

PSP0201

Week 6

Writeup

Group Name: ikun no 1

Members

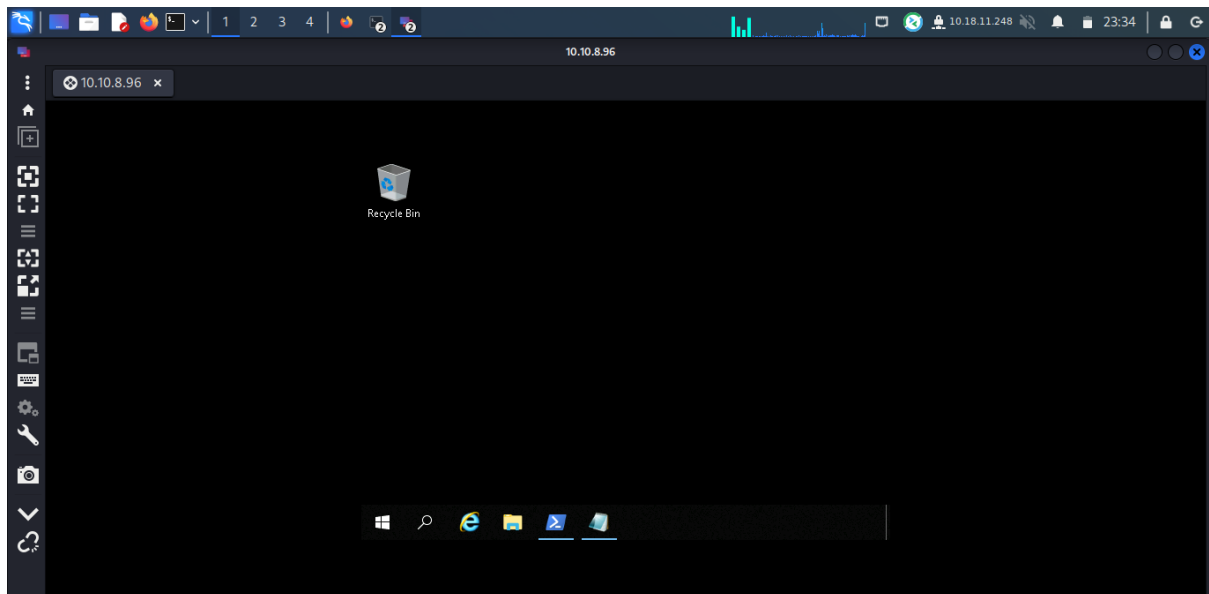
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 21: Blue Teaming Time for some ELForensics

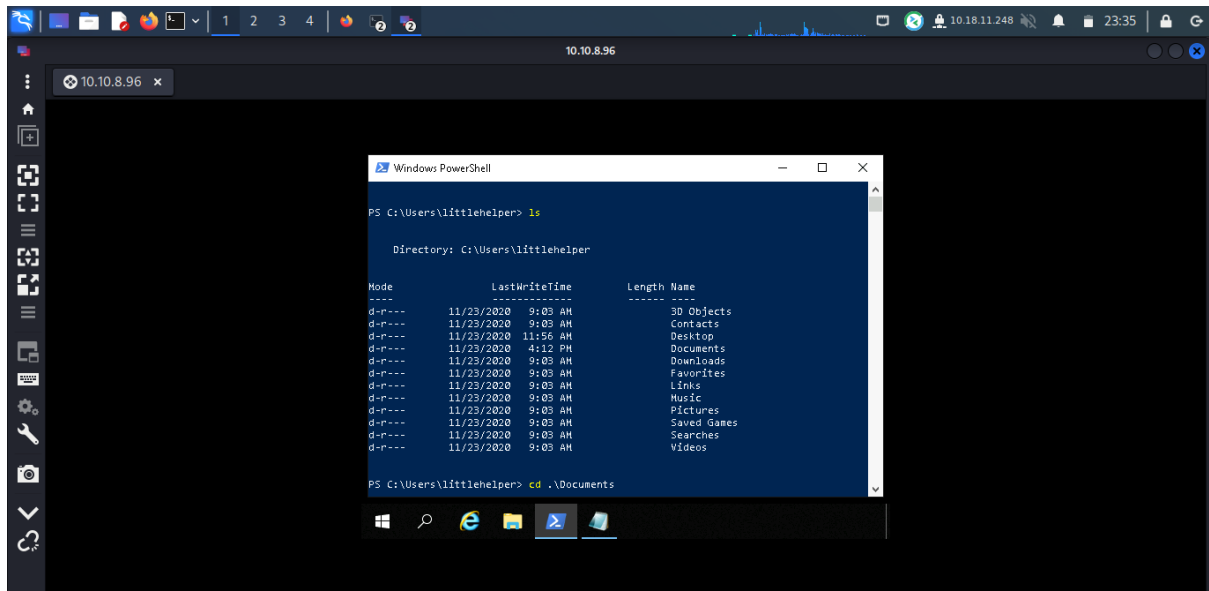
Tool used: Kali-Linux, Remmina, Powershell

Solution/walkthrough:

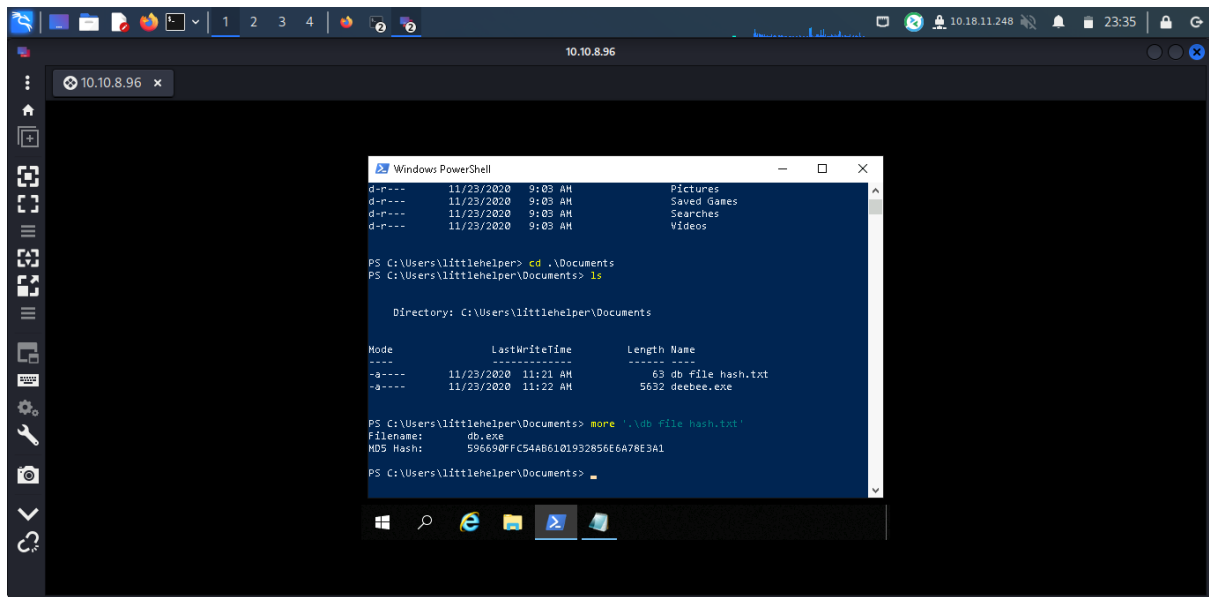
Question 1



Open Remmina with the server that had given.

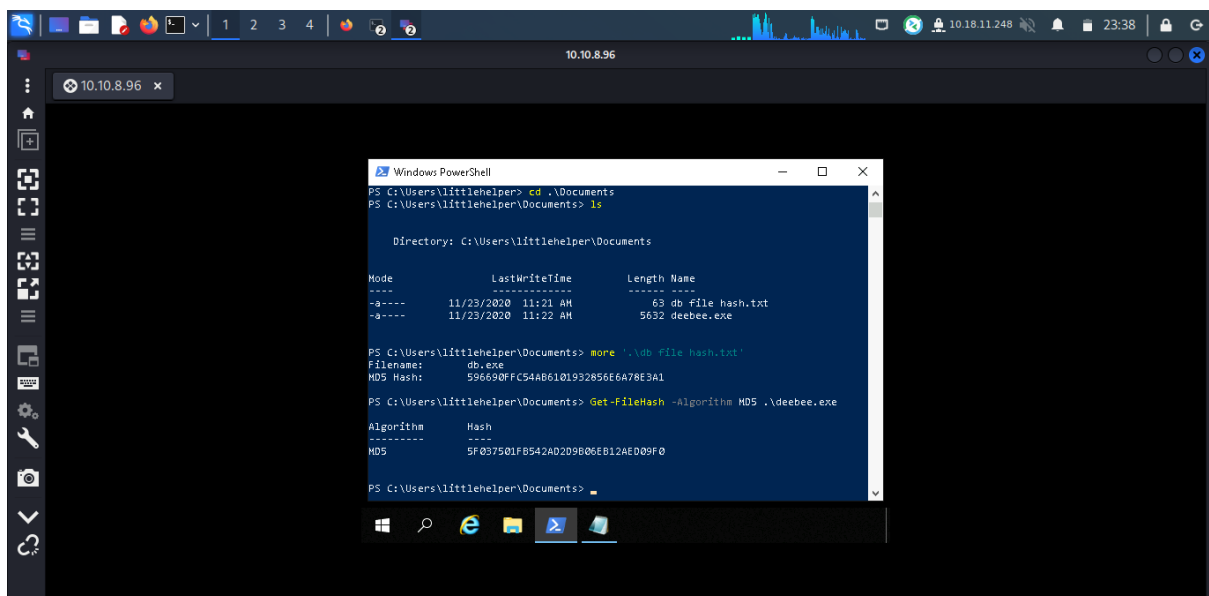


Open window PowerShell and check the list of the file.



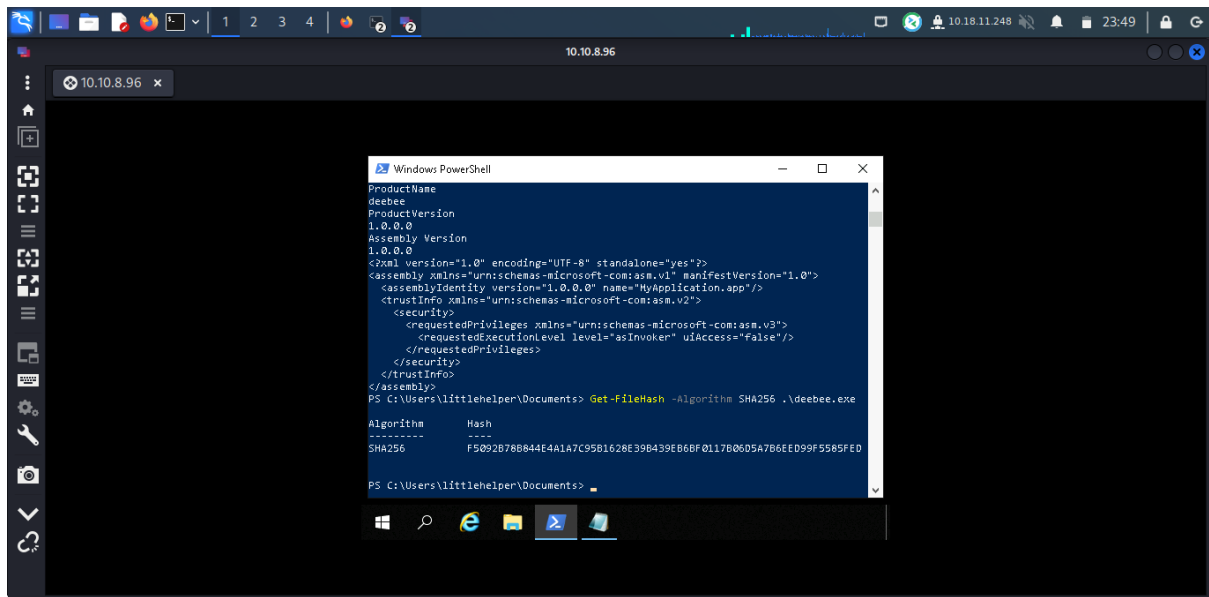
Then, open the Documents file and ls it. Use more '.\file.txt' to read the file hash.

Question 2



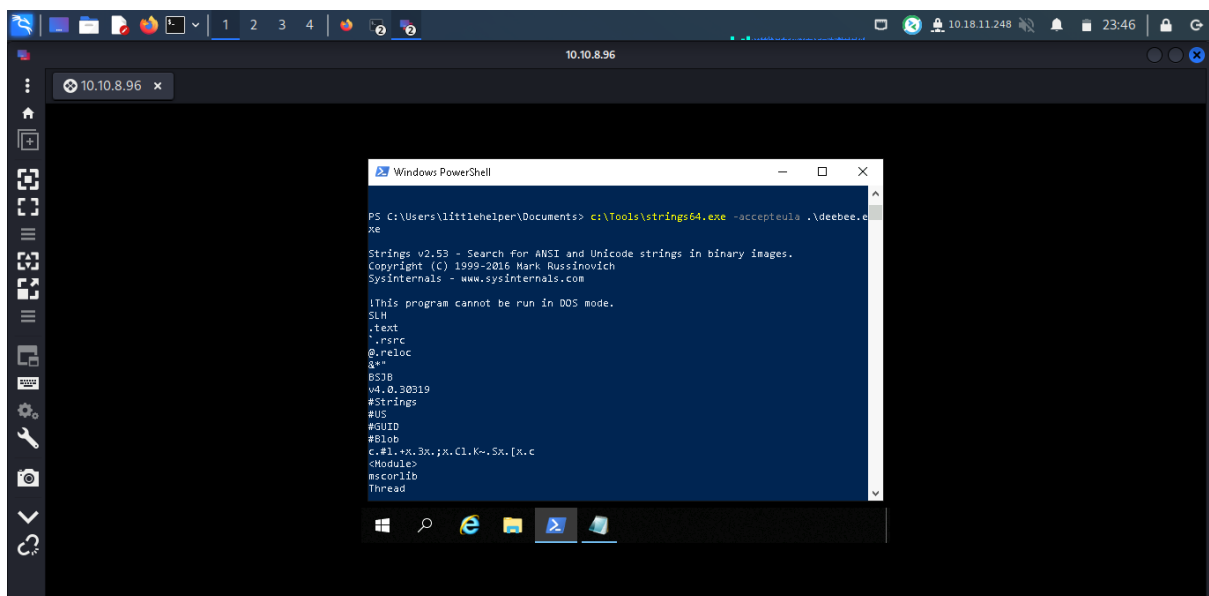
Use -Algorithms to see the hidden file and the hash shown.

Question 3



Change the MD5 into SHA256 and the hash shown.

Question 4



Use String.exe to scan the file.

```
Windows PowerShell
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
```

Then, scroll down to find the hidden flag.

Question 5

TryHackMe | 25 Days of C... TryHackMe Advent of Cyb... +

https://tryhackme.com/room/learnycyberin25days

Title	IP Address	Expires
AoC21	10.10.8.96	1h 13m 03s

The command to run for the Strings tool to scan the mysterious executable: `c:\Tools\strings64.exe -accepteula file.exe`

In the output, you should notice a command related to ADS. You know this by the end of the Powershell command `-Stream`.

Alternate Data Streams (ADS) is a file attribute specific to Windows NTFS (New Technology File System). Every file has at least one data stream (\$DATA) and ADS allows files to contain more than one stream of data. Natively Window Explorer doesn't display ADS to the user. There are 3rd party executables that can be used to view this data, but Powershell gives you the ability to view ADS for files.

Malware writers have used ADS to hide data in an endpoint, but not all its uses are malicious. When you download a file from the Internet unto an endpoint there are identifiers written to ADS to identify that it was downloaded from the Internet.

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

There are a few lines of output when you run this command. Pay particularly close attention to **Stream** and **Length**.

Recall that the database connector file is an executable file, and it's hidden within an alternate data stream for another file. We can use a built-in Windows tool, Windows Management Instrumentation, to launch the hidden file.

The command to run to launch the hidden executable hiding within ADS: `wmic process call create $(Resolve-Path file.exe:streamname)`

Note: You must replace file.exe with the actual name of the file which contains the ADS, and streamname is the actual name of the stream displayed in the

Study and find the answer in THM.

Question 6

The command to run for the Strings tool to scan the mysterious executable: `c:\Tools\strings64.exe -accepteula file.exe`

In the output, you should notice a command related to ADS. You know this by the end of the Powershell command `-Stream`.

Alternate Data Streams (ADS) is a file attribute specific to Windows NTFS (New Technology File System). Every file has at least one data stream (\$DATA) and ADS allows files to contain more than one stream of data. Natively Windows Explorer doesn't display ADS to the user. There are 3rd party executables that can be used to view this data, but Powershell gives you the ability to view ADS for files.

Malware writers have used ADS to hide data in an endpoint, but not all its uses are malicious. When you download a file from the Internet unto an endpoint there are identifiers written to ADS to identify that it was downloaded from the Internet.

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

There are a few lines of output when you run this command. Pay particularly close attention to Stream and Length.

Recall that the database connector file is an executable file, and it's hidden within an alternate data stream for another file. We can use a built-in Windows tool, Windows Management Instrumentation, to launch the hidden file.

The command to run to launch the hidden executable hiding within ADS: `wmic process call create $(Resolve-Path file.exe:streamname)`

Note: You must replace file.exe with the actual name of the file which contains the ADS, and streamname is the actual name of the stream displayed in the

Copy the command to launch the hidden executable hiding within ADS.

```

Length : 6144

PS C:\Users\littiehelper\Documents> wmic process call create $(Resolve-Path C:\Users\littiehelper\Documents\deebie.exe:hiddenb)
>>
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
Instance of __PARAMETERS
{
    ProcessId = 5104;
    ReturnValue = 0;
};
PS C:\Users\littiehelper\Documents>
  
```

Paste on the powershell and change file.exe.

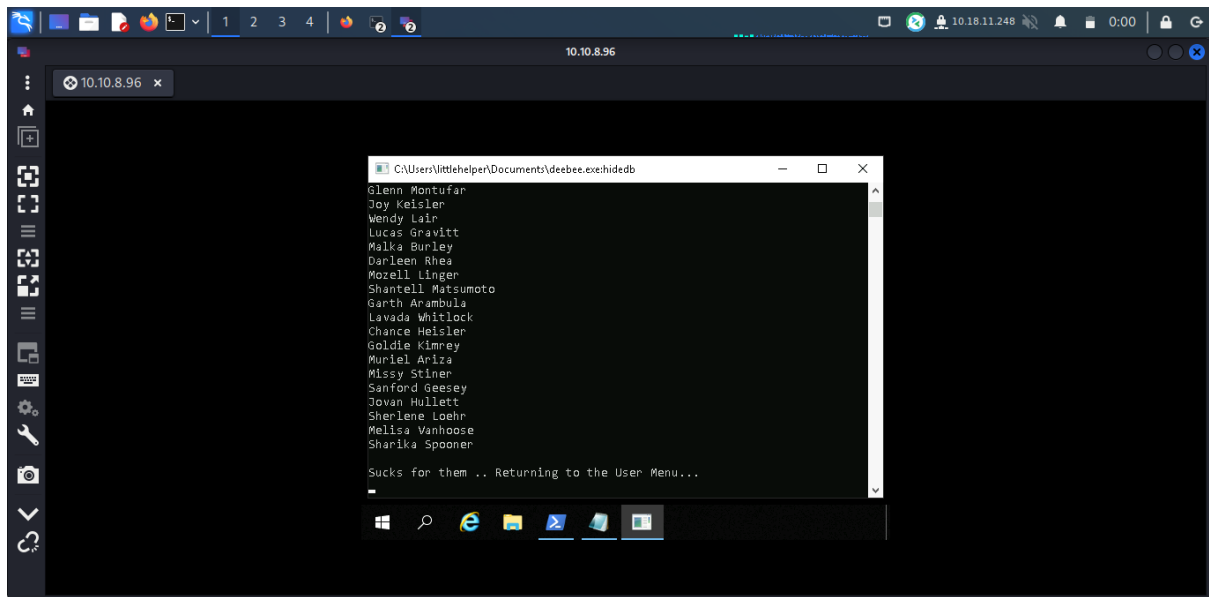
```

C:\Users\littiehelper\documents\deebie.exe:hiddenb
Choose an option:
1) Nice List
2) Naughty List
3) Exit

THM{088731ddc7b9fdeccaed982b07c297c}
Select an option:
  
```

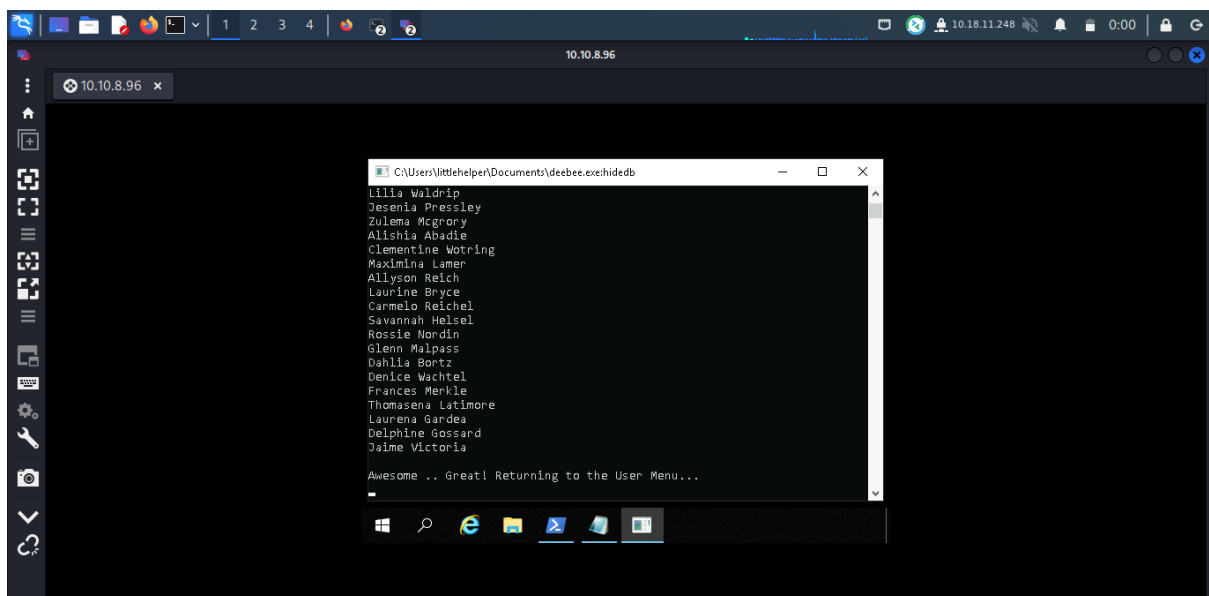
Then, the flag shown.

Question 7



Sharika is in naughty list.

Question 8



Jalme is in nice list.