CS2107 Assignment

Capture the Flag: Assignment 2

Last Updated: 14 Mar 2021

Contents

Introduction **1**
Acknowledgements . . . 2
Grading Scheme and Due Date . . . 2
Contact . . . 2
Rules and Guidelines . . . 2
Linux Environment . . . 3

Section A: Warm Up (2 Points) **3**
A.1 Inspector (1 Point) . . . 4
A.2 Time to REST (1 Point) . . . 4

Section B: Network (6 Points) **4**
B.1 Learn Wireshark (1 Point) . . . 4
B.2 Hide and Seek (5 Points) . . . 4

Section C: Web (58 Points) **4**
C.1 Vaccine (4 Points) . . . 4
C.2 Superior Vaccine (8 Points) . . . 4
C.3 Booster Vaccine (12 Points) . . . 4
C.4 aCross the Site (11 Points) . . . 5
C.5 Local Host Is Safer Than Web (11 Points) . . . 5
C.6 Web Tools (12 Points) . . . 5

Section D: Binary (34 Points) **5**
D.1 BofSchool (2 Points) . . . 5
D.2 CustomCat (8 Points) . . . 5
D.3 Vegas (12 Points) . . . 5
D.4 Address Book (12 Points) . . . 5

Conclusion **5**

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.

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 (AY19/20, AY 18/19), Lee Yu Choy (AY20/21, AY19/20, AY 18/19, AY 17/18), Nikolas Tay (AY 16/17) and Jeremy Heng (AY 16/17).

Grading Scheme and Due Date

This is an individual assignment. You are allowed to post questions on the LumiNUS forum but ensure that the questions do not ask for the solution. Additionally, do not post the answers to the challenges.

This assignment is worth 20% of the grade for the entire module. Assignment 2 is divided into the following sections:

1. Section A: Warm Up - 2 Points
2. Section B: Network - 6 Points
3. Section C: Web - 58 Points
4. Section D: Binary - 34 Points

The maximum number of points that can be obtained in this assignment is 100.

The assignment is due on **18 Apr 2021, 2359 HRS**. Score penalties will apply for late submissions:

- Late up to 2 hours beyond due date: **10% penalty** to points obtained in this period.
- Later than 2 hours: **30% penalty** to points obtained in this period.
- 24 hours beyond the due date: **Submissions will not be entertained after 18 Apr 2021, 2359 HRS**

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 TAs will **not** be debugging your code, but will only be around to discuss high level solutions. Do allow 3 working days for replies. Discussion on forums are highly encouraged.

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: `74 BA BA B7 DC 8B 28 20 CF 26 57 43 BF B9 91 80 F2 07 58 66`.
2. 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) The deadline for the write up is **20 Apr 2021, 2359**

HRS. 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.

3. Do not attack any infrastructure not **explicitly authorised** in this document.
4. Multiple flag submission is permitted on the scoring platform without any penalty, but **no bruteforcing of flag submission** will be tolerated.
5. 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.
6. 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.
7. 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.
8. 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.
9. All challenges have a solution. They are guaranteed to be solvable with assistance of the internet.
10. Ask the TAs for assistance only after you have exhausted every other avenue of self-help.
11. 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.
12. 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
```

Section A: Warm Up (2 Points)

The challenges here are to give you a feel of CTF challenges.

A.1 Inspector (1 Point)

Seems like Ms Petya is back and has been secretly communicating with other people through her resume website. Link: here

A.2 Time to REST (1 Point)

Time to REST here

Section B: Network (6 Points)

The challenges in this section are related to network forensics and have vary difficulty based on the points allocated. It is expected for the student to do some measure of independent research to solve the problems.

B.1 Learn Wireshark (1 Point)

Wireshark is required for this challenge. These are the installation options:

1. Ubuntu CLI: sudo apt-get install wireshark
2. Manual Installation If you are new to Wireshark, you are recommended to watch the Wireshark Tutorial For Beginners video to understand what it does and how it works.

B.2 Hide and Seek (5 Points)

Within the packets hide a sacred cow. Can you find it?

Section C: Web (58 Points)

The challenges in this section are related to web security and have varying difficulty based on the points allocated. Some of these challenges require a little scripting and quite some thinking. It is expected for the student to do some measure of independent research to solve the problems.

C.1 Vaccine (4 Points)

It's NotPetya's turn to sign up for her annual flu vaccine but she no longer remembers her credentials. Can you help her bypass this simple login?

Connect to http://cs2107-ctfd-i.comp.nus.edu.sg:5433

C.2 Superior Vaccine (8 Points)

A vaccine has been found to cure a new infectious virus out there and NotPetya wants to be the first person to take it! Unfortunately, she's no longer logged in. Can you help her out again?

Connect to http://cs2107-ctfd-i.comp.nus.edu.sg:5433

C.3 Booster Vaccine (12 Points)

This new superior vaccine must be done in 2 separate sessions. NotPetya needs to login to sign up for her second session urgently. Unfortunately, there is no persistent login function available. Can you help her bypass this login?

Connect to http://cs2107-ctfd-i.comp.nus.edu.sg:5433

C.4 aCross the Site (11 Points)

My webpage is very secure and so is my Admin Cookie :D Can you help me test it here? Let me know at my Admin Panel if you discover anything and I will visit it.

C.5 Local Host Is Safer Than Web (11 Points)

I am sure that no one can locally read my `flag.php` file when passing it via URL parameter `f`. Could you verify that you cannot read the file located in the same directory?

http://cs2107-ctfd-i.comp.nus.edu.sg:2780/

C.6 Web Tools (12 Points)

Hope you've had fun with the web challenges so far. I made this site with convenient access to my favorite tools.

http://cs2107-ctfd-i.comp.nus.edu.sg:2771/

Section D: Binary (34 Points)

The challenges in this section are related to binary exploitation and have vary difficulty based on the points allocated. Some of these challenges require a little scripting and quite some thinking. It is expected for the student to do some measure of independent research to solve the problems.

D.1 BofSchool (2 Points)

Welcome to BofSchool. More instructions are given in the challenge files.

```
nc cs2107-ctfd-i.comp.nus.edu.sg 2770
```

D.2 CustomCat (8 Points)

We have a program to help you read files on our server! Can you find the flag? You can try testing the binary offline before running your exploit on the server.

```
nc cs2107-ctfd-i.comp.nus.edu.sg 2779
```

D.3 Vegas (12 Points)

Welcome to Las Vegas, the bustling city of lights where people gather in huge casinos. If you are lucky enough, you might strike millions. Perhaps some guessing would do the trick... or maybe not. Security here is tight, better not get caught!

```
nc cs2107-ctfd-i.comp.nus.edu.sg 2773
```

D.4 Address Book (12 Points)

Address Book is back. CS students love it.

```
nc cs2107-ctfd-i.comp.nus.edu.sg 2774
```

Conclusion

We hope you enjoyed the assignment and have learnt something new. 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