Homework #12 - Security

Due Time: 2024/06/08 (Sat.) 23:59
Contact TAs: vegetable@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 submit you answer through Gradescope.

Grading

- Part I accounts for 100 points while Part II accounts for 120 (20 points as bonus) points, and **both of them will account 3 points** in your semester grade (totally 6 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 (Part I) +3 (Part II) bonus points, graded by TA.

Security – Part I

說明

- 請不要用 ChatGPT 回答，完全用 ChatGPT 回答的我們會斟酌扣分
- 題目中的 flag 的格式皆為 `HW12{XXX}`。
- 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. 好想吃摩斯漢堡 (Cryptography) (27 points)

(a) (5 points) 有一天下午，你正在德田館地下室寫著 nasa 作業。突然，你聽到了一個神祕的聲音傳來, 請將神祕聲音的內容解密出來, 並以 flag 的形式寫出 — HW12{XXX}。
Hint: 這種加密方式常用於電報

(b) (5 points) 聽到神秘聲音後，你突然超想吃摩斯漢堡。但是在你想要離開地下室時，發現門被鎖了起來，而且門把無法旋轉，但是門上貼了一張寫有密文的紙條，並且多了可以輸入密碼的電子鎖。請將紙條上的密文解密並寫出。
Hint 1: 紅字和使用到的加密方法有關
Hint 2: 「旋轉」的英文翻譯是 *rotate*

(c) (5 points) 當你打開門後，一個人影朝你靠近。原來是外國交換學生blaise。他給你一張紙條就離開了。你發現紙條上的文字好像被加密過了，而你能看懂的只有最下方的MOSBURGER，於是你決定 decode 紙條上的文字，看看 blaise 想和你說甚麼。
Hint 1: 紅字和使用到的加密方法有關
Hint 2: 這個加密方法和 *blaise* 這個人物有關

(d) (5 points) 當你走到小福門口後，發現大門關了起來，並且門上貼了告示。但是告示上的文字有點奇怪，於是你決定將告示的內容進行解密，找出小福大門緊閉的原因，並看看有沒有甚麼替代的方法可以買到摩斯漢堡。
Hint 1: 紅字和使用到的加密方法有關
Hint 2: 「替代」的英文翻譯是 *substitute*

(e) (7 points) 歷經千辛萬苦後你終於來到了摩斯漢堡，當你像要看看今天有沒有限定漢堡時，你發現menu有點怪怪的。於是你決定要將真正的 menu 找出來。
Hint: 摩斯漢堡的 *menu* 應該只有一張圖片

2. DNS security (25 points)

討論(a)(c)差異

(a) (5 points) 請解釋甚麼是 DNS Spoofing，以及它如何影響 DNS 服務。

(b) (5 points) 請解釋 DNSSEC 的原理，以及如何利用這個技術防止 DNS Spoofing。

(c) (5 points) 請解釋甚麼是 DNS Cache Poisoning，以及它如何影響 DNS 服務。

(d) (5 points) 請解釋甚麼是 NXDOMAIN 攻擊，以及這種攻擊如何影響 DNS 服務。

(e) (5 points) 假如你今天是 DNS server 的管理者，當 DNS service 遭受攻擊時，你會採取那些措施來預防和檢測 DNS 攻擊。

3. CIA Triad & Threat Modeling (18 points)

課堂上有提到 CIA 一般用來當作資訊安全的準則，其中 C, I, A 三個字母分別代表 Confidentiality, Integrity 和 Availability，其實也就是一個「正常的服務」所應具備的要素。

(a) (6 points) 請舉出兩個現實生活中的資安事件，說明其違反 CIA 的哪幾項，並說明原因。

為了達成 CIA，我們會透過 threat modeling 來搞清楚我們可能會面對的攻擊手法，並針對攻擊做出相應的防禦。以下的題目會提出許多不同的系統 (System) 與安全需求 (Security requirement)，你需要提出不超過 4 個合理的假設 (Assumption) 與 2 種不同的 threat model，每種 threat model 都需要提供一個應對措施。不同題目間的 threat model 不能太相似，否則批改者會認定你是偷懶而斟酌扣分。

題目舉例

- System: 系上網路列印服務
- Security requirement: 同學們可以使用網路列印功能，在送出請求的三分鐘之內取得列印完成的印刷品

參考解答

- Assumption:
  1. 電子設備的電子元件皆狀態良好
- Threat model:

Threat Model	Countermeasure
有人嘗試利用網路列印頁面的網頁漏洞來攻擊服務	定期將 server 更新至最新版本
有人透過大量列印來耗盡印表機的資源（紙張或碳粉匣）	在資源剩餘量低落時，限制每個人的使用量，並通知管理員補充列印資源

題目

(b) (4 points)

- System: 個人筆電
- Security requirement: 沒有被擁有者允許的人不能使用

(c) (4 points)

- System: 簡訊實聯制
- Security requirement: 任何人皆以自己的真實身份進行實聯制掃描並傳送簡訊

(d) (4 points)

- System: NASA 線上期末考
- Security requirement: 考試期間，各組不得以任何方式與非同組的人類進行交流

4. Web Security (30 points)

`OWASP Juice Shop`: https://github.com/juice-shop/juice-shop

`OWASP Juice Shop` 是一個相當**不安全**的網頁服務，一般用於資安相關的訓練或競賽。其中包含了 OWASP Top Ten 以及其他現實生活中的資安漏洞。本題希望同學們能夠透過 OWASP Juice Shop 上的題目來學習到 web security 相關的知識。在本題中，請參考上方連結自行架設一個 `OWASP` 伺服器（建議用 Docker 架設），並完成以下要求。

Note. 你可以在 `/#/score-board` 找到 Scoreboard，在 Scoreboard 中可以找到題目，以及要解開題目需要做哪些操作以及提示。

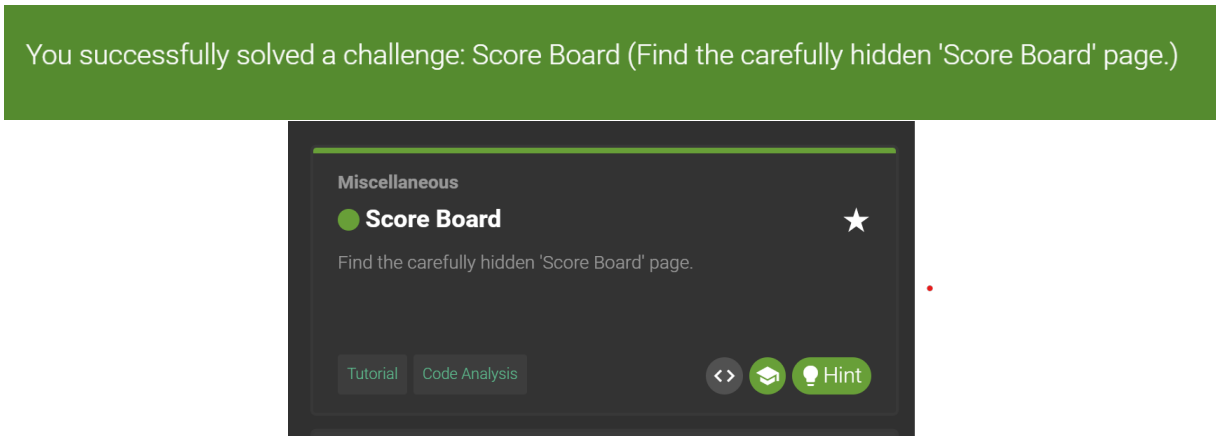
(1) (20 points) 請同學們做

(a) DOM XSS;
(b) Bonus Payload;
(c) Confidential Document;
(d) Error Handling;
(e) Login Admin 以上 5 題，並附上 Scoreboard 截圖。

請同學們附上解題過程，並說明題目介紹的漏洞類型以及原理，並給出解決漏洞的方法。

Hint: Scoreboard 提供的 *Hint* 很有用

範例: 當同學們第一次進入 *scoreboard* 時，應該能夠看到自己成功解出第一題，網頁會跳出 *You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)*



(2) (10 points) 請簡單介紹 CSRF 是什麼以及背後的原理。

Security – Part II

說明

- 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。
- 請不要用 chatGPT 回答，完全用 chatGPT 回答的我們會斟酌扣分
- 題目中的 flag 的格式皆為 `NASA{XXX}`
- 如果你有寫了 script 或程式來進行解題，請在作業的 zip 中附上檔案，放在 security 資料夾底下，並在 report 中提及。
- 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。
- **建議同學早點設置好環境，設置環境很可能就已經花了一些時間**。

0. Setup

裏面寫了啥

請在工作站上執行 `/tmp2/nasa-hw12/run.py` 並等待一會，這個指令會再 `/tmp2/< 你的學號 >/nasahw12/` 中生成以下兩題以及 Lab 所需要的虛擬機環境。完成後會輸出 VNC 的密碼，且執行 `virsh list --all` 會出現 nasa-sec-vm 的虛擬機。

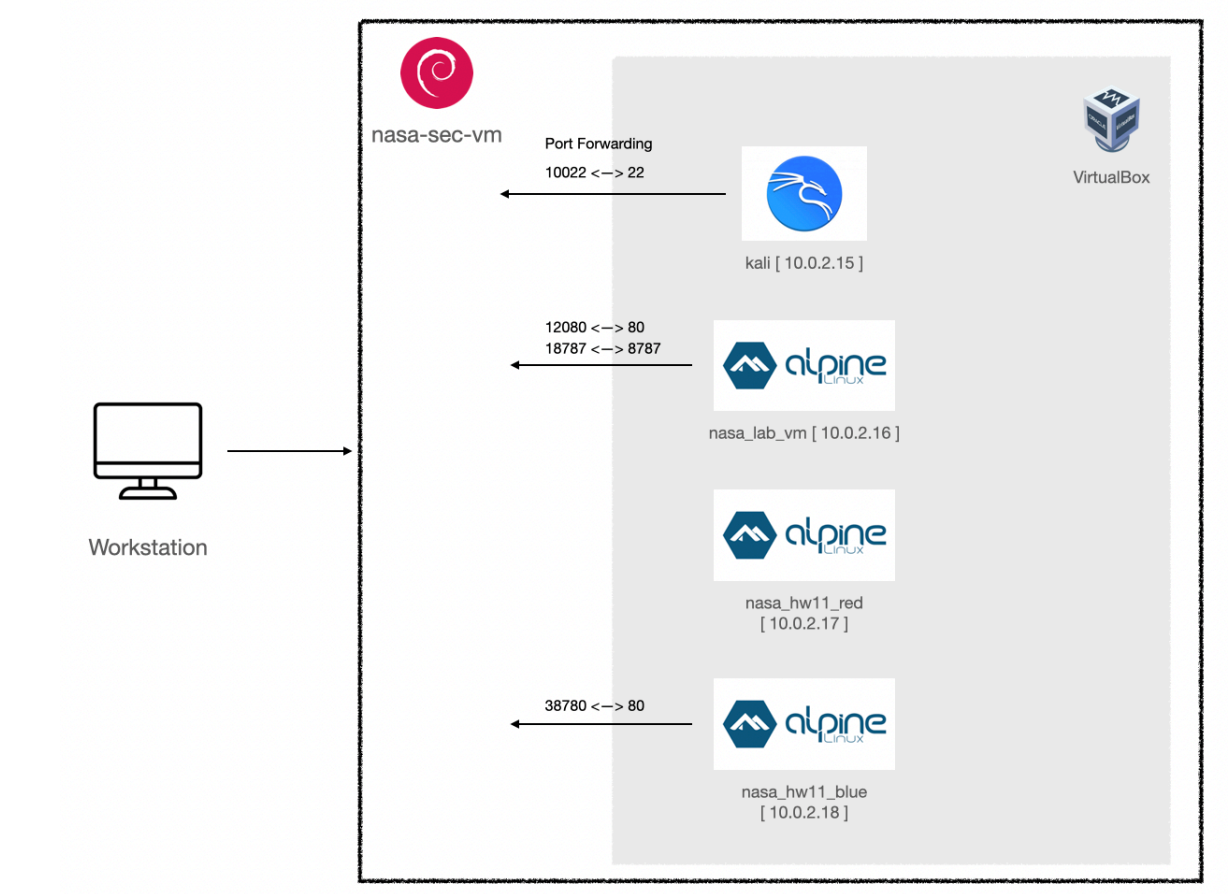
```
b09902078@ws1 [/tmp2/b09902078] virsh list --all
 Id   名稱           狀態
-------------------------
 -    b09902078      關機
 -    nasa-sec-vm    關機
```

接下來請執行 `virsh start nasa-sec-vm` 來開啟這台虛擬機。接著你可以透過任何 VNC client，並透過指令 `virsh vncdisplay nasa-sec-vm` 得到 vnc port，並連結至該機器。輸入之前所顯示的 VNC 密碼（若忘記密碼可以在 `/tmp2/< 你的學號 >/nasahw12/nasa-sec-vm.xml` 找到你的 VNC 密碼），你會看到 Debian 的畫面。該 Debian 機器會有額外的 4 個 nested 虛擬機分別為：

- kali → 我們主要會使用的機器
- nasa_lab_vm → Lab 會使用的機器
- nasa_hw11_red → Red Team 題目所使用的機器
- nasa_hw11_blue → Blue Team 題目所使用的機器

該 Debian 的帳密分別為 `nasa2024` 以及 `nasa2024`。登入後，可以在 `/home/nasa2024/` 發現有 4 個分別開啟不同機器的 scripts，且也有 4 個分別關閉不同機器的 scripts，同學可以使用這些 scripts 開啟/關閉機器，就不需要開啟 VirtualBox 來開啟/關閉這些虛擬機。另外，這些 scripts 會以 **headless** 的模式開啟虛擬機，也就是不會有任何畫面，以減少使用資源。**此外也建議同學解題目時只同時開啟最多兩個機器**，即為 kali 以及你要解的題目虛擬機。

以下圖片可以讓同學了解機器之間的關係以及框架：



其中，你可以透過 port forwarding 來直接 `ssh` 進 kali 機器以方便解題。

1. Red Team (50% + Bonus 10%)

你的朋友告訴你他發現 XX 系所所管理的機器似乎疏於管理，且他們完全沒有任何資訊安全意識。基於你是資安高手，你的朋友拜託你幫忙滲透該機器，取得 root 帳號並用之登入，將滲透的過程寫進報告，以便他可以回報給該 XX 系所。該機器為 nasa_hw11_red，你可以執行 `/home/nasa2024/starthw_red.sh` 來開啟該機器。

(a) (10%) 你的朋友給了你 `student` 帳號的 ssh key，並放在了雲端。請利用 `ssh` 登入 `student` 帳號並在家目錄取得 `flag1`。

(b) (15%) 你的朋友告訴你他得知了 `nasa2023` 以及 `nasa2024` 似乎正在做交接，且為了方便交接，他們特地寫了一個服務。請問你可以找到這個服務，並且得到 `nasa2023` 的密碼，用來登入並在家目錄取得 `flag2` 嗎？
Hint: 謠言都來自中間人

(c) (25%) 你的朋友很八卦，他聽說 `nasa2024` 是一個很不注重資安以及貪方便的人，請問你可以利用這點來登入他的帳號並在家目錄取得 `flag3` 嗎？
Hint 1: *nasa2023* 家目錄底下似乎有什麼 ?!
Hint 2: 偷偷給你 *source code*，不要告訴別人喔

(d) (Bonus 5%) 請問你可以在不登入 `root` 的情況下執行 `/root/flag4` 得到 `flag4` 嗎？
Hint 1: *Everything is a file in linux.*
Hint 2: *Reverse Engineering is bad :<*
Hint 3: *GodBolt* 超好用，我希望我不會寫錯它的名字 *https://dogbolt.org*

(e) (Bonus 5%) 登入 `root` 帳號。
Hint 1: 請不要暴力破解密碼，你會破解到天荒地老
Hint 2: 有什麼方法可以不用密碼就登入？

2. Blue Team (50% + Bonus 10%)

你的朋友很急地跑過來跟你說他的機器似乎被駭入了！他得知你是資安高手，且你學過 `nginx` 相關的知識，所以他拜託你幫忙調查該機器哪裡出問題，並抓出攻擊者，以及幫忙修補該機器以便讓他能繼續安全的維持它的服務。他將 root 帳號的 ssh key 放在 kali 機器的 `/home/nasa2024/.ssh/` 中。該機器為 nasa_hw11_blue，你可以執行 `/home/nasa2024/starthw_blue.sh` 來開啟機器。

(a) (7%) 請問該機器有開著什麼服務呢？

(b) (8%) 請問該機器的什麼服務被攻擊？

(c) (5%) 請問攻擊者的 IP 是什麼？

(d) (12%) 請問該服務有什麼漏洞？攻擊者可以如何利用這個漏洞執行任意指令？

(e) (18%) 請問攻擊者對這台機器執行了什麼指令？攻擊者想要做什麼？

(f) (Bonus 5%) 請問你會如何修補該服務的漏洞？請附上修改後的程式碼

(g) (Bonus 5%) 請問你會如何修補該機器，使得攻擊者無法再次攻擊或是對這台機器執行任意指令？
Note: 你的回答必須保證攻擊者無法透過其他方法再次攻擊。以將攻擊者 *IP* 加入黑名單為例子，攻擊者可以簡單的更換 *IP* 繼續攻擊，故此回答無法取得滿分。