Penetration Testing

Penetration Testing is a targeted, real-world simulation of an attack against an organization's security program that is designed to identify technical, procedural, and physical weaknesses that could allow an attacker to compromise the confidentiality and integrity of sensitive information and business assets. Penetration Testing evaluates an organization's ability to detect and respond to security events as well as the varied defense mechanisms that have been put in place to thwart intrusion attempts.

> "Penetration Testing evaluates an organization's ability to detect and respond to security events as well as the varied defense mechanisms that have been put in place to thwart intrusion attempts."

After testing, all findings are documented along with a detailed walkthrough of exploited vulnerabilities to provide your organization with a clear understanding of the issues discovered and the logical progression in access. Detailed recommendations are a key component of a Penetration Test and documentation will include expert advice on how to address the issues discovered during testing.

BTB utilizes a data driven approach to penetration testing and discovered weaknesses will be exploited to the extent necessary to obtain access to the resources or information deemed most important to your organization. After all, what's more important, administrative access to "Server A" or access to 50,000 customer records containing financial information? That's why it's key for BTB to understand your organization's business and goals regarding information security before any testing begins.

Penetration Testing is often customized to meet specific requirements set forth by our clients. While each Penetration Test is unique, the following activities are often included:

- Technical testing of Internet-based systems and devices (web sites, remote access, routers, firewalls, etc.)
- Social engineering of employees (phishing, phone calls, social media, etc.)
- Technical testing of internal systems/devices
- Physical testing of facility security (data centers, buildings, secure areas, etc.)
- Vulnerability Identification after manual testing is complete