**APPLICATIONS**

- Identifying and prioritizing security risks.
- Identifying higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities.
- Identifying vulnerabilities that may be difficult or impossible to detect with vulnerability scanning alone.
- Assessing the magnitude of potential business and operational impacts of successful attacks.
- Testing the ability of network defenses.
- Identifying risk full end-user behavior.
- Safely simulate attacks on your network to uncover security issues.
- Other: test security controls, track mitigation efforts, manage phishing exposure, and audit web applications.

**INTENDED FOR**

- Law firms and solicitors.
- Financial institutions.
- Insurance companies.
- Healthcare providers.
- Investigative companies.
- Brokerage.
- Government agencies.
- Information driven wholesale and retail enterprises.
- International operating enterprises.

**Penetration Testing**

A penetration test is an authorized attempt to test the strength of an organization’s information security chain. Under controlled circumstances, system vulnerability exploits are being identified and utilized to try to compromise computer- and network- systems. However, without the intention of actually harming the system.

More specifically, penetration testing encompasses attacks of a technical nature on a computer system with the intention to gain access to the system, and control its functionality and data. This is done in the same way a hacker with malicious intent would. A penetration test provides insight into the organization’s defenses that were sufficient and the ones that were defeated or circumvented.

Penetration testing can also be utilized to validate the efficiency of in-place command-, control-, and security- mechanisms, as well as end-users’ compliance with information security policies.

**Objective**

The main objective of penetration testing is to determine if an automated information system is vulnerable to attack by a hacker, or person or organization with malicious intent. Penetration testing typically includes network security testing and application security testing, as well as controls and processes around the infrastructure.

**Vulnerability scanning VS penetration testing**

Penetration testing distinguishes itself from general vulnerability scanning but the two phrases are commonly interchanged. However, their meaning, implications, and objectives are very different. A vulnerability scan only identifies and reports vulnerabilities. Whereas a penetration test emphatically attempts to exploit the identified vulnerabilities to determine whether unauthorized access or other malicious activity is possible. This way, certain information security issues can be discovered that might be difficult to find using manual analysis or vulnerability scanning techniques alone.