Unified Kill Chain

Framework that is used to help understand how cyber attacks occur.
WHAT IS A "kILL CHAIN"

Originating from the military, a "Kill Chain" is a term used to explain the various stages of an attack. In the realm of cybersecurity, a "Kill Chain" is used to describe the methodology/path attackers such as hackers or APTs use to approach and intrude a target.

For example, an attacker scanning, exploiting a web vulnerability, and escalating privileges will be a "Kill Chain". We will come to explain these stages in much further detail later in this room.

The objective is to understand an attacker's "Kill Chain" so that defensive measures can be put in place to either pre-emptively protect a system or disrupt an attacker's attempt.

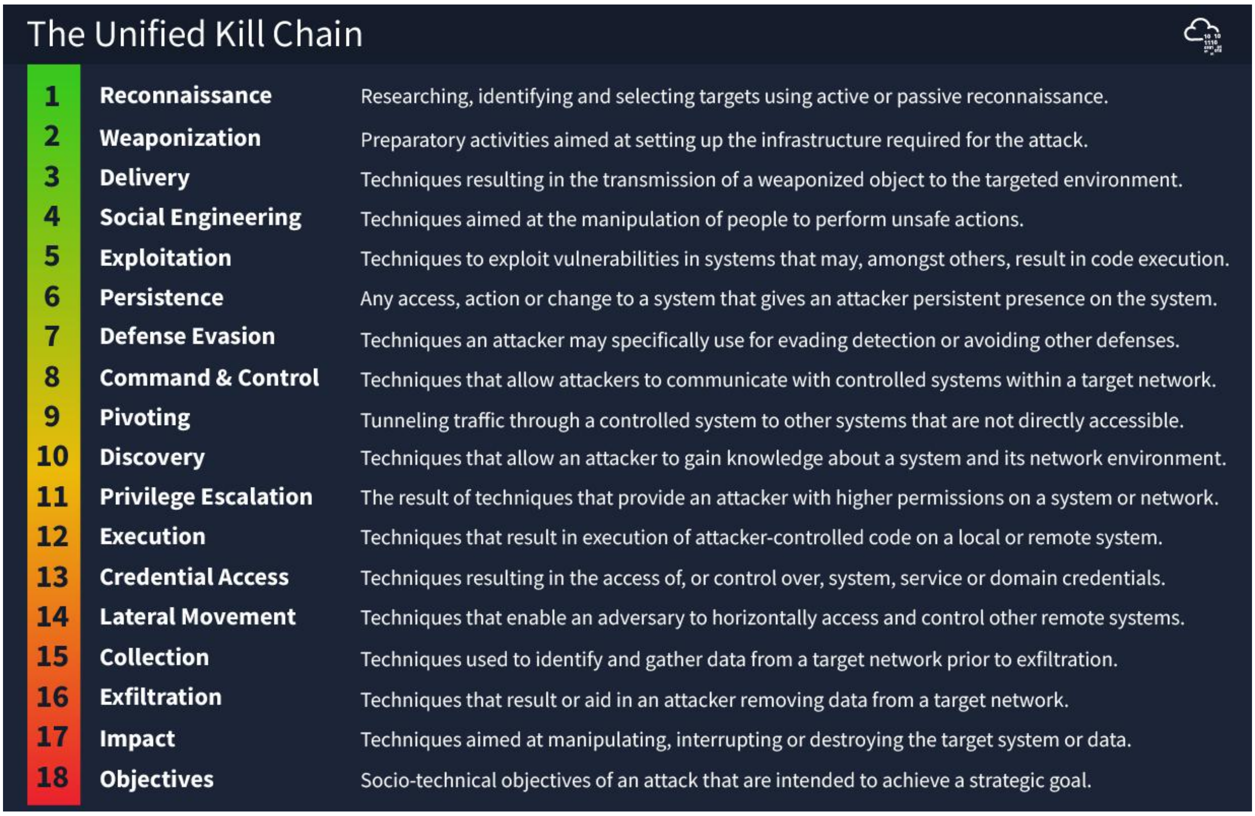
What is "threat modlling"

Threat modelling, in a cybersecurity context, is a series of steps to ultimately improve the security of a system. Threat modelling is about identifying risk and essentially boils down to:

1. Identifying what systems and applications need to be secured and what function they serve in the environment. For example, is the system critical to normal operations, and is a system holding sensitive information like payment info or addresses?
2. Assessing what vulnerabilities and weaknesses these systems and applications may have and how they could be potentially exploited
3. Creating a plan of action to secure these systems and applications from the vulnerabilities highlighted
4. Putting in policies to prevent these vulnerabilities from occurring again where possible (for example, implementing a software development life cycle (SDLC) for an application or training employees on phishing awareness).

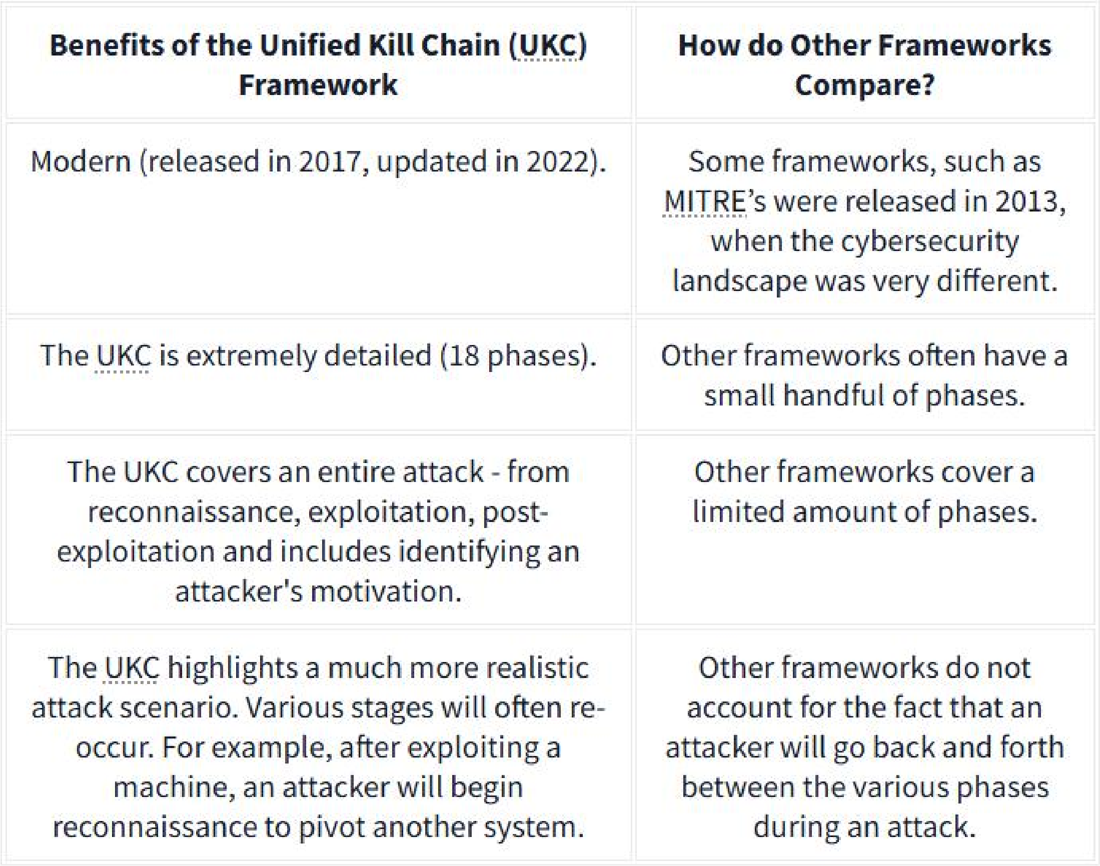
Threat modelling is an important procedure in reducing the risk within a system or application, as it creates a high-level overview of an organisation's IT assets (*an asset in IT is a piece of software or hardware*) and the procedures to resolve vulnerabilities.

The UKC can encourage threat modelling as the UKC framework helps identify potential attack surfaces and how these systems may be exploited.



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.



Benefits of the Unified Kill Chain (UKC) Framework	How do Other Frameworks Compare?
Modern (released in 2017, updated in 2022).	Some frameworks, such as MITRE's were released in 2013, when the cybersecurity landscape was very different.
The UKC is extremely detailed (18 phases).	Other frameworks often have a small handful of phases.
The UKC covers an entire attack - from reconnaissance, exploitation, post-exploitation and includes identifying an attacker's motivation.	Other frameworks cover a limited amount of phases.
The UKC highlights a much more realistic attack scenario. Various stages will often re-occur. For example, after exploiting a machine, an attacker will begin reconnaissance to pivot another system.	Other frameworks do not account for the fact that an attacker will go back and forth between the various phases during an attack.

Phase IN

Reconnaissance (MITRE tactic TA0043)

This phase of the UKC describes techniques that an adversary employs to gather information relating to their target. This can be achieved through means of passive and active reconnaissance. The information gathered during this phase is used all throughout the later stages of the UKC (such as the initial foothold)

Weaponization (MITRE Tactic TA0001)

This phase of the UKC describes the adversary setting up the necessary infrastructure to perform the attack. For example, this could be setting up a command and control server, or a system capable of catching reverse shells and delivering payloads to the system.

Social Engineering (MITRE Tactic TA0001)

This phase of the UKC describes techniques that an adversary can employ to manipulate employees to perform actions that will aid in the adversaries attack.

Exploitation (MITRE Tactic TA0002)

This phase of the UKC describes how an attacker takes advantage of weaknesses or vulnerabilities present in a system. The UKC defines "Exploitation" as abuse of vulnerabilities to perform code execution.

Persistence (MITRE Tactic TA0003)

This phase of the UKC is rather short and simple. Specifically, this phase of the UKC describes the techniques an adversary uses to maintain access to a system they have gained an initial foothold on

Defence Evasion (MITRE Tactic TA0005)

The "Defence Evasion" section of the UKC is one of the more valuable phases of the UKC. This phase specifically is used to understand the techniques an adversary uses to evade defensive measures put in place in the system or network

Command & Control (MITRE Tactic TA0011)

The "Command & Control" phase of the UKC combines the efforts an adversary made during the "Weaponization" stage of the UKC to establish communications between the adversary and target system.

Pivoting (MITRE Tactic TA0008)

"Pivoting" is the technique an adversary uses to reach other systems within a network that are not otherwise accessible (for example, they are not exposed to the internet). There are often many systems in a network that are not directly reachable and often contain valuable data or have weaker security.

Phase: Through

Pivoting (MITRE Tactic TA0008)

Once the attacker has access to the system, they would use it as their staging site and a tunnel between their command operations and the victim's network. The system would also be used as the distribution point for all malware and backdoors at later stages.

Discovery (MITRE Tactic TA0007)

The adversary 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 (MITRE Tactic TA0004)

Following their knowledge-gathering, the adversary would try to gain more prominent permissions within the pivot system. They would leverage the information on the accounts present with vulnerabilities and misconfigurations found to elevate their access to one of the following superior levels:

- SYSTEM/ ROOT.
- Local Administrator.
- A user account with Admin-like access.
- A user account with specific access or functions.

Execution (MITRE Tactic TA0002)

This is where they deploy their malicious code using the pivot system as their host. Remote trojans, C2 scripts, malicious links and scheduled tasks are deployed and created to facilitate a recurring presence on the system and uphold their persistence.

Credential Access (MITRE Tactic TA0006)

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 (MITRE Tactic TA0008)

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 stealthier the technique used, the better.

Phase: OUT

Collection MITRE Tactic (TA0009)

After all the hunting for access and assets, the adversary will be seeking to gather all the valuable data of interest. This, in turn, compromises the confidentiality of the data and would lead to the next attack stage – Exfiltration. The main target sources include drives, browsers, audio, video and email.

Exfiltration (MITRE Tactic TA0010)

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 (MITRE Tactic TA0040)

If the adversary seeks to compromise the integrity and availability of the data assets, they would manipulate, interrupt or destroy these assets. The goal would be to disrupt business and operational processes and may involve removing account access, disk wipes, and data encryption such as ransomware, defacement and denial of service (DoS) attacks.

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. In other instances, the attacker may seek to damage the reputation of the business, and they would release private and confidential information to the public.