Red Teaming

Stop the breach before it starts!

Do you feel confident about the cybersecurity of your company?

Although vulnerabilities may seem small on their own, when they're tied together to form an attack path, they can cause significant damage. Our Red Team demonstrates how a real-world adversary might attack a system and how that system would hold up against an attack. After a Red Teaming exercise, you'll have a better understanding of your organization's security posture as it relates to specific threat actors attacking a set of defined assets. Most importantly you'll know where to focus your efforts for improvement.

How does Red Teaming work?

It's a technique that combines information gathering, blackbox penetration testing, and social engineering. The goal is to simulate an attack, exactly how real hackers would do it. Therefore, you don't test just your system unit, but the whole infrastructure, together, with your own employees. So the positive thing is that your IT/ IT Security Team can also test if they would be able to detect an attack. "This is one of the best ways to practice the procedure, and better yet, with trusted hackers on your side!"

Red Team exercises are conducted to practice and foster security awareness and communication between teams and identify potential deficiencies.

A Red Team exercise covers three aspects of security:

People/Cultural Vigilance

A company's own employees are often the weakest link. We can test awareness of social engineering and physical security controls like gates, locks, sensors, etc.

Technology/Assets and Controls

Targets existing and/or planned technology assets or systems, configurations, and vulnerabilities Processes/Security Response.

Processes/Security Response

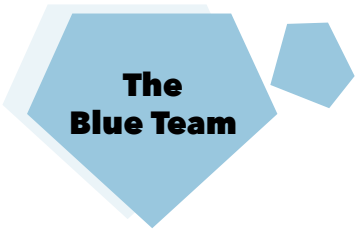
What actually happens in an attack? How will your teams respond? How will they escalate and coordinate with other teams to contain the incident?

To get started, let's take a look at the main differences between standard penetration testing and Red Teaming:

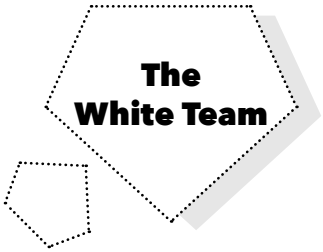
PENETRATION TESTING	RED TEAMING
Broad testing - Find as many vulnerabilities as possible.	In-depth testing - Find the one major vulnerability to get into the system and take full advantage of it to achieve the objective.
A short period of time	A longer period of time
The goal is to identify the vulnerabilities of a specific area (unit).	The goal is to test the resilience of the entire company's defenses.
Clearly defined scope of the project (several systems or applications)	The scope of the project is to test the entire company's security and vulnerabilities.
The IT department knows about the testing and closely cooperates with the security/ pentesting company.	The scope of the project is to test the entire company's security and vulnerabilities to achieve the objective and identify aspects that could be misused.
To test the system unit.	The goal is to test the IT department's ability to recognize and defends against any random cybersecurity attack.
Applications are tested according to the OWASP methodology.	Is not possible to follow any methodology .

This is a game of 3 teams, let's meet the players.

This team is composed of senior ethical hackers whose goal is to infiltrate the company in any way possible.



This is the team of professional security or infrastructure protectors. They're usually the client's system administrators, whose goal is to detect attacks. In order to simulate a real attack, the Blue Team doesn't have a clue about the planned attack.



This is a small group of people from the company who ordered the Red Teaming and who are actually aware of the attack.

So how does it work? Let's take a deeper look in to the individual phases of Red Teaming:

1. Information Gathering (OSINT)

The aim of this introductory phase is to gather as much information as possible. The sources are usually publicly available (databases, registers, search engines, social networks, etc). To gather this kind of information, we use the Open-source intelligence (OSINT) framework.

2. External Attack of the Infrastructure

After the information is gathered, the next phase begins by starting an attack on the infrastructure without any physical access.

Black box penetration testing
We examine the functionality of the infrastructure without peering into its internal structures or inner workings. The main goal is to get any access to the internal infrastructure (usually by using a compromised server).

Social engineering
(without the need for physical access)
In this phase, we use all of the methods of social engineering, except for physical infiltration techniques (i.e. spear phishing), with specially modified malware that will allow us to get into the internal network.

3. An Infrastructure Attack with Physical Access

In this part, we implement various situations in which employees could get caught up. For example, we've used the "baiting" attack by which we spread our USB flash drives around the company. In addition to standard USB sticks, we also dispose of so-called "rubber duckies", which are improved by our firmware.

4. Physical Intrusion (Getting Someone into the Building)

In this part, the task is to infiltrate the system by getting a member of the Red Team inside of the company. The goal is usually to get into their network, steal sensitive documentation or hack unlocked PCs (the "rubber ducky" tactic). This is one of the fun parts, though the potential results tend to be a bit unclear during the planning stage. As you can imagine, it also requires a great deal of creativity. Luckily, or unluckily rather, there are many ways to infiltrate a company. For example, someone could go in for a job interview, or even pretend that they are a delivery person with mail or other items to be dropped off.

5. Lateral Movements

In this case, we've already infiltrated the company's infrastructure by hacking a server, or based on "spear phishing"/"baiting", we're able to hack the employee's desktop. Now the task is to get from the unit server or desktop further into their network and obtain some sensitive data. By obtaining that sensitive information, we have fulfilled our task and at this stage, we inform the white team on how to communicate the steps we took. Usually, our job in the field is over at this point.

6. Final Report

The last stage is where we hand the client an in-depth report. The report usually consists of a detailed description of:

- **All of the tactics that we used**
- **The paths that we have tried (including the wrong ones)**
- **How we exploited the vulnerabilities**
- **Instructions on how to eliminate an individual vulnerability**

We then read out the report with the appropriate organization stakeholders to review each vulnerability that has been identified during the assessment. We answer any questions that the team might have about each vulnerability, and most importantly, we discuss mitigation/remediation strategies.

CITADELO

Protect what's important!

According to the Art of Cyber War, "The enemy does not care what systems were in scope for testing." So let Citadelo protect your weak points!

Contact our Sales Team (**sales@citadelo.com**) to learn more about Citadelo Red Teaming services, and start planning your improved cybersecurity today!

www.citadelo.com