

PSP0201

Week 5

Writeup

Group Name: Amway

Members:

ID	Name	Role
1211100903	TAN XIN YI	Leader
1211101998	WESLEY WONG MIN GUAN	Member
1211101843	YAP HAN WAI	Member
1211101186	TAM LI XUAN	Member

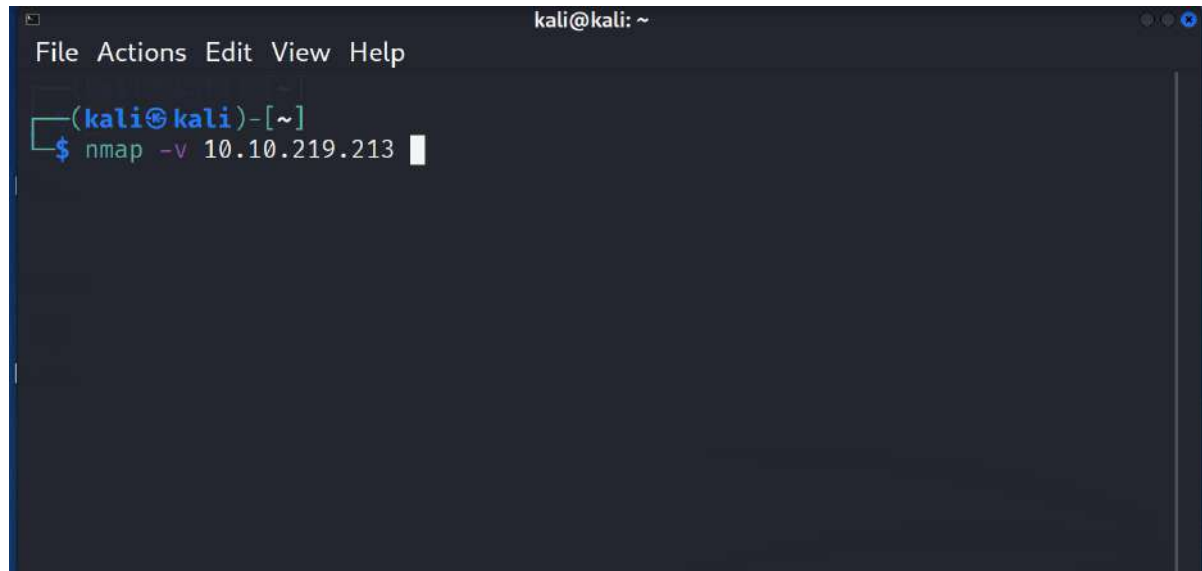
Day 16: Scripting - Help! Where is Santa?

Tools used: Firefox, Python

Solution/walkthrough:

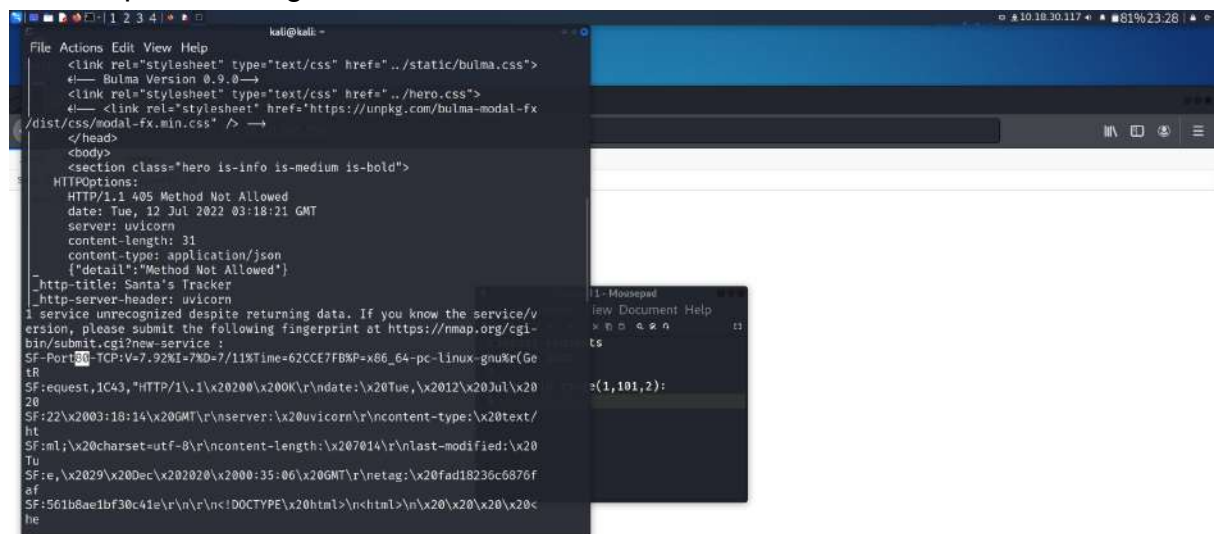
Question 1

After start the machine, type `nmap -v` and the IP address



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -v 10.10.219.213
```

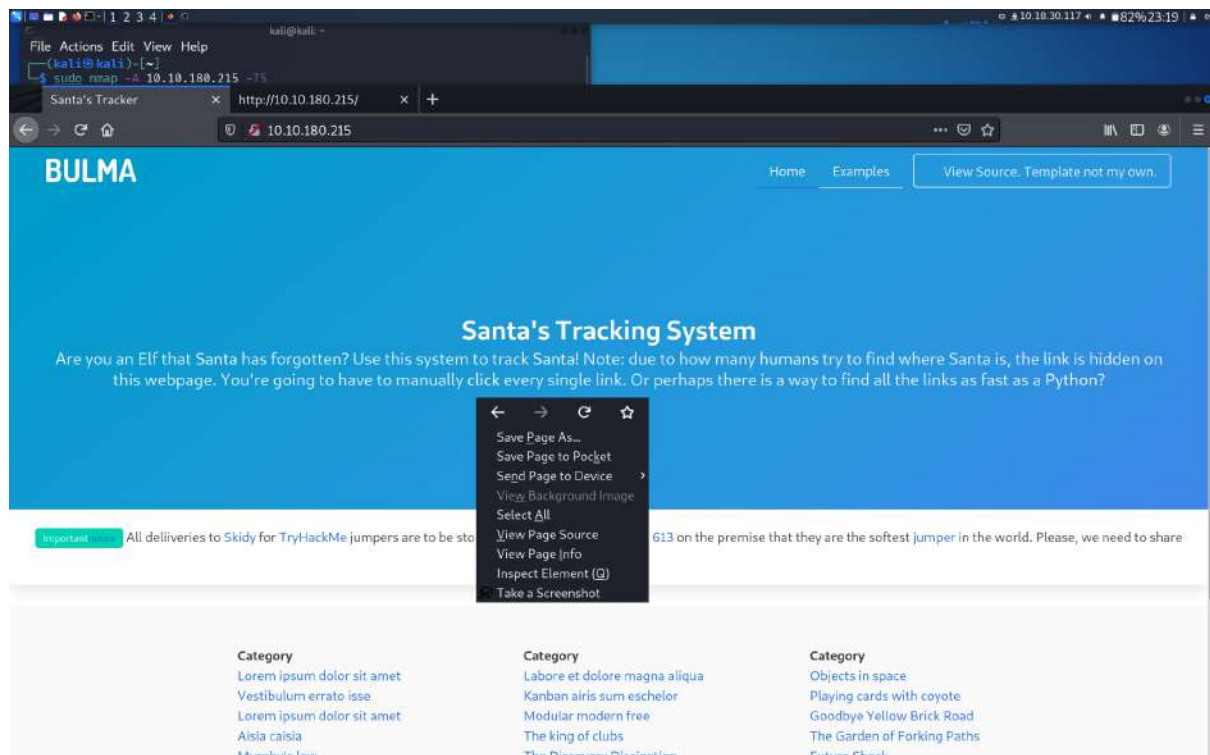
And the port will be given



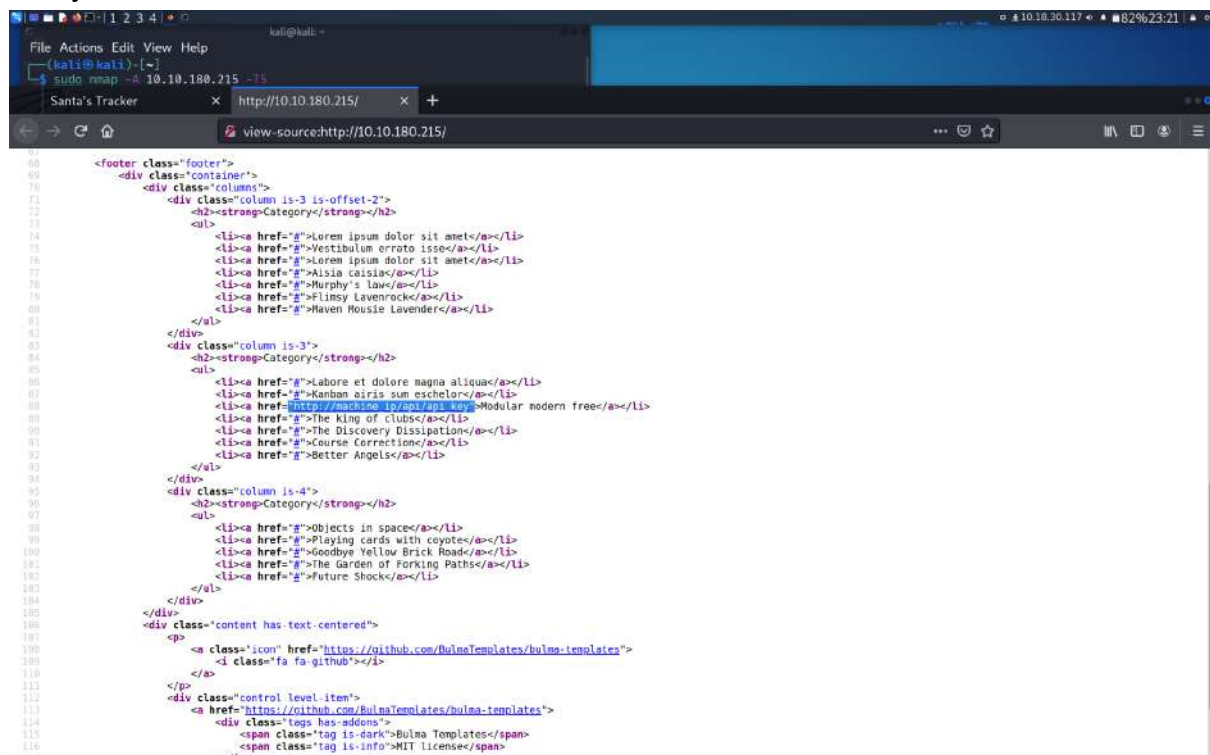
```
kali@kali: ~  
File Actions Edit View Help  
<link rel="stylesheet" type="text/css" href=".. /static/bulma.css">  
e|— Bulma Version 0.9.0—>  
<link rel="stylesheet" type="text/css" href=".. /hero.css">  
e|— <link rel="stylesheet" href="https://unpkg.com/bulma-modal-fx  
/dist/css/modal-fx.min.css" /> —>  
</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  
I 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 80-TCP:V=7.92XI=7ND=7/11%Time=62CCE7FB&P=x06_64-pc-linux-gnu&r(Ge  
tr  
SF:request,1C43,"HTTP/1.1\\x20200\\x200K\\r\\ndate:\\x20Tue,\\x2012\\x20Jul\\x20  
20  
SF:22\\x2003:18:14\\x20GMT\\r\\nserver:\\x20uvicorn\\r\\ncontent-type:\\x20text/  
ht  
SF:m1;\\x20charset=utf-8\\r\\ncontent-length:\\x207014\\r\\nlast-modified:\\x20  
Tu  
SF:e,\\x2029\\x20Dec\\x202020\\x2000:35:00\\x20GMT\\r\\netag:\\x20fad18236c6876f  
ef  
SF:561b8ae1bf30c41e\\r\\n\\r\\n<!DOCTYPE\\x20html>\\n<html>\\n\\x20\\x20\\x20<  
he
```

Question 2

In the firefox, enter the IP address and right click to view page resource



And you will see the API



Question 3

After that, create a new python with nano brute.py. Then, 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

Thus, use python3 and brute.py and show the result

```
kali@kali: ~  
File Actions Edit View Help  
[root@kali ~]# nano brute.py  
[root@kali ~]# python3 brute.py
```

Category: Learn python data all smet
Vestibulum arcuata

Category: Learn python
Vestibulum arcuata

Thus, we can know where is santa now

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

Question 4:

Finally, the correct API key will also be shown and it is an odd number as well.

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

Thought Process/Methodology:

This is a python scripting task so that we need to script a little bit to do it. Firstly, type nmap -v and the IP address after starting the machine. Then, find out the port, it will be given somewhere. Also, enter the IP address in the firefox and right click to view page resources as well. Later, we can type the IP address and :8000 to look for it. Also, we can try /api/... and api key to try it behind the port. After that, create a new python with nano brute.py. Then, import requests. There are multiple ways to use the command by the way. And then, I have created a new python which is brute.py. After finishing the command, use python3 and brute.py. After that, save it and modify it. Furthermore, type python3 and brute.py behind the python3. it will show you the result. Hence, we can know where Santa is now, which is winter wonderland, hyde park, london. With the command I type, I can directly know the API key as well, which is 57.

Day 17: Reverse Engineering - ReverseELFneering

Tools used: Command Prompt, elfmceager

Solution/walkthrough:

Question 1

First, login as *elfmceager@IPaddress* and key in the password given by THM which is *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 the file is analysed, open the file “challenge 1” and enter the main file and get the value of local_ch is 1.

```
= attach 1795 1795
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
```

Find the value of eax which is resulted as 6 and the value of local_4h which is also 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:

First, login as *elfmceager@IPaddress* and key in the password given by THM which is *adventofcyber*. Then we open the file “challenge 1” and get into the main page in the “main page” we can get the value of *local_ch* when its corresponding *movl* instruction is called is 1 and the value of *eax* when the *imul* instruction is called $1 \times 6 = 6$ and the value of *local_4h* before *eax* is set to 0 is 6 also.

Day 18: Reverse Engineering - The Bits of Christmas

Tools used: Remmina

Solution/walkthrough:

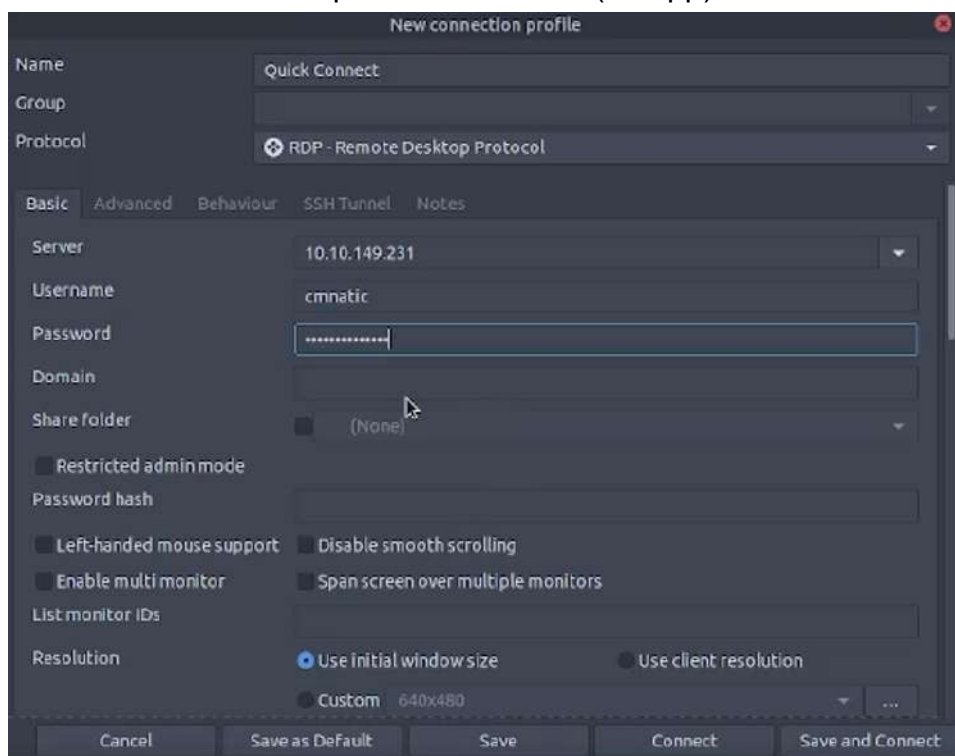
Question 1

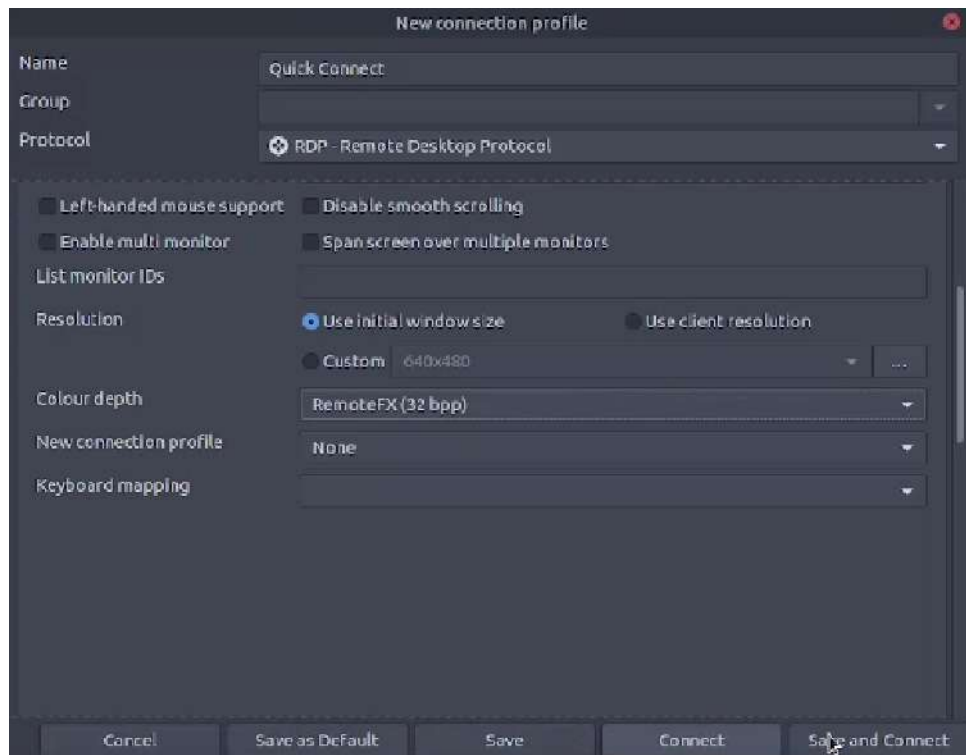
After installing Remmina, Remmina will ask for a password to save the session, we can press “Cancel”.



Question 2

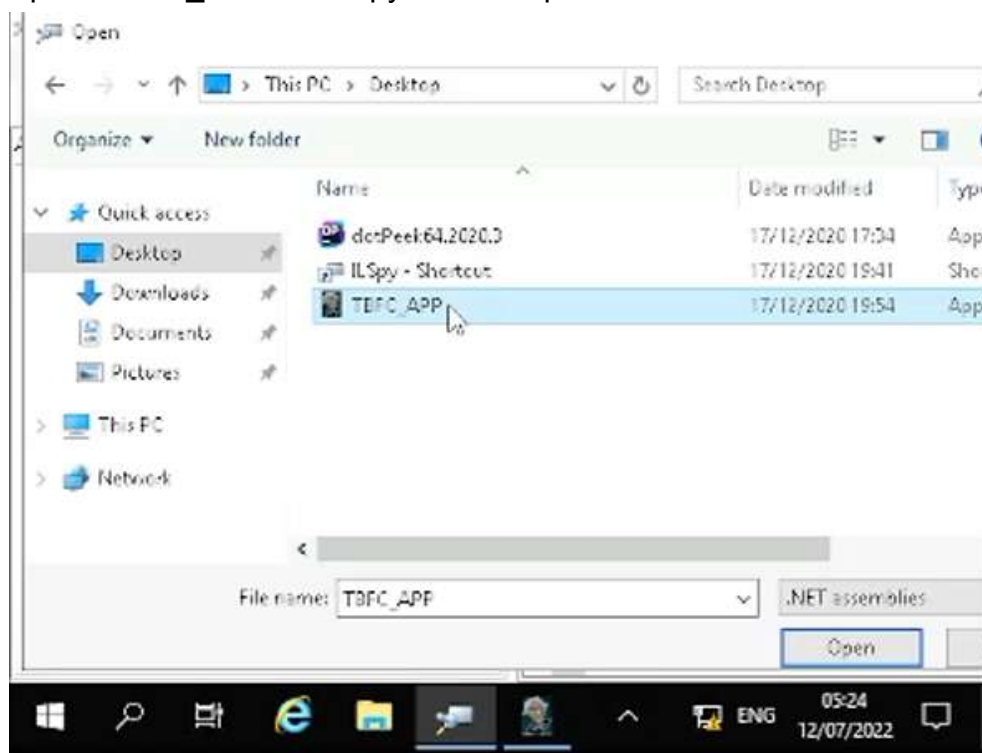
Fill in the IP Address, username “*cmnatic*” and password “*Adventofcyber!*” given by THM. Set the colour depth to “RemoteFX (32 bpp)” then “*save and connect*”.

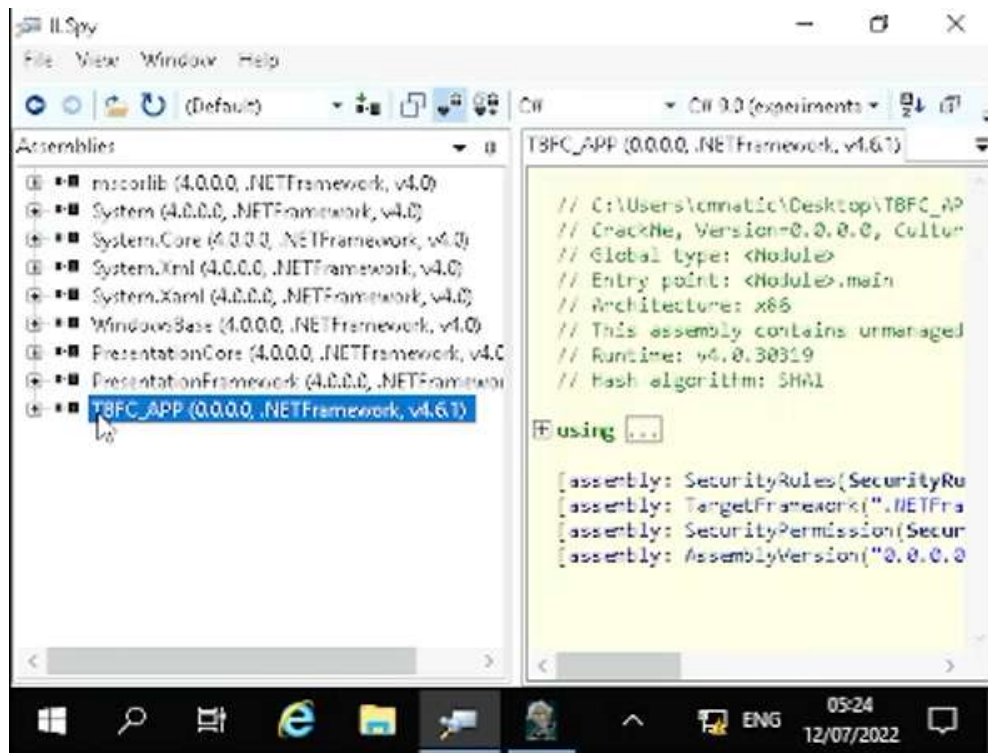




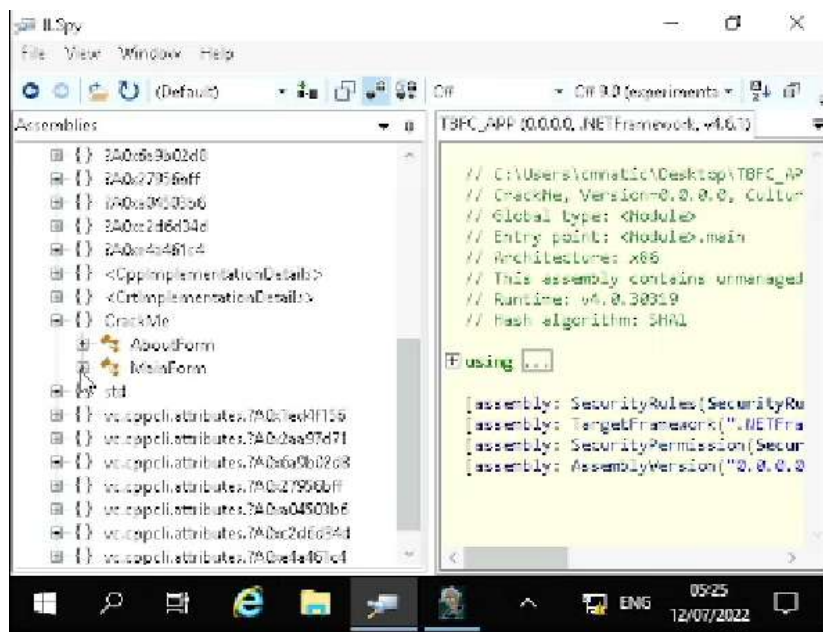
Question 3

Open "TBFC_APP" in ILSpy to decompile the code.



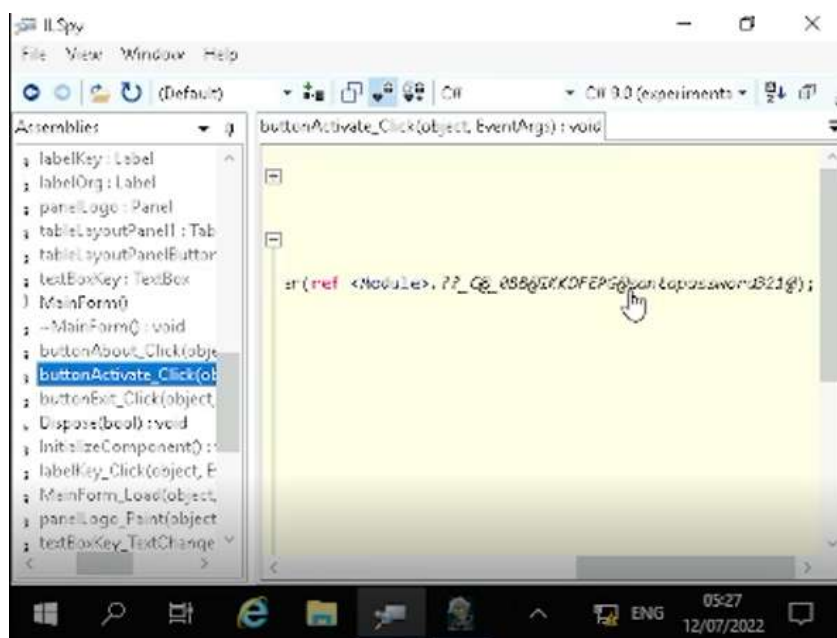
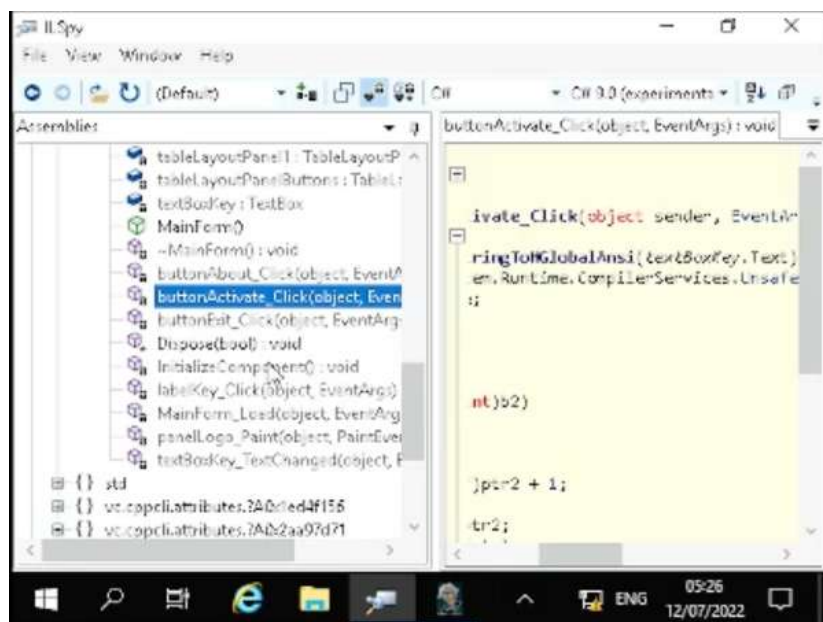


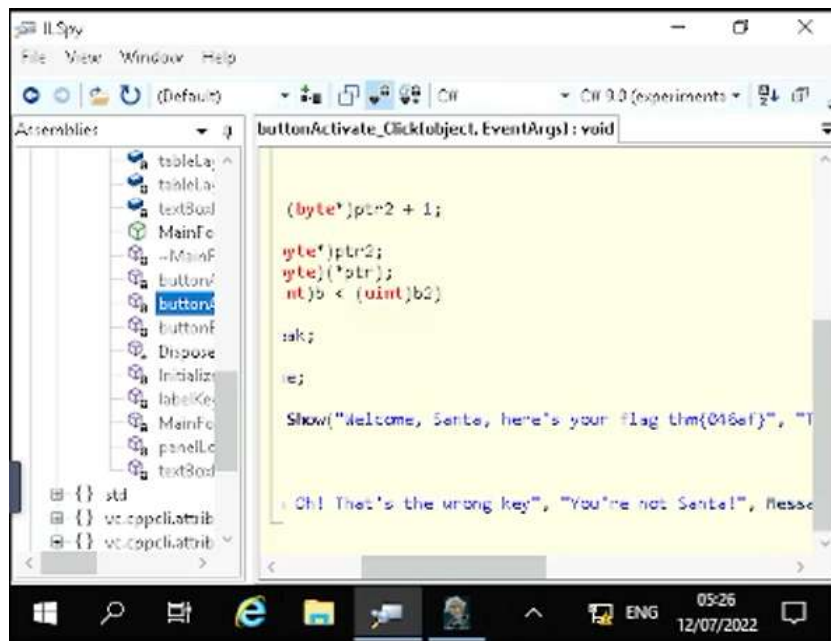
Expand TBFC_APP resources, then expand the “CrackMe” button and find MainForm.



Question 4

Look for “*buttonActivate_Click (object,EventArgs)*” to find santa password which is “*santapassword321*” and capture the flag.





Thought Process/Methodology:

In this task in order to capture the flag, we need to use Remmina. When we open Remmina, it will ask for a password to save the session but it is safe to "Cancel" it. Afterwards, Remmina will lead us to a *New Connection Profile*, we need to fill in the IP Address, username "cmnatic" and password "Adventofcyber!" given by TryHackMe. Then, set the colour depth to "RemoteFX (32 bpp)" and only can Save and Connect. It will lead us to a homepage, and we used the ILSpy App instead of dotPeek64. Then we open TBFC_APP from File in ILSpy to decompile the code. We expand TBFC_APP resources, then expand the CrackMe button and find MainForm. Lastly we look for buttonActivate_Click (object,EventArgs) in order to find santa password which is "santapassword321" and capture the flag "thm{046af}".

Day 19: Web Exploitation - The Naughty or Nice List

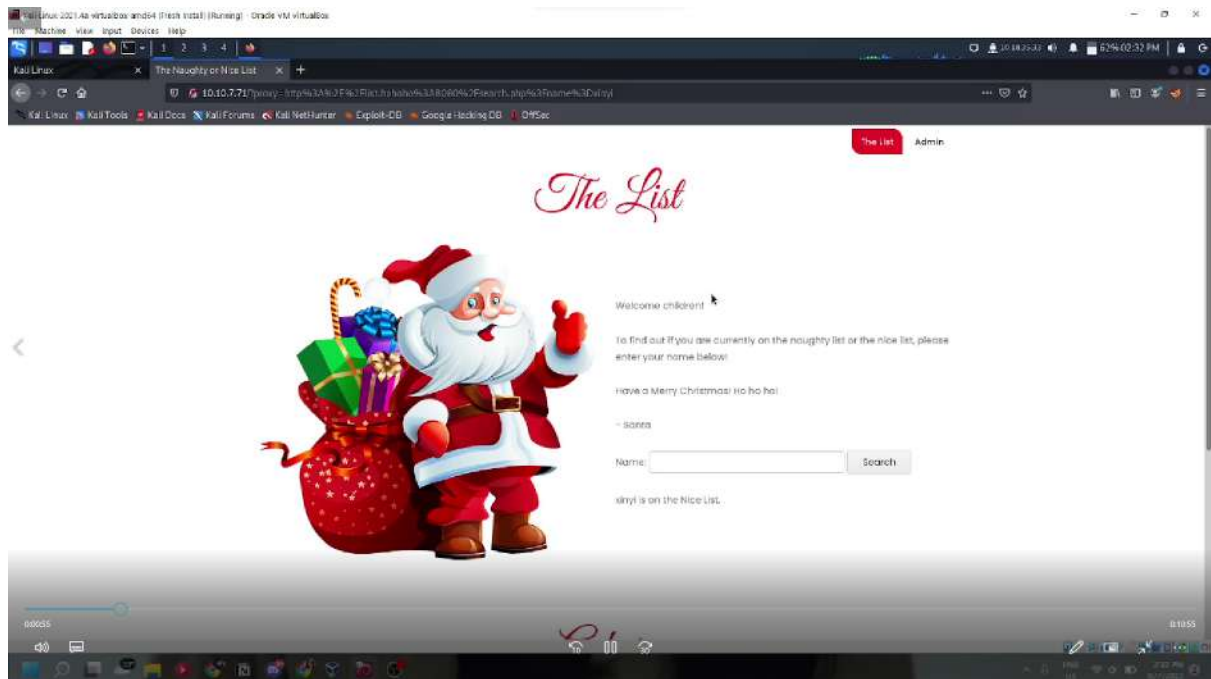
Tools used: Firefox

Solution/walkthrough:

Question 1

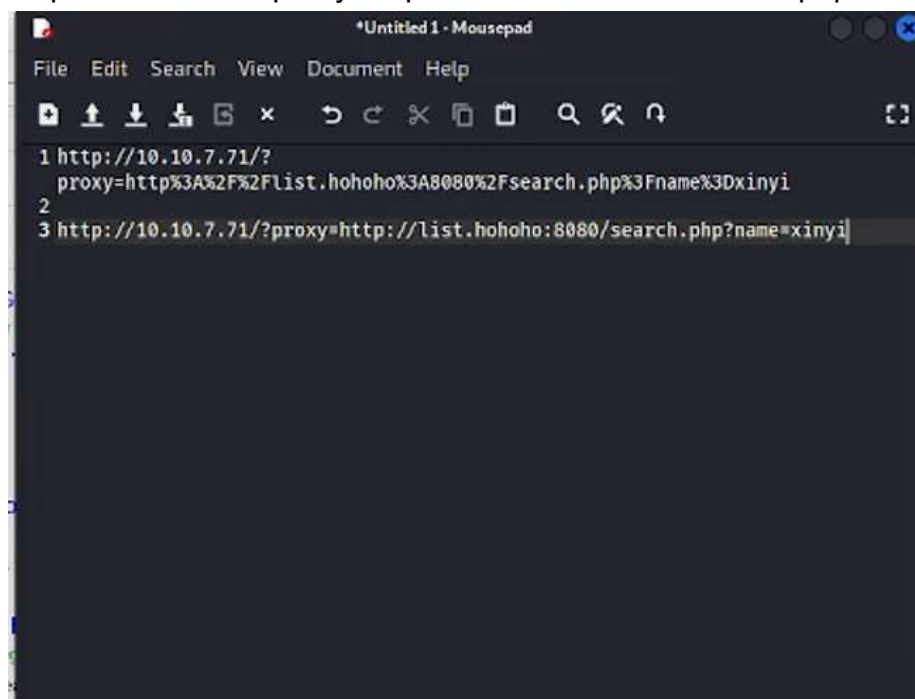
Connect to the web app by using the IP machine address given by THM. Enter a name in the form and the url will become

“http://10.10.7.71/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3Dxinyi”



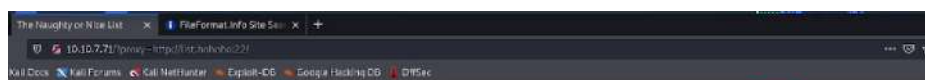
We use the url decoder to find the value of the parameter, we get

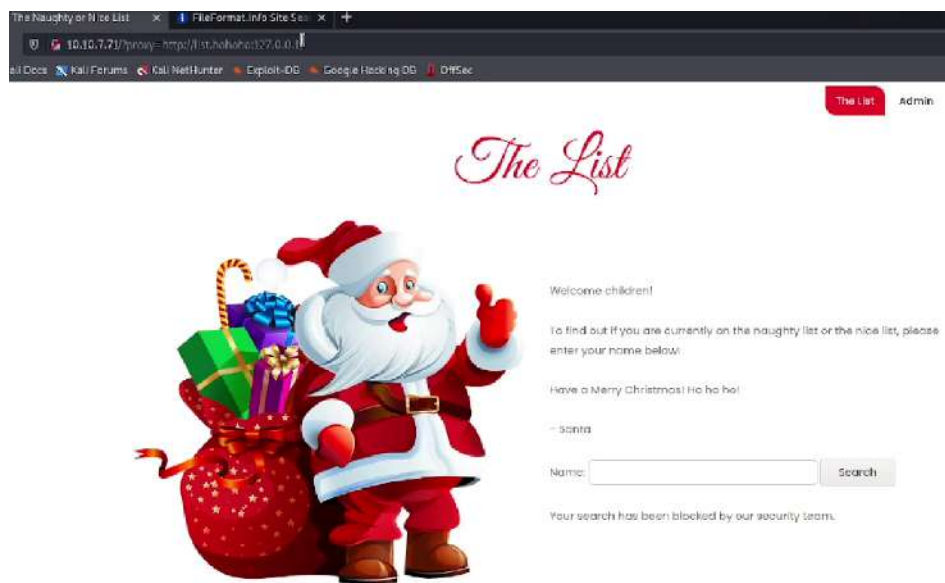
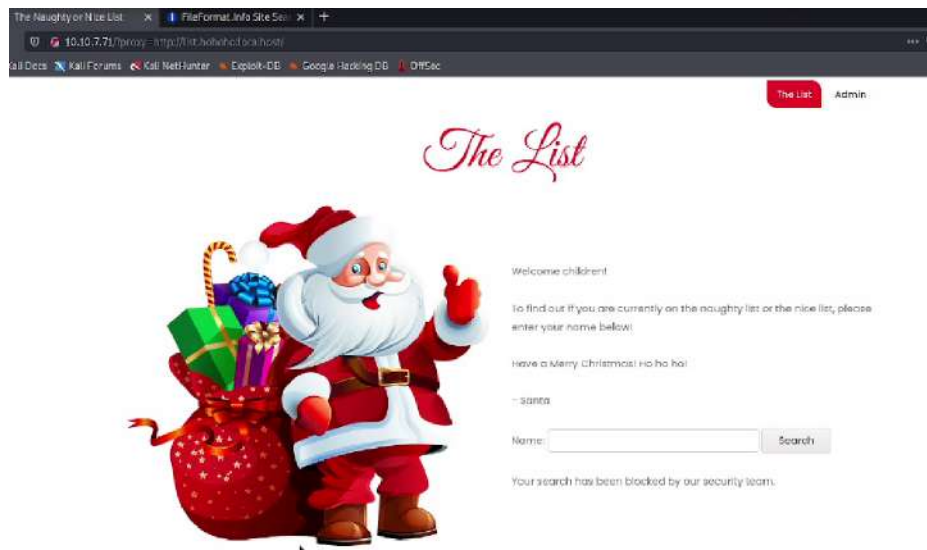
“http://10.10.7.71/?proxy=http://list.hohoho:8080/search.php?name=xinyi”



Question 2

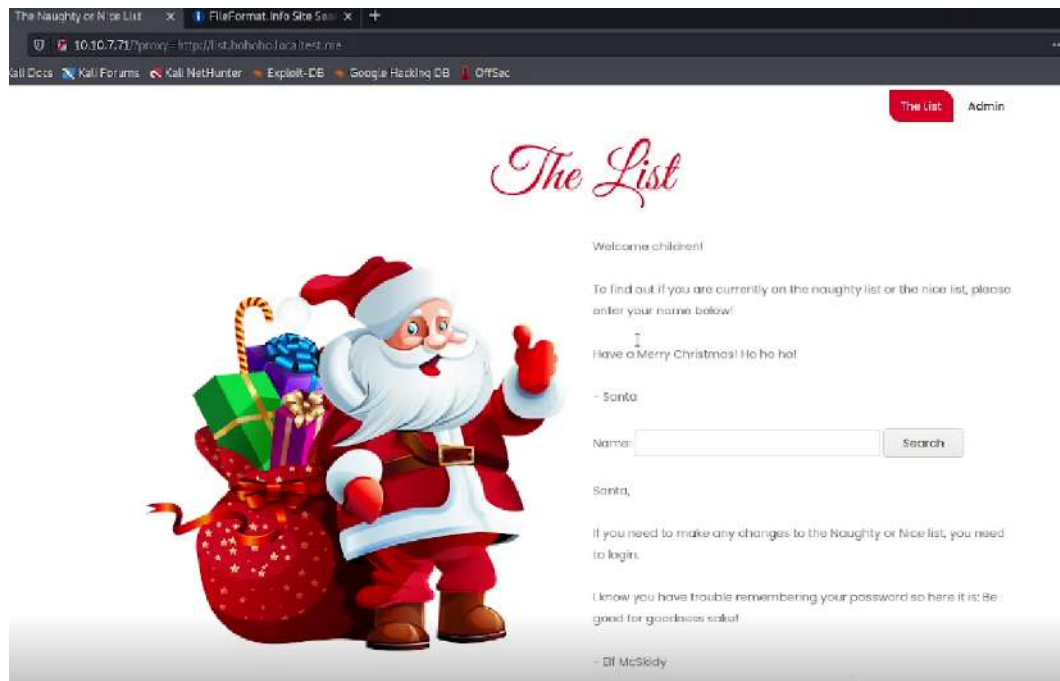
To fetch the root and try to find valid URLs for the "list.hohoho" site, we tried different port number and hostname such as changing port 8080 to 80, changing 8080 to 22 (which is the default SSH port), changing hostname from "list.hohoho" to "localhost" and "127.0.0.1". Yet it still can't be accessed.





Question 3

Therefore, we set the hostname in the URL to "list.hohoho.localtest.me", and it succeeded. We found Santa's password which is "Be good for goodness sake!"

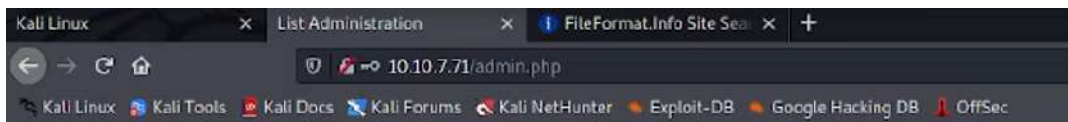


Then we input the username and password we found into the admin form.



Question 4

Delete the naughty list to find the challenge flag which is
“THM{EVERYONE_GETS_PRESENTS}”

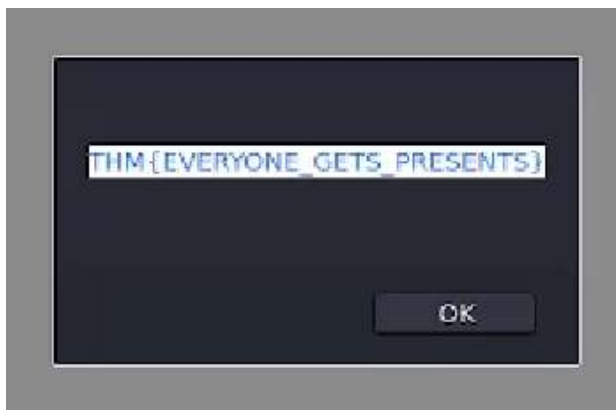


List Administration

This page is currently under construction.

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

DELETE NAUGHTY LIST



Thought Process/Methodology:

To capture the flag, we only require Firefox. Firstly, we connect to the web app by using the IP machine address given by TryHackMe. Fill up the form with a name and press the "Search" button. When the website is loaded, it informs us that the name is on the Nice List. Then we use a URL decoder on the value of the proxy parameter and we get `http://10.10.7.71/?proxy=http://list.hohoho:8080/search.php?name=xinyi`. Since "list.hohoho" is not a valid hostname on the Internet, we need to try to fetch the root, and we tried different port number and hostname such as changing port 8080 to 80, changing 8080 to 22 (which is the default SSH port), changing hostname from "list.hohoho" to "localhost" and "127.0.0.1". Yet it still can't be accessed. But we found out the hostname can easily be bypassed. The one we will be using is "localtest.me", which resolves every subdomain to 127.0.0.1. Therefore, we set the URL to "`http://10.10.7.71/?proxy=http://list.hohoho.localtest.me`", and it succeeded. It appears a message from Elf McSkidy which contains Santa's password which is "Be good for goodness sake!" Then we entered the username and password we found into the admin form. Lastly, we *delete the naughty list* to find the challenge flag which is "THM{EVERYONE_GETS_PRESENTS}"

Day 20: Blue Teaming - Powershell to the rescue

Tools used: Terminal

Solution/walkthrough:

Question 1

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

ssh mceager@10.10.180.153

pass: *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:X2ViBkLLQoHmAsXFoem36jkL9faKH+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>
```

Search for the hidden file using the following 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 using the following 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

Change the file location to *Desktop* and search for the hidden directory using the following 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> 
```


Change the file location to the hidden directory and list the files inside it using *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

Change the file location to `C:\Windows\system32\` and filter the hidden directory with number 3 by using the 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>
```

Change the file location to the hidden directory and list the files inside 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

Measure the amount of words by using the following 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 using the following 2 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

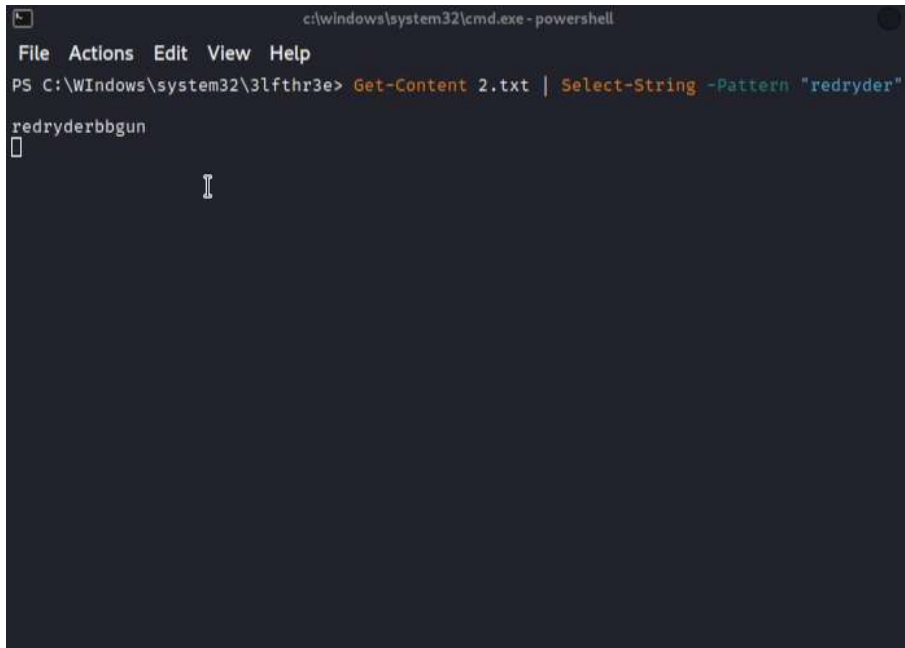
Count      : 9999
Average    :
Sum        :
Maximum    :
Minimum    :
Property   :

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

Search the 2.txt by using the following 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 and login to the Windows remote machine by using *ssh mceager@10.10.180.153* with the password(*r0ckStar!*), we are required to activate powershell mode by entering *powershell*. For the first question, we change the file location to Documents by using *Set-Location -Path C:\Users\mceager\Documents* or *cd Documents*. In *Documents*, search for the hidden file by the command *Get-ChildItem -Hidden -File* which the output is *e1fone.txt* and if we use the listing command *ls*, the output will be *elfone.txt* which is different. After we find the hidden file, we need to view the file using the command *Get-Content e1fone.txt* which the output is '*2 front teeth*'. For the second question, we must change the file location to *Desktop* first before we search the hidden directory which is *elf2wo* using the command *Get-ChildItem -Hidden -Directory*. Now change the file location to *elf2wo*, we will find the *e70smsW10Y4k.txt* by the command *Get-ChildItem* and then open the *.txt* file by command *Get-Content e70smsW10Y4k.txt* which the output is '*Scrooged*'. For the third question, we need to change the file location to *C:\Windows\system32* and filter the hidden directory with number 3 by the command *Get-ChildItem -Hidden -Directory -Filter "*3*"*. After that, we will see the directory named *3lfthr3e*. For the fourth question, we need to open the *3lfthr3e* directory to find the *1.txt* inside it and find the count by the command *Get-Content 1.txt | Measure-Object* which the outcome is 9999. For the fifth question, we need to convert the 551 and 6991 inside *1.txt* by the commands *(Get-Content 1.txt)[551]* and *(Get-Content 1.txt)[6991]*. Then, we combine the 2 outputs which result in '*Red Ryder*'. For the sixth question, we search inside *2.txt* by the command *Get-Content 2.txt | Select-String -Pattern "redryder"* and the output is *redryderbbgun*.