Day 20 - PowershELlF to the rescue

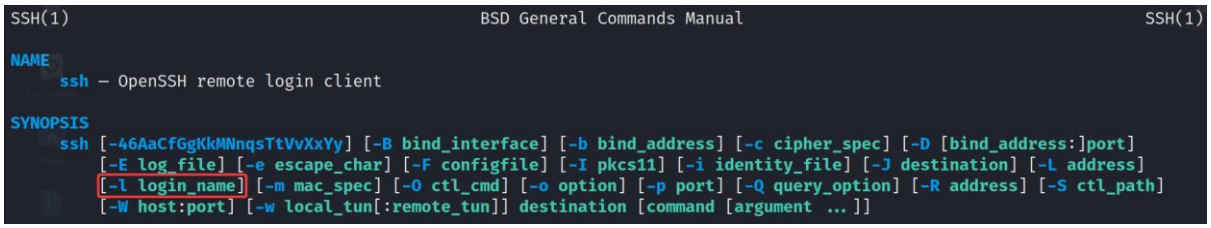
List of tools used: SSH, PowerShell

Question 1

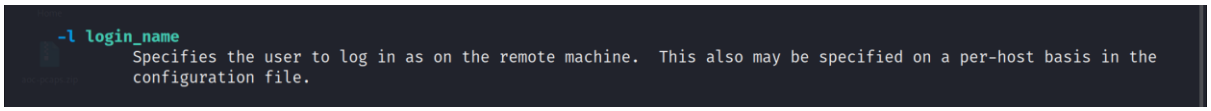
Check the ssh manual. What does the parameter -l do?

Methodology: We run command “man ssh” to see the manual of ssh,

We see that the parameter -l refer to login_name.



We scroll down and see more description about parameter -l.

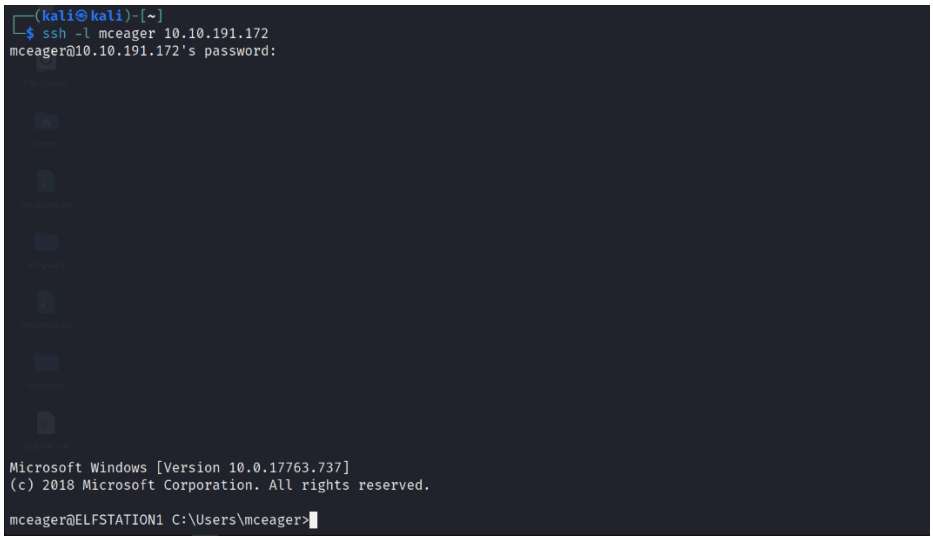


Answer: login name

Question 2

Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?

Methodology: We connect the machine with the given ssh command and password.



We type command “powershell” to enter the powershell environment. We use command “Set-Location” (same as cd) to navigate to Documents. Then, we use command “Get-ChildItem” (same as ls) to view the content inside the directory, we also use -File and -Hidden after the command to narrow down the search result and only show hidden file. We see there is 2 hidden files, and our target is e1fone.txt. We use the command “Get-Content” (same as cat) to view the content of the txt file. Then, we can see the answer is 2 from teeth.

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

mceager@ELFSTATION1 C:\Users\mceager>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\mceager> Set-Location Documents
PS C:\Users\mceager\Documents> Get-ChildItem -File -Hidden


    Directory: C:\Users\mceager\Documents


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'!!!
```

Answer: 2 front teeth

Question 3

Search on the desktop for a hidden folder that contains the file for Elf 2. Read the contents of this file. What is the name of that movie that Elf 2 wants?

Methodology: We navigate to Desktop. Then, we use the same Get-ChildItem command, but this time change the flag to directory. We see the name of the hidden directory, and we navigate into it. There is a txt file, and inside the txt file is the answer, Scrooged.

```
PS C:\Users\mceager\Documents> Set-Location ..
PS C:\Users\mceager> Set-Location Desktop
PS C:\Users\mceager\Desktop> Get-ChildItem -Directory -Hidden


    Directory: C:\Users\mceager\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--h--        12/7/2020  11:26 AM                elf2wo


PS C:\Users\mceager\Desktop> Set-Location 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> Get-Content e70smsW10Y4k.txt
I want the movie Scrooged <3!
```

Answer: Scrooged

Question 4

Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder? (This command will take a while)

Methodology: We navigate system32. We use the same Get-ChildItem command, and we use the hint from tryhackme to futher narrow down the search result. The hint is to use -Filter and it will only find directory which name has a digit 3 in it. Then, we see the name of the hidden directory is 3lfthr3e.

```
PS C:\Windows\system32> Get-ChildItem -Directory -Hidden -Filter "*3*"


    Directory: C:\Windows\system32


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


PS C:\Windows\system32> Set-Location 3lfthr3e
PS C:\Windows\system32\3lfthr3e> Get-ChildItem
PS C:\Windows\system32\3lfthr3e> Get-ChildItem -Hidden


    Directory: C:\Windows\system32\3lfthr3e


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-arh--        11/17/2020  10:58 AM          85887 1.txt
-arh--        11/23/2020   3:26 PM       12061168 2.txt
```

Answer: 3lfthr3e

Question 5

How many words does the first file contain?

Methodology: We navigate into the directory and find 2 hidden txt file. We see the content of the first txt file and it is fill with words and lines.

```
PS C:\Windows\system32\3lfthr3e> Get-Content 1.txt
the
of
and
to
in
for
is
on
that
by
this
with
you
it
not
or
be
are
from
an
at
as
your
all
have
new
more
```

We use the same Get-Content command but this time we add Measure-Object -Word in the end to measure the txt file in words measurement. We see the output is 9999.

```
bent
laos
subjective
monsters
asylum
lightbox
robbie
stake
cocktail
outlets
swaziland
varieties
arbor
mediawiki
configurations
poison
PS C:\Windows\system32\3lfthr3e> Get-Content 1.txt | Measure-Object -Word

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

Answer: 9999

Question 6

What 2 words are at index 551 and 6991 in the first file?

Methodology: We use the same Get-Content command but this time we add Select-Object in the end and provide indexes to get the words with index of 551 and 6991. We see the output is Red and Ryder.

```
PS C:\Windows\system32\3lfthr3e> Get-Content 1.txt | Select-Object -Index 551, 6991
Red
Ryder
```

Answer: Red Ryder

Question 7

This is only half the answer. Search in the 2nd file for the phrase from the previous question to get the full answer. What does Elf 3 want? (use spaces when submitting the answer)

Methodology: We use the same Get-Content command on 2nd txt file but this time we add Select-String in the end. We use the hint from tryhackme to filter out the pattern of words inside the txt file. The hint is to use -Pattern "redryder" to find words that have the redryder pattern. We see the output is redryderbbgun.

```
PS C:\Windows\system32\3lfthr3e> Get-Content 2.txt | Select-String -Pattern "redryder"

redryderbbgun
```

Answer: redryderbbgun