

# Fawn

So this is my second machine, I'll provide all the Q/A as images in the file.

openvpn 10.129.13.195 - with sudo to connect to it.

## 10.129.13.195

### Q/A SECTION:

#### TASK 1

What does the 3-letter acronym FTP stand for?

File Transfer Protocol

SUBMIT ANSWER

HINT

#### TASK 2

Which port does the FTP service listen on usually?

21

SUBMIT ANSWER

HINT

FTPS (also known as FTP-SSL and FTP Secure) is an extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and, formerly, the Secure Sockets Layer (SSL, which is now prohibited by RFC7568) cryptographic protocols.

### THE ANSWER FOR THE NEXT QUESTION IS SFTP

#### TASK 3

What acronym is used for the secure version of FTP?

\*\*\*p



Show Answer

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 5

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

vsftpd 3.0.3

SUBMIT ANSWER

HINT

TASK 6

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

Unix

SUBMIT ANSWER

HINT

ANSWER:

**ftp-h**

TASK 7

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

\*\*\* -h



Show Answer

8. Using an FTP program or the FTP command interface, the user enters **"anonymous"** as a user ID. Usually, the password is defaulted or furnished by the FTP server. Anonymous FTP is a common way to get access to a server in order to view or download files that are publicly available.

TASK 8

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

SUBMIT ANSWER

HINT

9. The server sends a **230** code in response to a command that has provided sufficient credentials to the server to grant the user access to the FTP server.

TASK 9

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

SUBMIT ANSWER

HINT

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 ANSWER

HINT

## TASK 11

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

SUBMIT ANSWERHINT

## SUBMIT FLAG

Submit root flag

SUBMIT FLAG

# SCANNING SECTION

## NMAP COMMANDS:

```
(root@kali) - [/home/scarly]
# nmap -sV 10.129.13.195 -P
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-15 20:39 CST
Nmap scan report for 10.129.13.195
Host is up (0.38s latency).
Not shown: 999 closed tcp ports (reset)
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 2.99 seconds
```

Here we were able to see what version is FTP running on the target  
on 21/tcp open ftp vsftpd 3.0.3

OS: Unix

# CTF

```
(root@kali) - [/home/scarly]
# ftp 10.129.13.195
Connected to 10.129.13.195.
220 (vsFTPd 3.0.3)
Name (10.129.13.195:scarly): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -a
229 Entering Extended Passive Mode (|||33844|)
150 Here comes the directory listing.
drwxr-xr-x    2 0          121          4096 Jun 04  2021 .
drwxr-xr-x    2 0          121          4096 Jun 04  2021 ..
-rw-r--r--    1 0           0           32 Jun 04  2021 flag.txt
226 Directory send OK.
ftp> ls
229 Entering Extended Passive Mode (|||28639|)
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 (|||61480|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |*****| 32 26.77 KiB/s
226 Transfer complete.
32 bytes received in 00:00 (0.15 KiB/s)
ftp> exit
```

```
(root@kali) - [/home/scarly]
# ls
Descargas Escritorio Imágenes Plantillas Vídeos
Documentos flag.txt Música Público
# cat flag.txt
035db21c881520061c53e0536e44f815
```