PSP0201 Week 6 Writeup

Group Name: ikun no 1

Members

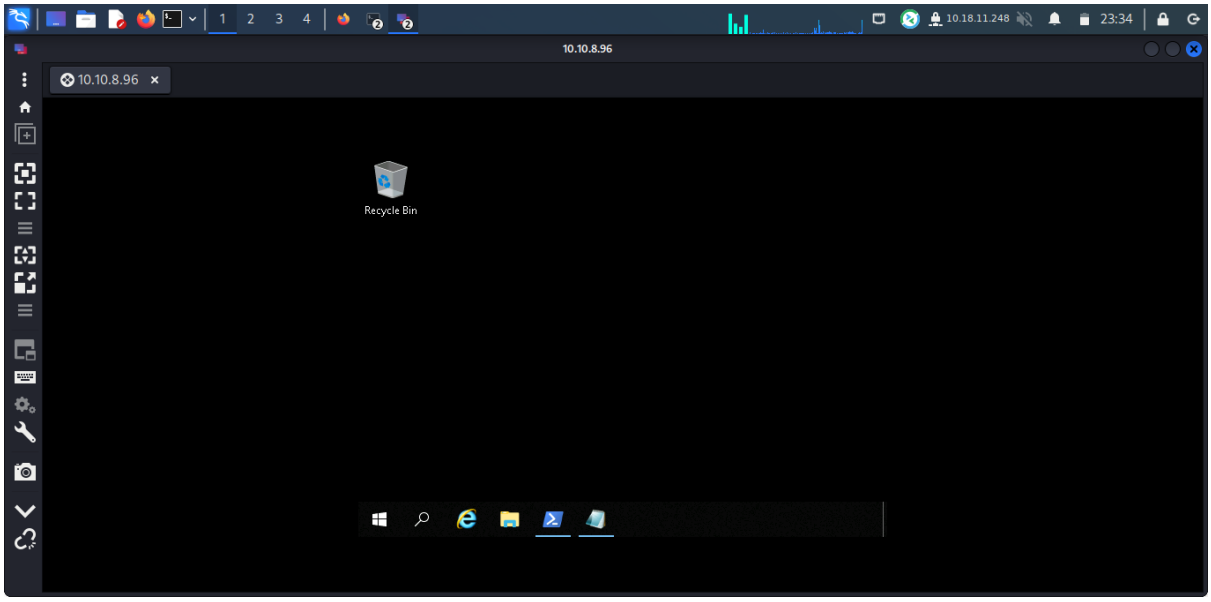
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 21: Blue Teaming Time for some ELForensics

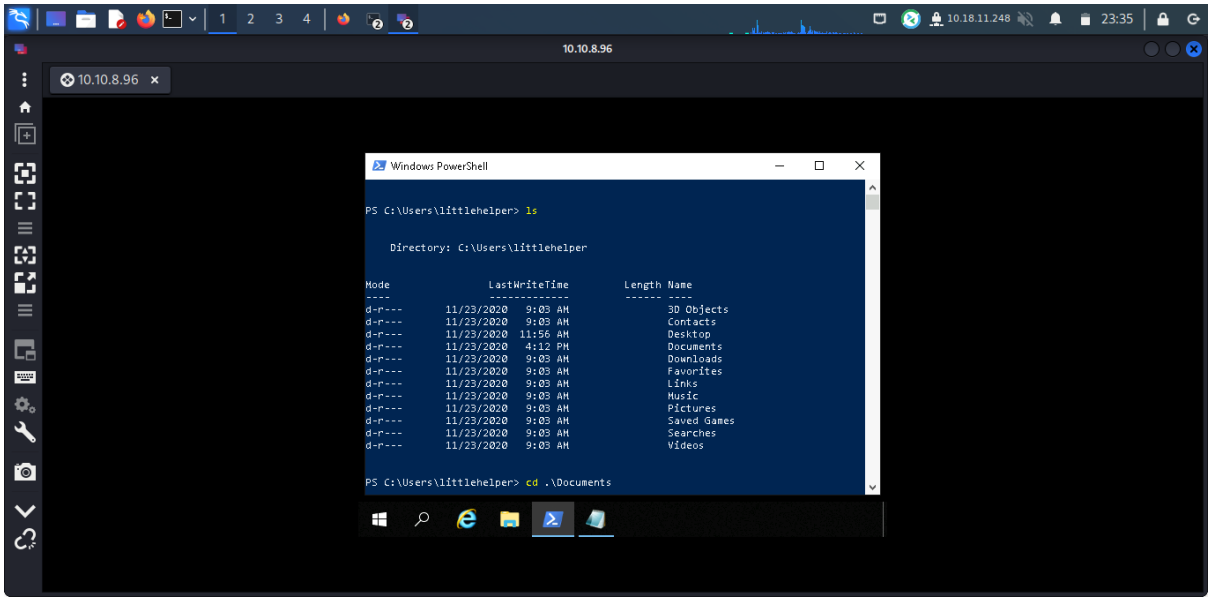
Tool used: Kali-Linux, Remmina, Powershell

Solution/walkthrough:

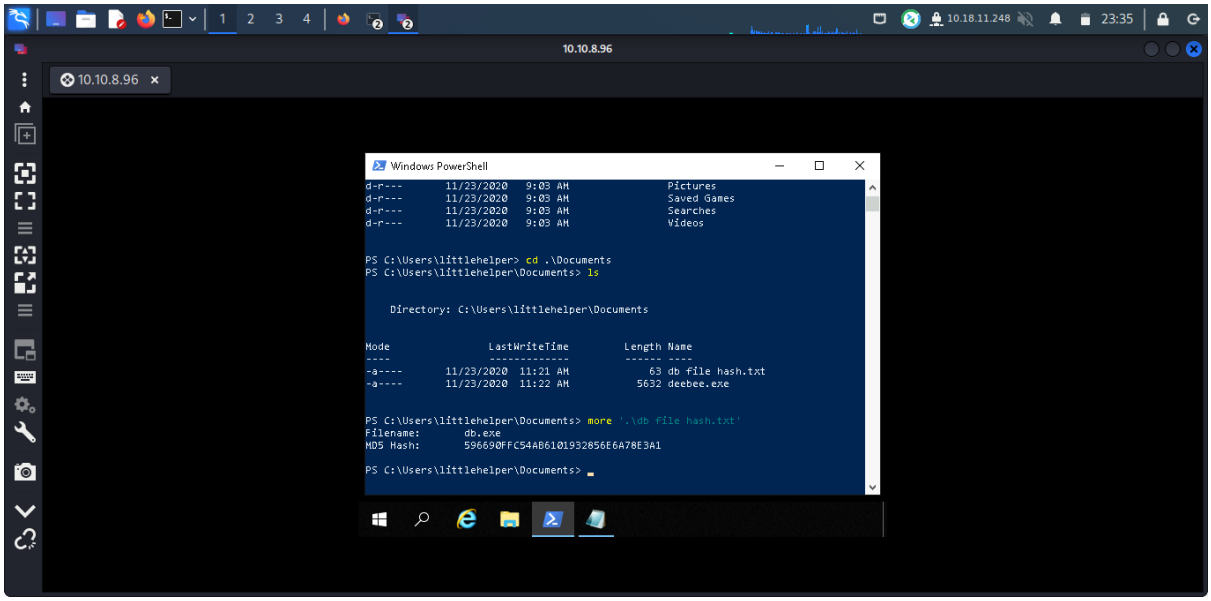
Question 1



Open Remmina with the server that had given.

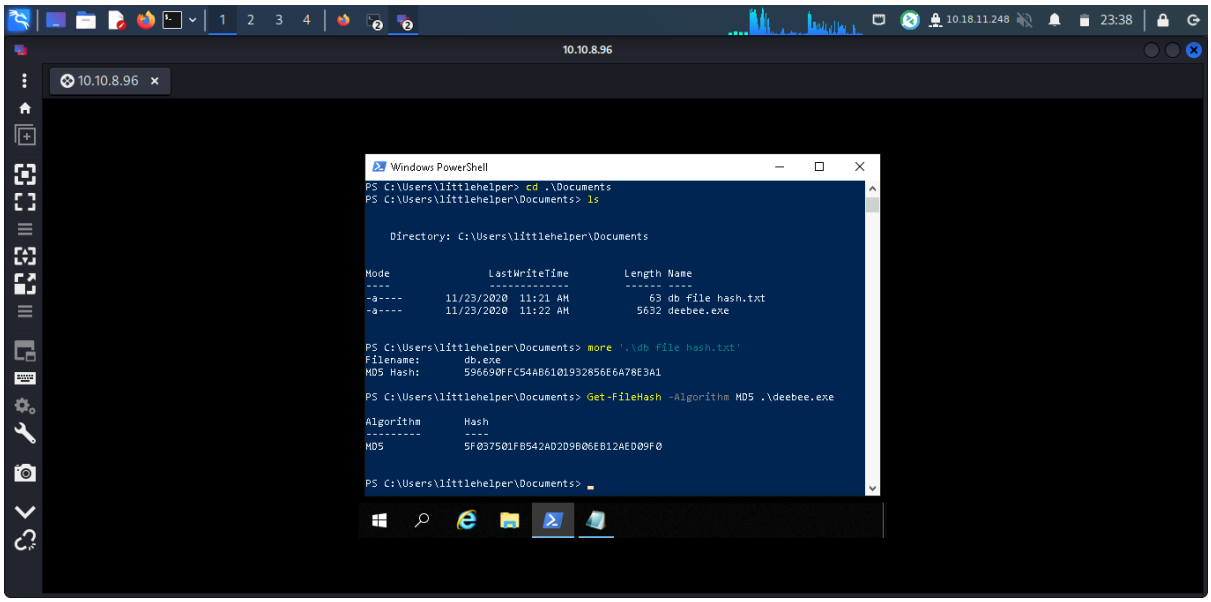


Open window PowerShell and check the list of the file.



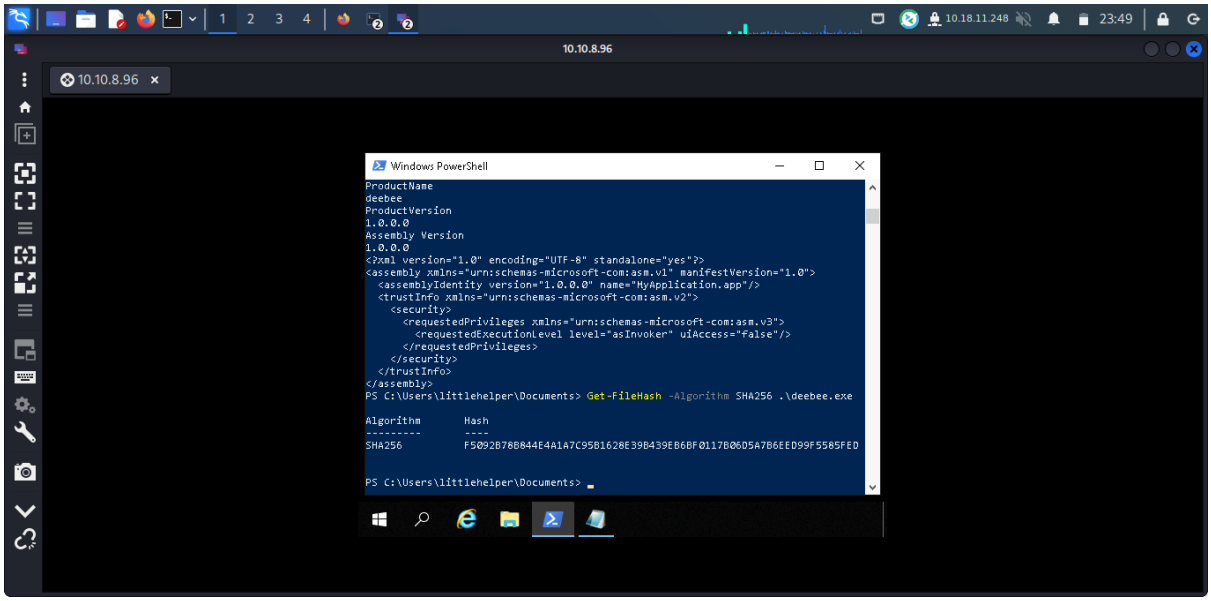
Then, open the Documents file and ls it. Use more '.\file.txt' to read the file hash.

Question 2



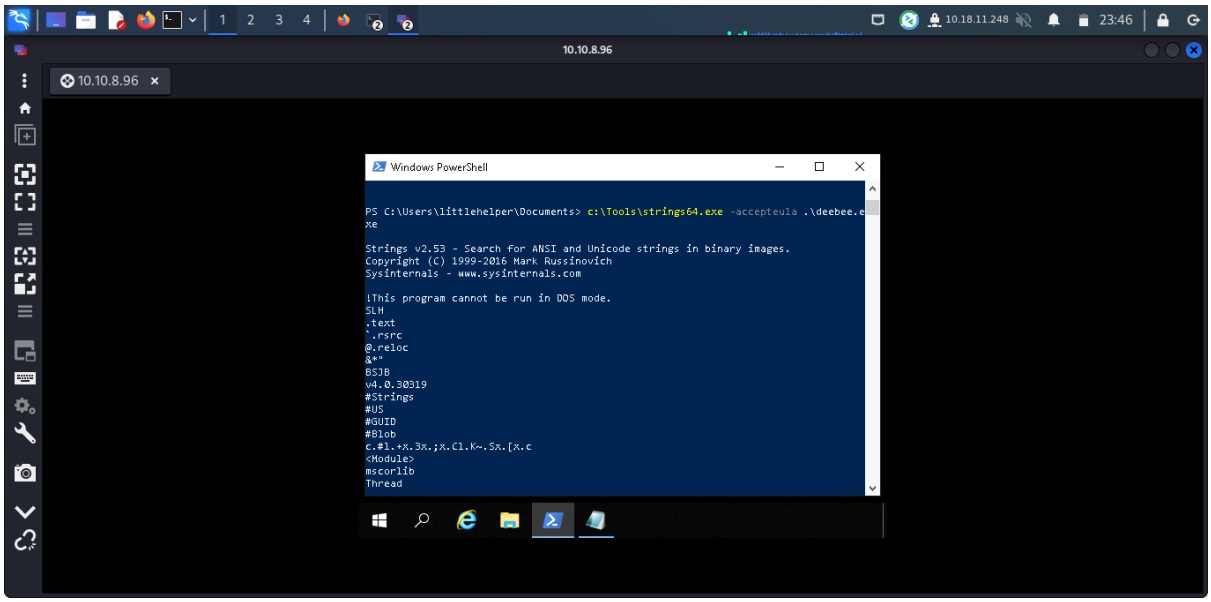
Use -Algoriths to see the hidden file and the hash shown.

Question 3

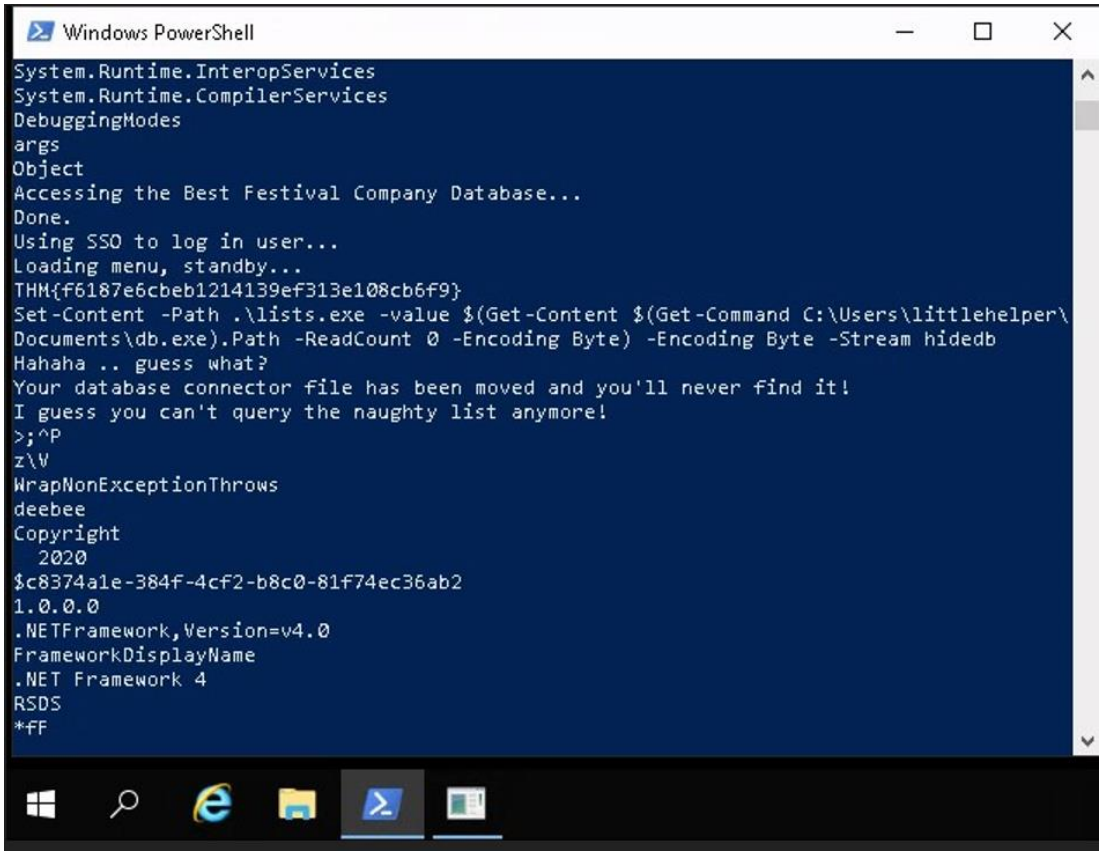


Change the MD5 into SHA256 and the hash shown.

Question 4

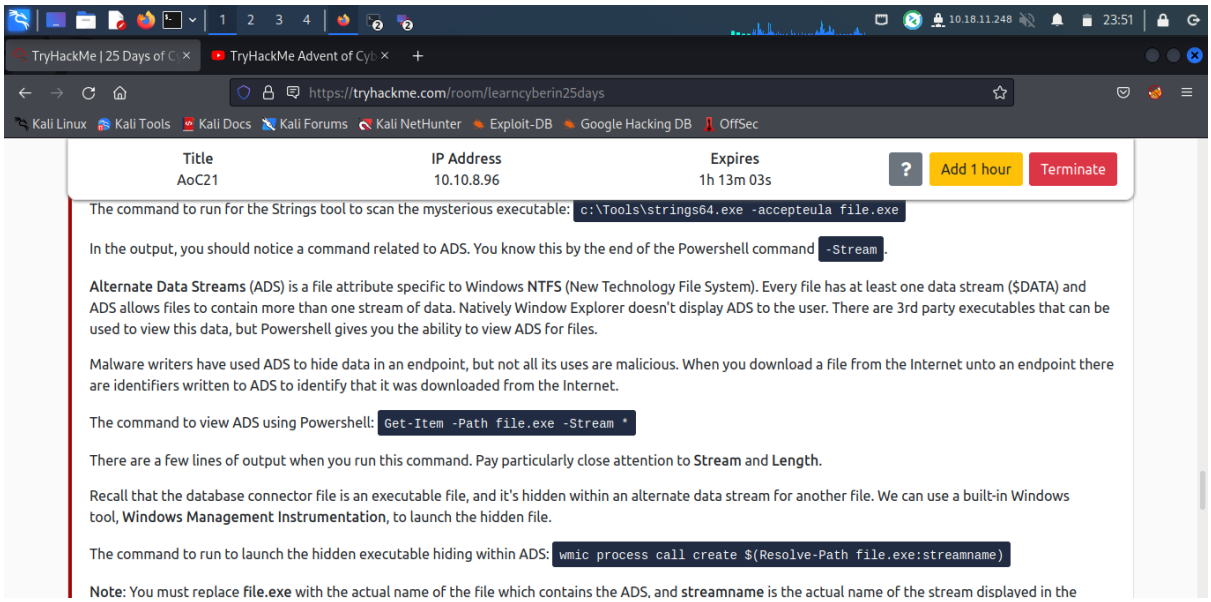


Use String.exe to scan the file.



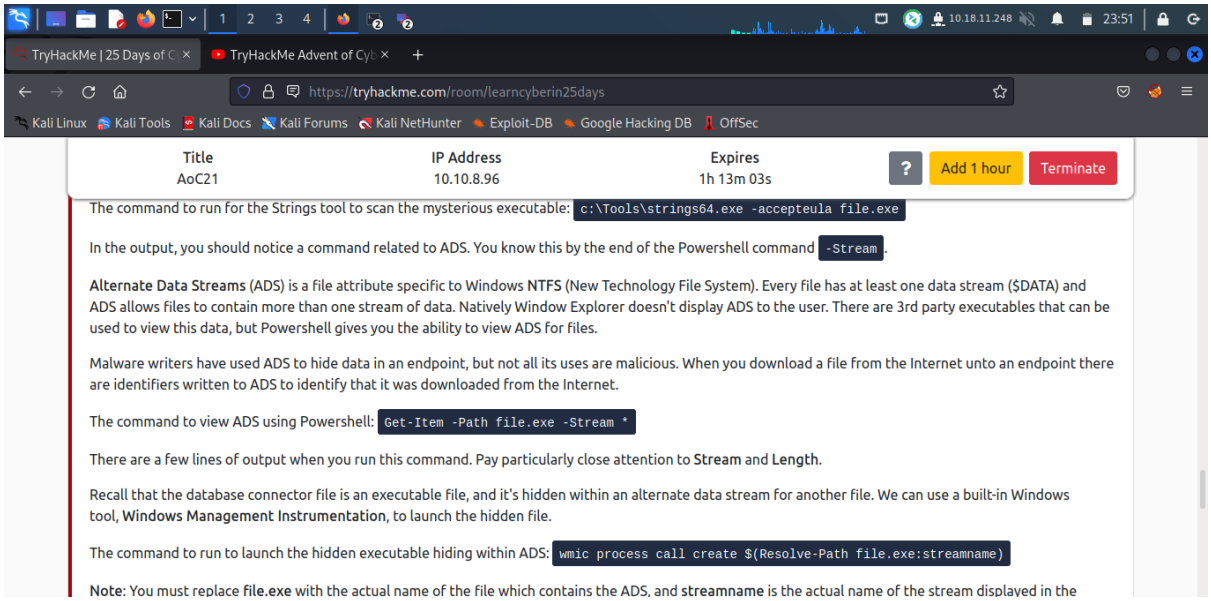
Then, scroll down to find the hidden flag.

Question 5

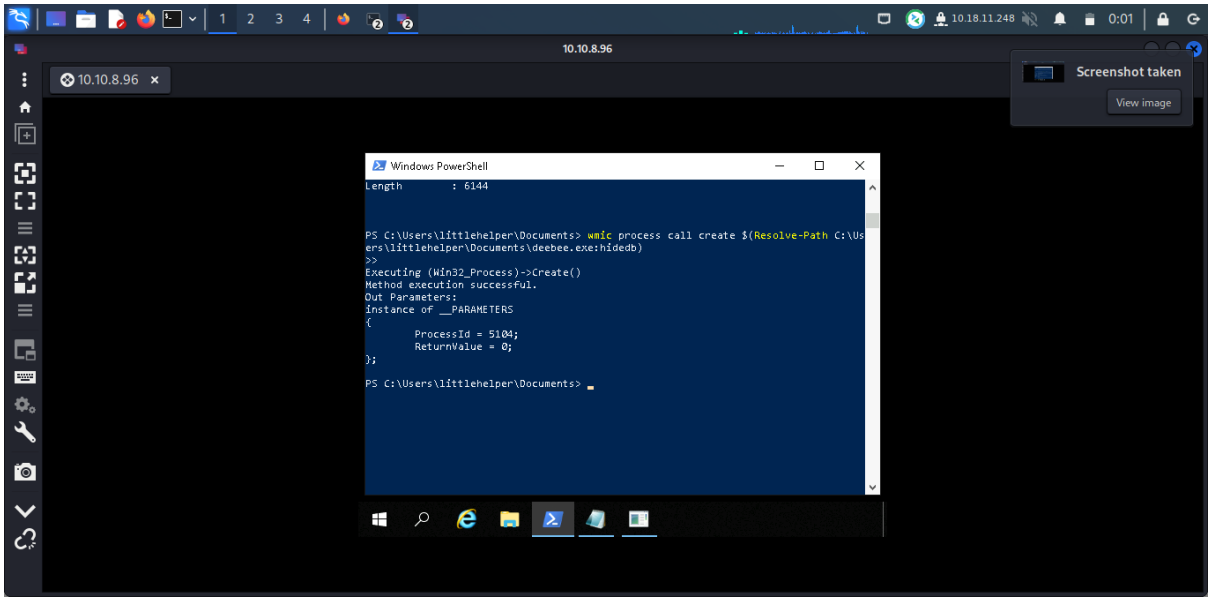


Study and find the answer in THM.

Question 6



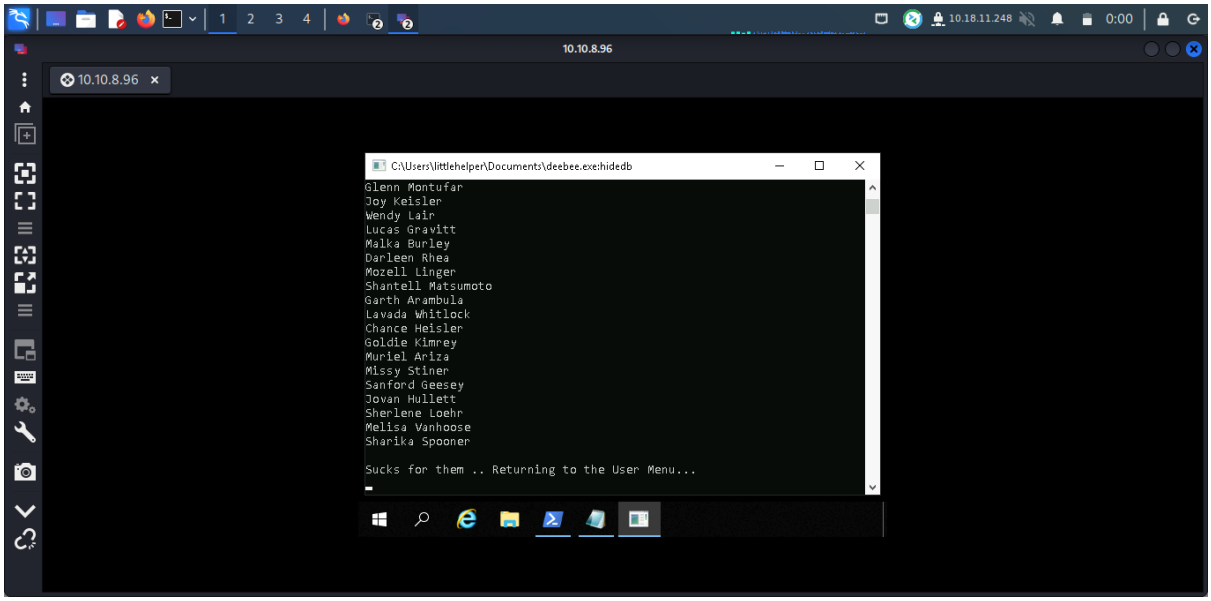
Copy the command to launch the hidden executable hiding within ADS.



Paste on the powershell and change file.exe.

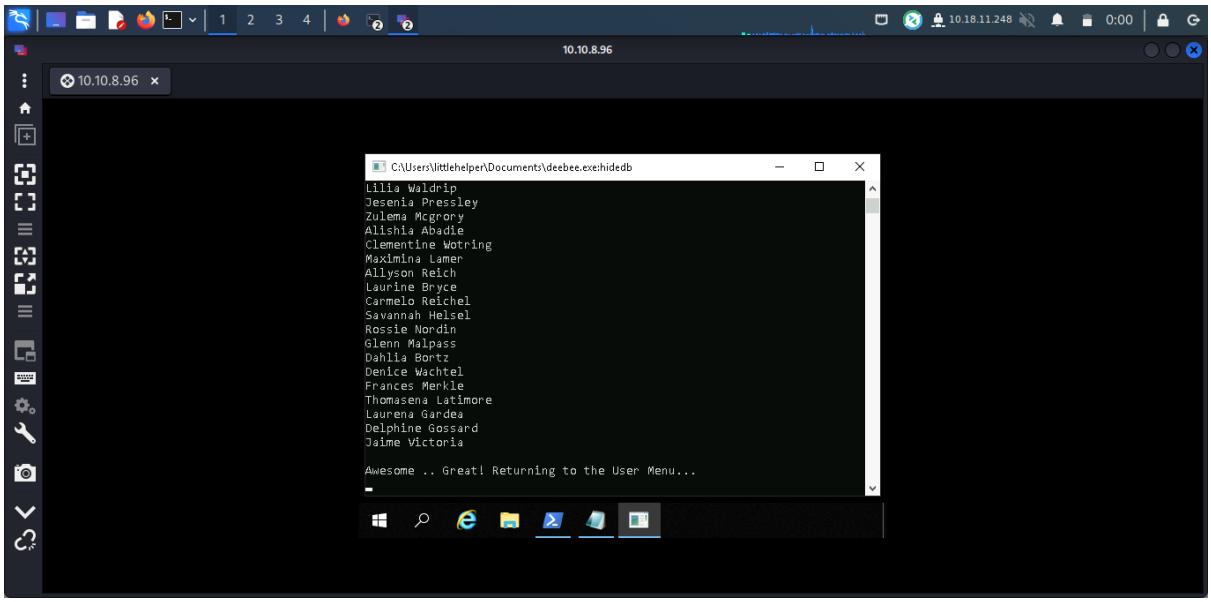
Then, the flag shown.

Question 7



Sharika is in naughty list.

Question 8



Jalme is in nice list.