HACKTHEBOX

Tier 0 Medium Offensive

During an assessment, it is very common for us to transfer files to and from a target system. This module covers file transfer techniques leveraging tools commonly available across all versions of Windows and Linux systems.

By Saezel

Last Updated: 05 November 2024

# Windows File Transfer Methods

*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*

Download flag.txt

```
└─$ wget <target-ip>/flag.txt
```

After successfully downloaded, view the content of the file.

```
└─$ cat flag.txt
```

*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*

Download the upload_win.zip to the attacker machine:

```
└─$ wget
https://academy.hackthebox.com/storage/modules/24/upload_win.zip
```

Run webserver on attacker machine

```
└─$ python -m http.server 8000
```

Connect to target via RDP:

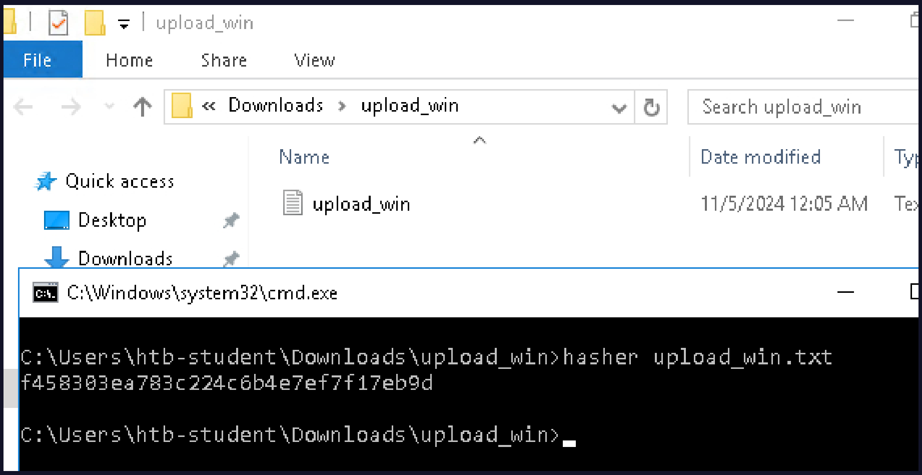
```
└─$ xfreerdp /v:<target-ip> /u:htb-student /p:HTB_@cademy_stdnt!
```

Download file from attacker machine:

```
└─ firefox:/> http://<target-ip>:8000/upload_win.zip
```

Extract the .zip archive and run command prompt in that directory.

```
└─$ hasher upload_win.txt
```



```
C:\Users\htb-student\Downloads\upload_win>hasher upload_win.txt
f458303ea783c224c6b4e7ef7f17eb9d

C:\Users\htb-student\Downloads\upload_win>_
```

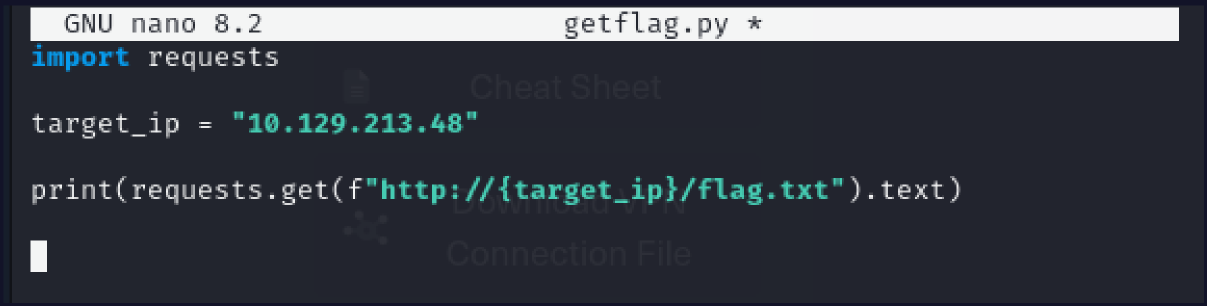
## Linux File Transfer Methods

*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*

Create a python file to download the flag.txt file

```
└─$ nano getflag.py
```



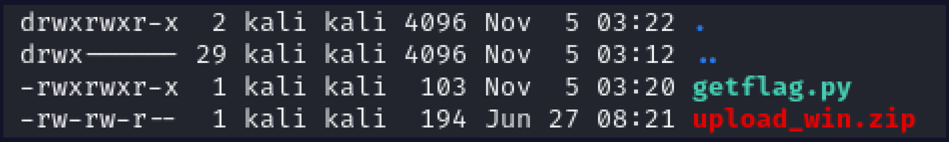
```
import requests

target_ip = "10.129.213.48"

print(requests.get(f"http://{target_ip}/flag.txt").text)
```

Give exec permission to getflag.py

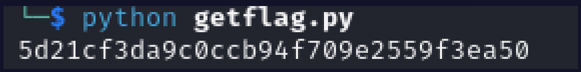
```
└─$ chmod +x getflag.py
```



```
drwxrwxr-x  2 kali kali 4096 Nov  5 03:22 .
drwx------ 29 kali kali 4096 Nov  5 03:12 ..
-rwxrwxr-x  1 kali kali  103 Nov  5 03:20 getflag.py
-rw-rw-r--  1 kali kali  194 Jun 27 08:21 upload_win.zip
```

Execute getflag.py and get the flag

```
└─$ python getflag.py
```



```
└─$ python getflag.py
5d21cf3da9c0ccb94f709e2559f3ea50
```

*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*

wget from the target machine failed. Instead, I'll host a webserver on my attacker machine.

```
└─$ python3 -m http.server
```

Download the file to the attacker machine:

```
└─$ wget
https://academy.hackthebox.com/storage/modules/24/upload_nix.zip
```

SSH to the target:

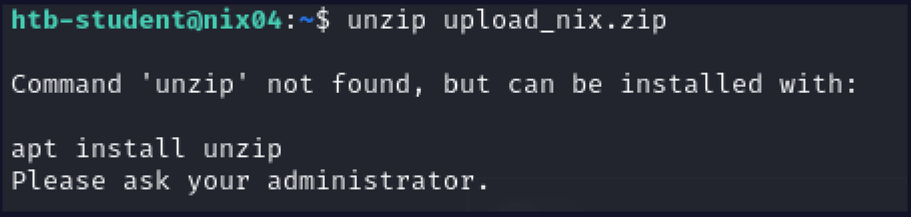
```
└─$ ssh htb-student@<target-ip>
```

From the target machine, download the file from my attacker machine.

```
└─ htb-student $ wget <attacker-ip>:8000/upload_nix.zip
```

Attempt to unzip the file

```
└─ htb-student $ unzip upload_nix.zip
```



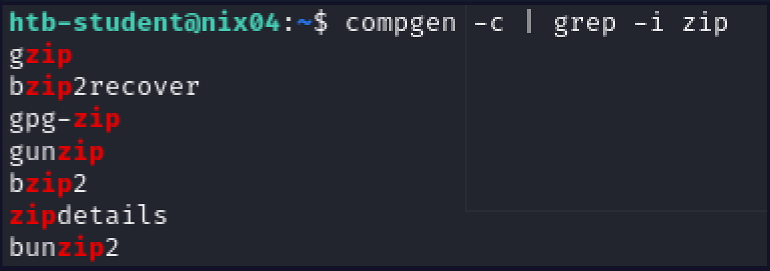
```
htb-student@nix04:~$ unzip upload_nix.zip

Command 'unzip' not found, but can be installed with:

apt install unzip
Please ask your administrator.
```

Unzip is not installed in target machine.
1. You can unzip on attacker machine and download that to the target machine.
2. Find an alternative program that can unzip. I will proceed to find alternatives

```
└─ htb-student $ compgen -c | grep -i zip
```

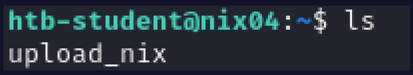


```
htb-student@nix04:~$ compgen -c | grep -i zip
gzip
bzip2recover
gpg-zip
gunzip
bzip2
zipdetails
bunzip2
```

After some research, I use gunzip:

```
└─ htb-student $ gunzip -S .zip upload_nix.zip
```

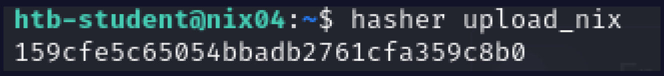
```
└─ htb-student $ ls
```



```
htb-student@nix04:~$ ls
upload_nix
```

Finally, check the hash:

```
└─ htb-student $ hasher upload_nix
```



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