

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

1. Planning the Engagement

RED TEAM ENGAGEMENTS

ISSUE 2
TRYHACKME COMICS

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

Figura 1 (Compromiso 1)

2. Recopilación de inteligencia

2. Intelligence Gathering

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

Figura 2 (Compromiso 2)

3. Emulando TTP: Campaña de phishing

3. Emulating TTP: Phishing campaign

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

Figura 3 (Compromiso 3)

4. Emulación de TTP: Escalada de privilegios y persistencia

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 COULDN'T 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 : 31d6cfe0d18ae931b73c59d7e0c089c0

RID : 000003e9 (1001)
User : Backups
NTLM : 5fb8724896a778fcc3eeeca1c28ac51f5
```

Next

Figura 4 (Compromiso 4)

5. Emulación de TTP: Movimiento lateral

5. Emulating TTP: Lateral Movement

LATERAL MOVEMENT

BOB-PC → DBA-PC → DB

DETECTED

BACKUPS login attempt on:
10.1.1.1(10:21:10)
10.1.1.2(10:21:11)

SUSPICIOUS LOGS

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

Figura 5 (Compromiso 5)

6. Informes y análisis - (Flag encontrada)

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}

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>