

CS2107 Assignment

Capture the Flag: Starter Pack

Last Updated: 2 Feb 2021

Contents

Introduction	1
Contact	1
Acknowledgements	1
Rules and Guidelines	2
Linux Environment	2
Remote Access to Platform	3
Before You Begin	3
Conclusion	3

Introduction

This assignment takes the form of an information security capture-the-flag (CTF) style competition. In a CTF, participants solve problems involving security weaknesses to bypass defences to obtain a sensitive piece of information called the ‘**flag**’.

In this assignment, participants are exposed to some of the common skills required to play in these competitions.

When using the Assignment Platform, do not change your username. For password reset, it may take up to 5 working days so do use a secure yet memorable password.

Contact

Please direct any inquiries about the assignment to

1. wsl@u.nus.edu (Daniel Lim)
2. e0319164@u.nus.edu (Debbie Tan)
3. jaryl.loh@u.nus.edu (Jaryl Loh)
4. wen_junhua@u.nus.edu (Wen Junhua)
5. akarsh@u.nus.edu (Akarsh Agarwal)

Note that the TA will **not** be debugging the student code and will only be there to discuss high level solutions. Do allow 3 working days for replies. Discussion on forums are highly encouraged.

Acknowledgements

This assignment is a collective work of present and past teaching assistants, including Debbie Tan (AY 20/21), Jaryl Loh (AY 20/21), Wen Junhua (AY 20/21), Daniel Lim (AY 20/21), Chenglong (AY 19/20), Shi Rong (AY 17/18, AY 19/20), Glenice Tan (AY 19/20, AY 18/19), Ngo Wei Lin (AY 19/20, AY 18/19), Lee Yu Choy (AY 20/21, AY 19/20, AY 18/19, AY 17/18), Nikolas Tay (AY 16/17) and Jeremy Heng (AY 16/17).

Rules and Guidelines

PLEASE READ THE FOLLOWING BEFORE BEGINNING

1. You are required to log in to <https://cs2107-ctfd-i.comp.nus.edu.sg:8000/> (accessible only within NUS Network) to submit flags. Please verify the self-signed SSL certificate presented by the website before proceeding. The SHA-1 fingerprint is: DC 8E D8 6D 79 06 87 F6 89 79 63 C6 EF 10 C8 5C A2 52 53 D0.
2. You should have received your credentials for logging in to the scoring platform by now (sent to your @u.nus.edu email). If you have not received it, please contact the TAs for assistance.
3. You are required to upload a zip file with filename format StudentID_Name.zip (e.g. A01234567_AliceTan.zip) containing
 - All source codes and scripts if any
 - Useful screenshots
 - A simple write up documenting the approach you took in solving every problem. This must be in PDF format with the following filename format: StudentID_Name_WU.pdf (e.g. A01234567_AliceTan_WU.pdf) Note that grades are not determined by this writeup. However, if there is insufficient evidence that one has done the work individually, further probing and investigation would be conducted. You are required to upload this writeup into the Files->Assignments->Assignment 1->Writeup Submission folder by **23 Feb 2021, 2359 HRS**.
4. Do not attack any infrastructure not **explicitly authorised** in this document.
5. Multiple flag submission is permitted on the scoring platform without any penalty, but **no bruteforcing of flag submission** will be tolerated.
6. Hints will be released gradually as the assignment progresses. They will be announced at <https://cs2107-ctfd-i.comp.nus.edu.sg:8000/announcements>, as well as in the LumiNUS forum / announcements.
7. Work **individually**. Discussion on the forum is allowed but refrain from posting solutions. The university takes plagiarism very seriously. Any sharing of answers detected will be reported and disciplinary actions will be taken.
8. Students may be randomly selected to satisfactorily explain how they obtain their flags; or else a zero mark will be given on their unexplainable challenges.
9. The skills taught in this assignment are not to be used on any system you do not own or have express permission to test. This is a **criminal offence** under the Singapore Computer Misuse and Cybersecurity Act.
10. All challenges have a solution. They are guaranteed to be solvable with assistance of the internet.
11. Ask the TAs for assistance only after you have exhausted every other avenue of self-help.
12. Every challenge will contain a flag and will provide the accepted flag format. Please ensure your submissions meet the flag format stated **exactly**. This means include the `cs2107{}` portion unless otherwise stated.
13. The challenges are tested from the NUS WiFi within the School of Computing and outside of NUS. Connectivity cannot be guaranteed anywhere else in NUS.

One of the most important skills in the information security field is the skill of seeking an answer independently. It is expected that the participant be able to utilise resources discovered through Google or any other search engine to achieve the tasks.

While the challenges might not be covered in entirety in class, the topics in the assignment are very applicable to security problems in real life. In the long run, the practical skills gained would benefit participants immensely.

Linux Environment

A Linux system is crucial for solving some of the challenges, the challenges in this section will prepare you for the more advanced sections by presenting some elementary tasks to solve. It is expected that the participant has rudimentary proficiency in using a Linux system that can be gleaned by reading the tutorial at this link: <https://www.digitalocean.com/community/tutorials/an-introduction-to-the-linux-terminal>.

However, more knowledge might be needed, and it is expected that the participant do some self-exploration.

Do note that you should use a 32-bit / 64-bit Linux environment to aid you in completing some of the challenges. Please also take note that if you are running 64-bit Linux, you may need to run the following commands in Linux to run 32-bit binary executables:

```
sudo dpkg --add-architecture i386
sudo apt-get update
sudo apt-get install -y libc6:i386
```

Remote Access to Platform

As <https://cs2107-ctfd-i.comp.nus.edu.sg:8000/> is accessible only within NUS Network, you may need to install the School of Computing VPN for remote access. The setup guide is available here: <https://dochub.comp.nus.edu.sg/cf/guides/network/vpn>. For more information on the VPN setup, please approach the Level 1 IT Helpdesk at School of Computing.

Before You Begin

To ensure that you understand how to use the platform, you are required to submit the following flag to the **Sanity Check** challenge before you start working on the assignment: `cs2107{246c00aeecddfe7aa0ffa1ac5adf948}`.

Note: You need to complete this challenge. Otherwise, all your flag submissions will be considered invalid and you will not be awarded any marks for this assignment.

Conclusion

I hope the assignment in the upcoming semester will be interesting and engaging. Again, please make sure that your flags are correct and contain the flag format **EXACTLY** as stated. This includes the `cs2107{}` tags.

If you found this interesting and would like to play with harder and more interesting CTF problems, please do feel free to contact us at NUS Greyhats.

Best regards, CS2107 Assignment Team