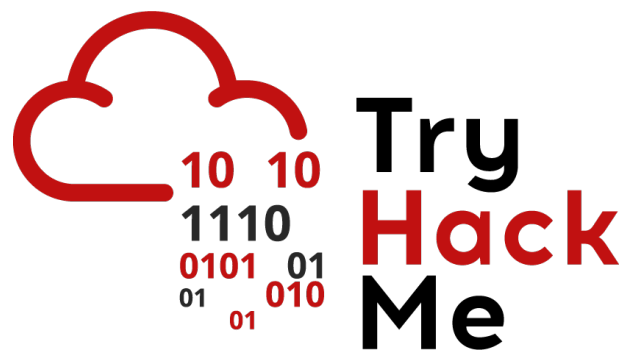


Writeup: Sala *Pentesting Fundamentals*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

1. Introducción	2
2. Sala	2
2.1. Tarea 1 - ¿Qué son las pruebas de penetración?	2
2.2. Tarea 2 - Ética de las pruebas de penetración	2
2.3. Tarea 3 - Metodologías de pruebas de penetración	3
2.4. Tarea 4 - Caja Negra, Caja Blanca y Caja Gris	3
2.5. Tarea 5 - Práctica: Prueba de penetración ACME	4
3. Conclusión sobre la Sala	10

1. Introducción

En esta sala vamos a introducirnos en los conceptos básicos del pentesting, iremos paso a paso aprendiendo conceptos esenciales para comenzar en el mundo de la ciberseguridad ofensiva. También, se abordan temas fundamentales como el reconocimiento, escaneo, enumeración, explotación y post-explotación.

2. Sala

2.1. Tarea 1 - ¿Qué son las pruebas de penetración?

En esta primera tarea, aprenderemos el concepto de una prueba de penetración como un proceso autorizado y controlado que simula ataques reales para identificar vulnerabilidades en sistemas, redes o aplicaciones. Además, su importancia en la ciberseguridad, destacando cómo ayuda a fortalecer la defensa de una organización.

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

2.2. Tarea 2 - Ética de las pruebas de penetración

Ahora, abordaremos la importancia de la ética en las pruebas de penetración, destacando que todo análisis debe realizarse con autorización explícita y siguiendo un marco legal. Además, conoceremos como los hackers son clasificados en tres categorías, según su ética y las motivaciones de sus acciones:

- **White Hat**
- **Grey Hat**
- **Black Hat**

Una vez que logramos comprender la importancia de la ética en las pruebas de penetración, vamos a contestar las siguientes preguntas.

Preguntas: You are given permission to perform a security audit on an organisation; what type of hacker would you be?

Respuesta: **White Hat**

Preguntas: You attack an organisation and steal their data, what type of hacker would you be?

Respuesta: **Black Hat**

Preguntas: What document defines how a penetration testing engagement should be carried out?

Respuesta: **Rules of Engagement**

2.3. Tarea 3 - Metodologías de pruebas de penetración

Aprenderemos sobre las distintas metodologías utilizadas para llevar a cabo pruebas de penetración de manera estructurada y efectiva. Conoceremos algunos marcos como **OWASP**, **PTES** y **NIST**, los cuales guían las etapas del pentesting desde la recolección de información hasta la explotación y el reporte.

Ahora, una vez comprendido las metodologías para las pruebas de penetración, responderemos algunas preguntas para completar la tarea.

Pregunta: What stage of penetration testing involves using publicly available information?

Respuesta: **Information Gathering**

Pregunta: If you wanted to use a framework for pentesting telecommunications, what framework would you use? Note: We're looking for the acronym here and not the full name?

Respuesta: **OSSTMM**

Pregunta: What framework focuses on the testing of web applications?

Respuesta: **OWASP**

2.4. Tarea 4 - Caja Negra, Caja Blanca y Caja Gris

Ahora, aprenderemos sobre los tres enfoques principales utilizados en pruebas de penetración, según el nivel de acceso o información previa que se tiene sobre el sistema objetivo.

- **Black Box:** El pentester no posee ningún conocimiento interno, simulando un atacante externo.
- **White Box:** El pentester tiene acceso completo al sistema, código fuente o arquitectura.
- **Grey Box:** Combina ambos enfoques, con acceso limitado a ciertos datos o credenciales.

Una vez entendido los diferentes enfoques, procederemos a responder las siguientes preguntas:

Pregunta: You are asked to test an application but are not given access to its source code - what testing process is this?

Respuesta: **Black Box**

Pregunta: You are asked to test a website, and you are given access to the source code - what testing process is this?

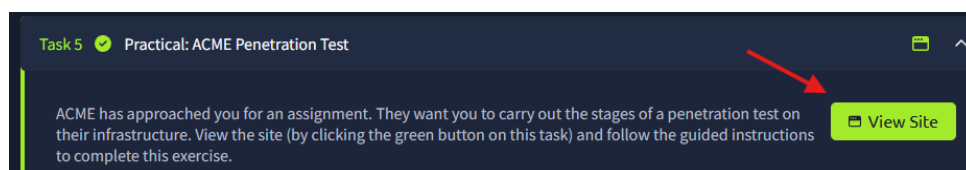
Respuesta: **White Box**

2.5. Tarea 5 - Práctica: Prueba de penetración ACME

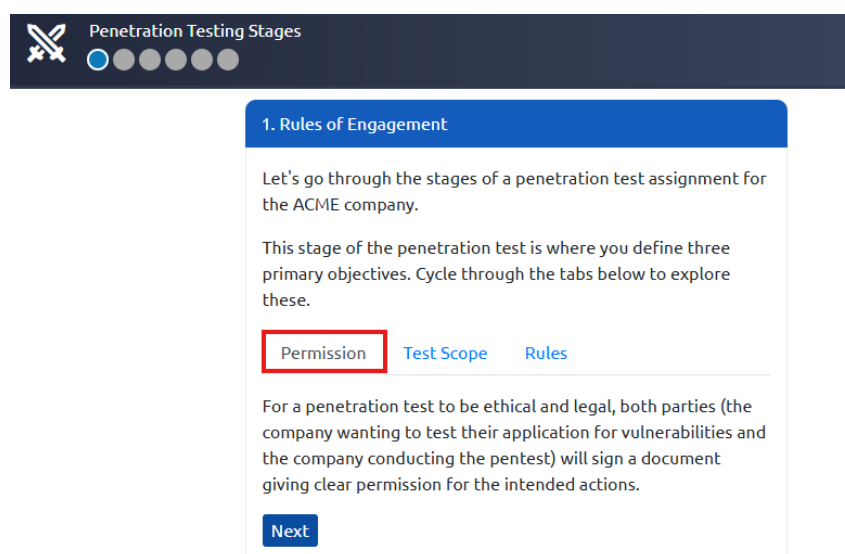
Vamos a realizar una práctica con el objetivo de realizar una prueba de penetración controlada contra una máquina simulada de la empresa ficticia ACME.

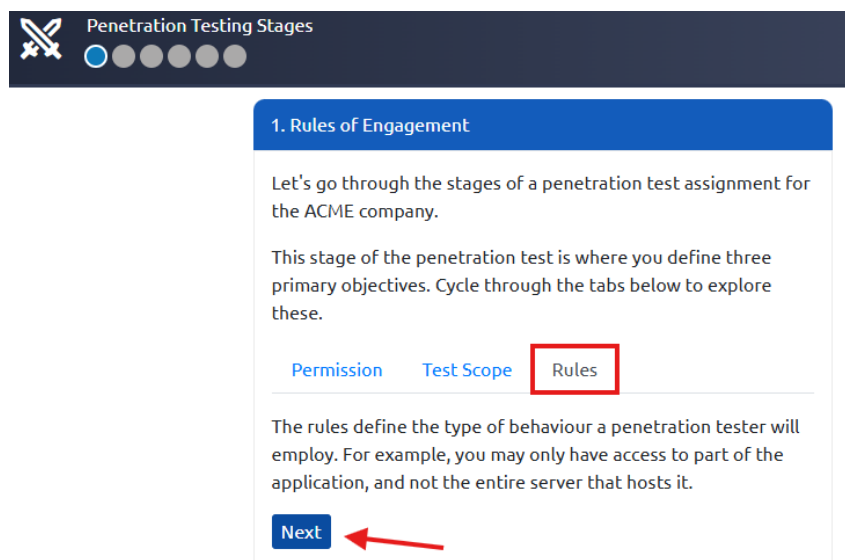
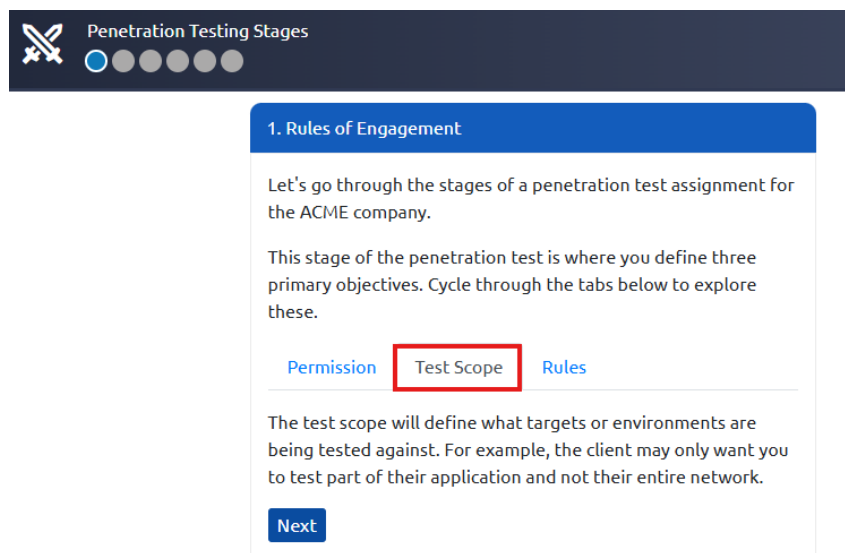
Pregunta: Complete the penetration test engagement against ACME's infrastructure

Para comenzar debemos desplegar el sitio donde llevaremos a cabo la tarea, para ello, haremos clic en **View Site** en el lado superior.

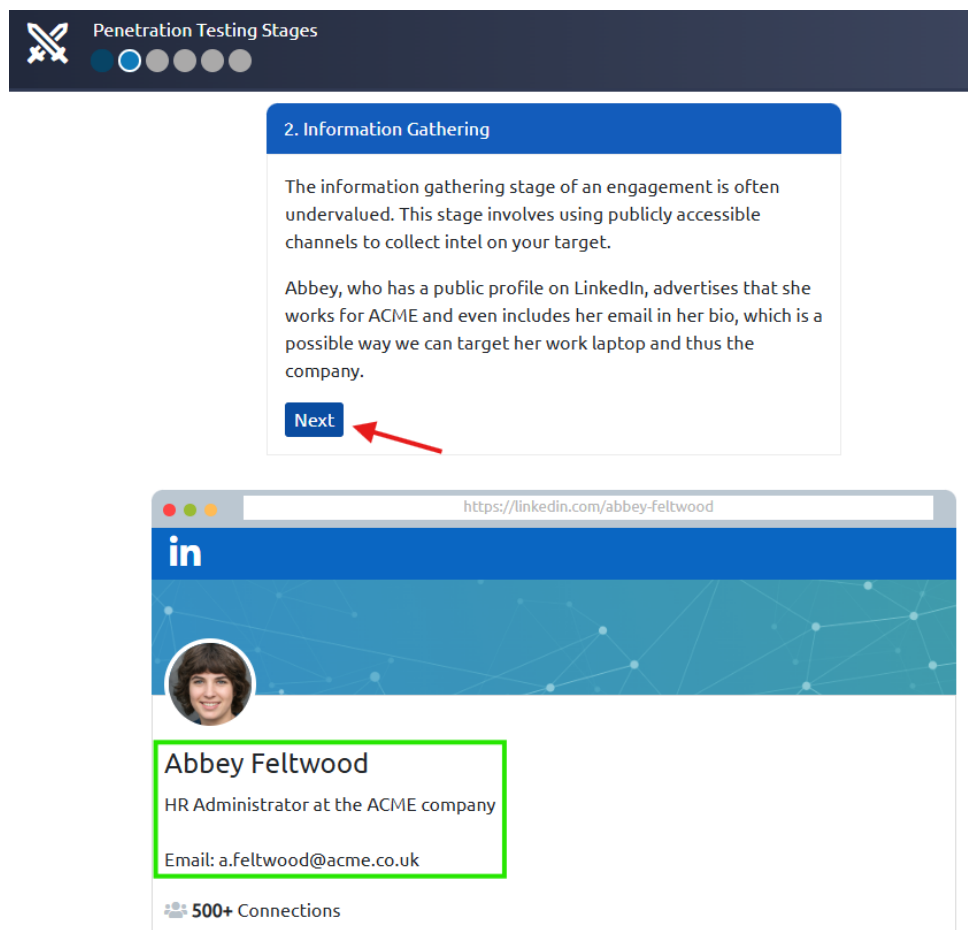


Una vez que desplegamos el sitio, vamos a empezar a recorrer las distintas etapas de una prueba de penetración. La primera etapa aprenderemos conoceremos las reglas de intervención. Simplemente iremos explorando las distintas pestañas y leyendo su contenido, después que comprendemos esta etapa, haremos clic en **Next** para continuar con la siguiente.





Ahora, nos encontraremos en la etapa 2 de recopilar información. Aprenderemos como en fuentes públicas como LinkedIn podemos encontrar información útil (como correo electrónico, puesto, nombres, etc) de una persona de dicha empresa. Posterior a eso, haremos clic en **Next** para continuar.



Penetration Testing Stages

2. Information Gathering


The information gathering stage of an engagement is often undervalued. This stage involves using publicly accessible channels to collect intel on your target.

Abbey, who has a public profile on LinkedIn, advertises that she works for ACME and even includes her email in her bio, which is a possible way we can target her work laptop and thus the company.

[Next](#)

https://linkedin.com/abbey-feltwood

in



Abbey Feltwood
HR Administrator at the ACME company
Email: a.feltwood@acme.co.uk

500+ Connections

Aprenderemos ahora de la etapa de enumeración que es muy importante, los hallazgos vulnerables que encontremos serán útiles para luego realizar la explotación del sistema objetivo (étapa 4).

En este caso vamos a introducirnos en una situación donde suponemos que encontramos una IP y debemos realizar un escaneo para conocer si contiene alguna vulnerabilidad la empresa ficticia.

Penetration Testing Stages

3. Enumeration & Scanning

The goal of this stage is to get a complete picture of your target. A penetration tester will try to identify user accounts, machines on their network, network shares, applications etc. Information gathered from stage 2, and the engagement scope document will help in enumerating your target.

The enumeration phase is very important as your findings are used to exploit your target's systems (stage 4).

Let's pretend Abbey from stage 2 made a post on LinkedIn sharing a blog post she wrote about ACME. From this post, you find ACME's web server's IP "96.37.50.151" try scanning it.

[Next](#)

IP Address Scan Target

attacker switch target

```
user@thm:~$ scan
```

Vamos a escribir la IP y procederemos a escanear al objetivo y conoceremos las vulnerabilidades disponibles. Posterior a eso, vamos a darle a **Next** para seguir con la siguiente etapa.

3. Enumeration & Scanning

The goal of this stage is to get a complete picture of your target. A penetration tester will try to identify user accounts, machines on their network, network shares, applications etc. Information gathered from stage 2, and the engagement scope document will help in enumerating your target.

The enumeration phase is very important as your findings are used to exploit your target's systems (stage 4).

Let's pretend Abbey from stage 2 made a post on LinkedIn sharing a blog post she wrote about ACME. From this post, you find ACME's web server's IP "96.37.50.151"; try scanning it.

[Next](#)

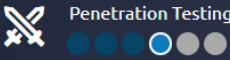
96.37.50.151 Scan Target

attacker switch target

```
user@thm:~$ scan 96.37.50.151
Starting vulnerability scan
Vulnerability scan for 96.37.50.151
Service Vulnerable?
Web Yes
Login No
```

Nos entraremos en la etapa 4 de explotación donde se usa una vulnerabilidad descubierta para obtener acceso no autorizado a un sistema objetivo. Aprenderemos que el conocimiento obtenido de una enumeración es para conseguir identificar y explotar vulnerabilidades.

Una vez que comprendemos esta etapa, haremos clic en **Next** para seguir.



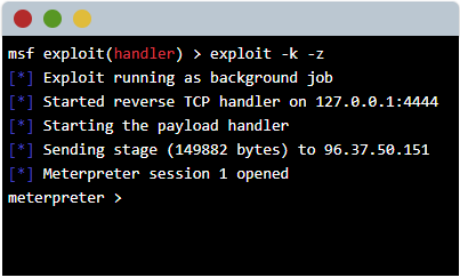
4. Exploitation

The exploitation stage involves the knowledge from your enumeration to now identify and exploit vulnerabilities in any of their applications (that are in scope).

For example, we enumerated ACME's website in stage 3 and found that it was vulnerable. We would now exploit this vulnerability, thus (ethically) hacking ACME's website.

Exploitation is the use of a vulnerability discovered to gain unauthorised access to an information security system or data.


Next



```
msf exploit(handler) > exploit -k -z
[*] Exploit running as background job
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] Starting the payload handler
[*] Sending stage (149882 bytes) to 96.37.50.151
[*] Meterpreter session 1 opened
meterpreter >
```

Attacker


The target machine is being attacked using a tool called Metasploit, something you'll learn about on TryHackMe



Target

Esta etapa de post-explotación comienza cuando logramos obtener acceso no autorizado a un sistema, los principales objetivos serán mantener el acceso al sistema y escalar privilegios dentro del sistema hasta un superusuario o usuario administrador. Una vez logrado, vamos a extraer información sensible del sistema y atacaremos otros componentes del entorno.

Después de comprender esta etapa, haremos clic en **Next** para continuar.

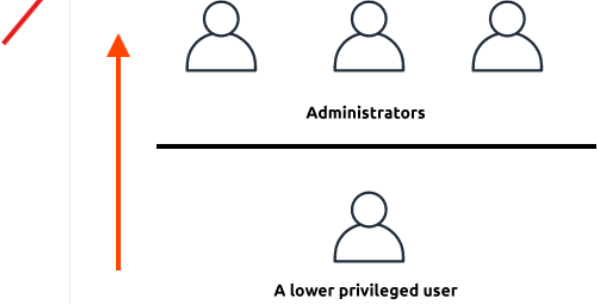
 Penetration Testing Stages

5. Post Exploitation

The post exploitation stage starts when you've gained unauthorised access to a system. At this stage of the engagement, your main goals will be to maintain access to the system and escalate your privileges within the system to a super user or administrator user. Systems are usually set up with normal users that don't have access to various sensitive files and functions - Gaining access to higher privileged users (such as administrators) will allow you to perform actions that you wouldn't be able to as a normal user (such as reading sensitive files and gaining access to all programs within the system).


After doing this, you'll be extracting sensitive information from the system and attacking other components in the environment (e.g. if the system is part of a network, you will attempt to gain access to other machines in the network).

Next



En esta última etapa aprenderemos sobre el objetivo que tenemos en explicar al cliente los resultados del trabajo. Esto suele ser un informe que contiene detalles sobre los problemas de seguridad que encontramos y cómo mitigarlos. El cliente utilizará este informe para comprender los problemas de seguridad y corregir los fallos.

Al final de la explicación de esta etapa, tendremos la flag que necesitamos para finalizar la práctica.

 Penetration Testing Stages

●●●●●○

6. Pentest Report & Clearing-up

This stage usually occurs at the end of a penetration test. As a penetration tester, you will have to explain the results of your engagement to the client. This is usually done in the form of a report that contains details regarding any security issues you've found and how to mitigate them. The client will use this report to understand the security issues and fix the flaws in the technology stack that was tested.

It's also best practice to clean up the environment you've been testing (where possible). For example, if you were provided access to machines or tooling by the client, you need to delete any artefacts that have been created as a result of testing.

Use **THM{PENTEST_COMPLETE}** to answer the task question on TryHackMe.

Respuesta: **THM{PENTEST_COMPLETE}**

3. Conclusión sobre la Sala

En esta sala hemos logrado obtener un conocimiento sólido sobre el mundo de las pruebas de penetración, abordando desde conceptos esenciales hasta metodologías y tipos de enfoques prácticos. Aprendimos qué es el pentesting, su importancia ética y legal, cómo se estructura un proceso profesional y se aplica todo en un ejercicio práctico.