PSP 0201
Week 5 Writeup

Group name: Dude Not Perfect

ID	Name	Role
1211102399	Ho Teck Fung	Leader
1211102289	Tan Teng Hui	Member
1211101802	Tan Wei Tong	Member
1211101795	Ong Zi Yang	Member

Day 16: Scripting – Help! Where is Santa?

Tools used: Terminal, kali linux, firefox

Solution/Walkthrough:

Question 1

Use nmap -v 10.10.249.218 to know the port number for the web server and the answer is 80.

```
┌──(1211102289㉿kali)-[~]
└─$ nmap -v 10.10.249.218
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-06 22:16 EDT
Initiating Ping Scan at 22:16
Scanning 10.10.249.218 [2 ports]
Completed Ping Scan at 22:16, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:16
Completed Parallel DNS resolution of 1 host. at 22:16, 0.01s elapsed
Initiating Connect Scan at 22:16
Scanning 10.10.249.218 [1000 ports]
Discovered open port 22/tcp on 10.10.249.218
Discovered open port 80/tcp on 10.10.249.218
Increasing send delay for 10.10.249.218 from 0 to 5 due to max_successful_tryno increase to 4
Increasing send delay for 10.10.249.218 from 5 to 10 due to max_successful_tryno increase to 5
Increasing send delay for 10.10.249.218 from 10 to 20 due to max_successful_tryno increase to 6
Increasing send delay for 10.10.249.218 from 20 to 40 due to 11 out of 13 dropped probes since last increase.
Increasing send delay for 10.10.249.218 from 40 to 80 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 10.10.249.218 from 80 to 160 due to 11 out of 12 dropped probes since last increase
.
Completed Connect Scan at 22:18, 77.97s elapsed (1000 total ports)
Nmap scan report for 10.10.249.218
Host is up (0.19s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 78.37 seconds
```

Question 2

To find out the correct API key we need to create a python file and I named it to brute.py. Then nano the python file and type out the codes so that we can get the answer.

```
┌──(1211102289㉿kali)-[~/Desktop/py]
└─$ nano brute.py
```

```
  GNU nano 6.2
import requests
#    http://10.10.249.218:80/api/4
    {"item_id":5,"q":"Error. Key not valid!"}
url = 'http://10.10.249.218:80/api/'
#r = requests.get(url)

#print(r.text)


for i in range(1,100,2):
        r = requests.get(url+str(i))
        if 'Error' not in r.text:
                print(i)
                print(r.text)
```

```
┌──(1211102289㉿kali)-[~/Desktop/py]
└─$ python3 brute.py
57
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}
```

Thought Process/Methodology: First, I need to nmap the machine ip address to scan the web server so that Ican know the port number is 80. After that, I need to create a python file in the desktop/py and I named it to brute.py.At last, I nano the brute.py and type out the codes to get the answer for the correct API key and the location of santa.

Day 17: Reverse Engineering – ReverseELFneering

Tools used: Terminal

Solution/Walkthrough:

```
File  Edit  View  Search  Terminal  Help
root@ip-10-10-129-165:~# echo "10.10.59.238" > target.txt
root@ip-10-10-129-165:~# cat target.txt
10.10.59.238
root@ip-10-10-129-165:~# ssh elfmceager@10.10.59.238
The authenticity of host '10.10.59.238 (10.10.59.238)' can't be established.
ECDSA key fingerprint is SHA256:XrBuXSQs0wRKhvVRdrSfE/0F5ccAZQiXAhMhzB1dV7U.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.59.238' (ECDSA) to the list of known hosts.
elfmceager@10.10.59.238's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-128-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Jul 16 23:14:34 UTC 2022

  System load:  0.0                Processes:           92
  Usage of /:   39.4% of 11.75GB   Users logged in:     0
  Memory usage: 8%                 IP address for ens5: 10.10.59.238
  Swap usage:   0%


0 packages can be updated.
0 updates are security updates.


Last login: Wed Dec 16 18:25:51 2020 from 192.168.190.1
elfmceager@tbfc-day-17:~$ r2 -d ./challenge1
Process with PID 1571 started...
= attach 1571 1571
bin.baddr 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.bits 64
```

Start terminal and type echo "10.10.59.238" > target.txt, then type cat target.txt, then login ssh using username and password given, then type r2 -d ./challenge1

```
pdf @main

 WARNING : block size exceeding max block size at 0x006ba220
[+] Try changing it with e anal.bb.maxsize
 WARNING : block size exceeding max block size at 0x006bc860
[+] Try changing it with e anal.bb.maxsize
[x] Analyze all flags starting with sym. and entry0 (aa)
            ;-- main:in
/ (fcn) sym.main 35
|   sym.main ();
|           ; var int local_ch @ rbp-0xc
|           ; var int local_8h @ rbp-0x8
|           ; var int local_4h @ rbp-0x4
|              ; DATA XREF from 0x00400a4d (entry0)
|           0x00400b4d      55              push rbp
|           0x00400b4e      4889e5          mov rbp, rsp
|           0x00400b51      c745f4010000.   mov dword [local_ch], 1
|           0x00400b58      c745f8060000.   mov dword [local_8h], 6
|           0x00400b5f      8b45f4          mov eax, dword [local_ch]
|           0x00400b62      0faf45f8        imul eax, dword [local_8h]
|           0x00400b66      8945fc          mov dword [local_4h], eax
|           0x00400b69      b800000000      mov eax, 0
|           0x00400b6e      5d              pop rbp
\           0x00400b6f      c3              ret
[0x00400a30]>
THM AttackBox
```

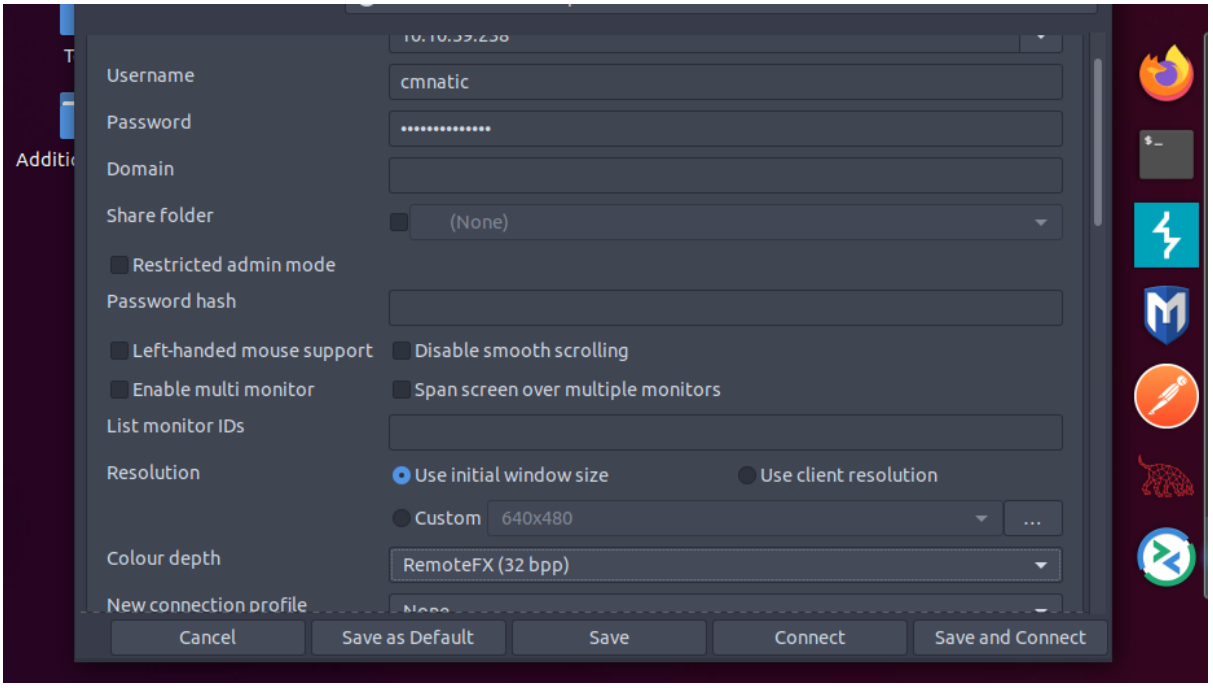
After that type pdf @main and you will get answers for question 1, 2 and 3. Answer for question 1 is 1, question 2 is 6, and question 3 is 6

Thought Process/Methodology: The first thing we want to do is SSH into our target machine with the username elfmceager and the password adventofcyber. Then use pdf @ main command to get a closer look at pdf and we will find answer there.

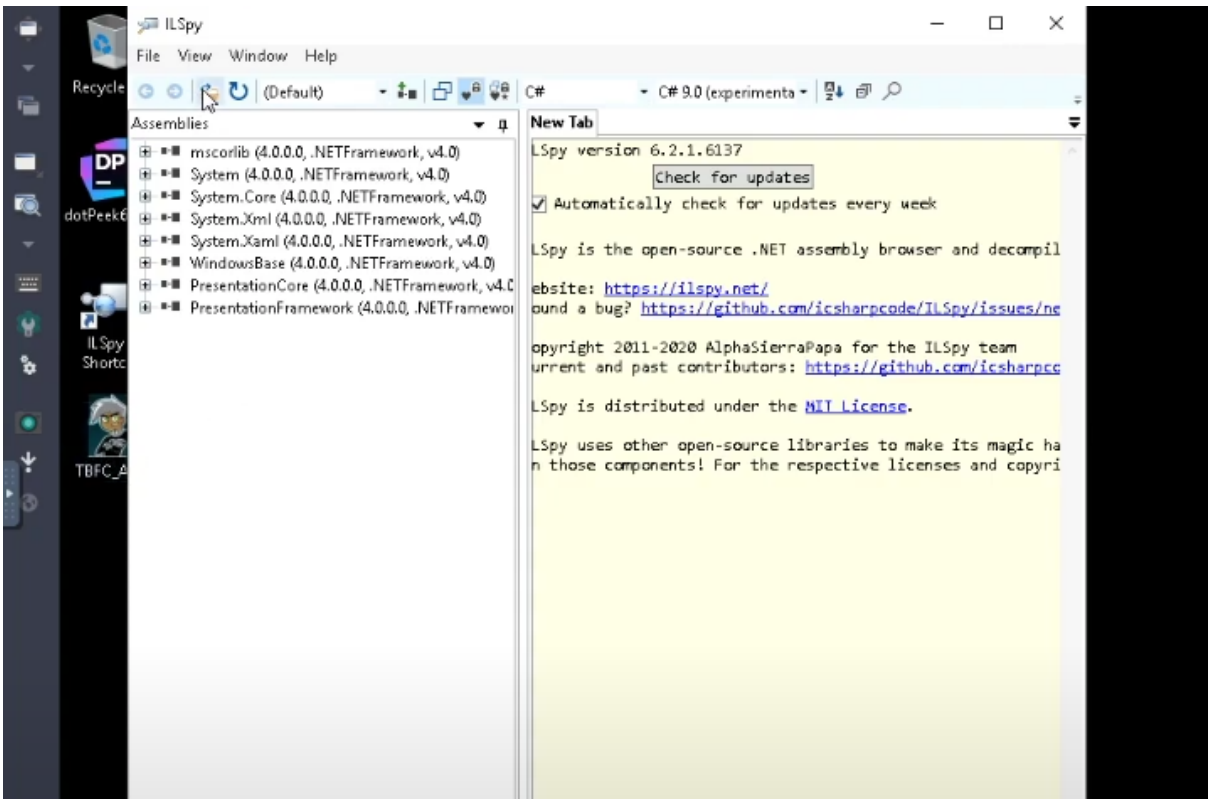
Day 18: Reverse Engineering – The Bits of Christmas

Tools used: remmina

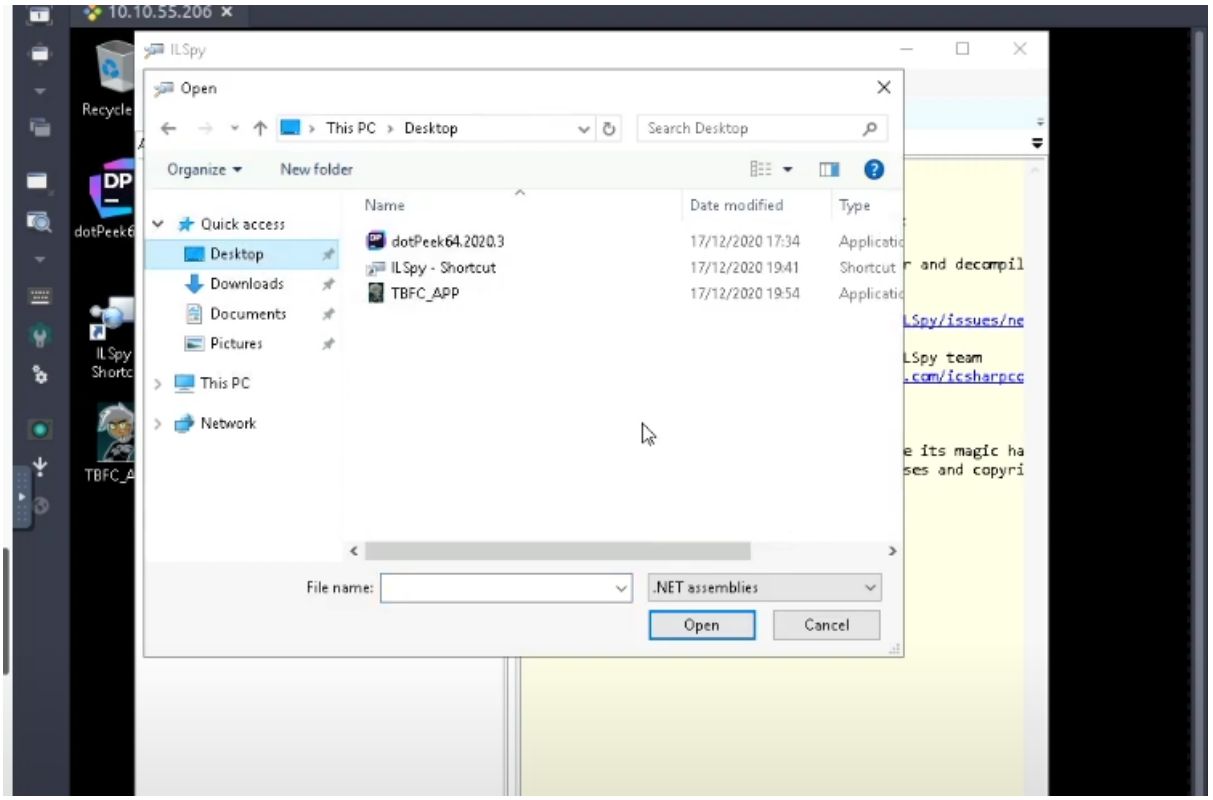
Solution/Walkthrough:



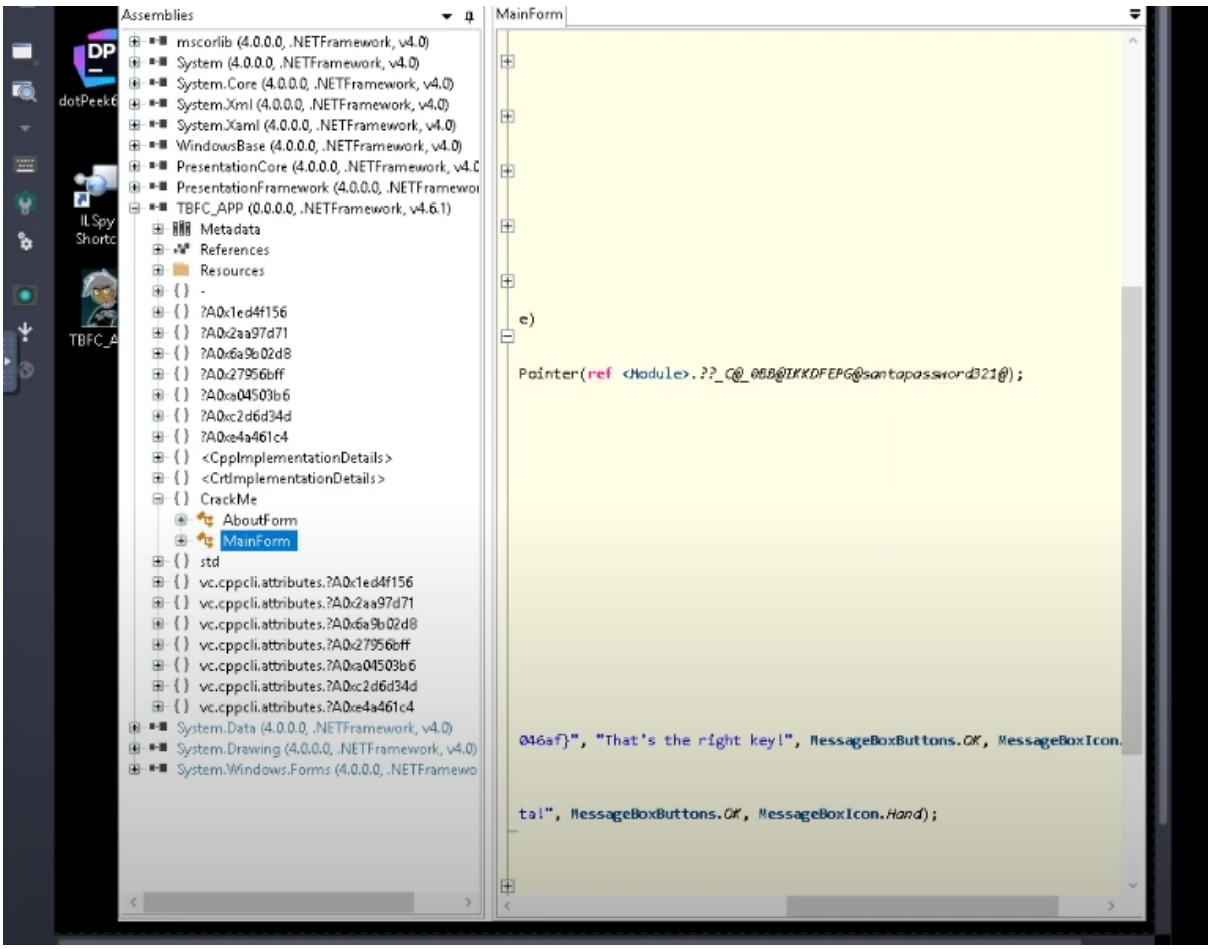
Open remmina, then log in using the username and password given and change the colour depth to remoteFX(32 bpp)



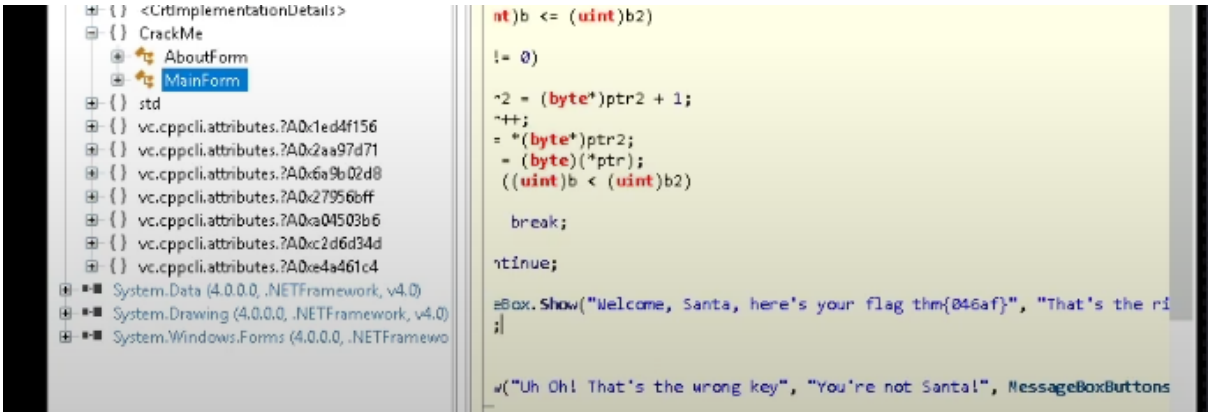
Then open IL Spy



Then open TBFC_APP



Then search for mainform and u will find password there and this password is question 1 answer, santapassword321



After that, u can also find the flag there, the flag is question 2 answer, thm{046af}

Thought Process/Methodology: Using the remmina to use ILspy to decompile the code of the TBFC_APP and all the answers can be found there

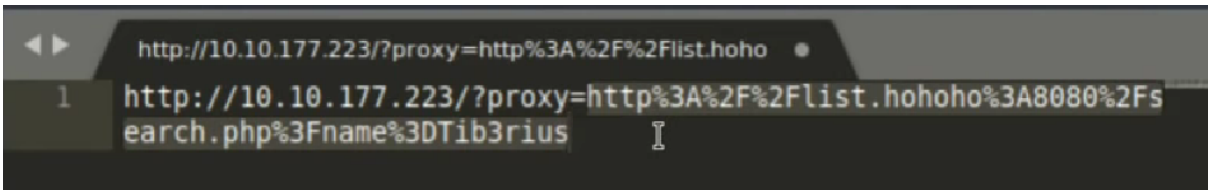
Day 19: Web Exploitation – The Naughty or Nice List

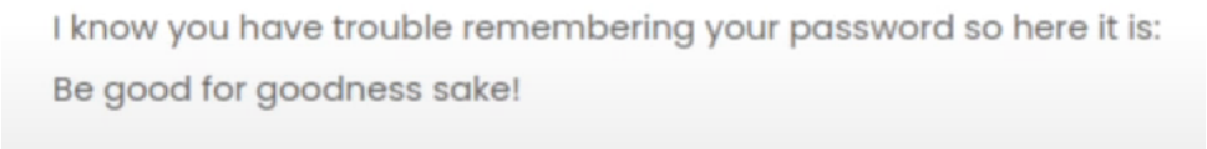
Tools used: Firefox, Sublime Text, CyberChef, Terminal

Solution/Walkthrough:

Question 1

Enter a name in the form and click the "Search" button.
When the page loads, it should tell you whether that name is on the Naughty List or the Nice List.
If we use a URL decoder on the value of the "proxy" parameter, we get:
http://list.hohoho:8080/search.php?name="name"

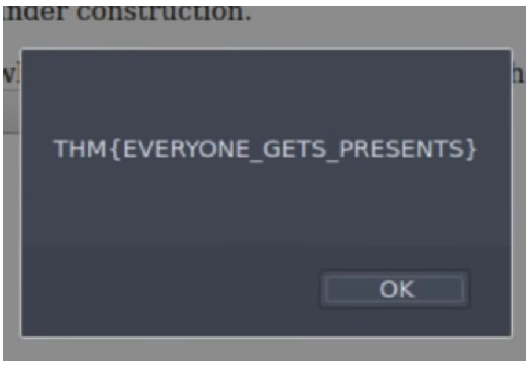




Santa's password is "Be good for goodness sake!"

Question 2

Click "DELETE NAUGHTY LIST"



The challenge flag is "THM{EVERYONE_GETS_PRESENTS}"

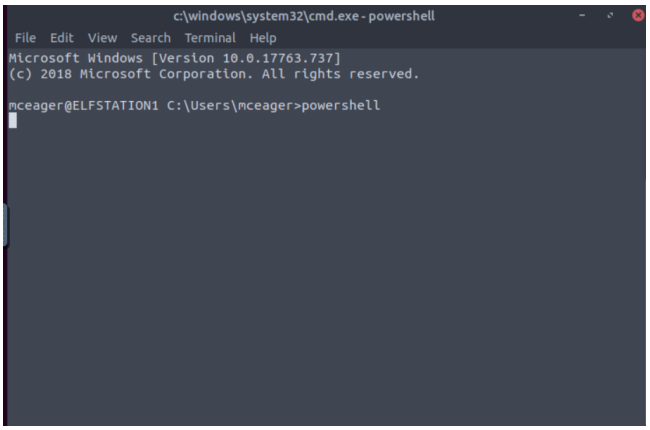
Thought Process/Methodology: Following the walkthrough, I've learned that using a URL decoder, I can get a URL.

Day 20: Blue Teaming – PowershELIF to the rescue

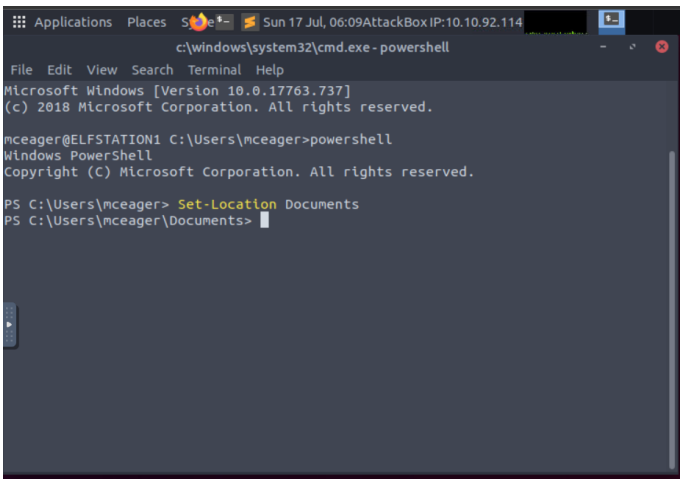
Tools used: **Solution/Walkthrough:Cmd**

Question 1

First, open cmd then enter the ssh command to connect mceager machine. Enter the powershell in cmd to launch powershell.



After powershell has launch navigate to document folder



Then use -file -hidden to search for hidden files

```
c:\windows\system32\cmd.exe - powershell
File  Edit  View  Search  Terminal  Help
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>
```

```
c:\windows\system32\cmd.exe - powershell
File  Edit  View  Search  Terminal  Help
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> Cat e1fone.txt
All I want is my '2 front teeth'!!!
PS C:\Users\mceager\Documents>
```

After that,the system will indicate two hidden files for you.Use cat to get the information in the file then you will be able to get the answer.

Question 2

Firstly use set-location to navigate to the desktop. Then use ls - hidden (-hidden is used to search for hidden items). After that, the system will show you two hidden items

```
c:\windows\system32\cmd.exe - powershell
File  Edit  View  Search  Terminal  Help
exist.
At line:1 char:1
+ cd ....
+ ~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Set-Location], PSArgumentE
   xception
    + FullyQualifiedErrorId : Argument,Microsoft.PowerShell.Commands.SetLocati
   onCommand

PS C:\Users\mceager\Documents> cd ..
PS C:\Users\mceager> set-location desktop
PS C:\Users\mceager\desktop> ls -Hidden

    Directory: C:\Users\mceager\desktop

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d--h--        12/7/2020  11:26 AM                elf2wo
-a-hs-        12/7/2020  10:29 AM            282 desktop.ini

PS C:\Users\mceager\desktop>
```

After that, use set-location to elf2wo then use get-childitem it will show you the directory

```
c:\windows\system32\cmd.exe - powershell
File  Edit  View  Search  Terminal  Help
PS C:\Users\mceager\desktop> set-location elf2wo
PS C:\Users\mceager\desktop\elf2wo> get-chliditem
get-chliditem : The term 'get-chliditem' is not recognized as the name of a
cmdlet, function, script file, or operable program. Check the spelling of the
name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ get-chliditem
+ ~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (get-chliditem:String) [], Comma
   ndNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

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>
```

Use cat to get the information inside the file.

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

Question 3

Enter cd c:/windows in cmd than enter cd system 32

```
c:\windows\system32\cmd.exe - powershell
File  Edit  View  Search  Terminal  Help
-a----         9/6/2019   5:28 PM         230848 xmllite.dll
-a----        9/15/2018  12:12 AM          22016 xmlprovi.dll
-a----        9/15/2018  12:12 AM          64000 xolehlp.dll
-a----        9/15/2018  12:12 AM         352768 XpsDocumentTargetPrint.dll
-a----        9/15/2018   2:08 AM         922112 XpsFilt.dll
-a----        9/15/2018  12:12 AM         471040 XpsGdiConverter.dll
-a----         9/6/2019   5:29 PM        1671680 XpsPrint.dll
-a----        9/15/2018  12:12 AM         582656 XpsRasterService.dll
-a----         9/6/2019   5:29 PM        4488192 xpsrchvw.exe
-a----        9/15/2018   2:08 AM          76060 xpsrchvw.xml
-a----         9/6/2019   5:29 PM        2879488 xpsservices.dll
-a----        9/15/2018   2:08 AM          99328 XPSSHHDR.dll
-a----        9/15/2018  12:12 AM           4014 xwizard.dtd
-a----        9/15/2018  12:12 AM          62464 xwizard.exe
-a----        9/15/2018  12:12 AM         448000 xwizards.dll
-a----        9/15/2018  12:12 AM         118272 xwreg.dll
-a----        9/15/2018  12:12 AM         257536 xwtpdui.dll
-a----        9/15/2018  12:12 AM         143360 xwtpw32.dll
-a----        9/15/2018  12:12 AM          79872 zipcontainer.dll
-a----         9/6/2019   5:29 PM         429568 zipfldr.dll
-a----        9/15/2018  12:12 AM          30720 ztrace_maps.dll

PS C:\Windows\system32>
```

Then enter get-childitem -Hidden -Directory - Filter “*3*” After that the system will show you the result .

```
c:\windows\system32\cmd.exe - powershell
File  Edit  View  Search  Terminal  Help
-a----        9/15/2018   2:08 AM          99328 XPSSHHDR.dll
-a----        9/15/2018  12:12 AM           4014 xwizard.dtd
-a----        9/15/2018  12:12 AM          62464 xwizard.exe
-a----        9/15/2018  12:12 AM         448000 xwizards.dll
-a----        9/15/2018  12:12 AM         118272 xwreg.dll
-a----        9/15/2018  12:12 AM         257536 xwtpdui.dll
-a----        9/15/2018  12:12 AM         143360 xwtpw32.dll
-a----        9/15/2018  12:12 AM          79872 zipcontainer.dll
-a----         9/6/2019   5:29 PM         429568 zipfldr.dll
-a----        9/15/2018  12:12 AM          30720 ztrace_maps.dll

PS C:\Windows\system32> get-childitem -Hidden -Directory -Filter "*3*"

    Directory: C:\Windows\system32

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

PS C:\Windows\system32>
```

Question 4

Once you enter the 3lfthr3e folder you will be able to see two files. Enter Get-content 1.txt | Measure-object the system will how many words the file contains

```
c:\windows\system32\cmd.exe - powershell
File  Edit  View  Search  Terminal  Help

    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

PS C:\Windows\system32\3lfthr3e> Get-content 1.txt | Measure-object

Count    : 9999
Average  :
Sum      :
Maximum  :
Minimum  :
Property :

PS C:\Windows\system32\3lfthr3e>
```

Question 5

In the same file use get-content 1.txt and indicate the number behind to locate the word that you needed.

```
c:\windows\system32\cmd.exe - powershell
File  Edit  View  Search  Terminal  Help
Average  :
Sum      :
Maximum  :
Minimum  :
Property :



PS C:\Windows\system32\3lfthr3e> (Get-content 1.txt)(551,6691)
At line:1 char:20
+ (Get-content 1.txt)(551,6691)
+                    ~
Unexpected token '(' in expression or statement.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordEx
  ception
    + FullyQualifiedErrorId : UnexpectedToken

PS C:\Windows\system32\3lfthr3e> (Get-content 1.txt)[551,6691]
Red
compressed
PS C:\Windows\system32\3lfthr3e> (Get-content 1.txt)[551,6991]
Red
Ryder
PS C:\Windows\system32\3lfthr3e>
```

Question 6

Use get-content to get content in the second file behind the command add | select-string - Pattern “redryder” than you will be able to get the answer.

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

redryderbbgun


PS C:\Windows\System32\3lfthr3e>
```

Thought Process/Methodology: Using powershell to find the hidden content.