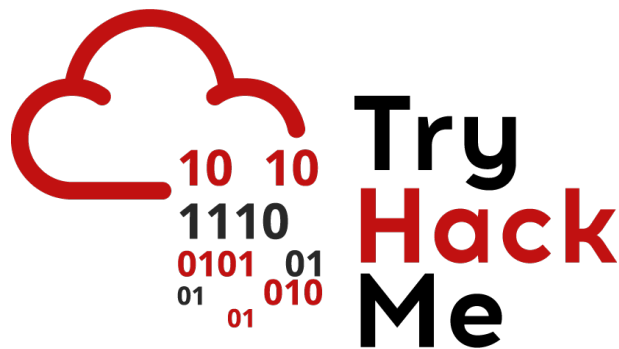


# Writeup: Sala *Red Team Fundamentals*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



## Índice

<b>1. Introducción</b>	<b>2</b>
<b>2. Sala</b>	<b>2</b>
2.1. Tarea 1 - Introducción . . . . .	2
2.2. Tarea 2 - Limitaciones de la evaluación de vulnerabilidades y pruebas de penetración . . . . .	2
2.3. Tarea 3 - Compromisos del Equipo Rojo . . . . .	3
2.4. Tarea 4 - Equipos y funciones de un compromiso . . . . .	3
2.5. Tarea 5 - Estructura de compromiso . . . . .	4
2.6. Tarea 6 - Descripción de un compromiso del equipo rojo . . . . .	4
<b>3. Conclusión sobre la Sala</b>	<b>9</b>

# 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?

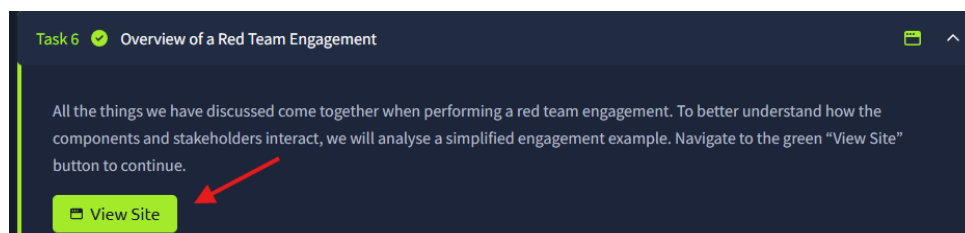
**Respuesta:** **Installation**

**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.

1. Planning the Engagement

## RED TEAM ENGAGEMENTS



RED AND WHITE TEAMS DEFINE THE GOAL OF THE EXERCISE:  
ACCESS THE TRANSACTIONAL DB OF THE BANK


White and red teams will define goals that align with the business' risk scenarios. Blue team is usually not informed at this stage about the exercise, as we want to analyze their natural response against an attacker.

Next

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.

2. Intelligence Gathering



RED TEAM GATHERS INTEL ON THE BANK...

...AND PLANS A STRATEGY BASED ON TTPs LIKED BY APTs TARGETING SIMILAR FINANCIAL INSTITUTIONS.

The red team gathers as much information as they can about the bank, including:

- Technologies in use
- List of employees
- Information on social media
- Photos
- Any other usable information...

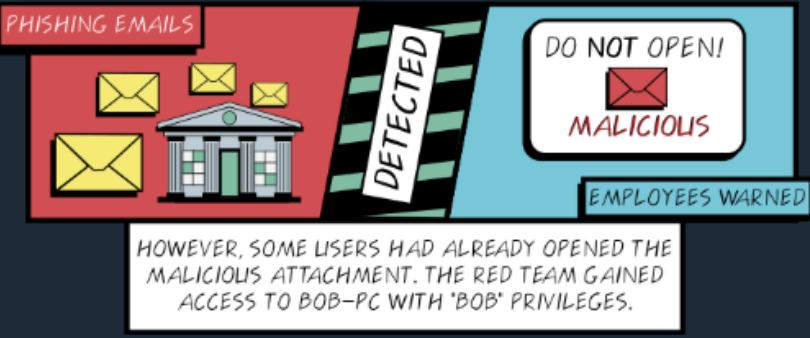
**Threat intelligence** sources are also used to check for APTs targeting similar companies to get a better grasp of the TTPs and tools they use. As an example, you can check Carbanak's information.

With all the information at hand, the red team will create a plan that includes several TTPs that fit the target and get it approved by the white team.

Next

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.

3. Emulating TTP: Phishing campaign

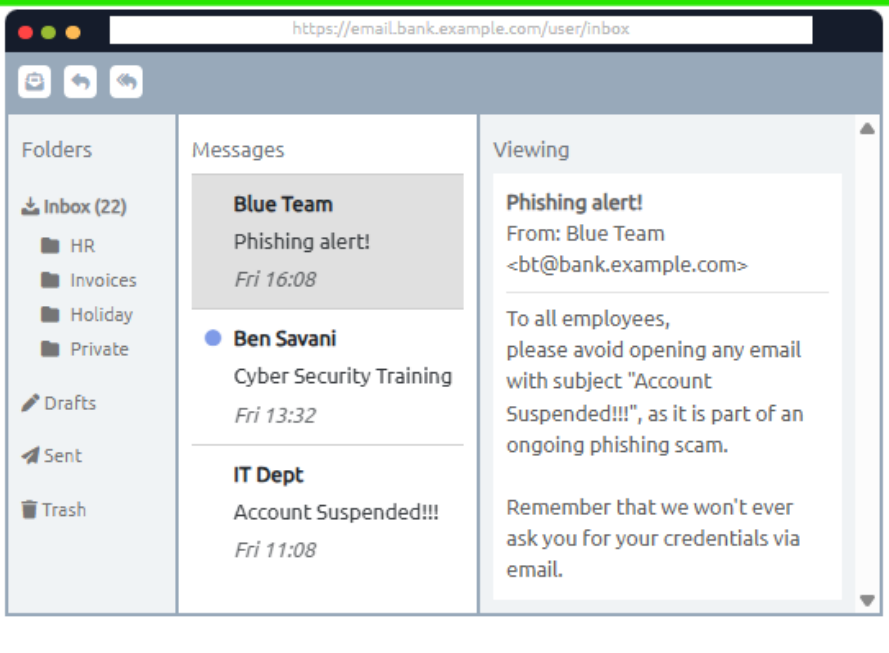


HOWEVER, SOME USERS HAD ALREADY OPENED THE MALICIOUS ATTACHMENT. THE RED TEAM GAINED ACCESS TO BOB-PC WITH 'BOB' PRIVILEGES.

The red team starts the engagement by emulating a phishing campaign against a list of emails they made, based on employees' names found on LinkedIn and a detected pattern in their email addresses.

julie.smith@bank.example.com  
john.watson@bank.example.com

The phishing campaign was detected. The blue team sent an email to all employees to warn them of the ongoing threat. This still allowed the attack to carry on, as there was no process in place to check for possibly infected PCs or even delete any copies of the malicious email from all users' inboxes.



Next

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.

4. Emulating TTP: Privilege Escalation and Persistence

LOCAL PRIVILEGE  
ESCALATION & PERSISTENCE

C:\> whoami  
BOB-PC\SYSTEM

UNDETECTED

BY APPLYING ANTIVIRUS  
EVASION TECHNIQUES, IT  
WAS POSSIBLE TO CLOAK A  
KNOWN LOCAL EXPLOIT TO  
GAIN SYSTEM ACCOUNT  
PRIVILEGES WITHOUT BEING  
DETECTED

BY DUMPING LOCAL ACCOUNTS, A PASSWORD  
HASH FOR A LOCAL ADMIN "BACKUPS" WAS  
OBTAINED. THE HASH COULDNT BE CRACKED...

The red team found missing Windows patches on BOB-PC. One of them allowed for PrintNightmare exploitation.

While the available public exploit was detected by many AV solutions, some AV evasion techniques were successfully applied to avoid triggering any alarms, obtaining SYSTEM privileges.

The red team was able to upload and run a modified mimikatz to extract local password hashes, including the local administrator account "Backups".

```
mimikatz #lsadump::sam
Domain : BANK
SysKey : 606c5f914ffd4c3bc8553b69b968e0c7

SAMKey : fdb2b417771ad800254c6324e213ad64

RID : 000001f4 (500)
User : Administrator
LM :
NTLM : 31d6cfe0d16ae931b73c59d7e0c089c0

RID : 000003e9 (1001)
User : Backups
NTLM : 5fb8724896a778fcc3eeca1c28ac51f5


mimikatz #
```

Next

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.

### 5. Emulating TTP: Lateral Movement



A DIRECT CONNECTION FROM BOB-PC TO THE DATABASE WAS BLOCKED BY THE FIREWALL. USING PASS-THE-HASH IT WAS POSSIBLE TO CONNECT TO DBA-PC USING "BACKUPS" USER'S PASSWORD HASH. USING CREDENTIALS FOUND ON A TXT FILE ON DBA-PC'S DESKTOP, IT WAS POSSIBLE TO ACCESS THE DB.

The red team used a Pass-the-Hash attack against all hosts on the network to check if the "Backups" user could login to other hosts. No direct connection could be made to the DB server, as firewall policies were in place to prevent it.

After doing some additional recon, a workstation called DBA-PC was identified. Using Pass-the-Hash, DBA-PC was compromised and used as a pivot to connect to the DB server.

While the Pass-the-Hash attempts triggered many alerts on login attempts from the user "Backups", the blue team ignored them as they were confused with a batch backups process which runs monthly.


Next

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.



6. Reporting and Analysis



IN THE END, RED, WHITE AND BLUE TEAMS WILL CHECK TOGETHER HOW SECURITY CONTROLS CAN BE IMPROVED IN ORDER TO BE READY FOR A REAL THREAT

After finishing with the exercise, red, white and blue teams will meet and discuss about how to improve the security of the bank.

Although we are focusing on the specific TTPs that allowed the red team to reach its objective, in a real-life engagement, you will usually have failed attempts as well. It is important to note that those "failed" attempts can still provide valid information for the exercise. Suppose, for example, that you ran some brute force attacks against the DB server and never got any valid credentials from it. It might still be interesting to check if the Blue Team detected the attack at the end of the engagement.

Also, remember that many things might take unexpected turns during the engagement. Maintaining clear communication between the red and white teams is vital to make decisions that will direct the exercise in the right course and avoid conflicts at the end of the road.

THM{RED\_TEAM\_ROCKS}

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.