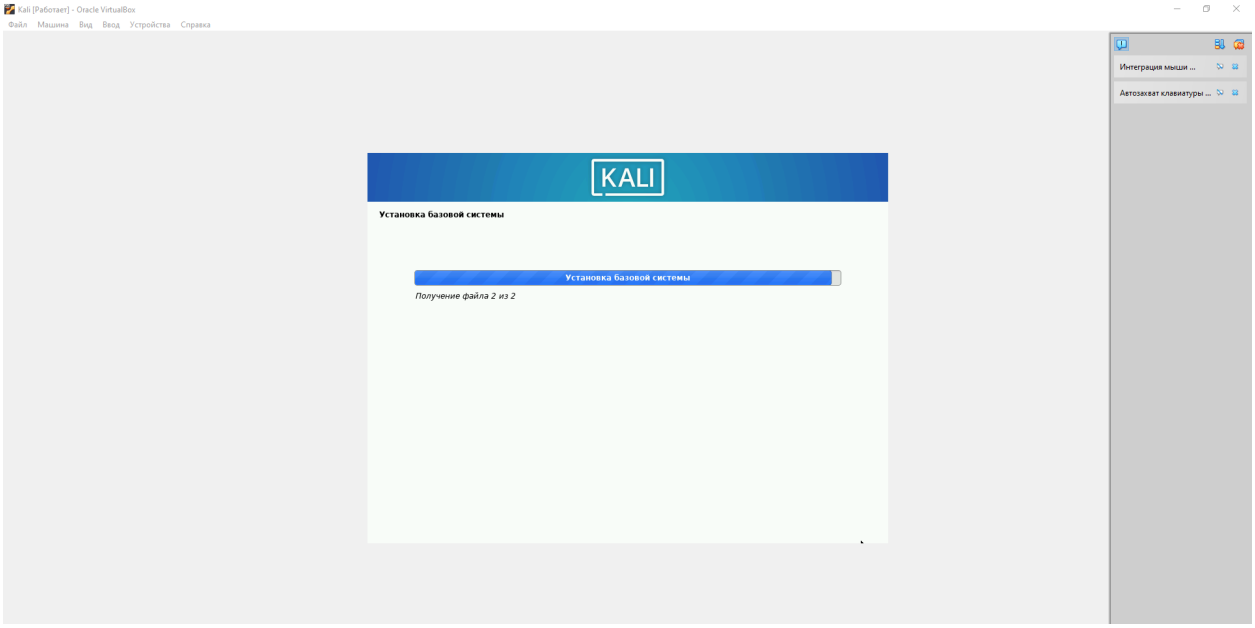
Практическая работа 4

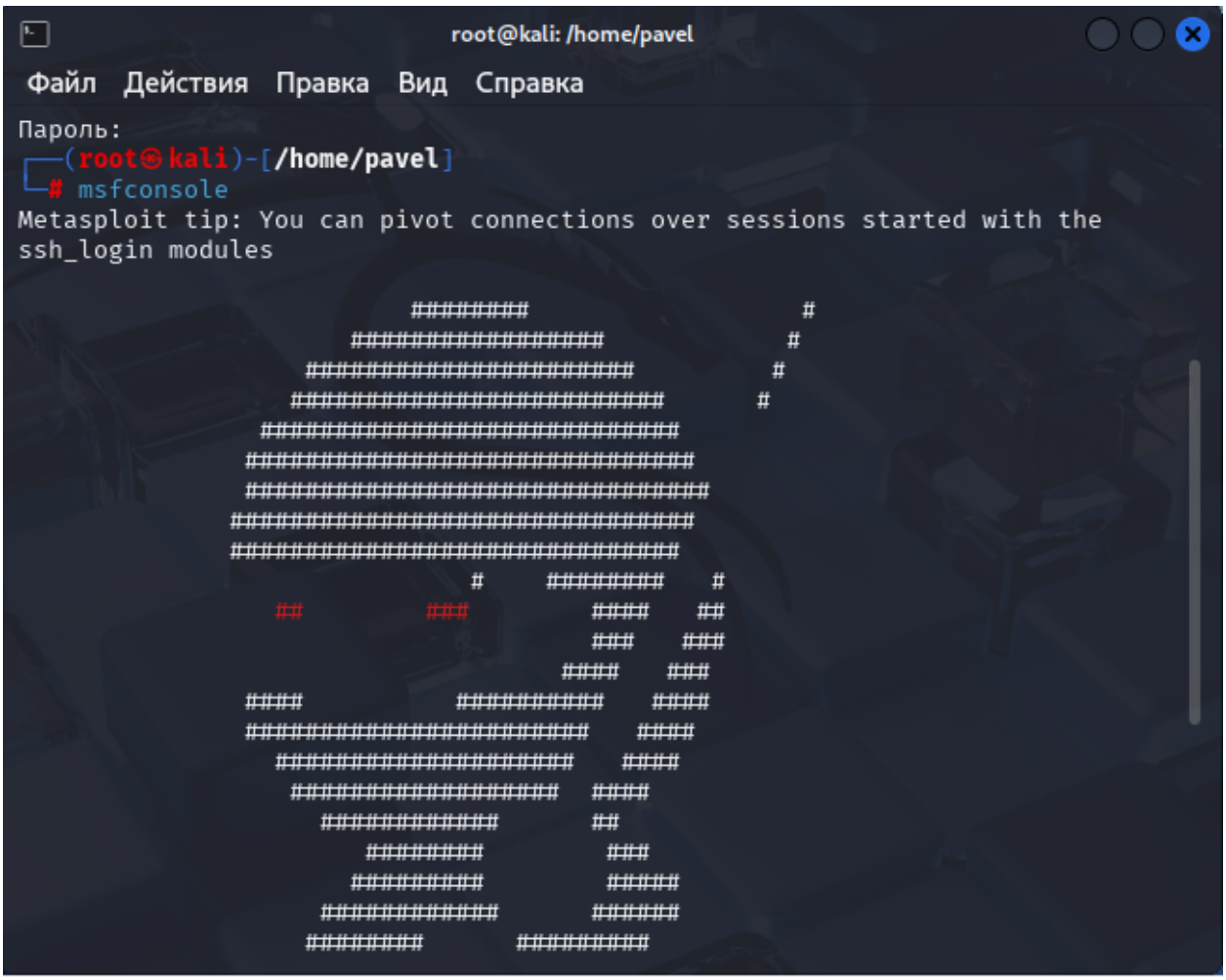
Задание:

Изучить возможности средства Metasploit

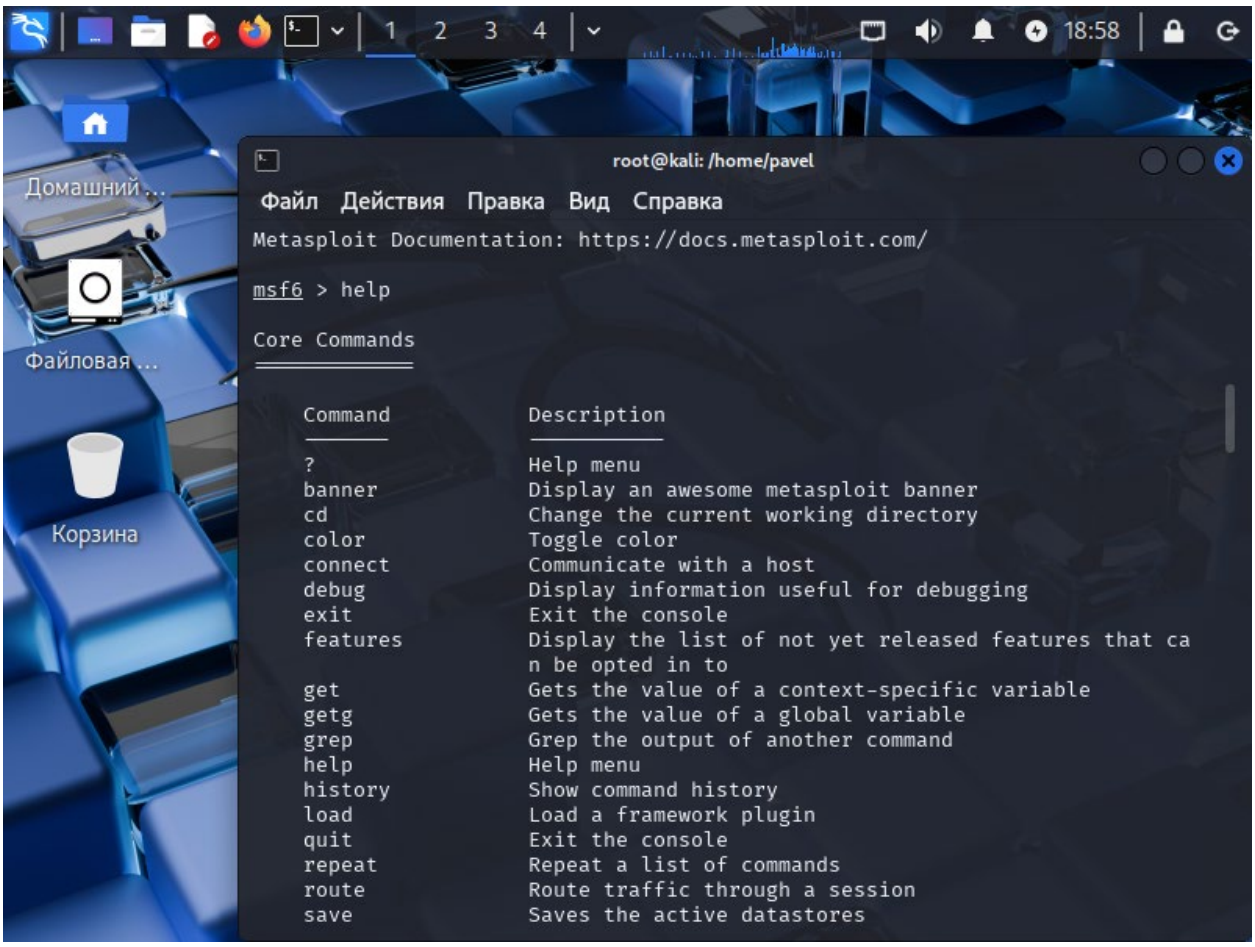
Установлю Kali



Открою интерактивную среду, где буду выполнять команды для тестирования безопасности.



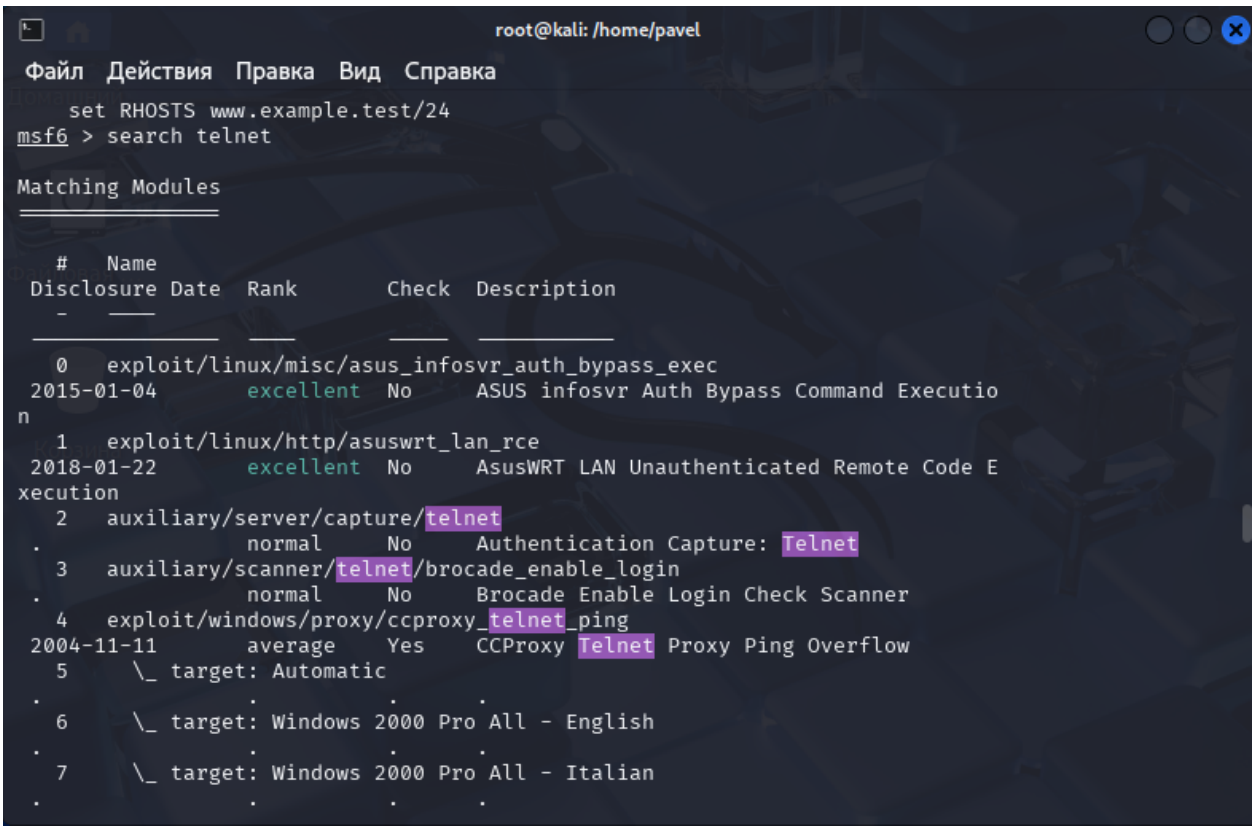
С помощью help можно посмотреть доступные команды



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.

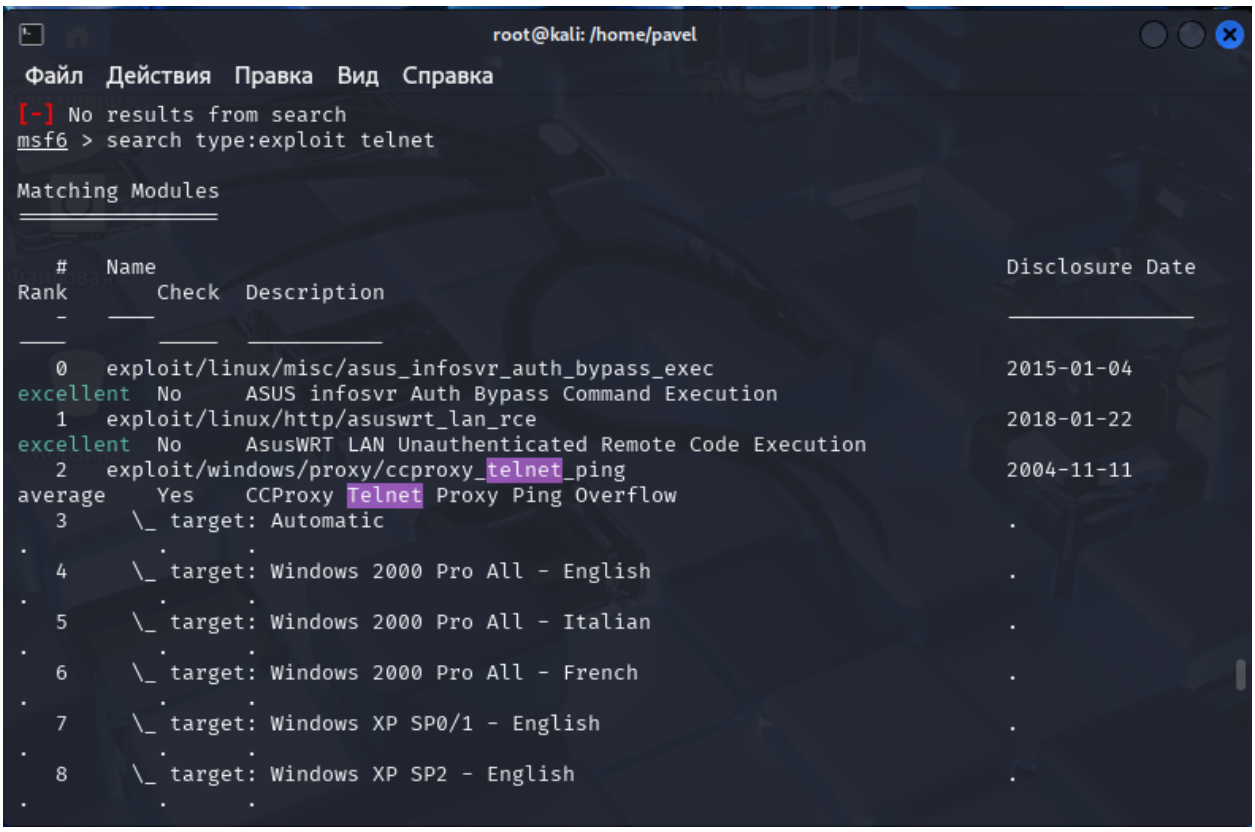
Например, у вас есть браузер, и есть уязвимость в нем, которая позволяет исполнить «произвольный код», то есть установить и запустить некую вредоносную программу на вашей системе без вашего ведома или спровоцировать какое-либо иное не ожидаемое вами поведение системы. Чаще всего первым шагом злоумышленников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

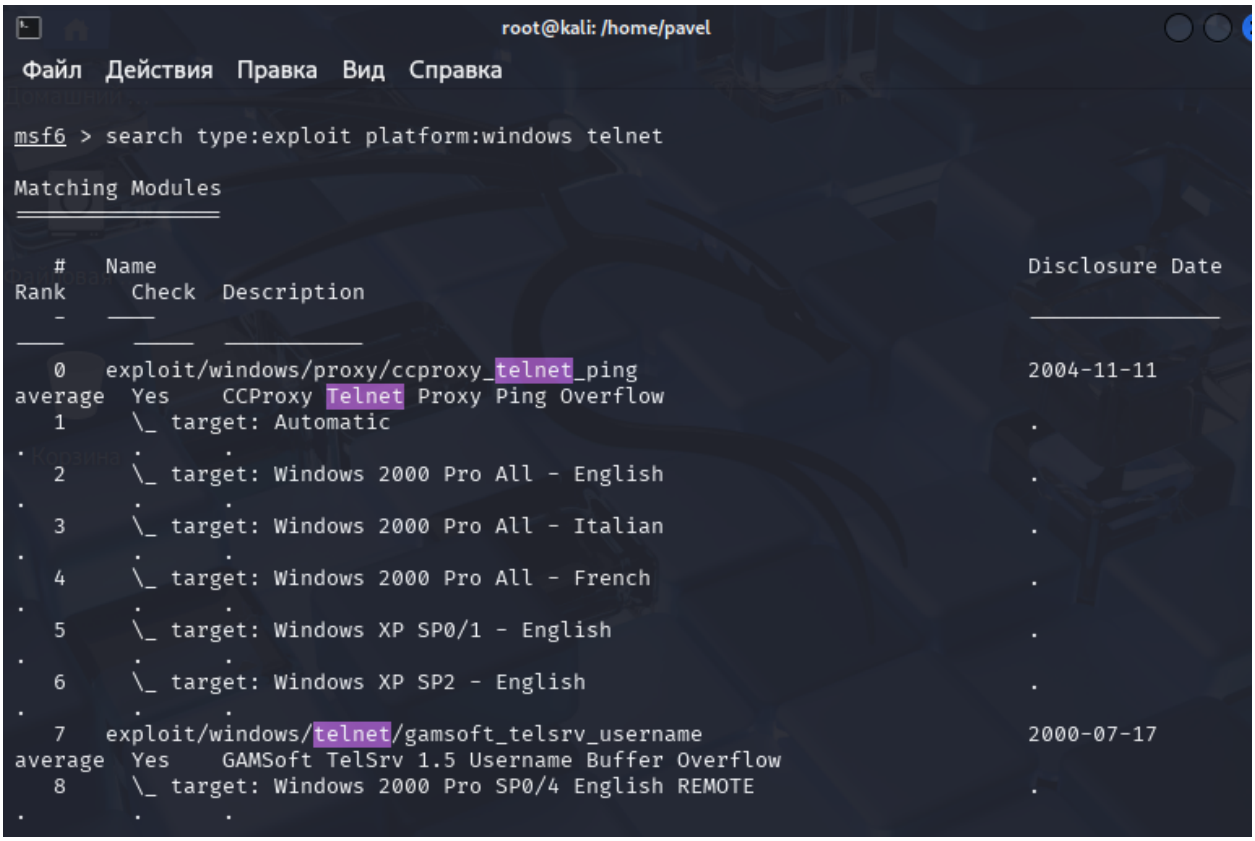


auxiliary модули представляют собой инструменты, которые не являются эксплойтами, но могут выполнять различные вспомогательные функции, такие как сканирование, сбор информации или тестирование на уязвимости. Эти модули помогают исследователям безопасности в процессе анализа и тестирования систем.

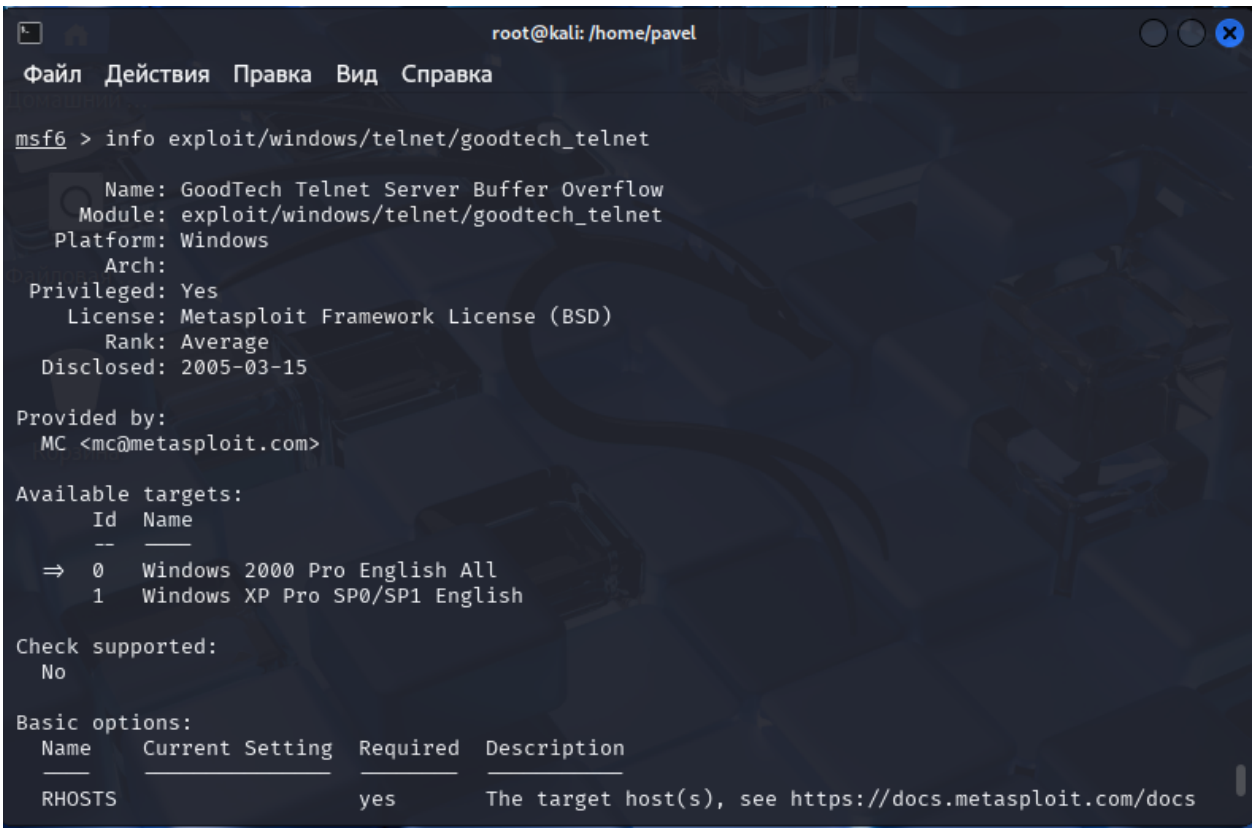
Для того, чтобы искать только эксплоиты, то введу следующую команду:



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



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

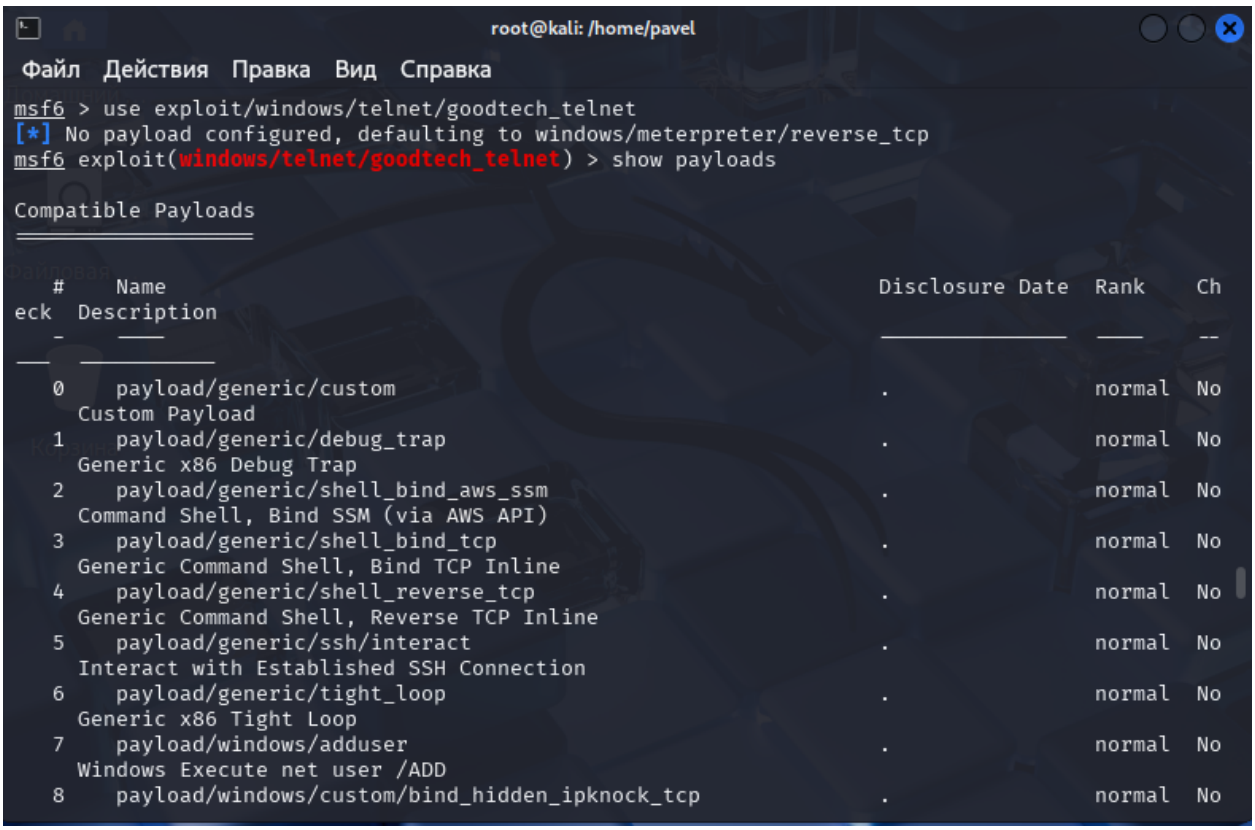


Можно перейти к настройке конкретного эксплойта:

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:

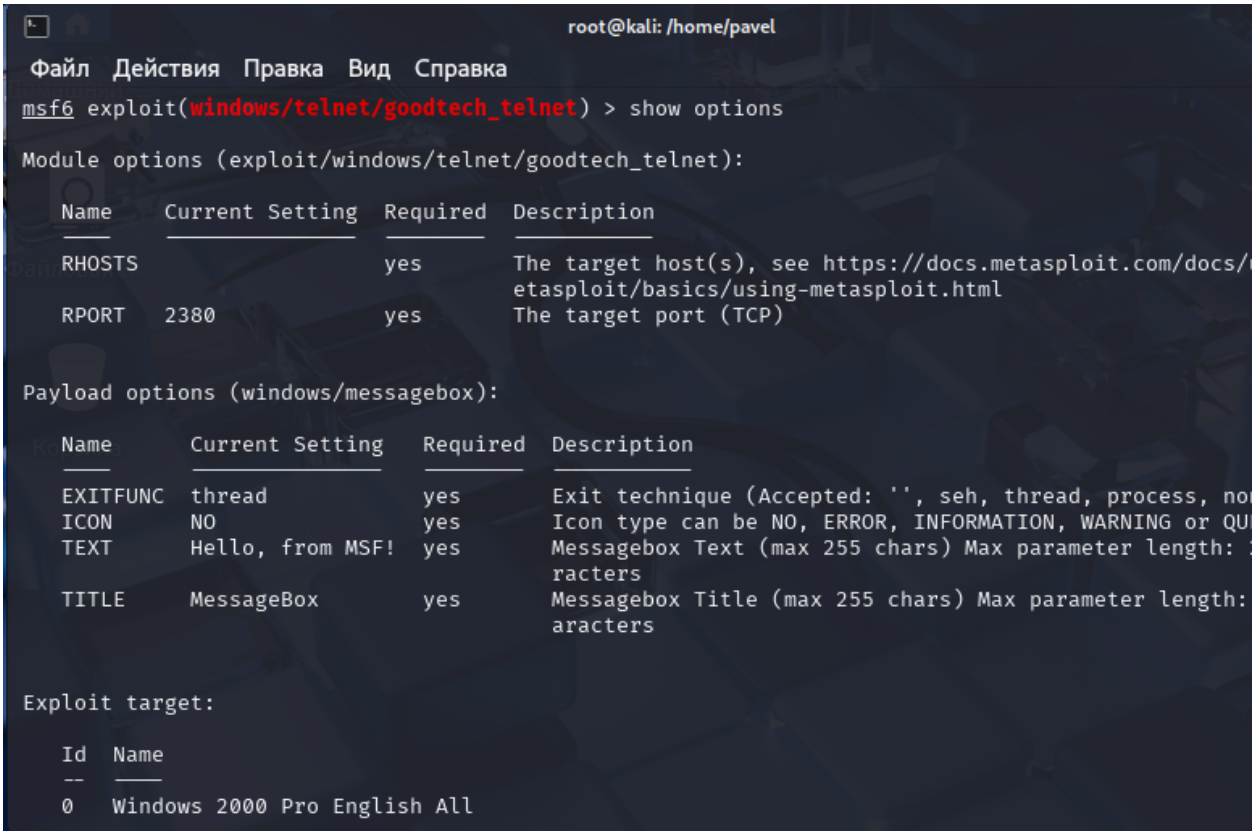


Посмотрю информацию о конкретном пэйлоиде:

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

```
msf6 exploit(windows/telnet/goodtech_telnet) > set payload windows/messagebox
payload ⇒ windows/messagebox
msf6 exploit(windows/telnet/goodtech_telnet) >
```

Теперь можно посмотреть настройки:



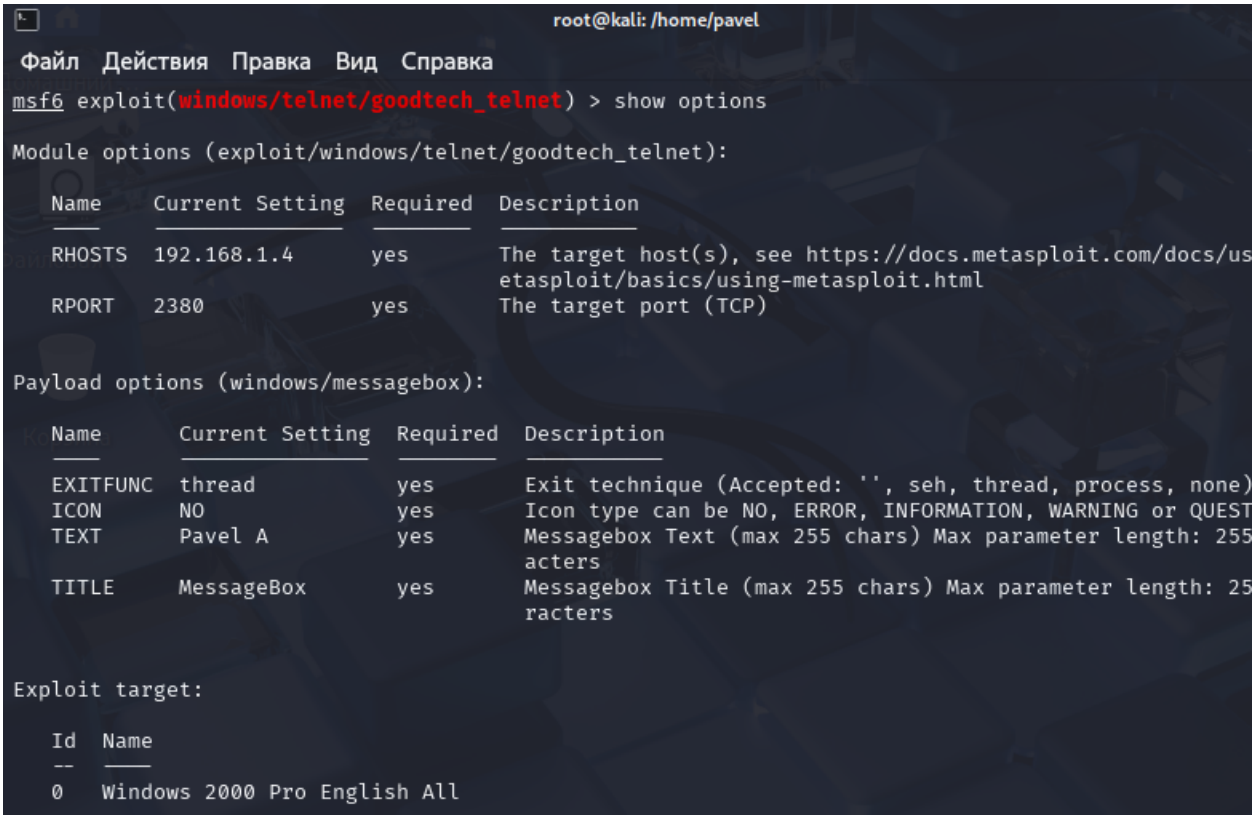
RHOST – IP адрес удалённого хоста.

RPORT – номер порта на удалённой машине

Requred означает обязательно для заполнения.

Необходимо заполнить RHOST. И ещё поменяю текст.

```
msf6 exploit(windows/telnet/goodtech_telnet) > set rhost 192.168.1.4
rhost ⇒ 192.168.1.4
msf6 exploit(windows/telnet/goodtech_telnet) > set text Pavel A
text ⇒ Pavel A
msf6 exploit(windows/telnet/goodtech_telnet) >
```


root@kali: /home/pavel
Файл Действия Правка Вид Справка
msf6 exploit(windows/telnet/goodtech_telnet) > show options
Module options (exploit/windows/telnet/goodtech_telnet):
Name Current Setting Required Description
RHOSTS 192.168.1.4 yes The target host(s), see https://docs.metasploit.com/docs/us
etasploit/basics/using-metasploit.html
RPORT 2380 yes The target port (TCP)
Payload options (windows/messagebox):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
ICON NO yes Icon type can be NO, ERROR, INFORMATION, WARNING or QUEST
TEXT Pavel A yes Messagebox Text (max 255 chars) Max parameter length: 255
acters
TITLE MessageBox yes Messagebox Title (max 255 chars) Max parameter length: 25
racters
Exploit target:
Id Name
0 Windows 2000 Pro English All


[*] Exploit completed, but no session was created.