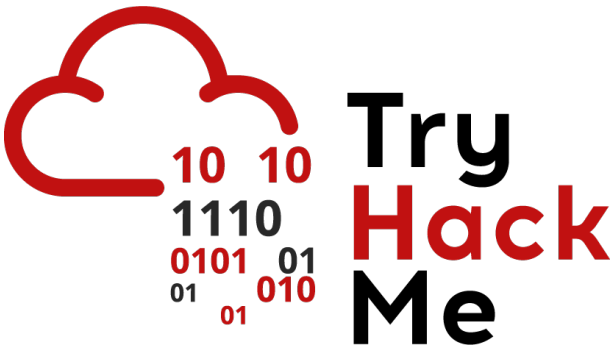
Writeup: Sala *Cyber Kill Chain*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

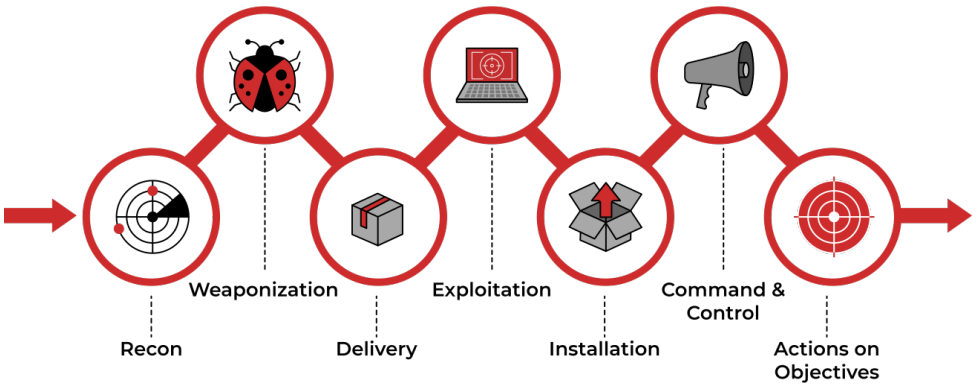
1. Introducción

La sala Cyber Kill Chain de TryHackMe consta de 10 tareas donde vamos a aprender los fundamentos de un modelo ampliamente utilizado en ciberseguridad, veremos como se descompone un ciberataque en siete fases distintas. Además, aprenderemos cómo los atacantes planifican y ejecutan intrusiones, y cómo cada etapa puede ser identificada y detenida.

2. Sala

2.1. Tarea 1 - Introducción

Empezamos con una introducción a la Cyber Kill Chain que es un modelo desarrollado gracias a **Lockheed Martin** en 2011, basado en conceptos militares donde describe las etapas que sigue un atacante para llevar a cabo un ciberataque exitoso. Este marco ayuda en identificar y detener ataques en cada fase del proceso.



Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

2.2. Tarea 2 - Reconocimiento

En esta tarea aprenderemos como el atacante recolecta información sobre su objetivo antes de realizar cualquier ataque directo. Este proceso puede incluir la búsqueda

de datos en redes sociales, dominios públicos, direcciones IP, tecnologías utilizadas, correos electrónicos y cualquier dato útil que permita planificar un ataque más preciso. También aprendemos la diferencia entre una recolección de información **pasiva** y **activa**.

Por último, se mencionan herramientas como **theHarvester**, **Shodan** o simplemente técnicas de **OSINT** (Open Source Intelligence) que son comunes en esta etapa.

Ahora que aprendimos sobre la fase de reconocimiento podemos responder las siguientes preguntas:

Pregunta: What is the name of the Intel Gathering Tool that is a web-based interface to the common tools and resources for open-source intelligence?

Respuesta: **OSINT Framework**

Pregunta: What is the definition for the email gathering process during the stage of reconnaissance?

Respuesta: **email harvesting**

2.3. Tarea 3 - Armatización

Aquí aprenderemos como el atacante toma la información obtenida durante el reconocimiento y la utiliza para crear una carga útil (**payload**) maliciosa personalizada. Esta etapa no involucra contacto directo con el objetivo, pero es crítica porque define cómo se ejecutará el ataque más adelante. Este proceso típico consta de:

- Seleccionar un exploit basado en una vulnerabilidad identificada.
- Luego, combinarlo con un malware o backdoor, como un troyano, para crear un archivo ejecutable o documento malicioso.
- Por último, preparar un vector de entrega, como un archivo adjunto de correo o un enlace malicioso.

Una vez que aprendimos esta tarea vamos a responder la siguiente pregunta:

Pregunta: This term is referred to as a group of commands that perform a specific task. You can think of them as subroutines or functions that contain the code that most users use to automate routine tasks. But malicious actors tend to use them for malicious purposes and include them in Microsoft Office documents. Can you provide the term for it?

Respuesta: **Macro**

2.4. Tarea 4 - Entrega

Ahora aprenderemos como el atacante realiza la entrega al sistema objetivo utilizando algún método de transmisión. Este sería el primer contacto directo con la víctima, y puede realizarse mediante técnicas como:

- Correos electrónicos de phishing con archivos adjuntos maliciosos o enlaces engañosos.
- Websites comprometidos o creados específicamente para alojar malware.
- Dispositivos físicos, como memorias USB infectadas.

En esta fase el objetivo es lograr que la víctima interactúe con el archivo o enlace malicioso sin sospechar. Aquí suele entrar como ayuda la ingeniería social, manipulando al usuario para que ejecute el archivo o visite el enlace.

Ahora vamos a responder la siguiente pregunta de esta tarea.

Pregunta: What is the name of the attack when it is performed against a specific group of people, and the attacker seeks to infect the website that the mentioned group of people is constantly visiting.

Respuesta: **Watering hole attack**

2.5. Tarea 5 - Explotación

Ahora aprenderemos en esta tarea como el atacante aprovecha las vulnerabilidades identificadas para ejecutar código malicioso en el sistema objetivo.

Por ejemplo, en el escenario presentado, el atacante Megatron utilizó dos correos electrónicos de phishing: uno con un enlace a una página falsa de inicio de sesión de Office 365 y otro con un archivo adjunto que contenía macros maliciosas. Ambos métodos lograron que las víctimas interactuaran con los elementos maliciosos, permitiendo al atacante obtener acceso inicial al sistema. Una vez que el atacante se encuentra dentro puede:

- Explotar vulnerabilidades adicionales en software o sistemas para escalar privilegios.
- Moverse lateralmente dentro de la red para acceder a otros sistemas o datos sensibles.
- Utilizar exploits de día cero (**Zero-day**), que son vulnerabilidades desconocidas para los proveedores y por lo tanto no tienen parches disponibles.

Ahora que aprendimos sobre la explotación procederemos a responder la siguiente pregunta:

Pregunta: Can you provide the name for a cyberattack targeting a software vulnerability that is unknown to the antivirus or software vendors?

Respuesta: **Zero-day**

2.6. Tarea 6 - Instalación

Esta tarea comprenderemos como un atacante busca establecer persistencia en el sistema comprometido para mantener el acceso incluso después de reinicios o intentos de remediación. Esto se logra mediante la instalación de puertas traseras (**backdoors**) o la modificación de configuraciones del sistema que permitan el acceso continuo sin ser detectado.

Algunas técnicas o métodos que utilizan los atacantes son:

- **Modificación de claves de registro:** Agregar entradas en las claves de registro de Windows para ejecutar malware al iniciar el sistema.
- **Carpetas de inicio:** Colocar archivos maliciosos en las carpetas de inicio para que se ejecuten automáticamente al iniciar sesión.
- **Web shells:** Instalar scripts maliciosos en servidores web que permitan el control remoto del sistema comprometido.
- **Técnicas de evasión:** Utilizar métodos como **timestomping** para modificar las marcas de tiempo de los archivos y evitar la detección.

Después de aprender como funciona la fase de instalación podemos responder las siguientes preguntas:

Pregunta: Can you provide the technique used to modify file time attributes to hide new or changes to existing files?

Respuesta: **Timestomping**

Pregunta: Can you name the malicious script planted by an attacker on the webserver to maintain access to the compromised system and enables the webserver to be accessed remotely?

Respuesta: **Web shell**

2.7. Tarea 7 - Comando y Control

Ahora aprenderemos como establece un canal de comunicación entre el sistema comprometido y su infraestructura de control, conocido como **C2 (Command & Control)**. Este canal permite al atacante enviar instrucciones, ejecutar comandos, exfiltrar datos o desplegar cargas útiles adicionales en el sistema víctima.

Un malware instalado en el sistema afectado puede iniciar conexiones periódicas con el servidor C2 del atacante, un proceso denominado **beaconing**. Estas comunicaciones pueden utilizar diversos protocolos, siendo los más comunes:

- **HTTP/HTTPS:** Utilizando los puertos 80 y 443, respectivamente, para camuflar el tráfico malicioso entre el tráfico legítimo y evadir sistemas de detección.
- **DNS:** Mediante una técnica conocida como **DNS Tunneling**, donde la máquina infectada realiza solicitudes DNS constantes a un servidor controlado por el atacante, permitiendo el intercambio de datos encubiertos.

Por último, deja a entender que es importante destacar que la infraestructura **C2** puede estar alojada en servidores controlados directamente por el atacante o en sistemas previamente comprometidos, lo que añade una capa adicional de complejidad a la detección y mitigación de estas amenazas.

Después de un profundo estudio de esta tarea podemos responder la siguiente pregunta:

Pregunta: What is the C2 communication where the victim makes regular DNS requests to a DNS server and domain which belong to an attacker.

Respuesta: **DNS Tunneling**

2.8. Tarea 8 - Acciones sobre los Objetivos

Esta tarea representa el objetivo final del atacante, donde se ejecutan las acciones planificadas tras haber obtenido acceso y control sobre el sistema comprometido. Dependiendo de las motivaciones del atacante, estas acciones pueden variar y resultar lo siguiente:

- **Exfiltración de datos sensibles**.
- **Escalada de privilegios**.
- **Reconocimiento interno**.
- **Movimiento lateral** (Desplazarse a través de la red).
- **Eliminación de copias de seguridad y copias sombra**.
- **Corrupción o destrucción de datos**.

Al final estas acciones buscan maximizar el impacto del ataque, ya sea mediante la interrupción de operaciones, la obtención de beneficios económicos o el daño a la reputación de la organización.

Ahora que aprendimos sobre las acciones sobre los objetivos de un atacante podemos pasar a responder la siguiente pregunta:

Pregunta: Can you provide a technology included in Microsoft Windows that can create backup copies or snapshots of files or volumes on the computer, even when they are in use?

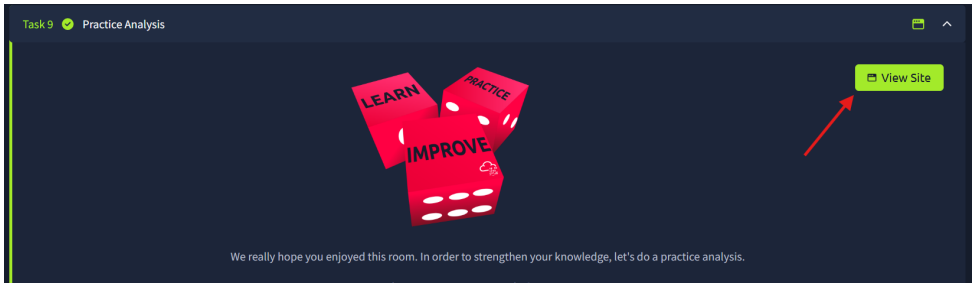
Respuesta: **Shadow Copy**

2.9. Tarea 9 - Análisis Práctico

Ahora en esta tarea haremos un ejercicio interactivo que te permite aplicar los conocimientos adquiridos sobre las fases de la cadena de ataque. Se presenta un sitio estático que simula un escenario basado en el ciberataque a Target en 2013, uno de los incidentes de seguridad más significativos de la historia.

El objetivo es asociar correctamente una serie de actividades maliciosas con las fases correspondientes de la **Cyber Kill Chain**. Cada actividad representa una técnica o acción utilizada por los atacantes durante las distintas etapas de un ataque. Una vez completado el ejercicio se proporcionara una flag de respuesta para completar la tarea.

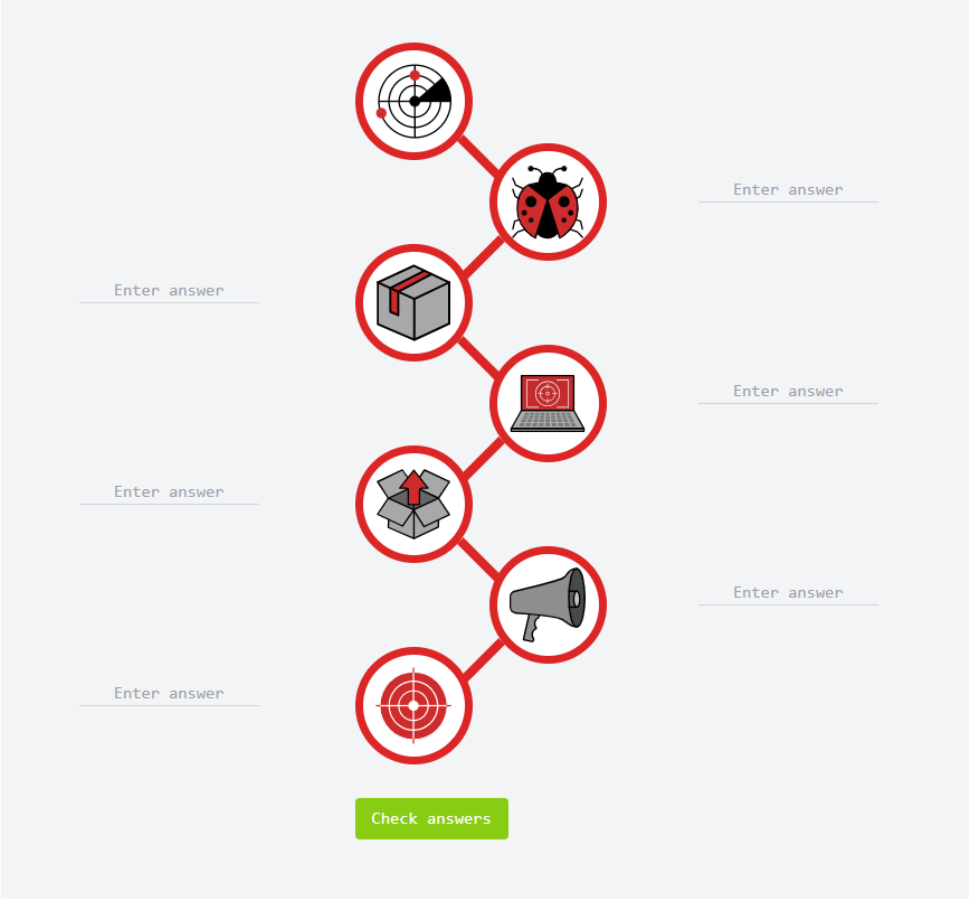
Para comenzar debemos hacer clic en el botón **View Site** proporcionado en la tarea para acceder al entorno interactivo.



Después que logramos iniciar el ejercicio debemos analizar las actividades listadas donde se presentan varias acciones que debes asociar con las fases de la Cyber Kill Chain. Las actividades son:

- **Exploit public-facing application**
- **Data from local system**
- **PowerShell**
- **Dynamic linker hijacking**
- **Spearphishing attachment**

- **Fallback channels**



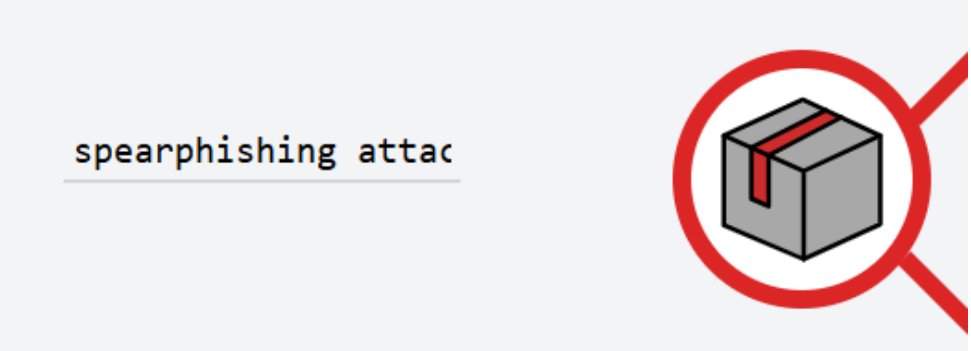
Ahora por último, tenemos que relacionar cada actividad con su fase correspondiente utilizando los conocimientos adquiridos en las tareas anteriores para determinar a qué fase pertenece cada acción.

Vamos a empezar desde arriba hasta la última fase de la cadena. La primera etapa del ejercicio es **Armatización** donde el atacante necesita crear un malware, para obtener la respuesta debemos tener en cuenta la terminología donde explicaban que es un programa o software diseñado para dañar, interrumpir u obtener acceso no autorizado a una computadora, por ende, teniendo en cuenta el listado anterior la respuesta es

- **Powershell**

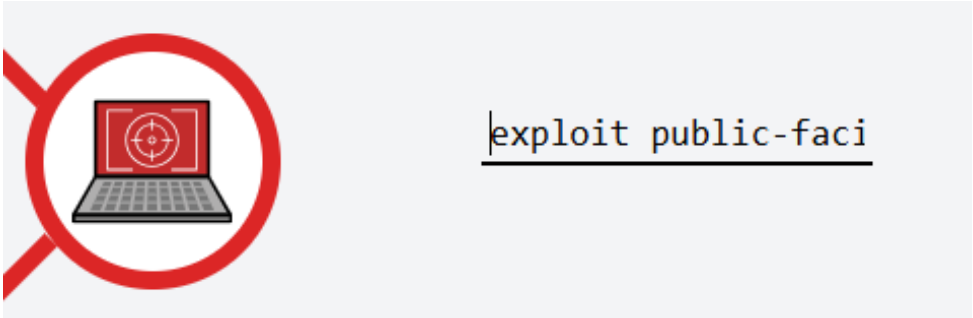
Siguiendo la cadena toca la fase de **Entrega**, para ello, debemos tener en cuenta las diferentes formas de entregar un malware a la PC de la víctima y en una de ellas se menciona a los correos electrónicos de phishing como una forma de entrega, una vez más analizando el listado podemos decir que la respuesta es la siguiente:

- **spearphishing attachment**



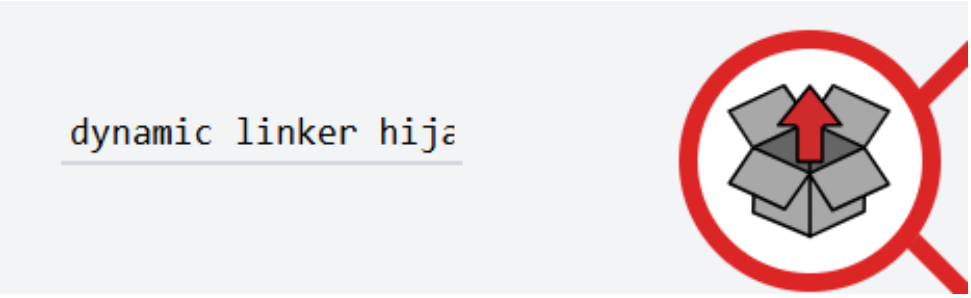
Continuando nos topamos con la fase de **Explotación** donde el atacante explotará un malware utilizado o una vulnerabilidad que se encuentra en el sistema. Teniendo en cuenta la tarea de explotación y el listado proporcionado podemos darnos cuenta que solo hay un elemento que incluye la palabra exploit y con esto concluimos que la respuesta correspondiente es

- **exploit public-facing application**



Ahora toca la **Instalación** donde podemos obtener la respuesta fácilmente ya que si nos fijamos en el listado, la mejor definición de enlace de instalación es el secuestro dinámico del enlazador que se utiliza para iniciar una PC y ejecutar la DLL para que navegue a un dicho enlace.

- **dynamic linker hijacking**

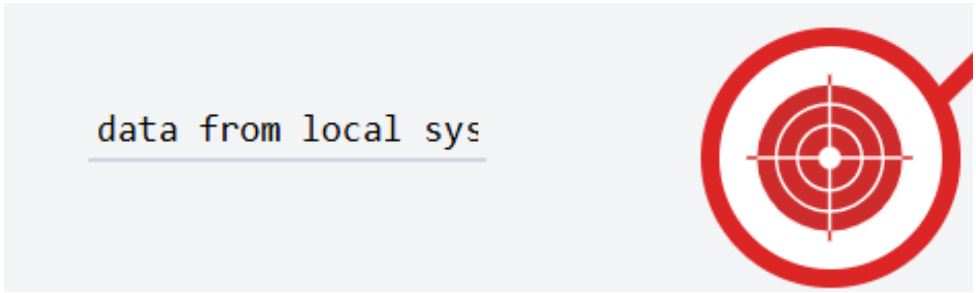


Encontrandonos ya en el final y quedando solo dos posibles respuestas en el listado para esta fase de **Comando y control** una resulta ser mejor que la otra teniendo en cuenta que un enlace de la cadena de eliminación se refiere a ser utilizado con fines de conectar al atacante con la PC de la víctima, entonces, la mejor respuesta a esta fase son los canales de resplado.

- **Fallback channels**

Ahora en la última etapa de la cadena de ciberataque que es la **Exfiltración** donde consiste que el atacante puede extraer información o datos del equipo de la víctima. En esta tarea se encontraba un listado de diferentes datos que un atacante podía extraer o corromper en el sistema de la víctima y teniendo en cuenta ese listado, la última respuesta va perfecta con el tema de los datos del sistema local.

- **Data from local system**



Una vez que escribimos todas las respuestas de las diferentes fases de un ciberataque procedemos a darle al botón de **Check Answers** y se nos mostrara en pantalla la flag de respuesta de la tarea.

Respuesta: **THM{7HR347_1N73L_12_4w35om3}**

3. Conclusión sobre la Sala

En esta sala hemos logrado aprender a como identificar y comprender las tácticas, técnicas y los procedimientos utilizados por los atacantes. Si bien, no solo comprendimos cada fase de la cadena de ataque, sino que también a estar mejor preparados para detectar y responder a incidentes de seguridad en las organizaciones.