Red teaming 101: An introduction to red teaming and how it improves your cyber security

Red teaming is an attack technique used in cyber security to test how an organisation would respond to a genuine cyber attack. It is done through an **Ethical Hacking team** or similar offensive security team.

The ‘red team’ that simulates the attack is often an independent cyber security provider, while the organisation’s defensive cyber security capability is known as the ‘blue team’. The blue team aren’t given warning of the exercise so that the organisation receiving the red teaming gains a realistic measure of its ability to respond to a genuine cyber attack.

In this post, the first in a short series on red teaming, we will look at how red teaming works and how it helps organisations understand the effectiveness of security controls when it comes to thwarting realistic attacks from common threat actors.

What is a Red Team?

A red team is a form of penetration test (pentest) that has a very different set of goals to the more traditional pentest. While a typical pentest focuses on finding vulnerabilities and potentially exploiting them within a predefined set of company systems, a red team is target-driven and seeks to gain access to predetermined objectives by exploiting relevant weaknesses anywhere within an organisation. It does not seek to provide an exhaustive list of vulnerabilities present.

The value of a red team is in simulating how an organisation could be targeted in a real world attack and testing how the blue team responds to such an attack. The tactics, techniques and procedures (TTPs) of a red team are modelled on real-world malicious threat actors, with the goal of highlighting gaps in the security response.

Unlike in a penetration test, the organisation’s security team is usually not made aware of the red team exercise. This serves to safely and realistically test an organisation’s capabilities to detect and respond to an attack. As the two teams get to work, the blue team has to respond to the evolving techniques of the red team and they in turn adapt to the blue team and attempt to evade the controls that are in place. It is through the teams learning about each other's tools and techniques that the organisation can get most real world value. An evolution of these techniques is to deliberately create a co-operative purple team, but that's the topic for another article.

How does a Red Team work?

Just as no two companies are identical, neither are two red teams; however, the standard attack path typically follows this chain:

Initial access → Persistence → Privilege escalation → Command and control → Objective → Exfiltration of data

The attack chain is often informed from a **threat Intelligence** report, identifying relevant threat actors which the red team should emulate, or from current trends seen in the wild (such as human-operated **ransomware**, campaigns), and through the company’s own assessment of its weaknesses. A particular threat actor could be simulated by using the techniques observed in the wild, targeting the same types of services. Alternatively their behaviour could be used as a baseline and adjusted to better suit the specific target.

The final attack may look something like this:

A list of company employee email addresses is obtained from social media and other open-source intelligence (OSINT) sources. A crafted phishing email is then sent to these addresses containing a lure and an attached document. When opened, this drops custom malware on the victims’ machines providing the red team with access to the corporate network.

Obtaining persistence through exploiting common machine misconfigurations/outdated software and hiding the custom malware somewhere where it is unlikely to be noticed by the security operations centre (SOC).

Exploiting and mapping the network, escalating privileges where required to grant further access while evading detection.

Identifying paths to predetermined objectives (e.g. a finance database) using privileged credentials to achieve those objectives.

Exfiltration of data from the target network to demonstrate the ways an attacker could remove sensitive information..

At any point in the assessment, the blue team may detect the malicious activity and terminate access. For example, the phishing campaign may be identified by an attentive user and reported. In these situations, a red team can adopt a ‘leg up’ where the target provides an initial foothold on the network without the need for the phishing campaign.

While this approach may seem counterintuitive, it serves to provide a more complete picture of an organisation's cyber security by allowing the red team to continue to the next step of the attack chain. An important philosophy in security is that you must assume controls will fail, and it is important to have layered security to mitigate and restrict the damage when they do. Many organisations unintentionally have an armadillo security model (hard on the outside, soft on the inside), and are shocked at the level of freedom an attacker has once any perimeter defences are bypassed.

With a sufficiently sophisticated social engineering campaign, an attacker will eventually succeed in persuading an employee to execute malware. When the internal network is compromised, there needs to be protection in place to limit the access of the attacker and to minimise the impact of the breach. This is where the leg-up grants a more complete picture of the target’s security. It shows what happens when individual protections fail and what the monitoring solution detects when attackers try to bypass them.

Red Team results

The test can last anywhere from weeks to months, but at the end the results are collated and a workshop is run with the blue team. The complexity of this workshop depends on the target. It can be:

- a high level summary of where they performed well and where they can improve;
- a technical review of each attack and counterattack between the two teams; or,
- or a set up for a larger “**find and fix**” project the company wants to launch on the back of the red team.

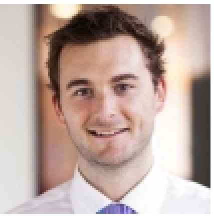
Red teams offer a means of measuring response to specific scenarios as business operations change. For example the ‘unattended laptop’ scenario which has changed, due to the dramatic shift to remote working in the pandemic, to a shared remote environment which has a different risk profile and possible attack paths. Red teams are ideal for companies that are keen to assess how good they are at preventing, detecting and responding to real world cyber attacks.

Related content

Asset & Wealth Management Revolution: Embracing Exponential Change

The asset & wealth management industry is accelerating at a rapid rate. Asset & wealth managers need to act now to survive and prosper.

Contact us



Kris McConkey

Cyber Threat Operations Lead Partner, PwC United Kingdom

Tel: +44 (0)7725 707360

in Email

Get in touch

First name (Required)

Last name (Required)

Job title (Required)

Company (Required)

Business email address (Required)

Please Click Here

☐ I'm not a robot

Submit

By submitting your information, you acknowledge that we may send you material relevant to your interests.
Please see our privacy statement for details of why and how we use personal data and your rights (including your right to object and to stop receiving marketing communications from us). To stop receiving marketing communications from us, click on the unsubscribe link in the relevant email received from us or send an email to uk_emailconsent@pwc.com.

Audit Consulting Deals Risk Tax Industries About us

Offices Media centre Careers Alumni Sitemap