?????????? ???????

База данных

В Kali запускаем postgresql и инициализируем базу данных. Создадутся базы msf и msf_test.

```
root@kali:~# systemctl start postgresql
root@kali:~# msfdb init
```

Управление данными

db_status	Статус соединения с базой
db_connect	Подключиться к бд. Без параметров - к локальной. Может быть удаленная `db_connect <user:[pass]>@<host:[port]>/<database>`
db_disconnect	Отключение
db_export -f <format> [filename]	Сохранение данных в файл. Формат xml или pwdump
db_import file1 [file2...]	Импорт данных из файла. Может быть импорт в виде *.xml, или **/*.xml
db_rebuild_cache	Пересчет кэша

Рабочее пространство. Способ организации хранения связанных данных.

workspace	Список пространств. * текущее.
workspace -a	Создать новое
workspace <name>	Переключиться на рабочее пространство name
workspace -d	Удалить

Таблицы

hosts	Обнаруженные хосты. IP-адрес, MAC-адрес, имя хоста, ОС, состояние, комментарии

services	Сетевые сервисы. Порт, протокол (TCP/UDP), состояние (open/closed), имя сервиса, версия
vulns	Уязвимости. Название, описание, ссылки, критичность, доказательства
notes	Дополнительная информация о хостах и сервисах. Содержит Различные данные (учетные записи, собранная информация)
loot	Извлеченные данные. Содержит: Хеши паролей, конфигурационные файлы, личные данные
creds	Учетные данные для аутентификации. Содержит: Логины, пароли, хеши, тип аутентификации
workspaces	Разделение проектов/задач
clients	Клиентские системы. Содержит: Данные о браузерах, пользовательских агентах
events	События. Содержит: Действия, выполняемые в рамках тестирования
exploited_hosts	Успешные эксплуатации. Содержит: Данные о взломанных системах
sessions	Открытые сессии. Содержит: Активные соединения с скомпрометированными системами
web_sites	Веб-сайты. Содержит: URL, виртуальные хосты, SSL-информация
web_pages	Веб-страницы. Содержимое страниц, формы, ссылки
web_forms	HTML-формы. Поля форм, методы отправки
web_vulns	XSS, SQLi, и другие веб-уязвимости

Ручное добавление данных: сначала создать объект, затем модифицировать его.

```
msf > hosts -a 192.168.0.1
msf > hosts 192.168.0.1 -m "first node"
msf > hosts

Hosts
=====

address      mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------      ---  ----  -------  ---------  -----  -------  ----  --------
192.168.0.1                                                      first node
```

Как я понял, ручное добавление нечасто используется.

Фильтрация

Ключ -S <term> Например

```
msf > hosts -S 0.1

Hosts
=====

address      mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------      ---  ----  -------  ---------  -----  -------  ----  --------
192.168.0.1                                                      first node
```

При фильтрации важно указывать колонки -c поскольку поиск полнотекстовый.

Использование данных

В свойствах таблицы есть параметр, который можно использовать в инструментах/... Например, в таблице hosts есть параметр RHOSTS.

```
msf > hosts -h
...
OPTIONS:
...
    -R, --rhosts                        Set RHOSTS from the results of the search
...
```

Это означает, что в случае использования в инструментах параметра RHOSTS его можно заполнить данными из БД. Пример запуска инструмента для хостов, отфильтрованных по 127. Параметр -R добавляет данные в параметр RHOSTS.

```
msf > hosts
Hosts
=====
address      mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------      ---  ----  -------  ---------  -----  -------  ----  --------
127.0.0.1
192.168.0.1                                                      first node

msf > use auxiliary/scanner/portscan/tcp

msf auxiliary(scanner/portscan/tcp) > show options
```

```
Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in
milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to
+/- DELAY) in milliseconds.
   PORTS        22               yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                        yes       The target host(s), see
https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   THREADS      1                yes       The number of concurrent threads (max one per host)
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds

msf auxiliary(scanner/portscan/tcp) > hosts -c address -S 127 -R

Hosts
=====

address
-------
127.0.0.1

RHOSTS => 127.0.0.1

msf auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in
milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to
+/- DELAY) in milliseconds.
   PORTS        22               yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS       127.0.0.1        yes       The target host(s), see
https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
```

```
   THREADS      1                yes       The number of concurrent threads (max one per host)
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds


View the full module info with the info, or info -d command.

msf auxiliary(scanner/portscan/tcp) > run
[*] 127.0.0.1             - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Сохранение данных в CSV

```
msf > hosts -S Linux -o /root/msfu/linux.csv
```

Архивация и восстановление данных

Архив:

```
# B msfconsole
db_export -f xml full_backup.xml
# или
db_export -f json full_backup.json
```

Восстановление:

```
db_import full_backup.xml
```

Revision #6
Created 1 October 2025 04:23:19 by Admin
Updated 6 October 2025 05:07:22 by Admin