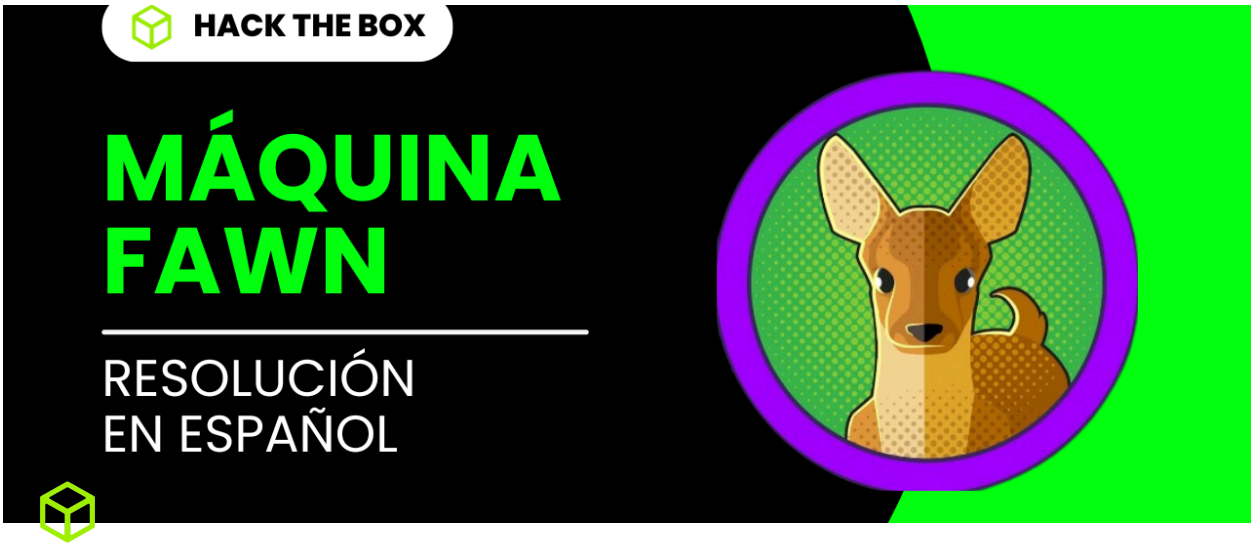


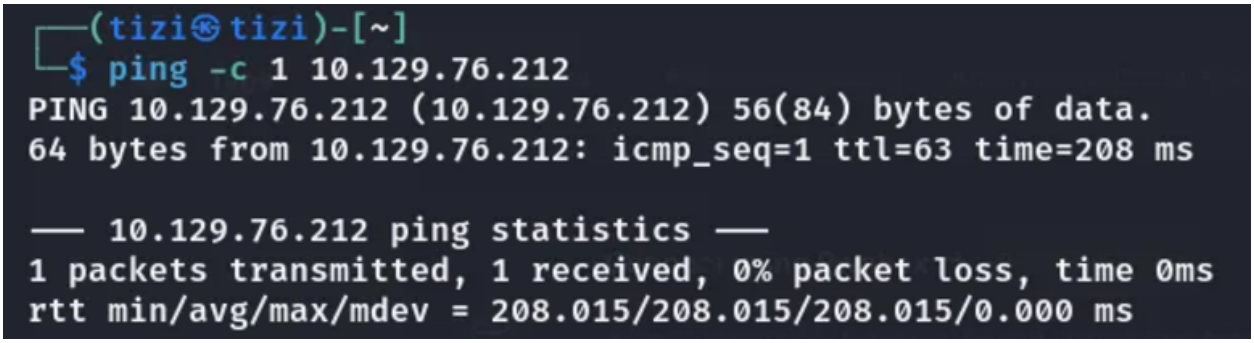
Hack the Box — Máquina Fawn

Máquina Fawn

- **Perfil**: Red Team - Pentesting
- **Sección**: Starting Point
- **Dificultad**: Muy fácil

El primer paso como siempre es **prender la máquina víctima** y observar la dirección IP, la cual en este caso, será **10.129.76.212**.

Vamos a contemplar un *ping* para corroborar que tenemos conexión con el equipo a vulnerar.



Confirmamos pues que la conexión con la máquina no presenta inconvenientes y funciona adecuadamente.

Comenzaremos a responder las preguntas que nos indica la plataforma:

Task 1:

> What does the 3-letter acronym FTP stand for?
>
> ***File Transfer Protocol*** *(Protocolo de Transferencia de Archivos)*

Este protocolo es uno de los más importantes en el ámbito de la informática. Permite la transferencia de archivos entre un host y otro mediante una red TCP como Internet.

Procederemos a realizar un **escaneo básico** para confirmar si esta máquina tiene activo el servicio.

Confirmamos tras el escaneo a través de *nmap* que el servicio FTP está corriendo a través del puerto 21.

Task 2:

> Which port does the FTP service listen on usually?
>
> ***21***

Task 3:

> What acronym is used for the secure version of FTP?
>
> ***SFTP***

SFTP (*Secure File Transfer Protocol* — Protocolo de Transferencia de Archivos de manera Segura) es la **versión segura para el protocolo FTP**, ofreciendo encriptación y autenticación para la transferencia de archivos.

Task 4:

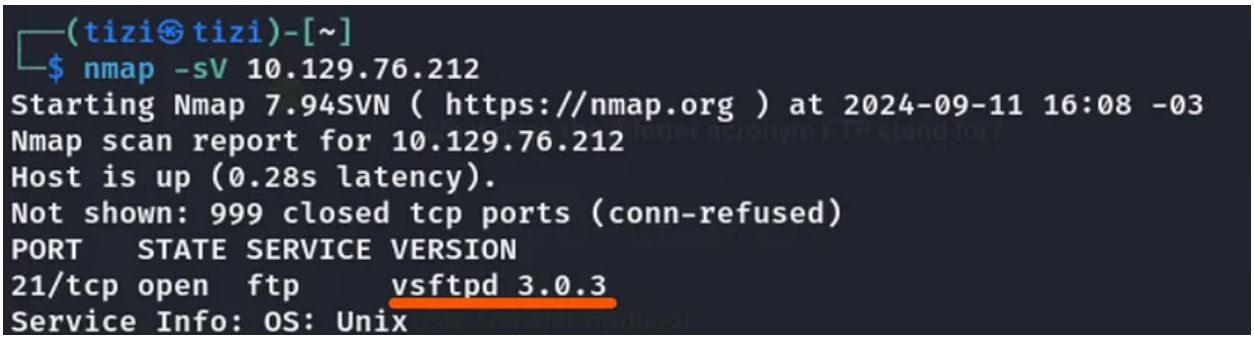
> What is the command we can use to send an ICMP echo request to test our connection to the target?
>
> ***ping***

Como hemos realizado previamente, el comando *ping* nos permite verificar si tenemos una conexión con el objetivo en cuestión.

Task 5:

> From your scans, what version is FTP running on the target?
>
> ***vsftpd 3.0.3***

Es importante utilizar el parámetro **-sV** para poder visualizar la versión servicio asociado. Caso contrario, no aparecerá por la pantalla.



Task 6:

> From your scans, what OS type is running on the target?
>
> ***Unix***

Task 7:

> What is the command we need to run in order to display the ‘ftp’ client help menu?
>
> ***ftp -h***

Este comando, junto con este parámetro, nos muestra el **menú de ayuda** del servicio FTP.

```
┌──(tizi㉿tizi)-[~]
└─$ ftp -h
ftp: -h: unknown option
usage: ftp [-46AadefginpRtVv] [-N NETRC] [-o OUTPUT] [-P PORT] [-q QUITTIME]
           [-r RETRY] [-s SRCADDR] [-T DIR,MAX[,INC]] [-x XFERSIZE]
           [[USER@]HOST [PORT]]
           [[USER@]HOST:[PATH][/]]
           [file:///PATH]
           [ftp://[USER[:PASSWORD]@]HOST[:PORT]/PATH[/][;type=TYPE]]
           [http://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
           [https://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
           ...
       ftp -u URL FILE ...
       ftp -?
```

Vamos a ingresar al FTP de esta dirección IP a ver qué podemos encontrar.

```
┌──(tizi㉿tizi)-[~]
└─$ ftp 10.129.76.212
Connected to 10.129.76.212.
220 (vsFTPd 3.0.3)
Name (10.129.76.212:tizi): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> _
```

Task 8:

> What is username that is used over FTP when you want to log in without having an account?
>
> ***anonymous***

Colocando este nombre de usuario y sin contraseña, accederemos.

Task 9:

> What is the response code we get for the FTP message ‘Login successful’?

> ***230***

Task 10:

> There are a couple of commands we can use to list the files and directories available on the FTP server. One is dir. What is the other that is a common way to list files on a Linux system.
>
> ***ls***

ls es un comando básico en Linux que nos permite **listar los elementos y archivos dentro de un directorio**. Procederemos a hacerlo en nuestra sesión FTP.

```
ftp> ls
229 Entering Extended Passive Mode (|||35662|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
226 Directory send OK.
ftp> _
```

A un costado, hemos encontrado el archivo que buscábamos, es decir, **flag.txt**. Posteriormente, procederemos a descargarlo hacia nuestro equipo.

Task 11:

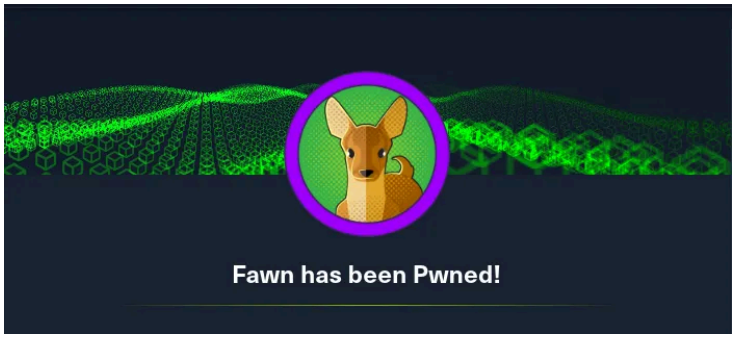
> What is the command used to download the file we found on the FTP server?
>
> ***get***

```
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||46467|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |***************************************|    32        0.16 KiB/s    00:00 ETA
226 Transfer complete.
32 bytes received in 00:00 (0.05 KiB/s)
ftp> exit_
```

Una vez descargado el archivo de texto, cerramos la sesión con *exit* y realizamos un *ls* en nuestra máquina para verificar que se haya descargado correctamente.

Hacemos un *cat flag.txt* para visualizar el contenido.

Colocamos esa secuencia de caracteres dentro de la plataforma de Hack The Box para dar por finalizada y completada la máquina vulnerable.



Oficialmente, la máquina fue completada con éxito.

RESOLUCIÓN EN VIDEO:

https://www.youtube.com/watch?v=g-8FXZiiDBQ