Cadena de muerte cibernética

El marco de Cyber Kill Chain está diseñado para la identificación y prevención de las intrusiones de la red. Aprenderá lo que los adversarios deben hacer para lograr sus objetivos.

Tarea 1: Introducción.

¿Por qué es importante entender cómo funciona Cyber Kill Chain?

Cyber Kill Chain nos ayudará a comprender y protegernos contra ataques de ransomware, violaciones de seguridad y amenazas persistentes avanzadas (APT). Puede utilizar Cyber Kill Chain para evaluar la seguridad de su red y sistema identificando los controles de seguridad faltantes y cerrando ciertas brechas de seguridad según la infraestructura de su empresa.

- **Respuesta:** Simplemente hacer clic para Enviar (no se necesita respuesta).

Tarea 2: Reconocimiento.

El reconocimiento, desde la perspectiva del atacante, consiste en recopilar información sobre la víctima y su sistema como fase de planificación de un ataque. Incluye el uso de OSINT para obtener datos públicos de la empresa y sus empleados, como correos y teléfonos, con el fin de identificar objetivos para futuros pasos del ataque.

- **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**

Tarea 3: Weaponizaciòn.

Tras el reconocimiento, el atacante crea una "arma de destrucción" usando un armador que combina malware y exploits en una carga útil para el ataque. El malware daña o accede al sistema, el exploit aprovecha vulnerabilidades y la carga útil es el código malicioso ejecutado en la víctima. Los atacantes avanzados suelen crear malware personalizado para evadir detección.

- **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**

Tarea 4: Entrega.

En la fase de entrega, el atacante elige cómo enviar la carga útil al objetivo. Puede usar phishing (correos con malware), dejar USB infectados en lugares públicos o realizar ataques de pozo de agua, comprometiendo sitios visitados por la víctima para que descargue malware sin darse cuenta.

- **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**

Tarea 5: Explotaciòn.

En la fase de explotación, el atacante usa vulnerabilidades para acceder al sistema, como enlaces de phishing o archivos maliciosos. Luego puede escalar privilegios o moverse lateralmente para obtener datos. También puede usar exploits de día cero, vulnerabilidades desconocidas que permiten el acceso antes de ser detectadas.

- **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**

Tarea 6: Instalaciòn.

Una puerta trasera permite al atacante eludir la seguridad y mantener acceso al sistema incluso si se pierde la conexión o se elimina el acceso inicial. Al instalar una puerta trasera persistente, el atacante puede volver a ingresar al sistema comprometido en el futuro.

- **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 web server to maintain access to the compromised system and enable the web server to be accessed remotely?
  - **Respuesta: Web Shell**

Tarea 7: Comando y Control.

En la fase de Comando y Control (C2), el atacante usa el malware para abrir un canal y controlar remotamente la máquina de la víctima. El host infectado se comunica con un servidor externo configurado por el atacante, permitiéndole tener control total del sistema comprometido.

- **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**

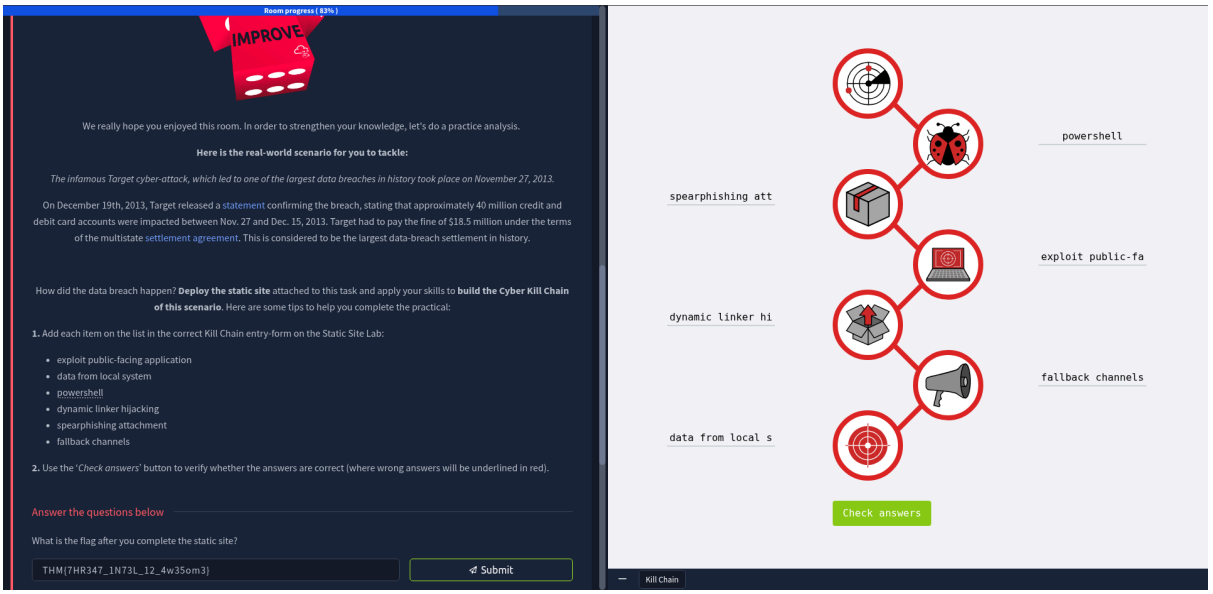
Tarea 8: Acciones sobre objetivos (Exfiltración).

En la fase final del ataque, el atacante logra sus objetivos: recopila credenciales, realiza escalada de privilegios, reconocimiento interno, movimiento lateral, exfiltra datos, elimina copias de seguridad (incluyendo Shadow Copy) y puede sobrescribir o corromper información en el sistema.

- **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**

Tarea 9: Análisis de Práctica.

Hacemos click en “View Site” y completamos el ejercicio para obtener la Respuesta.



- **Pregunta:** What is the flag after you complete the static site?
  - **Respuesta: THM{7HR347_1N73L_12_4w35om3}**

Tarea 10: Conclusión.

La Cyber Kill Chain es útil para mejorar la defensa de redes, pero no es perfecta ni suficiente por sí sola. Está desactualizada y se enfoca en amenazas de malware y perímetro, sin cubrir amenazas internas. Se recomienda complementar con MITRE ATT&CK y Unified Kill Chain para una defensa más completa.

- **Respuesta:** Simplemente hacer clic para Enviar (no se necesita respuesta).