Отчет по лабораторной работе №5 : Инструмент тестов на проникновение metasploit

Дедков Сергей

2015

Содержание

1 Цель работы

Изучить варианты использования metasploit.

2 Ход работы, теория

2.1 Используя документацию изучить основные понятия auxiliary, payload, exploit, shellcode, nop, encoder

- auxiliary - сканер, который использует уязвимости системы, для полкучения сведений о это системе.

- payload - полезная нагрузка - в компьютерной безопасности относится к той части вредоносных программ, который выполняет вредоносные действия. При анализе вредоносных программ, таких как черви, вирусы и троянские программы, это относится к вредным результатам данного программного обеспечения. Примеры полезных нагрузок включают разрушение данных, сообщений оскорбительного текста или ложных сообщений электронной почты, отправляемых с большим количеством людей. Таким образом, полезная нагрузка относится к фактическому назначению сообщение в коробке передач.

- exploit (англ. exploit — использовать) - это общий термин в сообществе компьютерной безопасности для обозначения фрагмента программного кода который, используя возможности предоставляемые ошибкой, отказом или уязвимостью, ведёт к повышению привилегий или отказу в обслуживании компьютерной системы.

- shellcode (англ. shellcode - код оболочки) - это двоичный исполняемый код, который обычно передаёт управление консоли, например `'/bin/sh'` Unix shell, command.com в MS-DOS и cmd.exe в операционных системах Microsoft Windows. Код оболочки может быть использован как полезная нагрузка эксплойта, обеспечивая взломщику доступ к командной оболочке (англ. shell) в компьютерной системе.

- nop (сокращение от англ.: «No OPeration») - инструкция процессора на языке ассемблера, или команда протокола, которая предписывает ничего не делать.

- encoder - это устройство преобразующее линейное или угловое перемещение в последовательность сигналов, позволяющих определить величину перемещения. Т.о. можно выделить линейные и поворотные энкодеры.

2.2 Запуск msfconsole

Запустим msfconsole и узнаем список допустимых команд (help).

При вводе команды help, можно посмотреть список доступных команд. Перечислять все не имеет смысле, какие-то описаны ниже, а какие-то мы уже знаем.

Фреймворк Metasploit обладает тремя рабочими окружениями: msfconsole, msfcli и msfweb. Основным и наиболее предпочтительным из трех перечисленных вариантов является первый - msfconsole. Это окружение представляет из себя эффективный интерфейс командной строки со своим собственным набором команд и системным окружением.

2.3 Базовые команды

Базовыми командами являются search (поиск по имени, типу, автору и др.), info, load, use.

- search <keyword> - запустив команду search без указания ключевых слов, выводится список всех доступных эксплоитов. Если значение <keyword> имеет имя определенного сплоита, то этой командой ищем такой в базе данных системы.
- info <type> <name> - если нужна конкретная и полная информация о каком-либо эксплоите или payload'е, можно применить команду info. Например, нужно подробное описание payload'а winbind. Тогда необходимо набрать в командной строке info payload winbind и получить справочную информацию по нему.
- load - команда используется для загрузки плагинов.
- use <exploit_name> - команда говорит Фреймворку Metasploi запустить эксплоит с указанным конкретным именем

2.4 Команды по работе с эксплоитом

Для работы с эксплоитом используются следующие команды:

- show exploits - указав команду show exploits, получим список всех доступных на данный момент эксплоитов. Имеются версии последних под различные платформы и приложения, включая Windows, Linux, IIS, Apache и так далее. Это поможет понять работу фреймворка Metasploit и почувствовать его гибкость и эффективность.
- show options - набрав в командной строке show options, будет выведет список опций, которые можно использовать. Каждый эксплоит или payload имеет свой собственный набор опций, который можно использовать при работе с ними.

- exploit - запускает эксплоит. Есть другая версия этой команды - rexploit, которая перезагружает код запущенного эксплоита и запускает его вновь. Эти две команды помогают работать с эксплоитами с минимальными усилиями, без перезапуска консоли.
- set RHOST <hostname_or_ip> - указываем этой командой Metasploit определенный хост в сети для его изучения. Хост можно задать как по его имени, так и по IP-адресу.
- set RPORT <host_port> - задает для Metasploit порт удаленной машины, по которому фреймворк должен подключиться к указанному хосту
- set payload <generic/shell_bind_tcp> - команда указывает имя payload'a, который будет использоваться.
- set LPORT <local_port> - задаем номер порта для payload'a на сервере, на котором был выполнен эксплоит. Это важно, так как номер этого порта открыт именно на сервере (он не может быть использован никакими другими службами этого сервера и не резервируется для административных нужд). Советую назначать такой номер из набора четырех случайных цифр, порядок которых начинается с 1024. И тогда у вас все будет хорошо. Также стоит упомянуть, что необходимо менять номер порта каждый раз, когда успешно запущен эксплоит на удаленной машине.

2.5 Команды по работе с БД

- db_connect - подключение к базе данных.
- db_status - проверка состояния базы данных.
- db_host - просмотр списка хостов в файле базы данных.
- db_del_host - удалить какой-либо хост из базы данных.

2.6 GUI оболочка Armitage

Графическая оболочка для набора утилит и библиотеки эксплоитов Metasploit. Armitage позволяет в наглядном виде представить все этапы атаки, включая: сканирование узлов сети, анализ защищенности обнаруженных ресурсов, выполнение эксплоитов и получение полного контроля над уязвимой системой. Все функции программы структурированы и легкодоступны из меню и вкладок программы, даже для начинающего исследователя компьютерной безопасности.

Запустим и протестируем работу Armitage. Укажем начальные параметры, как на рисунке 1. Далее жмем Connect.

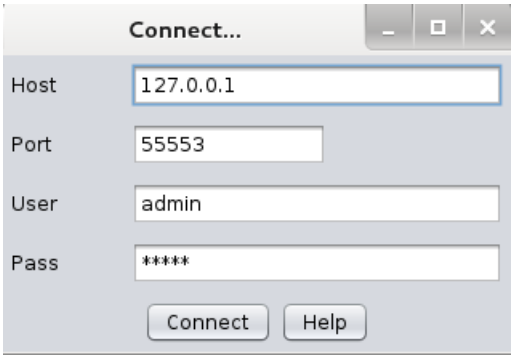

Рис. 1: Настройки подключения к armitage

После запуска введем ip атакуемой машины. Проведем эксперимент из пункта 2.2.1. Для этого в боковом меню найдем необходимую auxiliary (vnc_login) и укажем настройки. Далее нажимаем Launch. Результат выполнения успешен и представлен на рисунке 2.

2.7 GUI веб-клиент

3 Ход работы, практика

3.1 Подключиться к VNC-серверу, получить доступ к консоли

- Просканируем порты на гостевой ОС metasploitable2 Введем команду: `nmap 192.168.150.3 -sV`

  Откуда видно, что VNC сервер работает с портом 5900 и название сервиса - VNC (protocol 3.3)(см. рисунок 3)

- В msfconsole воспользуемся командой `search "VNC (protocol 3.3)"`

  Как видно из рисунка 4 присутствуем много эксплоитов. По каждому можно получить информацию командой `info <exploit_name>`

- Воспользуемся `auxiliary/scanner/vnc/vnc_login`

  Для этого введем команду `use auxiliary/scanner/vnc/vnc_login`

  Установим необходимые параметры `set RHOSTS 192.168.150.3`

  Запустим exploit - `exploit`

  Реузльтат на рисунке 5.

- Теперь, зная пароль запустим vncviewer

  Команда: `vncviewer 192.168.150.3:5900`

  Результат а рисунке 6

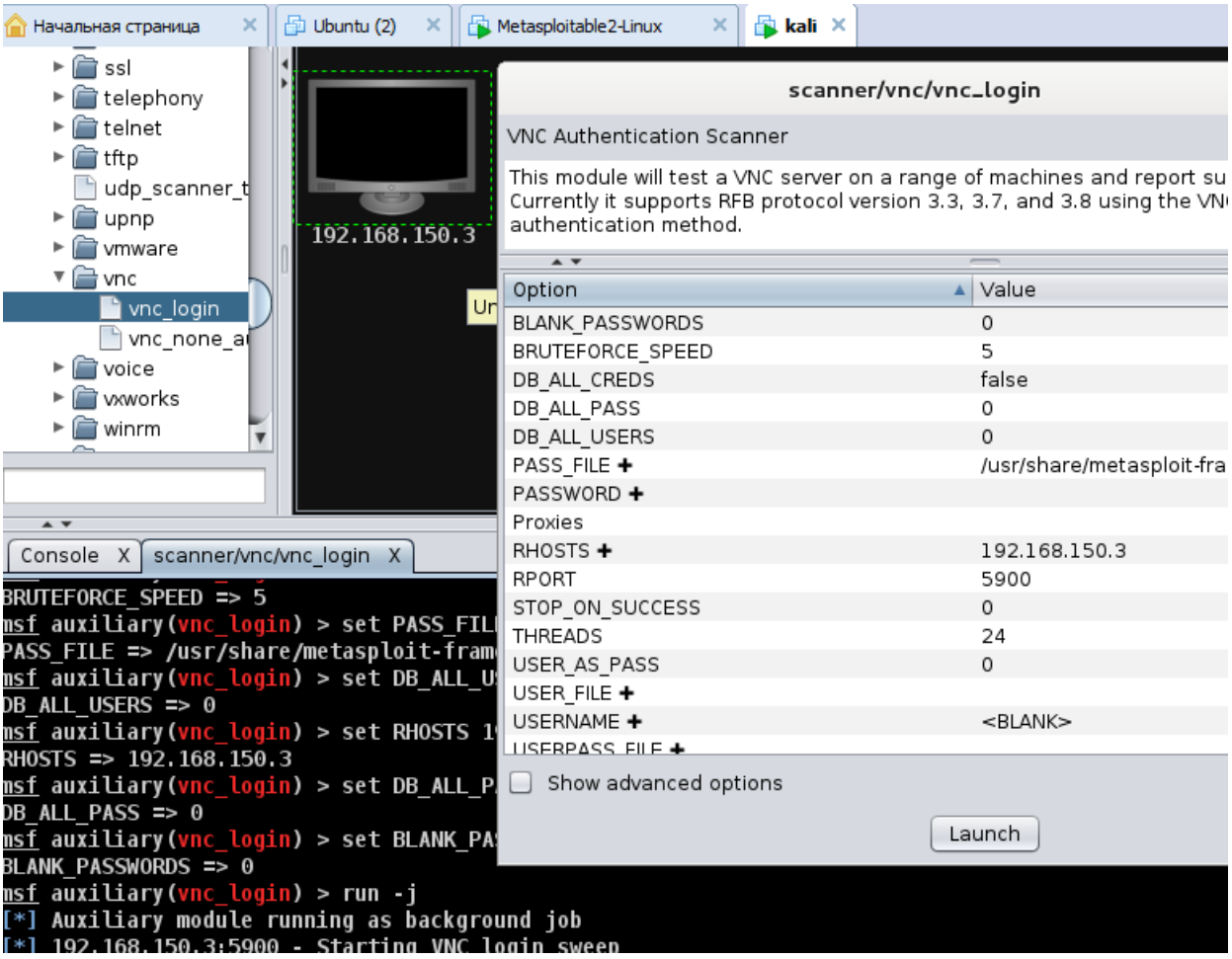

Рис. 2: Настройки подключения к armitage

Рис. 3: Поиск vnc сервиса

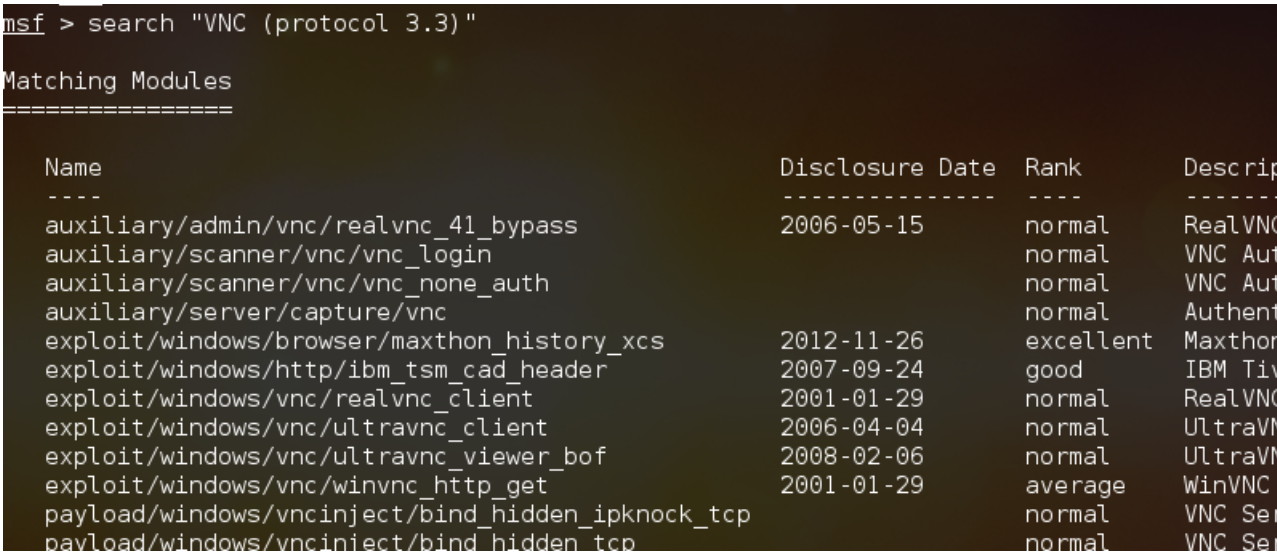

Рис. 4: Поиск эксплоитов vnc

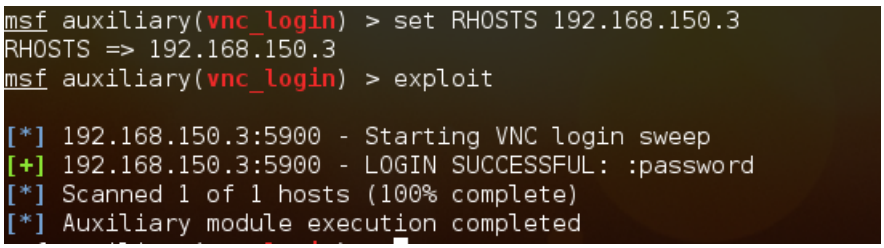

Рис. 5: vnc exploit

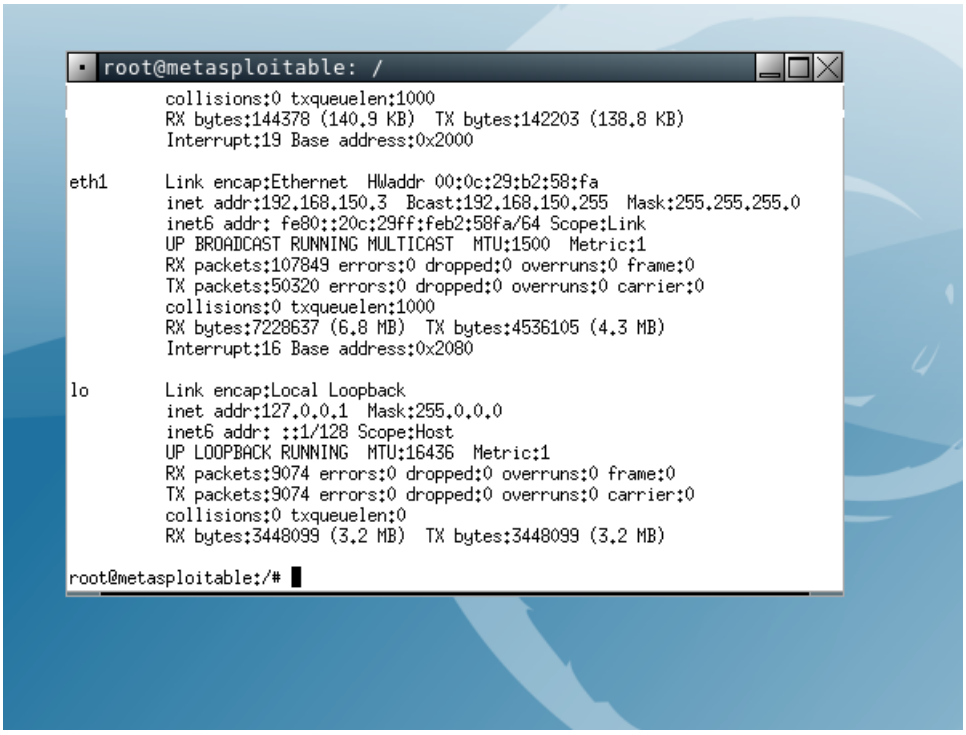

Рис. 6: vncviewer