CS2107 Assignment

Capture the Flag: Assignment 1

Last Updated: 3 Feb 2021

Contents

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

1. Section A: Warmup - 15 Points
2. Section B: Legit - 85 Points
3. Section C: Bonus (Optional) - 5 points

The maximum number of points that can be obtained in this assignment is 100. The bonus challenges are optional, and are outside the scope of the module. Regardless, you are awarded points if you solve them.

The assignment is due **21 Feb 2021, 2359 HRS**. Score penalties will apply for late submissions:

- Late up to 2 hours beyond due date: **10% penalty** to score obtained
- Later than 2 hours: Maximum marks obtainable for Assignment 1 is **capped at 70%**
- 24 hours beyond the due date: **Submissions will not be entertained after 22 Feb 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: `DC 8E D8 6D 79 06 87 F6 89 79 63 C6 EF 10 C8 5C A2 52 53 D0`.
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) 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**.

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: Warmup

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

A.1 Hashlet (5 Points)

“This above all: to thine own self be true” - For those who defy this must be MAD!

Though I’ve heard that we could weed this out with a simple MD5 checksum...

Please submit your flag in the following format: cs2107{checksum of existence.txt}

A.2 Grep what you want (5 Points)

I seemed to have misplaced the flag in the folder. Can you help me find it?

A.3 Convert Convert! (5 Points)

Alice has been trying to convey a secret message to Bob in long, but he is only able to understand bytes! Perhaps a little conversion would do the trick…

Section B: Legit

The challenges in this section 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.

B.1 Password Cracking (10 Points)

We heard that Petya Tan has access to some top secret information, and we want to hack her. Try to find her password from her public information.

Weak passwords are short, and normally made up of words related to a person's personal information, usually in lower case or title case. The words might be separated by underscores, hyphens, or nothing. Consider the following information:

1. Birth day / month / year
2. Parts of her name
3. Names of closed ones
4. Job role
5. Address
6. Phone number
7. Or anything the person likes

We found her portfolio here. Do some recon to find words that could possibly be part of her password.

Guide to brute forcing: 1. Find key information about the target based on her social media profile, and create a wordlist containing these information. 2. Join the words (consider both lower case and title case) together using underscores, hyphens, or nothing, to generate a list of passwords to try.

We do not know how many words are in the password, so we need to try the different possibilities one by one. First, consider the scenario where the password only contains 1 word, and try all the possible passwords containing 1 word. If it fails, try 2 words. If it fails again, try 3 words, and so on.

The top secret file is encrypted using the password, and we have also obtained the code used to encrypt it. Find the password to reveal the secret.

B.2 Dear Husband (10 Points)

Alice and Bob use the Diffie-Hellman key exchange public key encryption algorithm to send highly confidential information to each other. Bob has accidentally leaked out the following information and is very worried. On the other hand, Alice claims that Diffie-Hellman is irreversible and there is nothing to worry about. Should they really be worried..?

The flag is their shared secret key in the format cs2107{< shared secret key in ASCII >}. For example: If the secret key is "1234", then the flag is cs2107{1234}.

B.3 Custom Protocol (10 Points)

We just found out the encryption scheme used by Spy Co to send their messages. Now we just need a way to decrypt the files. Can you find a way to decrypt the file and get the super secret message?

B.4 Now XOR Never (10 Points)

Petya loves the convenience of recording her confidential data in images. She encrypts her files and claims that they are completely safe. She would be so impressed if anyone is able to decipher her secrets...

Note: You will not be able to open the png file, but there is nothing wrong with it, because it is encrypted. Decrypt it to view the contents.

B.5 Hacker Wall of Fame (15 Points)

A new task for you! Can you put yourself up on the Hacker Wall of Fame? I've given you the source. Make good use of it!

http://ctf.nus-cs2107.com:2771

B.6 Password Manager (15 Points)

Password managers are overrated. Check out mine.

B.7 Password Manager v2 (15 Points)

I've made my system more secure. Check out the latest version.

Section C: Bonus

The challenges in this section are more challenging. They are optional and for addtional learning.

C.1 Guessing Game (3 Points)

Life is random. That's what people say. Can you guess your way, to secure an A?

http://ctf.nus-cs2107.com:2774/

C.2 - Who is Petya? (2 Points)

It appears that there is a secret hint to Petya's mysterious identity in the folder we unlocked during spring cleaning.

Can you help us find out who Petya truly is?

Note: Read up on steganography

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