure is that the security measures are actively analyzed for design weaknesses, technical flaws and vulnerabilities.

## Why is penetration testing useful?

There are several reasons why organizations should choose to perform a penetration test. Reasons can range from technical to commercial but the most common are:

- Identify the threats facing your organisation's information assets - TOE (Target of evaluation) so that you can quantify your information risk and provide adequate information security expenditure.
- Reduce your organisation's IT security costs and provide a better return on IT security investment (ROSI) by identifying and resolving vulnerabilities and weaknesses. These may be known vulnerabilities in the underlying technologies or weaknesses in the design or bad implementation.
- Provide your organisation with thorough and comprehensive assessment of organisational security covering policy, procedure, design and implementation.
- Gain and maintain certification to an industry regulation (ISO17799, HIPAA etc).
- Adopt best practice by conforming to legal and industry regulations.

## Available types of tests

**1. External Penetration Testing** is the traditional approach to penetration testing. The testing is focused on all components of target system (TOS) including servers, infrastructure and the underlying software comprising the target. It may be performed with no prior knowledge of the site (method known as black box) or with full disclosure of the topology and environment (method known as white box). This type of testing consists of comprehensive analysis of publicly available information about the target, a network enumeration phase where target hosts are identified and analysed, and the behaviour of security devices such as screening routers and firewalls are analysed. Vulnerabilities and misconfigurations within the target hosts should then be identified, verified and the implications assessed.

### Test usually consists of:

- Network Surveying
- Port Scanning
- System Identification
- Services Identification

- Vulnerability Research & Verification
- Router Testing
- Firewall Testing
- Intrusion Detection System Testing
- Password Cracking
- Denial of Service Testing
- Containment Measures Testing

**2. Internal Security Assessment** follows a similar methodology to external testing, but provides a more complete overview of the overall security. Testing is typically performed from a number of network access points, representing each logical and physical segment. For example, this may include tiers and DMZ's within the environment, the corporate network or partner company connections.

### Test usually consists of:

- Network Surveying
- Port Scanning
- System Identification
- Services Identification
- Vulnerability Research & Verification
- Router Testing
- Firewall Testing
- Intrusion Detection System Testing
- Password Cracking
- Denial of Service Testing
- Trusted Systems Testing

**3. Application Security Assessment** is focused to identify and assess threats to the organisation through proprietary, customer made applications or systems. These applications may provide interactive access to potentially sensitive materials. It is vital that they be assessed to ensure that, firstly, the application doesn't expose the underlying servers and software to attack, and secondly that a malicious user cannot access, modify or destroy data or services within the system. Even in a well-deployed and secured infrastructure, a poorly secured application can expose the organisation to unacceptable risk.

### Test usually consists of:

- Application Security Testing
- Code Review



**4. Security Assessment of Wireless and Remote Access** consists of evaluating security risks associated with an increasingly mobile workforce. Home-working, broadband always-on Internet access, 802.11 wireless networking and a plethora of emerging remote access technologies have greatly increased the exposure of companies by extending the traditional perimeter ever further. It is important to know that the architecture, design and deployment of such solutions is secure and to ensure the associated risks are managed effectively.

**Test usually consists of:**

- Wireless Networks Testing
- Cordless Communications Testing
- Privacy Review
- Infrared Systems Testing

**5. Telephony Security Assessment** addresses security concerns relating to corporate voice technologies. This includes abuse of PBX's by outsiders to route calls at the target's expense, integration of voice over IP (VoIP) technology, unauthorised modem use and associated risks.

**Test usually consists of:**

- PBX Testing
- Voicemail Testing
- FAX review
- Modem Testing

**6. Social Engineering** addresses intrusions without specialized technical abilities. It relies on human interaction and involves tricking other people into breaking normal security procedures. Social engineering usually involves a scam; trying to gain the confidence of a trusted source by relying on the natural helpfulness of people as well as their weaknesses, appealing to their vanity, their authority and eavesdropping are natural techniques used. Other techniques involve searching refuse bins for valuable information, memorizing access codes by looking over someone's shoulder, or taking advantage of people's natural inclination to choose passwords that are meaningful to them but can be easily guessed.

**Test usually consists of:**

- Request Testing
- Guided Suggestion Testing
- Trust Testing

### **Methodology - basic requirement for success**

For the most part of testing it is the systematic analysis of the security measures at hand. Commonly used methodologies are: methodology OSSTMM and OWASP and documents of **National Institute of Standards and Technology** (NIST). NIST discusses penetration testing in Special Publication 800-42, Guideline on Network Security Testing. Implementation of these methodologies and standards provides consultant managed architecture of the key areas that should be tested, so that the overall test is complete and accurate.

### **Reports**

The most important phase of penetration testing is presentation of results. Individual phases of testing are documented and well described. These reports have usually two forms - high level report for management and detailed report for technicians. Important part of this report is part, describing recommendation how to fix identified vulnerability and how to minimize the risks.