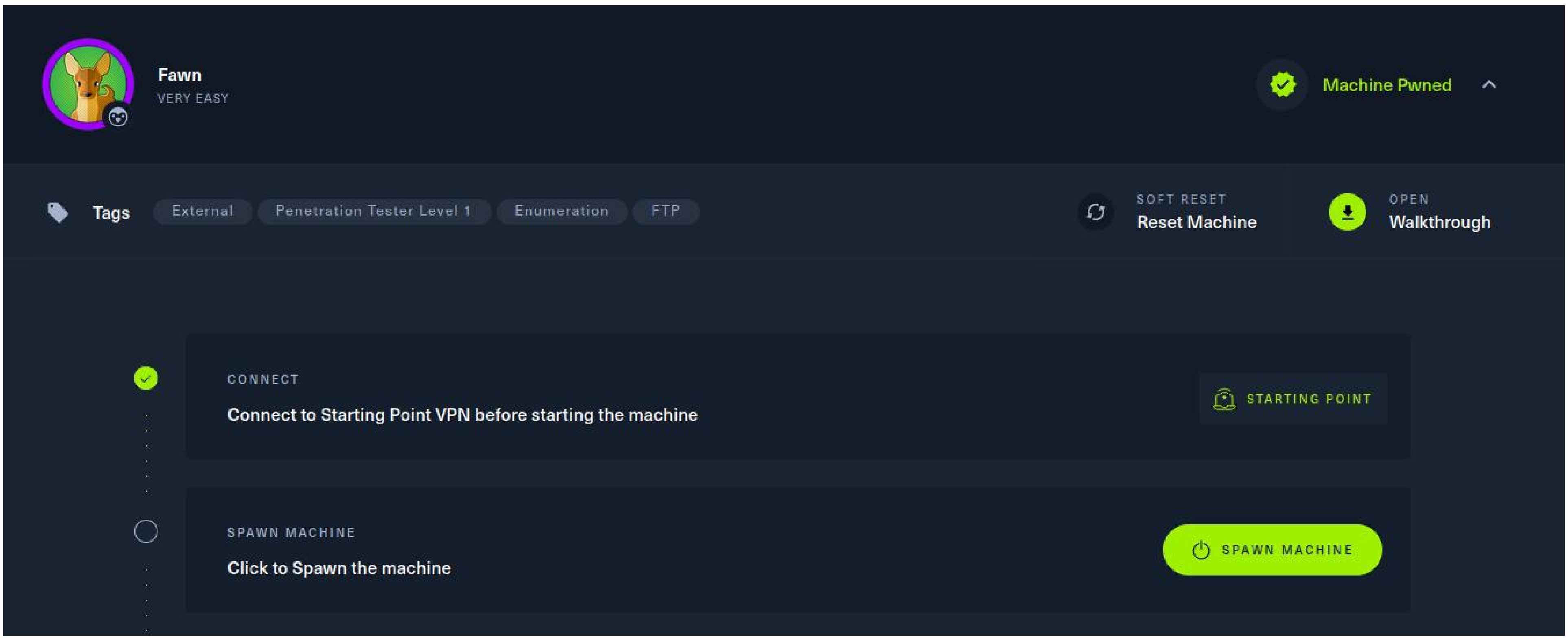
FAWN

- ✓ This writeup is a direct walkthrough to the flag. Hoping that you have given your best before referring this writeup.
- ✓ Assuming that you have using pwnbox or connected to **OPENVPN.** If not, do refer to vpn-connection file.



Fawn
VERY EASY

Machine Pwned

Tags: External, Penetration Tester Level 1, Enumeration, FTP

SOFT RESET
Reset Machine

OPEN
Walkthrough

CONNECT
Connect to Starting Point VPN before starting the machine

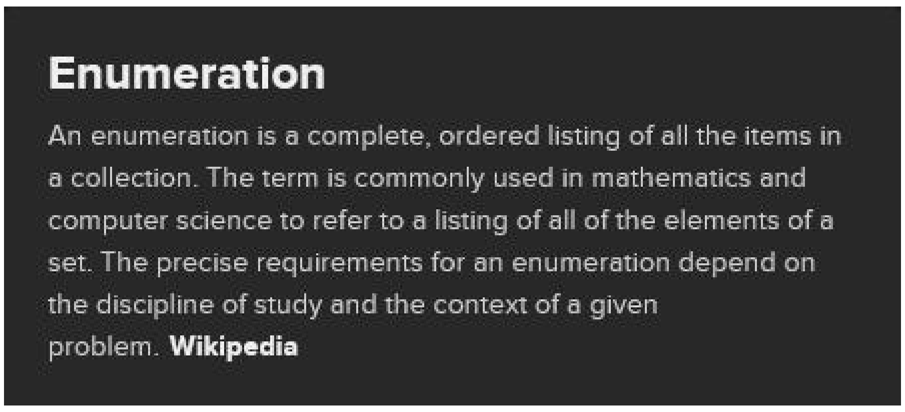
STARTING POINT

SPAWN MACHINE
Click to Spawn the machine

SPAWN MACHINE

- **Once the is spawned, machine ip will be given.**

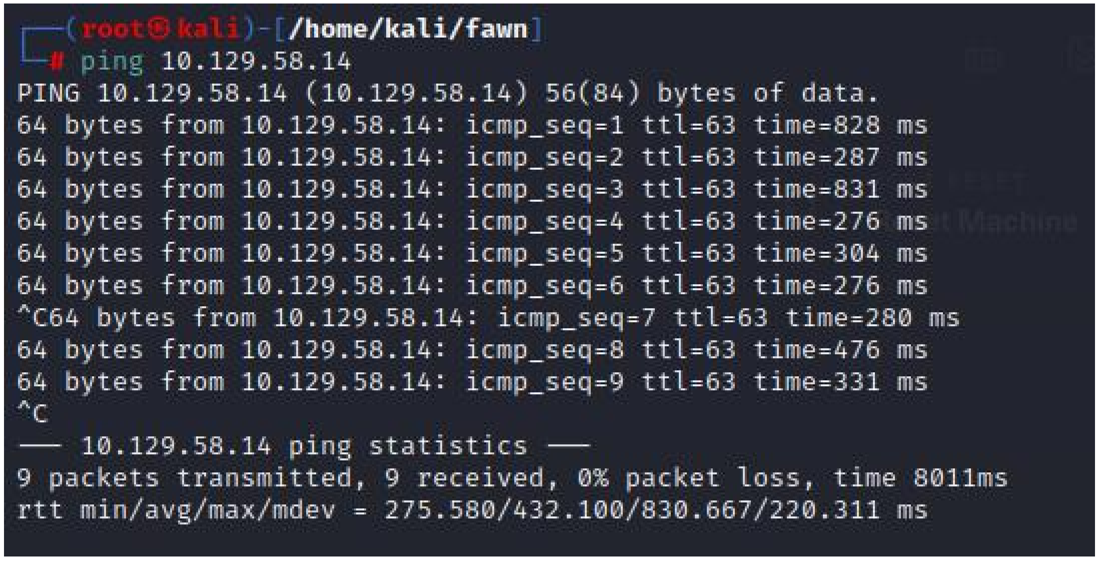
ENUMERATION:



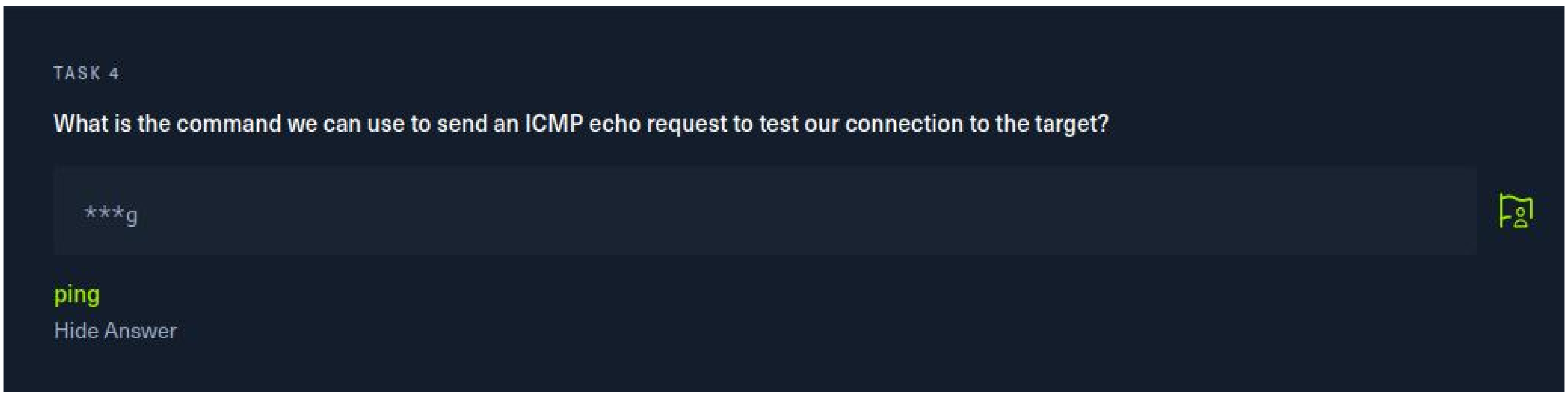
Enumeration

An enumeration is a complete, ordered listing of all the items in a collection. The term is commonly used in mathematics and computer science to refer to a listing of all of the elements of a set. The precise requirements for an enumeration depend on the discipline of study and the context of a given problem. **Wikipedia**

- Initially we could check IP (is this host up or not) by using a command : **ping <ip>**



```
┌──(root㉿kali)-[/home/kali/fawn]
└─# ping 10.129.58.14
PING 10.129.58.14 (10.129.58.14) 56(84) bytes of data.
64 bytes from 10.129.58.14: icmp_seq=1 ttl=63 time=828 ms
64 bytes from 10.129.58.14: icmp_seq=2 ttl=63 time=287 ms
64 bytes from 10.129.58.14: icmp_seq=3 ttl=63 time=831 ms
64 bytes from 10.129.58.14: icmp_seq=4 ttl=63 time=276 ms
64 bytes from 10.129.58.14: icmp_seq=5 ttl=63 time=304 ms
64 bytes from 10.129.58.14: icmp_seq=6 ttl=63 time=276 ms
^C64 bytes from 10.129.58.14: icmp_seq=7 ttl=63 time=280 ms
64 bytes from 10.129.58.14: icmp_seq=8 ttl=63 time=476 ms
64 bytes from 10.129.58.14: icmp_seq=9 ttl=63 time=331 ms
^C
── 10.129.58.14 ping statistics ──
9 packets transmitted, 9 received, 0% packet loss, time 8011ms
rtt min/avg/max/mdev = 275.580/432.100/830.667/220.311 ms
```



TASK 4

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

***g

ping

Hide Answer

- For enumeration we use tool called **nmap** which comes by default in kali-Linux .
- Open a new terminal type the following command to perform nmap scan:

  # **nmap -sVC -v -T4 <ip>**

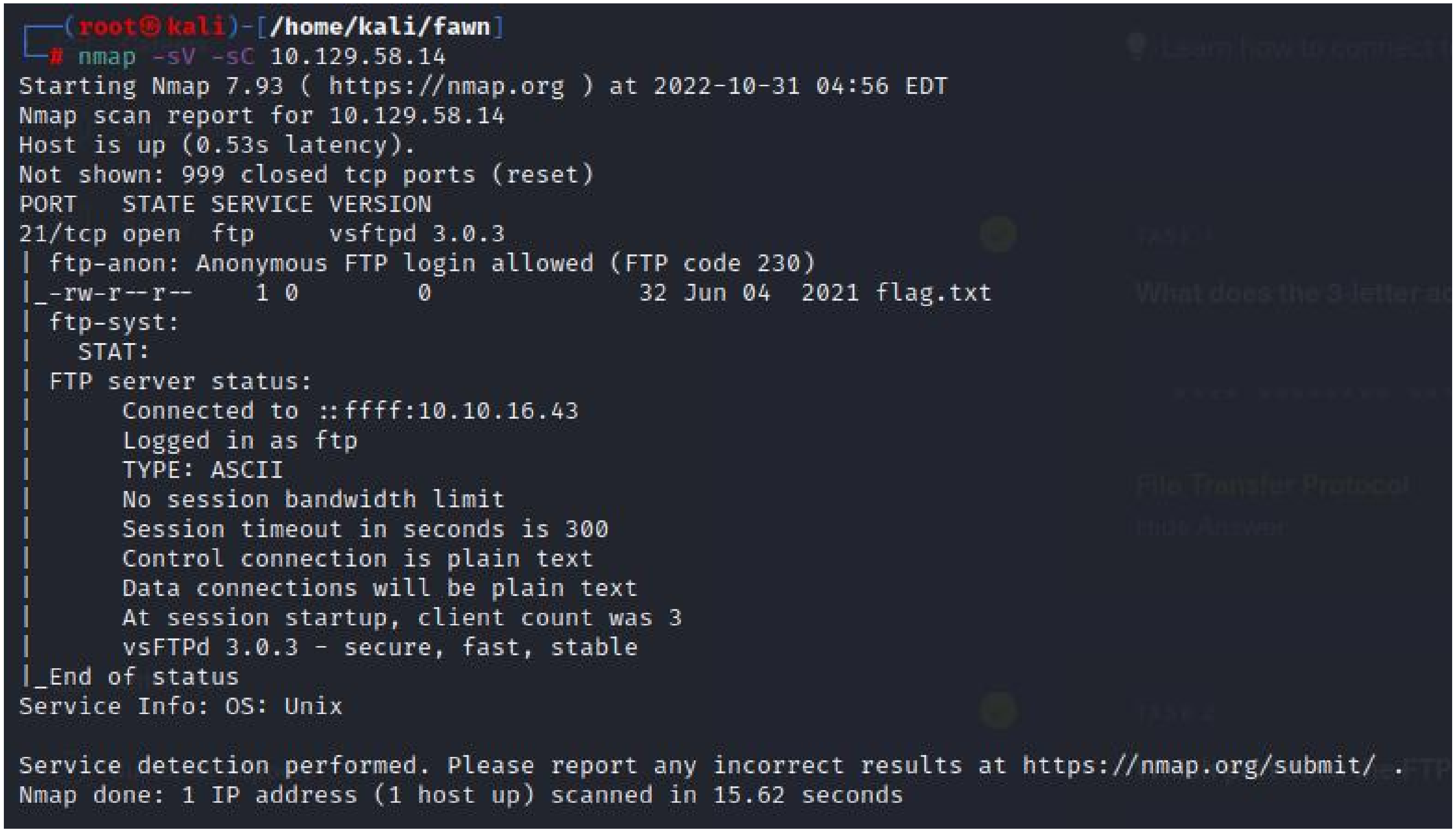
  -sVC : combination of -sV & -sC, used scan version of the open ports & perform basic scripts on open port (-sC is illegal to use on public ip)

  -v : used to make output more verbose and readable.

  -T4: used for decent balance of speed and info.

  <ip> : ip address of spawned machine.

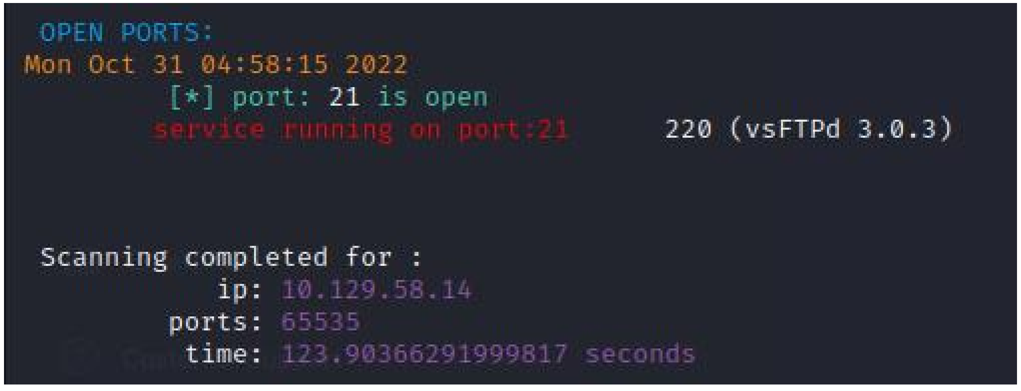
  Try cmd: **nmap --help** for more info about the tool



```
┌──(root㉿kali)-[/home/kali/fawn]
└─# nmap -sV -sC 10.129.58.14
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-31 04:56 EDT
Nmap scan report for 10.129.58.14
Host is up (0.53s 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:10.10.16.43
|      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 3
|      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 15.62 seconds
```

- *I usually perform one more scan using my **personal tool: portscanner** before analysing the nmap report.*



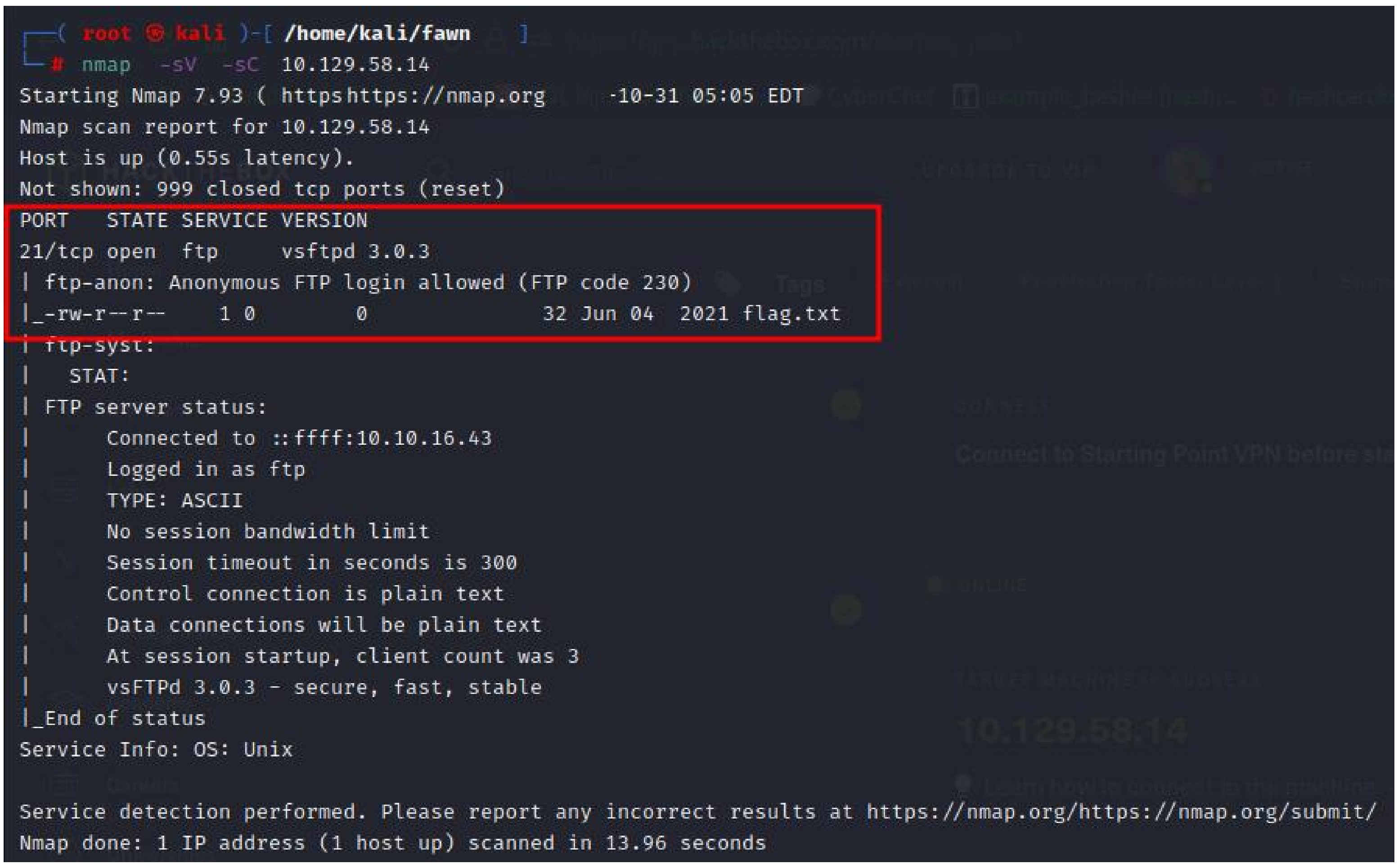
```
 OPEN PORTS:
Mon Oct 31 04:58:15 2022
         [*] port: 21 is open
        service running on port:21      220 (vsFTPd 3.0.3)



 Scanning completed for :
           ip: 10.129.58.14
        ports: 65535
         time: 123.90366291999817 seconds
```

~ I prefer this tool because of its speed as you can see it just took 123 seconds for scanning 65535 ports. Even still some improvements to be done

ANALYSING BOTH SCANS :

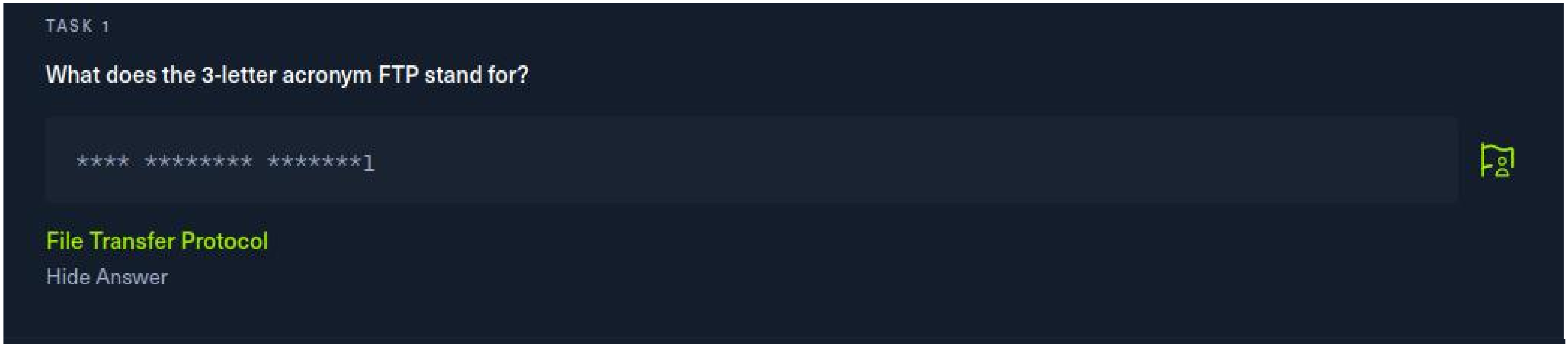


```
┌──( root ㉿ kali )-[ /home/kali/fawn  ]
└─# nmap  -sV  -sC  10.129.58.14
Starting Nmap 7.93 ( httpshttps://nmap.org     -10-31 05:05 EDT
Nmap scan report for 10.129.58.14
Host is up (0.55s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| 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:10.10.16.43
|      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 3
|      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/https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 13.96 seconds
```

~ By analysing this nmap scan most part of the lab will solved.

Operating System: **Unux**
Number of open ports : **1**
Port Number : **21**
Service Running : **ftp**
Version : **vsftpd 3.0.3**



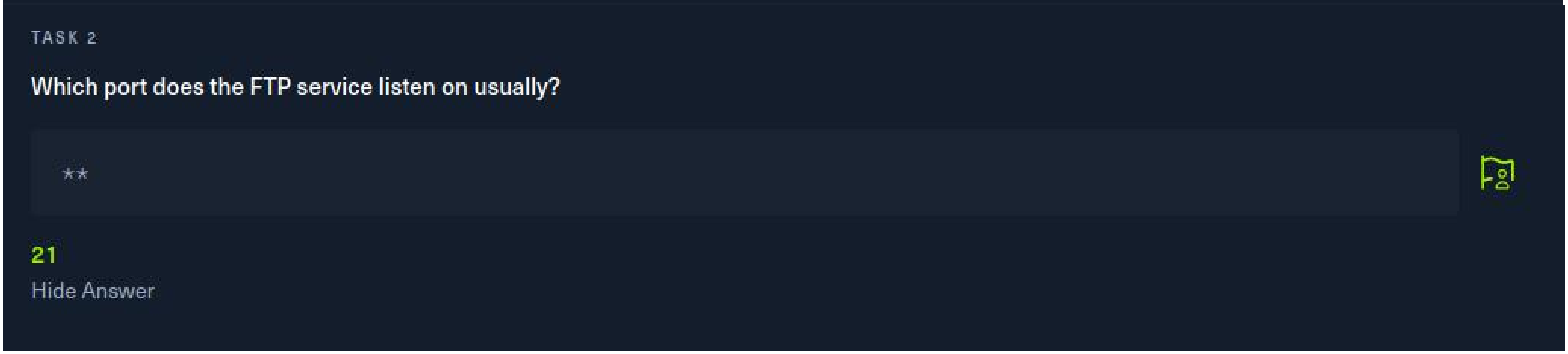
TASK 1

What does the 3-letter acronym FTP stand for?

```
**** ******** *******l
```

File Transfer Protocol

Hide Answer



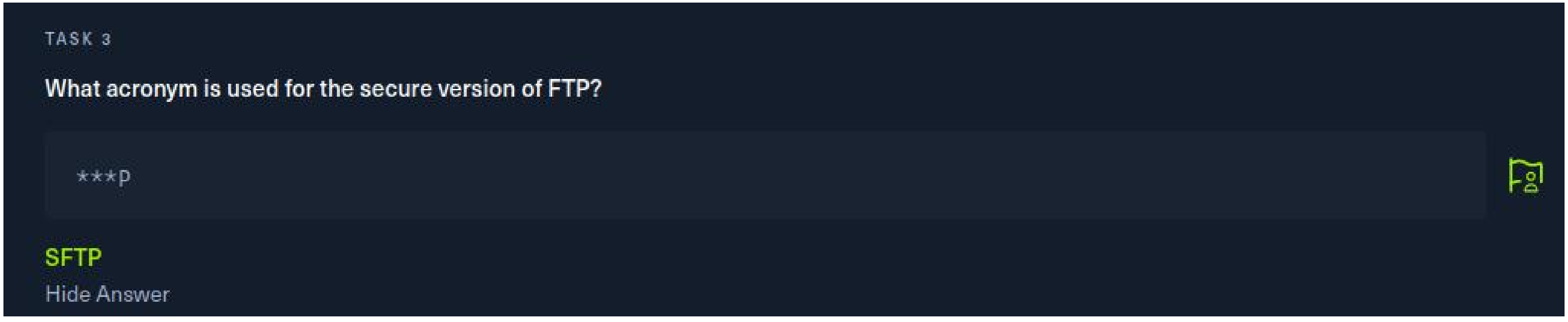
TASK 2

Which port does the FTP service listen on usually?

```
**
```

21

Hide Answer



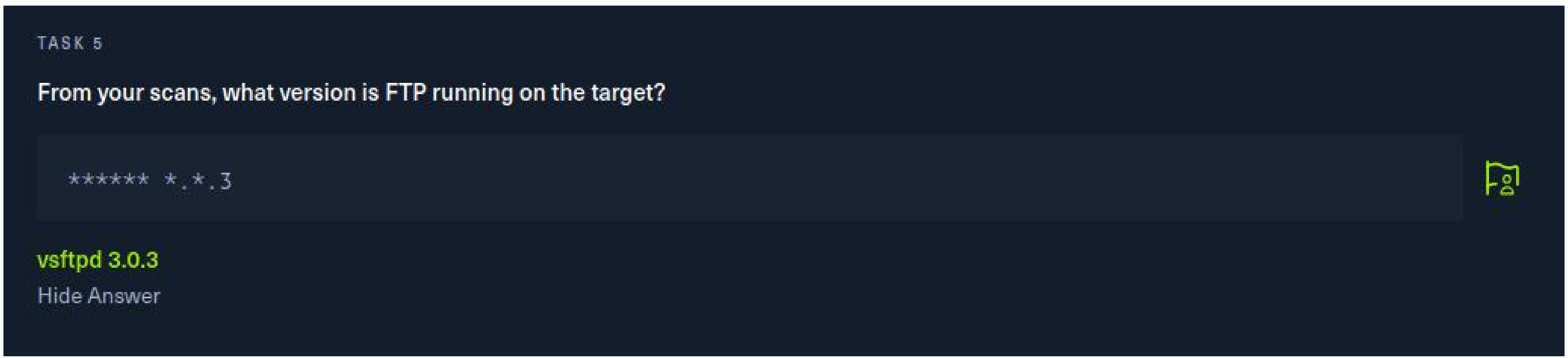
TASK 3

What acronym is used for the secure version of FTP?

```
***p
```

SFTP

Hide Answer



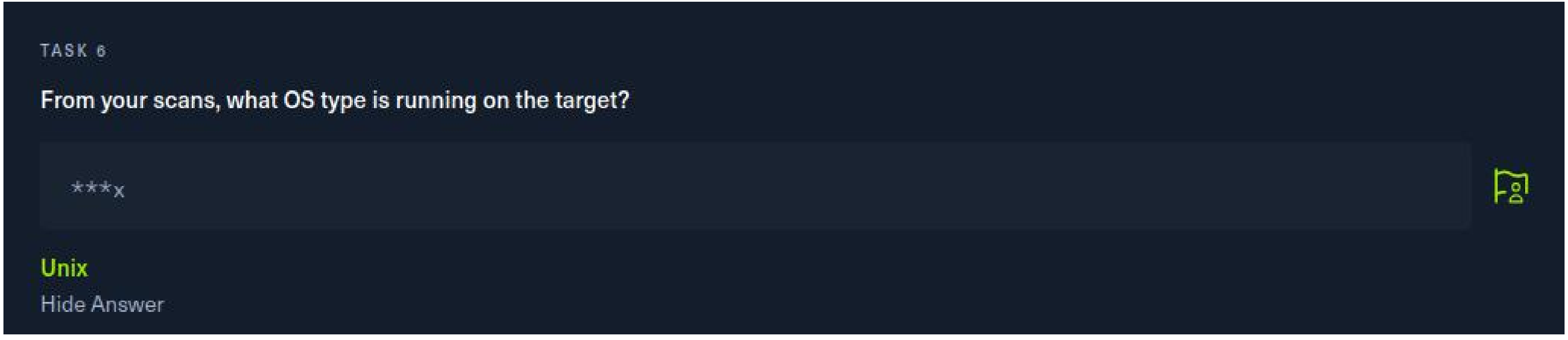
TASK 5

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

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

vsftpd 3.0.3

Hide Answer



TASK 6

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

```
***x
```

Unix

Hide Answer

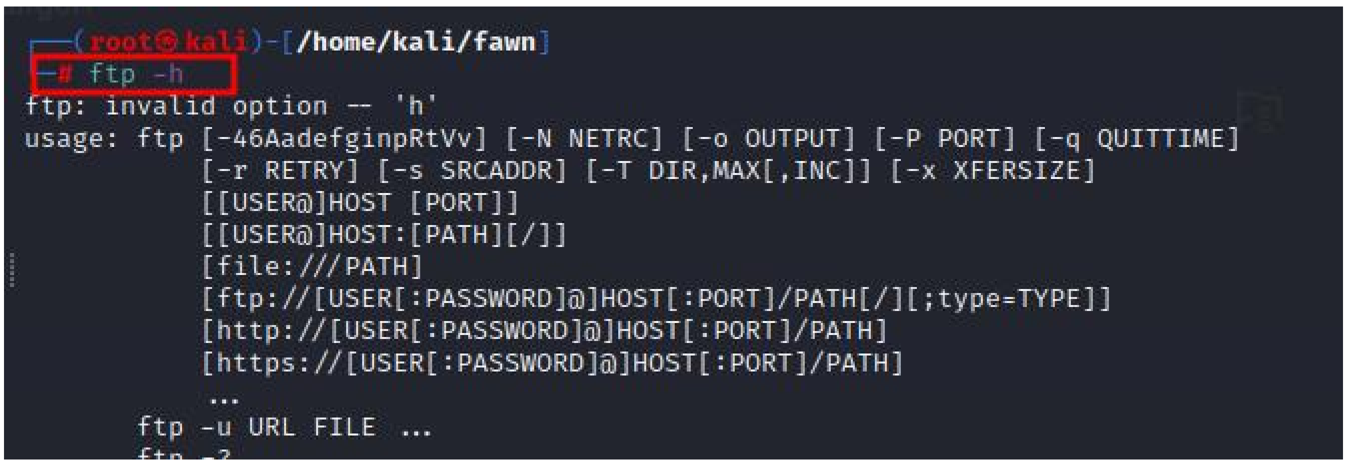
~ we have answered all these tasks by analysing the nmap scan above.

FOOTHOLD

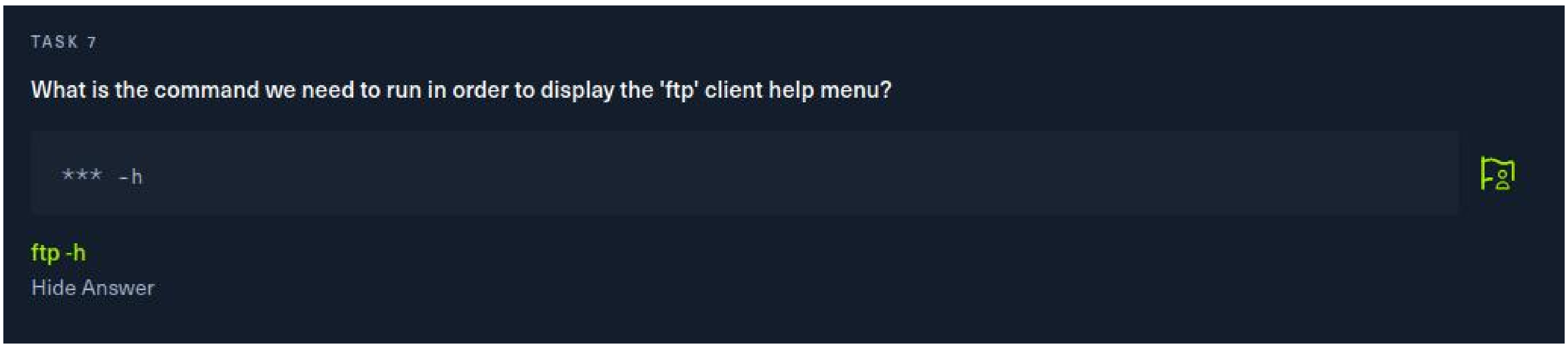
- The **FTP SERVICE** is running open on **port 21.**
- This ftp service Anonymous FTP login allowed

~ (*that means we can login to ftp server of this machine using the username: Anonymous and no password required*)

- For knowing further about this ftp tool we can use the **command: ftp - h** for tool usage and arguments required.



```
┌──(root㉿kali)-[/home/kali/fawn]
└─# ftp -h
ftp: invalid option -- 'h'
usage: ftp [-46AadefginpRtVv] [-N NETRC] [-o OUTPUT] [-P PORT] [-q QUITTIME]
           [-r RETRY] [-s SRCADDR] [-T DIR,MAX[,INC]] [-x XFERSIZE]
           [[USER@]HOST [PORT]]
           [[USER@]HOST:[PATH][/]]
           [file:///PATH]
           [ftp://[USER[:PASSWORD]@]HOST[:PORT]/PATH[/][;type=TYPE]]
           [http://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
           [https://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
           ...
       ftp -u URL FILE ...
```



TASK 7

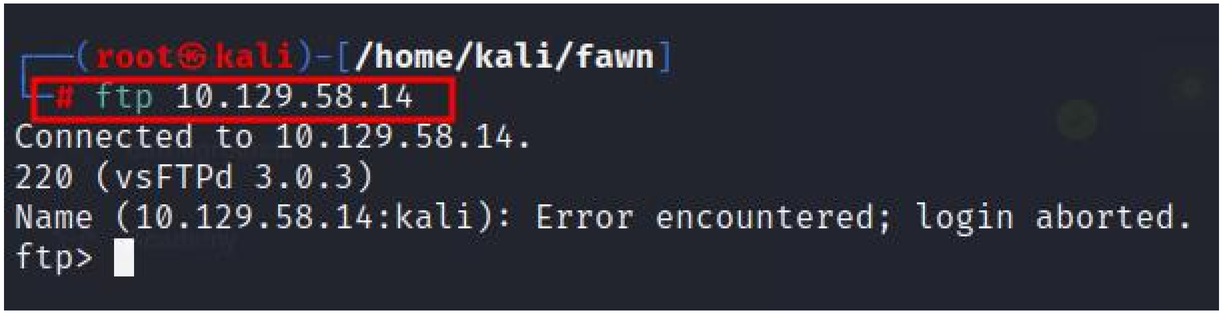
What is the command we need to run in order to display the 'ftp' client help menu?

*** -h

ftp -h

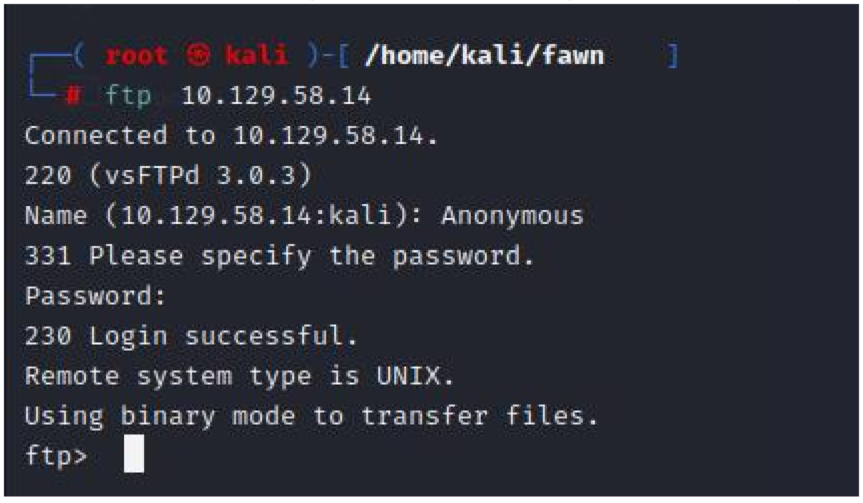
- ➢ Now we could try to connect with FTP using IP address and default credentials.
- ➢ Command for connecting FTP :

  # **ftp <ip>**

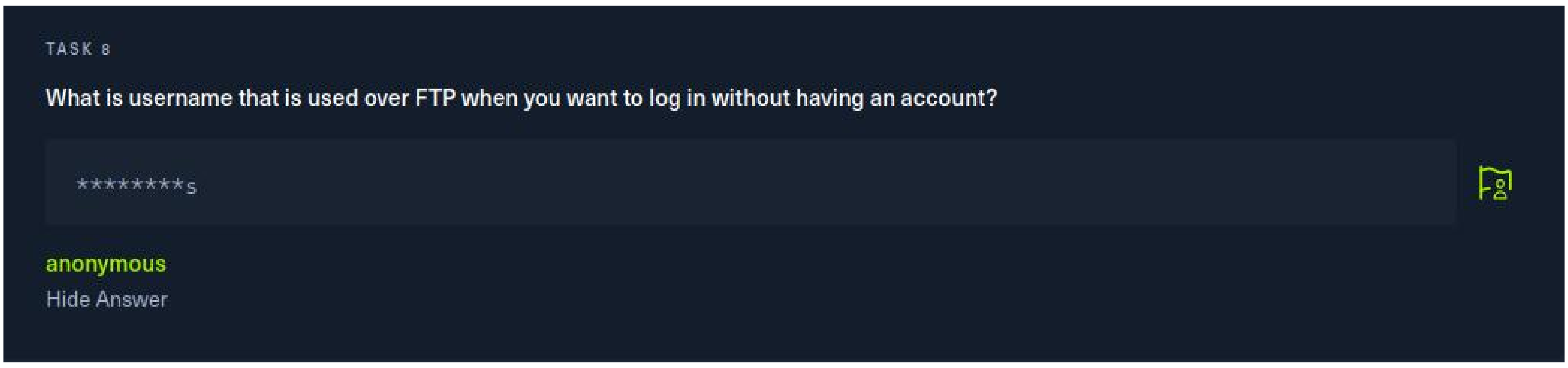


```
┌──(root㉿kali)-[/home/kali/fawn]
└─# ftp 10.129.58.14
Connected to 10.129.58.14.
220 (vsFTPd 3.0.3)
Name (10.129.58.14:kali): Error encountered; login aborted.
ftp> █
```

- ➢ As we have analyzed for nmap scan that this ftp service has **Anonymous login allowed**. So we will enter the **username: Anonymous and no password required** (just skip the password).



```
┌──( root ㉿ kali )-[ /home/kali/fawn    ]
└─# ftp  10.129.58.14
Connected to 10.129.58.14.
220 (vsFTPd 3.0.3)
Name (10.129.58.14:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```



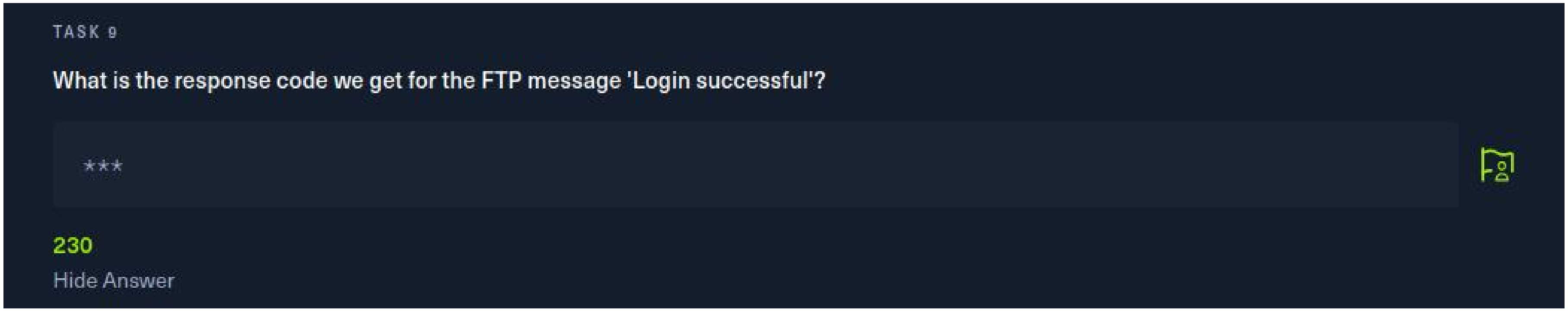
TASK 8

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

********s

anonymous

- ➢ The login was successful as we can see the code **230**.



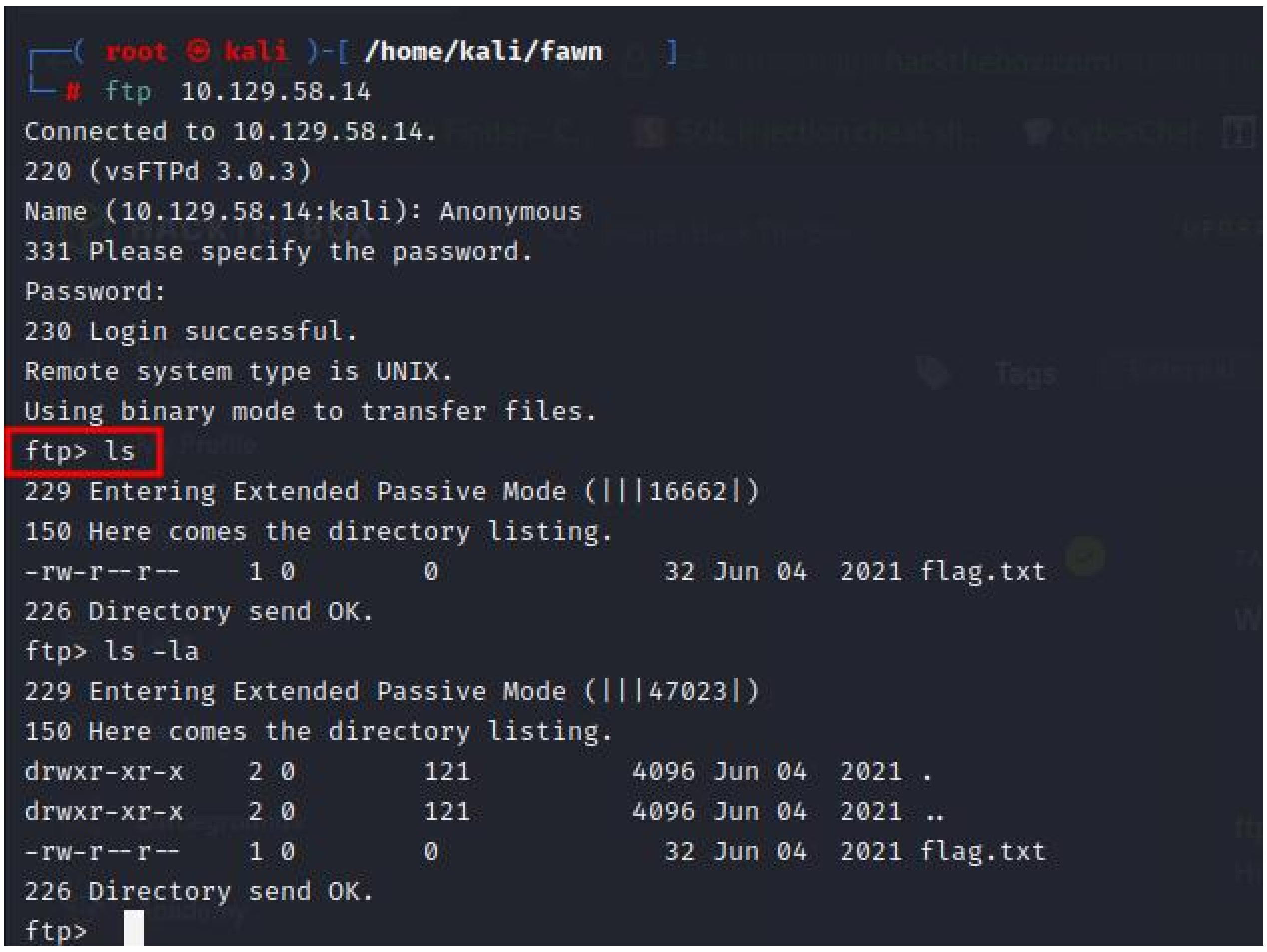
TASK 9

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

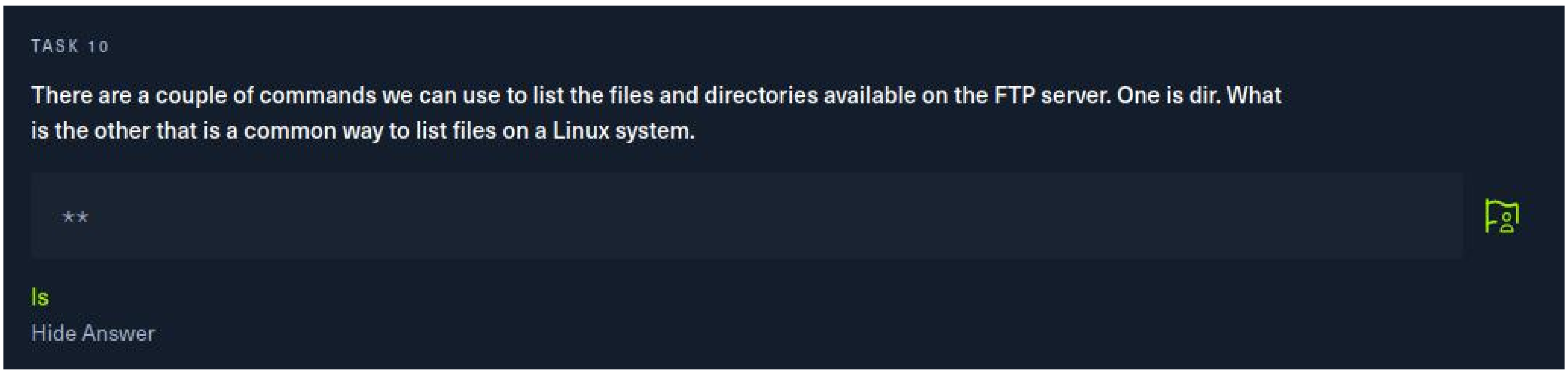
***

230

- Now we have to check what are the files and directories present on this service.
- For this we use a **command: ls**
- It is recommended to use the **command: ls -la** for long listing and hidden files. But for now we use the command: ls.



```
┌──(root㉿kali)-[/home/kali/fawn]
└─# ftp 10.129.58.14
Connected to 10.129.58.14.
220 (vsFTPd 3.0.3)
Name (10.129.58.14: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 (|||16662|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||47023|)
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>
```



TASK 10

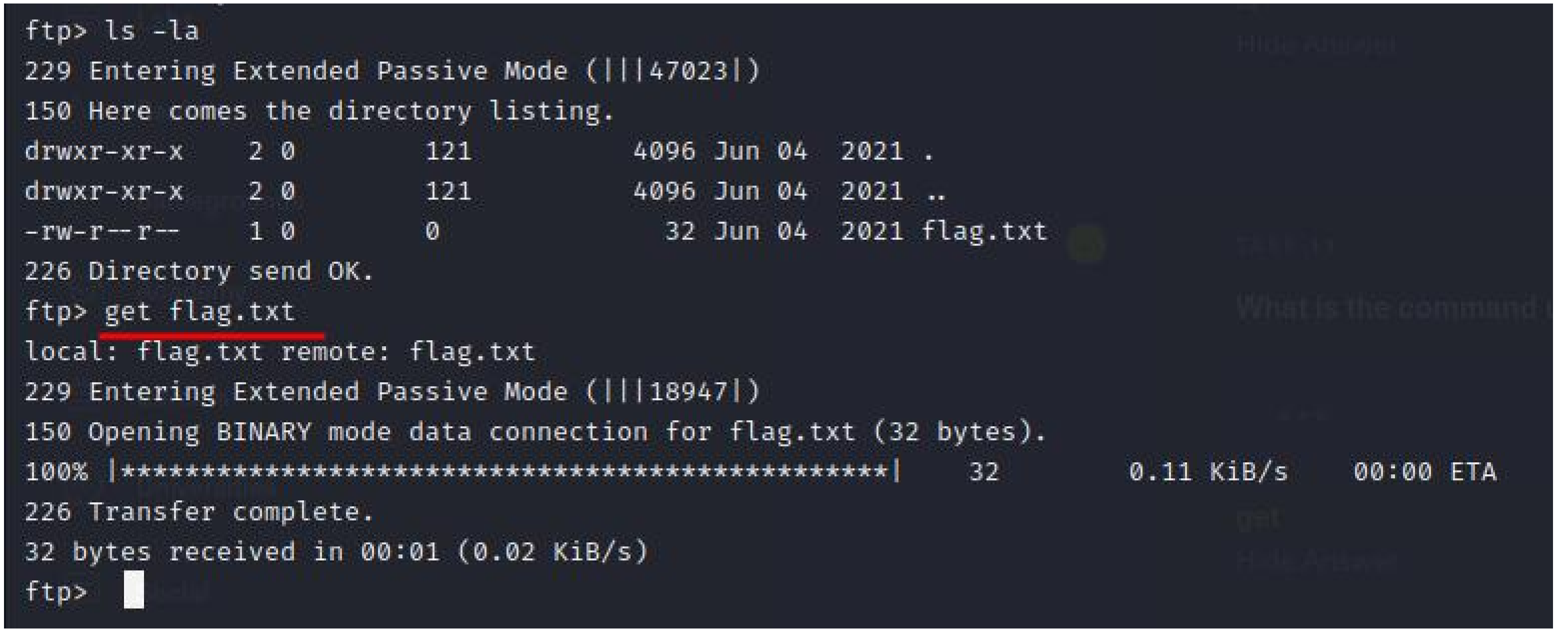
There are a couple of commands we can use to list the files and directories available on the FTP server. One is dir. What is the other that is a common way to list files on a Linux system.

**

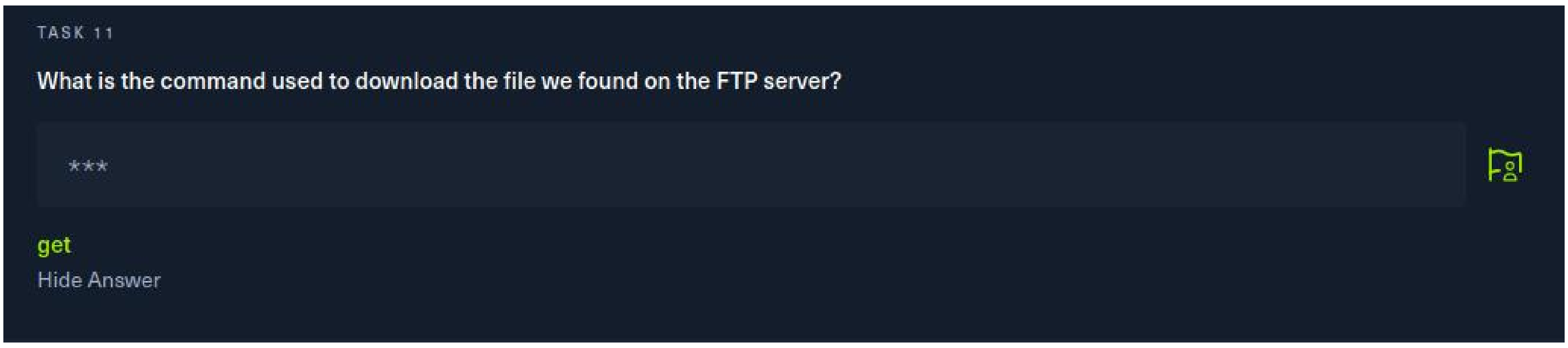
ls

Hide Answer

- We can also observe that there is a text file called **flag.txt** here.
- For getting that file (flag.txt) into our local system we a tool called get.
- **Command : get < file name >**



```
ftp> ls -la
229 Entering Extended Passive Mode (|||47023|)
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> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||18947|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |***************************************************|    32        0.11 KiB/s    00:00 ETA
226 Transfer complete.
32 bytes received in 00:01 (0.02 KiB/s)
ftp>
```



TASK 11

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

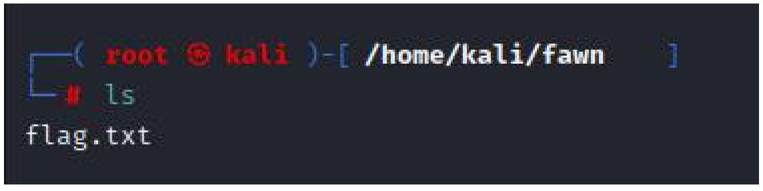
***

get

Hide Answer

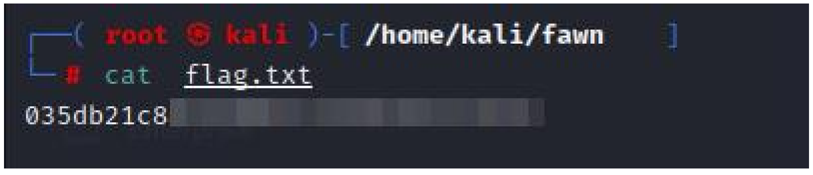
- Now the flag.txt will be on our local file system, So here we could open a new terminal or terminate the ftp connection as we have already captured the flag.

- On our local file system go to the same directory where the ftp login is performed.
- Once again use the **command: ls** for listing the files and directories on the system.



```
┌──( root ㉿ kali )-[ /home/kali/fawn    ]
└─# ls
flag.txt
```

- For viewing the content in the file we use the command: **cat < file name >**



```
┌──( root ㉿ kali )-[ /home/kali/fawn    ]
└─# cat  flag.txt
035db21c8[redacted]
```

✓ Here we have **successfully captured the flag** and do not forget to submit the flag on website for completion of lab.