Bitdefender

GUIDE TO RED TEAMING

The Red Team Attack Simulation Built Using The MITRE ATT&CK Framework

The Bitdefender Guide

Trusted. Always.

Contents

What Is Red Teaming?

Red teaming is an intelligence-led assessment that simulates real-life threat actors. The purpose of a red team assessment is to demonstrate how real-world attackers would attempt to compromise critical functions and underlying systems of an organization. Real-world actors can include cyber criminals, hacktivists, and state-sponsored actors using Advanced Persistent Threats (APTs) as well as insider threats.

A successful engagement involves identifying weakness in the internal security team detection and response capabilities, challenging staff security awareness and attacking the processes and underlying technologies. Ultimately, the aim of the assessment is to work with the organization to improve their security posture and enable better detection and response to such threats in the future.

Compared to a typical penetration test assessment, red teaming is goal-oriented and aims to assess the organization holistically by using Techniques, Tactics and Procedures (TTPs). TTPs are ways to define an adversary's behavior by their attack lifecycle, methodology, use of tools, attack methods, and many other characteristics. A penetration test assessment is typically loud and aims to find as many vulnerabilities as possible within the time constraints. A red team assessment is covert, targeted and usually lasts over a longer engagement period. Organizations may wish to test whether it is possible to obtain sensitive information from a particular server, access to the CEO's email or complete domain dominance.

What Is the MITRE ATT&CK framework?

The MITRE ATT&CK Framework is a well-documented knowledge base of TTPs. TTPs are patterns of behaviour that real world actors employ. An example of this would be the infamous report published by FireEye on the Mandiant APT1 espionage group. Within the report, FireEye have documented behaviour patterns, techniques, tactics, software, indicator of compromises, exfiltrated data and the timeline of the attacks. MITRE ATT&CK framework simplifies these results to include a list of APTs with the techniques and tools that were found in the wild. (Link 1 and Link 2)

This can be further visualised with MITRE ATT&CK Navigator where a red or blue teamer can identify and define an adversary's TTP. The framework is granular down to the different operating systems and cloud environments, as techniques are specific to its environment. MITRE ATT&CK also includes remediation and detection to help blue teamers to better protect and respond to these attacks.

As a supplement to the Cyber Kill Chain, MITRE ATT&CK framework is comprised of a detailed list of tactics which includes: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Exfiltration, Command and Control. Each of these tactics comprises a number of techniques that have grown over the years.

The purpose of a red team assessment is to replicate these attacks in a number of scenarios. A common misunderstanding is that a red team engagement is a one-off engagement. In fact, red teaming is an iterative and continuous process. Organizations should be getting repeated assessment to improve their own detection and response capabilities.

How Does Red Teaming Work?

The first stage in a red teaming assessment is to have a project initiation meeting where the scope is defined to meet client's requirements and expectations. The scope of the project will be dependent on maturity of the organization, time, cost and objectives as defined by the organization. The outcome of the meeting should be a list of objectives or goals for the red team, out-of-scope elements, scenarios, expectations and a timeline. For example, the goal may be to extract sensitive information from a particular server. However, the engineering department and SAP ERP are out-of-scope as they provide critical business functions to the organization, which cannot be covered in this round of engagement.

For red team engagements, an organization can either take a scenario-based or a complete black-box approach. With a scenario-based approach, specific use cases are tailored to the organization and can be used to gain better coverage and provide more value, particularly if time and cost is a determining factor. In some cases, a black-box approach may not be able to test specific security controls that can be overlooked. For example, it may not be able to take into consideration stolen laptops and employees with a specific access control. At the scoping phase, an attack path analysis will be performed to address the organization's needs and concerns. Each organization will have a different threat model, and individual scenarios will be built to address these issues. Some scenarios that we propose to clients are the following:

- **Assumed breach for both Wi-Fi and Network access** – An attacker may have gained physical access to the organization and have planted a backdoor to the network. Similarly, an attacker may have gained access to the corporate Wi-Fi through vulnerabilities in the wireless access point or weak encryption methods. This scenario does not assume that a corporate device has been physically taken and only network access was achievable.
- **Assumed stolen laptop** – Laptops may have been left unoccupied for a brief time or stolen. An attacker may have obtained credentials through shoulder surfing or installing a keylogger with a removable drive attacks such as USBNinja. In any case, to perform this scenario, an attacker has possession of the stolen device and will try to infiltrate the network using the corporate device.
- **Assumed malicious employee or a compromised box** – An employee such as a disgruntled former worker or an insider threat may pose a threat to the organization. A corporate device may be infected with malware through the use of phishing or drive-by downloads. In any case, an organization would provide the red team with remote desktop access to one of the machines to carry out this engagement. This can be performed from a low-level or even a high-level user depending on the scenario to be played.
- **Assumed compromised external users** – Employees may be susceptible to weak passwords or password reuse. For example, users' credentials may be leaked in password dumps which can provide us with certain access such as OWA, salesforce or even the VPN. The engagement will be carried out remotely imitating an outsider threat.
- **Assumed compromised public facing or internal box** – Public facing websites such as ecommerce, banking or any applications can be compromised and pose a risk particularly if it can access the corporate network. An attacker with access to the compromised web server or backend services like databases may be able to laterally move across the networks or provide a stepping stone to leverage other social engineering attacks. Similarly, internal applications are often developed without best security practices and can also be leveraged. For this scenario, remote access to the server will be given to the red team to determine how far they can go with it.
- **Classic phishing** – Phishing can be performed from an internal user or an external user with a phishing domain or even a spoofed domain, depending on the organization's security controls. The red team will work with the organization to discuss phishing scenarios and breadth of the test. If malware or credential phishing is a success, the red team will move forward to obtain the goal or objective.
- **Black Box** – In this scenario, only the goal is defined such as access to the service and any out-of-scope elements. The red team will employ any tactics within reason to obtain the goal.

The red team will carry out the scenarios as defined by the scope and work closely with the organization. All engagements start with a reconnaissance phase which includes performing Opensource intelligence (OSINT) on the organization such as the network layout, employees, technology stack, harvesting email addresses, social media, passwords leaks, and even minute details such as email signature and lanyards. Depending on the given scenario, the red team will aim to privilege escalate to a high-level user, maintain access, evade defenses, laterally move across the network and ultimately achieve the given goal. Each engagement will vary, but they will generally include:

- Social engineering through malware or credential phishing to assess the level of security staff's awareness and response.
- Challenging intrusion detection and prevention system to see the blue team's detection and response.
- Assessing the network and build segmentation to evaluate security controls, lateral movement, domain trust and firewall controls.
- Exploiting internal or external applications to chain attacks such as client-side attacks to more serious vulnerabilities such as remote code execution and complete compromise of the server.
- Exploiting internal processes and shared resources among different departments that can be used to escalate. An example of this would be finding secrets in a mailbox or shared drives.
- Evading endpoint security such as Antivirus and Endpoint Detection Response (EDR) through obfuscation and modern techniques to execute malicious code.
- Assessing and abusing workstation and server builds and group policies to privilege escalate, lateral movement, credential dumping, among other tactics.
- Assessing user groups and access control and abuse low-level user privileges to escalate and emulate insider threat attacks.
- Exploiting low-hanging fruit vulnerabilities such as outdated software versions, default credentials or weak passwords.
- Abusing active directory attacks and cloud security, depending on the environment such as on-premise, hybrid AD or cloud managed.

What to Expect

Bitdefender employs a team of specialists and we provide consultancy and an end deliverable report that will detail the findings consisting of an executive and technical level summary of your business risk as well as the methodology of the attacks. During the entire process, the red team will liaise with the trusted contact from your control group which may consist of a number of senior individuals that are positioned on top of the security incident escalation chain. These individuals will be aware of the engagement and will aid in communication. Depending on the engagement, the organization may wish for us to work with the blue team throughout the process. During each milestone or set intervals, the red team will present the findings and progression to the executives and technical members. Finally, a post assessment briefing will be provided to summarize the engagement and next steps.

Interested in a Red Team Engagement?

Reach out to Bitdefender to begin scoping out requirements.

CONTACT US

Bitdefender Red Team Methodology

The following sections outline the methodology adopted by Bitdefender for red team/ adversarial attack simulation engagements. The objective of Bitdefender red team engagements is to evaluate the organization's resilience against real-world cyber adversaries, across the prevention, detection and response spectrums, in a realistic and effective manner.

Bitdefender utilizes MITRE ATT&CK®, a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations, to perform realistic adversarial simulations.

Specifically, the ATT&CK® for Enterprise adversary model and framework is leveraged as a foundation to execute the tactics, techniques, and procedures (TTPs) cyber threats use when attacking enterprise networks, to achieve their objectives after successfully gaining initial access. The TTPS in the ATT&CK® for Enterprise framework encompasses the later stages of the Cyber Kill Chain® - Delivery, Exploitation, Installation, Command and Control, Actions on Objectives.

Two versions of the red team service are offered, designed at providing fulfilling different outcomes and objectives, depending on the requirements of the engagement. Both versions follow the same execution methodology.

Red team simulation engagements are recommended for organizations that would like an overview of their current defensive capabilities, across the prevention, detection and response spectrums. For this style of engagements, Bitdefender will work in a collaborative fashion with the blue team, to determine the effectiveness of the existing technical controls and escalation processes in place when dealing with cyber threats. Depending on the requirements of the engagement, a subset or all of the TTPS in the ATT&CK® Enterprise Matrix will be executed to benchmark the organization's current capabilities. This overview can then be used as a baseline for future improvements.

Scenario-based red team engagements are recommended for organizations that would like to gauge their current defensive capabilities (across prevention, detection, and response) against a predefined set of scenarios. As an example, an organization could have a well rounded education program in security and phishing awareness, that is effective against phishing attacks conducted to gain initial access. However there could be gaps around the existing controls and processes that would allow subsequent actions, such as lateral movement and exfiltration, to be executed. Scenario-based red team engagements aim to identify the existence of such gaps, and aim to provide a more realistic view on how the organization would react and respond if the scenarios were to occur.

Both versions of the red team service follow the same high level methodology, and the various stages are explained below.

PROJECT INITIATION

During the projection initiation stage, the following items will be finalized with the client in a kickoff meeting:

- Scope of engagement
- Project timeline
- Logistics required prior to commencement
- Establishment of notification and escalation routes
- Rules of engagement
- High level test plan

PROJECT EXECUTION

Depending on the specifics of the engagement or scenarios planned, the project execution phase may comprise all or a subset of the following techniques within the ATT&CK® Enterprise Matrix:

Initial Access

Initial Access consists of techniques that use various entry vectors to gain an initial foothold within a network. Techniques used to gain a foothold include targeted spear phishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

Execution

Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals,

like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

Persistence

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.

Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

Privilege Escalation

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives.

Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities. Examples of elevated access include:

- SYSTEM/root level
- Local administrator
- User account with admin-like access
- User accounts with access to specific system or perform specific function

These techniques often overlap with Persistence techniques, as OS features that let an adversary persist can execute in an elevated context.

Defense Evasion

Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics' techniques are cross- listed here when those techniques include the added benefit of subverting defenses.

Credential Access

Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

Discovery

Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective.

Lateral Movement

Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain access. Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

Collection

Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives. Frequently, the next goal after collecting data is to steal (exfiltrate) the data.

Common target sources include various drive types, browsers, audio, video, and email. Common collection methods include capturing screenshots and keyboard input.

Command and Control

Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.

Exfiltration

Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command and control channel or an alternate channel and may also include putting size limits on the transmission.

Impact

Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach.

The rules of engagement defined in the project initiation stage will be adhered to for the duration of the assessment, and notification and escalation routes used when scheduled or as necessary.

Depending on the earlier defined scope for the engagement, it will sometimes be necessary to "stage" certain phases of the assessment, to allow proper simulation and execution of the adversarial techniques in the organization's environment.

Reporting and Presentation

Upon completion of the assessment, a formal report will be compiled and provided to all relevant stakeholders. On a high level, the report will contain the following sections:

- Executive summary summarizing the objectives and assessment results.
- Findings section detailing the results and observations for each phase of the assessment. This will include details on the techniques executed, and an overall evaluation on how the organization's prevention, detection and response capabilities responded to the execution of these techniques.
- Analysis and recommendations across the prevention, detection and response spectrums

If requested, a formal presentation can be conducted to present the results of the assessment together with the recommendations to all relevant stakeholders.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com

Bitdefender-BSG-GUIDE-redteam-creat7284-en_EN
CD-10/20/23 • MD-October 24, 2023 7:50 pm