Pendulum–Ardham
Cyber Vulnerability Assessment Penetration Testing

What is a Penetration Test?

A **Penetration Test** is the process of actively evaluating your information security measures, most commonly by analyzing security measures for design weaknesses, technical flaws, and vulnerabilities. The results are delivered in a comprehensive report to executive, management, and technical audiences.

Why Would We Want a Penetration Test?

There are several reasons why organizations choose to perform a penetration test ranging from technical to commercial. The most common are:

- To identify the threats facing your organization's information assets for quantification of your information risk
- To provide an adequate expenditure for information security
- To reduce your organization's information technology (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 implementation
- To provide your organization with the assurance that comes with a thorough and comprehensive assessment of organizational security covering policy, procedure, design, and implementation
- To adopt best practices by conforming to legal and industry regulations
- To identify the overall security awareness of end users

Penetration Testing Types

External Penetration Testing is the traditional approach to penetration testing. This testing focuses on servers, infrastructure, and the underlying software comprising the target. It may be performed by the specialist/technician with no prior knowledge of the site (black box) or with full disclosure of the topology and environment (white/crystal box). This type of testing typically involves a comprehensive analysis of publicly available information about the target; a network enumeration phase through which target hosts are identified and analyzed; and analysis of the behavior of security devices, such as screening routers and firewalls. Vulnerabilities within the target hosts would then be identified, verified, and the implications assessed.

Internal Security Assessment follows a similar methodology to external testing but provides a more complete view of the site security. Testing will typically be performed from a number of network access points, representing each logical and physical segment. For example, this may include tiers and demilitarized zones (DMZs) within the environment, the corporate network, or partner company connections.

Wireless/Remote Access Security Assessment addresses the security risks associated with an increasingly mobile workforce. Home offices, 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 vital that the architecture, design, and deployment of such solutions are secure and sound to ensure the associated risks are managed effectively.

PENDULUM
RISK MANAGEMENT SERVICES

ardham
EXTRAORDINARY SOLUTIONS

Pendulum
4600B Montgomery Blvd. NE
Ste. 204
Albuquerque, NM 87109
(888) 815-8250
www.PendulumRisk.com

Powered by
Ardham Technologies, Inc.
www.Ardham.com

Social Engineering addresses a non-technical kind of intrusion; it relies heavily on human interaction and often 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 a person's vanity and authority, and eavesdropping are some 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.

Two Types of Approaches: "Black-box" and "White-box"

Penetration tests can be conducted in one of two ways: black-box (with no prior knowledge of the infrastructure to be tested) or white-box (with complete knowledge of the infrastructure to be tested). There are conflicting opinions about this choice and the value that either approach will bring to a project.

Some penetration testing suppliers will suggest that when given the choice, the black-box approach is the best because it closely simulates the process of a real hacker. This is not particularly true as it presupposes that an attacker does not have any knowledge of your systems, which is actually unlikely. If someone is targeting your organization specifically, there is a strong possibility that this person does indeed have detailed knowledge of your systems and procedures; for example, the person may be an ex-employee with a grudge. It would be wise to assume the worst—that any attacker has complete knowledge of your systems. If your security relies solely on the secrecy of your designs, you do not have any tangible security at all.

Secondly, a hacker will not be limited to any time constraints that might be applied to a penetration test. They will not have a week in which to circumvent your security measures. If undiscovered, the hacker will be able to probe away for years until a weakness that can be exploited is found.

There is also the question of value for money. In conducting a black-box test, it is necessary to spend a reasonable proportion of the time allocated for the project on discovering the nature of the infrastructure and how it connects and interrelates. Obviously, if the time is being spent on discovery, it is not being spent on actual testing for vulnerabilities.

This is not to say that black-box testing has no value. It does. It is useful for determining how information leaks from your systems that might be utilized by others (such as in mail headers). When choosing a black-box test, keep in mind that to get the same amount of time spent on accessing vulnerabilities as you would with white box testing, you will need to allocate more time to the project overall.

Deliverables

A penetration test will involve the systematic analysis of all the security measures in place. A full project should include some or all of the following areas, with the exact requirements agreed upon in a formal scoping document prior to commencing:

- Network Security
- Information Security
- Social Engineering
- Wireless Security
- Physical Security

PENDULUM
RISK MANAGEMENT SERVICES

ardham
EXTRAORDINARY SOLUTIONS

Pendulum
4600B Montgomery Blvd. NE
Ste. 204
Albuquerque, NM 87109
(888) 815-8250
www.PendulumRisk.com

Powered by
Ardham Technologies, Inc.
www.Ardham.com