

Machine Details

- Target Machine IP Address: 10.129.1.14
-

Enumeration

Nmap scan

I'm starting off with an Nmap scan. This should point us in the right direction.

Terminal:

```
(adhd@kali)-[~/Desktop/HTB/Notes/Starting Point/2 - Fawn]
└─$ sudo nmap -sV -sC 10.129.1.14
Starting Nmap 7.94 ( https://nmap.org ) at 2024-07-30 18:51 PDT
Nmap scan report for 10.129.1.14
Host is up (0.16s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE      SERVICE      VERSION
7/tcp     filtered  echo
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:10.10.14.42
|   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 1
|      vsFTPD 3.0.3 - secure, fast, stable
|_End of status
10001/tcp filtered scp-config
32785/tcp filtered unknown
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 13.38 seconds

Command Breakdown:

- `sC` : Runs script scan with the default scripts in Nmap and on your computer
 - You can see the default scripts on your computer by entering `locate *.nse` in your terminal.
- `sV` : Checks for versions

Key Information:

```
PORT      STATE      SERVICE      VERSION
7/tcp     filtered  echo
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:10.10.14.42
|    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 1
|    vsFTPD 3.0.3 - secure, fast, stable
|_End of status
10001/tcp filtered scp-config
32785/tcp filtered unknown
Service Info: OS: Unix
```

Result Breakdown:

- 4 ports are open: 7, 21, 10001, and 32785.
 - Port 7: This is **filtered** and runs the Echo Protocol. It relays ICMP datagrams.
 - Port 21: Is **open** and running FTP. FTP is File Transfer Protocol, which is a standard network protocol.
 - We can see it allows anonymous login.
 - We can see what version of FTP is being used (`vsftpd 3.0.3`). This could be potentially important so it's something to keep in mind.
 - We're also given a FTP status code of `230` , which means a connection was successful through anonymous login.
 - This is what we should be looking into!
 - Port 10001: This is **filtered** and this is the port for Network Data Management Protocol (NDMP). Used primarily for backup of network-attached storage (NAS) devices.
 - Not what we're looking for.
- [Ubiquiti](#) UniFi access points broadcast to 255.255.255.255:10001 (UDP) to locate the controller(s).
- Port 32785: This is **filtered**. I think it's an unassigned port.
 - Probably not something we're interested in.
- The target machine is running a Unix OS.

Foothold

Port 21 was our most interesting find. We're going to take a look at it and try to get a foothold using the FTP service it's running.

FTP Successful Login Attempt - anonymous

Usual login for FTP looks like this: `ftp username:password@my.domain.com` , but we can see we can login anonymously from our Nmap scan.

Terminal:

```
(adhd@kali)-[~/Desktop/HTB/Notes/Starting Point/2 - Fawn]
└─$ ftp 10.129.1.14
Connected to 10.129.1.14.
220 (vsFTPd 3.0.3)
Name (10.129.1.14:adhd): anonymous
331 Please specify the password.
Password:
```

```
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

Result breakdown:

`ftp 10.129.1.14`: We start off by connecting to FTP on the target machine. Once we're connected, we can try logging in.

After connecting, we're given confirmation on the version of FTP running, as well as the status code for a successful connection (`230`).

Logging in anonymously means we use `anonymous` as our username, and when we're prompted for a password, we don't type anything, and just hit the Enter button on our keyboard.

We're in!

Let's start poking around in the target machine.

Enumeration pt.2

Let's see what files are here.

Terminal:

```
ftp> ls  
229 Entering Extended Passive Mode (|||33584|)  
150 Here comes the directory listing.  
-rw-r--r--    1 0          0          32 Jun 04  2021 flag.txt  
226 Directory send OK.  
ftp>
```

Command Breakdown:

- FTP uses a few commands that are the same in Linux. What we want to do is list the items in our directory.

Result breakdown:

And we can spot there's a `flag.txt` file. Now we just need to read the flag.

Terminal:

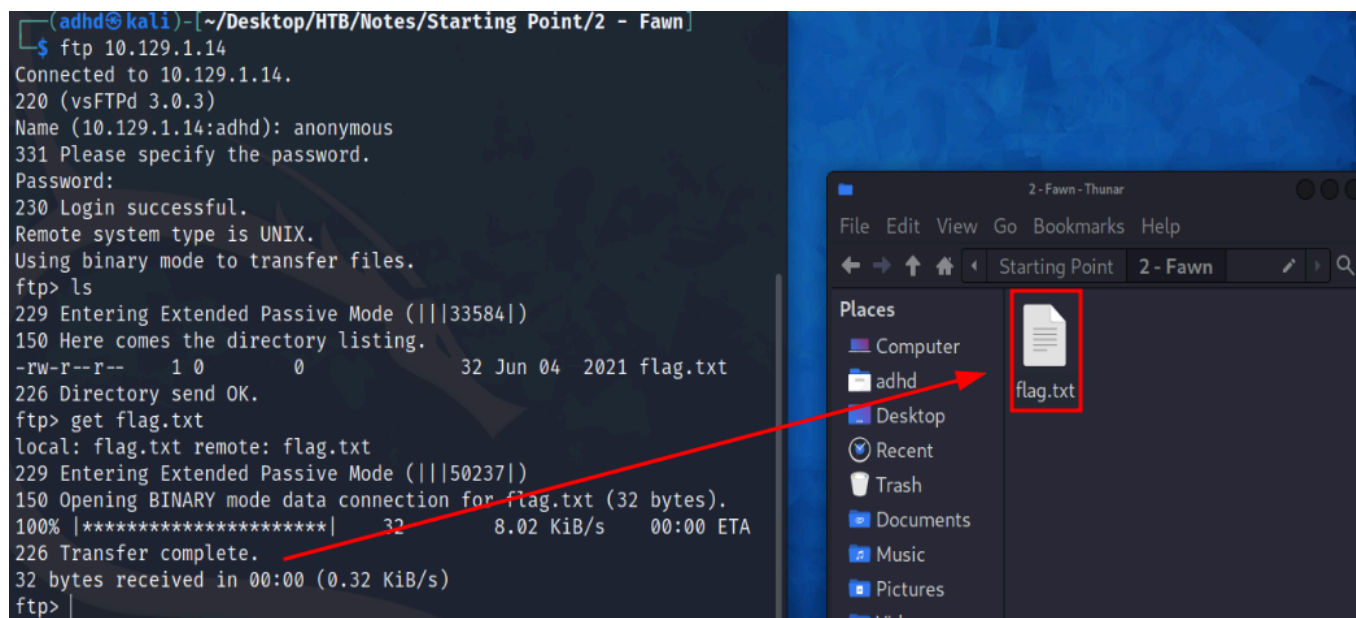
```
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||50237|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |*****| 32 8.02 KiB/s 00:00 ETA
226 Transfer complete.
32 bytes received in 00:00 (0.32 KiB/s)
ftp>
```

Command Breakdown:

- `get` is the command we use in FTP if we want to be able to read it. This command will download the file.

Result breakdown:

The file is downloaded into the directory where we have our terminal open in. We can go ahead and simply open it and read it!



Flag:

035db21c881520061c53e0536e44f815

HTB Tasks

HTB Task 1:

② What does the 3-letter acronym FTP stand for? >

File transfer Protocol

HTB Task 2:

② Which port does the FTP service listen on usually? >

21

HTB Task 3:

② 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? >

SFTP

HTB Task 4:

② What is the command we can use to send an ICMP echo request to test our connection to the target? >

ping

HTB Task 5:

② From your scans, what version is FTP running on the target? >

vsftpd 3.0.3

HTB Task 6:

② From your scans, what OS type is running on the target? >

Unix

HTB Task 7:

- ② What is the command we need to run in order to display the 'ftp' client help menu? >

```
ftp -h
```

HTB Task 8:

- ② What is username that is used over FTP when you want to log in without having an account? >

```
anonymous
```

HTB Task 9:

- ② What is the response code we get for the FTP message 'Login successful'? >

```
230
```

HTB Task 10:

- ② 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
```

HTB Task 11:

- ② What is the command used to download the file we found on the FTP server? >

```
get
```

Root Flag:

035db21c881520061c53e0536e44f815

-
- #FTP
 - #protocols
 - #reconnaissance
 - #Anonymous/GuestAccess