CS2107 Assignment 1

Last Updated: 18 February 2024

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.

Acknowledgements

This assignment is a collective work of present and past teaching assistants, including Yitian (AY23/24), Yong Liang (AY23/24), Ariana (AY23/24), Quang Vinh (AY23/24), Ashok (AY23/24), Arnav Aggarwal (AY23/24), Devesh Logendran (AY22/23, AY23/24), Akash (AY23/24, AY22/23), Sean Tay (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 Canvas Discussions forum but ensure that the questions do not ask for the solution. Additionally, do not post the answers to the challenges.

Assignment 1 is divided into the following sections:

1. **Easy (10 points each):** Answer all challenges (40 points total).
2. **Medium (20 points each):** Of the 4 challenges, solve at least 2 (40 points total).
3. **Hard (20 points each):** Of the 2 challenges, solve at least 1 (20 points total).

The maximum number of points that can be obtained in this assignment is **100** (worth 10% of the total score for the entire course). Solving the other bonus challenges 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 CTF assignment. **There are no partial marks.** Solving challenges more than the intended maximum for medium/hard will not give you additional marks.

To illustrate how the point calculation is done, you can consider the following 2 examples. Suppose Bob correctly answers all easy challenges, 4 medium challenges, and 0 hard challenges. Bob obtains 40+40+0=80. Alice, meanwhile, correctly answers all easy challenges, 2 medium challenges, and 2 hard challenges. Alice obtains 40+40+20=100.

The assignment is due **7 Mar 2024 (23:59)**.

Penalties

Late submission of challenges

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 10 Mar 2024 (23:59)**

Other Penalties

Full marks for this assignment is **100**.

1. Submission of past flags (per flag): -10 pts
2. Late submission of Writeup (see more about its submission below): -10 pts
3. No source code (if necessary for completeness): -10 pts
4. Unclear Writeup:
   - Interview to explain solve
   - Unable to explain = -30% (of the relevant challenge)
5. Blank Writeups: -40% (of the relevant challenge)
   - Will also be asked for interview
   - Unclear writeup deduction will also apply (total -70% of relevant challenge)

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. ariana@u.nus.edu (mailto:ariana@u.nus.edu) (Ariana Goh Zhi Hui)
2. yitian@u.nus.edu (mailto:yitian@u.nus.edu) (Cao Yitian)
3. yongliangang@u.nus.edu (mailto:yongliangang@u.nus.edu) (Ang Yong Liang)
4. nqvinh@u.nus.edu (mailto:nqvinh@u.nus.edu) (Nguyen Quang Vinh)

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.

Rules and Guidelines

PLEASE READ THE FOLLOWING BEFORE BEGINNING

1. You are required to log in to CTFd (https://cs2107-ctfd-i.comp.nus.edu.sg/) (accessible only within NUS SoC Network) to submit flags.

2. You are **required** to upload the required files **separately** to the “Assignment 1” folder on Canvas before the given deadline.

   - 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)

   - All source codes and scripts that you used while solving the problem, if any. Submit each script as a **separate file** named after the challenge it applies to.

   - **Note** that grades are not directly 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.

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 (https://webvpn.comp.nus.edu.sg/) 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 (http://nus.edu.sg/osa/docs/default-source/osa-doc/resources-and-policies/code-of-student-conduct.pdf?sfvrsn=14040e3d_4).

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 (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 (https://www.tecmint.com/netcat-nc-command-examples/) in your terminal. In short, you can just copy & paste `nc aaa.bbb.ccc.ddd xxxx` and run it directly.

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.

To dynamically with interact with TCP server, you can use pwntools (https://docs.pwntools.com/en/stable/)

```
from pwn import * # Import pwntools

r = remote("123.123.123.123", 15000) # Connect to 123.123.123.123 a

s = b'abcde'
r.sendline(s) # Send bytes s to the server
r.sendafter(b'message:', s) # Send bytes s after received bytes 'me

r.recvline() # Receive a line from the server
r.recvuntil(b'Nonce: ') # Receive until the bytes 'Nonce: ' from th
r.recvall() # Receive all bytes until EOF

r.interactive() # Change to interative mode
```

Note that all the received message are in bytes. So you might to some conversion if necessary.

You can also change to debug mode with

```
r = remote("123.123.123.123", 15000, level='debug')
```

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

Easy Challenges (40 marks total)

Answer **all** challenges.

E.0 Sanity Check (0 mark)

A flag, written in our flag format, is placed somewhere in the assignment instruction file.

Try to find and submit it!

Flag format: `CS2107{...}`

Author: Quang Vinh (nqvinh@u.nus.edu (mailto:nqvinh@u.nus.edu))

E.1 Rivest–Shamir–Adleman (10 marks)

Bob and Alice are good friends who have been sending each other secret messages. Unfortunately, Bob accidentally revealed some sensitive information while transmitting the secret message. Using sniffing techniques, Mallory managed to intercept the message from Bob and now wants to decrypt them. But how?

Author: Yong Liang (yongliangang@u.nus.edu (mailto:yongliangang@u.nus.edu))

E.2 xor_secure (10 marks)

One-time-pad is really strong, so how about four one-time-pad?? This should be four times as strong.

I have encrypted a secret message using four-time-pad, can you obtain that message? The code used and the output of the encryption is given.

Author: Quang Vinh (nqvinh@u.nus.edu (mailto:nqvinh@u.nus.edu))

E.3 Hash Browns (10 marks)

Can you "decode" the hashes? Wait it should be one-way right?

Ok your task will be to "decode" these list of hashes.

Author: Yong Liang (yongliangang@u.nus.edu (mailto:yongliangang@u.nus.edu))

E.4 Caesar with a capital C

Did you know that Caesar was assassinated with pugiones? Pugiones were actually a type of daggers used by Roman soldiers. There were some doors we found that used daggers as keys, can you help me find my dagger?

This is a caesar cipher challenge. The source code for the encryption is provided. The flag is in the form of `CS2107{flag_text}` where `flag_text` is replaced by the correctly decoded plaintext.

Author: Yitian (yitian@u.nus.edu (mailto:yitian@u.nus.edu))

Medium Challenges (40 marks total)

Answer **at least 2** challenges.

M.1 AES-ECB (20 marks)

I accidentally encrypted my file and forgot my password! Can you decrypt the file for me?

HINT: Flag is in printable ASCII format

Author: Ariana (ariana@u.nus.edu (mailto:ariana@u.nus.edu))

M.2 Baby Shark (20 marks)

Baby Shark, doo-doo, doo-doo, doo-doo Baby Shark, doo-doo, doo-doo, doo-doo Baby Shark, doo-doo, doo-doo, doo-doo Baby Shark ...

What files could be hidden within the pcapng file?

Flag Format: `CS2107{...}`

HINT: Wireshark could be useful in helping us to analyse pcapng files

HINT: Some HTTP file objects have been trasmitted, how can you extract those files?

HINT: https://www.wireshark.org/docs/wsug_html_chunked/ChIOExportSection.html (https://www.wireshark.org/docs/wsug_html_chunked/ChIOExportSection.html)

Author: Yong Liang (yongliangang@u.nus.edu (mailto:yongliangang@u.nus.edu))

M.3 hash_key (20 marks)

Haiyaa! Why does everyone always insist on generating some random string for AES key? I prefer random numbers! To make this even more secure than the silly random string, I even hash the number into a super long string that you can't possibly guess.

I have encrypted a secret message using this technique. The encryption source code, as well as the output of the encryption, are given.

Author: Quang Vinh (nqvinh@u.nus.edu (mailto:nqvinh@u.nus.edu))

M.4 Salad (20 marks)

We have intercepted an encrypted text file from a malicious hacker group, and we also managed to retrieve this weird python file that we think might have something to do with it, can you help us crack this encrypted message?

Author: Yitian (yitian@u.nus.edu (mailto:yitian@u.nus.edu))

Hard Challenges (20 marks total)

Answer **at least 1** challenge.

H.1 Broadcasting (20 marks)

I have a really cool message that I want to share to all my friends. To ensure that no sneaky people obtain this message, I will use RSA encryption. For extra safety, I will generate a different RSA key pair for each friend of mine.

Surely this is safe! I have provided the source code and the output that I sent to my friends.

Author: Quang Vinh (nqvinh@u.nus.edu (mailto:nqvinh@u.nus.edu))

H.2 Secure Password (20 marks)

I forgot my password and lost access to my secret vault :(Luckily I downloaded a copy of the website. Could you help me recover the password?

Author: Ariana (ariana@u.nus.edu (mailto:ariana@u.nus.edu))

CS2107{nice_job_reading_til_here!}