Red team assessment is an advanced security test that companies take to simulate a tailored, full-scale attack on your organization. It gives a holistic and bigger picture of your organization’s security from an attacker’s perspective. The process is designed to address the needs of complex organizations that handle a variety of physical, technical and process-based assets.

**Why Conduct a Red Team Assessment?**

The main purpose of carrying out a red team assessment is to show how real-world hackers can integrate unrelated exploits in order to achieve their goal. It effectively shows how sophisticated hackers can bypass even the strongest firewall. It also tests the ability of your organization to detect, safeguard and respond to an attack.

Whereas a penetration test provides you a comprehensive list of system vulnerabilities and proposes improvements, a red team assessment accurately measures how prepared your company is to an attack.

Because of its highly advanced and targeted nature, this assessment is suited more for organizations that regularly conduct penetration tests and believe that they have already fixed majority of their vulnerabilities.

**How to Conduct a Red Team Assessment?**

You will need the services of a read teaming consultancy that can effectively conduct the test for you. Generally, it includes the following steps.

1. A dedicated team works with you to outline your goals, discuss elements of scope and note down any prerequisites before the assessment starts.
2. The team uses a combination of technical knowledge, threat analysis, physical analysis and human analysis to test your organization and looks for ways to achieve the goal.
3. Throughout the assessment process, the team communicates and provides feedback.
4. The client receives a detailed report in the end which elaborates on the methods used and how the team achieved the goal.

**Some Common Red Team Tactics**

Let’s look at some common ways your red team assessors go beyond the conventional assessments.

**Network Service Exploitation**

By exploiting misconfigured or unpatched network services, the attacker gets access to sensitive information or networks that were not accessible earlier. They often leave a persistent back door so that they can access it again if the need arises.

**Social Engineering**

With a few phone calls and phishing emails, it gets much easier to extract required information and achieve the goals. This is usually the first tactic in a chain of complex attacks that ultimately lead to the goal.

**Application Layer Exploit**

An attacker often looks foremost at web applications of an organization. By exploiting vulnerabilities in web applications such as SQL injection and cross-site scripting, they can get a foothold for executing further attacks.

Get yourself assessed by a team of professionals for a thorough analysis of your organization’s security.

Get in touch with us today!