Основы построения защищенных компьютерных сетей

Лекция 3.2
Metasploit

Семён Новосёлов

2021

Что нам потребуется?

- VirtualBox
  https://www.virtualbox.org/
- Metasploitable 2
  https://sourceforge.net/projects/metasploitable/
- Metasploit
  https://www.metasploit.com/
- Nmap
  https://nmap.org/

есть в составе Kali Linux
https://www.kali.org/get-kali/

Metasploit Framework

- Фреймворк для проведения тестовых вторжений и разработки эксплойтов
- Разработчик: Rapid7
- Есть две версии:
  - консольная
  - Web-интерфейс (Pro)

www.metasploit.com

Запуск:
msfconsole

Модули Metasploit

exploits — модули для эксплуатации уязвимостей

auxiliary — модули для сбора информации, сканеры, ...

payload — полезная нагрузка эксплойтов

post — модули для постэксплуатации (сбор логинов, паролей, хешей, …)

Поиск/использование/настройка:
search [ключевое_слово]
use [модуль]
show options
set [опция] [значение]
run

Порядок работы

1. Разведка: Сканирование целевой сети или хоста
   - модули из раздела auxiliary
   - сканер Nmap (команда db_nmap)
2. Выбор и настройка эксплойта:
   - поиск и выбор подходящих модулей: search / use
   - установка настроек: show options / set
3. Запуск эксплойта
4. Постэксплуатация
   - выполнение команд на цели
   - вытаскивание данных из цели (модули post)

База данных MSF

- Используется для хранения результатов работы модулей (обычно postgresql)
  - хосты, информация о версиях ПО на них
  - подобранные пароли и т.д.

Первый запуск

```
service postgresql start
msfdb init
msfconsole
db_status
```

Последующие запуски

```
service postgresql start
msfconsole
db_status
```

Работа с базой данных

db_nmap сканирование сети с помощью nmap и запись результатов в базу

creds вывод ключевой информации (логины, пароли, хэши, …)

loot собранная информация (дампы баз, пользовательская история и т.п.)

hosts список хостов

services список сервисов их версий

vulns найденные уязвимости

notes заметки (остальная полезная информация)

Аудит виртуальной машины с Metasploitable

Metasploitable 2
https://sourceforge.net/projects/metasploitable/

Специализированная виртуальная машина для тренировки проведения тестовых вторжений.

Справка: Команды msfconsole

Общие команды

`help, quit, exit`
`set/setg` установка параметров
`show` вывод списка модулей и опций
`show exploits, show payloads, ...`
`reload_all` обновить список модулей

`>` нераспознанные команды передаются в ОС

Использование модулей

`search` поиск модулей по ключевым словам
`use` загрузка модуля
`use exploit/unix/ftp/vsftpd_234_backdoor`
`show options` вывод опций модуля
`show payloads` вывод поддерживаемой целевой нагрузки
`show targets` вывод поддерживаемых целей
`edit` редактирование исходного кода модуля в редакторе
`info` вывод информации о модуле
`check` проверка цели на уязвимость без использования
`run` запуск модуля на выполнение