PSP0201
Week 6
Writeup

Group Name: Undecided

Members:

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha binti Muhd Firdaus	Member

Day 20 : Blue Teaming – PowershELIF to the rescue

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1

Using manual option, we found out that -l parameter is used for login name as seen in the following attachment.

```
SYNOPSIS
     ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
         [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
         [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
         [-i identity_file] [-J destination] [-L address]
         [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option]
         [-p port] [-Q query_option] [-R address] [-S ctl_path]
         [-W host:port] [-w local_tun[:remote_tun]] destination
         [command]
```

Question 2

We use cat *file name* command to print out the file in the terminal and the output said that Elf 1 wants 2 front teeth.

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a-hs-        12/7/2020  10:29 AM            402 desktop.ini
-arh--       11/18/2020   5:05 PM             35 e1fone.txt


PS C:\Users\mceager\Documents> Get-content e1fone.txt
All I want is my '2 front teeth'!!!
```

Question 3

To find the name of the movie that Elf2 wants to watch, we first find what's under the elf2wo file. Then, we printed it and got the movie name which was Scrooged!

```
PS C:\Users\mceager\Desktop> cd elf2wo
PS C:\Users\mceager\Desktop\elf2wo> get-childitem


    Directory: C:\Users\mceager\Desktop\elf2wo


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/17/2020  10:26 AM             64 e70smsW10Y4k.txt


PS C:\Users\mceager\Desktop\elf2wo> cat e70smsW10Y4k.txt
I want the movie Scrooged <3!
PS C:\Users\mceager\Desktop\elf2wo>
```

Question 4

We needed to find the hidden folder using “Get-ChildItem -Hidden -Directory” command which is available in the system32 folder of Windows.

```
PS C:\Users\mceager> cd ..
PS C:\Users> cd C:/Windows
PS C:\Windows> Get-ChildItem -Hidden -Directory "*3*"
PS C:\Windows> cd system32
PS C:\Windows\system32> Get-ChildItem -Hidden -Directory "*3*"


    Directory: C:\Windows\system32


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--h--        11/23/2020   3:26 PM                3lfthr3e
```

Question 5

To find the number of words in the file, we used the command “Get-Content file | Measure-Object -Word” and it shows the total words which is 9999.

```
PS C:\Windows\system32\3lfthr3e> Get-Content 1.txt | Measure-Object -Wo
rd

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

Question 6

Through indexing method, we printed out the words of index 551 and 6991 as commanded. They are Red and Ryder.

```
PS C:\Windows\system32\3lfthr3e> (Get-Content 1.txt)[551]
Red
PS C:\Windows\system32\3lfthr3e> (Get-Content 1.txt)[6991]
Ryder
```

Question 7

We only found half of the answer to question 7, but we needed to find the full word. Hence, we used "-Pattern" parameter to search for the word.

```
PS C:\Windows\System32\3lfthr3e> Get-Content 2.txt | Select-String -Patte
rn "redryder"

redryderbbgun
```

Thought Process/Methodology:

For this task, we learned to use PowerShell. First, we needed to understand the function of -l parameter. We type in “man ssh” command and discover that it is used for login name. Then after login using the password, we turned on the PowerShell. After turning it on, we moved to the Document folder and tried finding the elf1 file. We tried to print the output of the visible file that we saw but it only printed “Nothing to see here”. We decided to check for any hidden file and found one. When we print the output of the hidden file, we found out that he wants 2 front teeth. After that, on the desktop, we found the 2nd file. Naturally, we print it out and it showed that Scrooged is the name of the movie he wants to watch. Now it’s the time to find the hidden directory. We took some time to find it but, in the end, it was located in windows/system32 folder. However, knowing that it is a hidden directory made the progress of finding it easier. After that, using Measure-Object, we discover the total words which was 9999. However, now we are given 2 index number and asked to find out the word in this index number. We used the index method and printed it out. In the end, we came to know the words we found are just half of the answer. Thus, we used the Select-String and -Pattern method to find out what Elf 3 really want.