Red Teaming

What is it?

Red Teaming is the next step in Cyber security assessments. It is a full-scope, multi-layered attack simulation aiming to measure how well the whole organization – i.e. people, networks and applications, and physical security controls - can withstand an attack from a real-life adversary. It is designed in such a way that it can also test the organization's detection and response capabilities, by attempting to gain access to sensitive information in any way possible, and as stealthily as possible.

Who is it directed at?

Organizations with a mature security level can greatly benefit from Red Teaming as they will be able to test their overall security posture against real word (advanced) attack scenarios. Red Teaming will reveal vulnerabilities and risks using a wealth of tools, techniques and capabilities specialized in many areas such as financial systems and services, core banking, web frameworks, malware analysis and creation, botnet tracking and many, many social engineering techniques.

Why is it important?

The new Cyber security era has driven attackers in using more specialized and advanced techniques in order to achieve their goal. Red Teaming helps a business remain competitive while securing its interests and assets, by leveraging real attack cases that combine all possible ways (people, physical, technical) to gain access to organization's assets.

Where is it taking place?

A Red Team will attack and exploit every possible entry point by combining advanced exploitation tactics, advanced social engineering attacks and physical security attacks to assess all key areas of security; Technology, People and Physical. Red Teaming scenarios can be specifically designed based on the organization's needs and help to assess: a) the physical security of buildings, offices, processing areas and warehouses, spotting weak entry points and ways that intruders can access restricted areas, b) any established security procedures and staff's awareness against social engineering attacks (physical and cyber) and c) networks, applications and appliances, as in traditional security assessments but in a more target oriented way.

When is it going to make an impact?

Red Teaming is not an instant gratification exercise and the testing process usually takes several weeks to complete, usually from 4 to 6 weeks along with the internal system attack, which probes the network and identifies assets of interest such as key systems and critical data.

How will it affect your business?

A red team considers the full ecosystem. Many organizations are building red teams in-house to improve security; some hire outside help. The main reason behind hiring a red team from outside is because it can grow and improve along with new defenses and tactics while experiencing different environments and attack situations. As security improves, so do the skills of red teamers. Offensive experts and defenders can attack one another, which will eventually improve enterprise security. External teams are also easier to justify from a budget perspective. Overall, the pros argue a full external red team can help prepare for modern attackers who will scour businesses for vulnerabilities and exploit them.

.