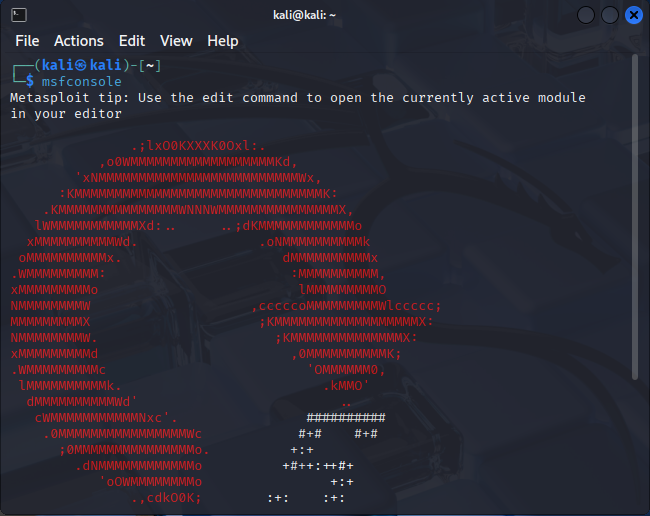
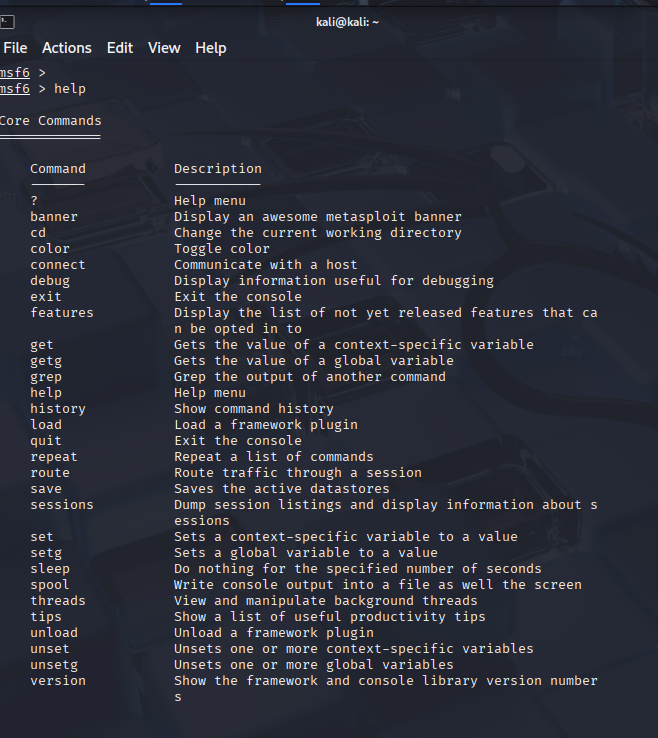
Задание 3. Изучить возможности средства Metasploit

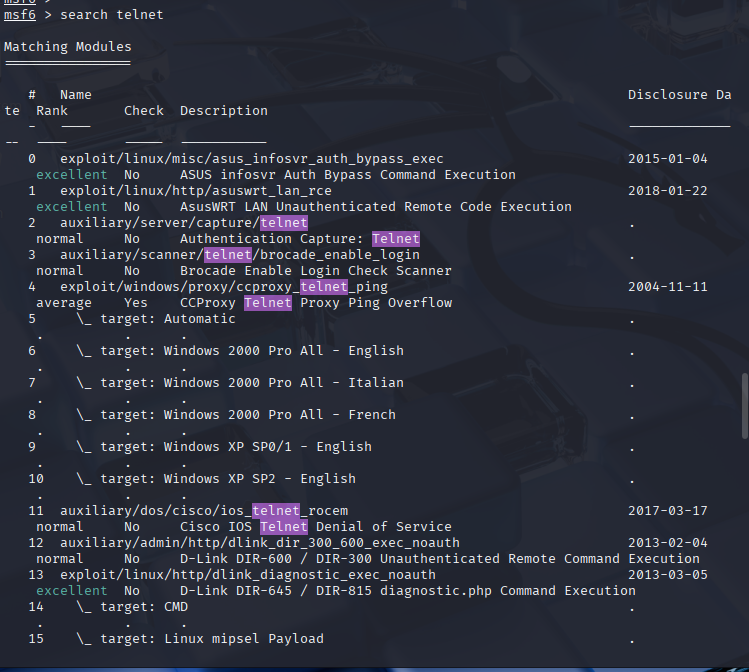




Эксплойты — это подвид вредоносных программ. Они содержат данные или исполняемый код, способный воспользоваться одной или несколькими уязвимостями в программном обеспечении на локальном или удаленном компьютере.

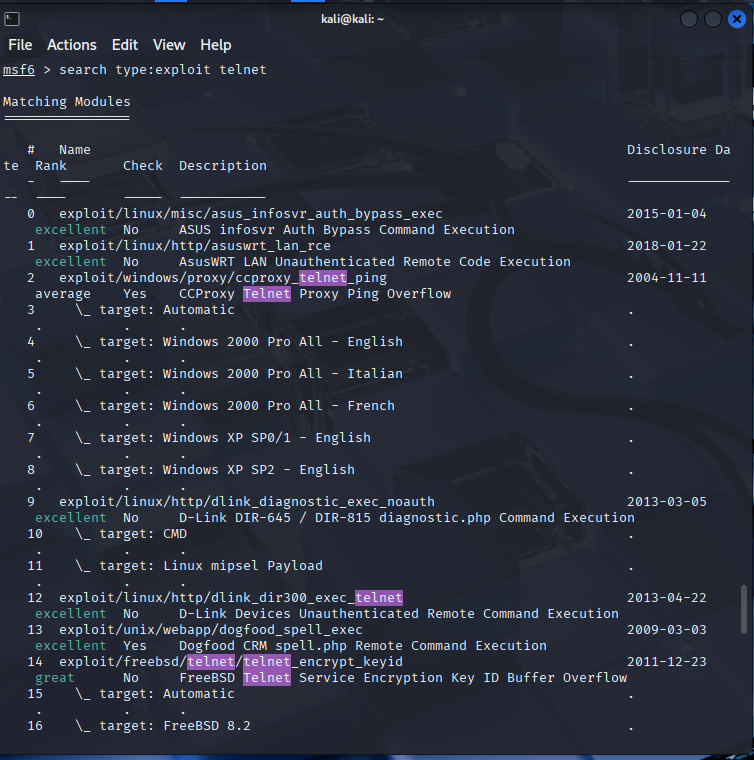
Например, у вас есть браузер, и есть уязвимость в нем, которая позволяет исполнить «произвольный код», то есть установить и запустить некую вредоносную программу на вашей системе без вашего ведома или спровоцировать какое-либо иное не ожидаемое вами поведение системы. Чаще всего первым шагом злоумышленников становится повышение привилегий, позволяющее делать в атакуемой системе все, что в голову взбредет.

Далее я, например, хочу найти эксплоит, который эксплуатирует уязвимость по протоколу telnet

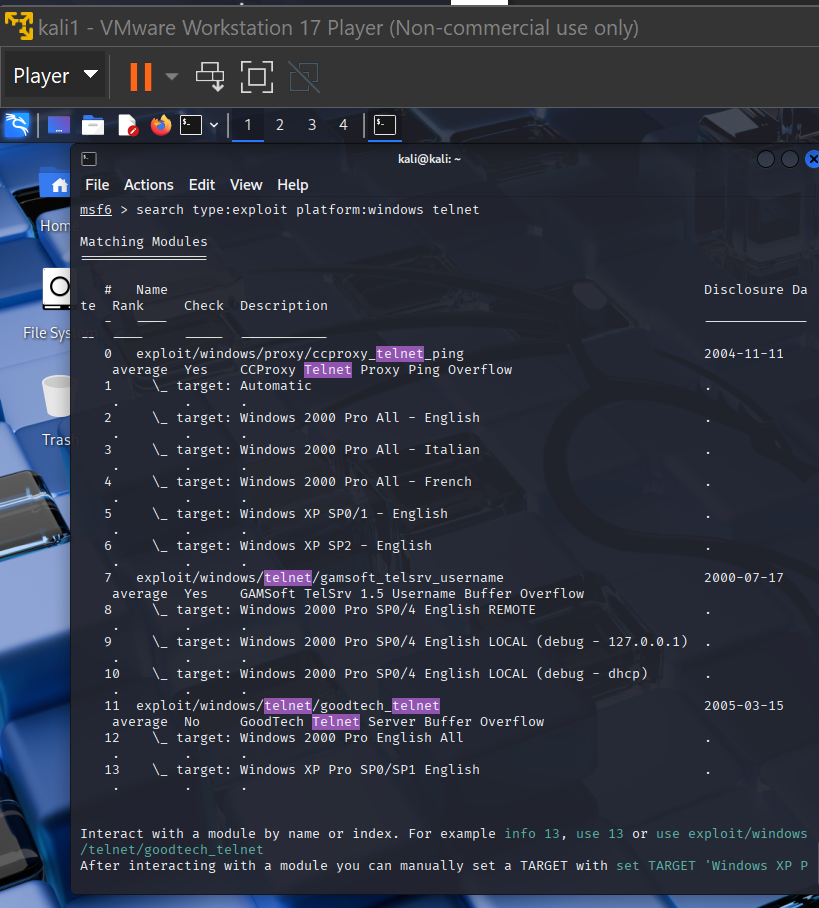


auxiliary модули представляют собой инструменты, которые не являются эксплойтами, но могут выполнять различные вспомогательные функции, такие как сканирование, сбор информации или тестирование на уязвимости. Эти модули помогают исследователям безопасности в процессе анализа и тестирования систем.

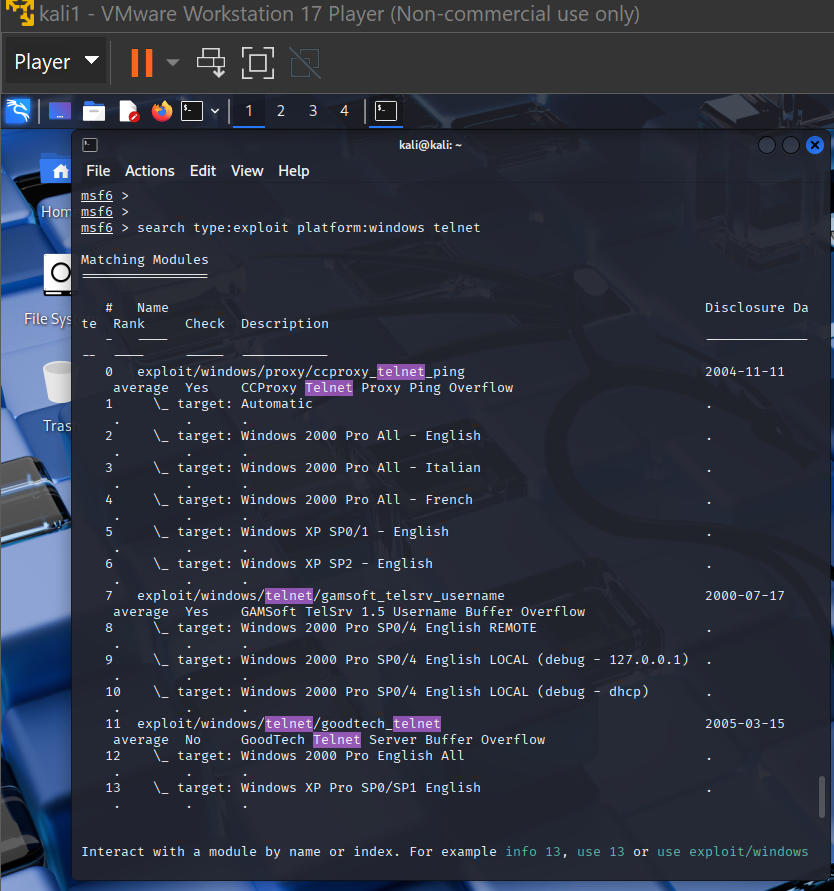
Для того, чтобы искать только эксплоиты, то введу следующую команду:



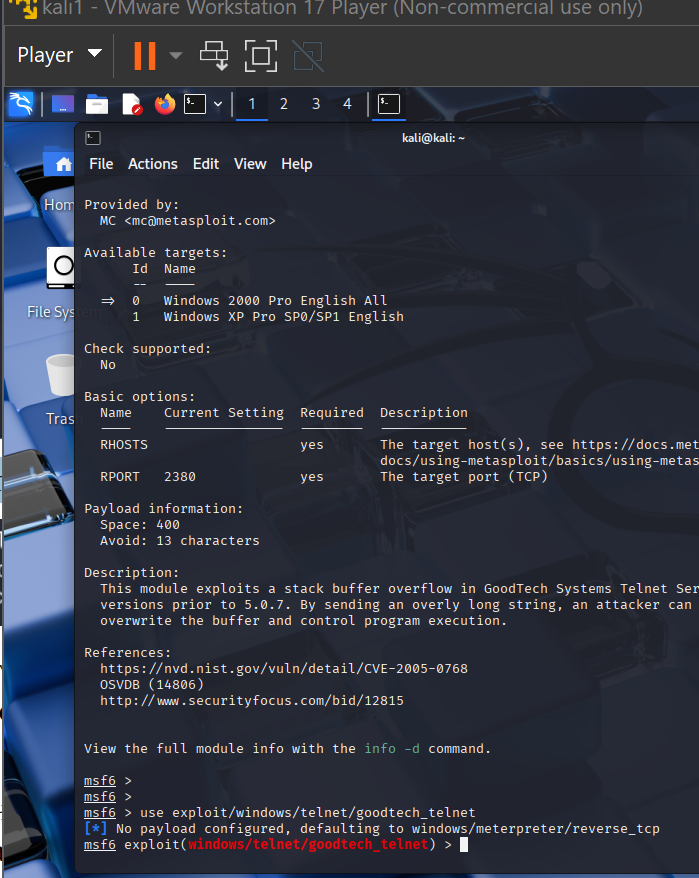
Если мне нужна определённая операционная система, то это можно явно указать:



Чтобы узнать подробную информацию о конкретном эксплоите, то введу следующую команду:

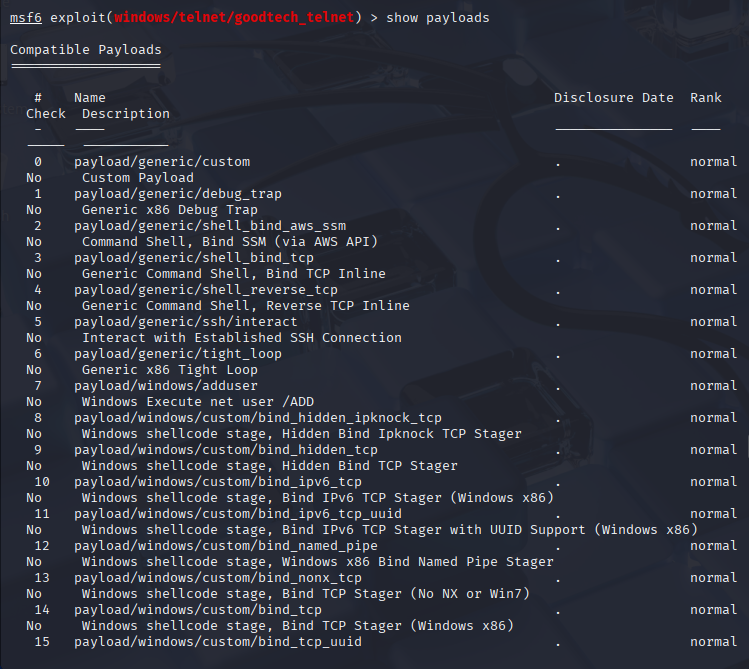


Можно перейти к настройке конкретного эксплойта:

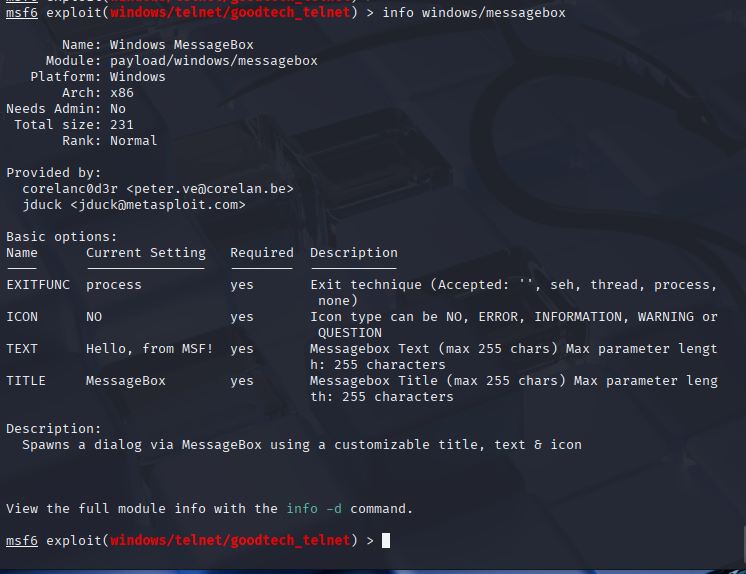


Эксплойт (Exploit) — программа или код, который использует уязвимость в программном обеспечении для получения контроля над системой или выполнения кода на целевой машине. Полезная нагрузка (Payload) — код или команда, которая выполняется на целевой системе после успешного использования эксплойта. Может выполнять различные действия, например, сбор информации, перехват пакетов.

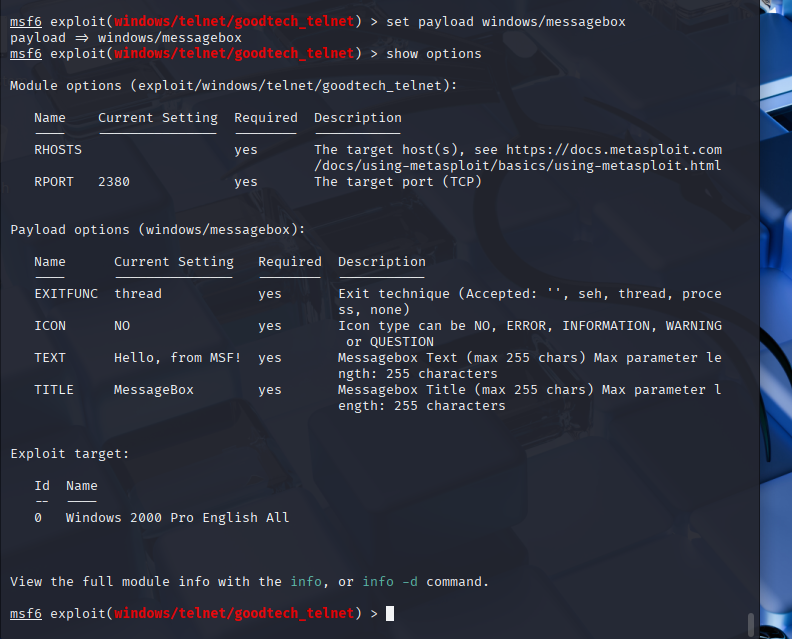
Далее посмотрю пэйлоиды, совместимые с данным эксплоитом:



Посмотрю информацию о конкретном пэйлоиде:



Для того, чтобы его использовать с данным типом эксплоита, то пропишу команду: и посмотрю настройки



RHOST – IP адрес удалённого хоста. RPORT – номер порта на удалённой машине Requred означает обязательно для заполнения. Необходимо заполнить RHOST.

И ещё поменяю текст

