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, Powershell

Solution/Walkthrough:

Q1

We log into the remote machine using Remmina. In the machine we found that there is a file named db.exe. We read the file and find out the file hash.

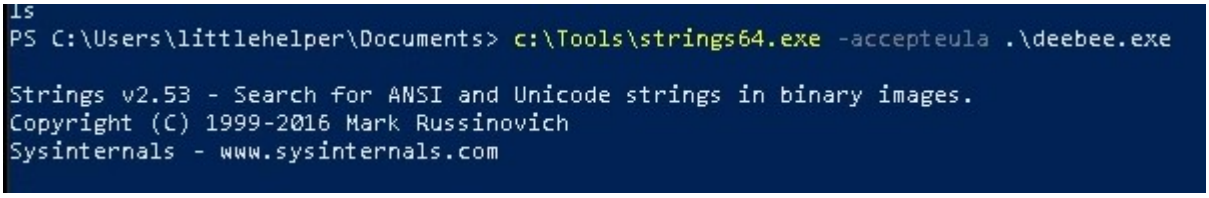
Q2

We open up the Powershell. In Powershell, we use the command from TryHackMe to get the hash of the file.

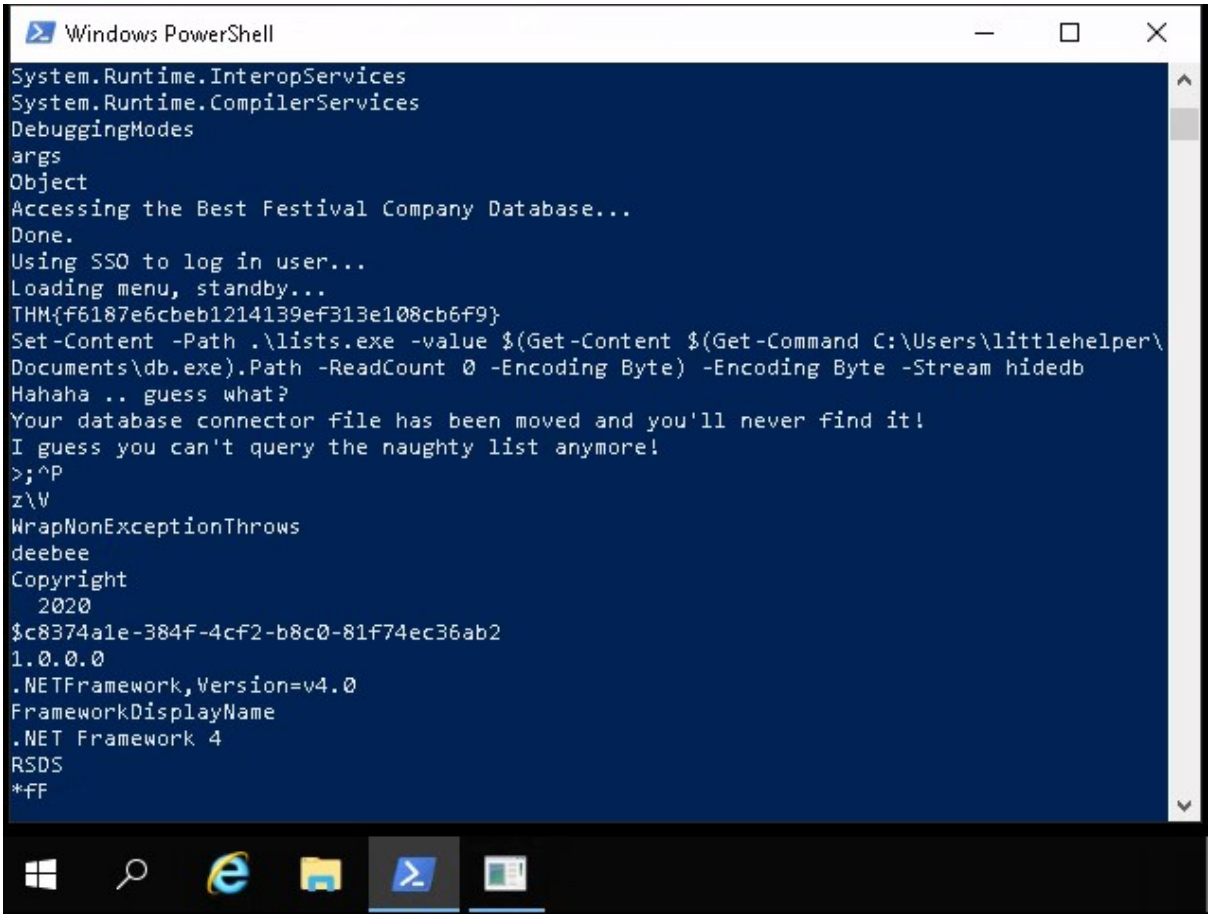
Q3

To see SHA256 file hash, we change the command from MD5 to SHA256, then we can get the hash of the file.

Q4



We then inspect the deebee.exe using the command from TryHackMe.



After running the command, we can scan the file and see the message as well as the hidden flag.

Q5

Copy from Try Hack Me.

Q6

To view ADS in Powershell, Try Hack Me has given us the command we need. We replace the file.exe to our target file, deebee.exe and that is the command we needed.

```
</assembly>
PS C:\Users\littlehelper\Documents> Get-Item -Path deebee.exe -Stream *


PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\d
e
                ebee.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\d
e
                ebee.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
```

After entering the command, we observe the ‘Stream’ and ’Length’. We can see a hidden file with the name of ‘hidedb’.

```
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>
```

We launch the hidden executable file by modifying the command provided by Try Hack Me, change the file.exe to deebee.exe and streamname to hidedb.

```
C:\Users\littlehelper\documents\deebee.exe:hidedb
Choose an option:
1) Nice List
2) Naughty List
3) Exit

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option:
```

We then can see the flag inside the file and also the missing naughty list.

<u>Q7&Q8</u>

We take a look at both lists to find out the name’s actual location.