INFOSIGHT®

VULNERABILITY ASSESSMENT & PENETRATION TESTING

Our Vulnerability Assessment and Penetration Testing provides a complete evaluation and holistic view of your organization's security posture. The evaluations are designed to proactively identify and prevent the exploitation of any existing IT vulnerabilities. Our main objective is to identify cyber security weaknesses and test how far a potential exploit can compromise the network. We also test the organization's security policy compliance, the effectiveness of its employees security awareness training program, as well as the organization's ability to identify and respond to cyber security incidents.

What's the difference between a Vulnerability Assessment and a Penetration Test?

In a Vulnerability Assessment, the susceptibilities and exposure are identified. A penetration test not only identifies the threats, but it creates an attempt to exploit them. When these two procedures are combined, they achieve a complete threat analysis and a comprehensive view of your security posture is obtained.

Our Methodology

Our assessment methodology includes structured review processes based on recognized "best-in-class" practices. The following diagram attempts to visually explain the stages of our assessment methodology.

1. Conduct an External Vulnerability Assessment (EVA). Begin reconnaissance and probing of perimeter firewalls, email, web application servers and other externally facing devices. Any vulnerabilities found would be exploited in a penetration test.

2. Internal network testing is performed for identification of vulnerabilities as part of an Internal Vulnerability Assessment (IVA). Weak areas are found by probing of internal software, servers, laptops, etc.

3. Complete discovery and evaluation of wireless networks. Vulnerabilities discovered would be exploited in a wireless penetration test.

4. Conduct social engineering in the form of impersonation by our assessor. This phase may include physical onsite security testing, or remote social engineering by using email phishing: telephone pretexting, website subversion, dumpster diving and other techniques.

5. Our Assessors will overtly attach to the network, run any final scans and perform complete testing of IT security controls. At the completion of this phase, an Assessment and Remediation Report will be written explaining discovered vulnerabilities with instructions for remediation.

www.InfoSightInc.com 877-557-9703 305-828-1003 Info@InfoSightInc.com

PROACTIVELY IDENTIFY VULNERABILITIES AND PREVENT EXPLOITATION

Key Differentiators

We provide you with two reports:

- Executive level
- Full detailed

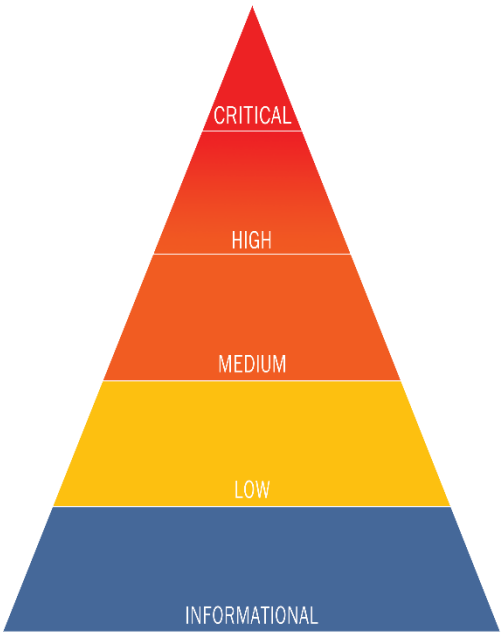
We utilize a wide variety of tools in order to acquire the information needed to write an individualized custom report, which is provided to you by our analysts.

Upon completion of the assessments, a final report will provide detailed information in the following format:

FINDING: We will clearly identify the vulnerability and in what manner it was discovered.

RISK: Indicates the potential for damage and the degree of probability of loss, if an attacker were to exploit the vulnerabilities.

Risks in this report are delineated in the following categories:



Critical/High: This level of risk is most serious as it relates to an actual breach in network security. Hosts listed as Critical/High represent the highest level of risk and require immediate attention and remediation. A Critical/High rating indicates that a penetration could occur either to the internal or external network during the course of your engagement.

Medium: Findings listed as medium indicate that while the exploit of the listed vulnerability would only elicit minimal damage or information leaks, the nature of the threat should be remedied.

Low: Findings in this section may not present an actual threat. The inclusion of a finding in this category indicates a policy or procedure that is not in keeping with industry best practices for logical and physical security controls.

Informational: Findings either do not relate to network security or highlight unique strengths in the security posture of the network.

RECOMMENDATIONS: We will provide clear and concise recommendations as to the proper method of vulnerability mitigation. These detailed instructions typically include both logical and technical solutions for dealing with risks appropriately. Recommendations generally include but are not limited to the following: sample configurations, patch and service pack recommendations, training (technical and/or security awareness), best practice recommendations, and vendor-specific guidance.

www.InfoSightInc.com 877-557-9703 305-828-1003 Info@InfoSightInc.com