

PSP0201

Week 5

Writeup

Group Name: DHM

Members:

ID	Name
1211101851	ANG ZHE JIE
1211103790	KOK YEW YAN
1211103039	OOI YI SIANG
1211104005	WONG CHUN RONG

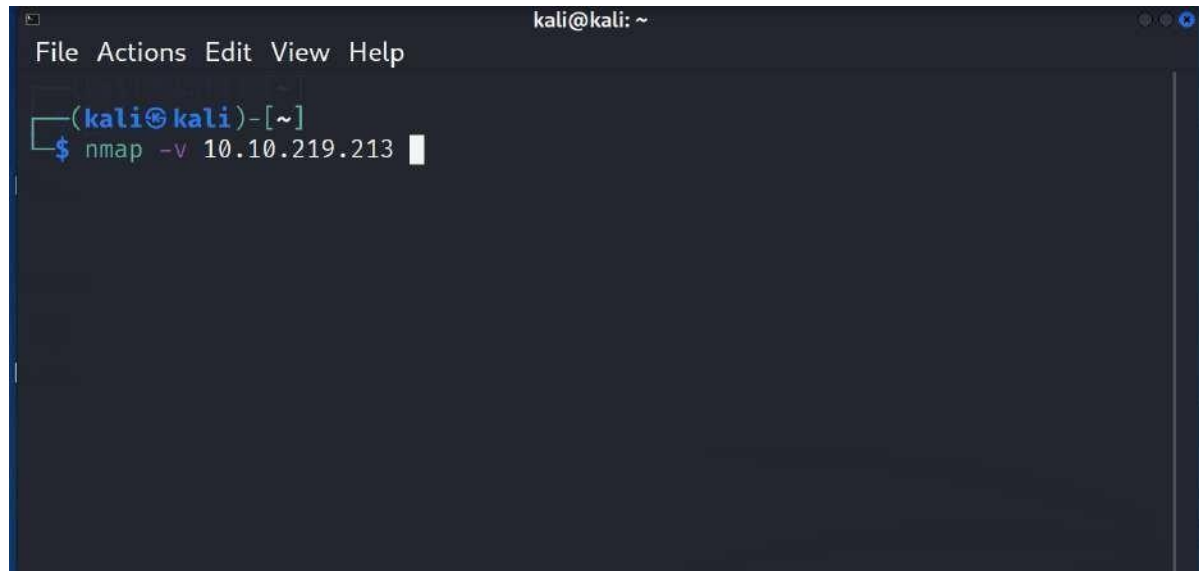
Day 16: Scripting - Help! Where is Santa?

Tools used: Firefox, Python

Solution/walkthrough:

Question 1:

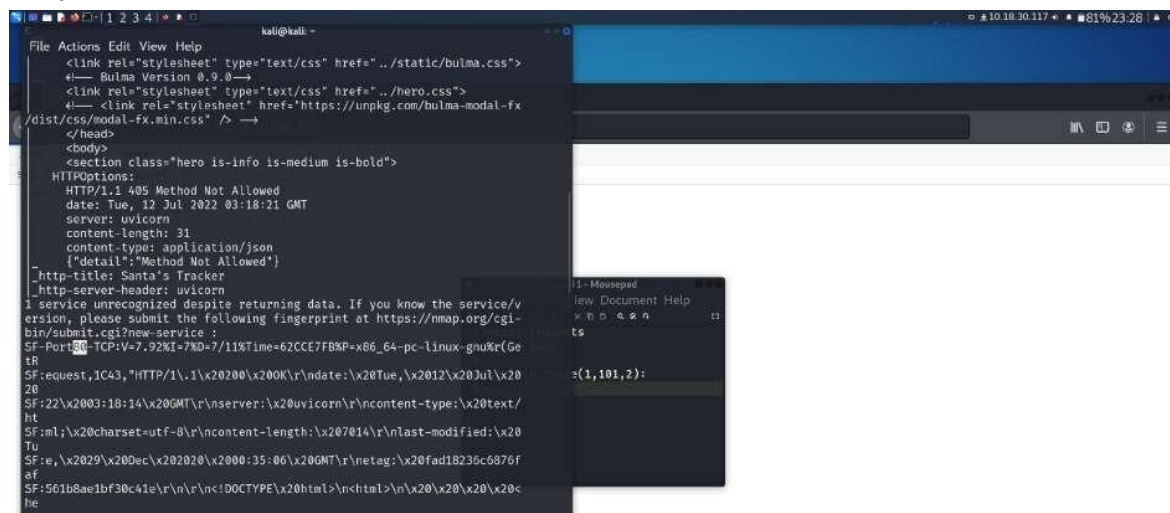
After starting the machine, type nmap -v and key in IP address

A terminal window titled 'kali@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(kali@kali)-[~]'. The command '\$ nmap -v 10.10.219.213' has been entered, and the cursor is at the end of the line.

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ nmap -v 10.10.219.213
```

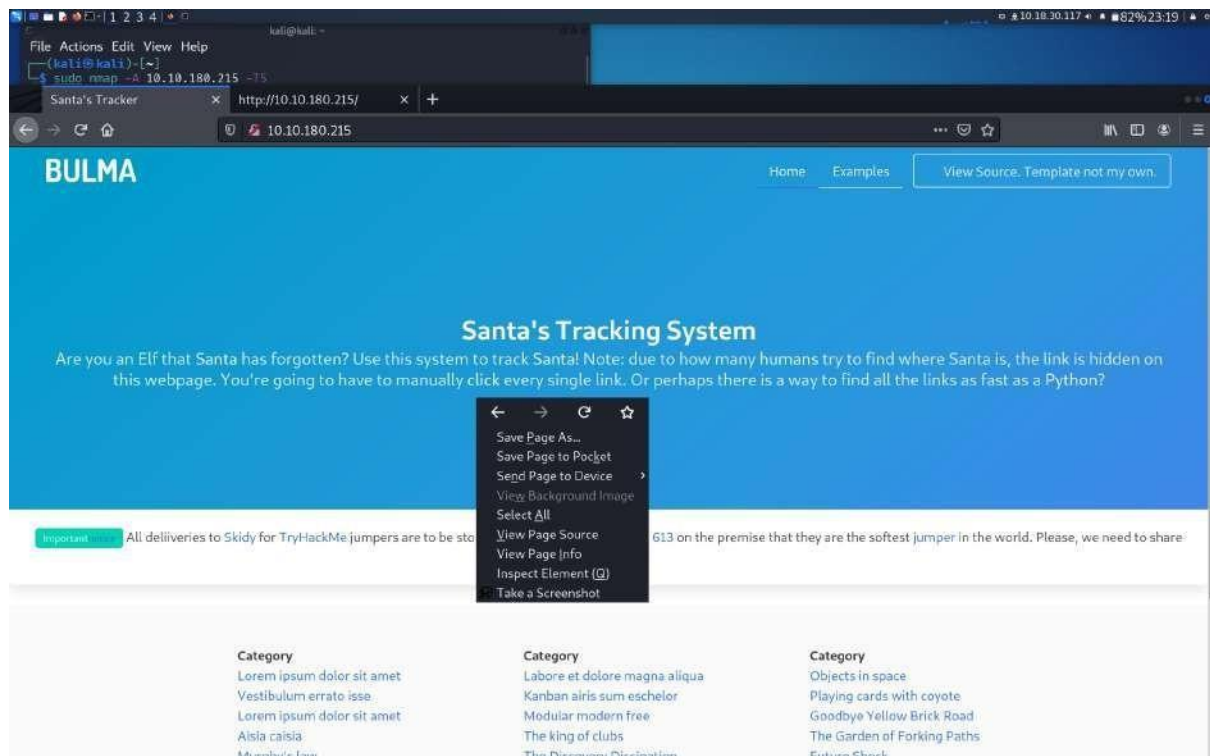
the port will be shown

Two screenshots are shown. The left one is a terminal window displaying the output of the nmap scan. The right one is a Firefox browser window showing a web page with a blue header and a white body. The terminal output shows the nmap command and its results, including the IP address 10.10.219.213 and the port 101.

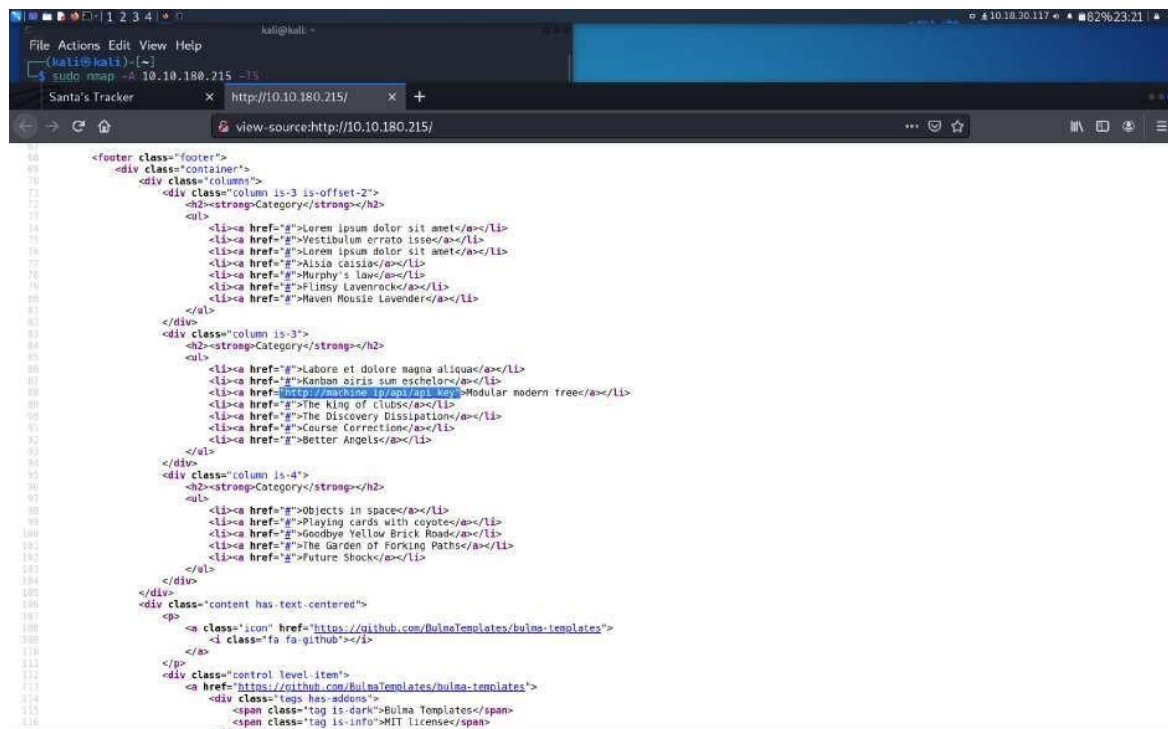
```
kali@kali: ~
File Actions Edit View Help
<link rel="stylesheet" type="text/css" href="..static/bulma.css">
<link rel="stylesheet" type="text/css" href="..hero.css">
<link rel="stylesheet" type="text/css" href="https://unpkg.com/bulma-modal-fx
/dist/css/modal-fx.min.css" />
</head>
<body>
<section class="hero is-info is-medium is-bold">
  HTTPOptions:
  HTTP/1.1 405 Method Not Allowed
  date: Tue, 12 Jul 2022 03:18:21 GMT
  server: uvicorn
  content-length: 31
  content-type: application/json
  {"detail": "Method Not Allowed"}
  _http-title: Santa's Tracker
  _http-server-header: uvicorn
  1 service unrecognized despite returning data. If you know the service/v
  ersion, please submit the following fingerprint at https://nmap.org/cgi-
  bin/submit.cgi?new-service :
  SF-Port:101-TCP:V=7.92I=7ND=7/11%Time=62CCE7FB&P=x86_64-pc-linux-gnu&r(Ge
  tr
  SF:quest,1C43,"HTTP/1\1\1x20200\200K\r\ndate:\x20Tue,\x2012\x20Jul\x20
  20
  SF:22\x2003:18:14\x20GMT\r\nserver:\x20uvicorn\r\ncontent-type:\x20text/
  ht
  SF:ml;\x20charset=utf-8\r\ncontent-length:\x207014\r\nlast-modified:\x20
  Tu
  SF:e,\x2029\x20Dec\x202020\x2000:35:06\x20GMT\r\netag:\x20fad18236c6976f
  af
  SF:561b8ae1bf30c41e\r\n\r\n<!DOCTYPE\x20html>\nhtml>\n\n\x20\x20\x20\x20<
  he
```

Question 2:

Open firefox, key in the IP address then right click to view the page resource



And API is shown



Question 3:

The next step, create a new python by using nano brute.py. After that, import requests

```
import requests

#      http://10.10.49.56:8000/api/4

#url = 'http://10.10.49.56:8000/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)
```

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Linter ^_ Go To Line

Then, use python3 and brute.py to show the result

```
kali@kali: ~  
File Actions Edit View Help  
[root]  
└─(kali@kali)-[~]  
└─$ nano brute.py  
└─(kali@kali)-[~]  
└─$ python3 brute.py
```

Santa's Tr

All deliveries to 5x10 for TeyH4ckMe jumpers are to be stopped. That man has i

Category: Lorem ipsum dolor sit amet
Category: Lorem ipsum dolor sit amet

Next, Santa location is shown

```
{"item_id":57,"q1":"Winter Wonderland, Hyde Park, London."}
```

Question 4:

Lastly, the right API key will be shown and it is an odd number.

```
57  
{"item_id":57,"q1":"Winter Wonderland, Hyde Park, London."}
```

Thought Process/Methodology:

First, after starting the machine, key in nmap -v and the IP address. Then, the port is shown. After that, open the firefox and key in the IP address then right click to view the page source. Use Ctrl+f and key in api to search it. The next step, create a new python by using nano brute.py. Next, import requests. And then, I have created a new python which is brute.py. After done command, use python3 and brute.py. Then save and modify it. Moreover, key in python3 and brute.py at the back of the python3. The result is shown. So, we know the location of Santa, which is winter wonderland, hyde park, London.

Day 17: Reverse Engineering - ReverseELFneering

Tools used: Command Prompt, elfmceager

Solution/walkthrough:

Question 1:

First, login by *elfmceager@IPAddress* and enter the password given by THM ----
adventofcyber.

```
(kali@kali)~$ sudo ssh elfmceager@10.10.83.71
[sudo] password for kali:
elfmceager@10.10.83.71'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 14:36:57 UTC 2022

System load:  0.0               Processes:    97
Usage of /:   39.4% of 11.75GB   Users logged in: 1
Memory usage: 10%              IP address for ens5: 10.10.83.71
Swap usage:   0%

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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Sat Jul 16 14:33:23 2022 from 10.18.31.224
elfmceager@tbfc-day-17:~$ ls
challenge1 file1
elfmceager@tbfc-day-17:~$ ls -lsa
ls-lsa: command not found
elfmceager@tbfc-day-17:~$ ls -lsa
total 1688
4 drwxr-xr-x 5 elfmceager elfmceager 4096 Jul 16 14:35 .
4 drwxr-xr-x 3 root      root      4096 Dec 16 2020 ..
0 lrwxrwxrwx 1 elfmceager elfmceager   9 Dec 16 2020 .bash_history -> /dev/null
4 -rw-r--r-- 1 elfmceager elfmceager 220 Apr  4 2018 .bash_logout
4 -rw-r--r-- 1 elfmceager elfmceager 3771 Apr  4 2018 .bashrc
4 drwx----- 2 elfmceager elfmceager 4096 Dec 16 2020 .cache
828 -rwxr-xr-x 1 elfmceager elfmceager 844648 Dec 16 2020 challenge1
4 drwxr-xr-x 2 elfmceager elfmceager 4096 Jul 16 14:35 .config
828 -rwxr-xr-x 1 elfmceager elfmceager 844736 Dec 16 2020 file1
4 drwx----- 3 elfmceager elfmceager 4096 Dec 16 2020 .gnupg
4 -rw-r--r-- 1 elfmceager elfmceager 807 Apr  4 2018 .profile
0 -rw-r--r-- 1 elfmceager elfmceager   0 Dec 16 2020 .sudo_as_admin_successful
```


Question 2:

After analyzing the file, open the file which named "*challenge 1*" and enter the main file ,you will get the value of *local_ch* which is 1.

```
= attach 1/95 1/95
bin.baddr 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.bits 64
[0x00400a30]> aa
[ 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)
[0x00400a30]> pdf @main
;-- main:
/ (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
```

Discover the value of *eax* and *local_4h* which is both 6

```
[0x00400a30]> pdf @main
;-- main:
/ (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
```

Thought Process/Methodology:

The first step, login by using *elfmceager@IPaddress* and enter the password given by THM ---- *adventofcyber*. Then open the file "*challenge 1*" and enter the main page ,then we obtain the value of *local_ch* which is 1 and the value of *eax* is Equal to 6 and the value of *local_4h* in front of *eax* is also 6.

Day 18: Reverse Engineering - The Bits of Christmas

Tools used: Remmina

Solution/walkthrough:

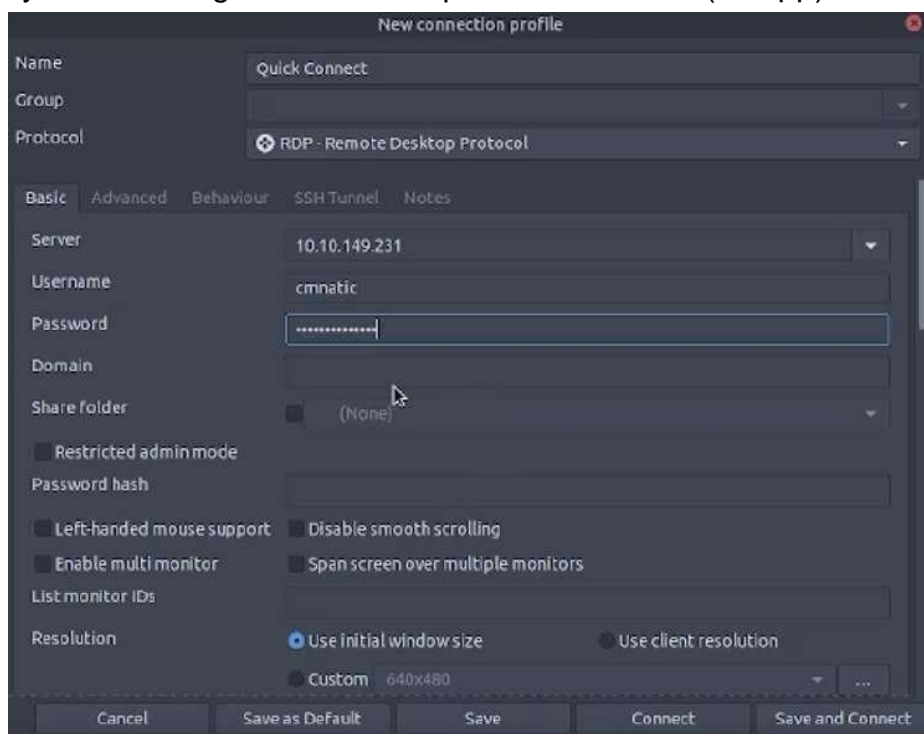
Question 1:

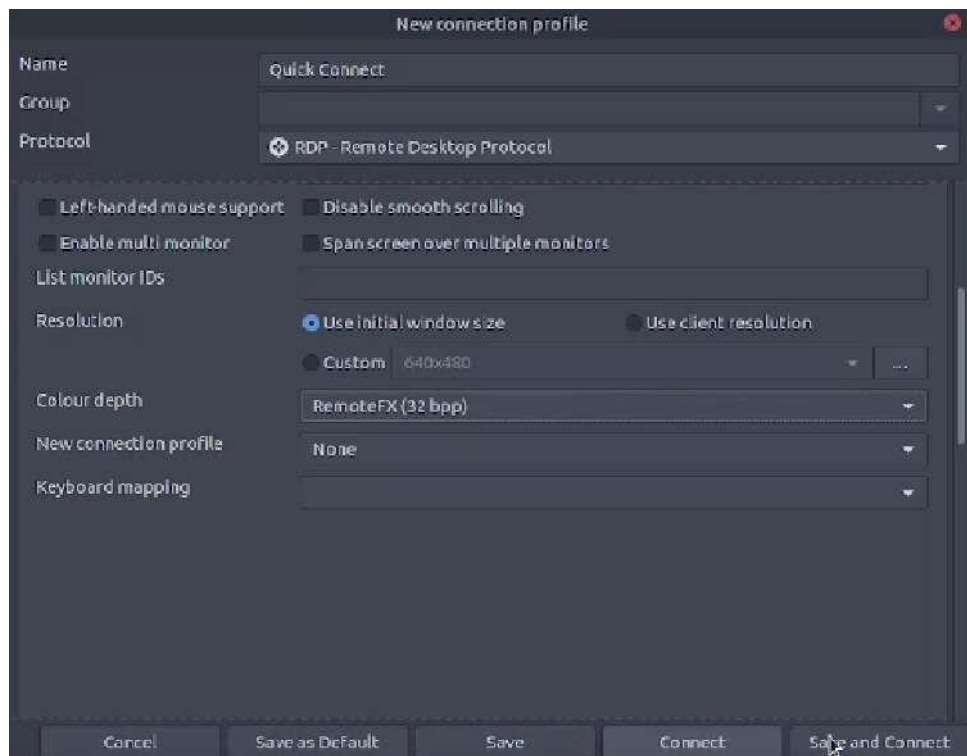
After installing Remmina, it required password to save the session, then press *"Cancel"*.



Question 2:

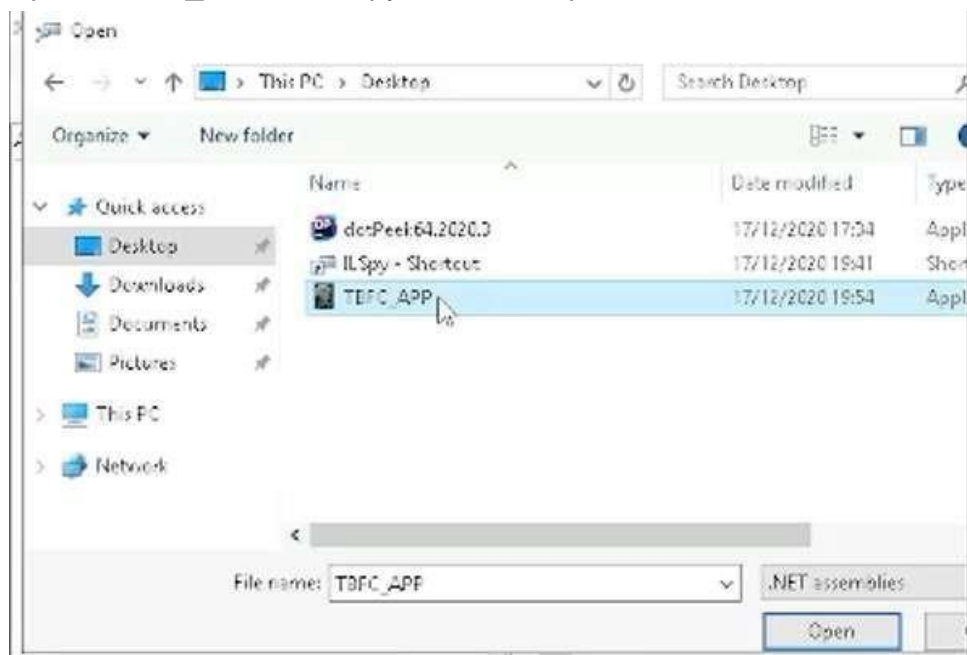
Enter the IP Address, using username *"cmnatic"* and password *"Adventofcyber!"* given by THM. Change the colour depth to *"RemoteFX (32 bpp)"* and *"save and connect"*.

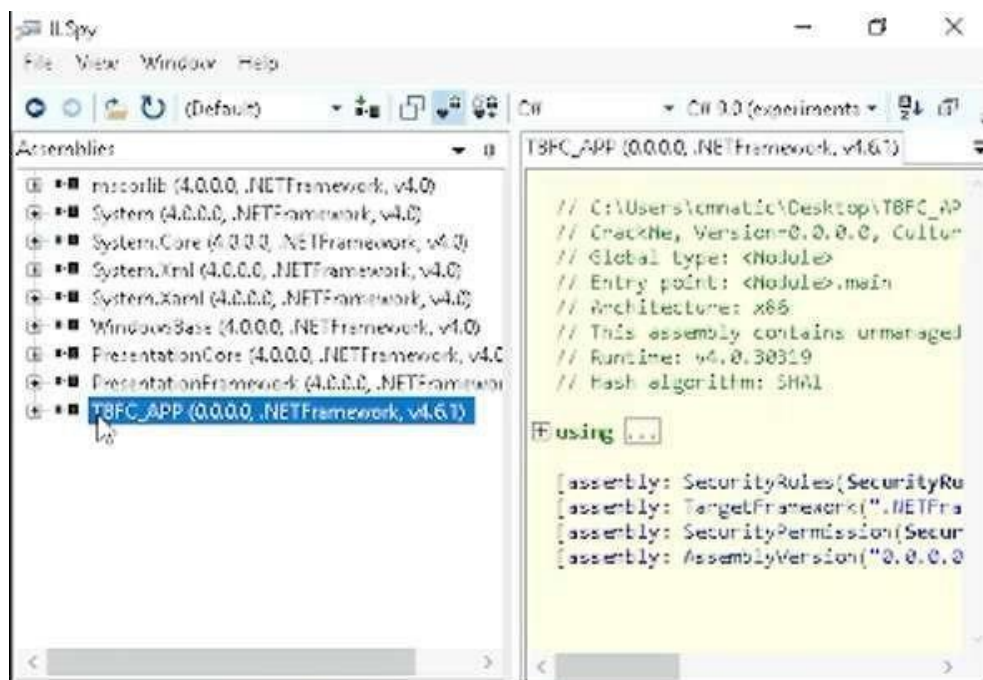




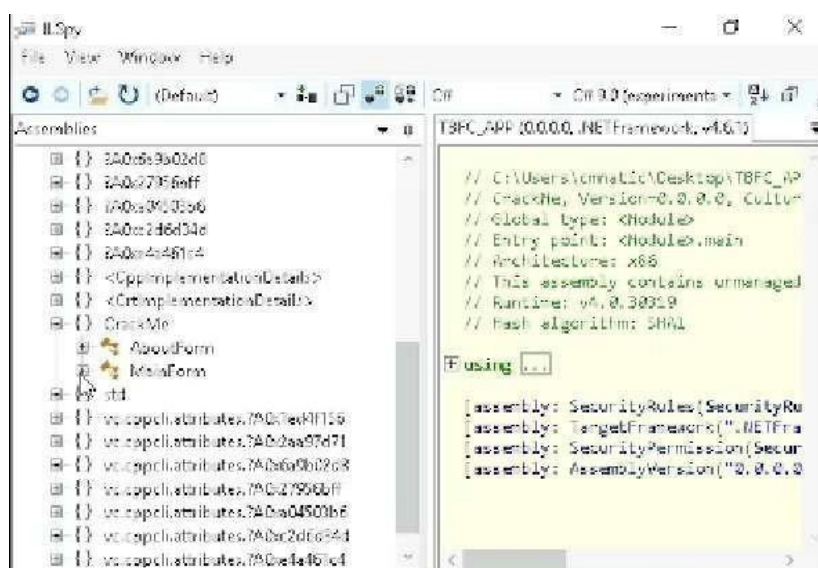
Question 3:

Open "TBFC_APP" in ILSpy and decompile the code.



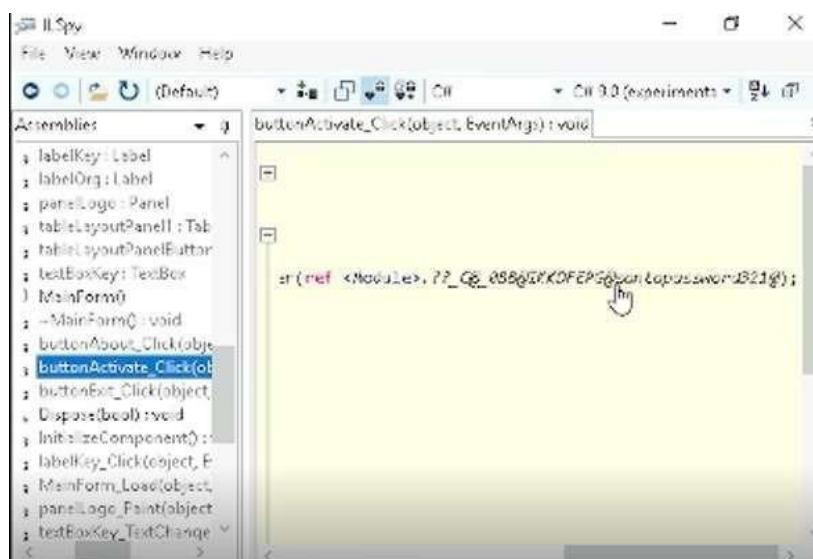
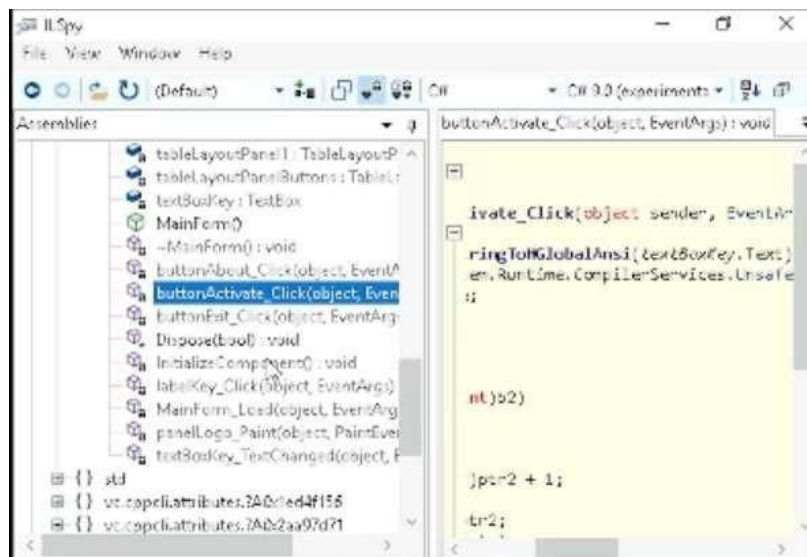


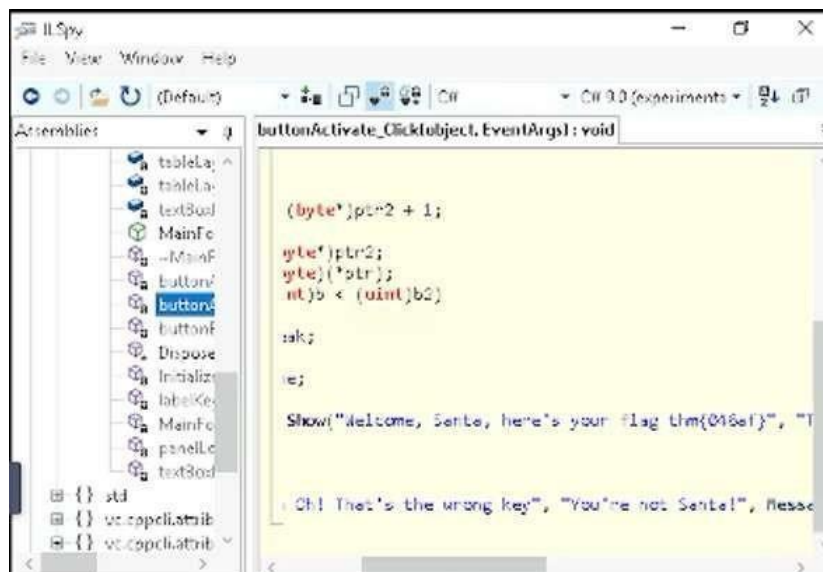
Expand TBFC_APP resources, next expand the “CrackMe” button and look for MainForm.



Question 4:

Find “*buttonActivate_Click (object,EventArgs)*” to look for santa password that is “*santapassword321*” and flag is obtained.





Thought Process/Methodology:

Install the Remmina. Open the Remmina, the password is required so that you can save the session and then press the "Cancel". Fill in the IP Address, username "cmnatic" and password "Adventofcyber!" given by TryHackMe. Next, change the colour depth to "RemoteFX (32 bpp)" and Save and Connect. It will bring us to a homepage, and used the ILSpy. Then open TBFC_APP to decompile the code. After that, expand TBFC_APP resources, and expand the CrackMe button and look for MainForm. The last step, search for buttonActivate_Click to look for santa password ---- "santapassword321" and the flag is obtained ---- "thm{046af}".

Day 19: Web Exploitation - The Naughty or Nice List

Tools used: Firefox

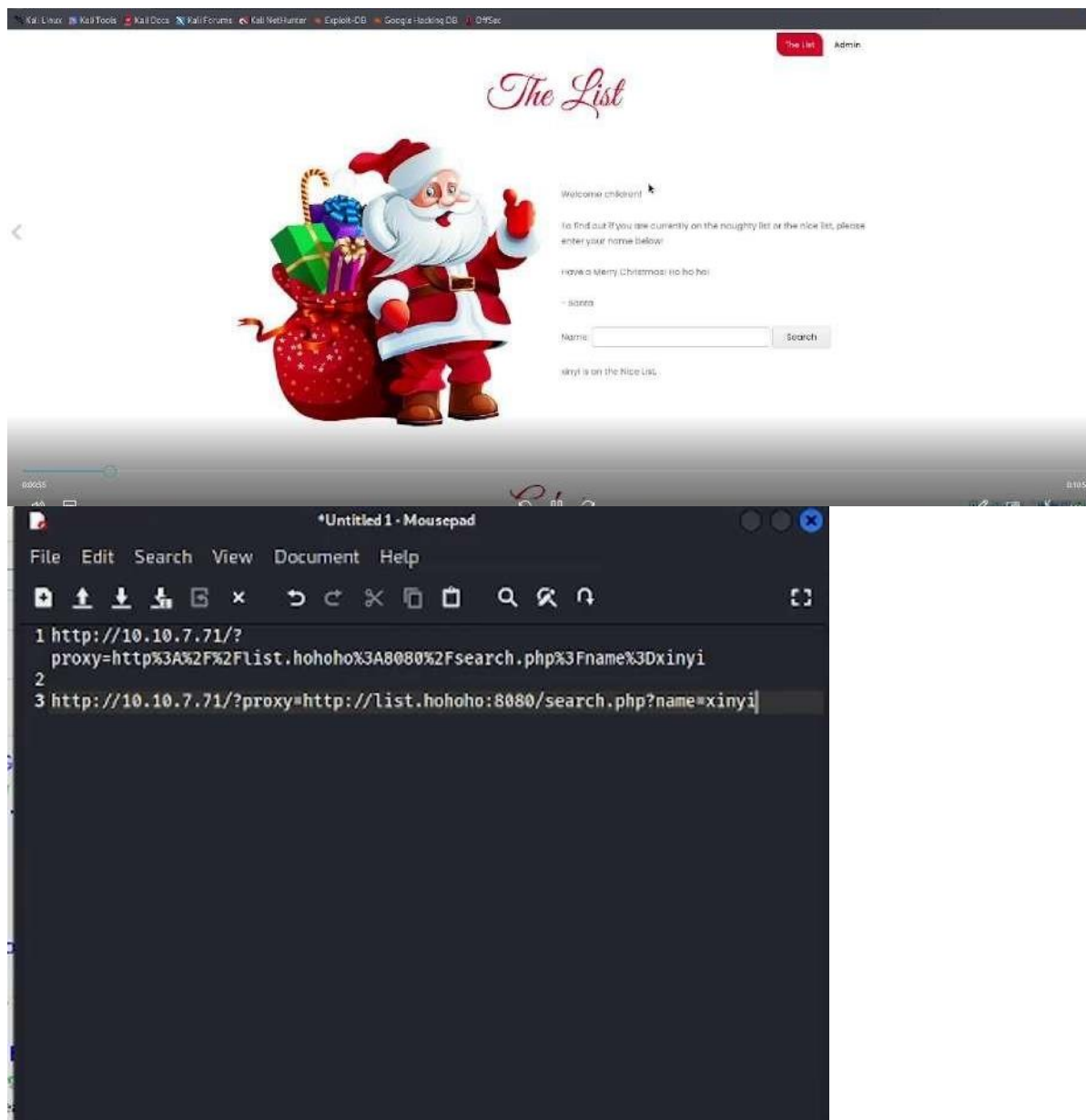
Solution/walkthrough:

Question 1:

Enter the IP machine address given by THM. Key in name in the blank and the url “http://10.10.7.71/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3Dxinyi” is shown.

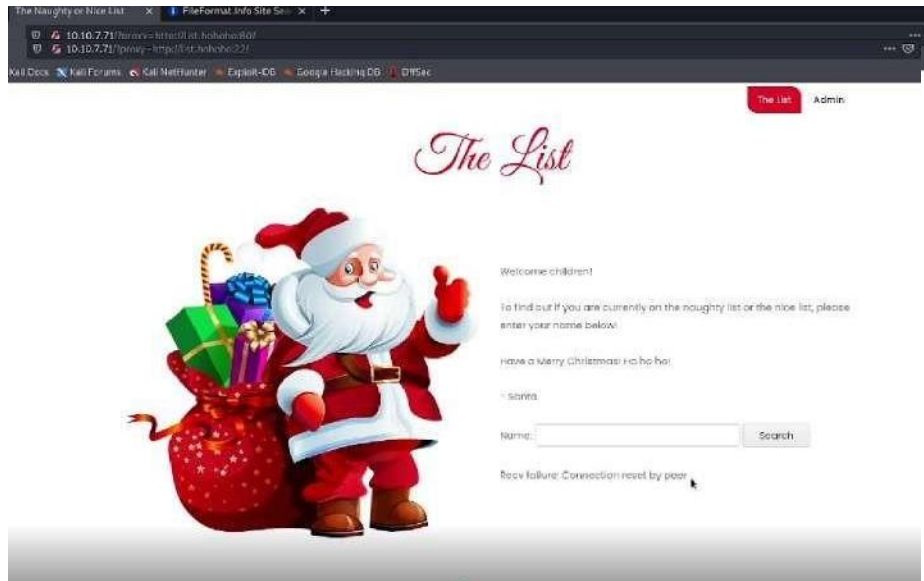
Look for the value of the parameter by using url decoder, then

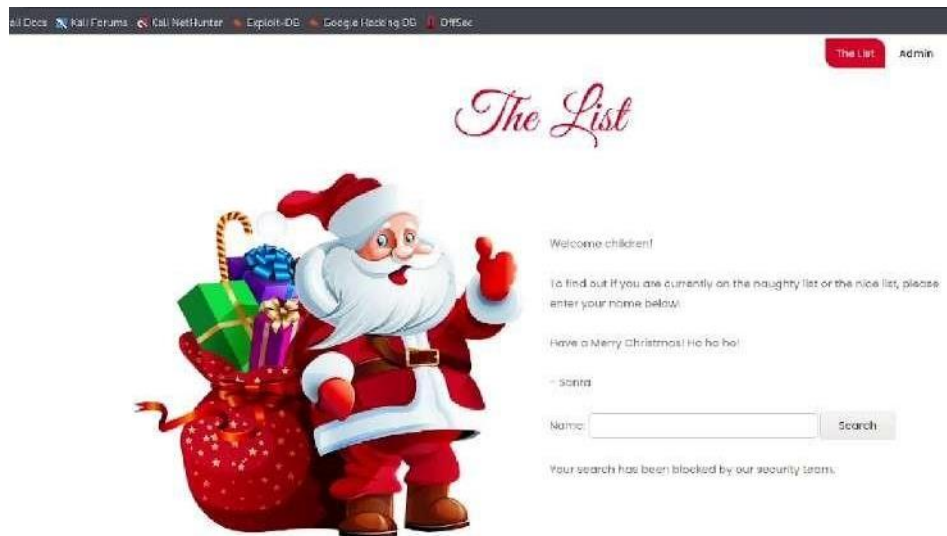
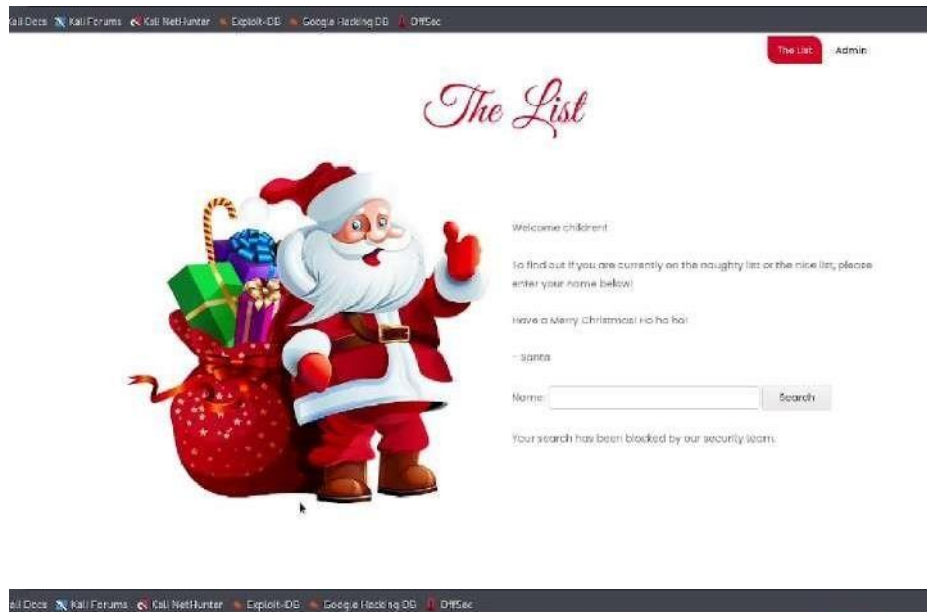
“http://10.10.7.71/?proxy=http://list.hohoho:8080/search.php?name=xinyi” is obtain



Question 2:

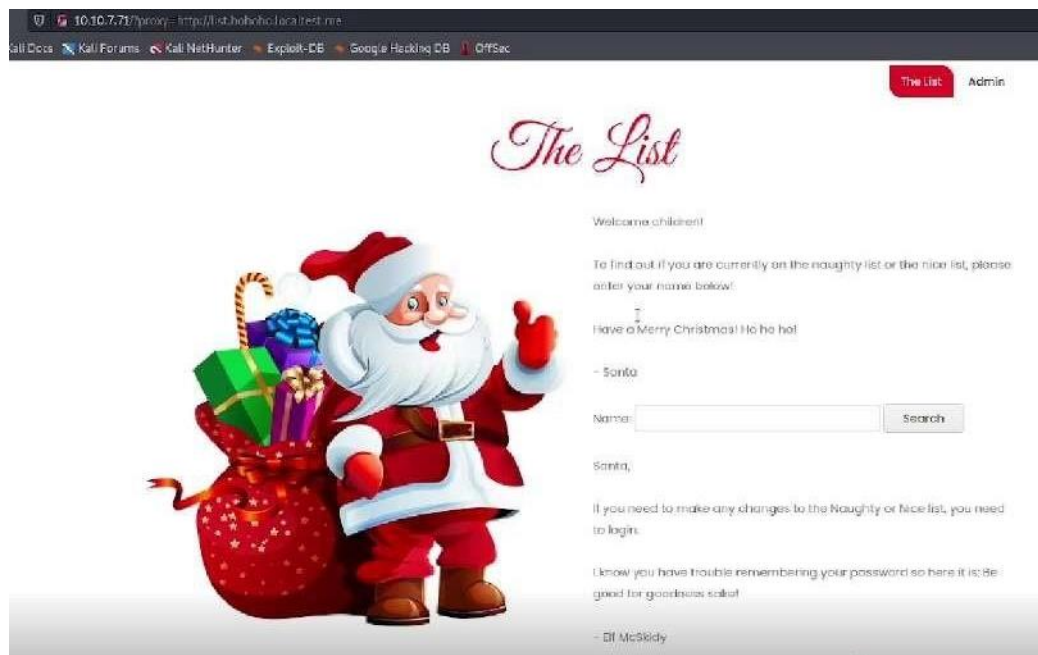
To fetch the root and find URLs of the "list.hohoho" site, try few port number and hostname For example: 8080 to 80, change port 8080 to 22, hostname to "localhost" and "127.0.0.1". But the URLs did not obtained





Question 3

Moreover, change the hostname in URL to "list.hohoho.localtest.me", and the correct URLs is obtained. We know that Santa's password ---- "Be good for goodness sake!"



Key in the username and password and it leads us to an admin form.



Question 4:

Delete the naughty list to look for the flag ----“THM{EVERYONE_GETS_PRESENTS}”

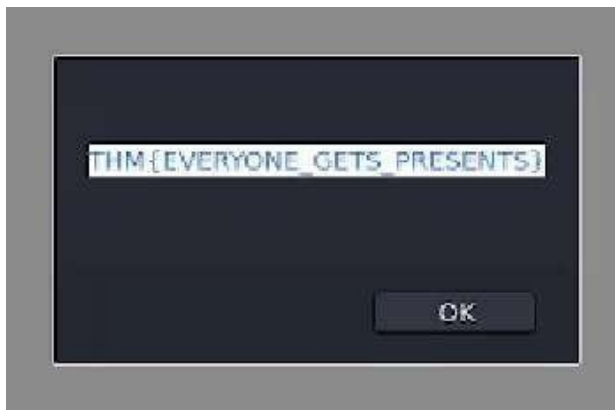


List Administration

This page is currently under construction.

Only press this button when emergency levels of Christmas cheer are needed!

DELETE NAUGHTY LIST



Thought Process/Methodology:

First step, enter the IP address given by TryHackMe. Enter a name and search. Next use URL decoder with the value of proxy parameter `http://10.10.7.71/?proxy=http://list.hohoho:8080/search.php?name=xinyi` is obtained. Next, try to fetch the root, and try few port number and hostname, for example: 8080 to 80, change port 8080 to 22, and hostname to "localhost" and "127.0.0.1". But the URLs did not obtained. Hence, change to "`http://10.10.7.71/?proxy=http://list.hohoho.localtest.me`", and correct URLs is obtained. We know that Santa's password is "Be good for goodness sake!" After that key in username and password and it leads us to admin form. Final step, *delete the naughty list* and the flag is obtained----- "THM{EVERYONE_GETS_PRESENTS}"

Day 20: Blue Teaming - Powershell to the rescue

Tools used: Terminal

Solution/walkthrough:

Question 1:

After connecting to machine IP, login to the Windows machine using SSH command:

ssh mceager@10.10.180.153 and the password is :r0ckStar!

```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)~  
$ ssh mceager@10.10.180.153  
The authenticity of host '10.10.180.153 (10.10.180.153)' can't be established.  
ED25519 key fingerprint is SHA256:X2Vi8kLLQoHmAsXFoem36jkL9faKH+Fr2lt2dd/kIWY.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.10.180.153' (ED25519) to the list of known hosts.  
mceager@10.10.180.153's password: █
```

Enter *powershell*

```
c:\windows\system32\cmd.exe - powershell  
File Actions Edit View 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> █
```

Change file location to *Documents*

```
c:\windows\system32\cmd.exe - powershell
File Actions Edit View Help
PS C:\Users\mceager> Set-Location -Path C:\Users\mceager\Documents
PS C:\Users\mceager\Documents>
```

Find the hidden file by key in the command:

Get-ChildItem -File -Hidden

```
c:\windows\system32\cmd.exe - powershell
File Actions Edit View Help
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 elfone.txt

PS C:\Users\mceager\Documents> ls

Directory: C:\Users\mceager\Documents

Mode                LastWriteTime         Length Name
----                -
-a-----       11/23/2020  12:06 PM          22 elfone.txt

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

View the hidden file by key in this command:

Get-Content -Path elfone.txt

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

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 elfone.txt

PS C:\Users\mceager\Documents> ls

Directory: C:\Users\mceager\Documents

Mode                LastWriteTime         Length Name
----                -
-a-----            11/23/2020   12:06 PM          22 elfone.txt

PS C:\Users\mceager\Documents> Get-Content -Path elfone.txt
Nothing to see here ...
PS C:\Users\mceager\Documents> Get-Content -Path elfone.txt
All I want is my '2 front teeth'!!!
PS C:\Users\mceager\Documents> 
```

Question 2:

Relocate the file to *Desktop* and look for the hidden directory by key in the command:

Get-ChildItem -Directory -Hidden

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

PS C:\users\mceager\documents> Set-Location -Path C:\Users\mceager\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> 
```


Relocate the file to the hidden directory and place the files inside by key in *Get-ChildItem* command

```
c:\windows\system32\cmd.exe - powershell
File Actions Edit View Help
PS C:\users\mceager\Desktop> ls -Hidden -Directory

Directory: C:\users\mceager\Desktop

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

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> 
```

View the file.txt using *Get-Content*

```
c:\windows\system32\cmd.exe - powershell
File Actions Edit View Help
PS C:\users\mceager\Desktop> ls -Hidden -Directory

Directory: C:\users\mceager\Desktop

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

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> Get-Content e70smsW10Y4k.txt
I want the movie Scrooged <3!
PS C:\users\mceager\Desktop\elf2wo> 
```

Question 3:

Relocate the file to *C:\Windows\system32* and filter the hidden directory with number 3 by key in this command:

*Get-ChildItem -Hidden -Directory -Filter "*3*"*

```
c:\windows\system32\cmd.exe - powershell
File  Actions  Edit  View  Help
PS C:\Windows> cd .\system32\
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>
```

Relocate file location to the hidden directory and place the files in it.

```
c:\windows\system32\cmd.exe - powershell
File  Actions  Edit  View  Help
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> cd .
PS C:\Windows\system32> cd .\3lfthr3e
PS C:\Windows\system32\3lfthr3e> ls
PS C:\Windows\system32\3lfthr3e> ls -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

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

Question 4:

Get the amount of words by key in command:

Get-Content 1.txt | Measure-Object



```
c:\windows\system32\cmd.exe - powershell
File Actions Edit View Help
PS C:\Windows\system32\3lfthr3e> Get-Content 1.txt | Measure-Object

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

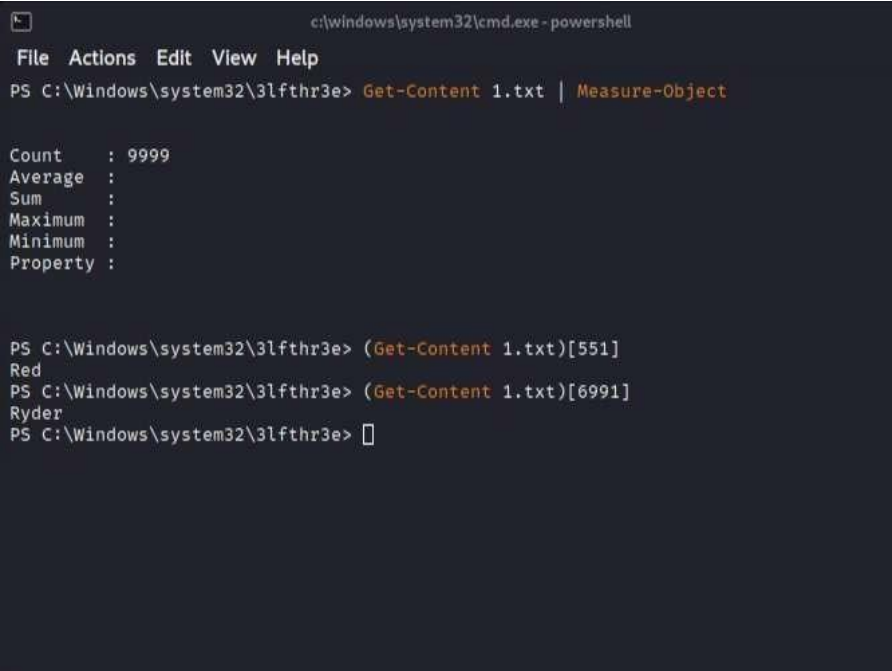
PS C:\Windows\system32\3lfthr3e> 
```

Question 5:

Convert the 551 and 6991 by entering these commands:

(Get-Content 1.txt)[551]

(Get-Content 1.txt)[6991]



```
c:\windows\system32\cmd.exe - powershell
File Actions Edit View Help
PS C:\Windows\system32\3lfthr3e> Get-Content 1.txt | Measure-Object

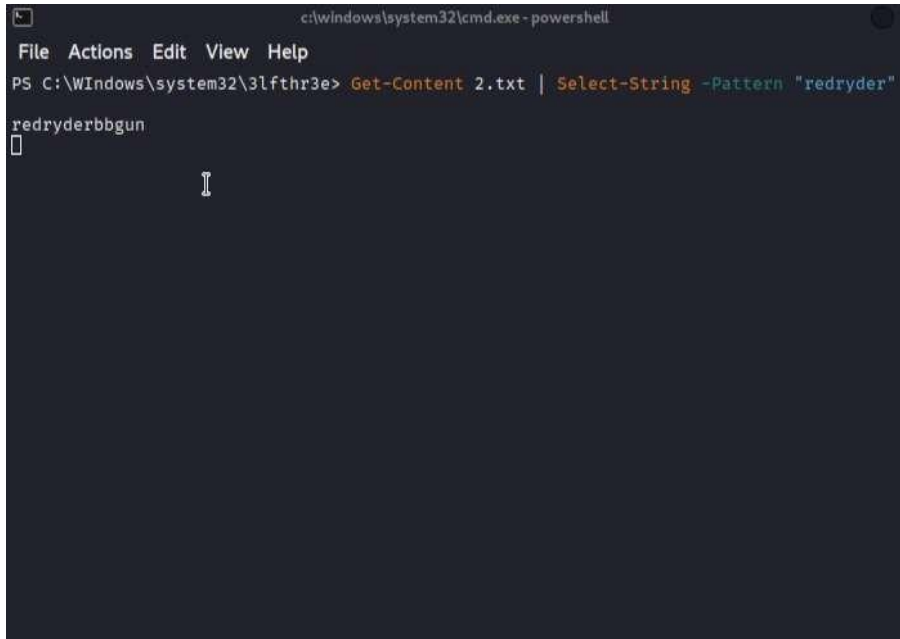
Count      : 9999
Average    :
Sum        :
Maximum    :
Minimum    :
Property   :

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

Question 6:

Find the 2.txt by key in command:

Get-Content 2.txt | Select-String -Pattern "redryder"



```
c:\windows\system32\cmd.exe - powershell
File Actions Edit View Help
PS C:\Windows\system32\3lfthr3e> Get-Content 2.txt | Select-String -Pattern "redryder"
redryderbbgun
```

Thought Process/Methodology:

After connecting ,login to the Windows machine by using *ssh mceager@10.10.180.153* and the password: *r0ckStar!*, then key in *powershell*. Firstly, change the file location to Documents by key in *Set-Location -Path C:\Users\mceager\Documents* . In Documents, look for the hidden file by key in command *Get-ChildItem -Hidden -File* and *e1fone.txt* is shown and if we use the listing command *ls*, the output will be *elfone.txt* which is different. After hidden file is found, view the file by key in the command *Get-Content e1fone.txt* and '2 front teeth' is shown. Secondly, relocate the file location to Desktop by key in command *Get-ChildItem -Hidden -Directory*. Next relocate the file to *elf2wo*, *e70smsW10Y4k.txt* is found by key in command *Get-ChildItem* and then open the .txt file by key in *Get-Content e70smsW10Y4k.txt* and 'Scrooged' is shown. Thirdly, relocate file location to *C:\Windows\system32* and filter the hidden directory with number 3 by key in command *Get-ChildItem -Hidden -Directory -Filter "*3*"*. Then, *3lfthr3e* directory is shown. Fourthly, open the *3lfthr3e* directory to look for the *1.txt* inside it and search for the count by key in command *Get-Content 1.txt | Measure-Object* which the outcome ----9999. Next, convert the 551 and 6991 in 1.txt by key in commands *(Get-Content 1.txt)[551]* and *(Get-Content 1.txt)[6991]*. Then, merge the 2 outputs and 'Red Ryder' is obtained. Lastly, search in 2.txt by key in command *Get-Content 2.txt | Select-String -Pattern "redryder"* and *redryderbbgun* is shown.