CS2107 Assignment 1

Last Updated: 31 January 2022

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 15% of the grade for the entire module. Assignment 1 is divided into the following sections:

1. **Easy (60 points):** Answer all challenges.
2. **Medium (75 points):** Answer at least 5 challenges from the given 7 challenges to get 75 points; the points from answering Medium-level challenges are capped at 75.
3. **Hard (15 points):** Answer at least 1 challenge; your correctly answered second challenge gives you 15 bonus points.

The maximum number of points that can be obtained in this assignment is 150. You only need to complete 1 question from Section C to obtain full marks, but the other 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 **20 Feb 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: **30% penalty** to total score obtained
- 48 hours beyond the due date: **Submissions will not be entertained after 22 Feb 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:8000/ (accessible only within NUS Network) to submit flags.
2. You are required to upload a zip file to the "Assignment > Assignment 1 > A1-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.

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 on the server** will be tolerated.
5. 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.
6. 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.
7. 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.

8. All challenges have a solution. They are guaranteed to be solvable with assistance of the internet and some research.
9. Ask the TAs for assistance only after you have exhausted every other avenue of self-help.
10. 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.
11. 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 (60 marks)

Answer **all** challenges.

E.1 Sanity Check (1 mark)

A flag, written in our flag format, is placed somewhere at the bottom Assignment 1 brief's PDF instruction file.

Try to find and submit it!

Flag format: `CS2107{...}`

Author: Weiu Cheng

E.2 Something's Off (9 marks)

I got a flag. When it's encrypted by a shift cipher according to the operations explained in the `Hints` section, the encryption output is:

`QgGFEL{JvFt7_qF3vH56_I5H_I_ufM_AI5a8d}`

Can you figure out the original flag (i.e. the plaintext) and submit it?

Author: Shawn

E.3 MAC (15 marks)

The term 'MAC' could mean many different things in computing. In cryptography, it stands for Message Authentication Code (MAC) which is often used to confirm message authenticity. Figure out a way to generate the MAC (keyed-hash) of the text.txt file using HMAC with SHA-256 with following alphanumeric string key: `CS21072022`.

Please submit your flag in the following format: `CS2107{MAC of file text.txt}`

Author: Jian Hao

E.4 Secret Penguin (20 marks)

Use `openssl` command to encrypt `tux.png` file using 128-bit **AES** in the **CBC (Cipher Block Chaining)** mode-of-operation.

For the encryption key, use the following 128-bit key given in hexadecimal string format as required by openssl: `1234567890abcdef1234567890abcdef`. Since AES in CBC requires a 128-bit IV, use the following hexadecimal string as the IV: `abcdef1234567890abcdef1234567890`.

Do submit the **SHA-256 digest** of your openssl's encryption output in the following flag format: `CS2107{SHA-256 digest of the encrypted file}`.

Author: Jaryl

E.5 Prime Time (15 marks)

We've sniffed out some information from RSA encrypted traffic. Can you decode it?

Author: Shawn

Medium Challenges (75 marks)

You may choose to answer **5 out of the 7** challenges from this section. Doing extra **will *not*** earn bonus points. However, you are welcome to answer more than 5 challenges, and we will take 5 of your correct answers in this section.

M.1 Insecure OTP (15 marks)

Someone just sent Grandma Susan'oo a new message...

Author: Kel Zin

M.2 Public Password (15 marks)

Wait... passwords aren't supposed to be public... Grandma Susan'oo just joined social media (she calls it "blue bird", how weird). Hope nothing goes wrong...

Just to make sure, I have a program at `nc cs2107-ctfd-i.comp.nus.edu.sg 4003` to check if anyone has her password. If her password is entered...

Author: Weiu Cheng

M.3 Offline Password Cracking (15 marks)

An attacker managed to steal a shadow password file `stolenshadow.txt` from a server. It contains the salted + hashed password of bob, which happens to use a weak password.

The attacker heard from his friend that offline password cracking tools like John the Ripper may be a good tool to find out the weak password.

Can the attacker find out the weak password of bob as reported by John the Ripper?

Submit your flag in the following format: `CS2107{reported password}`

Author: Prof. Sufatrio

M.4 Birthday Hash (15 marks)

Grandma Susan'oo has invited you to join her birthday party!

She has a gift for the best joker!

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

Author: Kel Zin

M.5 Perfect AES, Imperfect key (15 marks)

This code is so short, it must be perfect.

Author: Kel Zin

M.6 Substitution Cipher (15 marks)

This encrypted text is so long that I suspect it is the terms and condition of a software.

The flag is in the last line of the correctly recovered plaintext.

Author: Kel Zin

M.7 Oracle as a Service (15 marks)

Legend has it that this service leaks secret when questioned with a carefully crafted message...

```
nc cs2107-ctfd-i.comp.nus.edu.sg 4002
```

Author: Jaryl

Hard Challenges (15 marks + 15 marks)

You may choose **1 out of 2** challenges to solve. Extra points from solving both will count as bonus marks.

H.1 RSA-locked Doors (15 marks)

"When one door closes, another opens; but we often look so long and regretfully upon the closed door that we do not see the one which has opened for us." - Alexander Graham Bell

Author: Jaryl

H.2 Copper RSA (15 marks)

I use small exponent to encrypt faster!

Author: Kel Zin

CS2107{l3t_7He_j0uRn3Y_b3g1N}