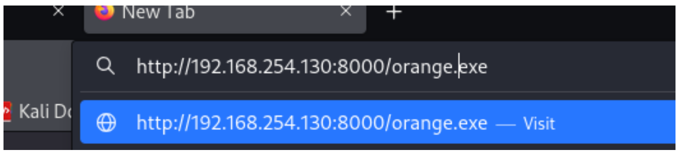
Malware Analysis

▼ **Download additional_samples.zip from this module's resources (available at the upper right corner) and transfer the .zip file to this section's target. Unzip additional_samples.zip (password: infected) and use IDA to analyze orange.exe. Enter the registry key that it modifies for persistence as your answer. Answer format: SOFTWARE____**

I first tried the command below, but It didnt work. I think its because

```
$ python3 -m http.server 8080
#In Powershell
curl.exe -o "C:\Users\htb-student\Downloads\orange.exe" "http://192.168.254.13
```

- I check the browser to see if its working and it is. I was trying `python3` , lets try `python`

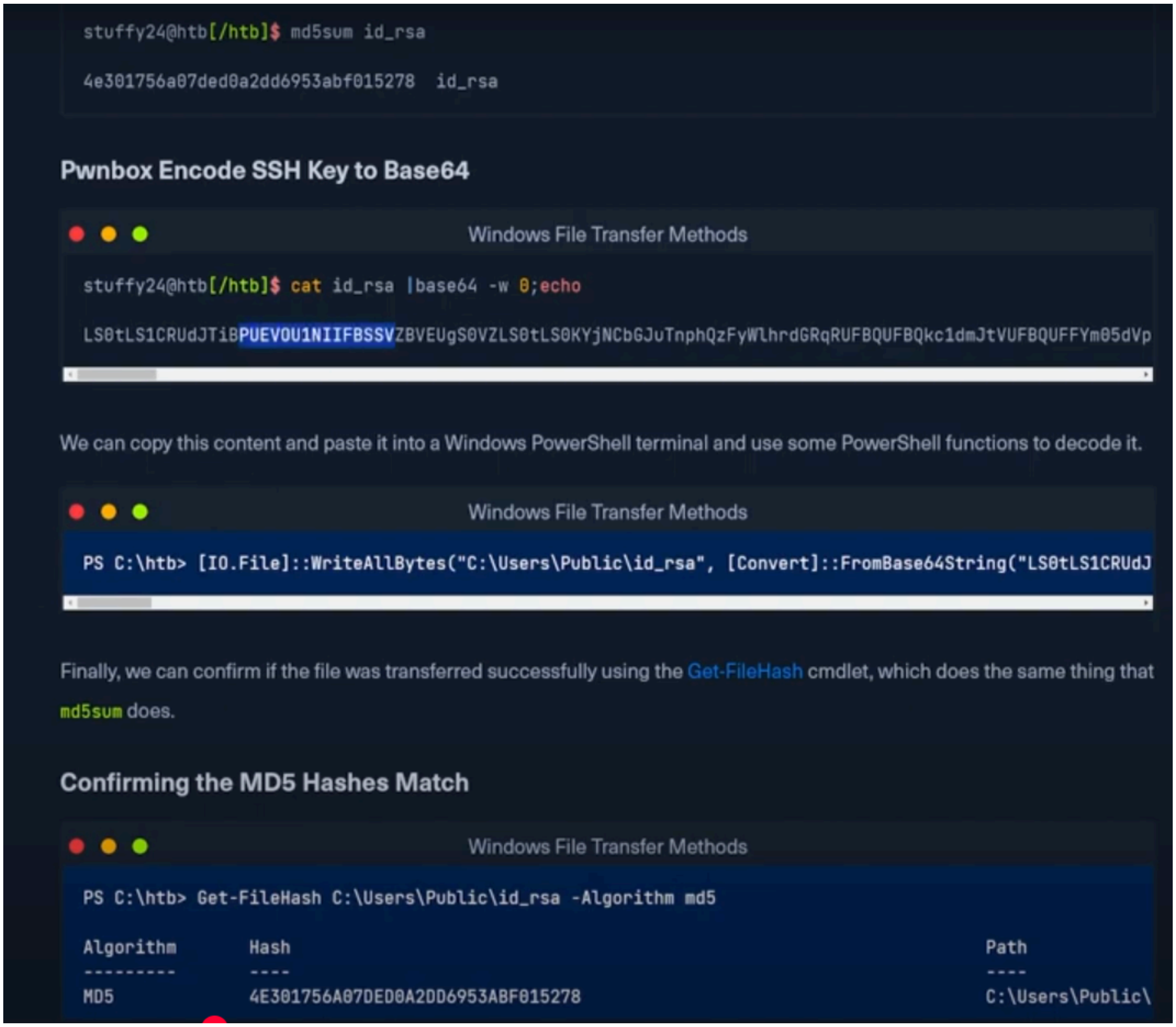


http://192.168.254.130:8000/orange.exe

http://192.168.254.130:8000/orange.exe

```
python -m http.server 8080
#In Powershell
curl.exe -o "C:\Users\htb-student\Downloads\orange.exe" "http://192.168.254.13
```

I still recevied a timeout error



```
stuffy24@htb[/htb]$ md5sum id_rsa

4e301756a07ded0a2dd6953abf015278  id_rsa
```

Pwnbox Encode SSH Key to Base64

```
stuffy24@htb[/htb]$ cat id_rsa |base64 -w 0;echo

LS0tLS1CRUdJTiBPUEVOU1NIIFBSSVZBVEUgS0VZLS0tLS0KYjNCbGJuTnphQzFyWlhrdGRqRUFBQUFBQkc1dmJtVUFBQUFFYm05dVp
```

We can copy this content and paste it into a Windows PowerShell terminal and use some PowerShell functions to decode it.

```
PS C:\htb> [IO.File]::WriteAllBytes("C:\Users\Public\id_rsa", [Convert]::FromBase64String("LS0tLS1CRUdJ
```

Finally, we can confirm if the file was transferred successfully using the Get-FileHash cmdlet, which does the same thing that md5sum does.

Confirming the MD5 Hashes Match

```
PS C:\htb> Get-FileHash C:\Users\Public\id_rsa -Algorithm md5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             4E301756A07DED0A2DD6953ABF015278                                       C:\Users\Public\
```

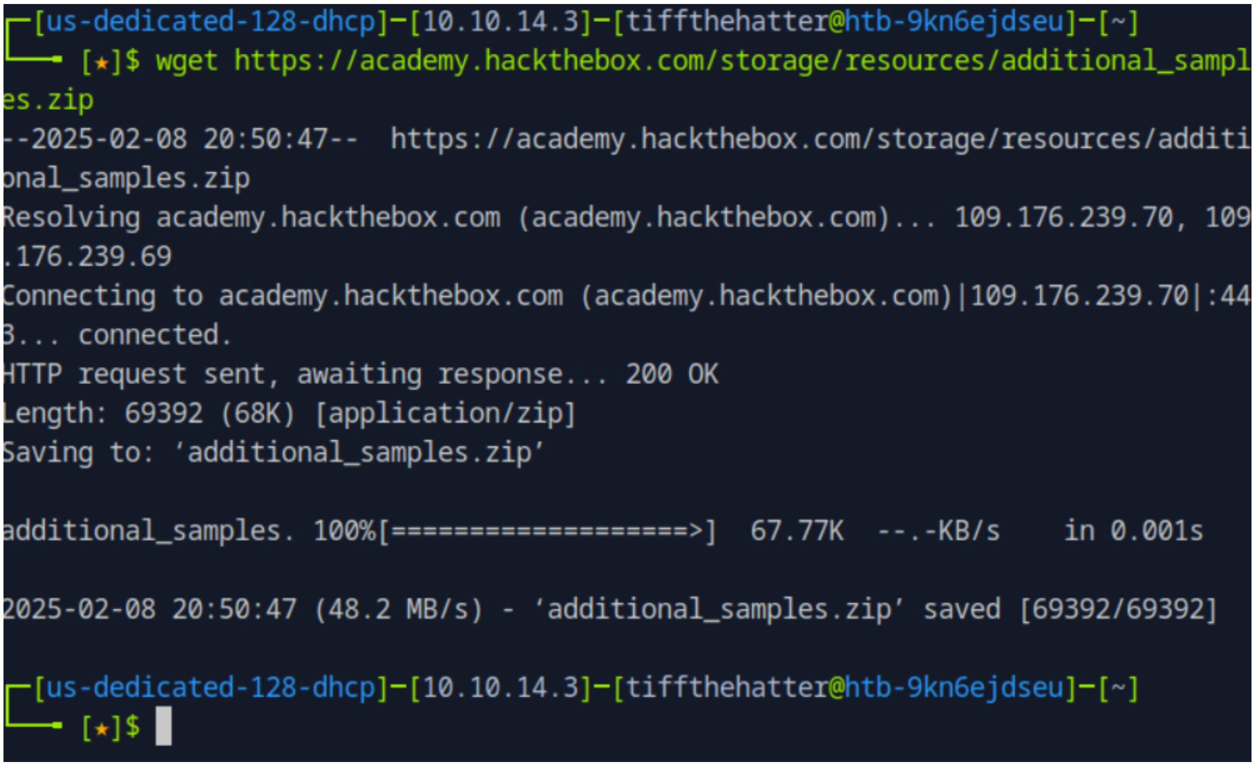
```
cd /home/kali/Downloads/additional_samples

python3 -m http.server 8000

(New-Object System.Net.WebClient).DownloadFile("http://192.168.254.130:8000/
```

curl.exe -o "C:\Users\htb-student\Downloads\orange.exe" "http://192.168.254.130:8080/orange.exe"

curl -o "/home/tiffthehatter/Downloads/orange.exe" "http://192.168.254.130:8080/orange.exe"



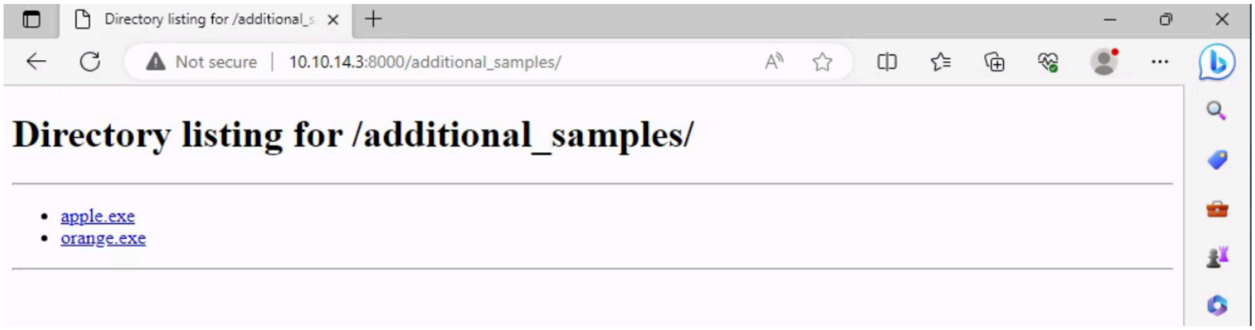
```
┌─[us-dedicated-128-dhcp]─[10.10.14.3]─[tiffthehatter@htb-9kn6ejdseu]─[~]
└──╼ [★]$ wget https://academy.hackthebox.com/storage/resources/additional_sampl
es.zip
--2025-02-08 20:50:47--  https://academy.hackthebox.com/storage/resources/additi
onal_samples.zip
Resolving academy.hackthebox.com (academy.hackthebox.com)... 109.176.239.70, 109
.176.239.69
Connecting to academy.hackthebox.com (academy.hackthebox.com)|109.176.239.70|:44
3... connected.
HTTP request sent, awaiting response... 200 OK
Length: 69392 (68K) [application/zip]
Saving to: ‘additional_samples.zip’

additional_samples. 100%[===================>]  67.77K  --.-KB/s    in 0.001s

2025-02-08 20:50:47 (48.2 MB/s) - ‘additional_samples.zip’ saved [69392/69392]

┌─[us-dedicated-128-dhcp]─[10.10.14.3]─[tiffthehatter@htb-9kn6ejdseu]─[~]
└──╼ [★]$ 
```

```
$ python3 -m http.server 8080
```


Directory listing for /additional_s
Not secure
10.10.14.3:8000/additional_samples/

Directory listing for /additional_samples/

- apple.exe
- orange.exe

THen I received the flag after examining the files with IDA