LevelBlue

PRODUCT BRIEF

LevelBlue Consulting Adversary Simulation Service

LevelBlue Consulting's Adversary Simulation service gives security teams hands-on experience combatting real-world cyber-attacks.

LevelBlue's Red Team uses adversary Tactics, Techniques, and Procedures (TTPs) to provide a realistic assessment of the true risk posed by an attack by advanced threats.

Whether the organization's objectives involve testing tools and visibility, security response, controls around specific assets, defenses against a specific attacker, or any combination of those objectives, LevelBlue uses these requirements to tailor a test that specifically meets their needs. LevelBlue Consulting Adversary Simulation follows the well-known MITRE ATT&CK framework for conceiving of and executing each phase of an advanced attack.

Adversary Simulation Methodology

Whether the objectives involve testing tools and visibility, security response, controls around specific assets, defenses against a specific attacker, or any combination of those objectives, LevelBlue uses these requirements to tailor a test that specifically meets the organization's needs.

LevelBlue Consulting's Adversary Simulation follows the well-known MITRE ATT&CK framework for conceiving of and executing each phase of an advanced attack.

Initial Reconnaissance

Depending on the engagement, recon can be remote or on location. Remote recon is safer, since most of it is done via a computer or by using people that already live at the location and can perform the recon for you. On the other hand, sometimes the project calls for physical recon on-site, or due to security controls at the target, you might need to be physically present at the location. This type of recon sometimes can be a bit more challenging and dangerous.

Below are types of reconnaissance:

- Digital Recon
- Physical Recon

Benefits

- Strengthen security posture through application of real world tactics, techniques and procedures (TTPs)
- Define and evaluate a set of key objectives
- Partner with vendor-neutral security experts
- Leverage security expertise from a trusted advisor

Initial Access

Initial access represents the vectors adversaries use to gain an initial foothold within a network. Below are examples of some of the techniques used by the LevelBlue Red Team to gain initial access.

- Drive-by Compromise
- Exploit Public-Facing Application
- Spearphishing
- Trusted Relationship
- Valid Accounts

Establish Persistence

Persistence is any access, action, or configuration change to a system that gives an adversary a persistent presence on that system. Adversaries will often need to maintain access to systems through interruptions such as system restarts, loss of credentials, or other failures that would require a remote access tool to restart or alternate backdoor for them to regain access. Below are examples of some of the techniques used by the LevelBlue Red Team to establish persistence:

- Create Account
- Component Object Model Hijacking
- External Remote Services
- File System Permissions Weakness
- Executable Installers

Defense Evasion

Defense evasion consists of techniques an adversary may use to evade detection or avoid other defenses. Sometimes these actions are the same as or variations of techniques in other categories that have the added benefit of subverting a particular defense or mitigation. Defense evasion may be considered a set of attributes the adversary applies to all other phases of the operation. Below are examples of some of the techniques used by the LevelBlue Red Team to evade detection.

- Access Token Manipulation
- Bypass User Account Control
- DLL Side-Loading
- Disabling Security Tools
- Code Signing

Privilege Escalation

Privilege escalation is the result of actions that allows an adversary to obtain a higher level of permissions on a system or network. Certain tools or actions require a higher level of privilege to work and are likely necessary at many points throughout an operation. A user account with administrator-like access can also be used. User accounts with permissions to access specific systems or perform specific functions necessary for adversaries to achieve their objective may also be considered an escalation of privilege. Below are examples of some of the techniques used by the LevelBlue Red Team to escalate privileges.

- Process Injection
- Access Token Manipulation
- File system permissions weakness
- Hooking
- Create new service

Command and Control

Command and Control represents how adversaries communicate with systems under their control within a target network. There are many ways an adversary can establish command and control with various levels of covertness, depending on system configuration and network topology.

Below are examples of some of the techniques used by the LevelBlue Red Team to establish Command and Control:

- Commonly used ports
- Communication through removable media
- Domain Fronting
- Remote Access Tools
- Web Services

Internal Reconnaissance

Internal Reconnaissance consists of techniques that allow the adversary to gain knowledge about the system and internal network. When adversaries gain access to a new system, they must orient themselves to what they now have control of and what benefits operating from that system give to their current objective or overall goals during the intrusion. Below are examples of some of the techniques used by the LevelBlue Red Team to conduct internal reconnaissance:

- Account Discovery
- Application Discovery
- File and Directory Discovery
- Network Service Discovery
- Network Share Discovery

Credential Access

Credential access represents techniques resulting in access to or control over system, domain, or service credentials that are used within an enterprise environment. Adversaries will likely attempt to obtain legitimate credentials from users or administrator accounts (local system administrator or domain users with administrator access) to use within the network.

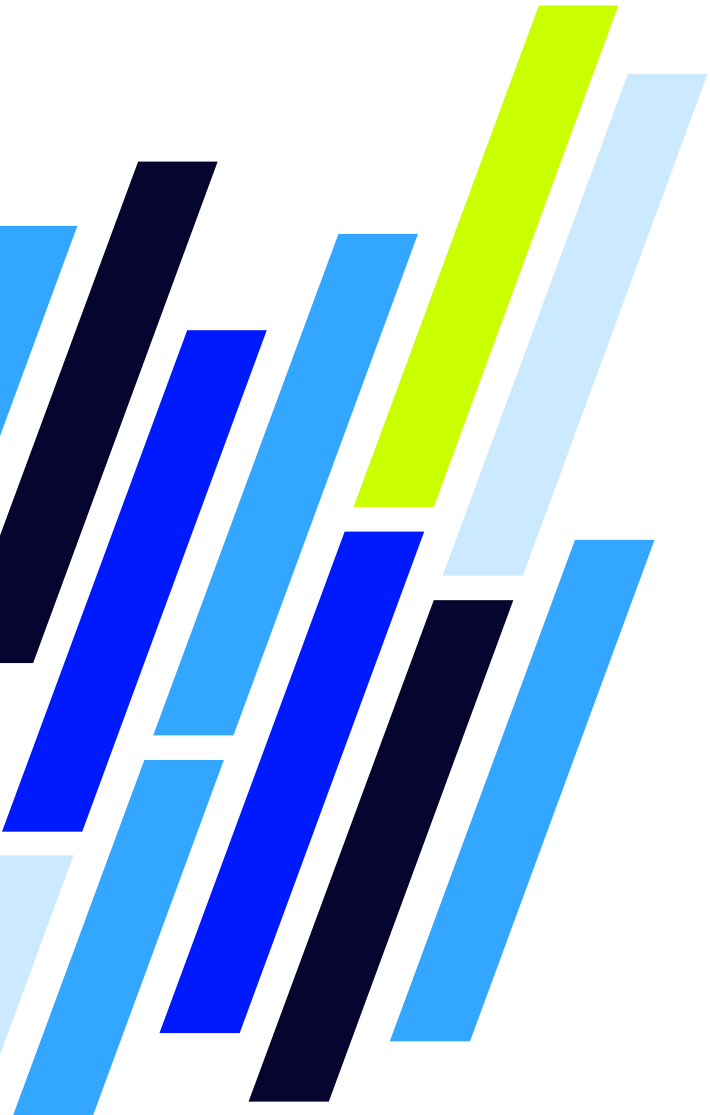
This allows the adversary to assume the identity of the account, with all of that account's permissions on the system and network and makes it harder for defenders to detect the adversary. With sufficient access within a network, an adversary can create

accounts for later use within the environment. Below are examples of some of the techniques used by the LevelBlue Red Team to obtain credential access:

- Credential Dumping
- Cached Credentials
- Plaintext Credentials
- DCSCYNC
- Credentials in Files

Lateral Movement

Lateral movement consists of techniques that enable an adversary to access and control remote systems on a network.



An adversary can use lateral movement for many purposes, including remote Execution of tools, pivoting to additional systems, access to specific information or files, access to additional credentials, or to cause an effect.

Movement across a network from one system to another may be necessary to achieve an adversary's goals. Below are examples of some of the techniques used by the LevelBlue Red Team to conduct lateral movement:

- Pass the Hash
- Pass the Ticket
- Remote Desktop Protocol
- SSH Hijacking
- Distributed Component Object Model

Data Collection

Data Collection consists of techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration. Below are examples of some of the techniques used by the LevelBlue Red Team to collect data:

- Audio Capture
- Clipboard Data
- Email Collection
- Input Capture
- Screen Capture

Exfiltrate and Complete Mission

Exfiltration refers to techniques and attributes that result or aid in the adversary removing files and information from a target network. Below are examples of some of the techniques used by the LevelBlue Red Team to exfiltrate data:

- Encrypt Data
- Exfiltration over Command and Control Channel
- Exfiltration over Physical Medium
- Compress Data
- Data Transfer Size Limits

LevelBlue

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

Contact us to learn more, or speak with your LevelBlue sales representative.