PSP0201

Week 5

Writeup

Group Name: ikun no 1

Members

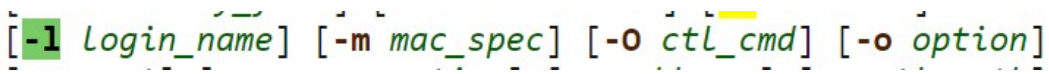
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 20 - [Blue Teaming] PowershELIF to the rescue

Tool used: kali Linux,

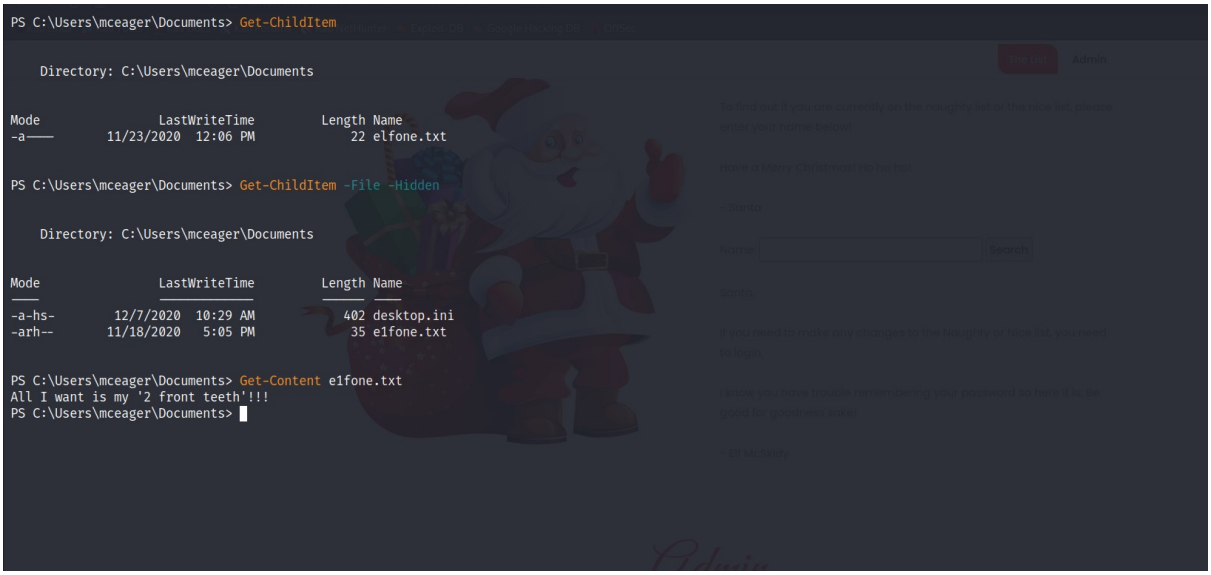
Solution/Walkthrough:

Q1



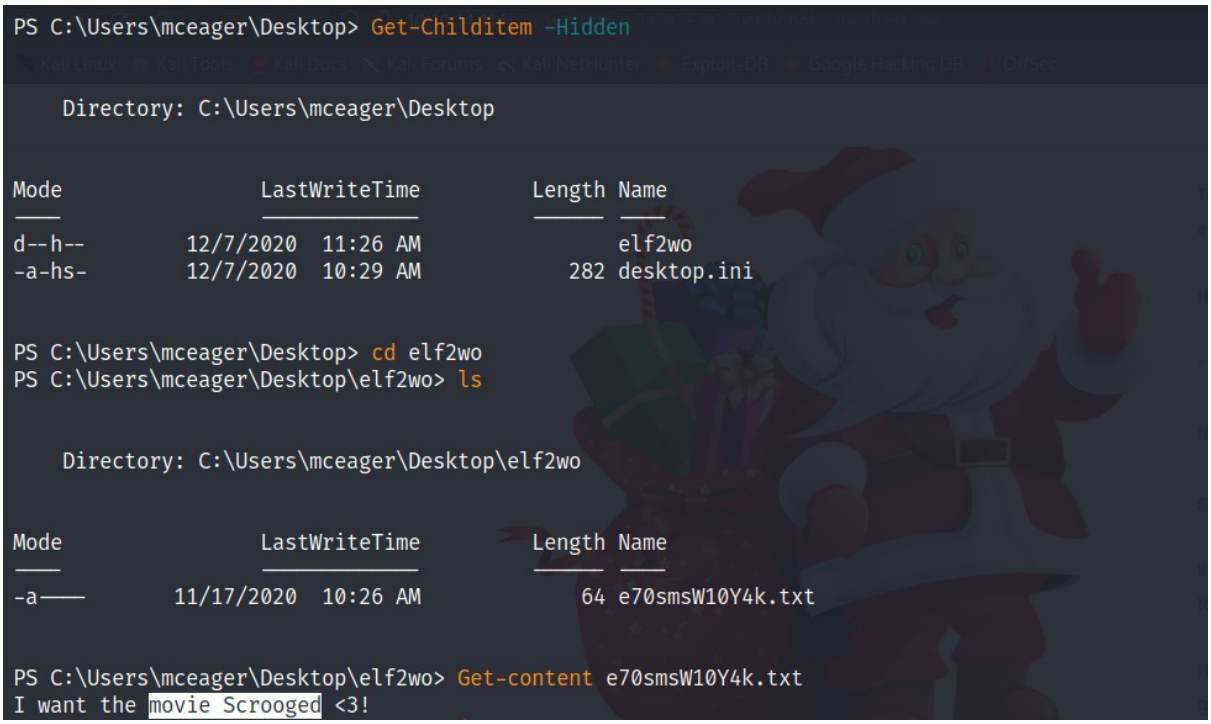
Match the answer after examining the ssh manual.

Q2.



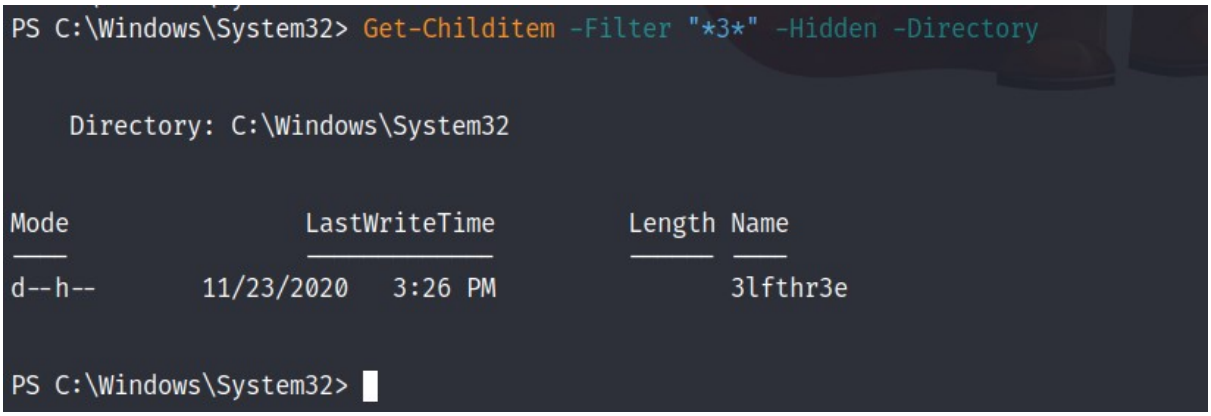
Using the get-childitem command with the filter -FIle -Hidden we can find a hidden .txt file which is e1fone.txt. Open the .txt file and the answer can be found.

Q3.



Change the directory to Desktop. Find out the list and add a -Hidden filter to find the hidden file in Desktop. Elf2wo file then can be found. Open the folder and open the text file inside it and the movie name can be found.

Q4.



Change the directory to System32. Add in some filter such as -Filter”*3*” to find a file with 3, -Hidden to find hidden files and -Directory to find a folder. The folder then can be found.

Q5.

```
PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt |Measure-Object -Word

Lines Words Characters Property
----- ----- ---------- --------
       9999
```

By using |Measure-Object -Word, we can find out the word count in the text file.The content shows where mcskidy saves all the jungle tones.

Q6.

```
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[551,6991]
Red
Ryder
PS C:\Windows\System32\3lfthr3e>
```

Using the “(Get-Content -Path file.txt)[index]” command, which is 551 and 6991 in the index, we can find out the exact value of the correct position.

Q7.

```
PS C:\Windows\System32\3lfthr3e> Get-content 2.txt | Select-string -Pattern "redryder"

redryderbbgun
```

We open up the 2.txt file in the directory. By using the hint given at THM, we use the -Pattern”reddryer” command to find out the results in 2.txt which contains ‘reddryer’ word in it.