THM **Rodriguez Suar Mateo**

Cadena de Muerte Cibernética

Tarea 1: Introducción
P: Lea lo anterior.
R: No se necesita respuesta

Tarea 2: Reconocimiento
P1: ¿Cuál es el nombre de la herramienta de recopilación de información de Intel, que es una interfaz basada en la web para las herramientas y recursos comunes de inteligencia de código abierto?
R1: OSINT Framework / Marco Osint

P2: ¿Cuál es la definición del proceso de recopilación de correo electrónico durante la etapa de reconocimiento?
R2: email harvesting / Recolección de correo electrónico

Tarea 3: Armamentización
P: Este término se refiere a un grupo de comandos que realizan una tarea específica. Se pueden considerar subrutinas o funciones que contienen el código que la mayoría de los usuarios usan para automatizar tareas rutinarias. Sin embargo, los actores maliciosos tienden a usarlos con fines maliciosos e incluirlos en documentos de Microsoft Office. ¿Podrías indicar el término?
R: Macro

Tarea 4: Entrega
P: ¿Cómo se llama el ataque cuando se realiza contra un grupo específico de personas y el atacante busca infectar el sitio web que dicho grupo de personas visita constantemente?
R: Watering hole attack / Ataque de abrevadero

Tarea 5: Exploitation
P: ¿Puede proporcionar el nombre de un ciberataque dirigido a una vulnerabilidad de software que es desconocida para los proveedores de antivirus o software?
R: Zero-day / Día Cero

Tarea 6: Instalacion
P1: ¿Puede proporcionar la técnica utilizada para modificar los atributos de tiempo del archivo para ocultar archivos nuevos o cambios en los existentes?
R1: Timestomping

P2: ¿Puede nombrar el script malicioso plantado por un atacante en el servidor web para mantener el acceso al sistema comprometido y permitir que se acceda al servidor web de forma remota?
R2: Web shell

Tarea 7: Comando y control
P: ¿Qué es la comunicación C2 donde la víctima realiza solicitudes DNS regulares a un servidor DNS y un dominio que pertenecen a un atacante?
R: DNS Tunneling

Tarea 8: Acciones sobre Objetivos (Exfiltración)
P: ¿Puede proporcionar una tecnología incluida en Microsoft Windows que pueda crear copias de seguridad o instantáneas de archivos o volúmenes en la computadora, incluso cuando estén en uso?
R: Shadow Copy / Instantaneas

Tarea 9: Análisis de la práctica

Esperamos que hayan disfrutado de esta sala. Para reforzar sus conocimientos, hagamos un análisis práctico.

Aquí está el escenario del mundo real para que lo aborden:

El infame ciberataque a Target, que provocó una de las mayores violaciones de datos de la historia, tuvo lugar el 27 de noviembre de 2013.

El 19 de diciembre de 2013, Target emitió un comunicado confirmando la filtración de datos, indicando que aproximadamente 40 millones de cuentas de tarjetas de crédito y débito se vieron afectadas entre el 27 de noviembre y el 15 de diciembre de 2013. Target tuvo que pagar una multa de 18,5 millones de dólares según los términos del acuerdo transaccional multiestatal . Este se considera el mayor acuerdo transaccional por filtración de datos de la historia.

¿Cómo ocurrió la filtración de datos? **Implementa el sitio estático** asociado a esta tarea y aplica tus habilidades para **construir la Cadena de Cibercrimen de este escenario** . Aquí tienes algunos consejos para ayudarte a completar la práctica:

1. Agregue cada elemento de la lista en el formulario de entrada de Kill Chain correcto en el Laboratorio del sitio estático:

- **exploit public-facing application** / explotar una aplicación pública
- **data from local system** / datos del sistema local
- **powershell** / powerShell
- **dynamic linker hijacking** / secuestro de enlazadores dinámicos
- **spearphishing attachment** / archivo adjunto de phishing selectivo
- **fallback channels** / canales de respaldo

2. Utilice el botón ' *Verificar respuestas* ' para verificar si las respuestas son correctas (las respuestas incorrectas aparecerán subrayadas en rojo).

Respuestas del Laboratorio:

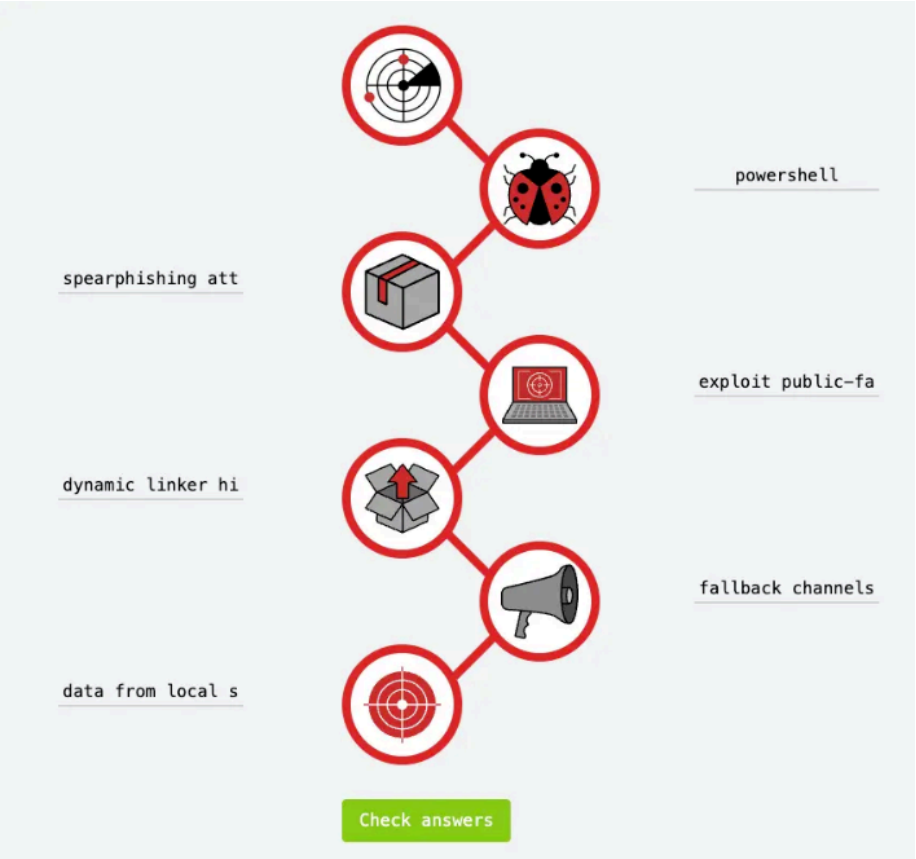

Figura 1 (Static Site Lab)

Bandera obtenida:

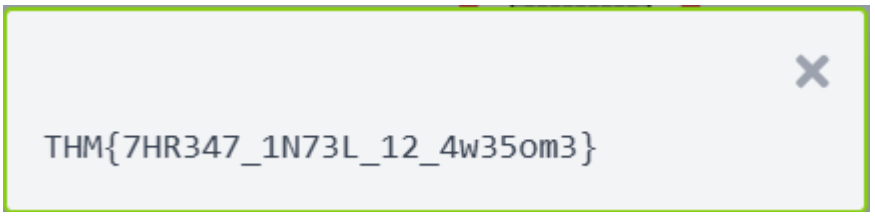

Figura 2 (Flag)

P¿Cuál es la bandera después de completar el sitio estático?
R: THM{7HR347_1N73L_12_4w35om3}

Tarea 10: Conclusión
P: Lea lo anterior.
R: No se necesita respuesta

💼**LinkedIn:**https://www.linkedin.com/in/mateo-rodr%C3%ADguez-suar-202695249/
💻 **GitHub:** https://github.com/MaateoSuar