CTF Report

Full Name: Syed Junaid Ahmad Andrabi

Program: HCS - Penetration Testing 1-Month Internship

Date : 14/08/2024

Introduction

This report document hereby describes the proceedings and results of a Black Box security assessment conducted against the **Week {4} Labs**. The report hereby lists the Flags that were found in challenge section labs.

Wh@t7he####(Cryptography)

1

⇨ Passing the cipher into a cipher identifier on decod.fr I gave me an alternate language.

Cipher

```
----------]<-<---<-------<---------->>>>+[<<<<--,------,+++++++++++,------,-------------------,>------------,>-
-------------------,<<+++++,+++++++++++++++++,------------,-,>>,<<+++++++++++++++,,,+++++,>>----
,+++++++,<<,-----
---,>>---,<<-------------,>-------------,<+++++++,>>,<<----------------,
```

FLAG: flag{R3vers3ddd_70_g3t_m3}

L0Ck_Web(web)

2

⇨ To solve this I used burp-suite intruder to brute for the 4 digit pin on the url at https://hacktifylockweb.chals.io/check-pin?pin=

FLAG: flag {V13w_r0b0t5.txt_c4n_b3_u53ful!!!}

Hidden Pathways(web)

3

- ⇨ Looking at the source code I saw a hidden directory on visit it I noticed I can few it just normal GET method so I used the POST request which gave another page, which when viewing the source code I saw ../hidden/superhidden so in the full url to the flag https://hacktifyhiddenpathway.chals.io/hidden/superhidden

FLAG: flag{w3ll_d0n3_tr4v3ll3r!}

Wifi (Network Forensics)

4

- ⇨ We were given an capture wifi handshake. So I used airmo-ng (wifi cracker) to get the password.

Command used:

```
"aircrack-ng  wifi_capture-01.cap -w /usr/share/wordlists/rockyou.txt"
```

FLAG: flag{allmines}

Sneaker(Network Forensics)

5

- ⇨ Looking through the TCP packets I saw this string:

“666c61677b706c3479316e675f773174685f7034636b3374357d”

decoding the string from hex.

FLAG: flag{pl4y1ng_w1th_p4ck3t5}

The World(web)

6

⇨ Brute-forcing for directory with the ‘.txt’ extension, I saw the ‘secret.txt’ direct and visited it on the url https://hacktify-theworld.chals.io/secret.txt

FLAG: flag{Y0u_hav3_3xpl0reD_th3_W0rLd}

Corrupted (Network Forensics)

7

⇨ Trying to open the png file but it was not a valid png, so checking the hexadecimal values I noticed the header is not a png header so google png header hex and changed the image header with hex_editor and I was able to get the flag.

FLAG: flag{m3ss3d_h3ad3r$}