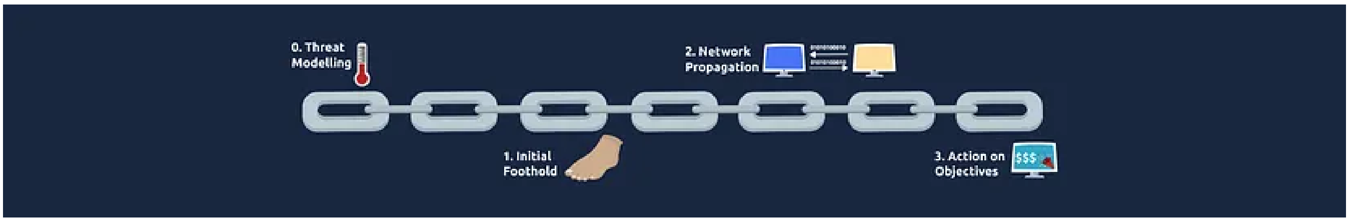
Unified Kill Chain | Tryhackme Writeup/Walkthrough | By Md Amiruddin

Md Amiruddin · Follow

13 min read · Feb 18, 2023

Listen Share More

The Unified Kill Chain is a framework which establishes the phases of an attack, and a means of identifying and mitigating risk to IT assets.



Task 1 : Introduction

Understanding the behaviours, objectives and methodologies of a cyber threat is a vital step to establishing a strong cybersecurity defence (known as a cybersecurity posture).

In this room, you will be introduced to the UKC (Unified Kill Chain) framework that is used to help understand how cyber attacks occur.

Learning Objectives:

- Understanding why frameworks such as the UKC are important and helpful in establishing a good cybersecurity posture
- Using the UKC to understand an attacker’s motivation, methodologies and tactics
- Understanding the various phases of the UKC
- Discover that the UKC is a framework that is used to complement other frameworks such as MITRE.

Task 2 : 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.

Answer the questions below :

```
   Where does the term "Kill Chain" originate from?
1. For this answer, you must fill in the blank!: The ********
A. military
```

Task 3 : What is “Threat Modelling”

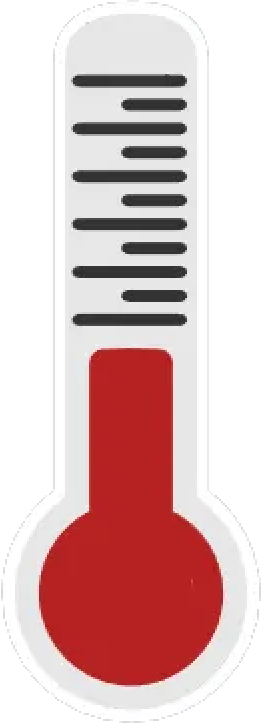
Threat modelling, in a cybersecurity context, is a series of steps to ultimately improve the security of a system. Threat modelling is about identifying risk and essentially boils down to:

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.

STRIDE, DREAD and CVSS (to name a few) are all frameworks specifically used in threat modelling. If you are interested to learn more, check out the "Principles of Security" room on TryHackMe.

Answer the questions below :

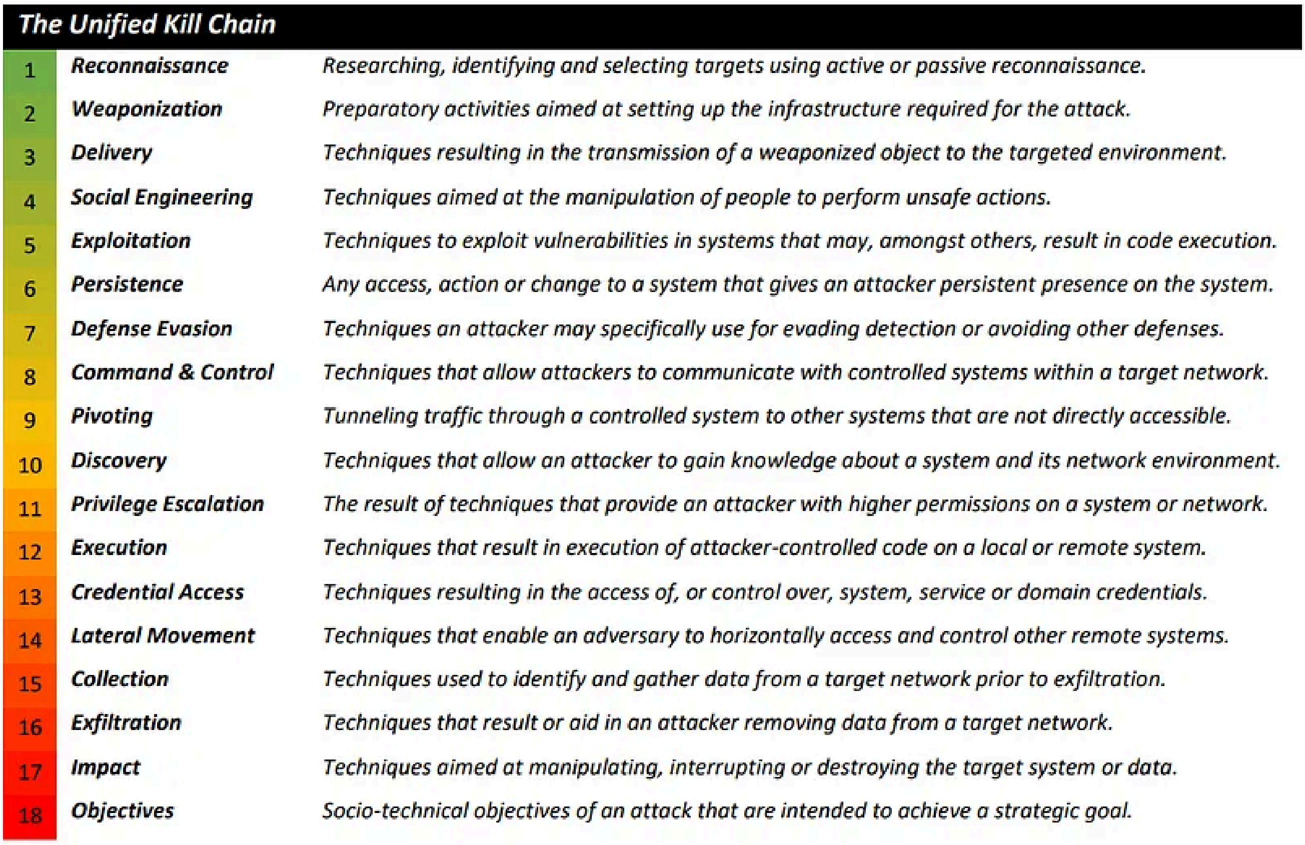
```
1. What is the technical term for a piece of software or hardware in IT (Inform
A. asset
```

Task 4 : Introducing the Unified Kill Chain

To continue from the previous task, the Unified Kill Chain published in 2017, aims to complement (**not compete**) with other cybersecurity kill chain frameworks such as Lockheed Martin's and MITRE's ATT&CK.

The UKC states that there are 18 phases to an attack: Everything from reconnaissance to data exfiltration and understanding an attacker's motive. These phases have been grouped together in this room into a few areas of focus for brevity, which will be detailed in the remaining tasks.

Some large benefits of the UKC over traditional cybersecurity kill chain frameworks include the fact that it is modern and extremely detailed (**reminder**: it has 18 phases officially, whereas other frameworks may have a small handful)



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

Modern (released in 2017, updated in 2022)

The UKC is extremely detailed (18 phases).

The UKC covers an entire attack — from reconnaissance, exploitation, post-exploitation and includes identifying an attacker's motivation.

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.

How do Other Frameworks Compare?

Some frameworks, such as MITRE's were released in 2013, when the cybersecurity landscape was very different.

Other frameworks often have a small handful of phases.

Other frameworks cover a limited amount of phases.

Other frameworks do not account for the fact that an attacker will go back and forth between the various phases during an attack.

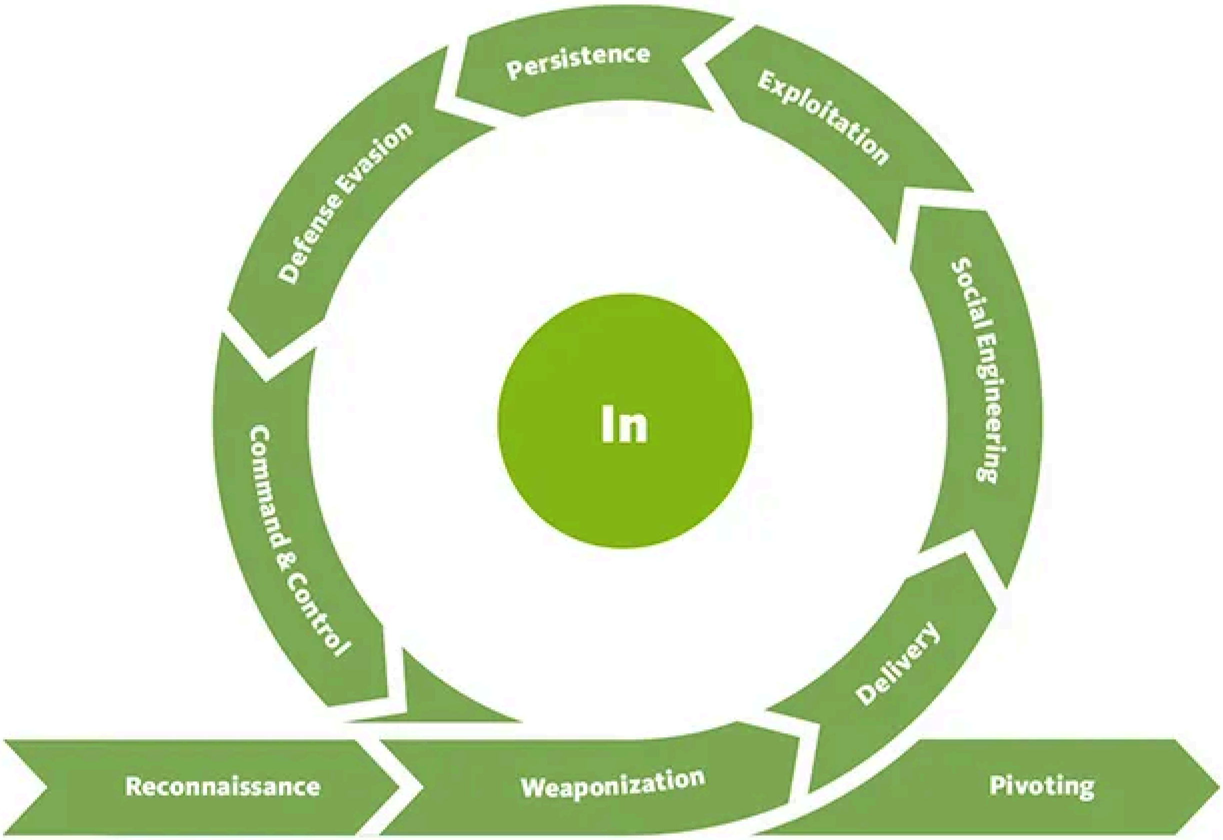
Answer the questions below :

```
1. In what year was the Unified Kill Chain framework released?
A. 2017

2. According to the Unified Kill Chain, how many phases are there to an attack?
A. 18

3. What is the name of the attack phase where an attacker employs techniques to
A. Defense Evasion

4. What is the name of the attack phase where an attacker employs techniques to
A. Exfiltration

5. What is the name of the attack phase where an attacker achieves their object
A. Objectives
```

Task 5 Phase: In (Initial Foothold)

The main focus of this series of phases is for an attacker to gain access to a system or networked environment.

An attacker will employ numerous tactics to investigate the system for potential vulnerabilities that can be exploited to gain a foothold in the system. For example, a common tactic is the use of reconnaissance against a system to discover potential attack vectors (such as applications and services).



This series of phases also accommodates for an attacker creating a form of persistence (such as files or a process that allows the attacker to connect to the machine at any time). Finally, the UKC accounts for the fact that attackers will often use a combination of the tactics listed above.

We will explore the different phases of this section of the UKC in the headings below:

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).

Information gathered from this phase can include:

- Discovering what systems and services are running on the target, this is beneficial information in the weaponisation and exploitation phases of this section.
- Finding contact lists or lists of employees that can be impersonated or used in either a social engineering or phishing attack.
- Looking for potential credentials that may be of use in later stages, such as pivoting or initial access.
- Understanding the network topology and other networked systems can be used to pivot too.

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. For example, a social engineering attack could include:

- Getting a user to open a malicious attachment.
- Impersonating a web page and having the user enter their credentials.
- Calling or visiting the target and impersonating a user (for example, requesting a password reset) or being able to gain access to areas of a site that the attacker would not previously be capable of (for example, impersonating a utility engineer).

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. For example:

- Uploading and executing a reverse shell to a web application.
- Interfering with an automated script on the system to execute code.
- Abusing a web application vulnerability to execute code on the system it is running on.

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. For example:

- Creating a service on the target system that will allow the attacker to regain access.
- Adding the target system to a Command & Control server where commands can be executed remotely at any time.
- Leaving other forms of backdoors that execute when a certain action occurs on the system (i.e. a reverse shell will execute when a system administrator logs in).

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. For example, this could be:

- Web application firewalls.
- Network firewalls.
- Anti-virus systems on the target machine.
- Intrusion detection systems.

This phase is valuable when analysing an attack as it helps form a response and better yet — gives the defensive team information on how they can improve their defence systems in the future.

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.

An adversary can establish command and control of a target system to achieve its action on objectives. For example, the adversary can:

- Execute commands.
- Steal data, credentials and other information.
- Use the controlled server to pivot to other systems on the network.

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.

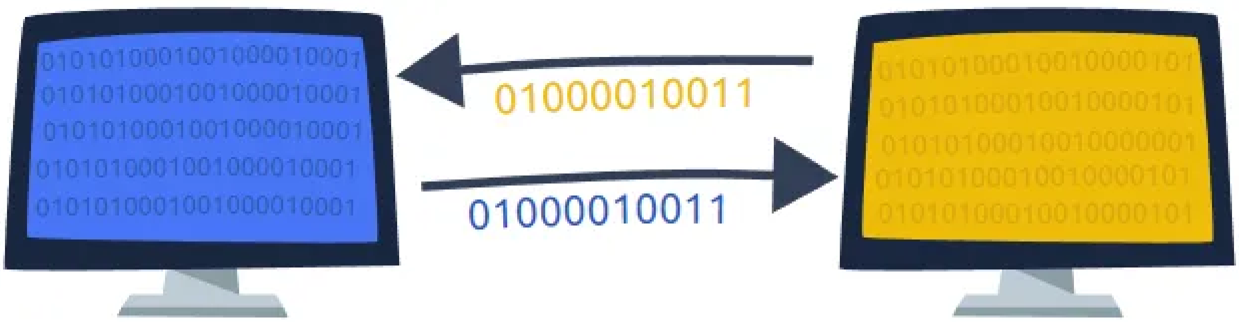
For example, an adversary can gain access to a web server that is publically accessible to attack other systems that are within the same network (but are not accessible via the internet).

Answer the questions below :

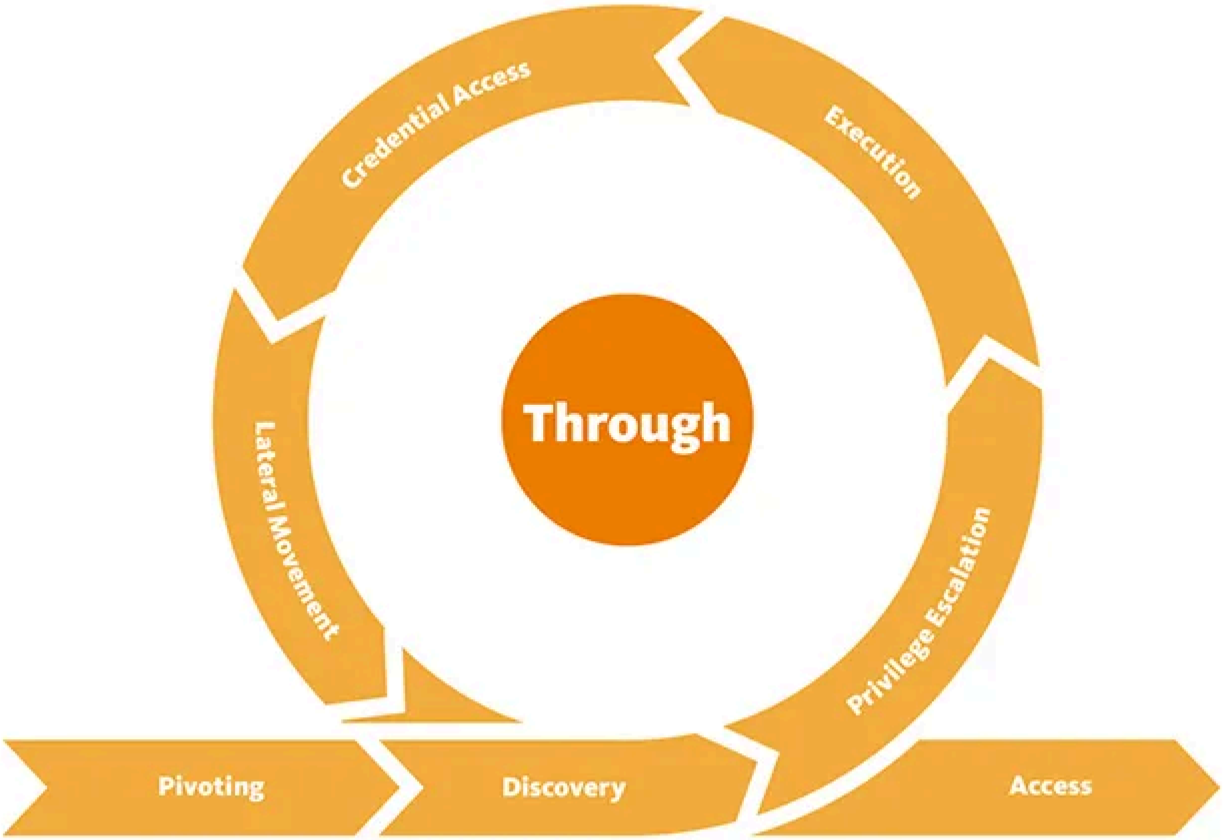
```
1. What is an example of a tactic to gain a foothold using emails?
A. Phishing

2. Impersonating an employee to request a password reset is a form of what?
A. Social Engineering

3. An adversary setting up the Command & Control server infrastructure is what
A. Weaponization

4. Exploiting a vulnerability present on a system is what phase of the Unified
A. Exploitation

5. Moving from one system to another is an example of?
A. Pivoting
```

```
6. Leaving behind a malicious service that allows the adversary to log back int
A. Persistence
```

Task 6 Phase: Through (Network Propagation)



This phase follows a successful foothold being established on the target network. An attacker would seek to gain additional access and privileges to systems and data to fulfil their goals. The attacker would set up a base on one of the systems to act as their pivot point and use it to gather information about the internal network.



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)

Recall when the adversary set up their attack infrastructure. 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. and weaponised payloads? 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)

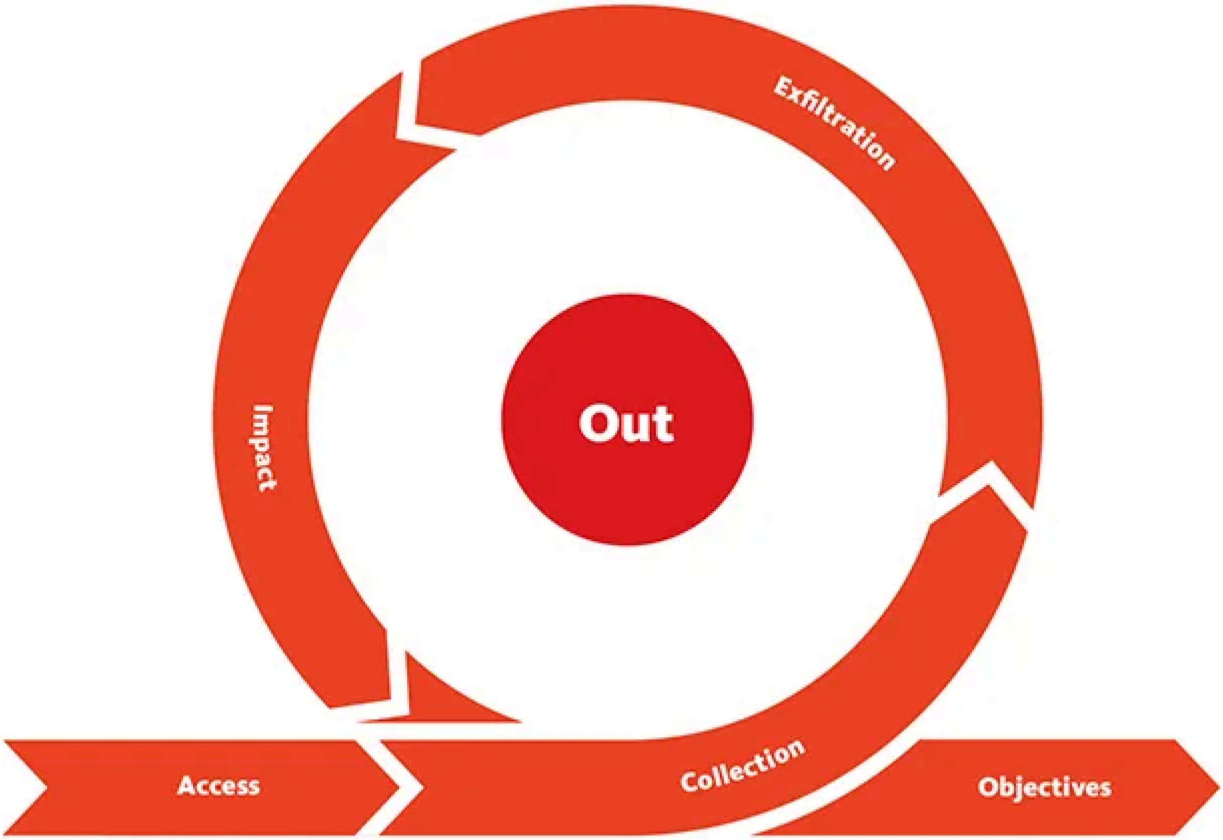
With the credentials and elevated privileges, the adversary would seek to move through the network and jump onto other targeted systems to achieve their primary objective. The stealthier the technique used, the better.

Answer the questions below :

```
1. As a SOC analyst, you pick up numerous alerts pointing to failed login attem
A. Privilege Escalation

2. Mimikatz, a known attack tool, was detected running on the IT Manager's comp
A. credential dumping
```

Task 7 Phase: Out (Action on Objectives)

This phase wraps up the journey of an adversary's attack on an environment, where they have critical asset access and can fulfil their attack goals. These goals are usually geared toward compromising the confidentiality, integrity and availability (CIA) triad.



The tactics to be deployed by an attacker would include:

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.

Answer the questions below :

```
1. While monitoring the network as a SOC analyst, you realise that there is a s
A. Exfiltration

2. Personally identifiable information (PII) has been released to the public by
A. confidentiality
```

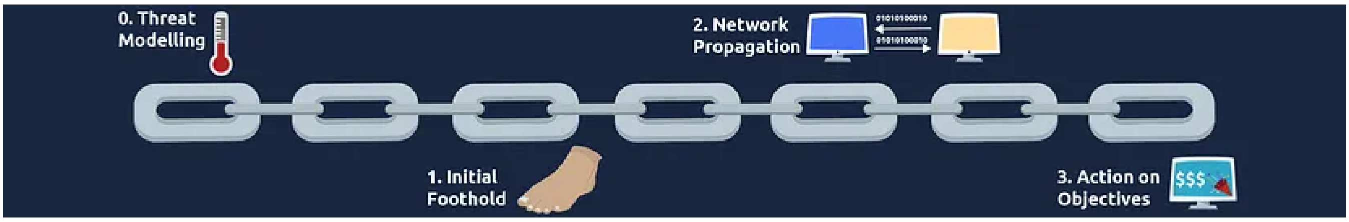
Task 8 : Practical

Deploy the static site attached to the task. You will need to match the various actions of an attacker to the correct phase of the Unified Kill Chain framework to reveal the flag.

Answer the questions below :

```
1. Match the scenario prompt to the correct phase of the Unified Kill Chain to
A. THM{UKC_SCENARIO}
```

Task 9 : Conclusion



Congrats on making it through the Unified Kill Chain room. Hopefully, you understand the importance that frameworks such as the UKC play in identifying risk and potential mitigating attacks by reconstructing the various steps an attacker took.

As mentioned in this room, the UKC is a modern extension of other frameworks, such as Lockheed Martin's "Cyber Kill Chain" framework. If you are interested in learning more about frameworks in cybersecurity (highly recommended!), you should check out these rooms on TryHackMe:

- Principles of Security
- Pentesting Fundamentals
- Cyber Kill Chain

Thankyou For Reading.

> *Please Follow for more such amazing Content.*

Tryhackme Cybersecurity Security Information Technology

Information Security

Follow

Written by Md Amiruddin

155 Followers · 6 Following

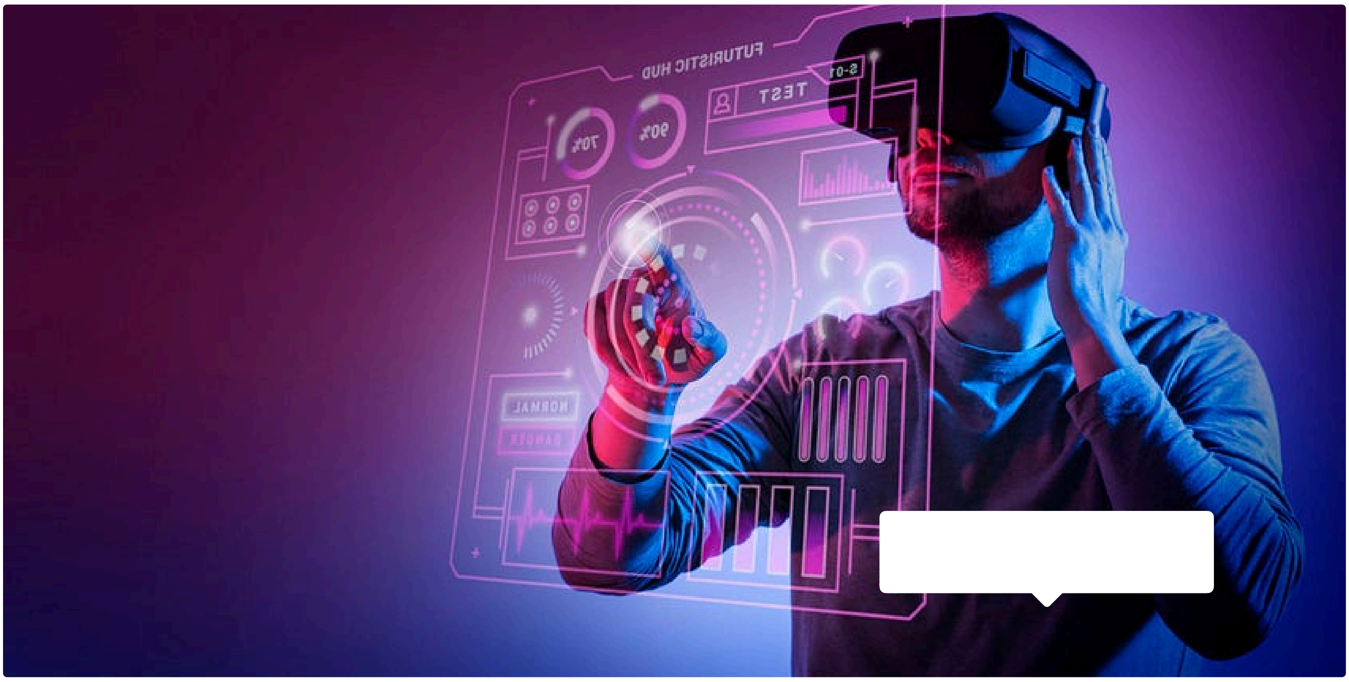
This is a profile of a cybersecurity enthusiast and CTF writer. He is an experienced information security professional and highly motivated individual.

No responses yet

What are your thoughts?

Respond

More from Md Amiruddin



In InfoSec Write-ups by Md Amiruddin

Vulnhub Writeup/Walkthrough SickOS 1.1 | By Md Amiruddin

This CTF walkthrough is similar to the labs found in the OSCP exam course.

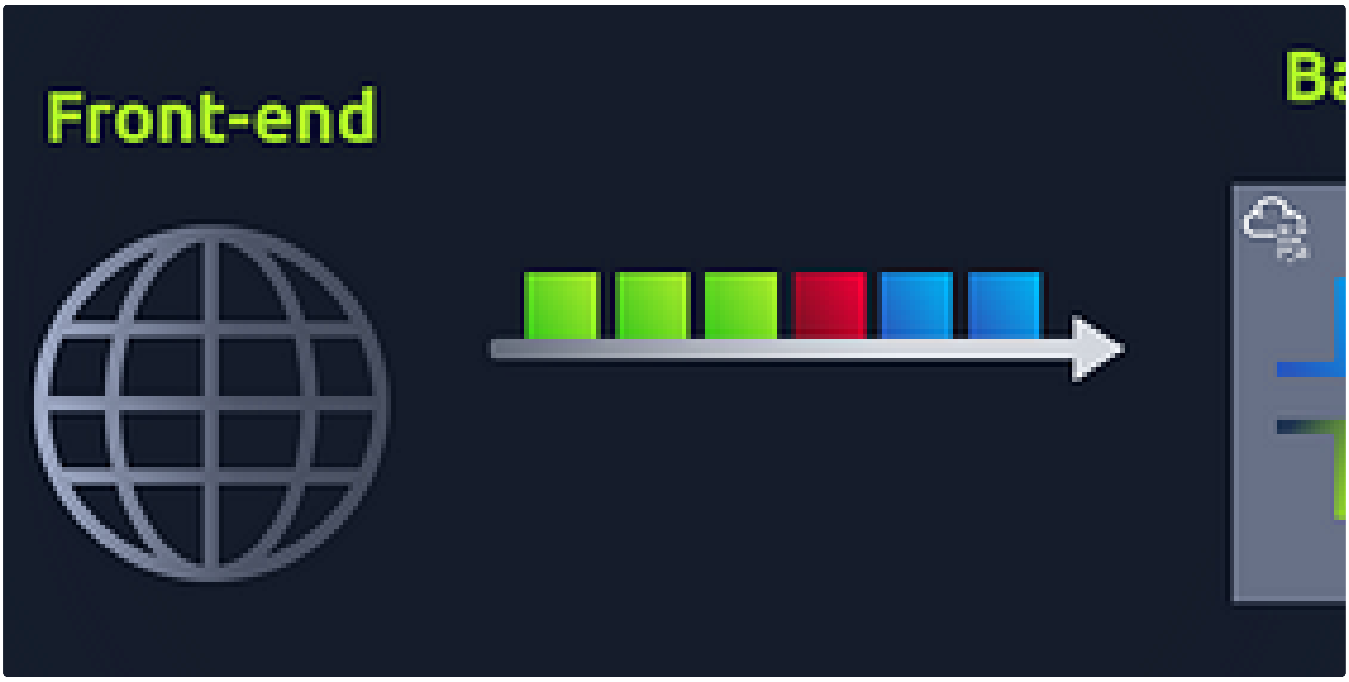
Dec 21, 2022

In InfoSec Write-ups by Md Amiruddin

Intro to Docker | Tryhackme Writeup/Walkthrough | By Md Amiruddin

Learn to create, build and deploy Docker containers!

May 5, 2023 5



In InfoSec Write-ups by Md Amiruddin

HTTP Request Smuggling | Tryhackme Writeup/Walkthrough | By Md Amiruddin

Learn about HTTP Request Smuggling and its different techniques.

Jan 29, 2024 109 2

In InfoSec Write-ups by Md Amiruddin

MITRE | Tryhackme Room Writeup/Walkthrough | By Md Amiruddin

This room will discuss the various resources MITRE has made available for the cybersecurity community.

Mar 20, 2023 2

See all from Md Amiruddin

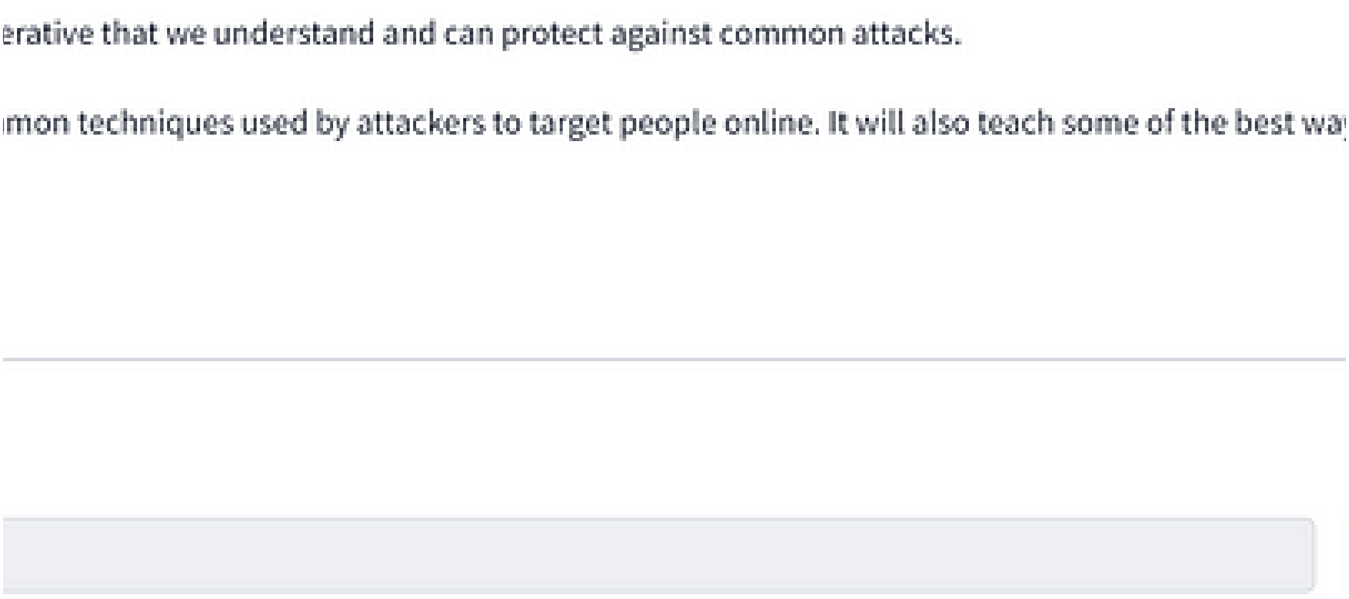
Recommended from Medium

Trnty

TryHackMe | Introduction To Honeypots Walkthrough

A guided room covering the deployment of honeypots and analysis of botnet activities

Sep 7, 2024 10



erative that we understand and can protect against common attacks.

mon techniques used by attackers to target people online. It will also teach some of the best wa

Daniel Schwarzentraub

Tryhackme Free Walk-through Room: Common Attacks

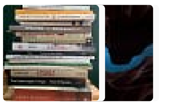
Tryhackme Free Walk-through Room: Common Attacks

Sep 13, 2024

Lists

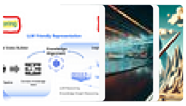
Open in app ↗

Medium Search



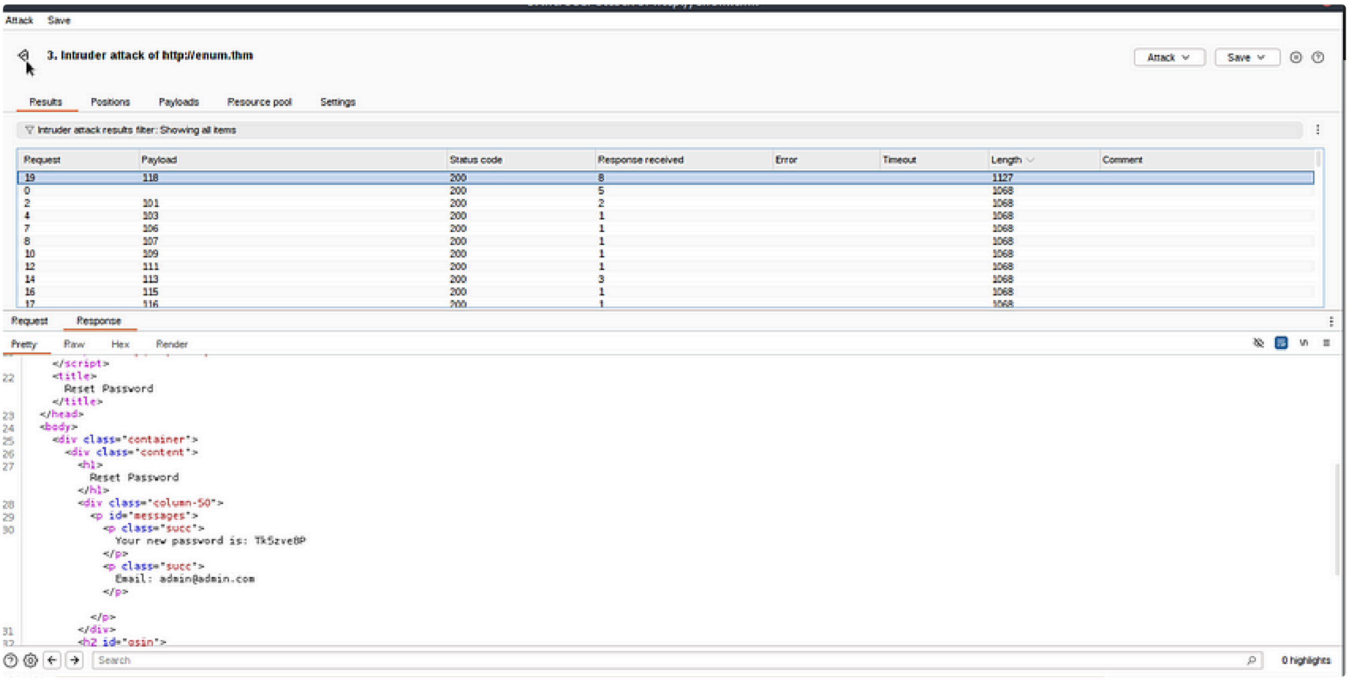
Staff picks

793 stories · 1548 saves



Natural Language Processing

1883 stories · 1521 saves


Attack Save
3. Intruder attack of http://enum.thm
Attack
Save
Results
Positions
Payloads
Resource pool
Settings
Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
19	118	200	8			1127	
0		200	5			1068	
2	101	200	2			1068	
4	103	200	1			1068	
7	106	200	1			1068	
8	107	200	1			1068	
10	109	200	1			1068	
12	111	200	1			1068	
14	113	200	3			1068	
16	115	200	1			1068	
17	116	200	1			1068	

```
    </script>
    <title>
      Reset Password
    </title>
  </head>
  <body>
    <div class="container">
      <div class="content">
        <h1>
          Reset Password
        </h1>
        <div class="column-50">
          <p id="messages">
            <p class="succ">
              Your new password is: Tk5zve8P
            </p>
            <p class="succ">
              Email: admin@admin.com
            </p>

          </p>
        </div>
        <h2 id="osin">
```

embossdotar

TryHackMe — Enumeration & Brute Force — Writeup

Key points: Enumeration | Brute Force | Exploring Authentication Mechanisms | Common Places to Enumerate | Verbose Errors | Password Reset…

✦ Jul 31, 2024 👏 26

Abhijeet Singh

Advent of Cyber 2024 [Day 3] Even if I wanted to go, their vulnerabilities wouldn’t allow it.

So, Let's Start with the Questions. I hope you already read the story and all the given instructions —

✦ Dec 4, 2024 👏 2

In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

✦ Nov 28, 2024 👏 50

Sunny Singh Verma [SuNnY]

Multi-Factor Authentication TryHackMe Writeup | Detailed | → SuNnY

Room PreRequisites

Sep 4, 2024 👏 50

See more recommendations