Metasploit Cheat Sheet Cheat Sheet

by Alexynior (alexismon) via cheatography.com/121671/cs/22368/

Comandos de Meterpreter

sysinfo	Mostrar información del sistema
ps	Lista y muestra procesos en ejecución
kill (PID)	Terminar un proceso en ejecución
getuid	Mostrar ID de usuario
upload o download	Cargar / descargar un archivo
pwd o lpwd	Mostrar directorio de trabajo (local / remoto)
cd o lcd	Cambiar directorio (local o remoto)
cat	Mostrar contenido del archivo
bglist	Mostrar scripts en ejecución en segundo plano
bgrun	Hacer que un script se ejecute en segundo plano
bgkill	Terminar un proceso en segundo plano
background	Mover sesión activa al segundo plano
edit	Editar un archivo en el editor vi
shell	Shell de acceso en la máquina de destino
migrate	Cambiar a otro proceso
idletime	Mostrar el tiempo de inactividad del usuario
screenshot	Tomar una captura de pantalla
clearev	Borrar los registros del sistema
?	Comandos disponibles
exit / quit	Salir de la sesión de Meterpreter
shutdown / reboot	Reiniciar el sistema
use	Carga de extensión

Comandos de Meterpreter (cont)

channel	Mostrar canales activos

Comandos de red

ipconfig	Mostrar la configuración de la interfaz de red
portfwd	Reenviar paquetes
route	Ver/editar tabla de enrutamiento de red

Comandos de interfaz/salida

enumdesktops	Mostrar todos los escritorios disponibles
getdesktop	Mostrar escritorio actual
keyscan_start	Iniciar keylogger en la máquina de destino
keyscan_stop	Detener keylogger en la máquina de destino
set_desktop	Configurar escritorio
keyscan_dump	Volcado de contenido del keylogger

Comandos de manejo de procesos

getpid	Mostrar la ID del proceso
getuid	Mostrar la ID de usuario
ps	Mostrar procesos en ejecución
kill	Detener y finalizar un proceso
getprivs	Muestra múltiples privilegios como sea posible
reg	Acceder al registro de la máquina de destino
shell	Acceder al shell de la máquina de destino
execute	Ejecuta un comando en el destino
migrate	Moverse a un ID de proceso de destino dado

Opciones de comando msfvenom

-p	Mostrar opciones estándar de payload
-l	Listar el tipo de módulo (payloads, encoders)
-f	Formato de salida
-e	Definir qué codificador usar
-a	Definir qué plataforma usar
-s	Definir la capacidad máxima de payload
-b	Definir conjunto de caracteres para no usar
-i	Definir el número de veces que se usará el codificador.
-x	Definir un archivo personalizado para usar como plantilla
-o	Guardar Payload
-h	Ayuda

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com