Penetration Testing

Stay one step ahead to protect your business

Statistics reveal a huge increase in cyber attacks aimed at business dealing with new challenges, like sudden work-from-home movements, 5G, and hybrid environments that are difficult to secure. These rapid changes make it necessary to know if your current security controls and defenses are sufficient enough to help prevent a malicious attack. A penetration test by an experienced, industry certified penetration tester can help to identify the weaknesses introduced by these changes.

Penetration tests and attack simulation are offered either as a one-time or on a scheduled basis per your business needs.

- **External:** Simulates an attacker probing servers and network devices to identify vulnerabilities that could be exploited to gain inside access.
- **Internal:** Simulates an attacker who has breached the perimeter or a malicious insider attempting to gain elevated privileges or sensitive data.
- **Wireless:** Complete evaluation of your wireless network using both automated and manual methods to identify vulnerabilities.
- **Social Engineering:** A variety of methods—including phishing and voice—are used to entice employees to divulge information that may assist an attacker in future attacks.
- **Web Applications:** Penetration tests on both unauthenticated and authenticated portions of your apps and APIs for flaws and other potential vulnerabilities.
- **Physical Security:** Assessment of the physical security of your facility using social engineering and once inside, collection of information and access.
- **IoT:** Evaluation of IoT devices and associated infrastructure for end-to-end security to help identify vulnerabilities and minimize risk.

Value Proposition

A properly planned and executed penetration test (Pentest) can provide details about an organization's security weaknesses.

Key Benefits:

- Discovering and defending against more sophisticated attack vectors
- Identifying higher-risk vulnerabilities
- Identifying vulnerabilities that may be impossible to detect with automated scanning
- Evaluating the extent of potential business and operational impacts of successful attacks
- Testing the response capabilities of your security operations
- Providing justification for increasing security investment
- Compliance requirements
- Post-security incident, review of network and endpoint security hardening

CBTS assists our clients by providing awareness of risks, proper risk mitigations, and the needed empirical data to validate compliance with regulations and best practices (i.e. HIPAA, PCI, CIS Top 20 CSC, NIST SP 800-53, ISO 27000 Series, SOX, and other similar standards).

Is a Penetration Test right for your company?

A CBTS Penetration Test is the ideal choice for companies that:

- Lack in-house experience to conduct penetration tests effectively.
- Are considering cyber insurance and unsure if they'll meet standards.
- Feel they've hardened their endpoints and network but wonder if they've truly addressed all of the gaps.
- Need their IT teams to focus on core business initiatives instead of regular testing.
- Are mandated to have third-party testing to meet compliance and regulatory standards.
- Want to partner with an experienced security solutions provider to help harden infrastructure and data.

Why CBTS

Our security engineers specialize in penetration testing, hold industry-recognized certifications and are solely dedicated to performing your test. Their assessment experience spans across all industries and are sized from Fortune 500 companies to small start-ups.

Upon completion of the penetration test, our security engineers will meet with you and provide an analysis that includes a detailed plan with recommendations for strengthening your security posture.

CBTS Infrastructure Portfolio

Network Infrastructure

Compute Solutions

Data Management Solutions

Security Solutions