CS2107 Assignment 2

Last Updated: 17 October 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 Akash (AY22/23), Kel Zin (AY22/23, AY21/22), Weiu Cheng (AY22/23, AY21/22), Wen Junhua (AY22/23, AY20/21), Shawn Chew (AY 21/22), Chan Jian Hao (AY21/22), Ye Guoquan (AY21/22), Debbie Tan (AY20/21), Jaryl Loh (AY20/21, AY21/22), Daniel Lim (AY20/21), Chenglong (AY19/20), Shi Rong (AY17/18, AY19/20), Glenice Tan (AY19/20, AY18/19), Ngo Wei Lin (AY19/20, AY18/19), Lee Yu Choy (AY20/21, AY19/20, AY18/19, AY17/18), 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 (75 points):** Answer all challenges.
2. **Medium - Web Security (30 points):** Answer only one challenge; Solving the other challenge **does not** earn you bonus points.
3. **Medium - System Security (30 points):** Answer only one challenge; Solving the other challenge **does not** earn you bonus points.
4. **Hard (15 points):** Answer only one challenge; Solving the other challenge **does not** earn you bonus points.
5. **Bonus (15 points):** *Optional*. Solve **all** challenges to obtain 15 bonus points.

The maximum number of points that can be obtained in this assignment is 150. Solving **all** questions in the bonus section 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: 2 CTF assignments (30%) and 1 Group Presentation (5%).

To illustrate how the point calculation is done, you can consider the following 2 examples. Suppose Bob correctly answers all easy challenges, 4 medium (2 web, 2 system) challenges, and 0 hard challenges. Bob obtains: 75+30+30+0=135. Alice, meanwhile, correctly answers all easy challenges, 1 medium (system) challenge, 2 hard challenges and all bonus questions. Alice obtains: 75+30+0+15+15=130. Alice actually earns her 15 bonus points, which are then used to directly top up her A2 points.

The assignment is due **13 November 2022 (Sunday), 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 36 hours beyond due date: **20% penalty** to total score obtained
- Later than 36 hours but up to 72 hours beyond due date: **30% penalty** to total score obtained
- 72 hours beyond the due date: **Submissions will not be entertained after 16 November 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.

Please avoid submitting old flags from past assignments of this module. If you are caught submitting a past flag to a challenge, your points to that challenge will be capped to 70% of its possible points. Note that past flags won't work anyway.

Contact

Please direct any inquiries about the assignment to

1. kelzin@u.nus.edu (Tan Kel Zin)
2. weiucheng.tan@u.nus.edu (Tan Weiu Cheng)
3. wen_junhua@u.nus.edu (Wen Junhua)
4. c.akash@u.nus.edu (Akash Chandrasekaran)
5. 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 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.

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.

The nc Command

Throughout the assignments, if you see challenge with `nc aaa.bbb.ccc.ddd xxxx`, then it means that the challenge is hosted on the `aaa.bbb.ccc.ddd` server on `xxxx` port.

You can connect to the server by using the `nc` command in your terminal. In short, you can just copy & paste `nc aaa.bbb.ccc.ddd xxxx` and run it directly.

If you wish to host a TCP server locally, you can use ncat `ncat -lvk -p 15000 -e "python3 main.py"`

Then connect to it with `nc localhost 15000`

Python3 Cheatsheet

Some challenges in the assignment might require some scripting to solve. Although you can use any programming languages you prefer, we recommend Python3.

Here's a link to a cheatsheet: https://gist.github.com/DavidTan0527/43edbf49fc550100a5a88d23627480ff

If you prefer a PDF file, you can download it from the assignment folder.

System Security Cheatsheet

You can find the cheasheet here: https://gist.github.com/DavidTan0527/ec2a73972284d38b1233bcd7d757f793

If you prefer a PDF file, you can download it from the assignment folder.

Easy Challenges (75 marks)

Answer **all** challenges.

E.1 Wireshark (15 mark)

Bob is sending his password unencrypted through the network. We (hackers) have successfully sniffed and captured Bob's packets from the network, but there is a lot of noise from other irrelevant packets.

Can you help us to find his password using WireShark?

His password is in the format of: `CS2107{...}`

Author: Kel Zin

E.2 Offline Password Cracking (15 marks)

An attacker managed to steal a shadow password file `shadow.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: Kel Zin

E.3 Inspect Element (15 marks)

I started a new personal web project, but it's still work in progress. There is nothing to see here, or is there?

http://165.22.244.105:12345

Flag format : `CS2107{...}`

Author: Weiu Cheng

E.4 NMAP Reconnaissance (15 marks)

I think there is some suspicious network service (HTTP) running on this IP address: `165.22.244.105`

Access the network service to get the flag!

Note: please ignore the ports 12345, 48787 as they are not related to this challenge. Other common ports like 80, 443 etc. should also be ignored.

Author: Weiu Cheng

E.5 Cookie Inspection (15 marks)

What are cookies? Hmm are they edible? I have hidden my cookies :D. Can you find them?

http://cs2107-ctfd-i.comp.nus.edu.sg:16061/

Author: Junhua

Medium Challenges (System Security) (30 marks)

You must choose to answer only 1 out of the 3 challenges from this section. Doing more than 1 **will *not*** earn bonus points. However, you are welcome to answer all the challenges.

M.1 udp_viewer (30 marks)

I made a UDP Packet Viewer for one of my classes, but someone said that there was something wrong with it?! Can you find out what?

`nc cs2107-ctfd-i.comp.nus.edu.sg 16303`

Author: Akash

M.2 firm_bouncer(30 marks)

The bouncer got replaced, now this one is just *firm*. Uh, mind hacking him so that I can get some tequilas?

`nc cs2107-ctfd-i.comp.nus.edu.sg 16302`

Author: Akash

M.3 bouncer (30 marks)

This bouncer just won't let me go inside to the shell! Can you just hack him?

`nc cs2107-ctfd-i.comp.nus.edu.sg 16301`

Author: Akash

Medium Challenges (Web Security) (30 marks)

You must choose to answer only 1 out of the 3 challenges from this section. Doing more than 1 **will *not*** earn bonus points. However, you are welcome to answer all the challenges.

M.4 Baby XSS (30 marks)

Learn how to execute an XSS attack with step by step instructions on the website

http://cs2107-ctfd-i.comp.nus.edu.sg:16062/

Author: Junhua

M.5 XSS with Filter (30 marks)

I have implemented a filter :D. Can you bypass it?

http://cs2107-ctfd-i.comp.nus.edu.sg:16063/

Author: Junhua

M.6 sqli_notes (30 marks)

Special Queryable L33t In Notes (sqli_notes) might be exploitable! Find the flag in the secret note!

http://cs2107-ctfd-i.comp.nus.edu.sg:16305/

Author: Akash

Hard Challenges (15 marks)

You may choose **1 out of 2** challenges to solve.

H.1 Shellcoding (15 marks)

Shellcoding is a traditional way of writing code on turtle shells back when paper wasn't invented. Not everyone has shells to code with, can you try to get a shell yourself?

Author: Weiu Cheng

H.2 CSR Family (15 marks)

I have created this new webpage where everyone can keep their own secrets.

However, whats the fun of the secret if no one has a chance of finding it out?

I wonder how someone can do that :P.

http://cs2107-ctfd-i.comp.nus.edu.sg:16064/

Author: Junhua

Bonus Challenges (15 marks)

(This section is optional) These challenges are not in the scope of the module. You are required to do additional research yourself to solve the challenges.

You need to answer **all** 2 challenges here to obtain the 15 bonus marks. i.e Answering only 1 challenge will not give you any marks.

:warning: PROCEED WITH CAUTION :warning:

Bonus.1 banana

I couldn't think of a proper name, so this is called `banana`.

```
nc cs2107-ctfd-i.comp.nus.edu.sg 16304
```

Author: Akash

Bonus.2 Local Delicacies

Welcome to my Recipe shop with local delicacies. Feel free to view the various delicacies available.

http://cs2107-ctfd-i.comp.nus.edu.sg:16065/

Author: Junhua