

Ex. 7 & 8 - Penetration Testing - Metasploit

CSE3501 ISAA Lab - Week 7 & 8

FACULTY : Dr.Parkavi

NAME: P.NITYASREE

REGNO: 17MIS1007

Upload your document containing Metasploit Use to perform Penetration Testing, with all the options covered in the lab.

1) The ls command

```
msf5 > ls
[*] exec: ls

Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
msf5 > 
```

2) START COMMAND


```
msf5 > service postgresql start
[*] exec: service postgresql start

msf5 > service postgresql status
[*] exec: service postgresql status

• postgresql.service - PostgreSQL RDBMS
  Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; ver
  Active: active (exited) since Thu 2020-09-10 04:42:59 EDT; 37min ago
  Process: 1331 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
  Main PID: 1331 (code=exited, status=0/SUCCESS)

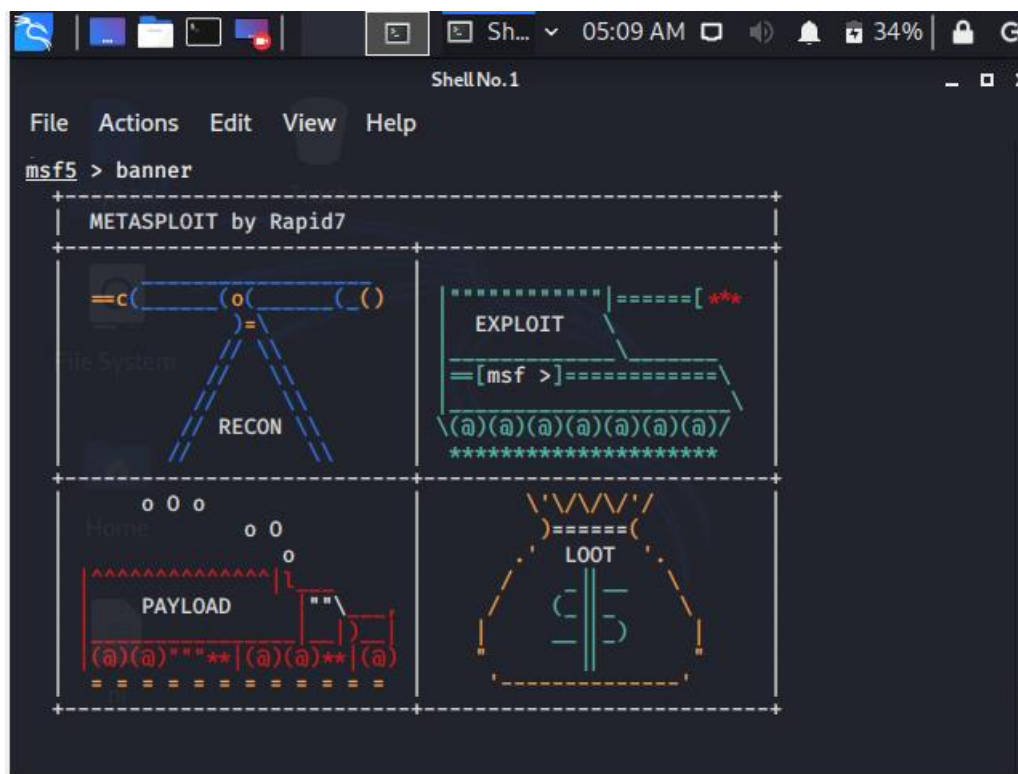
Sep 10 04:42:59 kali systemd[1]: Starting PostgreSQL RDBMS...
Sep 10 04:42:59 kali systemd[1]: Finished PostgreSQL RDBMS.
lines 1-8/8 (END)
```

```
ShellNo.1
File Actions Edit View Help
elp to learn more
msf5 > Interrupt: use the 'exit' command to quit
msf5 > Interrupt: use the 'exit' command to quit
msf5 > exit
root@kali:~# msfconsole
```



```
ShellNo.1
File Actions Edit View Help
+ -- --=[ metasploit v5.0.87-dev ]
+ -- --=[ 2006 exploits - 1096 auxiliary - 343 post ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops ]
+ -- --=[ 7 evasion ]

Metasploit tip: Writing a custom module? After editing your module, why not
try the reload command
msf5 > 
```



3) ALL THE BANNER AND VERSION COMMANDS

```
msf5 > version
Framework: 5.0.87-dev
Console : 5.0.87-dev
msf5 > 
```

```
msf5 > db_
db_connect      db_import      db_remove
db_disconnect   db_nmap        db_save
db_export       db_rebuild_cache db_status
msf5 > db_
```

```
msf5 > db_
db_connect      db_import      db_remove
db_disconnect   db_nmap        db_save
db_export       db_rebuild_cache db_status
msf5 > db_status
[*] Connected to msf. Connection type: postgresql.
msf5 > sessions
```

```
Active sessions
=====
No active sessions.
```

4) THE REVERSE_TCP COMMAND

```
msf5 > info payload/windows/meterpreter/reverse_tcp

Name: Windows Meterpreter (Reflective Injection), Reverse TCP Stager
Module: payload/windows/meterpreter/reverse_tcp
Platform: Windows
Arch: x86
Needs Admin: No
Total size: 283
Rank: Normal

Provided by:
skape <mmiller@hick.org>
sf <stephen_fewer@harmonysecurity.com>
OJ Reeves
hdm <x@hdm.io>

Basic options:
Name      Current Setting  Required  Description
-----
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thr
```

```
Provided by:
skape <mmiller@hick.org>
sf <stephen_fewer@harmonysecurity.com>
OJ Reeves
hdm <x@hdm.io>

Basic options:
Name      Current Setting  Required  Description
-----
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thr
ead, process, none)
LHOST      e specified)      yes       The listen address (an interface may b
LPORT      4444              yes       The listen port

Description:
Inject the meterpreter server DLL via the Reflective DLL Injection
payload (staged). Connect back to the attacker
```

6) THE FRAMEWORK COMMAND

Metasploit tip: Display the Framework log using the `log` command, learn more with `help log`

```
msf5 > use auxiliary/scanner/portscan/tcp
msf5 auxiliary(scanner/portscan/tcp) > show options
```

Module options (auxiliary/scanner/portscan/tcp):

Name	Current Setting	Required	Description
CONCURRENCY	10	yes	The number of concurrent ports to check per host
DELAY	0	yes	The delay between connections, per thread, in milliseconds
JITTER	0	yes	The delay jitter factor (maximum value by which to increase or decrease DELAY)
PORTS	1-10000	yes	Ports to scan (e.g. 22-25,80,110-900)
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
THREADS	1	yes	The number of concurrent threads (max one per host)
TIMEOUT	1000	yes	The socket connect timeout in milliseconds

```
msf5 > show options
-- --=[ metasploit v5.0.87-dev ]
-- --=[ 2006 exploits - 1096 auxiliary - 343 post ]
-- --=[ 562 payloads - 45 encoders - 10 nops ]
-- --=[ 7 evasion ]
```

Metasploit tip: You can use `help` to view all available commands

```
msf5 >
msf5 > use auxiliary/scanner/portscan/tcp
msf5 auxiliary(scanner/portscan/tcp) > set RHOSTS 157.48.161.80
RHOSTS => 157.48.161.80
msf5 auxiliary(scanner/portscan/tcp) > set threads 4
threads => 4
msf5 auxiliary(scanner/portscan/tcp) > run
```

7) THREADS ,RHOSTS COMMAND AND RUN COMMAND

```
File Actions Edit View Help
64 bytes from bom07s20-in-f4.1e100.net (172.217.166.164): icmp_seq=77 ttl=1
11 time=69.5 ms
64 bytes from bom07s20-in-f4.1e100.net (172.217.166.164): icmp_seq=78 ttl=1
11 time=77.2 ms
64 bytes from bom07s20-in-f4.1e100.net (172.217.166.164): icmp_seq=79 ttl=1
11 time=105 ms
64 bytes from bom07s20-in-f4.1e100.net (172.217.166.164): icmp_seq=80 ttl=1
11 time=72.7 ms
64 bytes from bom07s20-in-f4.1e100.net (172.217.166.164): icmp_seq=81 ttl=1
11 time=70.8 ms
64 bytes from bom07s20-in-f4.1e100.net (172.217.166.164): icmp_seq=82 ttl=1
11 time=64.5 ms
64 bytes from bom07s20-in-f4.1e100.net (172.217.166.164): icmp_seq=83 ttl=1
11 time=76.7 ms
64 bytes from bom07s20-in-f4.1e100.net (172.217.166.164): icmp_seq=84 ttl=1
11 time=75.3 ms
64 bytes from bom07s20-in-f4.1e100.net (172.217.166.164): icmp_seq=85 ttl=1
11 time=78.8 ms
64 bytes from bom07s20-in-f4.1e100.net (172.217.166.164): icmp_seq=86 ttl=1
11 time=72.1 ms
64 bytes from bom07s20-in-f4.1e100.net (172.217.166.164): icmp_seq=87 ttl=1
11 time=60.7 ms
```

```
Actions Edit View Help
thread, in milliseconds
JITTER 0 yes The delay jitter factor
value by which to +/- DELAY) in milliseconds.
PORTS 1-10000 yes Ports to scan (e.g. 2000)
RHOSTS 192.168.1.5 yes The target host(s), n
ntifier, or hosts file with syntax 'file:<path>'
THREADS 1 yes The number of concurr
(max one per host)
TIMEOUT 1000 yes The socket connect ti
liseconds

msf5 auxiliary(scanner/portscan/tcp) > set threads 5
threads => 5
msf5 auxiliary(scanner/portscan/tcp) > run

^Z
[11]+ Stopped msfconsole
root@kali:~# ping 192.168.1.5
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data.
^Z
[12]+ Stopped ping 192.168.1.5
root@kali:~#
```