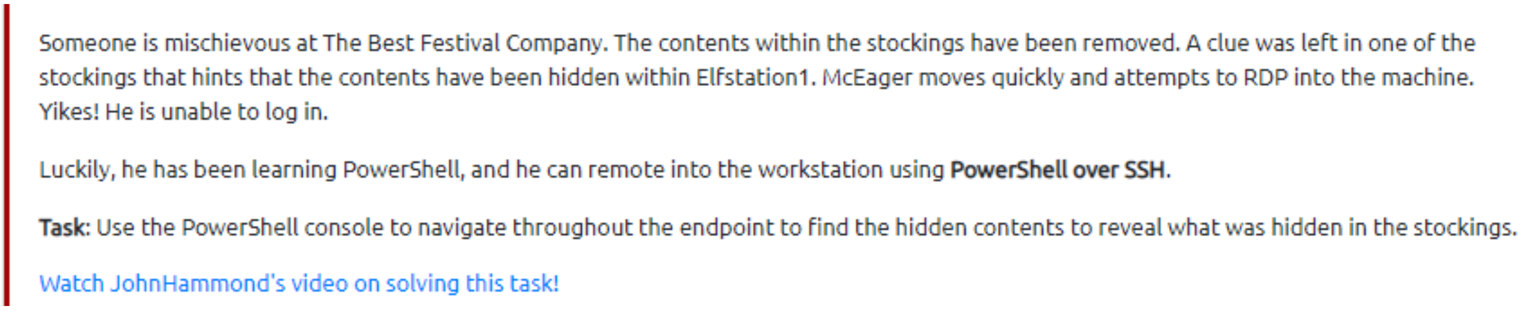
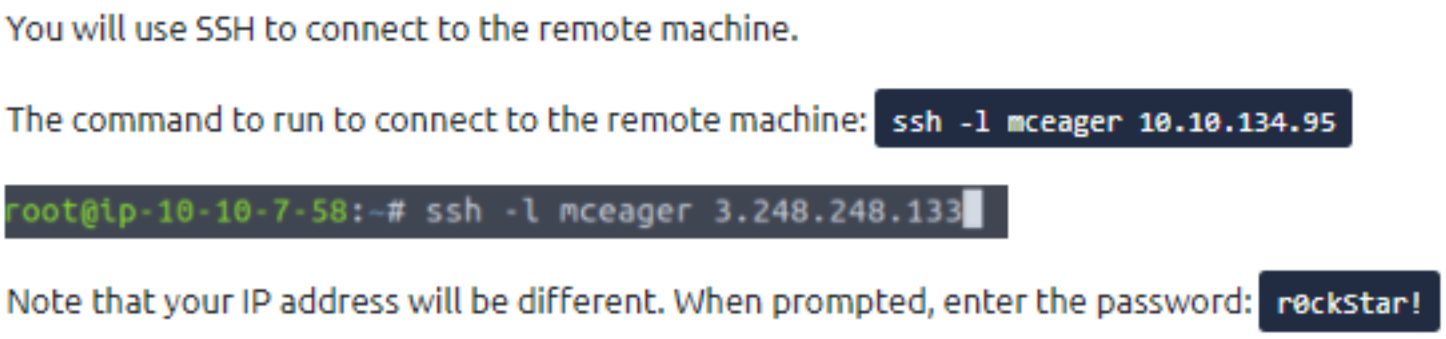
Day 20 - PowershELlF to the rescue

Scenario



> Someone is mischievous at The Best Festival Company. The contents within the stockings have been removed. A clue was left in one of the stockings that hints that the contents have been hidden within Elfstation1. McEager moves quickly and attempts to RDP into the machine. Yikes! He is unable to log in.
>
> Luckily, he has been learning PowerShell, and he can remote into the workstation using **PowerShell over SSH**.
>
> **Task:** Use the PowerShell console to navigate throughout the endpoint to find the hidden contents to reveal what was hidden in the stockings.
>
> Watch JohnHammond's video on solving this task!



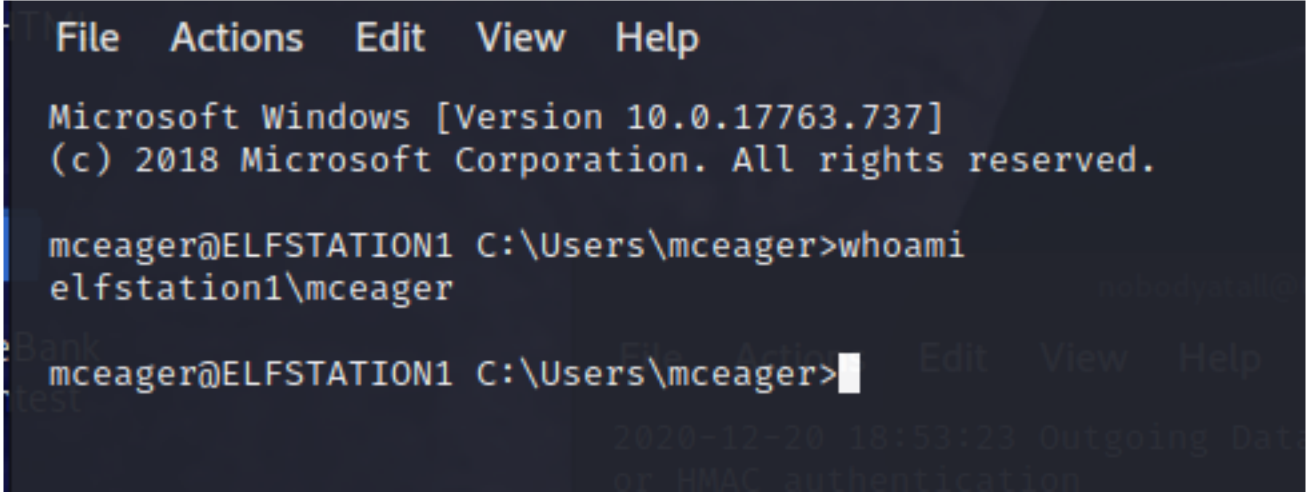
You will use SSH to connect to the remote machine.

The command to run to connect to the remote machine: `ssh -l mceager 10.10.134.95`

```
root@ip-10-10-7-58:~# ssh -l mceager 3.248.248.133
```

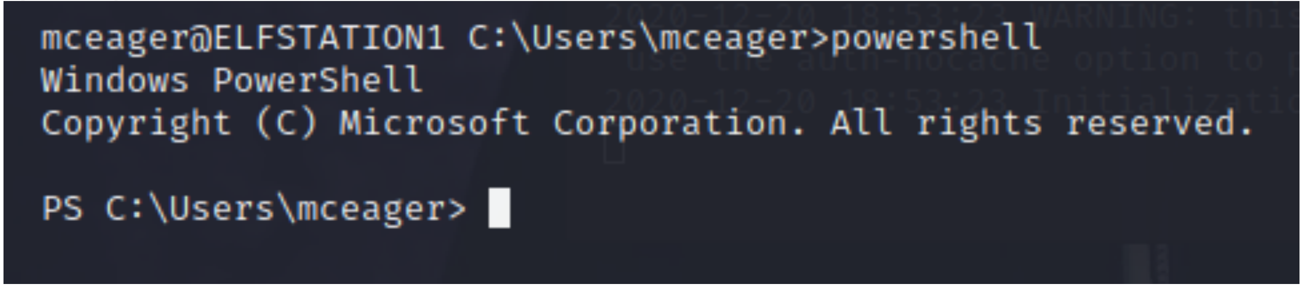
Note that your IP address will be different. When prompted, enter the password: `r0ckStar!`

gain access to the remote powershell via SSH



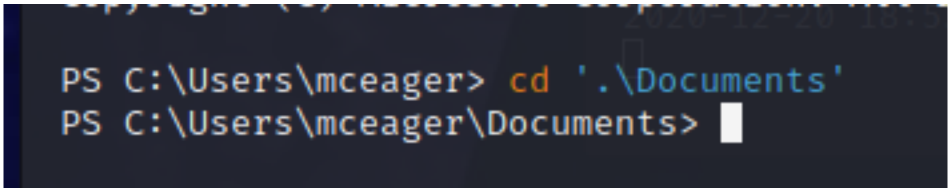
```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

mceager@ELFSTATION1 C:\Users\mceager>whoami
elfstation1\mceager

mceager@ELFSTATION1 C:\Users\mceager>
```

spawn powershell



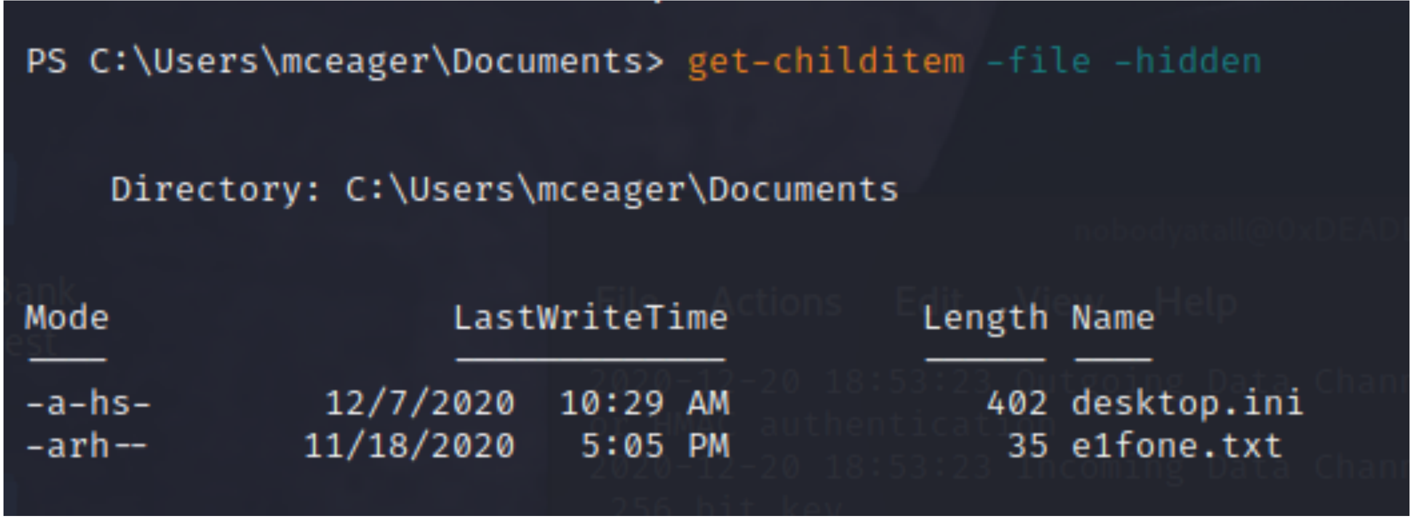
```
mceager@ELFSTATION1 C:\Users\mceager>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\mceager>
```

navigate to the Documents



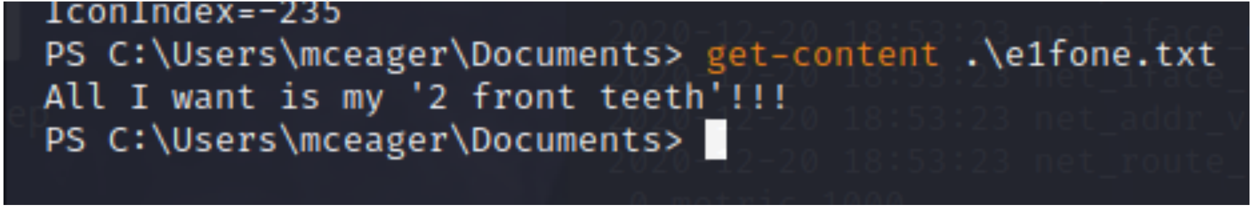
```
PS C:\Users\mceager> cd '.\Documents'
PS C:\Users\mceager\Documents>
```

finding the 1st hidden content in documents, the text file might be the one



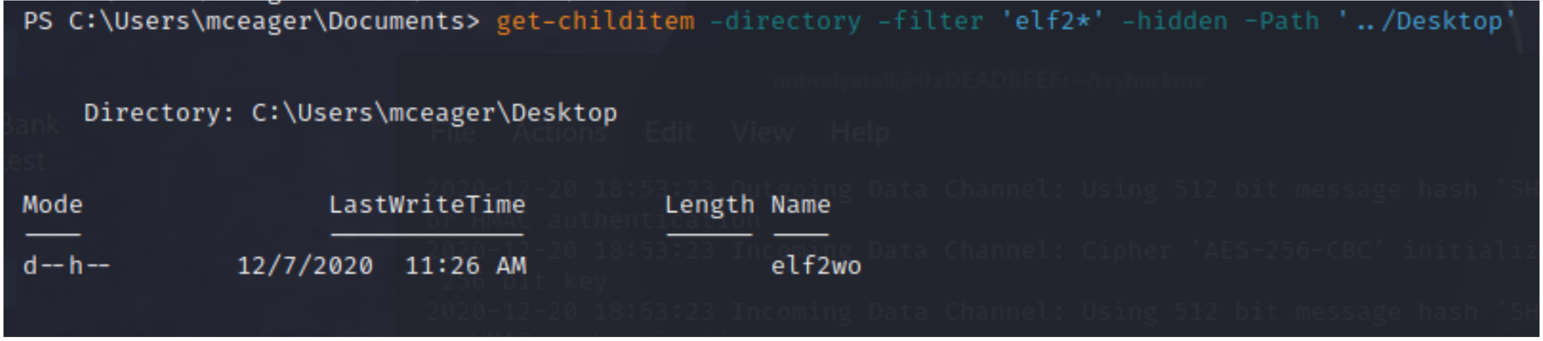
```
PS C:\Users\mceager\Documents> get-childitem -file -hidden


    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
```

content of e1fone.txt, so what elf 1 need was his own 2 front teeth



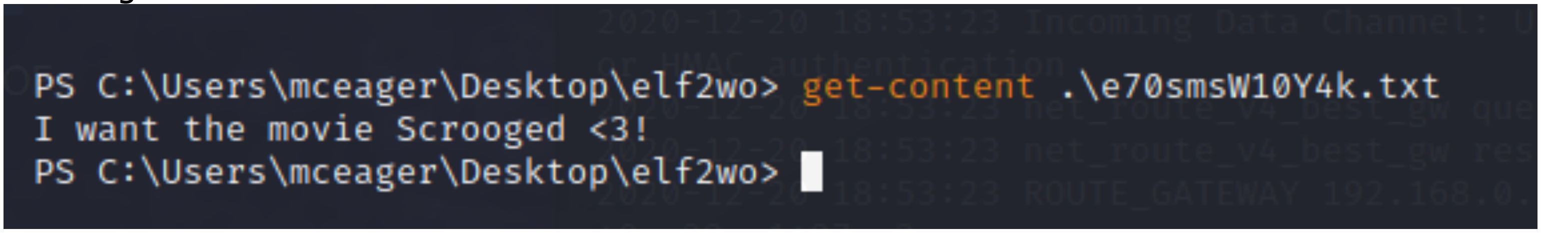
```
IconIndex=-235
PS C:\Users\mceager\Documents> get-content .\e1fone.txt
All I want is my '2 front teeth'!!!
PS C:\Users\mceager\Documents>
```

search for the hidden directory that contain elf2 this keyword & we found it in the Desktop directory



```
PS C:\Users\mceager\Documents> get-childitem -directory -filter 'elf2*' -hidden -Path '../Desktop'


    Directory: C:\Users\mceager\Desktop


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

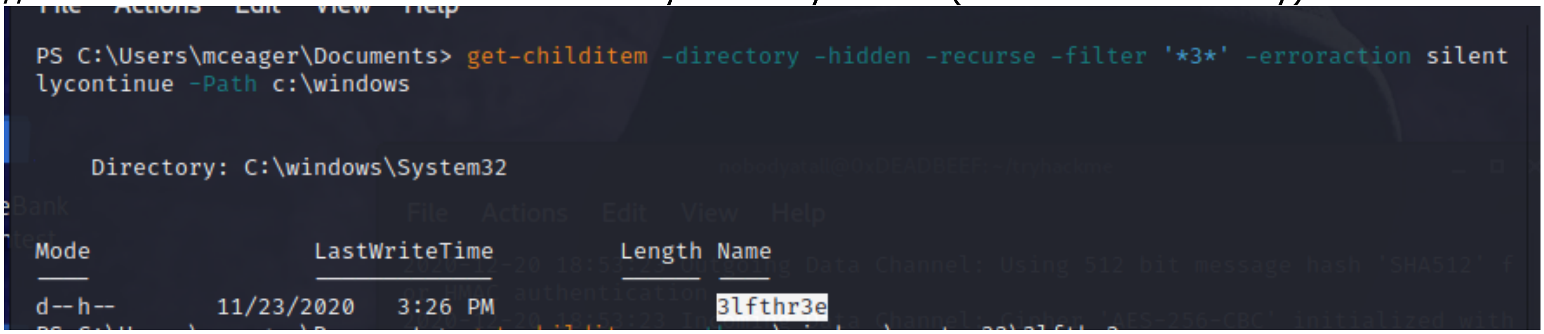
checking the content of it & we found what elf2 wants for movie



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

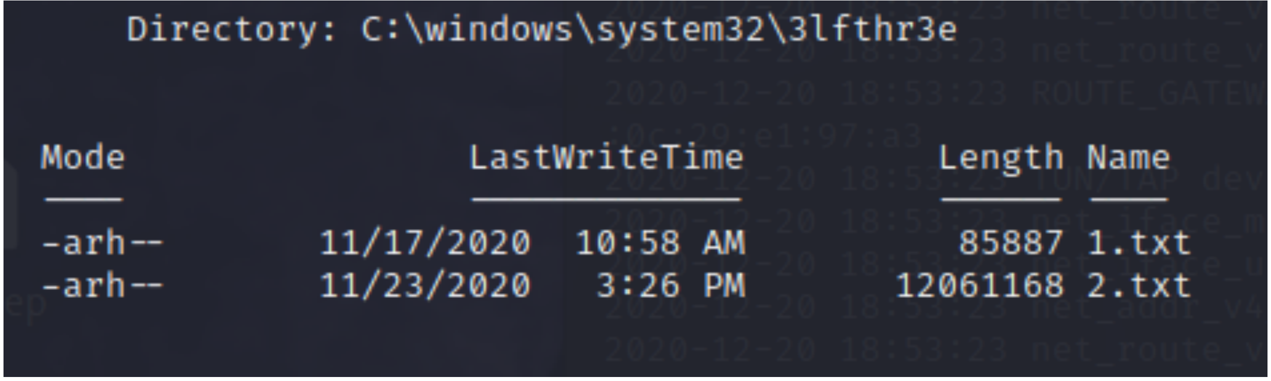
now let's search for the folder that contained Elf 3 files, based on the previous 2 result, the elf3 file might have a ‘3’ keyword in it

// and we've found the Elf3 hidden directory in the System32 (it's a hidden directory)



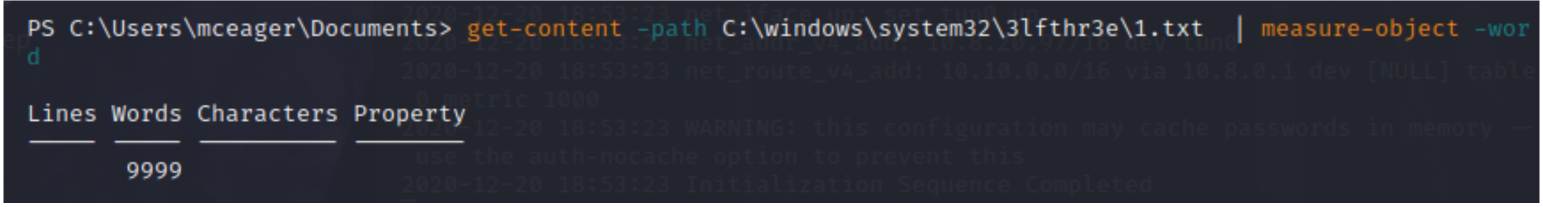
```
PS C:\Users\mceager\Documents> get-childitem -directory -hidden -recurse -filter '*3*' -erroraction silent
lycontinue -Path c:\windows


    Directory: C:\windows\System32


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

in the directory there's 2 files



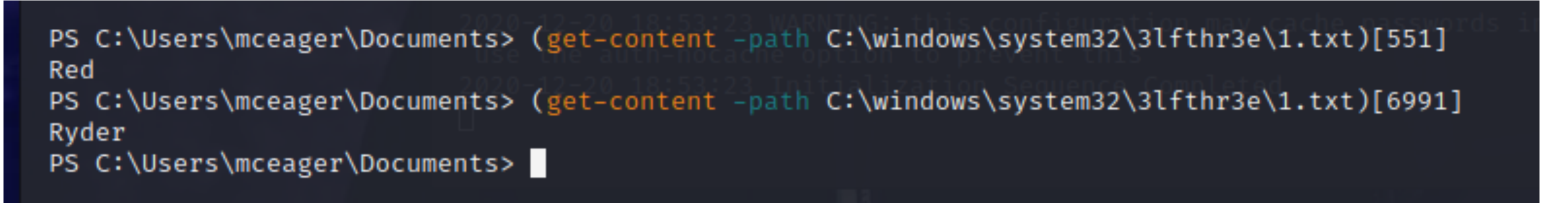
```
    Directory: C:\windows\system32\3lfthr3e


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

checking how many words contain in 1.txt



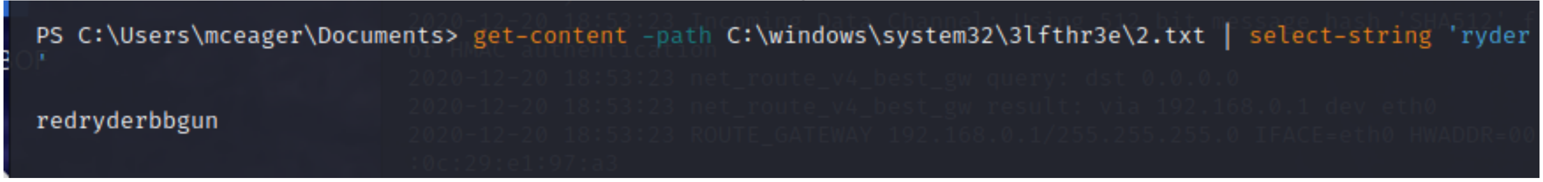
```
PS C:\Users\mceager\Documents> get-content -path C:\windows\system32\3lfthr3e\1.txt  | measure-object -wor
d

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

getting the 2 words(index 551 & 6991) from the 1.txt files



```
PS C:\Users\mceager\Documents> (get-content -path C:\windows\system32\3lfthr3e\1.txt)[551]
Red
PS C:\Users\mceager\Documents> (get-content -path C:\windows\system32\3lfthr3e\1.txt)[6991]
Ryder
PS C:\Users\mceager\Documents>
```

searching for the 2nd file & search for the string containing the keyword ‘red’ OR ‘ryder’
//& we've found the string
//after applied whitespace it would be: red ryder bbgun



```
PS C:\Users\mceager\Documents> get-content -path C:\windows\system32\3lfthr3e\2.txt | select-string 'ryder
'

redryderbbgun
```