**Lab - Windows 7 Privilege Escalation Using UAC Bypass**

**Overview**

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

**Lab Requirements**

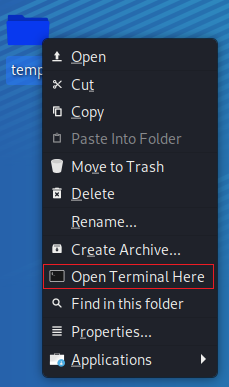
* One virtual install of Kali Linux.
* One virtual Install of Windows 7 Pro.
* An established Meterpreter session with your Windows 7 target.

**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,

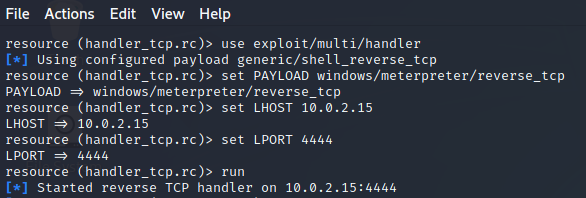
select **Open Terminal Here**.



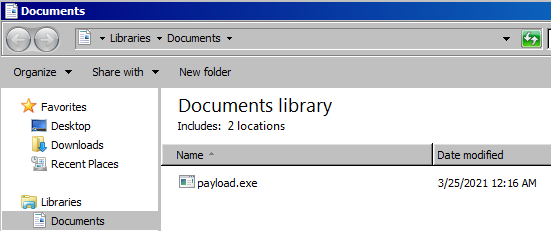
Use your meterpreter script to create a listener. At the terminal prompt, type:

msfconsole -r handler\_tcp.rc

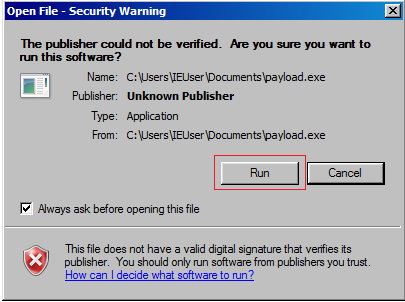
If the script completes successfully, your kali should be standing by for communication from your Windows 7 Pro machine when you launch the payload.exe.



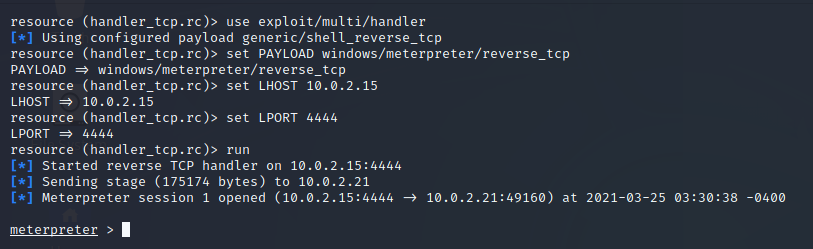
Return to your Windows 7 Pro machine. Open the Documents folder and 2X click the payload.exe file.



When prompt, click the Run button.

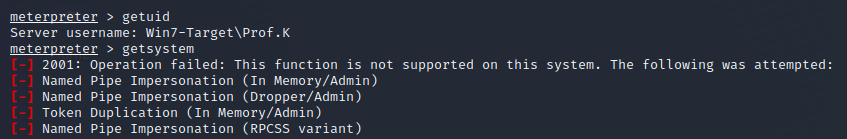


Return to your Kali terminal, and you should see a Meterpreter prompt.



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

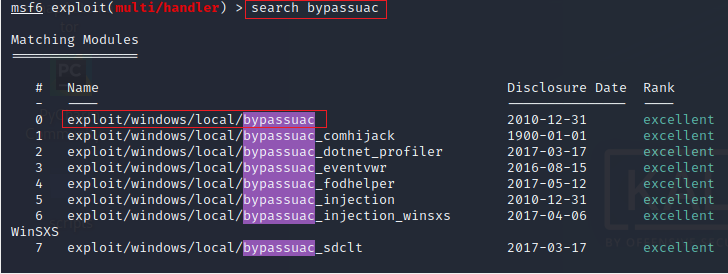
The getuid function returns the real user ID of the calling process. We can try and escalate our privileges using the **getsystem** command, but this operation fails as the command is not supported.

****

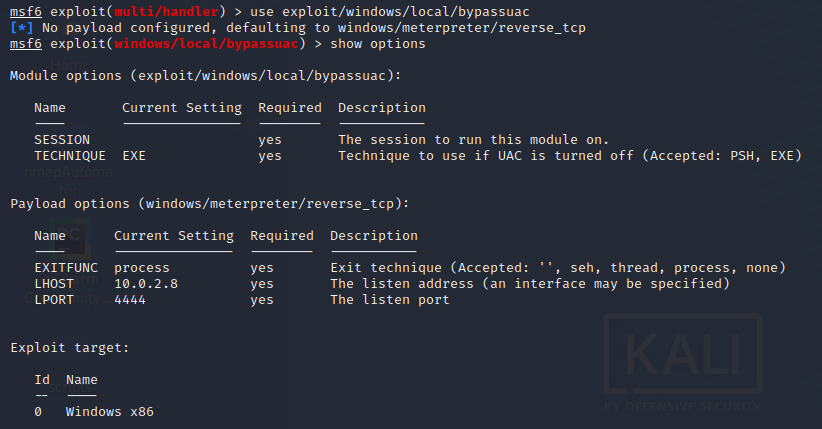
We need to bypass the UAC to get escalated privileges. To do this, we first need to background our current Meterpreter session. We do this by typing **background** at the prompt. Once the session has been background, we need to search for a UAC bypass exploit.



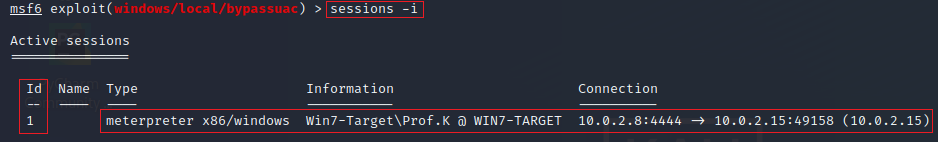
At the prompt, type, **search bypassuac**.



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

****

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

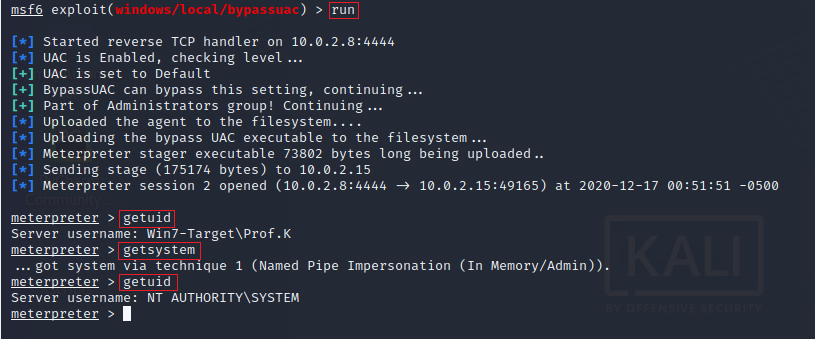


From the results, we know that our Metrepreter session is using the session ID of 1.

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



At the prompt, type run.



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!