Task 1

What does the 3-letter acronym FTP stand for?

TASK 1

What does the 3-letter acronym FTP stand for?

**** ******** *******1

File Transfer Protocol
Hide Answer

Task 2

Which port does the FTP service listen on usually?

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?

TASK 3

What acronym is used for the secure version of FTP?

***p

sftp
Hide Answer

Task 4

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

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

Task 5

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

Running the command "nmap -v -A 10.129.57.243

```
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
┌─[us-starting-point-1-dhcp]─[10.10.15.19]─[htb-proxyrambus@htb-tue7dkrxyp]─[~/Desktop]
└─[★]$ nmap -v -A 10.129.57.243
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-26 17:17 BST
NSE: Loaded 155 scripts for scanning.
```

This gives us the FTP version number


```
|_-rw-r--r--    1 0        0            32 Jun 04  2021 flag.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.15.19
|      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 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
Service Info: OS: Unix
```

Task 6

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

That same command also give us the targets OS

```
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:10.10.15.19
|      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 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
Service Info: OS: Unix
```

TASK 6

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

```
***x
```

Unix
Hide Answer

Task 7

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

TASK 7

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

```
***  -h
```

ftp -h
Hide Answer

Task 8

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

TASK 8

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

```
*******s
```

anonymous
Hide Answer

Task 9

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

Attempting to FTP into the target with the the provided username anonymous

```
[us-starting-point-1-dhcp]-[10.10.15.19]-[
    [*]$ ftp 10.129.57.243
Connected to 10.129.57.243.
220 (vsFTPd 3.0.3)
Name (10.129.57.243:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

TASK 9

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

***

230
Hide Answer

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.

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

Task 11

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

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

Searching the FTP server for the flag.txt file

```
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
226 Directory send OK.
ftp>
```
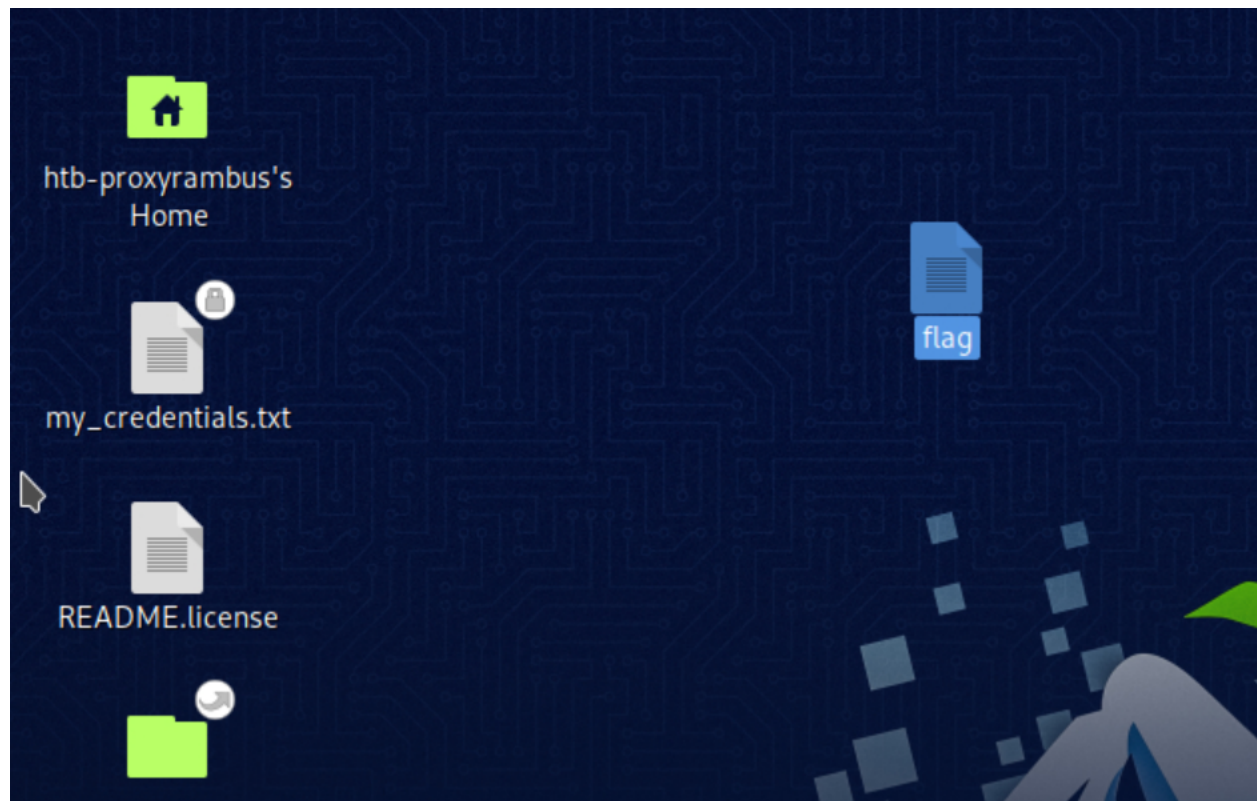
Setting the download location to be desktop with command "lcd /home/htb-proxyrambus/Desktop"
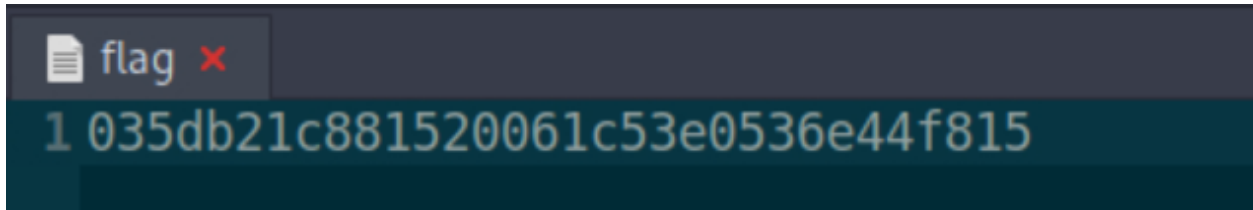
226 Transfer complete.
32 bytes received in 0.00 secs (106.2925 kB/s)
ftp> lcd /home/htb-proxyrambus/Desktop
Local directory now /home/htb-proxyrambus/Desktop
ftp>

Using the get command and naming the file flag

200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for flag.txt (32 bytes).
226 Transfer complete.
32 bytes received in 0.00 secs (538.7931 kB/s)
ftp>

Opening flag file from the Desktop

flag ✕

1 035db21c881520061c53e0536e44f815

Submitting the flag root file

SUBMIT FLAG

Submit root flag

****

035db21c881520061c53e0536e44f815

Hide Answer

Fawn has been Pwned!

Congratulations **ProxyRambus**, best of luck in capturing flags ahead!

26 Oct 2022

PWN DATE

OK   SHARE