


# Hack The Box Tier 0 Lab 2 "fawn" Walkthrough

## Connect To Starting Point VPN:


You must connect yourself to the starting point VPN before answering the question. You can choose one way to connect to the VPN from the following two ways shown below 📌.



**Connect using Pwnbox** → **RECOMMENDED**

A preconfigured, browser-based virtual machine with all the hacking tools you need pre-installed.

**Free 2h of Pwnbox** - Upgrade to VIP+ for Unlimited Access



**Connect using OpenVPN** →


Use your own machine for hacking. Download your VPN configuration and connect from your own environment.

**Having Trouble?** - Introduction to Lab Access

Once you're connected to the Starting Point VPN now spawn your machine by clicking on the SPAWN MACHINE button shown in the image below 📌.

SPAWN MACHINE

Spawn the target machine and the IP will show here

 **SPAWN MACHINE**

Now Let's start answering the questions.

## Task No 01:

What does the 3-letter acronym FTP stand for?

## Answer:

## File Transfer Protocol

TASK 1

What does the 3-letter acronym FTP stand for?

\*\*\*\* \* \* \* \*

**File Transfer Protocol**

Hide Answer

## Task No 02:

Which port does the FTP service listen on usually?

## Answer:

21

TASK 2

Which port does the FTP service listen on usually?

21

SUBMIT ANSWER HINT

## Task No 03:

FTP sends data in the clear, without any encryption. What acronym is used for a later protocol designed to provide similar functionality to FTP but securely, as an extension of the SSH protocol?

## Answer:

SFTP

TASK 3

FTP sends data in the clear, without any encryption. What acronym is used for a later protocol designed to provide similar functionality to FTP but securely, as an extension of the SSH protocol?

SFTP

SUBMIT ANSWER

HINT

## Task No 04:

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

## Answer:

ping

TASK 4

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

ping

SUBMIT ANSWER

HINT

## Task No 05:

From your scans, what version is FTP running on the target?

## Answer:

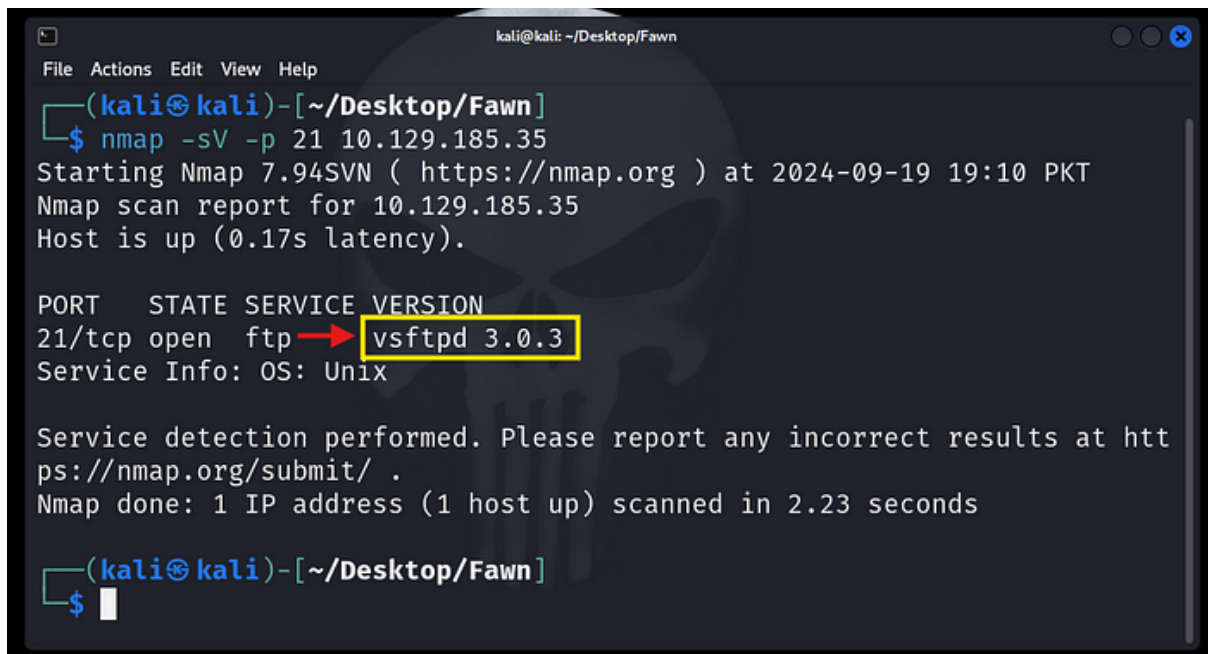
The answer is: ***vsftpd 3.0.3***

## How To Find FTP Version:

Let's find out what version of FTP is running on your target system. To find out the FTP version run this command in your bash.

```
nmap -sV -p 21 target-ip
```

After running the above command you should see an output like this.



```
kali@kali: ~/Desktop/Fawn
File Actions Edit View Help
(kali@kali)-[~/Desktop/Fawn]
$ nmap -sV -p 21 10.129.185.35
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 19:10 PKT
Nmap scan report for 10.129.185.35
Host is up (0.17s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp    vsftpd 3.0.3
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 2.23 seconds

(kali@kali)-[~/Desktop/Fawn]
$
```

The answer to task 5 is **vsftpd 3.0.3**.

## Command Explanation:

Now let's understand the above command briefly and see what each switch is doing.

- **nmap**: We use nmap for network mapping, vulnerability assessment, and network security auditing.
- **sV**: this switch will enable services version detection. This switch tells us the version of FTP of our target ip(system).
- **p 21**: this switch make sures that the scanning is only done on port 21 because that's the port used by FTP.

#### TASK 5

From your scans, what version is FTP running on the target?

```
***** *.*.3
```



**vsFTPd 3.0.3**

Hide Answer

## Task No 06:

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

## Answer:

The answer is: **Unix**

## How To Find OS Detail:

To find which Operating System is being used in your target system(ip given) we won't need any other command because the above command is also giving details about OS used in the target system.

Run this command once again 📌.

```
nmap -sV -p 21 target-ip
```

```
kali@kali: ~/Desktop/Fawn
File Actions Edit View Help
(kali@kali)-[~/Desktop/Fawn]
$ nmap -sV -p 21 10.129.185.35
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-19 19:10 PKT
Nmap scan report for 10.129.185.35
Host is up (0.17s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
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 2.23 seconds

(kali@kali)-[~/Desktop/Fawn]
$
```

The Operating System used in target system is **Unix**.

TASK 6

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

Unix

SUBMIT ANSWER HINT

## Task No 07:

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

## Answer:

ftp -h

TASK 7

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

ftp -h

SUBMIT ANSWER

HINT

## Task No 08:

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

## Answer:

anonymous

TASK 8

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

anonymous

SUBMIT ANSWER

HINT

## Task No 09:

What is the response code we get for the FTP message 'Login successful'?

## Answer:

230

```
kali@kali: ~/Desktop/Fawn
File Actions Edit View Help

(kali@kali)-[~/Desktop/Fawn]
$ ftp 10.129.185.35
Connected to 10.129.185.35.
220 (vsFTPd 3.0.3)
Name (10.129.185.35:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

TASK 9

What is the response code we get for the FTP message 'Login successful'?

230

SUBMIT ANSWER HINT

## Task No 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.

## Answer:

ls



#### 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.

SUBMIT ANSWERHINT

## Task No 11:

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

## Answer:

`get`

#### TASK 11

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

SUBMIT ANSWERHINT

## Task No 12:

Submit root flag

## Answer:

This root flag is: ***035db21c881520061c53e0536e44f815***

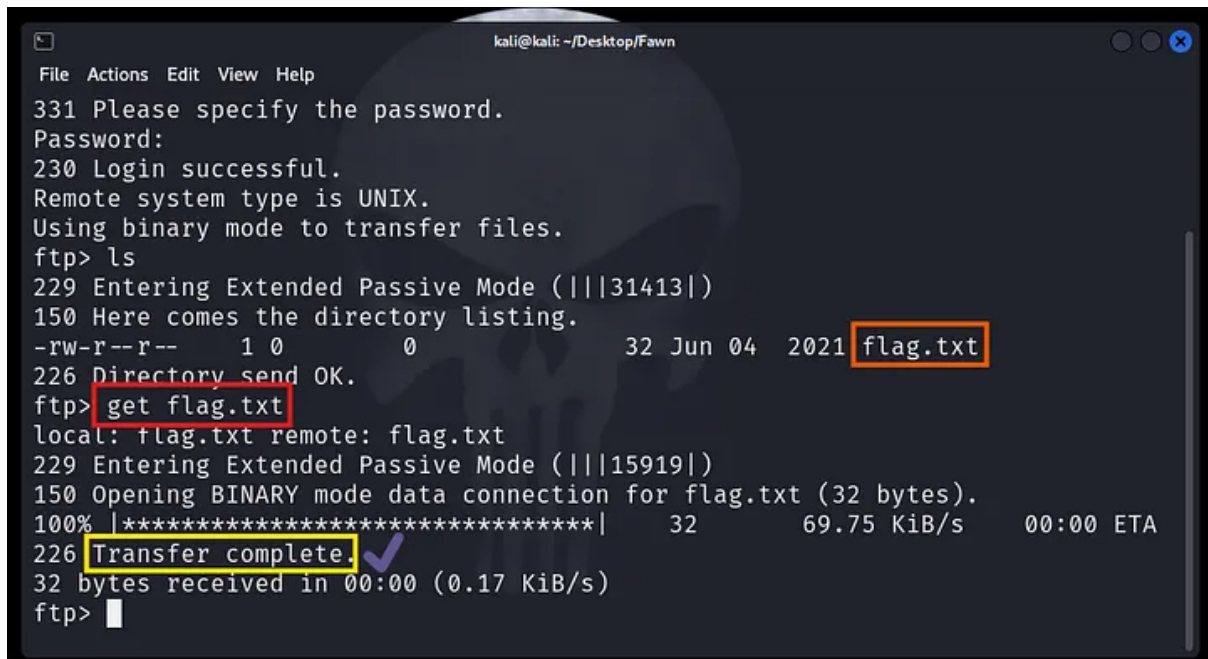
## How To Get The Root Flag:

This is fun part of this complete challenge because in this task you would need to download a file from the open port of the target ip. You would do so because the answer to this task is stored in a text file called `flag`.

First let's login to the open port of the target system. Enter the following command to login in to the the target ip's open port.

```
ftp target-ip
```

After entering the above 🖱️ command you will be prompted to enter a username and we know that when we try to enter an FTP port without having an account the username will be **anonymous**. So enter anonymous as your user and the password is **anon123**.



```
kali@kali: ~/Desktop/Fawn
File Actions Edit View Help
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 (|||31413|)
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 (|||15919|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |*****| 32 69.75 KiB/s 00:00 ETA
226 Transfer complete.
32 bytes received in 00:00 (0.17 KiB/s)
ftp>
```

Once you're logged in, now list down the files and folders in the current directory using ls command. You will see a text file named flag. Now download this file to your local system using the following command.

```
get flag.txt
```

The above 🖱️ command the flag.txt file into your local sytem. Now read the content of the file using cat command.

```
kali@kali: ~/Desktop/Fawn
File Actions Edit View Help

(kali@kali)-[~/Desktop/Fawn]
$ ls
flag.txt  starting_point_sohailburki.ovpn

(kali@kali)-[~/Desktop/Fawn]
$ cat flag.txt
035db21c881520061c53e0536e44f815

(kali@kali)-[~/Desktop/Fawn]
$
```

SUBMIT FLAG

Submit root flag

\*\*\*\*\*

035db21c881520061c53e0536e44f815

Hide Answer

Congratulation 🎉 you've successfully completed your second lab in hack the box Learning The Basics Of Penetration Testing Module.



**Fawn**  
VERY EASY

ACTIVE

**Machine Pwned** ▼