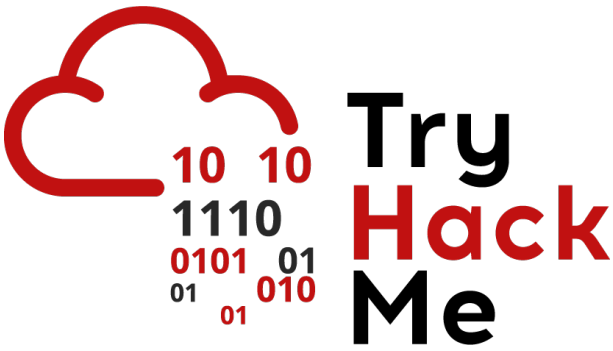
Writeup: Sala *Red Team Fundamentals*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

1. Introducción

En esta sala vamos a introducirnos en conceptos esenciales del **Red Team**, una rama de la ciberseguridad ofensiva enfocada en emular ataques reales para evaluar la postura defensiva de una organización.

2. Sala

2.1. Tarea 1 - Introducción

En esta primera tarea nos introducimos en la necesidad de enfoques más avanzados en ciberseguridad ante la evolución constante de las amenazas. Así que, se presenta al Red Team como una disciplina diseñada para simular ataques del mundo real y evaluar la capacidad de respuesta ante adversarios motivados.

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

2.2. Tarea 2 - Limitaciones de la evaluación de vulnerabilidades y pruebas de penetración

En esta tarea vamos a conocer como las evaluaciones de vulnerabilidades y los test de penetración tradicionales pueden no reflejar con precisión la resistencia de una organización ante ataques complejos y sostenidos. Aprenderemos algunas limitaciones clave, como el enfoque limitado en técnicas específicas o la falta de contexto realista, lo que justifica la necesidad de un enfoque más completo como el que ofrece el Red Team.

Una vez que comprendemos lo estudiado, procederemos a responder las siguientes preguntas:

Pregunta: Would vulnerability assessments prepare us to detect a real attacker on our networks? (Yay/Nay)
Respuesta: **Nay**

Pregunta: During a penetration test, are you concerned about being detected by the client? (Yay/Nay)
Respuesta: **Nay**

Pregunta: Highly organised groups of skilled attackers are nowadays referred to as
Respuesta: **Advanced Persistent Threats**

2.3. Tarea 3 - Compromisos del Equipo Rojo

Aprenderemos que estos simulacros están orientados a medir la eficacia de los procesos de detección y respuesta de la organización, más allá de simplemente identificar vulnerabilidades. El objetivo es simular ataques avanzados y persistentes (**APT**) para evaluar cómo respondería la defensa ante amenazas reales.

Después de profundizar en lo que constituye un "engagement" o ejercicio de Red Team, pasamos a responder las siguientes preguntas.

Pregunta: The goals of a red team engagement will often be referred to as flags or...
Respuesta: **crown jewels**

Pregunta: During a red team engagement, common methods used by attackers are emulated against the target. Such methods are usually called TTPs. What does TTP stand for?
Respuesta: **Tactics, techniques and procedures**

Pregunta: The main objective of a red team engagement is to detect as many vulnerabilities in as many hosts as possible (Yay/Nay)
Respuesta: **Nay**

2.4. Tarea 4 - Equipos y funciones de un compromiso

Ahora, aprenderemos como se presentan los distintos equipos involucrados en un ejercicio de Red Team:

- **Red Team**
- **Blue Team (defensivo)**
- **White Team (control y monitoreo del ejercicio)**

Cada uno cumple un rol específico para asegurar la integridad, el control y la efectividad de la simulación, garantizando que el proceso se mantenga dentro del alcance acordado y se obtengan resultados útiles para la organización.

Una vez comprendido las funciones y compromiso de estos diferentes roles, pasamos a responder las siguientes preguntas.

Pregunta: What cell is responsible for the offensive operations of an engagement?
Respuesta: **Red Cell**

Pregunta: What cell is the trusted agent considered part of?
Respuesta: **White Cell**

2.5. Tarea 5 - Estructura de compromiso

Esta tarea describe cómo se estructura un engagement típico. Incluye las fases claves de una **Cyber Kill Chain**. Esta estructura permite organizar el trabajo del Red Team de forma sistemática y estratégica, maximizando el realismo del ataque simulado y asegurando que se cumplan los objetivos establecidos.

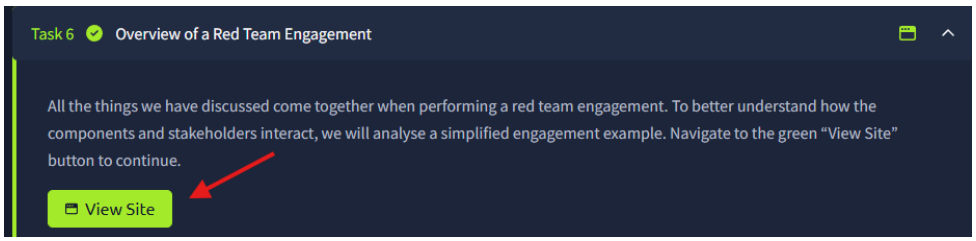
Ahora que comprendemos la estructura, vamos a responder las siguientes preguntas.

Pregunta: If an adversary deployed Mimikatz on a target machine, where would they be placed in the Lockheed Martin cyber kill chain?
Respuesta: **Installation**

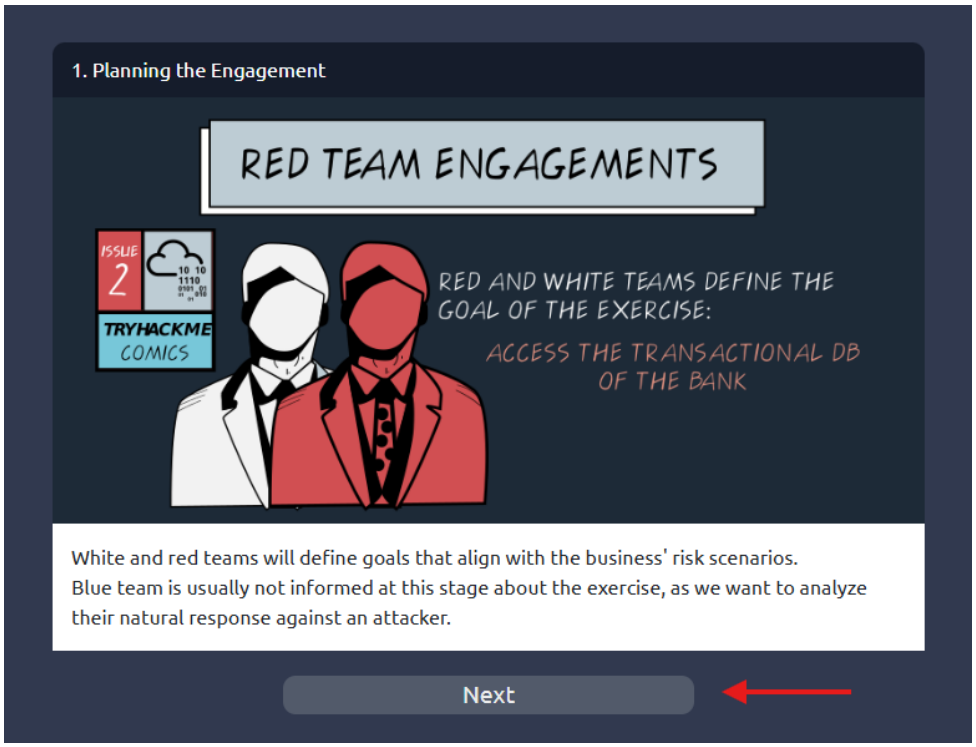
Pregunta: What technique's purpose is to exploit the target's system to execute code?
Respuesta: **Exploitation**

2.6. Tarea 6 - Descripción de un compromiso del equipo rojo

En esta tarea vamos a tener una visión general de principio a fin sobre cómo se lleva a cabo una operación de Red Team pasando por cada fase. Para ello, lo primero que haremos es desplegar el sitio de práctica haciendo clic en **View Site** en el lado superior.

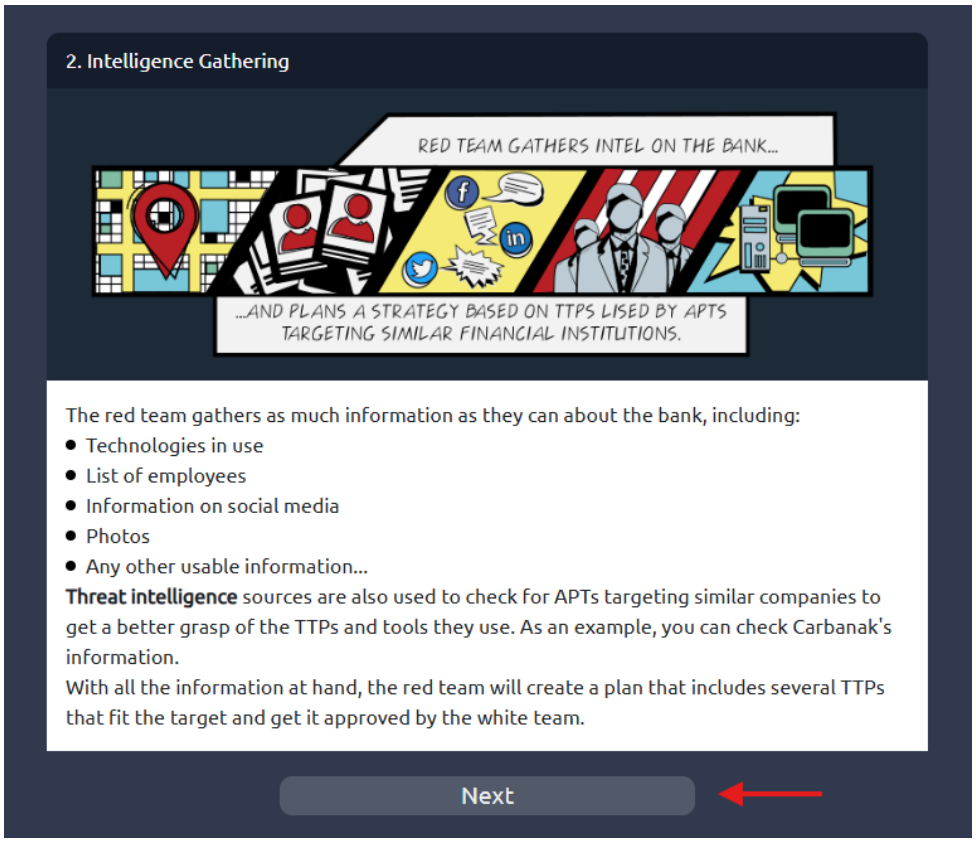


Una vez que desplegamos el sitio, empezamos con la primera fase que es el planeamiento del compromiso, después de comprender esta parte, haremos clic en **Next** para continuar con la que sigue.

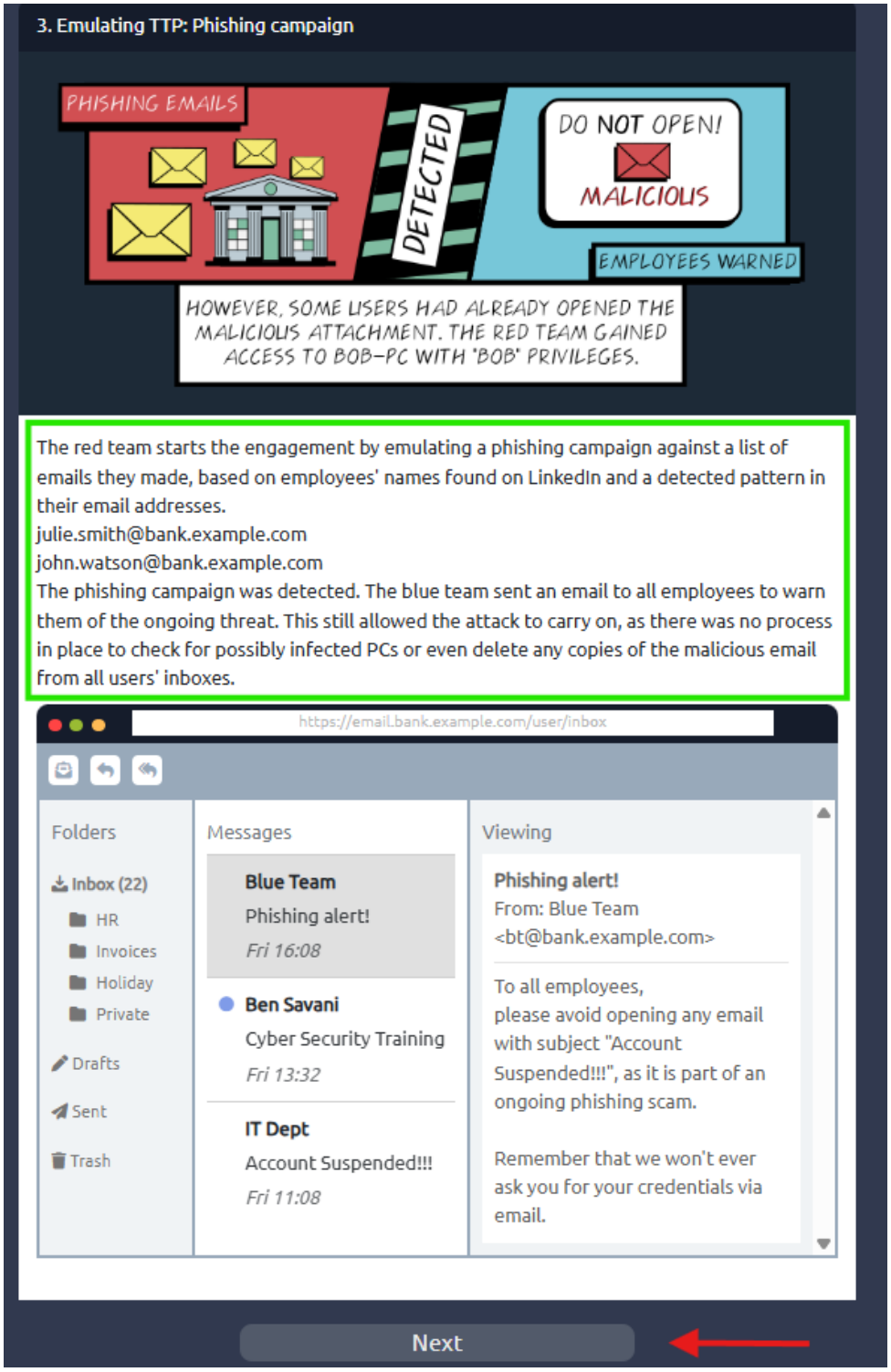


Ahora, nos encontramos en la fase 2 de recopilación de inteligencia, donde el equipo rojo recopila toda la información que puede sobre un banco, posterior a eso, creará un plan que incluya varias TTPs que se ajusten al objetivo y lo hará aprobar por el equipo blanco.

Haremos clic en **Next** para continuar con la siguiente fase.



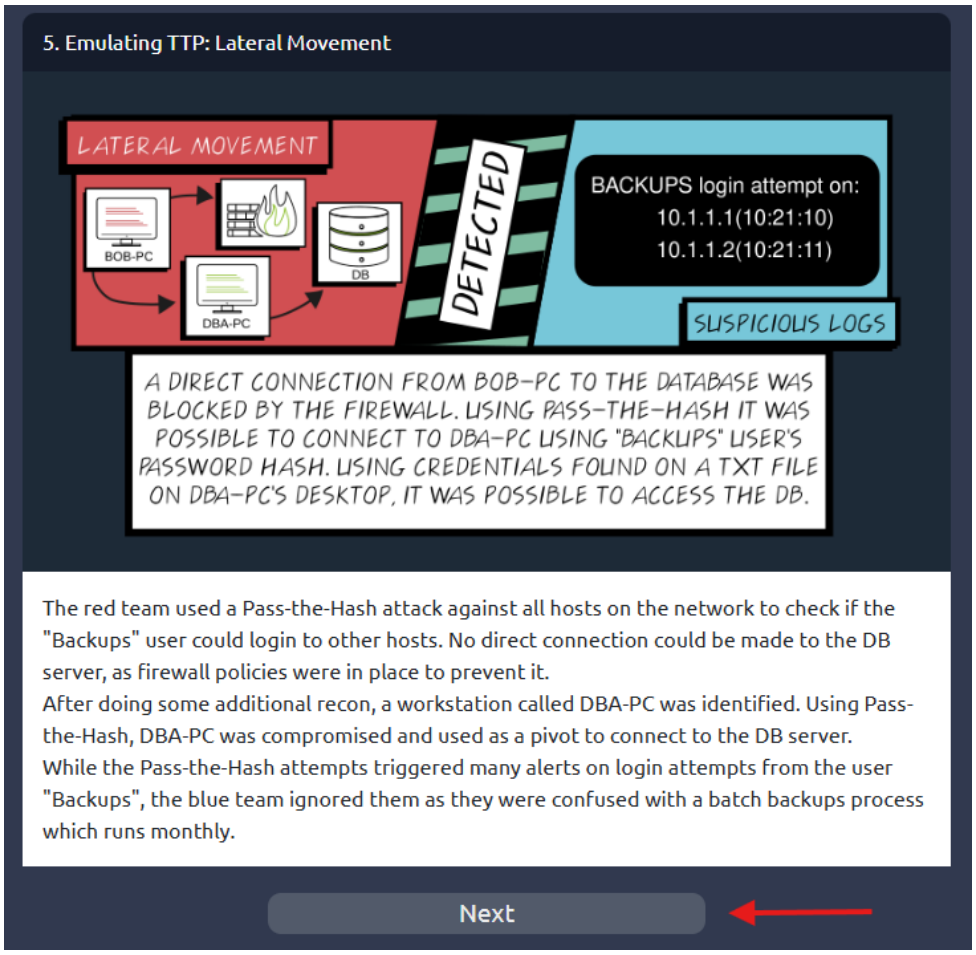
En esta fase 3, el equipo rojo realizara una emulación de TTP (campaña de phishing), una vez que hemos entendido se llevo a cabo la campaña de phishing, haremos clic en **Next** para continuar con la siguiente fase.



Ahora, nos encontramos en una fase donde el equipo rojo realizara una emulación de TTP de escalada de privilegios y persistencia. Después de entender esta fase, haremos clic en **Next** para continuar.

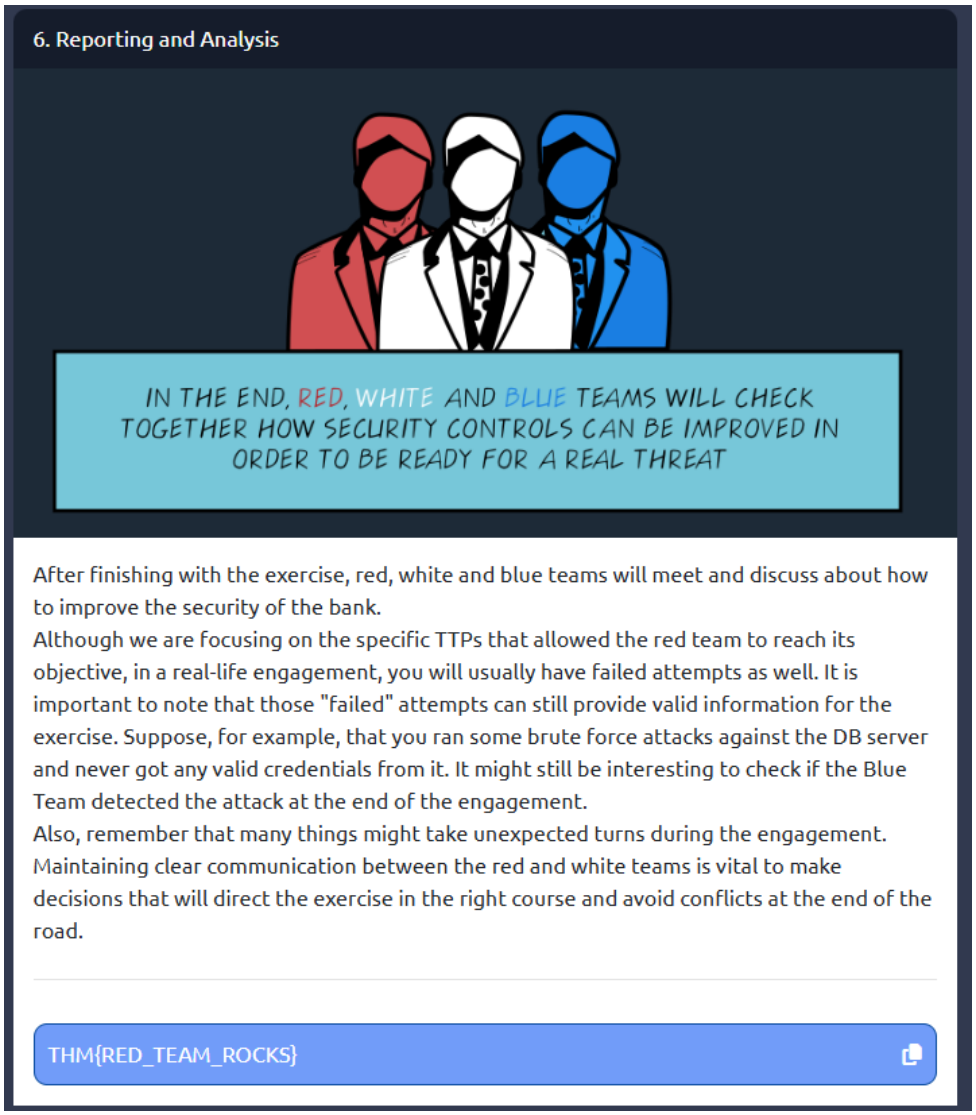
En esta fase el equipo rojo comenzara a realizar una emulación de TTP de movimiento lateral donde intentara establecer una conexión directa con el servidor de base de datos y realizar algunos reconocimientos adicionales.

Posterior a esto, haremos clic en **Next** para continuar a la siguiente fase.



Nos encontraremos en la última fase que es el de Informes y análisis. En este caso tras finalizar el ejercicio, los equipos rojo, blanco y azul se reunirán y debatirán sobre cómo mejorar la seguridad.

Al final de esta fase, tendremos la flag para completar la tarea.



Respuesta: **THM{RED_TEAM_ROCKS}**

3. Conclusión sobre la Sala

Esta sala ha logrado proporcionarnos una introducción sólida al mundo del Red Team, destacando su importancia como una práctica ofensiva avanzada que va más allá de las pruebas de penetración tradicionales. Hemos aprendido cómo se estructuran y ejecutan los ejercicios de Red Team, quiénes participan en ellos y cuál es su propósito dentro de un entorno corporativo.