Полезные нагрузки: meterpreter.
Основные команды.

?	**Help menu**	**Меню справки**
background	Backgrounds the current session	Перевести в фоновый режим текущую сессию
bg	Alias for background	Псевдоним для background
bgkill	Kills a background meterpreter script	Закрывает фоновый meterpreter скрипт
bglist	Lists running background scripts	Списки запущенных фоновых скриптов
bgrun	Executes a meterpreter script as a background thread	Выполняет скрипт meterpreter в качестве фонового потока
channel	Displays information or control active channels	Отображение информации или управление активными каналами
close	Closes a channel	Закрывает канал
disable_unicode_encoding	Disables encoding of unicode strings	Отключает кодирование строк Юникода
enable_unicode_encoding	Enables encoding of unicode strings	Включает кодирование строк Юникода
exit	Terminate the meterpreter session	Завершить сессию meterpreter
get_timeouts	Get the current session timeout values	Получить значения времени ожидания текущей сессии
guid	Get the session GUID	Получить GUID сессии
help	Help menu	Меню справки
info	Displays information about a Post module	Отображает информацию о модулях пост-эксплуатации
irb	Open an interactive Ruby shell on the current session	Откройте интерактивную оболочку Ruby в текущей сессии
load	Load one or more meterpreter extensions	Загрузите одно или несколько расширений meterpreter
machine_id	Get the MSF ID of the machine attached to the session	Получить идентификатор MSF компьютера, подключенного к сессии
migrate	Migrate the server to another process	Перенос сервера на другой процесс
pivot	Manage pivot listeners	Управление сводными слушателями
pry	Open the Pry debugger on the current session	Откройте отладчик Pry в текущей сессии
quit	Terminate the meterpreter session	Завершить meterpreter сессию
read	Reads data from a channel	Читает данные из канала
resource	Run the commands stored in a file	Запускает команды, хранящиеся в файле
sessions	Quickly switch to another session	Быстрое переключение на другую сессию
set_timeouts	Set the current session timeout values	Установите значения времени ожидания текущей сессии
sleep	Force Meterpreter to go quiet, then re-establish session.	Заставьте Meterpreter замолчать, а затем восстановите сессию
transport	Change the current transport mechanism	Изменить текущий транспортный механизм
use	Deprecated alias for "load"	Устаревший псевдоним для «load»
uuid	Get the UUID for the current session	Получить UUID для текущей сессии
write	Writes data to a channel	Записывает данные в канал
Stdapi: команды файловой системы		
cat	Read the contents of a file to the screen	Подать содержимое файла на стандартный вывод
cd	Change directory	Сменить директорию
checksum	Retrieve the checksum of a file	Получить контрольную сумму файла
cp	Copy source to destination	Скопировать источник в место назначения
dir	List files (alias for ls)	Список файлов (псевдоним для ls)
download	Download a file or directory	Скачать файл или каталог
edit	Edit a file	Редактировать файл
getlwd	Print local working directory	Вывести на экран локальный рабочий каталог
getwd	Print working directory	Вывести на экран рабочий каталог
lcd	Change local working directory	Изменить локальный рабочий каталог
lls	List local files	Список локальных файлов
lpwd	Print local working directory	Вывести на экран локальный рабочий каталог
mkdir	Make directory	Создать каталог
ls	List files	Список файлов

mv	Move source to destination	Переместить источник в пункт назначения
pwd	Print working directory	Вывести на экран рабочий каталог
rm	Delete the specified file	Удалить указанный файл
rmdir	Remove directory	Удалить каталог
search	Search for files	Поиск файлов
show_mount	List all mount points/logical drives	Показать подключенные файловые системы
upload	Upload a file or directory	Загрузить файл или каталог
Stdapi: сетевые команды		
arp	Display the host ARP cache	Показать ARP-кэш хоста
getproxy	Display the current proxy configuration	Показать текущую конфигурацию прокси
ifconfig	Display interfaces	Отобразить сетевые интерфейсы
ipconfig	Display interfaces	Отобразить сетевые интерфейсы
netstat	Display the network connections	Показать сетевые подключения
portfwd	Forward a local port to a remote service	Переадресация локального порта на удаленный сервис
resolve	Resolve a set of host names on the target	Разрешить устанавливливать имена хостов на цели
route	View and modify the routing table	Просмотр и изменение таблицы маршрутизации
Stdapi: системные команды		
clearev	Clear the event log	Очистить журнал событий
drop_token	Relinquishes any active impersonation token.	Сбросить все активные токены
execute	Execute a command	Выполнить команду
getenv	Get one or more environment variable values	Получить одно или несколько значений переменного окружения
getpid	Get the current process identifier	Получить идентификатор текущего процесса
getprivs	Attempt to enable all privileges available to the current process	Получить все привилегии, доступные текущему процессу
getsid	Get the SID of the user that the server is running as	Получить SID пользователя, на котором работает сервер meterpreter
getuid	Get the user that the server is running as	Получить имя пользователя, на котором работает сервер meterpreter
kill	Terminate a process	Завершить процесс
localtime	Displays the target system's local date and time	Отображает локальную дату и время целевой системы
pgrep	Filter processes by name	Фильтровать процессы по имени
pkill	Terminate processes by name	Завершить процессы по имени
ps	List running processes	Список запущенных процессов
reboot	Reboots the remote computer	Перезагружает удаленный компьютер
reg	Modify and interact with the remote registry	Модифицировать и взаимодействовать с удаленным реестром
rev2self	Calls RevertToSelf() on the remote machine	Вызывает RevertToSelf () на удаленной машине
shell	Drop into a system command shell	Запускает командную оболочку системы (CMDshell)
shutdown	Shuts down the remote computer	Выключает удаленный компьютер
steal_token	Attempts to steal an impersonation token from the target process	Попытки украсть токен целевого процесса
suspend	Suspends or resumes a list of processes	Приостановляет или возобновляет список процессов
sysinfo	Gets information about the remote system, such as OS	Получает информацию об удаленной системе
Stdapi: Команды пользовательского интерфейса		
enumdesktops	List all accessible desktops and window stations	Показывает все доступные декстопы и оконные станции
getdesktop	Get the current meterpreter desktop	Получить текущий счетчик рабочего стола
idletime	Returns the number of seconds the remote user has been idle	Время последней активности
keyboard_send	Send keystrokes	Отправить сочетание клавиш
keyevent	Send key events	Отправить события
keyscan_dump	Dump the keystroke buffer	Дамп буфера нажатия клавиш
keyscan_start	Start capturing keystrokes	Захват нажатия клавиш

keyscan_stop	Stop capturing keystrokes	Закончить захват нажатия клавиш
mouse	Send mouse events	Отправить события мыши
screenshare	Watch the remote user's desktop in real time	Смотреть рабочий стол удаленного пользователя в режиме реального времени
screenshot	Grab a screenshot of the interactive desktop	Сделать скриншот удаленного рабочего стола
setdesktop	Change the meterpreters current desktop	Сменить текущий рабочий стол meterpreter
uictl	Control some of the user interface components	Управление некоторыми компонентами пользовательского интерфейса
Stdapi: команды веб-камеры		
record_mic	Record audio from the default microphone for X seconds	Запись звука с микрофона по умолчанию в течение X секунд
webcam_chat	Start a video chat	Начать видео чат
webcam_list	List webcams	Список веб-камер
webcam_snap	Take a snapshot from the specified webcam	Сделать снимок с указанной веб-камеры
webcam_stream	Play a video stream from the specified webcam	Воспроизвести видео с указанной веб-камеры
Stdapi: команды вывода звука		
play	play an audio file on target system, nothing written on disk	Воспроизвести аудиофайл на целевой системе(не оставляет файлов на удаленной системе)
Priv: команды повышения уровня доступа		
getsystem	Attempt to elevate your privilege to that of local system.	Попытаться повысить свои привилегии до привилегий локальной системы.
Priv: команды базы паролей		
hashdump	Dumps the contents of the SAM database	Сбрасывает содержимое базы данных SAM
Priv: команды Timestomp		
timestomp	Manipulate file MACE attributes	Манипулировать атрибутами файла MACE