PSP0201 Week 6 Writeup

Group Name: ikun no 1

Members

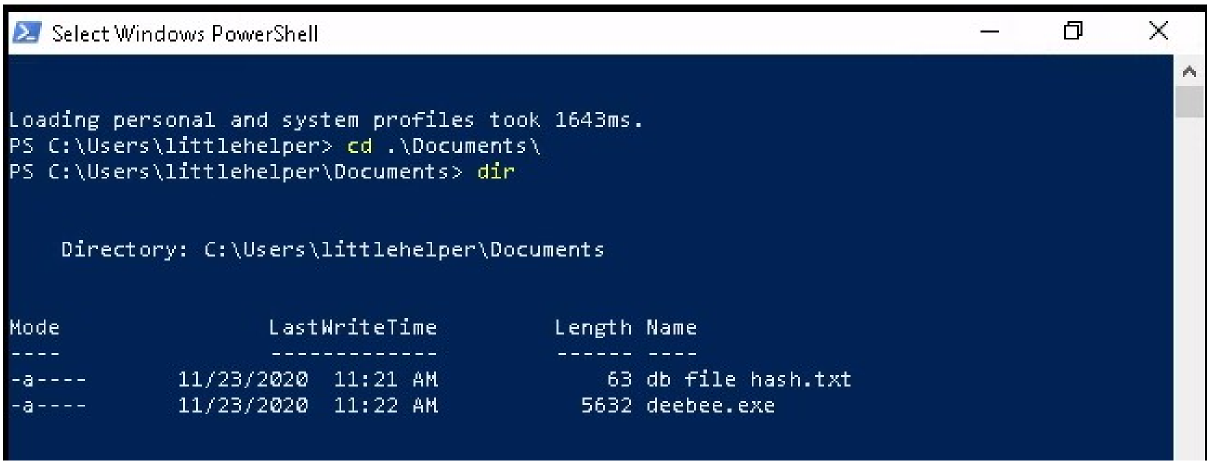
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 21 - [Blue Teaming] Time for some ELForensics

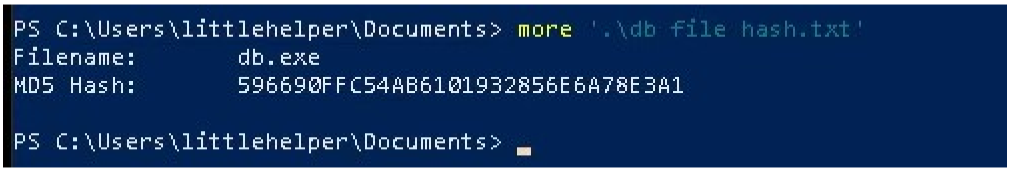
Tool used: kali Linux, Firefox, Remmina

Solution/Walkthrough:

Q1.



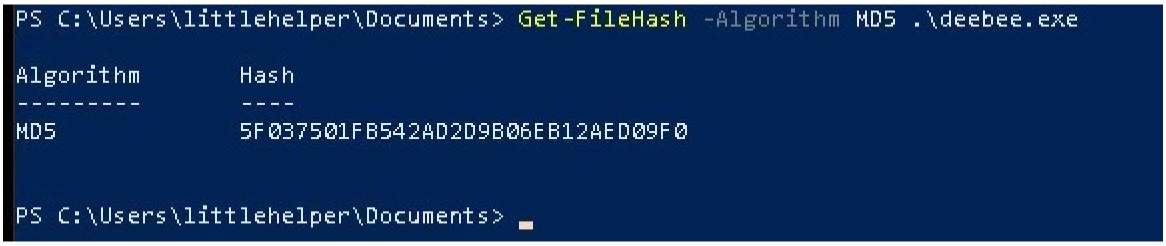
```
Loading personal and system profiles took 1643ms.
PS C:\Users\littlehelper> cd .\Documents\
PS C:\Users\littlehelper\Documents> dir


    Directory: C:\Users\littlehelper\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----       11/23/2020  11:21 AM             63 db file hash.txt
-a----       11/23/2020  11:22 AM           5632 deebee.exe
```



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

PS C:\Users\littlehelper\Documents>
```

Access to Remmina and log in to the machine. Open the db file hash.txt and the hash can be found

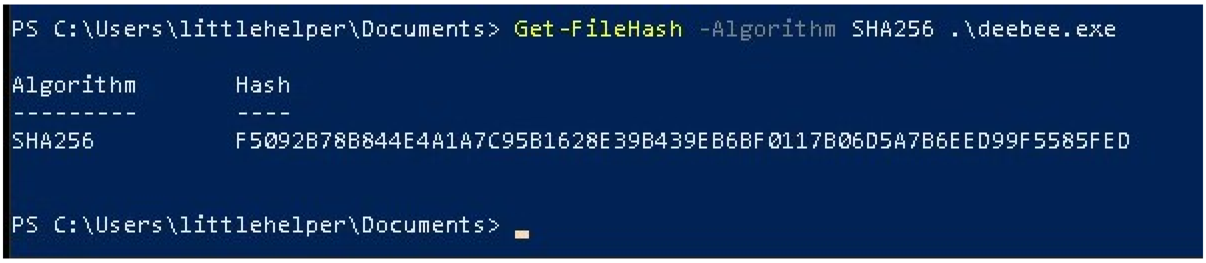
Q2.



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

Algorithm       Hash
---------       ----
MD5             5F037501FB542AD2D9B06EB12AED09F0


PS C:\Users\littlehelper\Documents>
```

Using Get-FileHash -Algorithm MD5 command, the MD5 hash file can be executed.

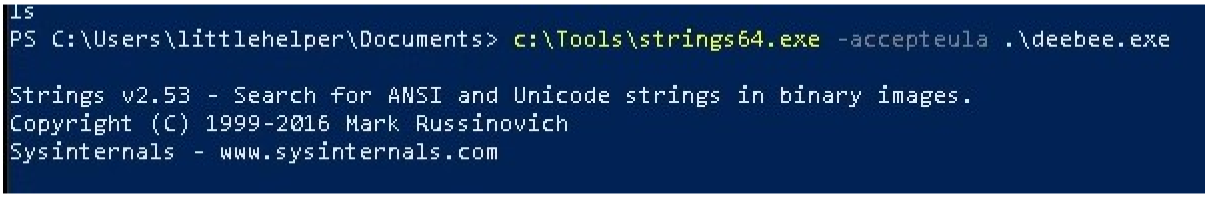
Q3.



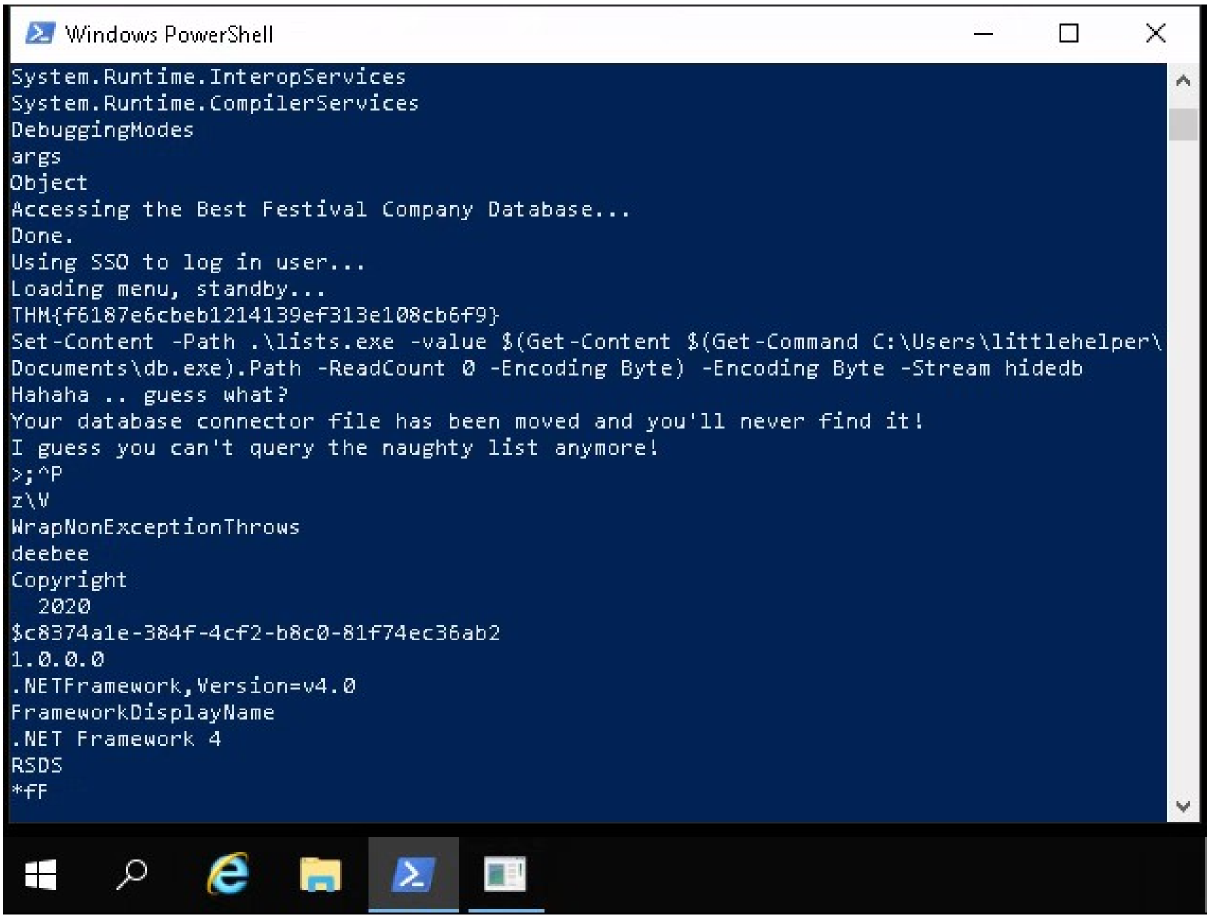
```
PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm SHA256 .\deebee.exe

Algorithm       Hash
---------       ----
SHA256          F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED


PS C:\Users\littlehelper\Documents> _
```

Change the filter from MD5 to SHA256 and the new result can be get.

Q4.



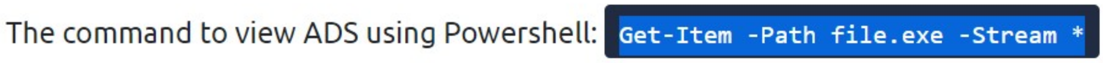
```
ls
PS C:\Users\littlehelper\Documents> c:\Tools\strings64.exe -accepteula .\deebee.exe

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



```
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 -Encoding Byte) -Encoding Byte -Stream hidedb
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
z\V
WrapNonExceptionThrows
deebee
Copyright
  2020
$c8374a1e-384f-4cf2-b8c0-81f74ec36ab2
1.0.0.0
.NETFramework,Version=v4.0
FrameworkDisplayName
.NET Framework 4
RSDS
*fF
```

By using the String command that can be found in THM, the file can be scanned and the flag will be shown after the scan.

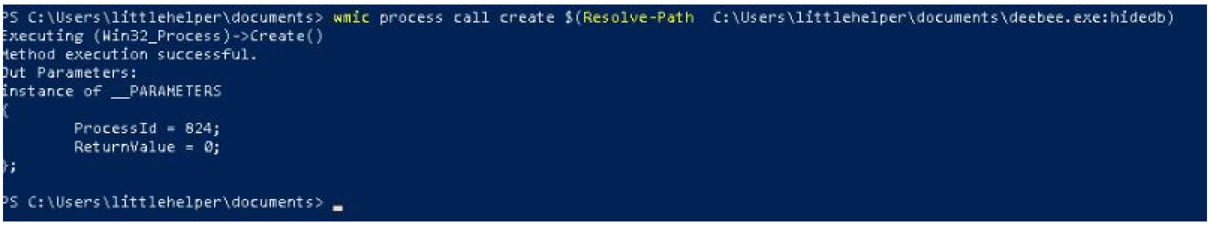
Q5.



The command to view ADS using Powershell: `Get-Item -Path file.exe -Stream *`

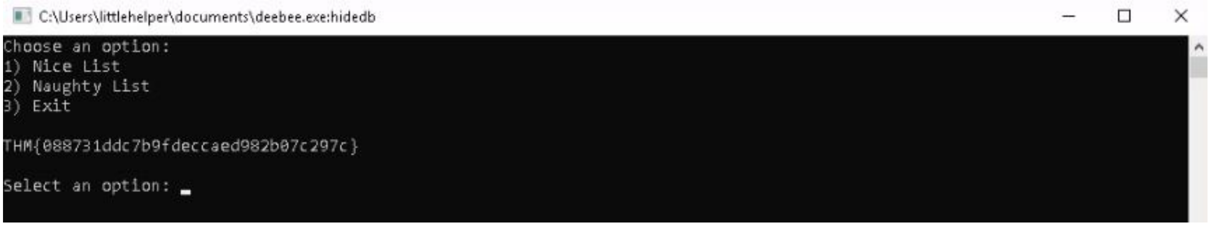
Examine from THM.

Q6.



```
PS C:\Users\littlehelper\documents> wmic process call create $(Resolve-Path  C:\Users\littlehelper\documents\deebee.exe:hidedb)
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 824;
        ReturnValue = 0;
};

PS C:\Users\littlehelper\documents> _
```

Run the command that can launch the hidden executable within ADS.



C:\Users\littlehelper\documents\deebee.exe:hidedb

```
Choose an option:
1) Nice List
2) Naughty List
3) Exit

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option: _
```

The flag can be captured after the run.

Q7,Q8

Open the list we found in the program we run at Q6 and examine the results after the options is chosen.