Fundamentos del Equipo Rojo

Tarea 1: Introducción
P: Haga clic para continuar con la siguiente tarea.
R: No se necesita respuesta

Tarea 2: Limitaciones de la evaluación de vulnerabilidades y pruebas de penetración
P1: ¿Las evaluaciones de vulnerabilidad nos prepararían para **detectar** un atacante real en nuestras redes? (Sí/No)
R1: Nay / No

P2: Durante una prueba de penetración, ¿te preocupa que el cliente te detecte? (Sí/No)
R2: Nay / No

P3: A los grupos altamente organizados de atacantes hábiles se les conoce hoy en día como...
R3: Advanced Persistent Threats (APT) / Amenazas Persistentes Avanzadas (APT)

Tarea 3: Compromisos del Equipo Rojo
P1: Los objetivos de un compromiso del equipo rojo a menudo se denominan banderas o…
R1: Crown Jewels / joyas de la corona

P2: Durante una intervención del equipo rojo, se emulan contra el objetivo métodos comunes de los atacantes. Estos métodos suelen denominarse TTP. ¿Qué significa TTP?
R2: Tactics, techniques and procedures / Tácticas, técnicas y procedimientos

P3: El objetivo principal de una intervención del equipo rojo es detectar tantas vulnerabilidades en tantos hosts como sea posible (Sí/No)
R3: Nay / No

Tarea 4: Equipos y funciones de un compromiso
P1: ¿Qué célula es responsable de las operaciones ofensivas de un enfrentamiento?
R1: Red Cell / Celula Roja

P2: ¿De qué célula se considera que forma parte el agente de confianza?
R2: White Cell / Celula Blanca

Tarea 5: Estructura de compromiso
P1: Si un adversario implementara Mimikatz en una máquina objetivo, ¿dónde se ubicaría en la cadena de ciberataque de Lockheed Martin?
R1: Installation / Instalación

P2: ¿Qué técnica tiene como propósito explotar el sistema del objetivo para ejecutar código?
R2: Exploitation / Explotación

Tarea 6: Descripción general de un compromiso del equipo rojo
P: Haga clic en el botón "Ver sitio" y siga el ejemplo de interacción para obtener la bandera

1. Planificación del compromiso

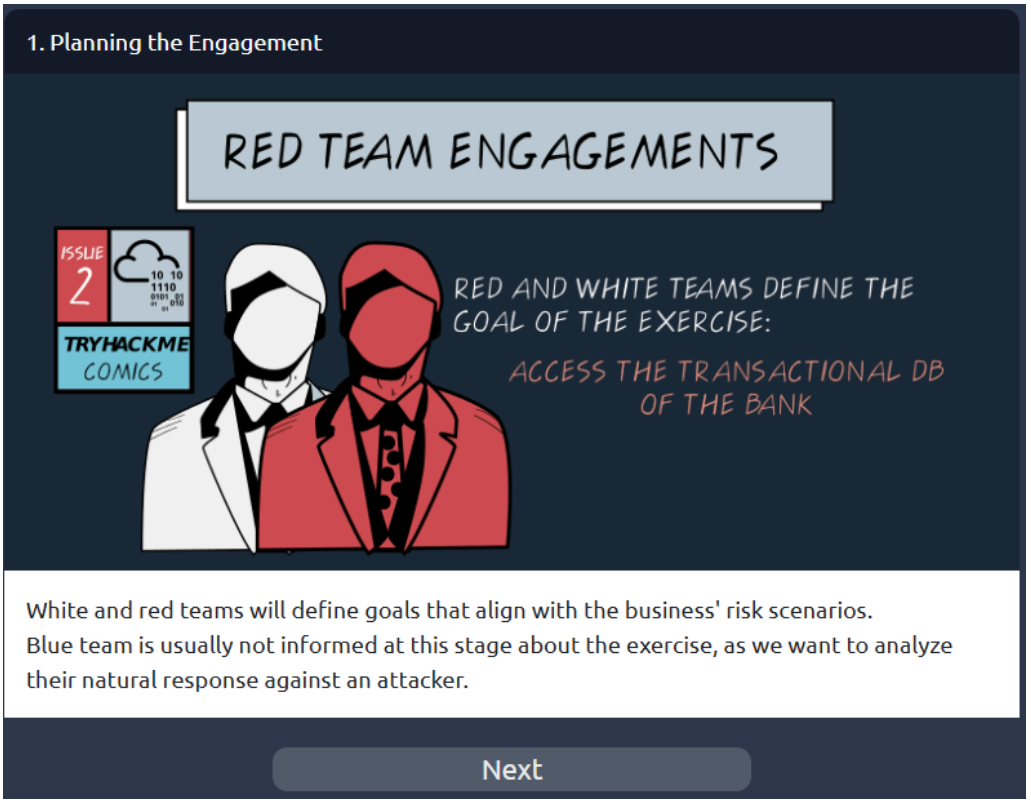

Figura 1 (Compromiso 1)

2. Recopilación de inteligencia

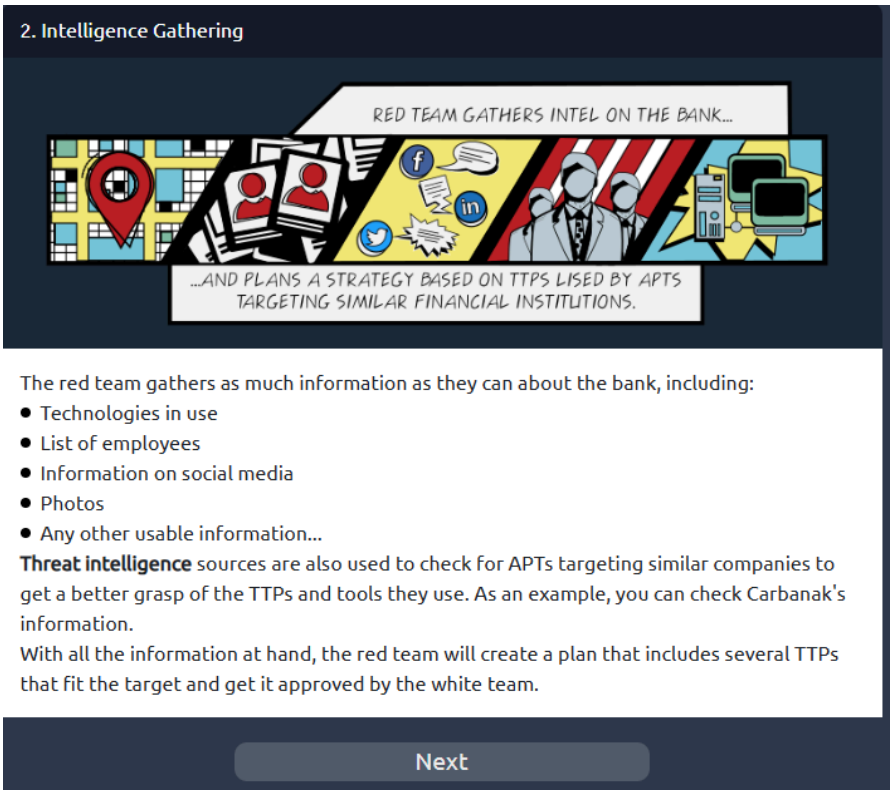

Figura 2 (Compromiso 2)

3. Emulando TTP: Campaña de phishing

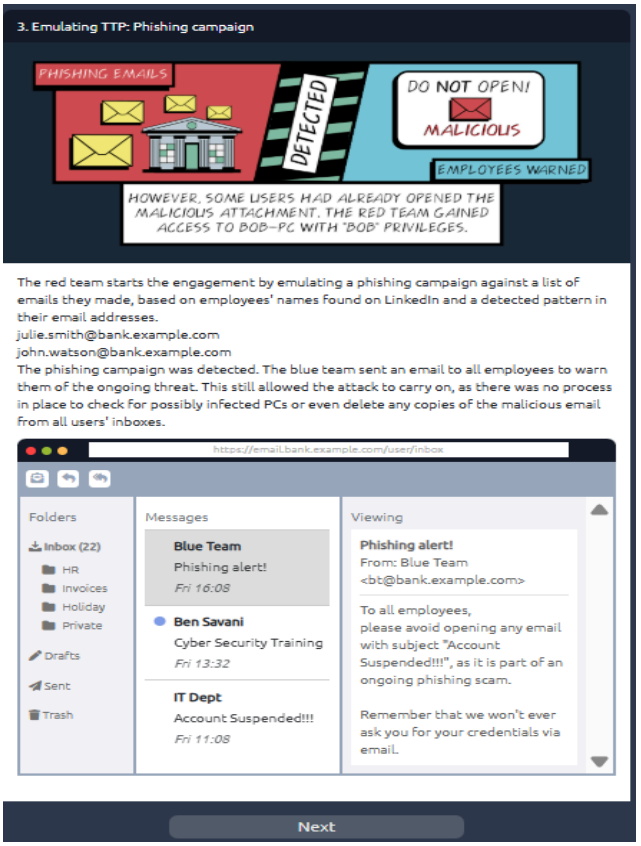

Figura 3 (Compromiso 3)

4. Emulación de TTP: Escalada de privilegios y persistencia

Figura 4 (Compromiso 4)

5. Emulación de TTP: Movimiento lateral

Figura 5 (Compromiso 5)

6. Informes y análisis - (Flag encontrada)

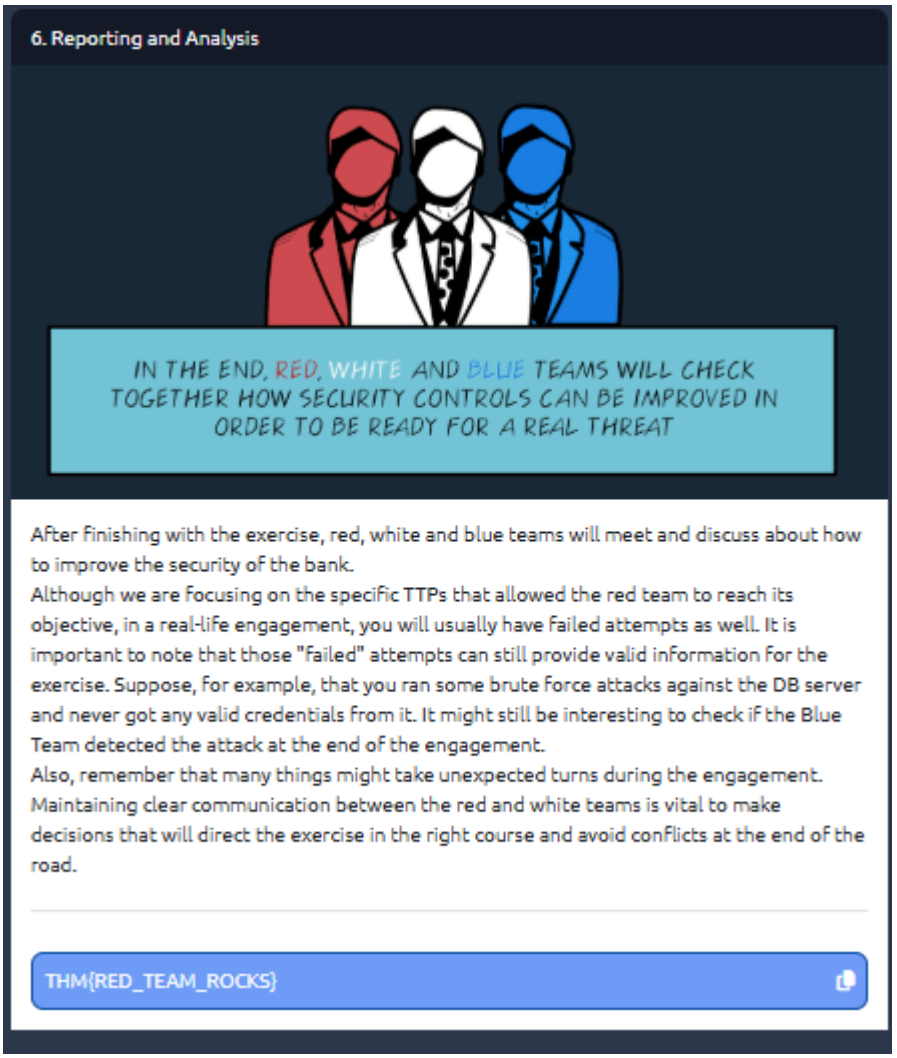

Figura 6 (Compromiso 6)

R: THM{RED_TEAM_ROCKS}

Tarea 7: *Conclusion*

En esta sala se ofrece una visión general simplificada de los Enfrentamientos del Equipo Rojo. Se han presentado los conceptos, componentes y partes interesadas principales para que comprendan estos ejercicios. En las siguientes salas, aprenderá toda la planificación de un enfrentamiento real, así como muchas técnicas interesantes que un atacante real usaría, incluyendo cómo usar la inteligencia de amenazas a su favor, evadir los mecanismos de seguridad presentes en cualquier host moderno, realizar movimientos laterales e intentar evitar la detección a toda costa.

P: ¡Lee lo anterior y continúa aprendiendo!
R: No se necesita respuesta

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