

# Final Exam

Arthur Liou

March 21, 2019

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/challenge completed and 5 for how you obtained an invitation code]

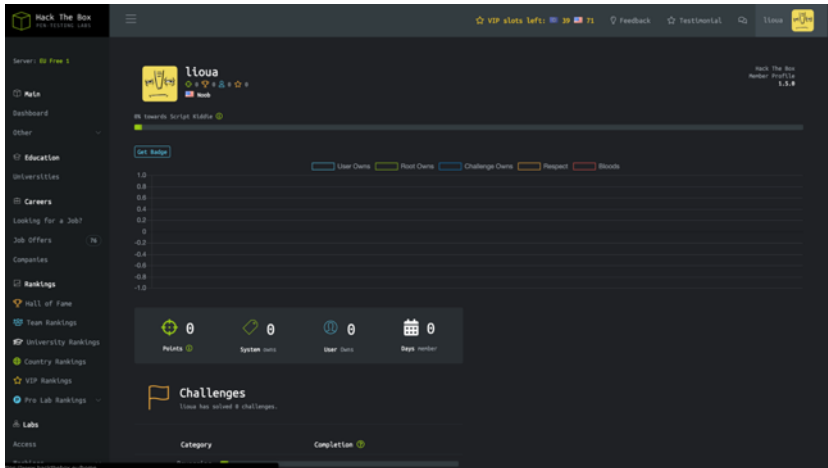
As you can see above, the write-up is the majority of the points. As such, your priority should be on the write-up. The write-up, as usual, can be either a website or a tex document (or the PDF output thereof).

Response

Im 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>



Profile once I first created

2) Challenges Completed: Total Points: 60 points

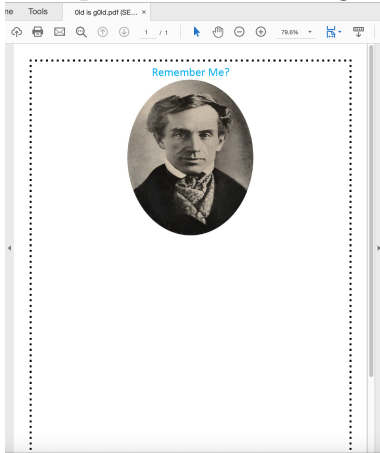
3) I started off the final with generating my own invitation code. On my own I was able to get as far as inspecting elements in ChromeDevTools, `makeInviteCode()`, generating the code, but as far as trying to decode the base64, I needed help so I utilized decoder tools, then hit a Post API call, before 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.

Challenge 1: 0ld is g0ld (10 points) and 1.5k Liked with easy level.

- 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.
- On Mac, I knew of a few password crackers available via homebrew
- I installed pdfrack via homebrew - 'brew install pdf crack
- 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.
- Ran 'pdfrack -f "0ld is g0ld.pdf" -w rockyou.txt' to brute force the PW



- 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.
- 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.
- Flag: HTBR1PSAMU3LM0RS3

Challenge 2: fs0ciety (30 points) and 1.6k liked with easy level

- 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
- Similarly to challenge one, I found a password cracker
- I installed fcrackzip via homebrew - 'brew install fcrackzip
- Using the same rockyou.txt from above to compare
- Ran 'fcrackzip -u -D -p 'rockyou.txt' fsociety.zip'
- PW: justdoit
- Resulting sshcreds-datacenter.txt contained encrypted SSh credentials
- I found base64 and saw the = flag at the end so I realized we needed to convert from base64 to binary.
- Tool: <https://www.base64decode.org/>
- MDExMDEwMDEgMDExMDAxMTAgMDEwMTEwMTEgMDExMTEwMDEgMDAxMTAwMDAg
- The result was binary, so I used another tool to convert that to text. <https://www.rapidtables.com/convert/text/binary-to-ascii.html>
- 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
- Flag: HTB if<sub>y</sub>0u<sub>c</sub>@nm3ll<sub>w</sub>h@t<sub>i</sub>h3r0ck<sub>i</sub>s<sub>c</sub>00king

### Challenge 3: Art (20 points)

- Downloaded Zip, similar to above.
- Art.png was unzipped. Looking at this, I thought this could be some kind of stenography code and looked at some tools around the web that could do something like that.
- Tool: <https://www.bertnase.de/npviet/npviet-execute.php>
- Decoded. see image below.



COMPLETE

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

