PSP0201 Week 6 Writeup

Group Name: Undecided

Members:

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha binti Muhd Firdaus	Member

Day 21 : Blue Teaming – Time for some ELForensics

Tools used: Kali Linux, Remmina, Firefox

Solution/walkthrough:

To start the task, we first connected to the server provided with the credentials for the user account.

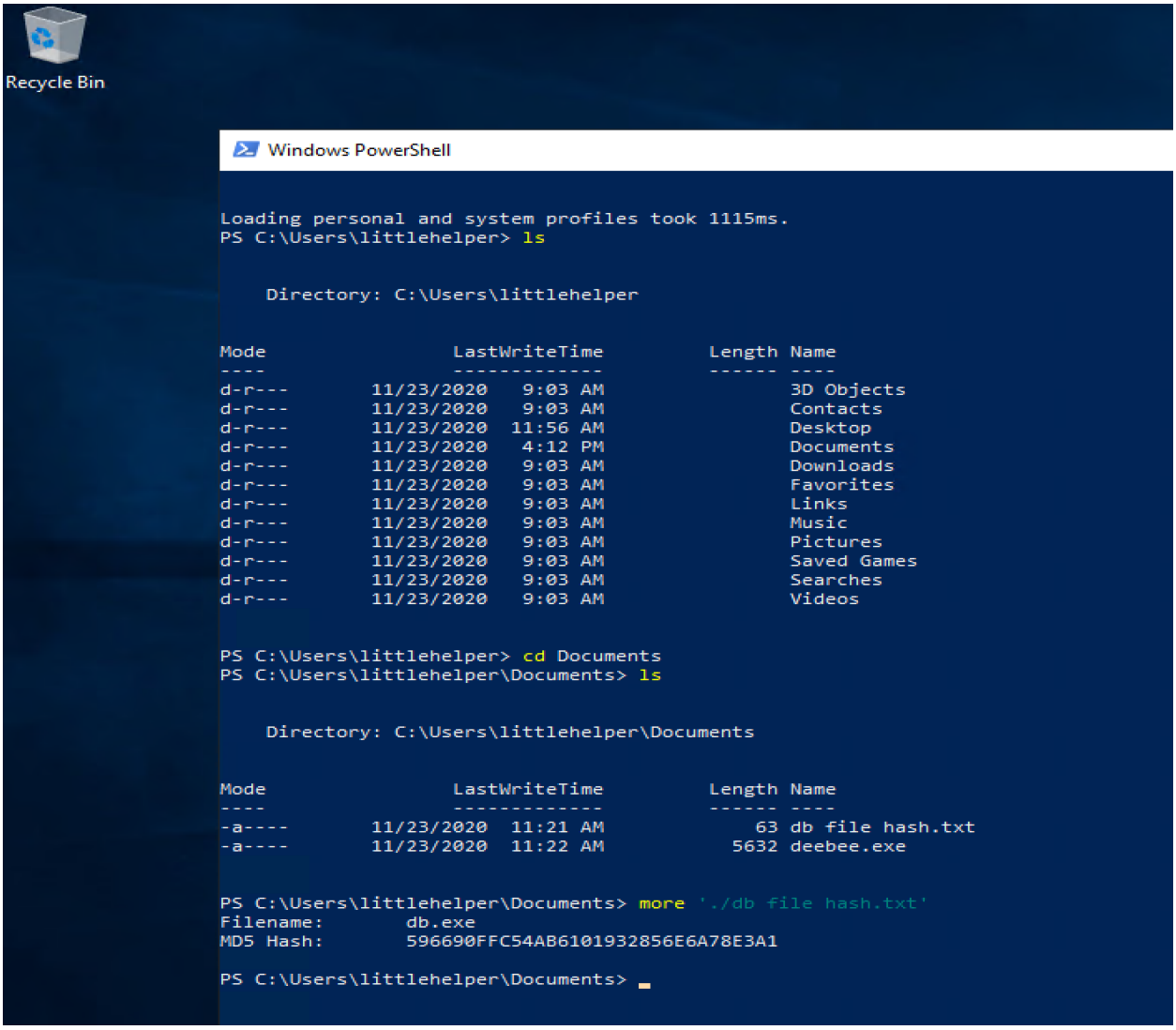
User name: littlehelper

User password: iLove5now!

Using the credentials given, we accepted the certificate and logged into the remote system.

Question 1

At first, we were asked to find the file hash. After logging in and opening PowerShell, we tried to find the file in the document folder. After that, using the code, we found the file hash as shown below.



Question 2

After that we need to find the MD5 file hash of that mysterious file named deebee.exe. So, we executed the hash file by command Get-FileHash -Algorithm MD5 ./deebee.exe and we found this.

```
PS C:\Users\littlehelper\Documents> more './db file hash.txt'
Filename:       db.exe
MD5 Hash:       596690FFC54AB6101932856E6A78E3A1

PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm MD5 ./deebee.exe

Algorithm       Hash                                                                   P
---------       ----                                                                   -
MD5             5F037501FB542AD2D9B06EB12AED09F0                                       C
```

Question 3

As an extra question for learning purpose, we need to find the SHA256 file hash for this file. So, we just changed the MD5 to SHA256 and found a new hash.

```
PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm SHA256 ./deebee.exe

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED       C:\Users\littlehelper\Documents\deebee.exe
```

Question 4

Now we need to find the flag using tool strong, we executed the command C:\Tools\Strongs64.exe -accepteula ./deebee.exe and found this.

```
PS C:\Users\littlehelper\Documents> c:\Tools\strings64.exe -accepteula ./deebee.exe

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
```

Here in the lower part of the printed part we got the flag which we were asked to find.

```
System
Main
System.Reflection
Sleep
Clear
.ctor
System.Diagnostics
System.Runtime.InteropServices
System.Runtime.CompilerServices
DebuggingModes
args
Object
Accessing the Best Festival Company Database...
Done.
Using SSO to log in user...
Loading menu, standby...
THM{f6187e6cbeb1214139ef313e108cb6f9}
Set-Content -Path .\lists.exe -value $(Get-Content $(Get-Command C:\Users\littlehelper\Documents\db.exe).Path -ReadCount 0 -Enc
Hahaha .. guess what?
Your database connector file has been moved and you'll never find it!
I guess you can't query the naughty list anymore!
>;^P
```

Question 5

The PowerShell command to view ADS is: wmic process call create $(Resolve-Path .\deebee.exe:hidedb), but for this we needed to find the stream name. Thus, to find it, we used another command `Get-Item -Path ./deebee.exe -Stream *`

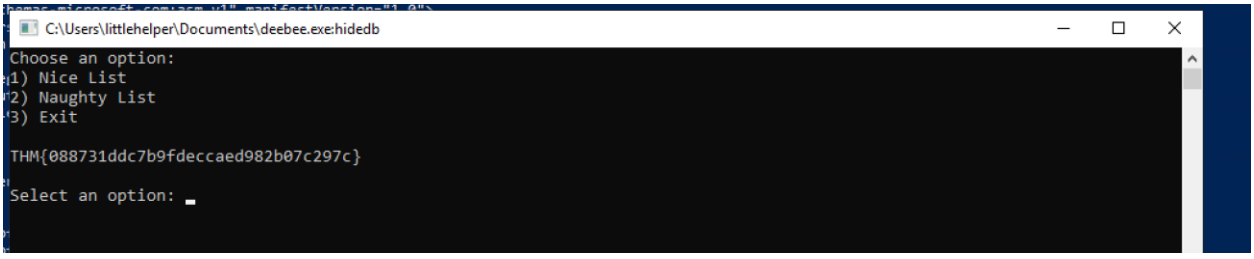
```
PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebee.exe::$DATA
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents
PSChildName   : deebee.exe::$DATA
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\littlehelper\Documents\deebee.exe
Stream        : :$DATA
Length        : 5632

PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebee.exe:hidedb
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents
PSChildName   : deebee.exe:hidedb
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\littlehelper\Documents\deebee.exe
Stream        : hidedb
Length        : 6144
```

```
PS C:\Users\littlehelper\Documents> wmic process call create $(Resolve-Path .\deebee.exe:hidedb)
Executing (Win32_Process)->Create()
```

Question 6

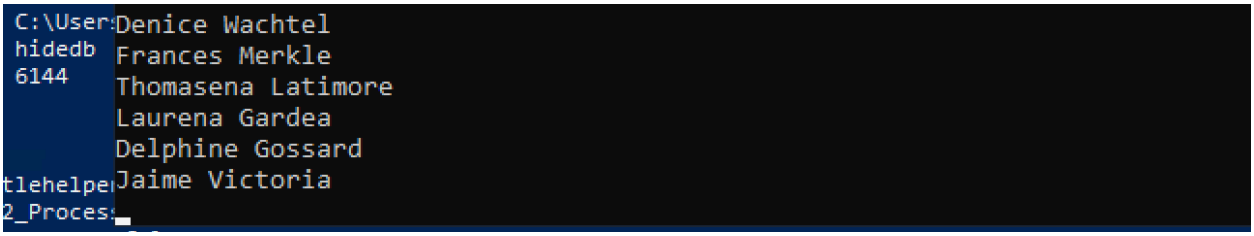
After executing the ADS view command, a new page opens, and we waited a while for it to fully load. After that, we can see the flag as shown below.



Question 7 & 8

In the question above we can see the list of things we can do with the database.

So, we printed the Nice List and the Naughty List respectively (1&2).



Note: Sharika Spooner is in the Naughty List and Jaime Victoria is the in the Nice List.

Thought Process/Methodology:

At first, using the login credentials, we logged into the system with the help of Remmina. After logging in we opened PowerShell on the remote machine and searched for the files in Documents. We needed to print the file hash of the first file. With the command: more './db file hash.txt' and command: Get-FileHash -Algorithm MD5 ./deebee.exe, we found the file hash of the mysterious named file. To find the SHA256 file hash, we just changed the MD5 keyword to SHA256. Then, using the String Tool, we found the first flag using the command: C:\Tools\Strongs64.exe -accepteula ./deebee.exe. In order to find the main flag and to run the program, we needed to find the stream name. We used the command: Get-Item -Path ./deebee.exe -Stream * to find the stream name within the ./deebee.exe path. For ADS view, we executed the program by running the command "wmic process call create $(Resolve-Path .\deebee.exe:hidedb)". After clicking enter, we waited a few seconds to load the database. Once it's done, a new page opened where we can see the ultimate flag, and the Nice and Naughty List. We printed the list by entering 1 or 2 in the select an option line.

Note: The list is printed for about 3 seconds and then the program goes back to the main menu.