

Fundamentos de las pruebas de penetración

Tarea 1: ¿Qué son las pruebas de penetración?

P: ¡Léame!

R: No se necesita respuesta

Tarea 2: Ética de las pruebas de penetración

P1: Te dan permiso para realizar una auditoría de seguridad en una organización;

¿qué tipo de hacker serías?

R1: White Hat / Sombrero Blanco

P2: Si atacas una organización y robas sus datos, ¿qué tipo de hacker serías?

R2: Black Hat / Sombrero Negro

P3: ¿Qué documento define cómo se debe llevar a cabo una prueba de penetración?

R3: Rules of Engagement / Reglas de Compromiso

Tarea 3: Metodologías de pruebas de penetración

P1: ¿Qué etapa de la prueba de penetración implica el uso de información disponible públicamente?

R1: Information Gathering / Recopilación de información

P2: Si quisieras usar un framework para realizar pruebas de penetración en telecomunicaciones, ¿qué framework usarías? Nota: Buscamos el acrónimo, no el nombre completo.

R2: OSSTMM

P3: ¿Qué marco se centra en la prueba de aplicaciones web?

R3: OWASP

Tarea 4: Pruebas de penetración de caja negra, caja blanca y caja gris

P1: Se le pide que pruebe una aplicación, pero no se le da acceso a su código fuente: ¿qué proceso de prueba es este?

R1: Black Box / Caja Negra

P2: Se le pide que pruebe un sitio web y se le da acceso al código fuente: ¿qué proceso de prueba es este?

R2: White Box / Caja Blanca

Tarea 5: Práctica: Prueba de penetración ACME

P: Completar la prueba de penetración contra la infraestructura de ACME.

Etapas de las pruebas de penetración

1) Reglas de enfrentamiento

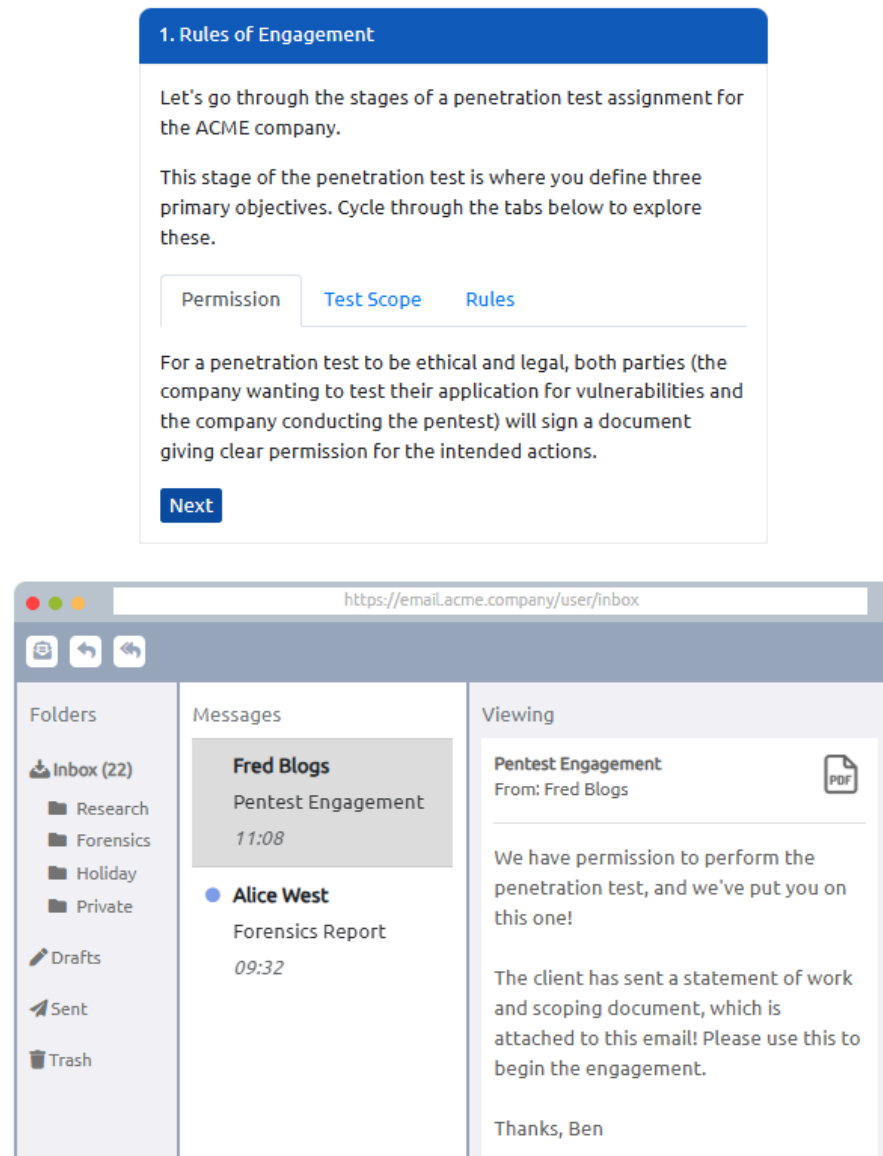


Figura 1 (Etapa 1)

2) Recopilación de información

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

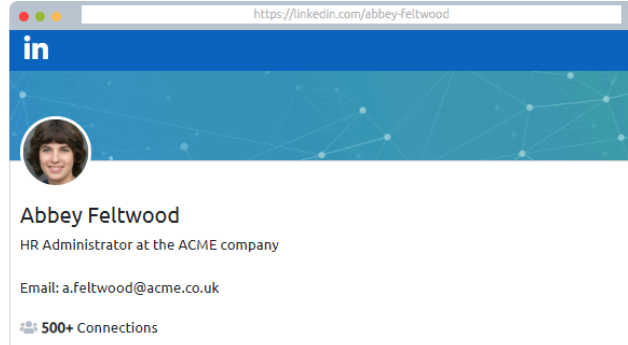


Figura 2 (Etapa 2)

3) Enumeración y escaneo

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

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
user@thm:~$ scan 96.37.50.151
```

Figura 3 (Etapa 3)

4) Explotación

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

Figura 4 (Etapla 4)

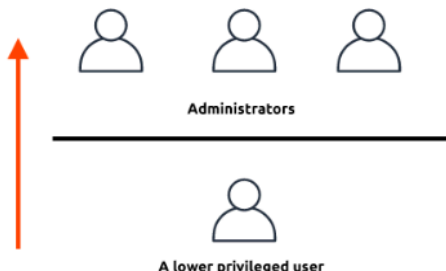
5) Post explotación

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](#)



Administrators

A lower privileged user

Figura 5 (Etapla 5)

6) Informe de prueba de penetración y limpieza

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.

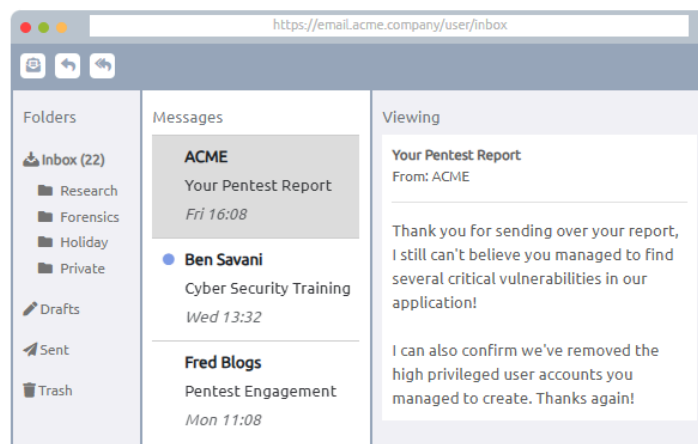


Figura 6 (Etapla 6)

R:THM{PENTEST_COMPLETE}

 **LinkedIn:** <https://www.linkedin.com/in/mateo-rodr%C3%ADguez-suar-202695249/>

 **GitHub:** <https://github.com/MaateoSuar>