**Red Team Methodology**

Red Teams exists alongside many other teams in the cybersecurity landscape. Blue Teams can work alongside Red Teams but are focused on improving system security from the inside. Purple Teams use a combination of adversarial and defensive approaches. Red Teaming, though, is one of the least understood practices in cybersecurity management, and many organizations are still reluctant to use the practice.

In this guide, we’ll explain exactly what Red Teaming is, and how bringing Red Team practices into your organization can help improve your security. Our goal is to show you how Red Teaming can dramatically improve the security of your IT systems.

**What is red teaming?**

Red teaming is a multi-layered, full-scope cyberattack simulation designed to test the effectiveness of an organization’s security controls. This includes networks, applications, physical safeguards, and even employees. As stated above, the purpose of conducting red teaming is to allow companies to understand how resistant they are to real-world hacking adversaries.

Your Blue Team will then be tasked with defending the attack as if it was a real one.

Red teaming is similar to ethical hacking, during which actors don’t attempt any actual harm but instead hack into systems to uncover vulnerabilities with the goal of improving defenses. Red teaming is based on the idea that a company can’t really know how secure its systems are until they are attacked. Rather than running the risk of real-world damage that may come from a genuinely malicious attack, simulating one first via red teaming will uncover an organizations’ vulnerabilities so they can be addressed before it’s too late.

**How does red teaming work?**



The best way to understand the details of red teaming is by looking at the process of how a typical red team exercise unfolds. Most red teaming simulations have several stages:

* **Goal-mapping:** Organizations will first set primary goals for their red team. For example, one goal may be to extract a particular piece of sensitive data from a particular server.
* **Target reconnaissance:**Once the red team is clear on their objectives, they will begin mapping out the systems to be targeted, including networks, web applications, employee portals, and even physical spaces.
* **Exploit vulnerabilities:**This is where the action in red teaming exercises really begins. Once the red team knows which attack vectors they’ll use, they will employ tactics such as phishing or XSS exploits to access your systems.
* **Probing and escalation:**Your red team will then try to move within your systems to achieve their primary goal, and determine if there are additional vulnerabilities to exploit. Red teams will continually escalate until the target is reached.
* **Reporting and analysis:**After the red team’s simulated attack is complete, you’ll go through a reporting and analysis process to determine the path forward. You’ll see how your blue (defensive security) team performed and which key vulnerabilities need to be addressed.

Experienced red teams use a wide variety of techniques to perform each of these steps. The main thing to consider when reviewing the attack is that small vulnerabilities in single systems can build into catastrophic failures when chained together. Real-world hackers will always be greedy and look to exploit more systems and data than they originally came for.

**Red teaming tools and common tactics**

When executed properly, red teaming will result in a mock full-spectrum attack on your networks, systems, and data. Red teams will use as many tools and techniques available to malicious hackers as they can. Some of the more common red teaming tools and tactics are:

* **Application penetration testing:** App-level pen testing is designed to identify application layer flaws such as cross-site request forgery, injection flaws, and weak session management.
* **Network penetration testing:** This type of pen test is for identifying network and system-level flaws. This includes misconfigurations, wireless network vulnerabilities, rogue services, and more.
* **Physical penetration testing:** You also need to understand the strength and effectiveness of physical security controls through real-life exploitation. Red teams may try to stroll past physical controls directly into server rooms or employee work terminals.
* **Intercepting communication:** To map your network or gain more information about the environment, red teams will circumvent common security techniques by hacking communications such as internal emails, texts, or even phone calls. to.
* **Social engineering:** Red teams will try to exploit weaknesses in people within your organization by relying on human nature. They’ll try to manipulate employees into giving up access credentials via phishing, phone calls, text messaging, or falsifying an identity on-site.

Red teaming is a full-scope, multi-layered attack simulation designed to measure how well your people, networks, application, and physical security controls can withstand an attack from a real-life adversary. Therefore, a strong red team will employ an array of tools, tactics, and strategies to breach your defenses.

**Red teaming benefits**

At the broadest level, the value of red teaming is that it provides a comprehensive picture of cybersecurity within your organization. Red teams should be as creative and resourceful as real-life malicious actors who will inevitably probe and test every square inch of the potential attack surface.

The assessment doesn’t conclude after initial vulnerabilities are discovered and exposed, however. The exercise will extend towards re-testing, lateral movement, and remediation phases that will test just about every aspect of your cybersecurity strategy. You’ll be able to completely assess your capability to detect, remediate and prevent targeted attacks.

In fact, the real work typically begins *after* a red team intrusion, when you’ll perform forensic analysis of the attack and formulate ways to mitigate vulnerabilities. Red teaming also offers several other benefits when used in conjunction with other threat analysis techniques:

* **Identification** of the [risk and susceptibility of attack](https://www.varonis.com/products/datadvantage?hsLang=en) against key business information assets and technology systems.
* **Simulation**of techniques, tactics, and procedures (TTPs) used by genuine threat actors in a risk-managed and controlled environment.
* **Assessment** of your organization’s ability to detect, respond, and prevent sophisticated and targeted threats before they take place.
* **Encouragement** of close engagement with internal incident response teams to provide meaningful mitigation and comprehensive post-assessment debrief workshops.
* **Compliance**assistance; strengthen your cyber defense posture to be up to par with relevant frameworks such as CCPA, FISMA, or HIPAA.
* **Training** and cybersecurity education of your entire staff, from the executive level down to rank-and-file workers.
* **Performance**-metric gathering with regards to cyber defenses without the downside of a real-life attack. You’ll collect measurements that are relevant to real-world performance.
* **Prioritization** of cybersecurity initiatives and expenses based on the results of the exercise. Become more cost-efficient and address the most pressing needs first.

These are just a few of the main benefits that red teaming provides. Next, we’ll cover how to decide if your organization needs red teaming and who benefits.

**Who needs red teaming?**

Just about any company and organization – public or private – can benefit from some form

of red teaming. Even if your company doesn’t work in technology or isn’t necessarily IT-focused, it’s still likely that red teaming will be useful as hackers might be after the personal sensitive information of customers in data stores or internal employees.

For smaller firms, it’s understandably more costly and difficult to deploy the significant resources needed for comprehensive red teaming exercises. In this case, it’s typically worthwhile to contract out the red teaming process, using experienced cybersecurity and compliance partner.

**Red teaming considerations**

Though almost every company can benefit from red teaming, the best time to undertake this practice –and how frequently to do it – will vary according to your sector and the maturity of your cybersecurity defenses.

Here are some key considerations to make when planning your future red teaming exercises:

* **Automation:**You should already be engaged in activities such as asset investigation and vulnerability analysis. Your organization should also be combining automated technology with human intelligence by implementing regular, [robust penetration testing](https://www.varonis.com/blog/varonis-six-part-guide-to-penetration-testing?hsLang=en). Process automation will make it easier to conduct, and measure the results of, red teaming.
* **Preparation:** Once you’ve completed several business cycles of vulnerability and pen testing, you can start red teaming. Only after you’ve completed these preparations can the total value of red teaming be realized. Attempting to bring in red teaming before establishing a solid and consistent cybersecurity baseline will produce very little value.
* **Comparison:**To be truly effective, the insights produced by the red team need to be given context by comparing against previous penetration testing and vulnerability assessment activity.

We’ve mentioned penetration testing as both a tactic and key consideration within the realm of red teaming. Therefore, it’s important to understand the differences and similarities between red teaming and pen-testing.

**Red teaming vs. penetration testing**

Though pen testing is important, it is only one part of what a red team does. Red team operations have broader objectives than pen testers, whose goal is often just to get access to a network.

Red team exercises are designed to emulate a more real-world advanced persistent threat (APT) scenario and result in reviewing defensive strategies and detailed risk analysis. Penetration testing is only a small part of red teaming. Red teaming includes evasion and persistence, privilege escalation, and exfiltration, whereas penetration testing exercises only the first part of the[cyber kill chain](https://www.varonis.com/blog/cyber-kill-chain?hsLang=en).

**Time box**

This is the time frame in which each activity is conducted. For pen testing, the time box is extremely narrow – typically less than one day. For red teaming, the time box can be extended over multiple days, weeks, and even months.

**Tooling**

Pen testing and red teaming also employ different tools and technologies. Employees will typically conduct a pen test using commercially available software. Red teams are encouraged to use any tool, trick, or tactic in their arsenal and think creatively while attempting to breach systems.

**Awareness**

This is one of the most distinct differences between Pen Testing and red teaming. With Pen Testing, most of your employees are aware of what’s taking place. But red teaming exercises require that your organization is completely unaware to get a real picture of your cyber defenses.

**Vulnerabilities**

Which vulnerabilities are attacked will also differ. In pen testing, known vulnerabilities are specified and targeted to see how well-defended they are. Red teams won't just exploit a single vulnerability, however. They’ll also seek out new ones in your network and attempt to move laterally.

**Targeting**

When conducting penetration testing, your test target vulnerabilities will be narrow and pre-defined. You’ll target a specific firewall or password system, for instance. Red team targets are more fluid, ranging across multiple domains and networks.

**Testing**

Penetration testing involves testing each system independently, one at a time, and is a much more siloed approach than red teaming. When implementing red teaming, all your systems are targeted simultaneously throughout the time box, giving you a better idea of your plan of defense and response to a real hack.

Now that you’re informed about what red teaming is  (and what it isn’t)it’s time to get up-to-speed on what’s involved in the process and preparation.

**What’s involved in a red team exercise?**

To get the most out of a red team exercise, you’ll need to make the right preparations. This includes knowing who and what will be involved. The systems and processes used by each organization are different, and a high-quality red team exercise needs to be specifically tailored toward finding vulnerabilities in your systems. For that reason, it’s important to understand several factors.

**Know what you’re looking for**

First, it’s important to understand which systems and processes you want to test. It’s possible that you know you want web application testing, but you don’t have a sense of what that means for you, and which of your other systems are integrated with your web apps. You need to understand your systems well and patch any obvious vulnerabilities before you start a red team exercise.

**Know your network**

The better able you are to quantify your testing environment, the more accurate and specific your red teaming exercises will be. Knowing the technical specifications of your network will also make post-analysis more effective and valuable.

**Know your budget**

Red teaming can be performed at various levels of intensity, and a full spectrum simulated attack on your network can prove costly, as you'll need to include social engineering and physical intrusion for a comprehensive exercise. For this reason, it’s important to understand how much you are willing to spend on your red team exercise and to set your scope accordingly.

**Know your risk level**

Some organizations tolerate a high level of risk as part of their standard business procedures. Others, and particularly those working in industries in which there are detailed and complex compliance requirements, need to have far lower risk tolerance. When conducting a red team exercise, it’s important to focus on risks that present consequences for your business.

**Red teaming examples**

A great way to understand the basics of red teaming is to review some examples of how exercises take place and what’s involved. Below are four different red team scenarios that illustrate what you can potentially expect.

**Social engineering:**After online research of individuals within your organization, the red team then attempts a social engineering attack. Legitimate-seeming emails or social media messages are sent to try and trick employees to give up their access credentials or download malware. If the red team does manage to fool someone, they’ll continue to move about the system undetected indefinitely while testing even more vulnerabilities along the way.

**Filtering bypass:**The red team will test your web-based vulnerability by attempting to overcome your file filtering system using an SQL injection. During a filtering bypass exercise, red teams will likely exploit any software or safeguards that haven’t been patched because external attacks are easier when the operating systems or programs are outdated. When complete, these scenarios relay exactly how many vulnerable, unpatched programs or operating systems are present in a network.

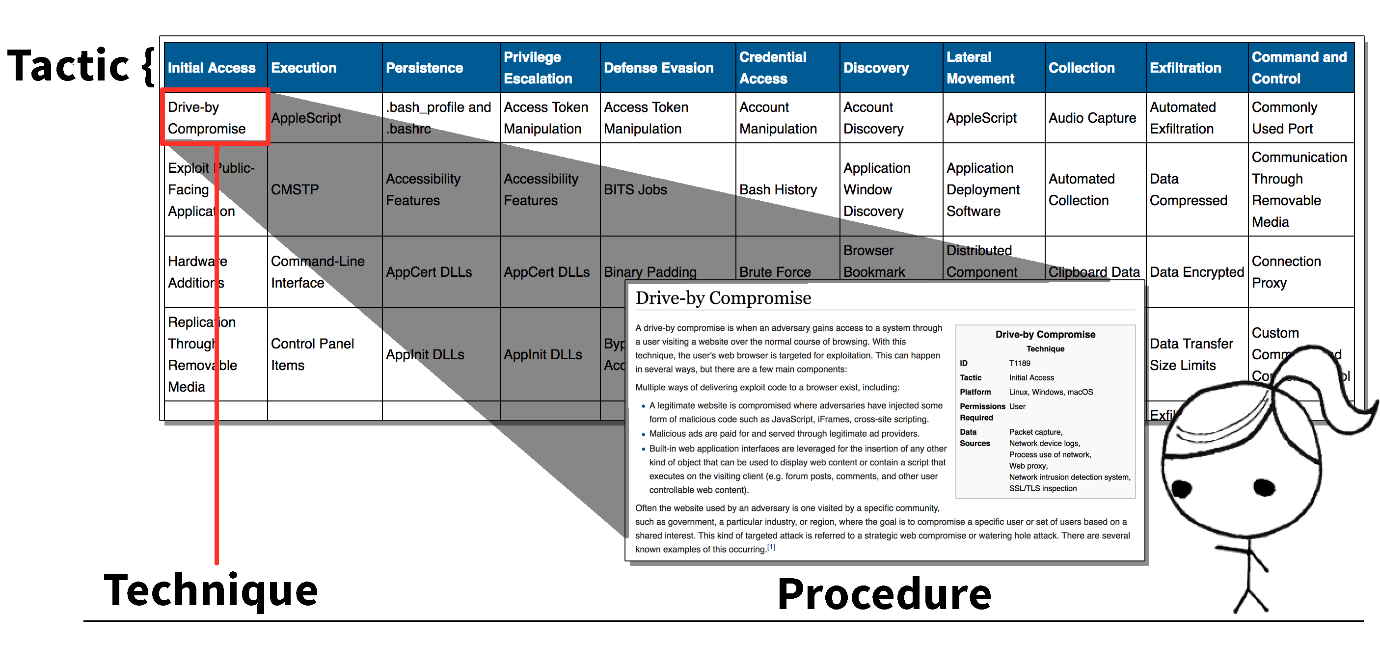
**Physical breach:**During the reconnaissance phase, red teams will closely examine and monitor your physical security measures in relation to your IT systems. They’ll see who comes and goes and how they enter. They’ll then attempt to physically enter your server room by using a cloned employee badge or building PIN code acquired via social engineering efforts. And in the case of extremely weak physical access controls, red teams may even be able to walk the premises undetected and unimpeded.

**Application exploit:**Web applications are often the first thing attackers encounter when looking at a network perimeter, thereby presenting them with the most immediate opportunity of compromise. The red team will attempt to exploit web application vulnerabilities through tactics such as cross-site scripting, SQL injections, and cross-site request forgery. Once the ethical hackers gain control over a single web application, they’ll use it as a springboard for further attack exercise activities.

These are simply a few potential scenarios of how red teaming might look at your organization. You’ll want to work directly with your cybersecurity or red team partner to create and customize exercises and scenarios that best suit your organization.

# MITRE ATT&CK[¶](https://threatexpress.com/redteaming/mitre_attack/#mitre-attck)

MITRE’s Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary’s lifecycle and the platforms they are known to target. ATT&CK is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying defenses work as expected.



**ATT&CK is broken into Tactics, Techniques, and Procedures**

* **Tactics** are the tactical goals a threat may use during an operation.
* **Techniques** describe the actions threats take to achieve their objectives.
* **Procedures** are the technical steps required to perform the action.

This frameworks provides a classification of all threat actions regardless of the underlying vulnerabilities.

Red teams can emulate realistic TTPs through research and experience. Much of this information has been complied in to ATT&CK. ATT&CK can be thought of a menu of TTPs. Red teams can use this to ensure they have a comprehensive set of threat TTPs, and blue teams can use this to build a scorecard of how well they are able to defend against various TTPs.

## References[¶](https://threatexpress.com/redteaming/mitre_attack/#references)

| Description | Link |
| --- | --- |
| ATT&CK | <https://attack.mitre.org/wiki/Main_Page> |
| PRE-ATT&CK | <https://attack.mitre.org/pre-attack/index.php/Main_Page> |
| ATT&CK Navigator | <https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/the-attck%E2%84%A2-navigator-a-new-open-source> |
| ATT&CK Navigator Example | <https://mitre.github.io/attack-navigator/enterprise/> |

**References of MITRE ATTACK**

# **Adversary Emulation and Red Teaming**

ATT&CK provides a common language and framework that red teams can use to emulate specific threats and plan their operations.  
  
[Getting Started with ATT&CK: Adversary Emulation and Red Teaming Blog Post](https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3)  
This blog post describes how you can get started using ATT&CK for adversary emulation and red teaming at three different levels of sophistication. (July 2019)  
  
[Do-It-Yourself ATT&CK Evaluations to Improve Your Security Posture Presentation](https://www.sans.org/presentations/do-it-yourself-att-ck-evaluations-to-improve-your-security-posture/)  
This presentation explains how defenders can improve their security posture through the use of adversary emulation by performing their very own ATT&CK Evaluations. (June 2019)  
  
[APT ATT&CK - Threat-based Purple Teaming with ATT&CK Continued Presentation](https://www.x33fcon.com/slides/x33fcon19_ThreatbasedPurpleTeamming_JamieDaniel.pdf)  
This presentation takes a deep-dive into using ATT&CK for purple teaming, including lessons learned from ATT&CK Evaluations. (May 2019)  
  
[To Blue with ATT&CK-Flavored Love Presentation](https://www.youtube.com/watch?v=9X-LO7aGr2s)  
This presentation provides a red teamer’s perspective to show how ATT&CK is a valuable tool to help red and blue teams work together to improve their defenses. [Slides are also available](https://www.sans.org/cyber-security-summit/archives/file/summit_archive_1555000088.pdf). (July 2019)  
  
[Finding Cyber Threats with ATT&CK-Based Analytics](https://www.mitre.org/publications/technical-papers/finding-cyber-threats-with-attck-based-analytics)  
Presents a methodology for using ATT&CK to build, test, and refine behavioral-based analytic detection capabilities. (June 2017)  
  
[Adversary Emulation Plans](https://attack.mitre.org/resources/adversary-emulation-plans)  
To showcase the practical use of ATT&CK for offensive operators and defenders, MITRE created Adversary Emulation Plans. We previously released [a plan for APT3](https://attack.mitre.org/docs/APT3_Adversary_Emulation_Plan.pdf) (as well as [an accompanying field manual](https://attack.mitre.org/docs/APT3_Adversary_Emulation_Field_Manual.xlsx)) and anticipate that we will release additional plans in the future.  
  
[CALDERA](https://github.com/mitre/caldera)  
CALDERA is an automated adversary emulation system that performs post-compromise adversarial behavior within Windows Enterprise networks. It generates plans using a pre-configured adversary model based on ATT&CK. [This presentation from BSides Charm](https://www.youtube.com/watch?v=gTGnHXgqZCo) provides an overview of CALDERA.  
  
[Threat-based Purple Teaming with ATT&CK Presentation](https://www.youtube.com/watch?v=OYEP-YAKIn0&index=3&list=PL7ZDZo2Xu332XUiwFHB5X-tXfqIwVkg5l&t=0s)  
This presentation discusses how purple teams can use ATT&CK as a common language for adversary emulation. [Slides are also available](https://www.slideshare.net/ChristopherKorban/purple-teaming-with-attck-x33fcon-2018). (June 2018)  
  
[ATT&CKing with Threat Intelligence Presentation](https://www.pscp.tv/w/1yoKMVDjbrkGQ)  
This presentation provides perspective on how to use threat intelligence for ATT&CK-based adversary emulation [Slides are also available](https://www.slideshare.net/ChristopherKorban/attcking-with-threat-intelligence).  
  
[ATT&CK Evaluations Adversary Emulation Summary](https://attackevals.mitre-engenuity.org/methodology-overview)  
This summary from the ATT&CK Evaluations website provides an introduction to how ATT&CK Evaluations used an adversary emulation approach.

###### **Adversary Emulation and Red Teaming**

**ATT&CK provides a common language and framework that red teams can use to emulate specific threats and plan their operations.**  
  
[Getting Started with ATT&CK: Adversary Emulation and Red Teaming Blog Post](https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3)  
This blog post describes how you can get started using ATT&CK for adversary emulation and red teaming at three different levels of sophistication. (July 2019)  
  
[Do-It-Yourself ATT&CK Evaluations to Improve Your Security Posture Presentation](https://www.sans.org/presentations/do-it-yourself-att-ck-evaluations-to-improve-your-security-posture)  
This presentation explains how defenders can improve their security posture through the use of adversary emulation by performing their very own ATT&CK Evaluations. (June 2019)  
  
[APT ATT&CK - Threat-based Purple Teaming with ATT&CK Continued Presentation](https://www.x33fcon.com/slides/x33fcon19_ThreatbasedPurpleTeamming_JamieDaniel.pdf)  
This presentation covers how to use ATT&CK to take cyber threat intelligence and operationalize it into behaviors that can drive relevant detections. (May 2019)

[View more resources about Adversary Emulation and Red Teaming](https://attack.mitre.org/resources/get-started/adversary-emulation-and-red-teaming)

###### **Assessment and Engineering**

**ATT&CK can be used to assess your organization’s capabilities and drive engineering decisions like what tools or logging you should implement.**  
  
[Getting Started with ATT&CK: Assessments and Engineering Blog Post](https://medium.com/mitre-attack/getting-started-with-attack-assessment-cc0b01769cb4)  
This blog post describes how you can get started using ATT&CK for assessments and engineering at three different levels of sophistication. (August 2019)  
  
[Lessons Learned Applying ATT&CK-Based SOC Assessments](https://www.youtube.com/watch?v=lMh9E8l1-ks)  
This keynote presentation discusses a process to gauge a SOC’s detective capabilities as they relate to ATT&CK, including MITRE’s practical experiences and lessons learned. (June 2019)  
  
[Finding Cyber Threats with ATT&CK-Based Analytics](https://www.mitre.org/publications/technical-papers/finding-cyber-threats-with-attck-based-analytics)  
Presents a methodology for using ATT&CK to build, test, and refine behavioral-based analytic detection capabilities. (June 2017)

[View more resources about Assessment and Engineering](https://attack.mitre.org/resources/get-started/assessment-and-engineering)