

itek External Penetration Testing

Overview

The External Penetration Test is a network security analyst-supported, full scope attack against client computing resources available via the Internet. This includes systems such as web servers, home banking systems, mail servers, and other network assets. The goal of the test is conclusive identification of those vulnerabilities that could allow an attacker to gain unauthorized access to components within the client's network.

An external penetration test consists of four distinct phases: Scanning, Fingerprinting, Vulnerability Mapping, and finally Exploitation. Each phase builds upon the information gathered during the preceding phases to better understand where there are weaknesses in the network infrastructure that would provide unauthorized access to the target system or network.

Deliverables

The client receives a documented assessment of:

- Results of all tests performed
- Identified Vulnerabilities
- Vulnerability Assessment
- Recommendations

Variations

- Black Box: No information other than external IP addresses is disclosed to tester.
- Grey Box: Tester is provided with complete description of infrastructure and applications
- Crystal Box: Tester is provided with complete knowledge of environment and supplied with User, Administrative and Service credentials

Get Protected Today

For a customized testing plan designed to meet the needs of your business, contact your US itek Sales Representative at 716-447-7000 or by email at Sales@USitek.com.

