Tier 0 Fawn Report

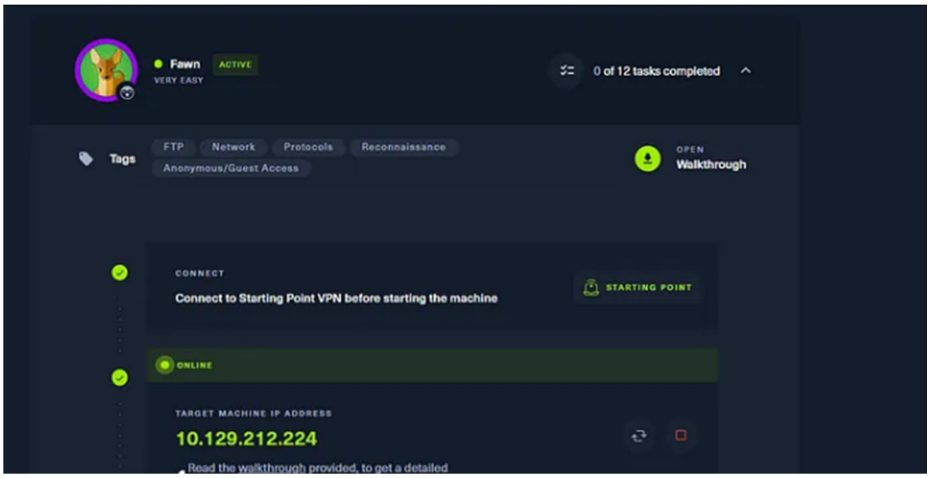
Prepared by: **Chanpreet Kaur**

Tools Used

- NMAP
- FTP

Procedure

I will cover solution steps of the "**Fawn**" machine, which is part of the '**Starting Point**' labs and has a difficulty rating of '***Very Easy***'.



The machine is now active and showing a target IP address **10.129.212.224**

Now, we have to solve all the available tasks by providing correct inputs, we can also use hints in case we are stuck.

- **What does the 3-letter acronym FTP stand for?**
  File Transfer Protocol

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

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

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

To solve next 2 tasks run nmap scan on the [Target_IP] as shown below –

```
┌──(root㉿kali)-[~/HTB/fawn]
└─# nmap 10.129.85.249 -p- -sC -sV -oN nmap_fawn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-06 09:55 EDT
Nmap scan report for 10.129.85.249 (10.129.85.249)
Host is up (0.15s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.18
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 857.30 seconds
```

After executing the command, I discovered the presence of an FTP service running.

Thanks to the '-sC' option, the default script has successfully retrieved the 'flag.txt' file using an anonymous login.

which means this server is subjected to anonymous login vulnerability. So let's start exploiting this.

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

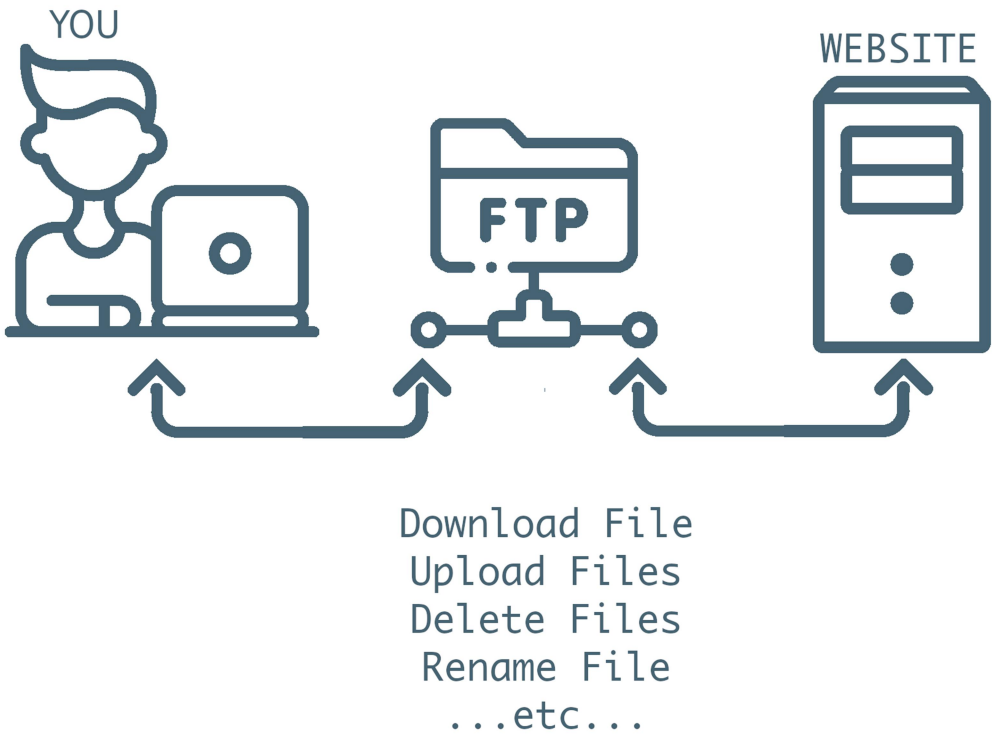
- **From your scans, what OS type is running on the target?**
  Unix

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

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

FTP .

FTP (File Transfer Protocol) is a network protocol for transmitting files between computers over Transmission Control Protocol/Internet Protocol (TCP/IP) connections. Within the TCP/IP suite, FTP is considered an application layer protocol.



To progress with the next task, we need to access the FTP service by utilizing the provided command:

'ftp [Target_IP]'

We can use “anonymous” as username which is already covered in previous task and in password field try default value i.e. “password”.

And that should log us in the ftp server, now we can get the flag file using the “get” command obviously.

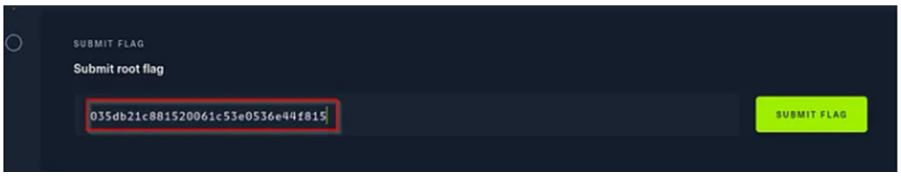
- What is the response code we get for the FTP message ‘Login successful’?
  220

- 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

- What is the command used to download the file we found on the FTP server?
  Get

Now, Open the downloaded file and copy the flag value

Submit the value in the browser to solve the last task as shown below –



Congratulations!!! You have made it…