Pendulum–Ardham

Cyber Vulnerability Assessment for a Law Firm

What is Penetration Testing?

Penetration Testing 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 a Law Firm Want Penetration Testing?

There are several reasons why firms choose to perform penetration testing, ranging from technical to commercial. The most common are:

- To identify the threats facing a firm's information assets for quantification of its information risk
- To provide an adequate expenditure for information security
- To reduce a firm'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 design and/or implementation
- To provide a firm 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

External Penetration Testing

External Penetration Testing is the traditional approach to penetration testing. This type of testing focuses on servers, infrastructure, and the underlying software that comprise the target. It may be performed by a 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 are then identified and verified, and implications are assessed.

Deliverables

An external penetration test will involve the systematic analysis of all security measures in place from a remote location. A full project will include:

- An external penetration test
- Two reports from scanning software
- One summary of vulnerabilities
- One detailed report of vulnerabilities
- One phone call from Ardham Technologies' CEO to review findings

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