CS2107 Assignment 2

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 Chan Jian Hao (AY 21/22), Ye Guoquan (AY 21/22), Debbie Tan (AY 20/21), Jaryl Loh (AY 20/21, AY 21/22), 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 1 is divided into the following sections:

1. **Easy (65 points):** Answer all challenges.

2. **Medium (105 points):** Answer at least 7 challenges from the given 8 challenges to get 105 points; the points from answering Medium-level challenges are capped at 105.

3. **Hard (30 points):** Answer at least 2 challenge; your correctly answered third challenge gives you 15 bonus points.

The maximum number of points that can be obtained in this assignment is 200. You only need to complete 2 question from Section C to obtain full marks, but the third one can help you earn additional bonus points. Note that any bonus points earned in this assignment can be used, if needed, to top up your the following CA components (capped at 40%): 2 CTF assignments (35%) and 1 Group Presentation (5%).

The assignment is due **17 April 2022, 2359 HRS**. Score penalties will apply for late submissions:

- Late up to 12 hours beyond due date: **10% penalty** to total score obtained

- Later than 12 hours but up to 1 day beyond due date: **20% penalty** to total score obtained

- Later than 24 hours but up to 2 days beyond due date: **30% penalty** to total score obtained

- 48 hours beyond the due date: **Submissions will not be entertained after 19 April 2022, 2359 HRS**

Note that submitting a late flag beyond the due date will make your whole submission be considered as a late submission, and the mentioned score penalty scheme applies to your total score obtained.

Contact

Please direct any inquiries about the assignment to

1. jaryl.loh@u.nus.edu (Jaryl Loh)

2. jianhao@u.nus.edu (Chan Jian Hao)

3. kelzin@u.nus.edu (Tan Kel Zin)

4. weiucheng.tan@u.nus.edu (Tan Weiu Cheng)

5. shawn.chew@u.nus.edu (Shawn Chew)

6. dcssu@nus.edu.sg (Prof. Sufatrio*)

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

- : Please cc me if you email your queries about the given challenges; For any issues with access to the CTFd server, please email your TAs

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/ (accessible only within NUS Network) to submit flags.

2. You are **required** to upload a zip file to the "Assignment > Assignment 2 > A2-supporting-files" folder on LumiNUS before the given deadline. The zip file should be named in the form of StudentID_Name.zip (e.g. A01234567_Alice Tan.zip) containing

- A **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_Alice Tan_WU.pdf) Note that grades are not determined by this writeup. However, your writeup should **sufficiently share the approach** that you took in solving every problem. Screenshots may be helpful in showing your steps too. If there are suspicion on plagiarism, your writeup may be analysed and you may need to be interviewed by the teaching team to explain your steps. This writeup also serve as proof of your work in case submission server malfunctions.

- All source codes and scripts, if any, in their respective folder based on the challenge name.

1. Do not attack any infrastructure not **explicitly authorised** in this document.

2. Multiple flag submission is permitted on the scoring platform without any penalty, but **no bruteforcing of flag submission on the server** will be tolerated.

3. Work **individually**. Discussion of concepts 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.

4. 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.

5. 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.

6. All challenges have a solution. They are guaranteed to be solvable with assistance of the internet and some research.

7. Ask the TAs for assistance only after you have exhausted every other avenue of self-help.

8. 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.

9. The challenges are tested from the NUS WiFi within the School of Computing and outside of NUS. Connectivity cannot be guaranteed anywhere else. SoC VPN is **required** if you are outside of school network.

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.

Academic Honesty

NUS students are expected to maintain and uphold the highest standards of integrity and honesty at all times. As this is an **individual assignment**, please refrain from any forms of academic dishonesty.

If any form of plagiarism or cheating is found, you will be penalized and be subject to disciplinary action by the University. You may read more about NUS Student Code of Conduct here.

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
```

Easy Challenges (65 marks)

Answer **all** challenges.

E.1 Nothing to See Here, Really? (10 mark)

Nothing to see here, really?

Connect to http://cs2107-ctfd-i.comp.nus.edu.sg:4000

Author: Shawn

E.2 Linux Access Control (10 marks)

Access Control is an essential component of the Linux filesystem. Figure out what is the Absolute Notation (octal/numerical format) of the file in the attachment.

For example, if the file permission is read, write, execute for all, then the flag for submission would be `CS2107{777}` *.*

Author: Jian Hao

E.3 Insecure Network Communication (10 marks)

We have managed to capture some top-secret communication. Find the secret message in the attached file.

Flag format: `CS2107{secret message}`

Author: Jian Hao

E.4 Host Reconnaissance (15 marks)

I think there is some suspicious network service running on this IP address… Access the network service to get the flag!

`178.128.126.127`

Author: Kel Zin

E.5 Certificate's Content (10 marks)

I just retrieved this certificate from a website… Can you find out the email address of the issuer for me, please?

Flag Format : `CS2107{email}`

Author: Kel Zin

E.6 What Powers Me? (10 marks)

Do visit luminus.nus.edu.sg, and find out the value of the `X-Powered-By` HTTP response header set by the web server.

The expected flag: `CS2107{value of the header}` .

Author: Prof. Sufatrio

Medium Challenges (105 marks)

You may choose to answer **7 out of the 8** challenges from this section. Doing extra **will *not*** earn bonus points. However, you are welcome to answer more than 7 challenges, and we will take 7 of your correct answers in this section.

M.1 Mallory in Action (15 marks)

Hi Mallory, your job is to be malicious as usual. Decipher the message sent by Bob.

`nc cs2107-ctfd-i.comp.nus.edu.sg 4001`

Author: Kel Zin

M.2 The Prequel (15 marks)

Here's a quick warmup for SQLi. Can you bypass the login to get admin privileges?

http://cs2107-ctfd-i.comp.nus.edu.sg:4002/login

Author: Shawn

M.3 Please Join the SQLi Games (15 marks)

You are invited to a series of fun SQLi games, can you win the grand prize?

Connect to http://cs2107-ctfd-i.comp.nus.edu.sg:4003 to join in the fun.

Author: Jian Hao

M.4 File Inclusion (15 marks)

I have a file `secret.php` stored on the server that outsiders cannot read. Oh, and I made a new feature on my website, check it out using URL parameter `f`.

http://cs2107-ctfd-i.comp.nus.edu.sg:4004/

Author: Jian Hao

M.5 ret2win (15 marks)

Just a basic buffer overflow challenge

`nc cs2107-ctfd-i.comp.nus.edu.sg 4005`

Author: Jaryl

M.6 Format String Theory (15 marks)

I have just discovered a new field of science: Format String Theory! I need to publish enough papers to get this theory going, but time is limited! Can you help me?

`nc cs2107-ctfd-i.comp.nus.edu.sg 4006`

Author: Weiu Cheng

M.7 Loophole (15 marks)

Can you find the loophole?

Note: This challenge requires you to spawn a shell on the server using the provided shellcode. It is similar to the basic buffer overflow, but with a little twist.

`nc cs2107-ctfd-i.comp.nus.edu.sg 4007`

Author: Jaryl

M.8 The End (15 marks)

Everything has an end to it, even C strings.

`nc cs2107-ctfd-i.comp.nus.edu.sg 4008`

Author: Weiu Cheng

Hard Challenges (30 marks + 15 marks)

You may choose **2 out of 3** challenges to solve. Extra points from solving all three will count as bonus marks.

H.1 ImpROPer Code (15 marks)

I don't know… I've always been coding like this. Why not you show me the proper way?

I only listen to those who can pop a shell. Prove you expertise to me by getting `/bin/sh` to run here:

`nc cs2107-ctfd-i.comp.nus.edu.sg 4009`

Author: Weiu Cheng

H.2 The Sequel (15 marks)

Well well well, it seems like you have gotten quite good at SQL injection vulnerabilities. For this challenge, login to the app via the credentials `bob:cs2107isthebest` .

http://cs2107-ctfd-i.comp.nus.edu.sg:4010/login

Get the admin password and submit it as the flag.

Author: Shawn

H.3 Genie (15 marks)

1, 2, 3, 4, 5. What numbers can we try?

`nc cs2107-ctfd-i.comp.nus.edu.sg 4011`

Author: Jaryl