ALTIMETRIK®

CYBERSECURITY

Red Teaming Strategies for Proactive Threat Defense

WHITEPAPER

Introduction

Red teaming is the practice of rigorously testing an organization's cybersecurity defenses by simulating real-world attacks from the perspective of malicious threat actors. A red team engages in ethical hacking to probe for vulnerabilities across the target's networks, applications, and human elements, with the goal of identifying weaknesses before they can be exploited by actual adversaries.

Cyber threats are becoming increasingly sophisticated and persistent, posing grave risks to organizations of all sizes and industries. Traditional defensive measures alone are often insufficient to keep pace with skilled attackers continually developing new tactics, techniques, and procedures (TTPs) to bypass security controls. Red teaming provides a proactive and adversary-emulated approach to continuously validate and improve an organization's security posture.

The ability to detect data breaches internally remains a significant challenge for organizations. Based on IBM's 2023 Breach Report, only one-third of companies discover breaches through their own security teams or tools. This statistic shows the pressing need to enhance threat detection capabilities within organizational cybersecurity programs. A staggering 67% of breaches are instead reported by external entities, either benign third parties or, alarmingly, by the attackers themselves.

When attackers are the ones disclosing a breach, it incurs a substantial cost increase for organizations, averaging nearly USD 1 million more compared to internally detected incidents. This significant fiscal impact highlights the critical importance of proactive and robust threat identification measures as a core component of an organization's comprehensive cybersecurity posture.

By emulating the mindset and methods of real-world attackers, red teaming offers numerous benefits to organizations. It helps identify blind spots and previously unknown vulnerabilities in their defenses, allowing them to remediate these issues before they can be exploited. It also tests the effectiveness of existing security controls, incident response plans, and the overall resilience of the organization's cyber defenses against realistic attack scenarios. Additionally, red teaming exercises help raise security awareness and improve the cyber skills of defensive teams through realistic, hands-on training experiences.

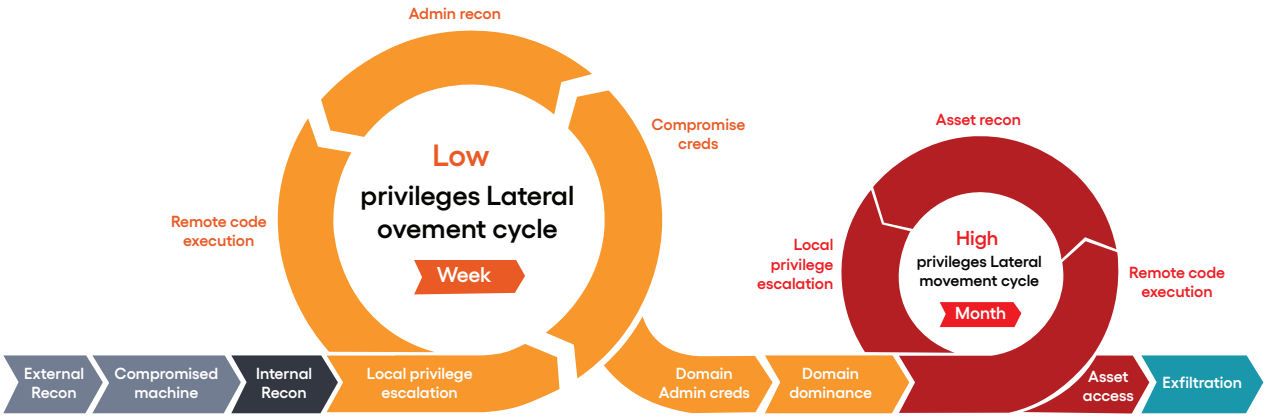
What is Red Teaming?

Red teaming is a full-scope, multi-layered security assessment that aims to provide a holistic evaluation of an organization's ability to detect, respond to, and mitigate real-world cyber threats. It involves a team of highly skilled ethical hackers, known as red teamers, who adopt the mindset and methods of actual threat actors to rigorously test the target's security posture.

While red teaming shares some similarities with penetration testing (pen testing), there are key differences in scope and approach. Penetration tests typically focus on identifying and exploiting specific technical vulnerabilities within a defined scope, such as a network, application, or system. Red teaming, on the other hand, takes a broader and more comprehensive approach, encompassing not only technical aspects but also examining an organization's processes, procedures, and human elements that contribute to its overall security posture.

The role of a red team is to emulate the tactics, techniques, and procedures (TTPs) employed by real-world threat actors, such as advanced persistent threats (APTs), nation-state actors, or highly skilled cybercriminals. This involves a combination of open-source intelligence gathering, social engineering, physical security assessments, and advanced hacking techniques to gain initial access, establish persistence, and move laterally within the target environment, all while evading detection.

The following image below summarizes the red teaming cycle from external recon to exfiltration. More detail will be covered in the next section on the red teaming process using the MITRE ATT&CK framework.



Source: Microsoft

The Red Teaming Process and MITRE ATT&CK

Red teams often structure their operations around the MITRE ATT&CK framework, which provides a comprehensive knowledge base of adversary tactics, techniques, and procedures (TTPs). The ATT&CK framework consists of several stages that outline the various phases of an attack lifecycle, and red teams can leverage this structure to emulate realistic threat scenarios.

Reconnaissance: The red teaming process typically begins with the reconnaissance stage, where the team gathers intelligence about the target organization. This may involve techniques such as open-source intelligence gathering (OSINT), social engineering, or physical surveillance. Red teams may use tactics like Active Scanning or Gathering Victim Host Information to collect valuable information about the target's infrastructure and personnel.

Initial Access: After gathering sufficient intelligence, the red team attempts to gain an initial foothold into the target environment. This can be achieved through various techniques, such as Phishing, Exploiting Public-Facing Applications, or leveraging Valid Accounts. Red teams may also employ physical attack vectors, such as dropping malware or replicating removable media, to gain access.

Execution: Once initial access is obtained, the red team aims to execute their malicious payloads or scripts within the target environment. This may involve techniques like Command and Scripting Interpreter, Deploy Container, or Deobfuscate/Decode Files or Information to run their tools and establish a foothold.

Persistence: To maintain access and ensure long-term presence within the target environment, red teams may employ persistence techniques. This could involve creating or modifying system processes, implanting Boot or Logon Initialization Scripts, or leveraging Valid Accounts to maintain access even after system reboots or defensive actions.

Privilege Escalation: To expand their access and capabilities, red teams often attempt to escalate their privileges within the target environment. Techniques like Exploit Public-Facing Application, Exploit for Privilege Escalation, or Hijack Execution Flow may be used to gain higher levels of access and control.

Defense Evasion: Throughout the engagement, red teams employ various defense evasion tactics to avoid detection and bypass security controls. This may involve techniques such as Obfuscated Files or Information, Impair Defenses, or Indicator Removal on Host to conceal their activities and evade defensive measures.

Credential Access: To facilitate lateral movement and access additional resources, red teams may attempt to obtain login credentials or access tokens. Techniques like OS Credential Dumping, Brute Force, or Unsecured Credentials can be employed to gain unauthorized access to sensitive information and systems.

Lateral Movement: After establishing a foothold, red teams often seek to move laterally within the target environment to expand their reach and access additional systems or data. Techniques like Remote Services, Exploitation of Remote Services, or Replication Through Removable Media may be used to facilitate lateral movement.

Collection: Throughout the engagement, red teams may gather sensitive data or information from the target environment. This could involve techniques such as Data from Local System, Data Staged, or Screen Capture to collect valuable intelligence or simulate data exfiltration.

Exfiltration: In the final stage, red teams may attempt to exfiltrate the collected data or payloads from the target environment. Techniques like Exfiltration Over C2 Channel, Transfer Data to Cloud Account, or Automated Exfiltration could be employed to simulate data theft or exfiltration of valuable assets.

By aligning their operations with the MITRE ATT&CK framework, red teams can accurately emulate the tactics, techniques, and procedures used by real-world threat actors, providing a comprehensive assessment of an organization's security posture and readiness to detect, respond to, and mitigate advanced cyber threats.

Popular C2 Frameworks

A C2 framework, which stands for Command-and-Control framework, is a set of tools used to communicate with and control compromised computer systems. These frameworks are used by both ethical hackers (red teams) during security assessments and by malicious actors (hackers) to maintain control over infiltrated devices.

As described in the previous section on the red teaming process, attackers will simply gain initial access through social engineering and phishing or by taking advantage of a vulnerable publicly exposed application wherein they can upload their malicious payload to create “beacons” which will interact with the attacker’s C2 framework. This will allow threat actors to streamline their attack process from initial compromise, privilege escalation and lateral movement across the network to get to their objective. C2 frameworks are an integral part of red teaming assessments.

The following are the top 5 most popular C2 (Command and Control) frameworks used in red teaming and penetration testing:

Cobalt Strike: A commercial, feature-rich framework offering a wide range of tools for reconnaissance, attack planning, and post-exploitation activities. It is known for its ease of use, extensive functionality, and advanced evasion techniques.

Metasploit: A free and open-source framework widely distributed with Kali Linux. It provides a vast collection of exploits, payloads, and auxiliary modules for various purposes. Metasploit is a great option for beginners due to its large community and extensive documentation.

Sliver: An open-source, multi-platform framework designed for automated adversary emulation and post-exploitation tasks. It offers cross-platform support for Windows, macOS, and Linux and focuses on stealth and living-off-the-land techniques.

Brute Ratel C4: A commercial red teaming and adversary simulation platform known for its automation capabilities, sophisticated attack techniques, and focus on mimicking real-world attacker behavior.

Havoc: A free, open-source framework valued for its ease of setup and lightweight design. Havoc is a good option for those seeking a simple and quick-to-deploy C2 solution for basic red teaming exercises.

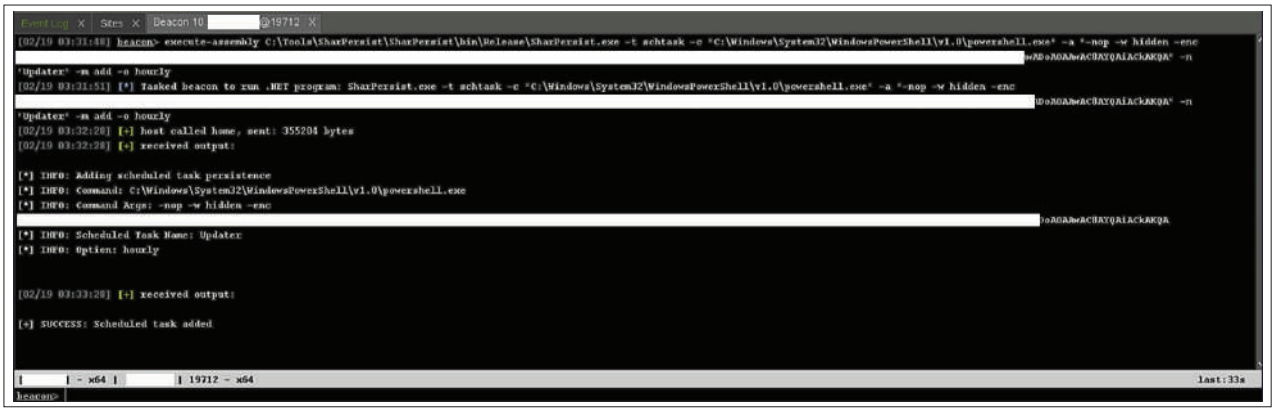
C2 Framework in Action

The following example illustrates the capabilities of Cobalt Strike and shows the step-by-step process of an attacker utilizing a C2 in a red teaming engagement.

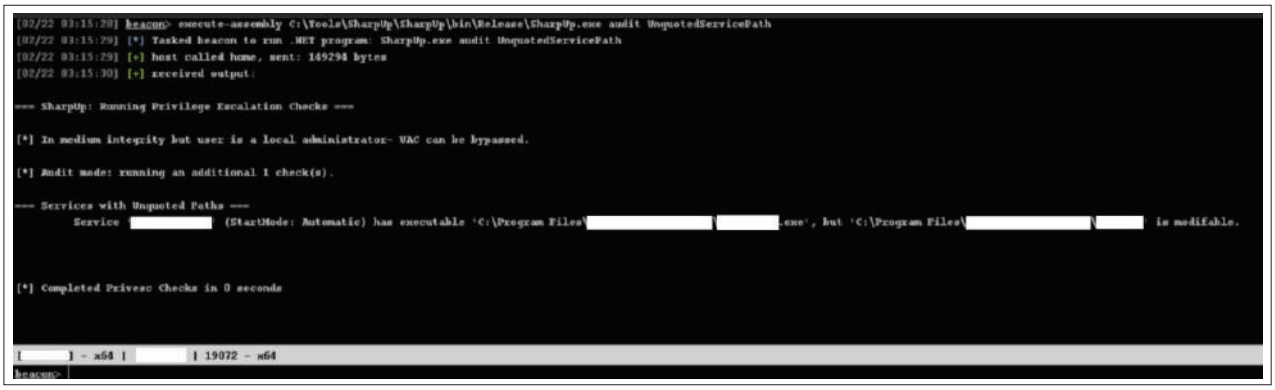
The attacker creates and hosts a malicious payload that will be sent to the target.

Next, the attacker will receive a connection back from the payload, in Cobalt Strike's case, their payload is called a beacon.

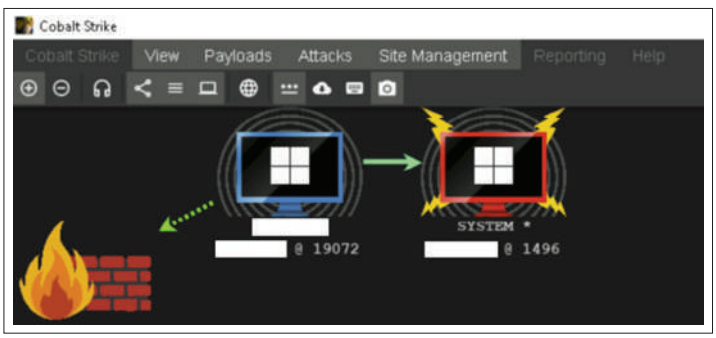
After gaining initial access, it is important for the attacker to maintain control of the target system by adding persistence. This is done through tools such as Sharpersist, which is executed on the target and creates persistence using scheduled tasks or events to connect back to the C2.



Next the attacker will attempt to escalate the privilege to obtain admin access on the machine to find potential hashes, credentials, or Kerberos tickets to gain access to other machines in the active directory network.

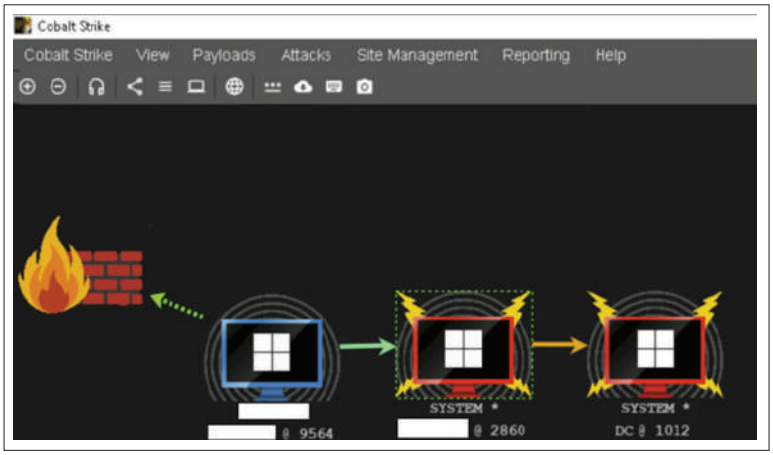


In this case, the attacker has found an unquoted service path to gain elevated privileges. The attacker will replace the vulnerable binary and run it to gain elevated access to the machine:



The main goal of the engagement is to gain control of the domain controller. At this point, the attacker can perform what is called an NTLM relay attack to steal tickets from other computers connecting to the domain controller and use that to authenticate to the domain controller and gain access, thus completing their goal:

Graphical interface showing the attacker has accessed and gained control over the domain controller.



Benefits of Red Teaming

One of the primary benefits of red teaming is its ability to identify and assess vulnerabilities across an organization's people, processes, and technology. By adopting an attacker's perspective, red teams can uncover weaknesses that may have gone unnoticed through traditional security assessments, such as gaps in security awareness, flawed processes, or misconfigurations that could be exploited.

According to IBM's 2023 Breach Report, rigorous security testing and effective incident response (IR) planning have emerged as a pivotal investment for organizations, yielding substantial cost savings in the event of a data breach. The fiscal impact of rigorous security testing and IR preparedness is significant – organizations with elevated levels of testing and IR planning realized cost savings averaging USD 1.49 million compared to those with inadequate IR readiness or testing

Additionally, a 2023 Ponemon Institute study on the state of offensive security surveyed 664 security practitioners for organizations with a mature security program using offensive security services. It was found that 30% of companies using red teaming and offensive security services were able to lower their cyber security premiums.

Red teaming also allows organizations to evaluate the effectiveness of their existing security controls and investments objectively. By launching realistic attack simulations, red teams can validate whether the implemented security measures are functioning as intended and capable of detecting and mitigating sophisticated threats. This assessment can help organizations optimize their security spending and prioritize areas requiring improvement.

Additionally, red teaming exercises provide a unique opportunity to test an organization's incident detection and response capabilities under realistic conditions. By simulating a real-world attack scenario, red teams can assess the effectiveness of an organization's security monitoring, incident response plans, and the coordination between various security teams, helping identify areas for improvement and enhancing overall preparedness.

Altimetrik Edge Security Services

Red Teaming Services
According to the 2023 Ponemon Institute study, 68% of organizations with mature security programs conduct red teaming activities – which helped them improve zero-day response capabilities, meet compliance and regulatory requirements and improve visibility into their attack surface. Additionally, 64% of respondents benefited from security testing and achieved their security and governance goals.

By adopting an adversarial mindset, our highly skilled Red Team emulates sophisticated cyber threats, providing actionable insights to strengthen your organization's resilience against potential breaches and minimize the risk of financial losses or reputational damage.

Identify Vulnerabilities Across Your Attack Surface
Our Red Teaming engagements are designed to uncover vulnerabilities across your organization's entire attack surface, including networks, applications, systems, processes, and human elements. Our team leverages advanced tactics, such as open-source intelligence gathering, social engineering, physical security assessments, and innovative hacking techniques, to gain initial access and establish a foothold within your environment.

Validate the Effectiveness of Your Security Controls
Investing in security controls is essential, but how can you be confident they are functioning as intended? Our Red Teaming service rigorously validates the effectiveness of your existing security measures by launching realistic attack simulations. This approach enables you to identify gaps or weaknesses in your defenses and optimize your security investments for maximum protection.

Insider Threats and Social Engineering
One of the most significant risks organizations face insider threats, whether intentional or unintentional. Our Red Teaming service includes comprehensive social engineering assessments, where our team ethically tests your employees' susceptibility to tactics like phishing, smishing, and other deceptive techniques. By identifying potential vulnerabilities in your human layer, we can help you implement effective awareness training and strengthen your overall security posture.

Proactive Risk Assessment and Breach Prevention
Altimetrik's Red Teaming services provide a proactive approach to risk assessment, enabling you to uncover potential breaches before they occur. Our team simulates real-world attack scenarios, identifying blind spots and vulnerabilities that may have gone unnoticed through traditional security assessments. By addressing these weaknesses, you can effectively prevent financial losses, data breaches, and reputational damage resulting from successful cyber-attacks.

Actionable Insights and Continuous Improvement
Throughout the Red Teaming engagement, our team meticulously documents their findings and provides detailed reports with actionable recommendations. These insights enable you to prioritize remediation efforts, enhance your security posture, and implement a culture of continuous improvement within your organization. By regularly conducting Red Teaming exercises, you can stay ahead of evolving threats and maintain a robust security stance.

Attack Surface Management

Maintaining a strong security posture requires a deep understanding of your organization's attack surface – the sum of all potential entry points for threats. Our Attack Surface Management service provides comprehensive visibility and analysis of your attack surface, enabling proactive identification and mitigation of vulnerabilities before they can be exploited by malicious actors.

Enhanced Threat Visibility and Attack Surface Reduction ROI
One of the biggest challenges organizations face is the lack of visibility into their complete attack surface, which can span networks, applications, cloud environments, and even human elements. Our service employs advanced techniques to map and monitor your entire attack surface, giving you unprecedented visibility into potential vulnerabilities and threats.

Continuous Monitoring and Threat Intelligence Integration
Effective attack surface management requires continuous monitoring and the ability to adapt to emerging threats. Our service leverages innovative threat intelligence to stay ahead of the latest attack vectors and techniques used by threat actors.

Through continuous monitoring and real-time updates, we ensure that your organization's attack surface is constantly evaluated, enabling rapid response to new vulnerabilities or emerging threats.

Proactive Threat Identification and Improved Security Posture
By taking a proactive approach to threat identification, our Attack Surface Management service empowers your organization to stay one step ahead of potential adversaries. Our team of experts utilizes advanced techniques, such as attack surface analysis, vulnerability scanning, and penetration testing, to identify and prioritize vulnerabilities based on their risk and potential impact.

Reporting and Analytics, Integrated with Security Operations Center (SOC)
Our Attack Surface Management service delivers comprehensive reporting and analytics, providing you with detailed insights into your organization's attack surface, vulnerabilities, and risk exposure. These reports can be seamlessly integrated with your existing Security Operations Center (SOC), enabling efficient threat monitoring, incident response, and security orchestration.

By combining our expertise with your SOC's capabilities, we create a powerful synergy, ensuring that your organization remains vigilant and responsive to potential threats across your entire attack surface.

Vulnerability Management

Vulnerabilities within your organization's infrastructure can pose significant risks, leaving you exposed to potential threats and data breaches. Our Vulnerability Management service provides a comprehensive and proactive approach to identifying, assessing, and remediating vulnerabilities across your entire attack surface.

Reduced Exposure and Improved Incident Response
By continuously assessing and prioritizing vulnerabilities, our service enables swift remediation, effectively reducing your organization's exposure to cyber threats. This proactive approach not only minimizes the risk of successful attacks but also enhances your incident response capabilities.

Reporting and Compliance Support
Maintaining compliance with industry regulations and security standards is crucial for many organizations. Our Vulnerability Management service provides detailed reporting and documentation, ensuring that you have the necessary information to demonstrate compliance and adhere to relevant security frameworks.

Prioritization and Risk Analysis
Not all vulnerabilities pose equal risks to your organization. Our Vulnerability Management service employs advanced risk analysis techniques to prioritize vulnerabilities based on their potential impact and likelihood of exploitation. By focusing on the most critical vulnerabilities first, we help you allocate resources effectively and maximize the impact of your remediation efforts.

Proactive Threat Mitigation and Machine Learning-Driven Detection
Our service goes beyond traditional vulnerability scanning by leveraging innovative technologies, such as machine learning and artificial intelligence. By continuously monitoring your environment and analyzing vast amounts of data, our advanced systems can detect emerging vulnerabilities and potential threats proactively.

Conclusion

Our comprehensive red teaming services provide a proactive and rigorous approach to assessing and fortifying your defenses against even the most sophisticated cyber threats. By emulating the tactics, techniques, and procedures of real-world adversaries, we uncover vulnerabilities that may have gone unnoticed, enabling you to remediate them before they can be exploited.

Threats are constantly evolving, and the consequences of a successful breach can be devastating. By partnering with Altimetrik, you are taking a proactive stance against potential adversaries, ensuring that your organization is prepared to defend against even the most sophisticated attacks.

Sign-up for Altimetrik's edge security services – red teaming, attack surface management and vulnerability management today and gain the confidence that your organization is prepared to detect, respond to, and mitigate even the most advanced cyber threats. Contact us to schedule a consultation and learn how our expertise can fortify your cybersecurity defenses.

About Altimetrik

Altimetrik is a pure-play digital business services company. We focus on delivering business outcomes with an agile, product-oriented approach. Our digital business methodology provides a blueprint to manage data as well as develop, scale, and launch new products to market faster. Our team of 6,000+ practitioners with software, data, cloud engineering skills help create a culture of innovation and agility that optimizes team performance, modernizes technology, and builds new business models. As a strategic partner and catalyst, Altimetrik quickly delivers results without disruption to the business.