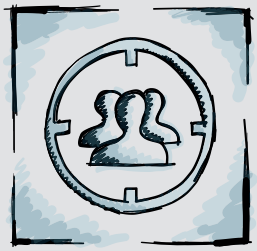
RED TEAM TEST

Test your organization's resilience against modern advanced attackers



Modern advanced attackers continue to breach companies, utilizing continuously evolving techniques. It is therefore imperative for organizations to start assessing their detection capabilities and resilience against modern advanced attackers.

A Red Team Test is as a simulation of a real-life attack on the organization, where the attacker uses a variety of advanced attack techniques that are targeting weak processes, technology, people and insufficient physical protection, to gain access to critical assets of the organization.

The engagement is defined with a wide scope, to reflect real-life attack vectors.

Value

- Test your organization's detection capabilities and resilience against modern advanced attackers
- Evaluate your security posture and protection of critical assets in your organization
- Identify weak or insufficient defence mechanisms
- Provide the IT security organization with a first-hand experience of dealing with an ongoing attack

Product

The deliverable of the test is a debrief workshop and a written report. The report contains 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 your organization's detection capabilities and resilience against modern advanced attackers

Method

Red Team engagements is a stealth operation. Just as a real attacker, we will utilize discrete techniques to move around in your organization's networks and attempt to be undetected. This will challenge your Blue Team and will put your implemented defence mechanisms to a realistic test.

Red Team engagements are always tailored to the targeted organization. This includes both cooperating with you about the scope and target(s) for the engagement, identification of relevant threat actors and agreeing on an engagement plan and attack scenarios.

The engagement will normally be divided into the following phases:

- Initial Reconnaissance - we utilize passive and active techniques to gather information about the organization and identify possible attack vectors
- Initial Compromise and Establish Persistence – we gain initial access to your network(s) using social engineering attacks on select employees, physical on-site entry or by exploiting vulnerable systems accessible from the Internet
- Internal Reconnaissance and Post Exploitation – we expand our attack to internal networks, where our specialized knowledge of hacking and techniques to compromise systems and networks is used to gain access to internal systems with the purpose of identifying and exploiting the defined targets
- Data Exfiltration and Mission Completion – when target(s) has been compromised we exfiltrate data or otherwise produce proof of compromise as per scope and target agreement
- Debrief Workshop – we host a debriefing workshop with management, security team and involved Blue Team members from your organisation or designated third party. We will walk through the engagement from our (the Red Team's) perspective and present the timeline and our performed actions. We will also share our perception of detecting or mitigating actions performed by the Blue Team during the engagement. This will enable the Blue Team to identify potential gaps in their ability to detect such actions and help to improve processes, procedures and/or technology

Involvement

During the engagement on-going involvement of your management and technical staff is required.

improsec

Improsec A/S
www.improsec.com
Telephone: (+45) 5357 5337
Email: info@improsec.com