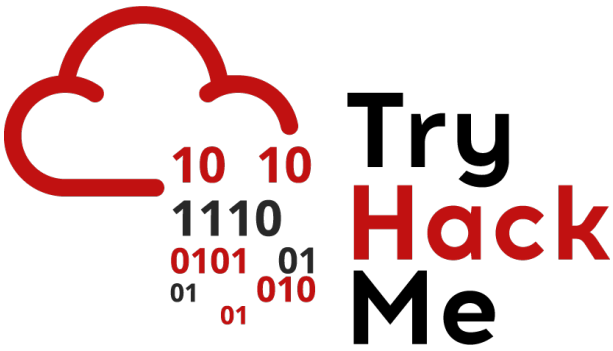
Writeup: Sala *Red Team Engagements*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

1. Introducción

En esta sala aprenderemos cómo planificar, estructurar y ejecutar compromisos de Red Team en entornos profesionales. También, vamos a conocer conceptos esenciales como la definición del alcance, las reglas de compromiso, la documentación operativa, la planificación de campañas y la gestión de recursos.

2. Sala

2.1. Tarea 1 - Introducción

En esta primera tarea conoceremos el contexto y propósito del módulo, explicando que se explorará el proceso completo de un compromiso de red team, desde la planificación hasta la documentación y ejecución.

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

2.2. Tarea 2 - Definición del alcance y los objetivos

En esta tarea, aprenderemos sobre la necesidad de establecer claramente los objetivos del cliente y el alcance técnico, como rangos IP autorizados, tipos de sistemas a evaluar, limitaciones y el uso potencial de white cards, generando una base sólida para toda la operación.

Una vez entendido los alcances y objetivos, pasamos a responder las siguientes preguntas:

Pregunta: What CIDR range is permitted to be attacked?
Respuesta: **10.0.4.0/22**

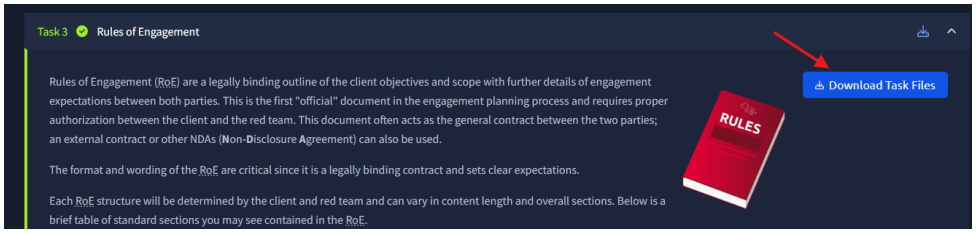
Pregunta: Is the use of white cards permitted? (Y/N)
Respuesta: **Y**

Pregunta: Are you permitted to access *.bethechange.xyz? (Y/N)
Respuesta: **N**

2.3. Tarea 3 - Reglas de compromiso

Ahora nos introduciremos en las directrices operativas que definen lo que está permitido y prohibido durante la misión, detallando restricciones explícitas y métodos de acceso aceptables, garantizando conformidad legal y seguridad del cliente.

Para resolver esta tarea, debemos descargar el modelo de normas de intervención que se encuentra en el lado superior de la tarea. Una vez descargado, lea el documento y responda a las preguntas siguientes.



Pregunta: How many explicit restriction are specified?
Respuesta: 3

Pregunta: What is the first access type mentioned in the document?
Respuesta: Phishing

Pregunta: Is the red team permitted to attack 192.168.1.0/24? (Y/N)
Respuesta: Y

2.4. Tarea 4 - Planificación de campañas

Aprenderemos sobre la creación de una estrategia estructurada que sirve de puente entre las reglas de compromiso y la documentación detallada del engagement, incluyendo fases, cronogramas y escenarios de ataque.

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

2.5. Tarea 5 - Documentación del compromiso

Conoceremos sobre la elaboración de artefactos formales como el plan de compromisos, reglas de enfrentamiento, registro de actividades, listas de control y formatos de reporte, que servirán de soporte a las fases operativas posteriores.

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

2.6. Tarea 6 - Conceptos de Operaciones (CONOPS)

En esta tarea se presenta un documento técnico que explica de forma no técnica cómo se estructura el engagement: objetivos, duración (1 mes), persistencia (3 semanas), tácticas empleadas (como fin6 o Cobalt Strike), y enfoque organizativo.

Para completar esta tarea debemos leer el ejemplo CONOPS y responder las siguientes preguntas.

Pregunta: How long will the engagement last?
Respuesta: **1 Month**

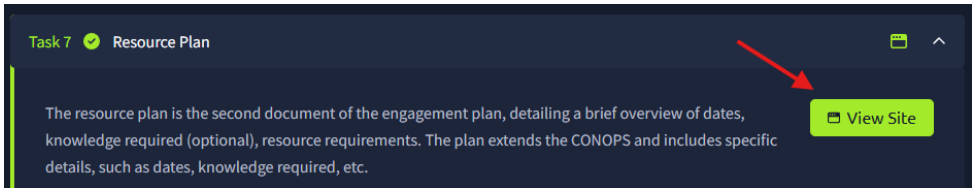
Pregunta: How long is the red cell expected to maintain persistence?
Respuesta: **3 Weeks**

Pregunta: What is the primary tool used within the engagement?
Respuesta: **Cobalt Strike**

2.7. Tarea 7 - Plan de recursos

Aprenderemos sobre una detallada planificación de los recursos necesarios, abarcando personal, hardware, cloud, fechas clave y cualquier requerimiento adicional para sustentar las fases de reconocimiento, acceso inicial y post-explotación.

Para completar esta tarea, debemos leer el plan de recursos. Una vez completado, responda las preguntas a continuación. Para leer el plan haremos clic en **View Site** en el lado superior.



Pregunta: When will the engagement end? (MM/DD/YYYY)
Respuesta: **11/14/2021**

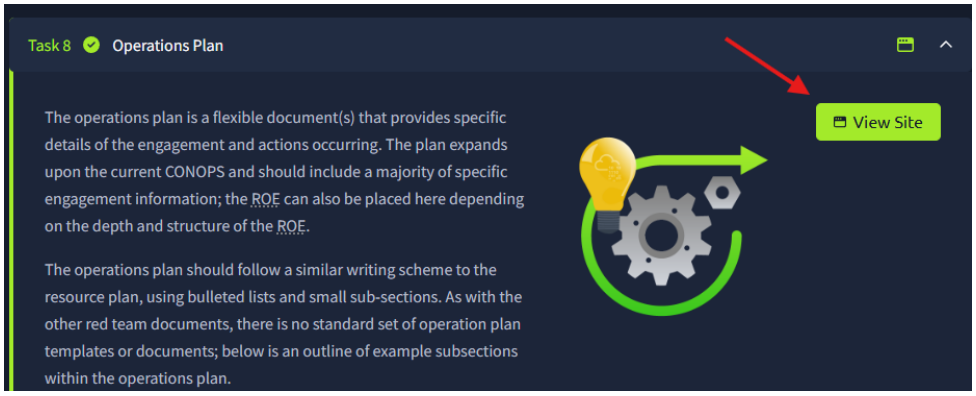
Pregunta: What is the budget the red team has for AWS cloud cost?
Respuesta: **$1000**

Pregunta: Are there any miscellaneous requirements for the engagement? (Y/N)
Respuesta: **N**

2.8. Tarea 8 - Plan de operaciones

En esta tarea vamos a aprender sobre las acciones tácticas a ejecutar, incluyendo roles del equipo, métodos de phishing (ej: spear-phishing), canales de comunicación (vectr.io), condiciones de fallo y protocolos en caso de interrupciones.

Para lograr completar esta tarea, debemos leer el plan de operaciones. Una vez completado, responda las preguntas a continuación.



Pregunta: What phishing method will be employed during the initial access phase?
Respuesta: **Spearphishing**

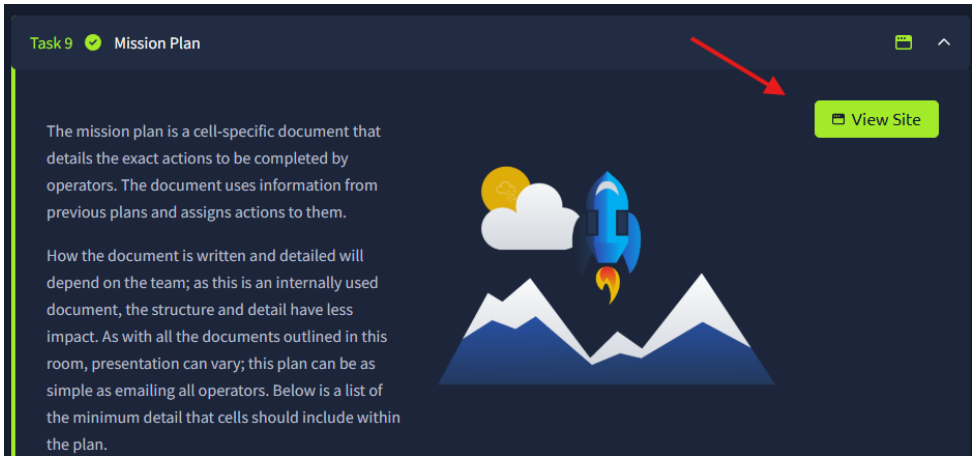
Pregunta: What site will be utilized for communication between the client and red cell?
Respuesta: **vectr.io**

Pregunta: If there is a system outage, the red cell will continue with the engagement. (T/F)
Respuesta: **F**

2.9. Tarea 9 - Plan de misión

Aprenderemos sobre una secuencia precisa de objetivos tácticos con cronograma, restricciones específicas sobre sistemas (por ejemplo no atacar cierta IP) y procedimientos a seguir ante condiciones de detención.

Para completar la tarea, vamos a leer el plan de misión. Una vez completado, responda las preguntas a continuación.



Pregunta: When will the phishing campaign end? (mm/dd/yyyy)
Respuesta: **10/23/2021**

Pregunta: Are you permitted to attack 10.10.6.78? (Y/N)
Respuesta: **N**

Pregunta: When a stopping condition is encountered, you should continue working and determine the solution yourself without a team lead. (T/F)
Respuesta: **F**

3. Conclusión sobre la Sala

Al finalizar esta sala, hemos logrado aprender cómo estructurar un compromiso de Red Team de principio a fin, entendiendo cada una de las fases clave desde la planificación inicial hasta la ejecución operativa y el reporte final.