INTERNAL PENETRATION TEST (ASSUME BREACH)

Test your infrastructure's resilience against modern advanced attackers

Modern attackers continue to breach companies, utilizing continuously evolving techniques. It is therefore imperative for organizations to start assessing the internal security instead of the perimeter defences and adopt an "Assume Breach" mentality.

Improsec evaluates your security posture and protection of critical assets when your external perimeter has been breached. We will assess the security state on a specific environment or entire infrastructure from the viewpoint of an attacker having gained internal foothold, or an attack from a malicious insider.

Value

- Test your infrastructure's resilience against modern attackers
- Evaluate your security posture and protection of critical assets when your external perimeter has been breached or you have a malicious insider
- Identify misconfigurations, known vulnerabilities and insufficient technical controls on the internal systems and network

Product

The deliverable of the analysis is a written report containing the following:

- A non-technical section with an Executive Summary for management and decision makers
- A technical section including detailed observations and tangible recommendations to improve the security level and hardening of the infrastructure

Method

Based on our specialized knowledge of hacking and techniques to compromise systems and networks, we apply Post Exploitation techniques, in which typical misconfigurations and vulnerabilities in Windows Enterprise Environments are discovered and exploited in the same manner as modern attackers compromise organizations.

Depending on the maturity of your organization the test can be performed with the sole purpose of identifying misconfigurations and vulnerabilities that will lead to an enterprise security breach. Additionally, we can also assess your Blue Team's capabilities in detecting well-known attacker techniques used in a cyber security breach. In the latter assessment, attack vectors such as Privilege Escalation, Credential Theft and Lateral Movement can be emulated in close sparring with the Blue Team, to identify potential gaps in their ability to detect such actions.

Indicators of Compromise, both in network traffic and in system memory, may be provided along the test, if relevant for the Blue Team to train their detection capabilities.

An Assume Breach test can therefore be a good alternative for an organization wanting to assess their detection capability, but do not want to perform, or do not have the maturity for, a full scope Red Team test.

The test is carried out with a starting point of a domain-joined computer provided by you along with non-privileged user credentials.

Involvement

The delivery requires minimal involvement of your technical staff.