EXTERNAL PENETRATION TESTING OF INFRASTRUCTURE

Standard infrastructure consists of a number of devices, most of which, if not all play a critical role in your information security.

Many publicized security incidents have shown that simply leaving one of these devices unsecured, missing updates, or weak passwords can lead to complete compromise of the systems.

Regular testing of the entire infrastructure is a strategic step not only to protect your data, but also to improve overall security in your company.

SERVICE OVERVIEW

The purpose of the external penetration test is to identify security vulnerabilities and misconfigurations in your external infrastructure in order to prevent attacks by real hackers.

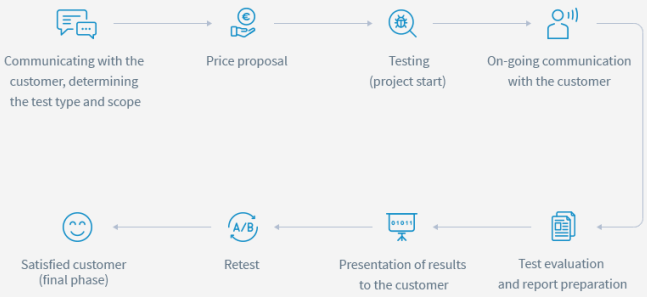
The test is carried out from the external environment and focuses on all systems and applications available from the Internet and verifies whether it is possible to exploit vulnerabilities in order to leak data, obtain higher privilege or execute an external/malicious code.

We manually review each identified vulnerability and we try to use it to compromise the target systems, or to exfiltrate sensitive data.

Upon completion of the testing, you will get a clear, prioritized vulnerability report along with an estimate of the technical risk the vulnerabilities pose. The report does not contain any "false-positive" findings, but only verified vulnerabilities and recommendations on how to remove them. On request, the results can be presented at a joint meeting.

The test can be performed using the BLACK BOX (no information about the tested infrastructure), GRAY BOX (partial information about the tested infrastructure) or WHITE BOX (all necessary information about the tested infrastructure) method.

The cost of the penetration test depends on the depth of the tests, the size and complexity of the tested infrastructure. The price is determined by mutual consultation with respect to other customer requirements (testing outside operation time / working hours, etc.).



DETAILED OVERVIEW OF THE SERVICE

For an external test, the usual goal is to get access to the internal infrastructure, focusing in particular on security perimeter devices (routers, firewalls, IDS, WAF). Another frequent goal is the exfiltration of sensitive data, such as emails, data from databases and internal and external portals.

We use a methodology that consists of the following phases:

- Determining the scope of testing

- Survey and enumeration of servers and other devices (if scope is not specified in advance)
- Mapping and service identification
- Vulnerability analysis
- Exploitation
- Escalation of privileges
- Reporting

Each test is tailored to the particular tested environment. We use a checklist to ensure that all important steps are addressed. The testing methodology can be adapted to security standards such as OSSTM.