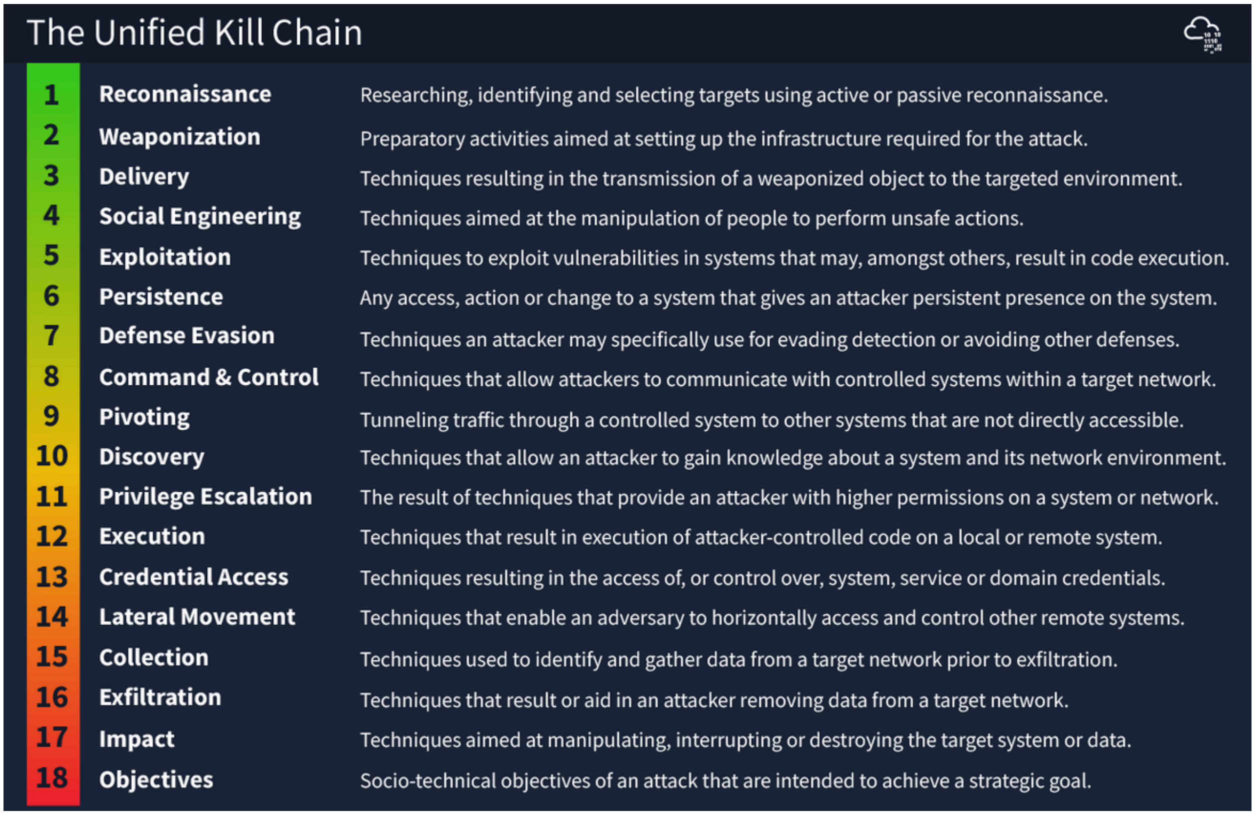
Unified Kill Chain
May 2025

TryHackMe.com
Alex Bondarchuk

27 May 2025

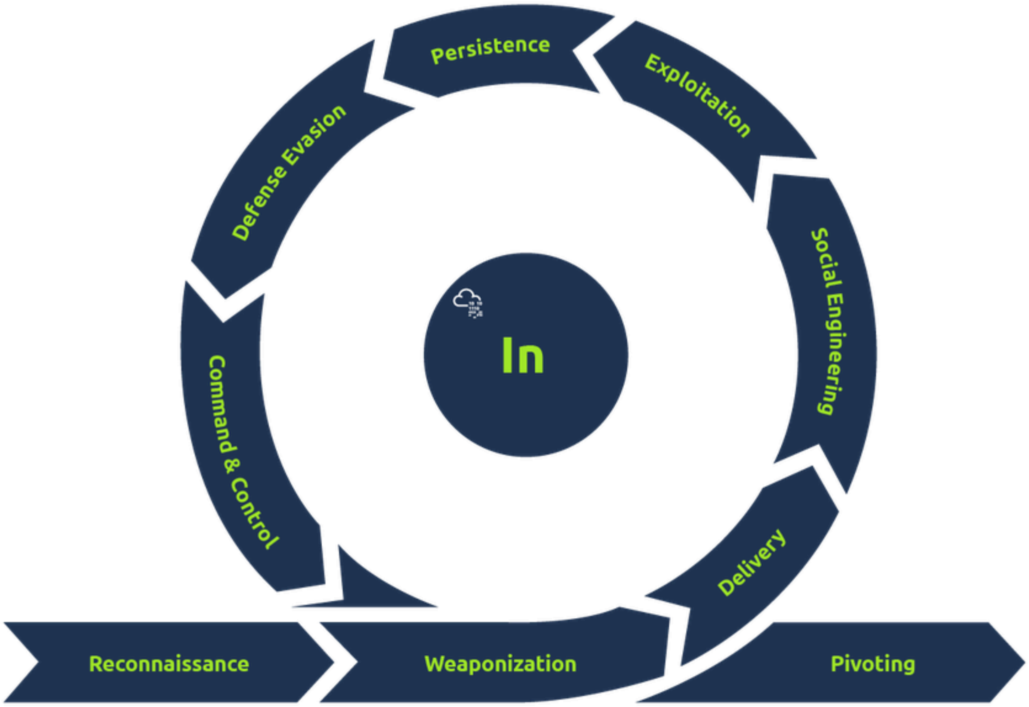
The UKC states that there are 18 phases to an attack: Everything from reconnaissance to data exfiltration and understanding an attacker's motive.



The Unified Kill Chain

1	**Reconnaissance**	Researching, identifying and selecting targets using active or passive reconnaissance.
2	**Weaponization**	Preparatory activities aimed at setting up the infrastructure required for the attack.
3	**Delivery**	Techniques resulting in the transmission of a weaponized object to the targeted environment.
4	**Social Engineering**	Techniques aimed at the manipulation of people to perform unsafe actions.
5	**Exploitation**	Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.
6	**Persistence**	Any access, action or change to a system that gives an attacker persistent presence on the system.
7	**Defense Evasion**	Techniques an attacker may specifically use for evading detection or avoiding other defenses.
8	**Command & Control**	Techniques that allow attackers to communicate with controlled systems within a target network.
9	**Pivoting**	Tunneling traffic through a controlled system to other systems that are not directly accessible.
10	**Discovery**	Techniques that allow an attacker to gain knowledge about a system and its network environment.
11	**Privilege Escalation**	The result of techniques that provide an attacker with higher permissions on a system or network.
12	**Execution**	Techniques that result in execution of attacker-controlled code on a local or remote system.
13	**Credential Access**	Techniques resulting in the access of, or control over, system, service or domain credentials.
14	**Lateral Movement**	Techniques that enable an adversary to horizontally access and control other remote systems.
15	**Collection**	Techniques used to identify and gather data from a target network prior to exfiltration.
16	**Exfiltration**	Techniques that result or aid in an attacker removing data from a target network.
17	**Impact**	Techniques aimed at manipulating, interrupting or destroying the target system or data.
18	**Objectives**	Socio-technical objectives of an attack that are intended to achieve a strategic goal.

The initial phase of the attack (AKA ‘in’) is the first 9 steps of the 18 steps in the UKC. in these steps the attacker mostly gathers information about systems, structure, social engineering approaches and secures their foothold.



Reconnaissance: The foothold step of the whole attack process, in this stage the attacker finds crucial information that will be used through-out their whole attack. Information such:

- Employees that can be social engineered.
- Systems that are used. These can be both software and hardware.
- Lingo that is used inside the organization that can be used for navigation or further selling social engineering.
- Network topology to be used for the first stages and post the 'pivoting' stage.

Weaponization: The stage where the attacker decides which approach they will take, whether it is a 'command and control', Reverse SSH, Ransomware, Malicious PDF or trojan to name a few.

Delivery: The Sage where the attacker tries to launch their attack. This can be done through multiple ways, most of which realistically involve Social Engineering. Examples of possible delivery methods: Phishing, Smishing, Watering Hole and etc.

Social Engineering: The stage where the attacker will manipulate employees to assist with their attack. Phishing, trying to get them to open malicious mail, impersonating a webpage, etc. They would try to establish access to the internal network either directly via a macro/script or even stealing employee credentials to then use as a part of the deployment and later post pivoting stage.

Exploitation: The stage where the attack exploits a vulnerability they found. It can be reverse shell via application, manipulation of a local script or SQL injection to name a few.

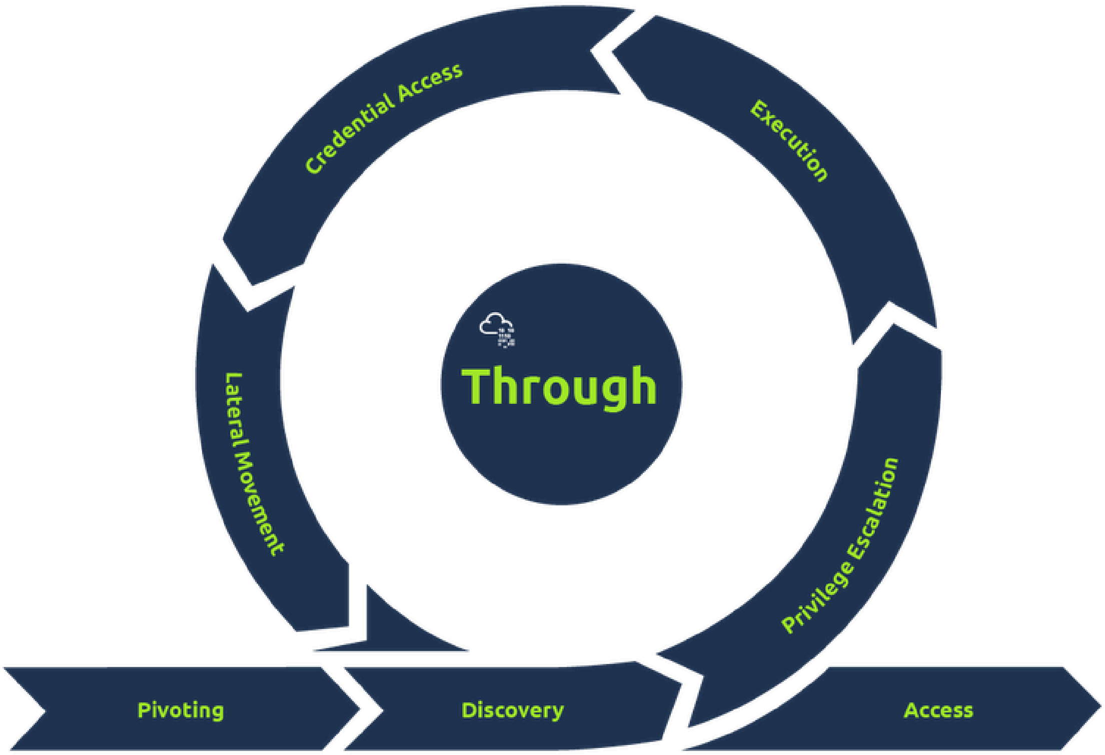
Persistence: A short stage in the attackers plan, this stage ensures the attacker can maintain access and control over the exploited environment like leaving a backdoor.

Defense Evasion: Perhaps the most crucial part, if this stage would have been a game mechanic it would be stealth and detection. The attacker will avoid detection systems that have been set in place. Firewalls, antiviruses and any other intrusion detection system.

Command & Control: Using the established method during the 'Weaponization' stage the attacker then establishes a direct connection between itself and the target.

Pivoting: The stage the attacker escalates their access inside the internal otherwise blocked off environment.

The next stage of the attack involves stage 9 to 14 of the UKC. These are the stages the attacker seeks to gain additional access to other systems and data needed for their goals.



Discovery: The attacker at this stage would uncover information about the system and the network it is connected to. Within this stage, the knowledge base would be built from the active user accounts, the permissions granted, applications and software in use, web browser activity, files, directories and network shares, and system configurations.

Privilege Escalation: Using the knowledge gathered in the last step the attacker then proceeds to gain more escalated access following the pivot concept. Using compromised high value admin accounts, or getting root access via other means.

Execution: This is where the attacker executes their malicious code on the pivoting system as the host. Back door is created here to maintain persistence.

Credential Access: Working hand in hand with the Privilege Escalation stage, the adversary would attempt to steal account names and passwords through various methods, including keylogging and credential dumping. This makes them harder to detect during their attack as they would be using legitimate credentials.

Lateral Movement: With the credentials and elevated privileges, the adversary would seek to move through the network and jump onto other targeted systems to achieve their primary objective.

The rest of the phases are focused on where the attacker has the access in the environment to achieve their desired goals.

Collection: At this stage the attacker uses all of their gained access to collect information and desired data compromising the privacy of the organization's data.

Exfiltration: At this stage to elevate their compromise, the adversary would seek to steal data, which would be packaged using encryption measures and compression to avoid any detection. The C2 channel and tunnel deployed in the earlier phases will come in handy during this process.

Impact: At this stage if the attacker seeks to compromise the integrity of the stolen data they can manipulate, wipe or steal it. They can do things such as DDOS, encrypt it for ransomware or even simply wipe it all.

Objectives: With all the power and access to the systems and network, the adversary would seek to achieve their strategic goal for the attack.For example, if the attack was financially motivated, they may seek to encrypt files and systems with ransomware and ask for payment to release the data.