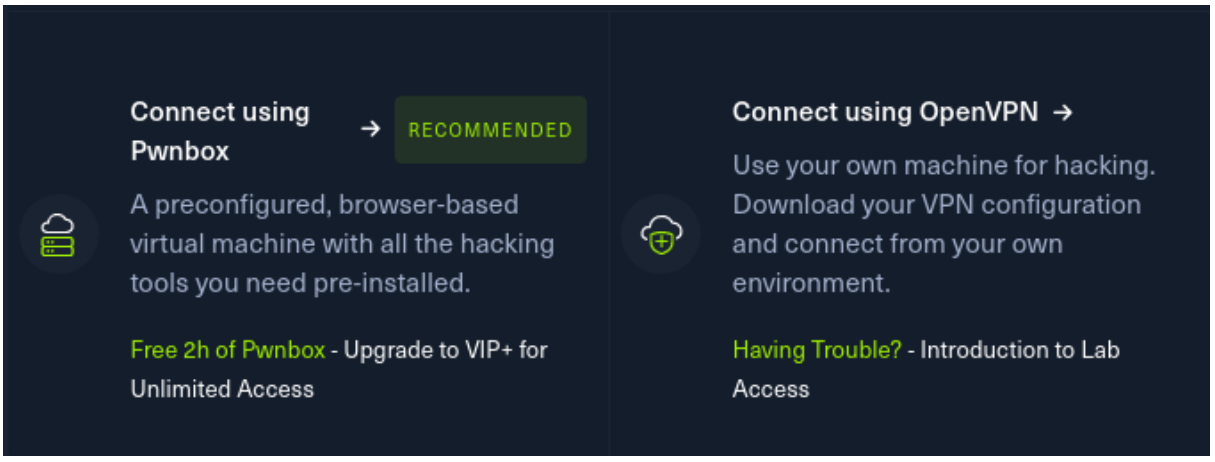
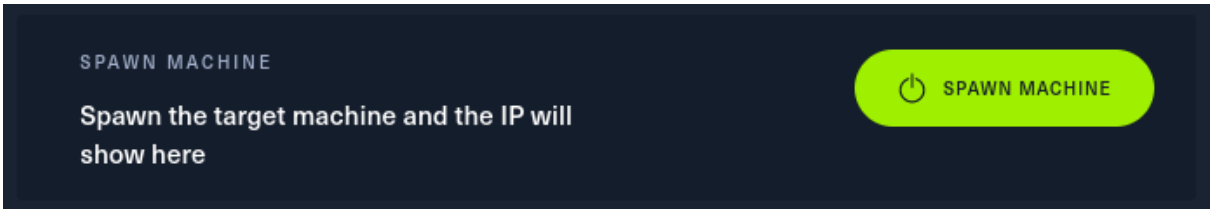
Hack The Box Tier 0 Lab 2 “fawn” Walkthrough

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 👇.



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 👇 .



Now Let’s start answering the questions.

Task No 01:

What does the 3-letter acronym FTP stand for?

Answer:

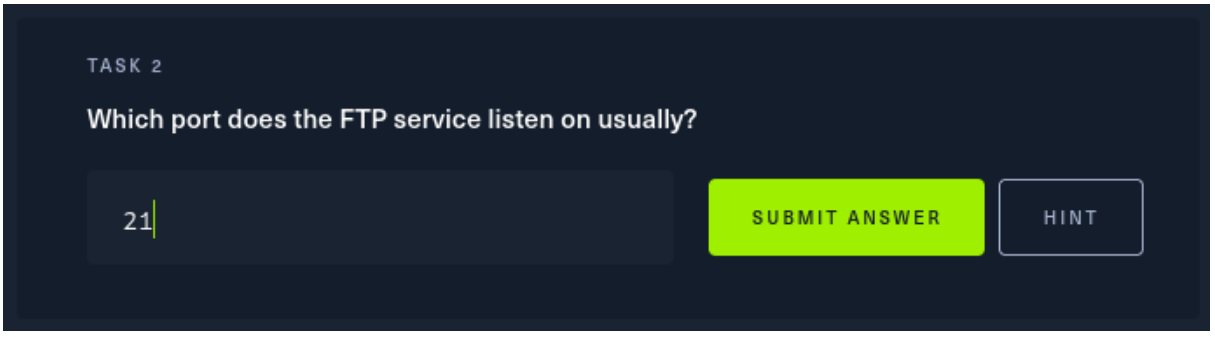
File Transfer Protocol

Task No 02:

Which port does the FTP service listen on usually?

Answer:

21

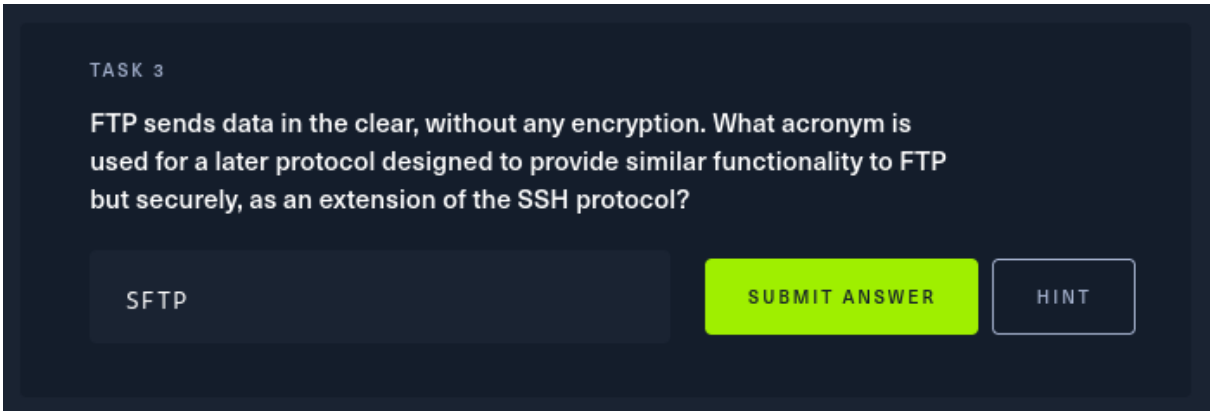


Task No 03:

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

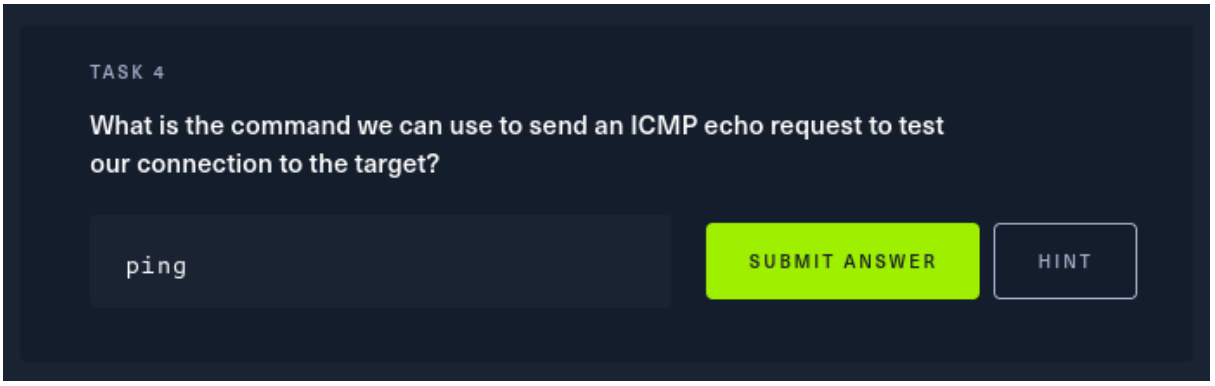


Task No 04:

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

Answer:

ping



Task No 05:

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

Answer:

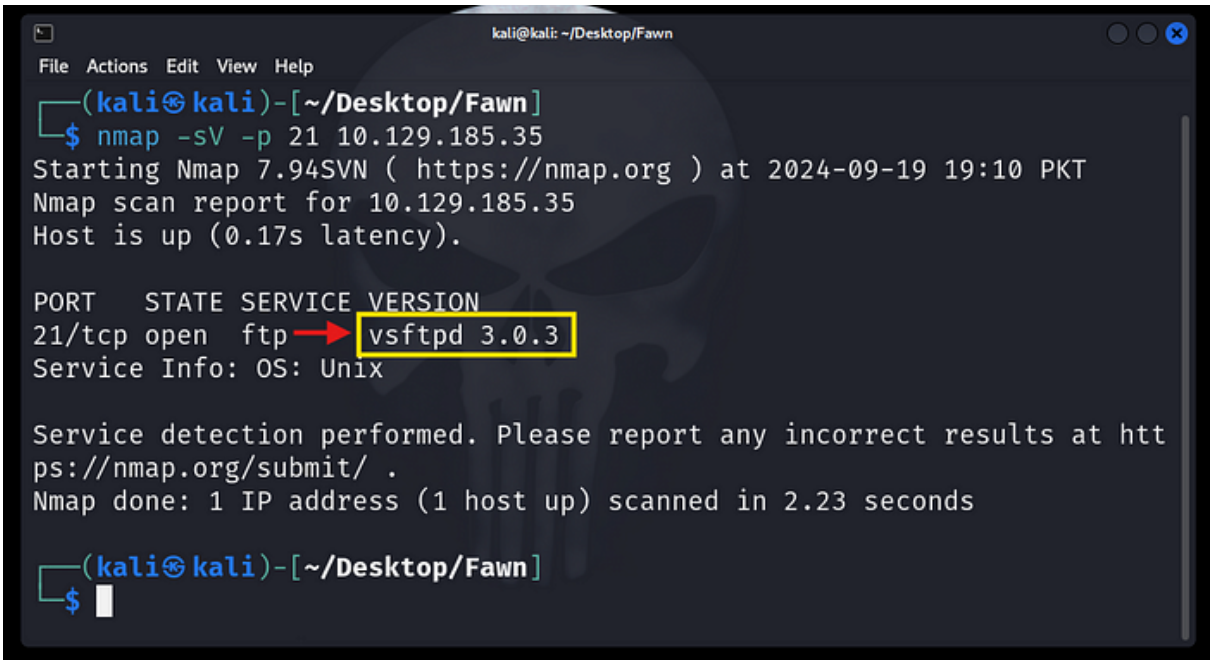
The answer is: ***vsftpd 3.0.3***

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.

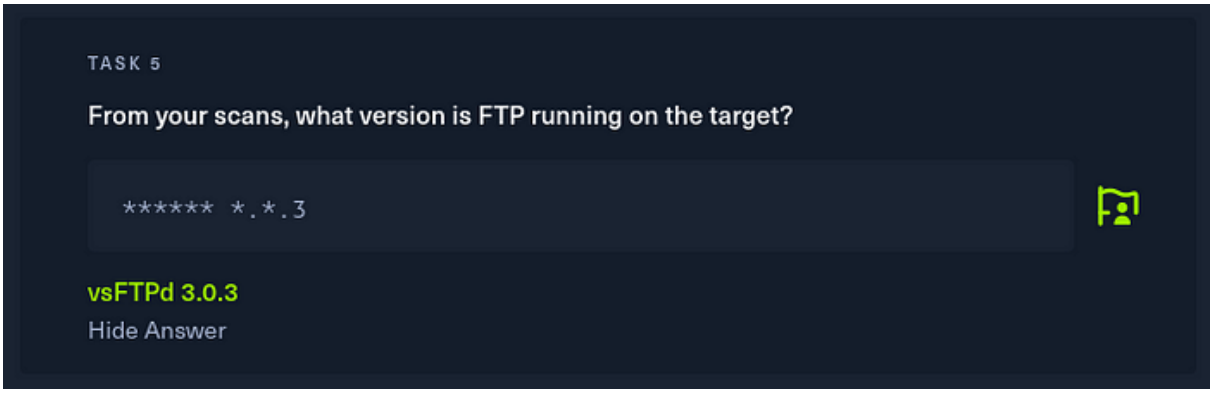


The answer to task 5 is ***vsftpd 3.0.3.***

Command Explanation:

Now let's understand the above command breifly 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 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 htt
ps://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

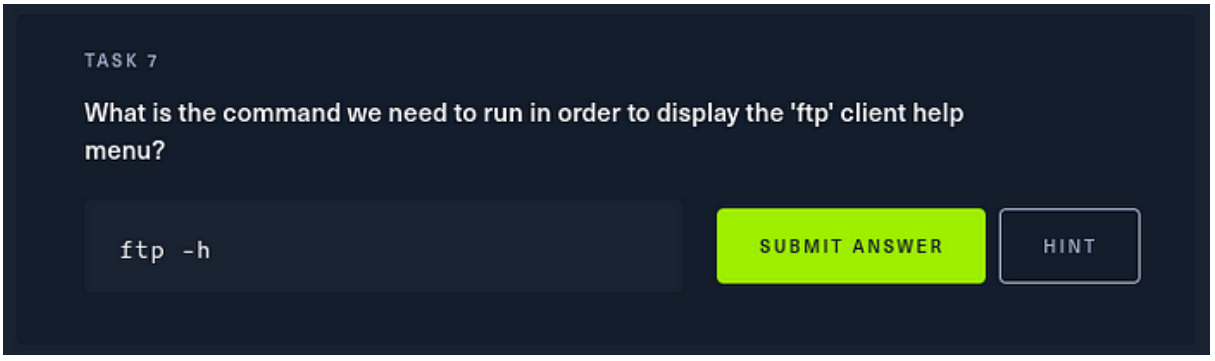
HINT

Task No 07:

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

Answer:

ftp -h

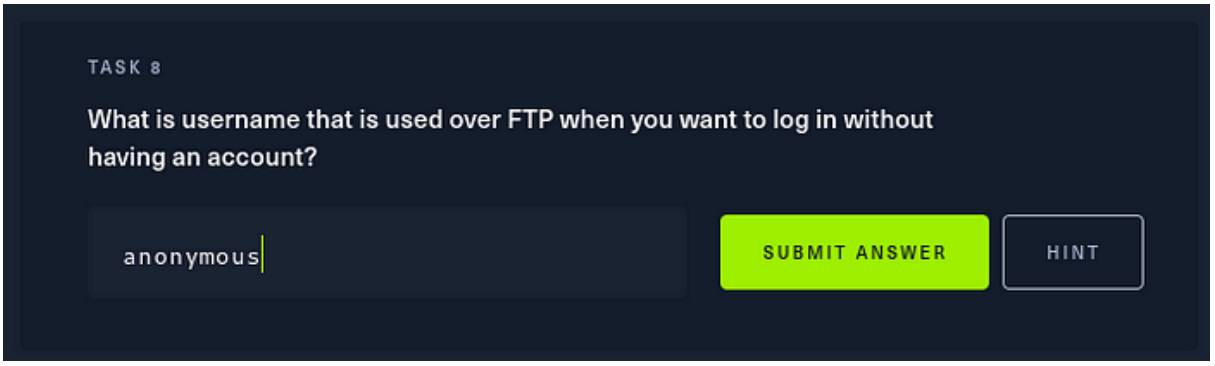


Task No 08:

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

Answer:

anonymous

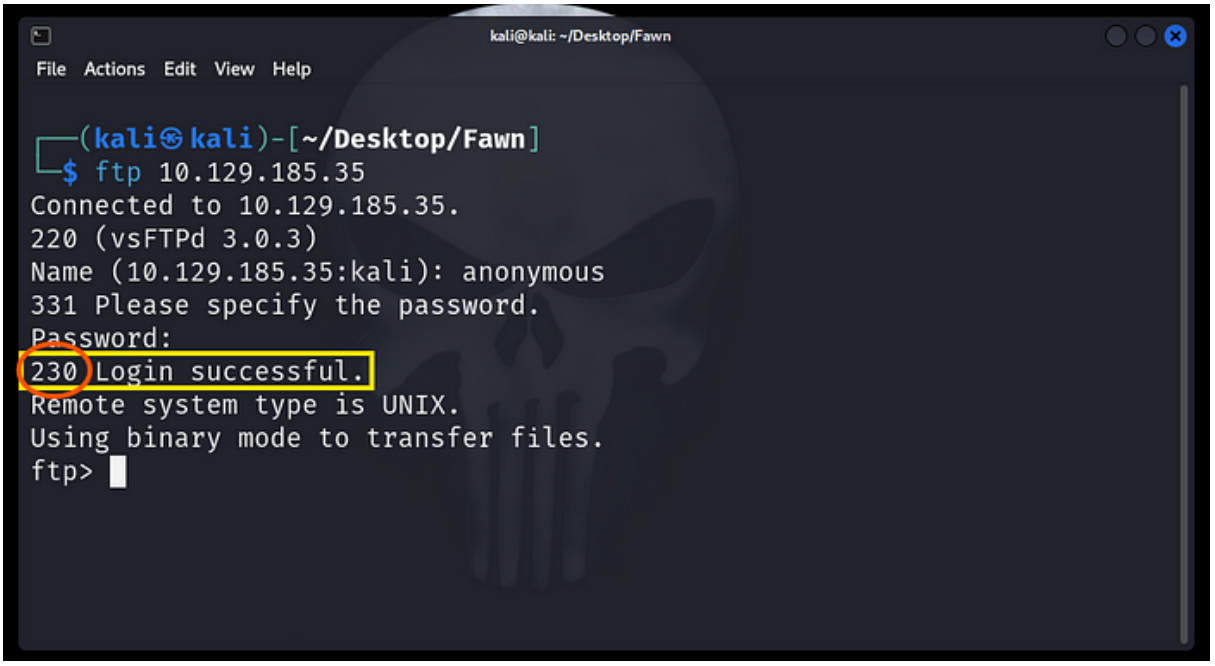


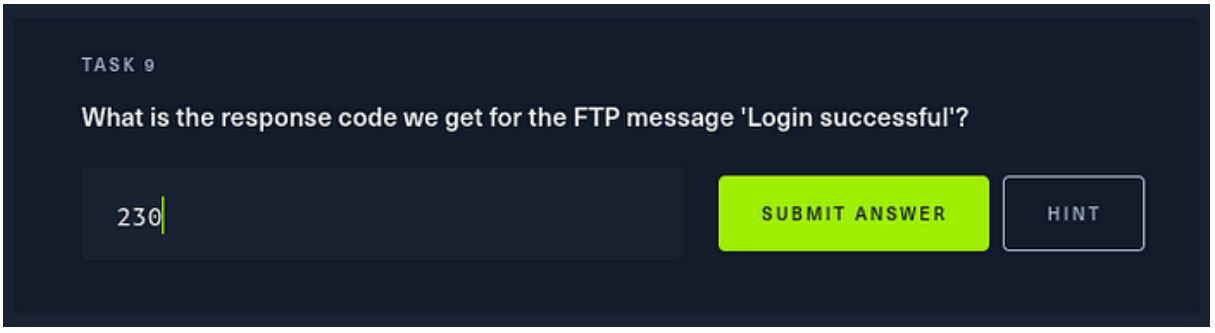
Task No 09:

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

Answer:

230



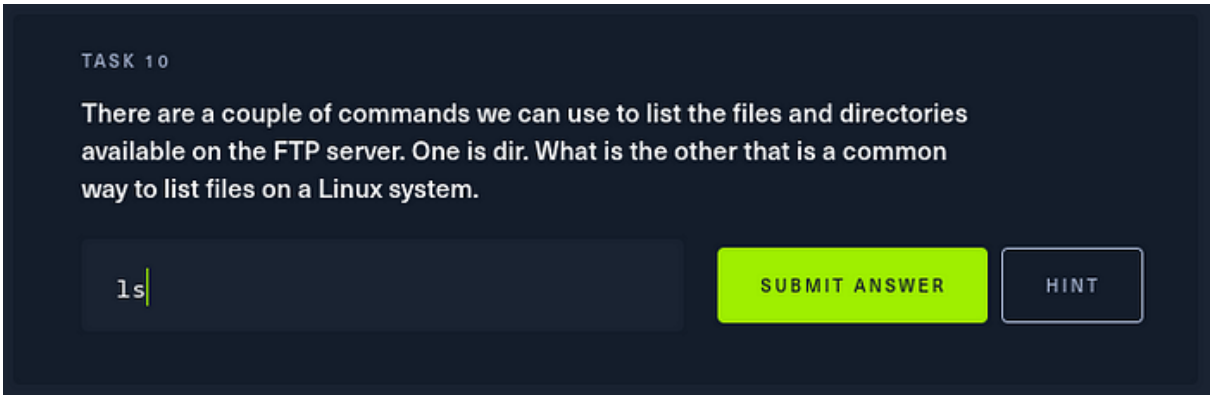


Task No 10:

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

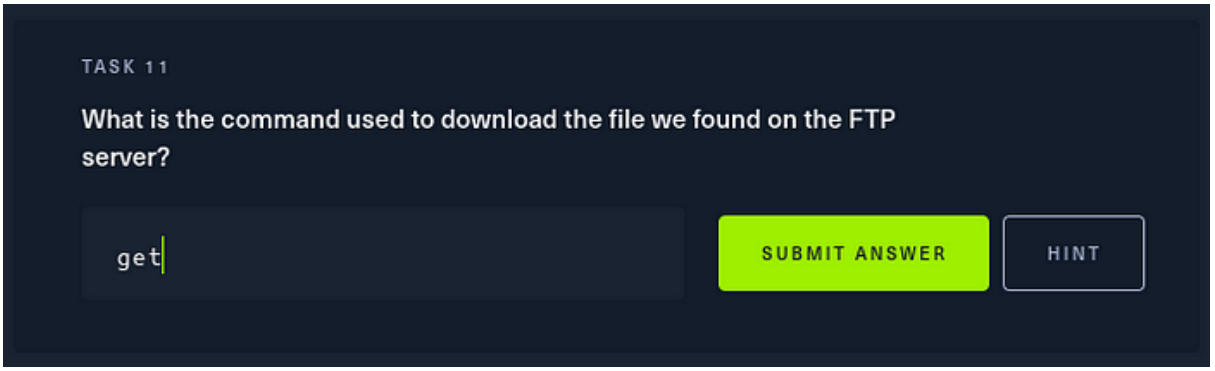


Task No 11:

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

Answer:

get



Task No 12:

Submit root flag

Answer:

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

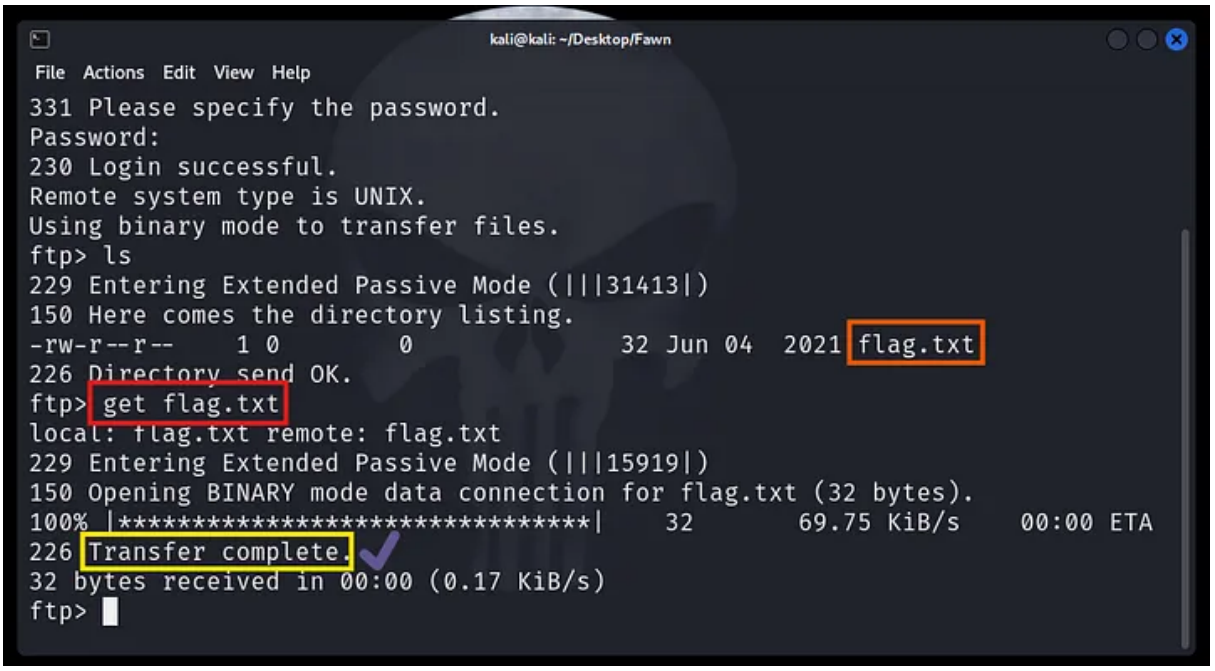
How To Get The Root Flag:

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
```

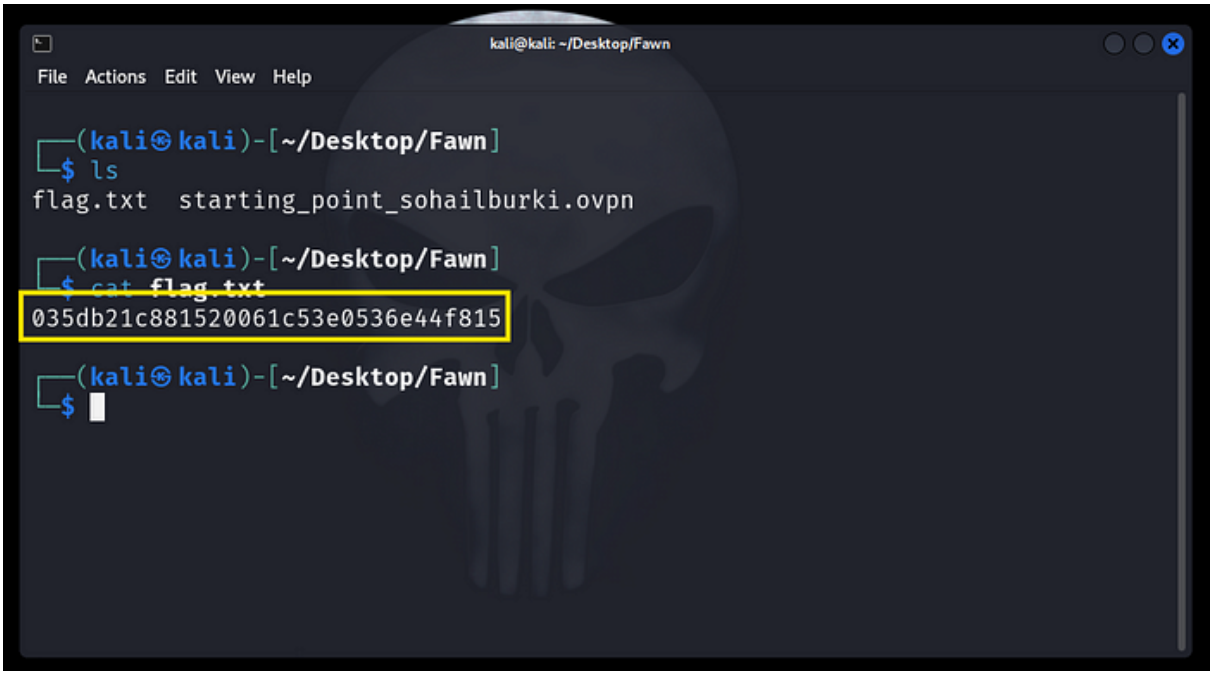
After entering the above 👆 command you will be prompted to enter a username and we know that when we try to enter an FTP port without having an account the username will be ***anonymous***. So enter anonymous as your user and the password is ***anon123***.

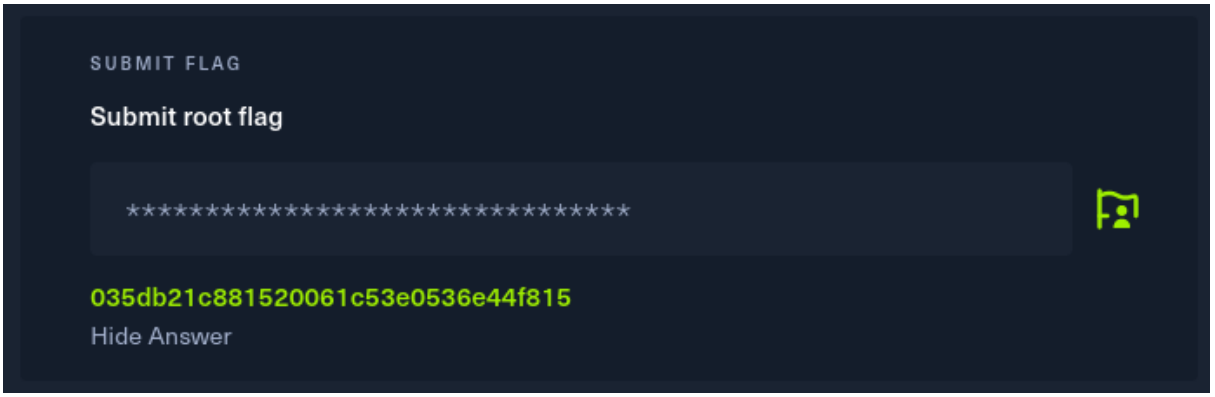


Once you're logged in, now list down the files and folders in the current directory using ls command. You will see a text file named flag. Now download this file to your local system using the following command.

```
get flag.txt
```

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





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