

HTB 0x01

发表于 2021-01-09 分类于 [Challenge](#), [2020](#), [CSICTF](#), [Linux](#)
[Challenge](#) | [2020](#) | [CSICTF](#) | [Linux](#) | [HTB 0x01](#)

[点击此处](#)获得更好的阅读体验

WriteUp来源

<https://dunsp4rce.github.io/csictf-2020/linux/2020/07/22/HTB-0x01.html>

by vishalananth

题目描述

I forgot my 'flag.txt' file on the server...

题目考点

解题思路

I ran a detailed nmap scan on the given IP using:

```
1 nmap -vvv -Pn -A 34.93.37.238
2 5001/tcp open  ftp                syn-ack      vsftpd 3.0.3
3 | ftp-anon: Anonymous FTP login allowed (FTP code 230)
4 |_Can't get directory listing: PASV IP 10.160.0.2 is not the same as 34.93.37.238
5 | ftp-syst:
6 |   STAT:
7 | FTP server status:
8 |     Connected to ::ffff:49.207.139.203
9 |     Logged in as ftp
10 |    TYPE: ASCII
11 |    No session bandwidth limit
12 |    Session timeout in seconds is 300
13 |    Control connection is plain text
14 |    Data connections will be plain text
15 |    At session startup, client count was 4
16 |    vsFTPD 3.0.3 - secure, fast, stable
17 |_End of status
```

There is an open TCP port - 5001 which accepts FTP connections. So I tried to open a FTP connection using:

```
1 ftp 34.93.37.238 5001
```

But somehow I was not able to run any command as it was not able to enter passive mode. So I downloaded ncftp FTP client and ran

```
1 ncftp -P 5001 34.93.37.238
```

It worked and I was able to get the flag using

```
1 cat pub/flag.txt
```

Flag

```
1 csictf{4n0nym0u5_ftp_l0g1n}
```

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge/2020/CSICTF/Linux/v21r4Tq9T7Z6xwu4ukvhTM.html>
- 版权声明: 本博客所有文章除特别声明外, 均采用 [BY-NC-SA](#) 许可协议。转载请注明出处!

[#Challenge #2020 #Linux #CSICTF](#)
[HTB 0x\[2-6\]](#)
[AKA](#)