Homework #12

Due Time: 2025/12/09 (Tue.) 23:59

Contact TAs: `vegetable@csie.ntu.edu.tw / nasa@csie.ntu.edu.tw`

Instructions and Announcements

- **NO LATE SUBMISSION OR PLAGIARISM IS ALLOWED.**
- Discussions with others are encouraged. However, you should write down your solutions **in your own words**. In addition, for **each and every** problem you have to specify the references (the URL of the web page you consulted or the people you discussed with) on the first page of your solution to that problem.
- Some problems below may not have standard solutions. We will give you the points if your answer is followed by reasonable explanations.

Submission

- Please place your answers in the same order as the problem sheet and do not repeat problem descriptions, just organize them by problem number in a tidy manner.
- Please zip the pdf file and xml file, name the zip file "`{your_student_id}.zip`", and submit it via NTU COOL. The directory layout should be the same as listed below:

```
{your_student_id}/
+-- {your_student_id}.pdf
+-- code/
    +-- ...
```

  The `code` directory should include all necessary scripts and files you used to solve the problems.

Grading

- The total score for the correctness and completeness of your answer is 115 points.
- It's possible you don't get full credits even if you have the correct answer. You should show how you get the answers step by step and list the references.
- Tidiness score: 3 bonus points, graded by TA.
- Final score = min(correctness score, 100) + tidiness score.

Security Part II

0. 注意事項

- 請不要用任何形式干擾其他人作答，或不是以解題為目的來攻擊本作業的各項設施。經舉發查證屬實者，將會受到非常嚴厲的懲罰。
- 本次作業會用到的檔案都能在這裡找到。
- 標有 (CTF) 的題目都會有 flag，flag 的格式都是 `HW12{[0-9A-Za-z_]+}`。請務必在你的作答中明寫出你所找到的 flag。
- 可以使用生成式 AI (包含 ChatGPT 及其他類似工具) 來分析 CTF 題的程式碼與釐清問答題相關概念，但嚴禁使用生成式 AI 完整作答題目。完全用生成式 AI 回答的助教會斟酌扣分。
- 如果你有寫腳本來進行解題，請放在 `code/` 資料夾底下，並在 report 中提及之。
- 動手操作的題目都需要詳細說明自己是如何做到的。請說服批改助教「你是真的有自己想過」還有「你是真的懂」。
- 即便沒解出來也請儘量作答，可以寫下錯誤的嘗試或是網路上搜尋到的資料。批改的助教將會依照方向與距離答案多遠來給予部份分數。
- 只要不是抄襲或作弊，非常歡迎你嘗試非預期解。

1. Linux 大小事 (25 points)

(a) (5 points) 請問在現行 Linux 系統下，會如何儲存使用者密碼？

(b) (5 points) 你會發現只有 `root` 有權限進行讀寫 `/etc/shadow`，那麼一般使用者又是如何使用 `passwd` 來達到更改密碼的效果呢？

(c) (5 points) 如果你有一台暴露在網際網路上的 server，就會發現每次 ssh 上去時，shell 顯示自從你上次登入以來有很多 login failure。請以 Ubuntu 為例（版本 $\geq$ 14.04），找到這些登入嘗試的 log 被放在哪個檔案，並說明那個檔案裡存了哪些資訊。

(d) (10 points) 以一個 server administrator 的角度來說，有甚麼方法能防範密碼被多次 ssh 暴力破解？請舉出兩種方法。

2. 畫中有話 (15 points)

wiwi 和 balu 是兩位 MyGO!!!!! 愛好者，他們天天都在用 MyGO 圖交流。乍看之下，就只是一堆正常的圖，但 fysty 覺得其中必有蹊蹺，他堅信每張圖裡面都藏著隱藏的資訊，於是他向通靈大師黑川特石尋求協助。黑川特石利用他的通靈能力通靈出兩人將訊息藏在圖片中的工具 hide.py。

(a) (5 points) 請解釋 `hide.py` 的運作原理，即它是如何將一串訊息藏在一張圖片中的。

(b) (10 points) (CTF) fysty 不擅長寫程式，但它擅長攔截訊息，secret_mygo.png 是它攔截到的其中一張圖，你能幫 fysty 找出藏在圖中的訊息嗎？

3. Alya Judge (60 points)

Alya Judge 是 nathan 某天心血來潮架設的 Online Judge。只花一天就產出的 Judge 肯定漏洞百出。

注意事項

- 如果發現服務掛了，或是有任何可能的不正常行為，請儘快寄信詢問。
- 在合理的理由下，短時間上傳大量 submission 是允許的。
- 再次提醒，無論最後有沒有成功獲得 flag 也請將做題過程寫清楚，我們會按照完成度斟酌給予部分分數。

Useful Resources

- Source code: alyajudge.zip
- Alya Judge: `http://140.112.187.51:45588`

(a) (20 points) (CTF) flag1 藏在 fysty 的上傳紀錄裡，你能把他找出來嗎？

Hint1: 聽說 fysty 的密碼有點弱，要是能看到真正的 `accounts.json` 就好了……

Hint2: 某個 route 似乎可以進行 path traversal 攻擊？(如果你發現 `..` 被吃掉了，可以試試看把一些 `.` 和 `/` 換成 `%2e` 和 `%2f` 。)

Hint3: fysty 的密碼在這裡出現過。

(b) (20 points) (CTF) nathan 不小心把未完成的題目公開了！你能成功獲得 Accepted 並找出 flag2 嗎？

Hint1: 如果把 flag2 當作 submission 上傳到在未完成的題目會獲得 Accepted。

Hint2: Alya Judge 是怎麼檢查並評分你所上傳的程式碼的？`special_judge` 函式在幹嘛？

Hint3: flag2（包含 `HW12{...}`）的長度為 15 個字元。

(c) (20 points) (CTF) flag3 藏在 admin 的上傳紀錄裡，你能把他找出來嗎？

Hint1: 有辦法在不知道 admin 密碼的情況下讓 server 覺得你是 admin 嗎？

Hint2: 餅乾很好吃，他是怎麼製作和運作的？

4. Introduction to gnireenignE esreveR (15 points)

相信大家在 HW0 都已見識過 `strings` 指令的美好，但很顯然的，這不是個萬能的指令，設計者很容易就能防止原始碼的字串被偷看到。這時候該怎麼辦呢？

沒錯，就是要對執行檔進行逆向工程 (Reverse Engineering)！透過一些工具，我們可以一定程度的還原執行檔的原始碼，再搭配組語以及 hex dump 一起分析就能好好還原程式碼的行為。

本題希望同學可以見識一下這些反編譯器，並透過觀察反編譯出的 source code 來了解執行檔的行為並破解它。

- Online decompiler: Dogbolt（建議用這個）
- Other disasemblers/decompilers: Ghidra, IDA, Binary Ninja
- Challenge executable: chal.exe

(a) (15 points) (CTF) 請找出 chal.exe 隱藏的 flag，並解釋 chal.exe 是如何運作的。