Arthur Liou
CS373
Final Exam

Final Exam Writeup

Prompt

In this class, we have covered a wide range of topics. From low level OS concepts up the stack to web and mobile security and exploitation.

For your final exam, I want you to do the following:

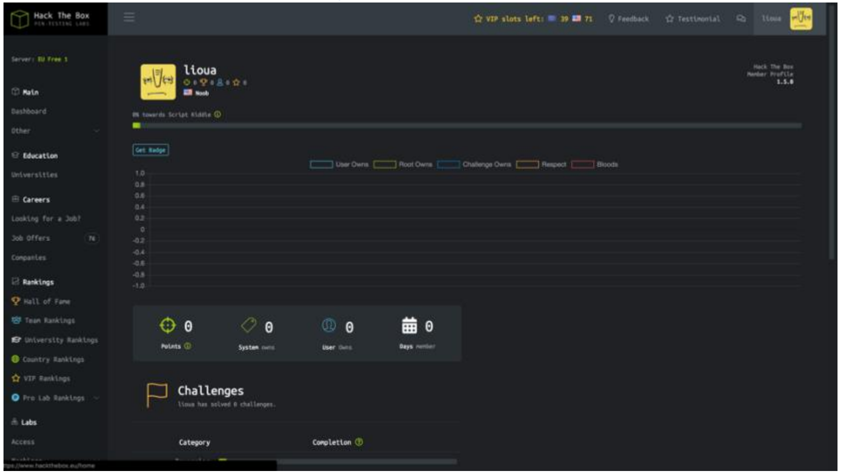
1. Obtain an account on Hack the Box. This requires generating your own invitation code. [5 points]
2. Complete a minimum of 3 challenges of your choice. These should sum to at least 50 points. Extra credit will be given for points over 75 in a 10:1 fashion -- every 10 points over 75 that you get, you get an extra point on your FINAL COURSE GRADE. [30 points -- 10/challenge completed]
3. Write up how you did the above. This include how you completed the challenge, your thought process that got you there, and a description of any tools you used and how you used them. [60 points -- 20/challege completed and 5 for how you obtained an invitation code]

As you can see above, the write-up is the majority of the points. As such, your priority should be on the write-up. The write-up, as usual, can be either a website or a tex document (or the PDF output thereof).

Response

I'm opting to submit the PDF output of the tex document for this writeup.

1) Account Username: lioua. https://www.hackthebox.eu/home/users/profile/117079



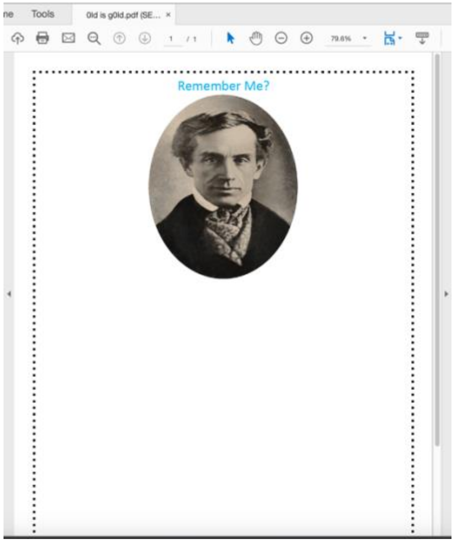
0% towards Script Kiddie

lioua has solved 0 challenges.

Profile once I first created

2) Challenges Completed
    a. Total Points: 60 points
3) I started off the final with generating my own invitation code. On my own I was able to get as far as inspecting elements in ChromeDevTools, makeInviteCode(), generating the

code, but as far as trying to decode the base64, I needed help so I utilized decoder tools, then hit a Post APi call, before decoding the resulting base64 return and finally getting the invitation code. From there, I reviewed the rules and access.

- a. Recalling I needed to complete 3 challenges for 50 total points. Since my preference for hacking challenges was Web, I navigated to the Web Challenges in the Nav. But after seeing mostly medium to hard difficulty changes, I moved onto a section with more easy challenges and took a look at the Misc Challenges.
- b. I took note of challenges that many liked / marked as easy and how many points each were.
- c. Challenge 1: 0ld is g0ld (10 points) and ~1.5k Liked with easy level.
    - i. In this challenge, I downloaded the zip file. Upon download and attempting to unzip, it prompted for a password, “hackthebox”. Unzipping the file extracted a protected PDF.
    - ii. On Mac, I knew of a few password crackers available via homebrew
    - iii. I installed pdfcrack via homebrew - `brew install pdf crack’
    - iv. Then downloaded a rockyou.txt that was a 133MB text file containing a list of “cracked” password. This rockyou.txt was taken from a google search.
    - v. Ran `pdfcrack -f "0ld is g0ld.pdf" -w rockyou.txt` to brute force the PW
    - vi. 

    - vii. I wasn’t sure who this individual was but my guess was that this individual who was from the 1700-1800s, and had something to do with hacking / codes.
    - viii. When I scrolled down, I saw tiny dots and lines, which I recognized as Morse code! So I used https://morsecode.scphillips.com/translator.html to decode this.
    - ix. Flag: HTB{R1PSAMU3LM0RS3}
- d. Challenge 2: fs0ciety (30 points) and ~1.6k liked with easy level
    - i. In this challenge, I downloaded the zip file. Upon download and attempting to unzip, it prompted for a password, “hackthebox”.

Unzipping the file revealed a password prompt for “sshcreds_datacenter.txt”

ii. Similarly to challenge one, I found a password cracker
   1. I installed fcrackzip via homebrew - `brew install fcrackzip’

iii. Using the same rockyou.txt from above to compare

iv. Ran `fcrackzip -u -D -p 'rockyou.txt' fsociety.zip`
   1. PW: justdoit

v. Resulting sshcreds_datacenter.txt contained encrypted SSh credentials

vi. I found base64 and saw the = flag at the end so I realized we needed to converted from base64 to binary. Tool: https://www.base64decode.org/
   1. MDExMDEwMDEgMDExMDAxMTAgMDEwMTExMTEgMDExMTEwMDEgMDAxMTAwMDAgMDExMTAxMDEgMDEwMTExMTEgMDExMDAwMTEgMDEwMDAwMDAgMDExMDExMTAgMDEwMTExMTEgMDAxMDAxMDAgMDExMDExMDEgMDAxMTAwMTEgMDExMDExMDAgMDExMDExMDAgMDEwMTExMTEgMDExMTAxMTEgMDExMDEwMDAgMDEwMDAwMDAgMDExMTAxMDAgMDEwMTExMTEgMDExMTAwMTAgMDAxMTAwMDAgMDExMDAwMTEgMDExMDEwMTEgMDEwMTExMTEgMDExMDEwMDEgMDExMTAwMTEgMDEwMTExMTEgMDExMDAwMTEgMDAxMTAwMDAgMDAxMTAwMDAgMDExMDEwMTEgMDExMDEwMDEgMDExMDExMTAgMDExMDAxMTE=

vii. The result was binary, so I used another tool to convert that to text. https://www.rapidtables.com/convert/number/binary-to-ascii.html
   1. 01101001 01100110 01011111 01111001 00110000 01110101 01011111 01100011 01000000 01101110 01011111 00100100 01101101 00110011 01101100 01101100 01011111 01110111 01101000 01000000 01110100 01011111 01110100 01101000 00110011 01011111 01110010 00110000 01100011 01101011 01011111 01101001 01110011 01011111 01100011 00110000 00110000 01101011 01101001 01101110 01100111

viii. Flag: HTB{ if_y0u_c@n_$m3ll_wh@t_th3_r0ck_is_c00king}

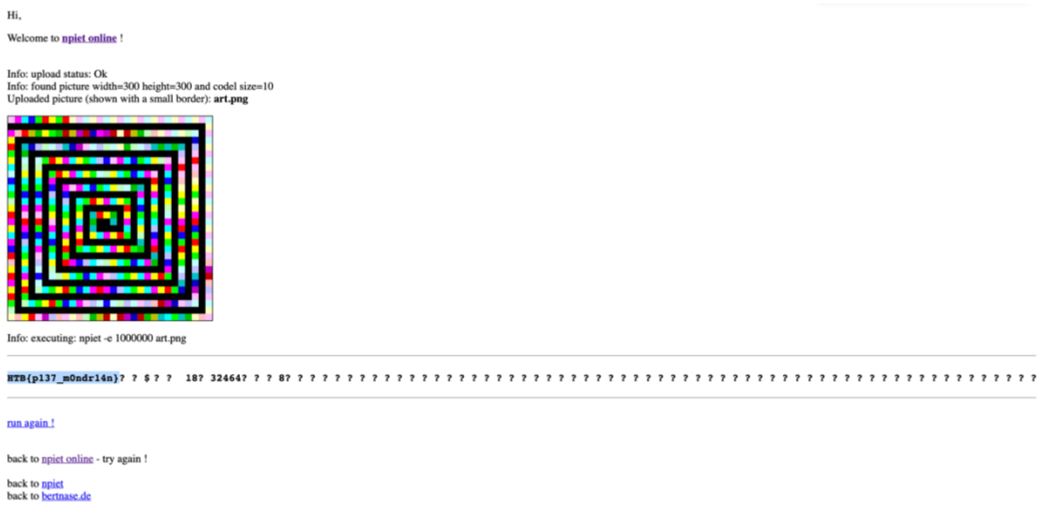
e. Challenge 3: Art (20 points)

   i. Downloaded Zip, similar to above.

   ii. Art.png was unzipped. Looking at this, I though this could be some kind of stenography code and looked at some tools around the web that could do something like that.

   iii. Tool: https://www.bertnase.de/npiet/npiet-execute.php

   iv. Decoded – see image below.



Hi,

Welcome to npiet online !

Info: upload status: Ok
Info: found picture width=300 height=300 and codel size=10
Uploaded picture (shown with a small border): **art.png**

Info: executing: npiet -e 1000000 art.png

```
HTB{p137_m0ndr14n}? ? $ ? ?  18? 32464? ? ? 8? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?
```

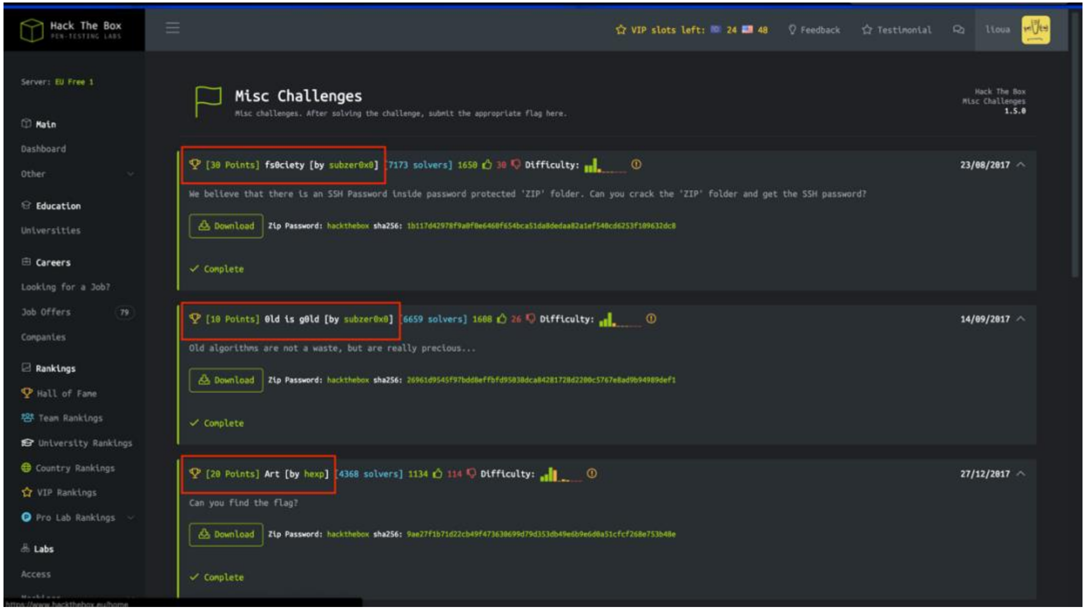
run again !

back to npiet online - try again !

back to npiet
back to bertnase.de

v.

f. Screenshot of all 3 challenges completed and points of each (60 total)



Misc Challenges

Misc challenges. After solving the challenge, submit the appropriate flag here.

Hack The Box
Misc Challenges
1.5.0

[30 Points] fs0ciety [by subzer0x0] [7173 solvers] 1650 30 Difficulty: 23/08/2017

We believe that there is an SSH Password inside password protected 'ZIP' folder. Can you crack the 'ZIP' folder and get the SSH password?

Download Zip Password: hackthebox sha256: 1b117d42978f9a0f0e6460f654bca51da8dedaa82a1ef540cd6253f109632dc8

✓ Complete

[10 Points] 0ld is g0ld [by subzer0x0] [6659 solvers] 1608 26 Difficulty: 14/09/2017

Old algorithms are not a waste, but are really precious...

Download Zip Password: hackthebox sha256: 26961d9545f97bdd0effbfd95038dca84281728d2200c5767e8ad9b94989def1

✓ Complete

[20 Points] Art [by hexp] [4368 solvers] 1134 114 Difficulty: 27/12/2017

Can you find the flag?

Download Zip Password: hackthebox sha256: 9ae27f1b71d22cb49f473630699d79d353db49e6b9e6d0a51cfcf268e753b48e

✓ Complete