Hackthebox

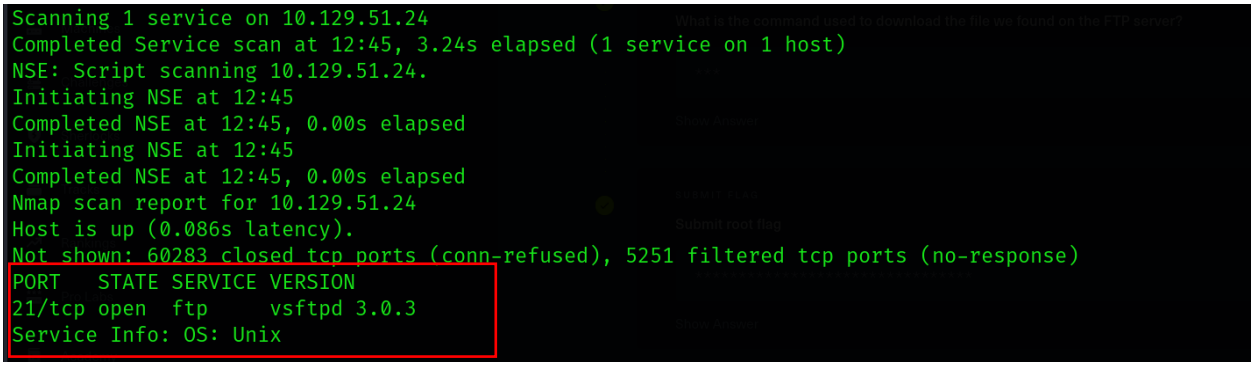
Hack The Box :: Starting Point

Fawn

STEP 1: Discover the network

Let's scan the network with nmap tool to see if there any ports is open.

$ nmap -Pn -p- -sV -v -T5 <IP>



we found one port open, this port is ftp.

STEP 2: connection with ftp

$ ftp <IP>

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.129.51.24
Connected to 10.129.51.24.
220 (vsFTPd 3.0.3)
Name (10.129.51.24:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

The ftp is accessible with anonymous login.

we can do the command

$ ls

to show the files.

```
ftp> ls
229 Entering Extended Passive Mode (|||13001|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
226 Directory send OK.
```

we found the file **flag.txt**

and we can install them with this command

$ get <filename>

this command displays the contents of the file

$ cat <filename>


┌──(kali㉿kali)-[~]
└─$ cat flag.txt