INTERNAL PENETRATION TESTING OF THE INFRASTRUCTURE

While most networks are relatively well protected from external networks, the opposite is true in the case of internal networks. Security incidents in internal networks have the potential to have a much greater security impact as the attacker can be an employee, who knows the environment.

Apart from such employee, the attacker can be anyone (hacker, external contractor, etc.), who has gained access to your internal network.

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 internal 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 internal environment and focuses on all systems and applications available on your internal network, and verifies whether it is possible to exploit vulnerabilities in order to leak data, obtain higher privilege or execute an external/malicious code.

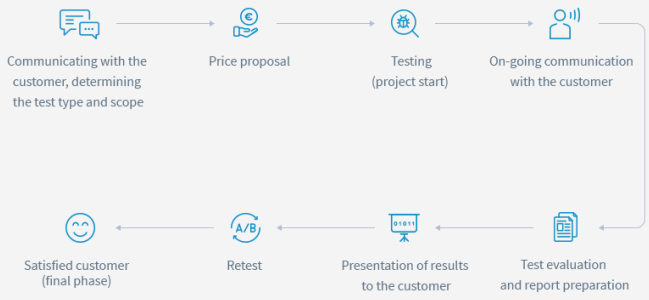
We manually review each identified vulnerability, and we try to use it to compromise the target systems or to exfiltrate sensitive data.

Upon completion of the testing, you will get a clear, prioritized vulnerability report along with an estimation of the technical risk that 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.

Testing can be done remotely using a PWNbox that we send to our customers. This device can be easily connected to an existing infrastructure. PWNbox creates an encrypted connection to our security experts, allowing them to work remotely and thus reduce the cost of the test.

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



DETAILED OVERVIEW OF THE SERVICE AND METHODOLOGY

Due to the complexity of information systems and networks, an attacker can find vulnerabilities in various components of your infrastructure, from network infrastructure issues and software without applied security patches, to system misconfiguration and vulnerabilities hidden in tailor-made applications.

The test can be performed from the perspective of an attacker with access to an internal network without login details, or from the perspective of an employee with restricted access to the domain.

An internal penetration test reveals vulnerabilities that can sometimes be combined to achieve a set goal, such as obtaining direct/privileged access to data or another network that is used to manage the environment or take control a domain administrator account.

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
- Pivoting
- Reporting

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