RED TEAMING

INTRODUCTION

A global telecoms company wanted to evaluate and test their existing physical security arrangements. A plan to perform red teaming was formulated through surveillance, research and social engineering to infiltrate both sites at different times of the day and night. The objective was to penetrate as deep into the premises as possible using non-violent methods. As a result of red teaming, full access was gained to both the sites. The activity enabled the company to identify the loopholes in its internal security procedures in close counters.

In another case, a retail giant was concerned about the massive rise in the use of social engineering attacks to help cyber attackers and criminals gain access to companies. The company wanted perform red teaming at their premises. After the initial consultation meeting with the business to understand their operating procedures and culture, a plan for red teaming was formulated. The activity helped the business understand the gaps in its internal security system and fix them at the earliest.

WHAT IS RED TEAMING?

Red teaming is process of testing the cyber security level of an organization by simulating real-world attacks by using the Techniques, Tactics and Procedures (TTPs). The role of the red team is to simulate an attack on the target organisation and to test the security posture with the help of a real-world attack scenario focused on revealing potential threats to the critical data.

THE RED TEAM AIMS TO:

Find out the vulnerabilities in network, applications, endpoints, and processes.

Document any weaknesses in your incident response policy and procedures.

Determine the effectiveness of your security monitoring and alerting.

Prioritize areas for improvement to assist stakeholder decision making around investing in further strengthening of security.

HOW DOES RED TEAMING WORK?

01

Goal-mapping – Set the goals for red team operations.

02

Target reconnaissance - As soon as red team goal is finalized, they will begin collecting the necessary information of the systems to be targeted, including networks, web applications, employee portals, and even physical spaces.

03

Exploit vulnerabilities – Red team will now start exploiting the vulnerable point inside the whole system based on the information collected during recon.

04

Probing and escalation – Post exploitation the red team will try to move within the network to find out critical data, possible more vulnerabilities, and escalation possibilities.

05

Reporting and analysis – Once the attack simulation is complete detailed report is prepared to decide the path ahead based on the results of red team activities conducted.

BENEFITS OF RED TEAMING:

02

Risk identification and susceptibility of attack against important business information assets and systems.

03

Organization's ability to detect, respond, and prevent sophisticated and targeted threats before they take place can be assessed and necessary actions can be taken.

01

Prioritization of cybersecurity practices and expenses based on the results of the red teaming activities become more cost-efficient.

04

Activities for training and awareness regarding the cyber security for the employees from the executive level down to rank-and-file workers can be exercised.

NEED FOR RED TEAMING

Red teaming provides wider perspective towards the security of an organization whether it is public or private, small scale or large scale. Even if the company doesn't work in technology or isn't necessarily IT-focused, it's still likely that red teaming will be useful in revealing how hackers might be able to access the personal sensitive information.

Smaller firms who cannot afford to have in-house red team can simply contract out the red teaming process, using experienced cybersecurity and compliance partner.

SKILLMINE CYBER SECURITY TEAM

Skillmine
Technology • Consulting • Services

#46/4, Novel Tech park,
Kudlu Gate, Bangalore
Karnataka-560 068

+91 9920663515
www.Skill-mine.com
info@Skill-mine.com

India | KSA | UK | USA

Stay connected