# Red Team in Cybersecurity

## What is a red team

In a red team cybersecurity simulation, the red team acts as an adversary, attempting to identify and exploit potential weaknesses within the organization’s cyber defenses using sophisticated attack techniques. These offensive teams typically consist of highly experienced security professionals or independent ethical hackers who focus on penetration testing by imitating real-world attack techniques and methods.

### Why does your security team need it?

**Red teaming** is the act of systematically and rigorously (but ethically) identifying an attack path that breaches the organization’s security defense through real-world attack techniques. In adopting this adversarial approach, the organization’s defenses are based not on the theoretical capabilities of security tools and systems, but on their actual performance in the presence of real-world threats. Red teaming is a critical component in accurately assessing the company’s prevention, detection, and remediation capabilities and maturity.

## Benefits of the Red team

## Implementing a red team strategy allows organizations to actively test their existing cyber defenses and capabilities in a low-risk environment. By engaging these two groups, it is possible to continuously evolve the organization’s security strategy based on the company’s unique weaknesses and vulnerabilities, as well as the latest real-world attack techniques.

Through red team exercises it is possible for the organization to:

* Identify misconfigurations and coverage gaps in existing security products
* Strengthen network security to detect targeted attacks and improve breakout time
* Raise healthy competition among security personnel and foster cooperation among the IT and security teams
* Elevate awareness among staff as to the risk of human vulnerabilities which may compromise the organization’s security
* Build the skills and maturity of the organization’s security capabilities within a safe, low-risk training environment

### Red Team skill set

A successful red team must be devious in nature, assuming the mindset of a sophisticated adversary to gain access to the network and advance undetected through the environment. The ideal team member for the red group is both technical and creative, capable of exploiting system weaknesses and human nature. It’s also important that the red team be familiar with threat actor tactics, techniques, and procedures (TTPs) and the attack tools and frameworks today’s adversaries use.

For example, a Florida teenager recently used spear-phishing tactics as well as social engineering techniques to obtain employee credentials and access internal systems at Twitter, resulting in a high-profile breach of [more than 100 celebrity accounts](https://www.abc.net.au/news/2020-08-01/teenager-arrested-for-twitter-hack-that-targeted-celebrities/12515224).

A member of the red team should have:

* A deep awareness of computer systems and protocols, as well as security techniques, tools, and safeguards
* Strong software development skills in order to develop custom-made tools to circumvent common security mechanisms and measures
* Experience in penetration testing, which would help exploit [common vulnerabilities](https://www.crowdstrike.com/cybersecurity-101/common-vulnerabilities-and-exposures-cve/) and avoid activities that are often monitored or easily detected
* Social engineering skills that allow the team member to manipulate others into sharing information or credentials

# 5 open-source offensive security tools for the Red team.

### **1. Metasploit Framework**

The [Metasploit Framework](https://github.com/rapid7/metasploit-framework) provides a common, standardized interface to many services of interest to pen testers, researchers and red teams. It includes working with exploits and payloads, as well as auxiliary tasks that don't use a payload.

Vulnerability researchers historically wrote exploitation scripts or proof-of-concept code for exploits they discovered. This often lead to usability challenges because some scripts were minimally documented, included nonstandardized usage conventions, or were unreliable when it came to using them as a test harness to validate issues. The Metasploit Framework helped remedy these issues.

Metasploit is the de facto standard interface for working with [exploit code and payloads](https://www.techtarget.com/searchsecurity/feature/How-to-conduct-Linux-privilege-escalations). It normalizes how red teams and pen testers interact with exploit code. From the red team's point of view, it streamlines work by providing important services such as payloads -- i.e., [shell code](https://www.techtarget.com/searchsecurity/answer/What-is-the-relationship-between-shellcode-and-exploit-code) -- so the red team can focus on the vulnerability itself. For the tester, it likewise provides a standard way to interact so they can concentrate on the issue they're testing and not the minutia of running the exploit code itself.

### **2. Zed Attack Proxy (ZAP)**

The offense involves more than just being able to run exploits. Particularly with web applications, it's important to be able to see and manipulate requests that occur between a browser and a web server. One category of tools that facilitate this is attack proxies. These tools sit between a browser and a remote web server so users can examine and even manipulate traffic between those devices. Likewise, attack proxies often contain automated mapping and crawling tools, automated website scanning tools, and informational tools such as URL, hex, and Base64 encoders and decoders.

### **3. Browser Exploitation Framework (BEeF)**

An attack proxy is great for exercising the functionality of a remote website, but what if you want to attack a given user more directly? For example, to test the resilience of users' browser habits or test whether they would notice warning signs of being part of an attack chain.

One way to do this is by using [tools that hook one or more tabs](https://www.techtarget.com/searchsecurity/tutorial/How-to-use-BeEF-the-Browser-Exploitation-Framework) within a target's browser and provide some level of control to an attacker. This in turn can be used as a forward "staging area" by an attacker to gain further traction within an environment or move laterally. The [Browser Exploitation Framework (BeEF)](https://beefproject.com/) enables red teams to do exactly that.

### **4. Atomic Red Team**

The [Atomic Red Team](https://github.com/redcanaryco/atomic-red-team) project is a set of scripts that can be used to simulate attacker activity. The project provides a set of portable tests, each mapped to the [MITRE ATT&CK framework](https://searchcloudsecurity.techtarget.com/tip/How-to-use-the-Mitre-ATTCK-framework-for-cloud-security), which can be used to exercise protections and hardening strategies in an organization.

Atomic Red Team is a useful tool for red and blue team members. For the blue team, it's a helpful way to validate the controls protecting the environment. On the offense side, deconstructing attack techniques can help red teams understand how those techniques work and how to apply them.

### **5. Social-Engineer Toolkit (SET)**

One often-overlooked area is testing the resilience of users against manipulation, coercion and trickery. The [Social-Engineer Toolkit (SET)](https://github.com/trustedsec/social-engineer-toolkit) provides mechanisms to quickly create artifacts that might appear legitimate to a user and that can be used to test different scenarios. With it, red teams can send a legitimate-looking email to target users, attempt a [spear phishing attack](https://www.techtarget.com/searchsecurity/feature/New-evasive-spear-phishing-attacks-bypass-email-security-measures) containing malicious attachments, and [spoof SMS messages](https://www.computerweekly.com/news/252506611/Smishing-attacks-up-sevenfold-in-six-months).