

Homework #5

Due Time: 2022/05/21 (Sun.) 22:00

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 zip all the files, including one PDF, and the security folder. Name the zip file “{your_student_id}.zip” and submit it through NTU COOL. The zip file should not contain any other files, and the directory layout should be the same as listed below:

```
{your_student_id}/  
+-- {your_student_id}.pdf  
+-- security/  
+---- {security scripts}  
+---- ...
```

Grading

- NA accounts for 50 points while SA accounts for 50 points. The final score is the sum between them.
- 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 = NA score + SA score + tidiness score.

Security

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。
- Security 的所有題目分數加總是 150 分，但超過 100 分會以 100 分計。你可以斟酌不作答某些題目。
- (*CTF*) 的題目都會有 flag，flag 的格式都是 HW5{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。

1. CIA Triad & Threat Modeling (9 points)

課堂上有提到 CIA 一般用來當作資訊安全的準則，其中三個字母分別為 confidentiality, integrity 和 availability，其實也就是一個「正常的服務」所應具備的要素。

- (1) (3%) 請分別簡述 CIA 所代表的三個性質，並幫每一個性質想一個「如果不滿足可能會造成什麼問題」的例子。

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。

例題

- 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 (2 points per problem)

- (2)
 - system: 個人筆電
 - security requirement: 沒有被擁有者允許的人不能使用
- (3)
 - 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
- (4)
 - 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

2. Web Security (20 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。在本題中，請參考上方連結自行架設一個 OWASP 伺服器（建議用 Heroku 架設以方便保存進度），並完成以下要求。

Note. 你可以在 `/#/score-board` 找到 Scoreboard

- (1) (10%) 拿到 15 分後附上 Scoreboard 截圖（不需附上過程）
- (2) (5%) 從 [OWASP Top Ten 2021](#) 中選擇三個介紹並簡單舉例（e.g. Injection 就是利用某某某來進行攻擊，像是某某某就可能被如此如此進行 injection）
- (3) (5%) 簡單介紹 SSRF 原理

3. Password Crack (25 points)

通常密碼不會以明文儲存，否則硬碟被駭之後，密碼就可以輕易被取出。於是各種資訊系統會先算出明文的 hash 值後儲存在硬碟中。這一題需要大家了解 Linux / Windows 儲存使用者密碼的方式，並且用暴力列舉的方式破解密碼

Hint: [一些常見的密碼](#)

- (1) (4%) 請問在現行 Linux 系統下，會如何儲存使用者密碼？
- (2) (4%) 破解出 Willy 的登入密碼 [Willy Ubuntu.ova](#)
提供解法時，解法不可包含直接分析所提供的 ova 檔，但可以透過此方法獲取靈感
- (3) (4%) 登入 Willy 帳號後找到桌面上的 flag
- (4) (5%) 請問在現行 Windows 系統下，會如何儲存使用者密碼？
- (5) (4%) 破解出 Alice 的登入密碼 [Alice Windows.ova](#)
提供解法時，解法不可包含直接分析所提供的 ova 檔，但可以透過此方法獲取靈感
- (6) (4%) 登入 Alice 帳號後找到桌面上的 flag

4. Proof of Work & DoS (31 points)

Chiffon 學長是一個充滿秘密的人。表面上作為資訊系學生，喜歡乾淨的 code、做甜點跟鴿子肥肥的肚子。一切看似很正常，但他在暗地裡其實是令狗派聞風喪膽的..... 貓。奴。大。將。軍！喜歡乾淨的 code 是因為貓都很愛乾淨，喜歡做甜點是因為想要把狗派們真的都做成派，至於鴿子肥肥的肚子就真的只是鴿子肥肥的肚子。Chiffon 立志要消滅世界上所有的狗派，為此每週一都一定要去愛貓協會吸貓，獲取貓貓之力。同時他也在強力招攬貓派新血，傳說在系館，每到週一晚上就可以聽見他的聲音「要不要..... 和我一起愛貓啊.....」，不少學弟妹也在他循循善誘、威逼利誘、又双叒發進入了愛貓協會。

狗派的 AnJ 為了能夠刺探敵情，只好宣稱自己是被貓派（被迫成為貓派的派），臥底在 Chiffon 學長底下替他做事。然而這種事情怎麼可能瞞過 Chiffon 大將軍的火眼金睛，AnJ 馬上就被看破手腳、被 Chiffon 大將軍發配去勞改。被迫用工作洗淨自己的罪孽，用工作證明自己會改過自新成為一個徹徹底底的貓派。

Note. 這個題目其實是 Chiffon 學長 (@ktpss95112) 前年在 NASA HW5 出的題目，要是跳過不寫的話小心他把你做成派 (X)。

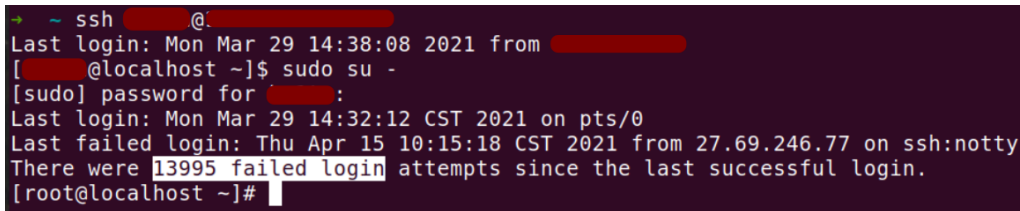
- 本題需要用到的...
 - 檔案：[server.py](#)
 - 連線：`nc linux[x].csie.ntu.edu.tw 6001`
[x] 可填入 7, 8, 9
- 要回答第 (3) 到 (5) 小題，請先讀懂 [server.py](#)。
- 要回答第 (3) 到 (5) 小題，可以參考這份 [example.py](#)。

- (1) (4%) DoS (denial-of-service), DDoS (distributed denial-of-service) 是兩種常被搞混的攻擊手法，請簡述他們是什麼以及他們的差別。
- (2) (4%) PoW (proof of work) 是一種防禦 DDoS attack 的手法。請簡述 PoW 的防禦原理，並簡介另外一種 proof of XXX 的方法。
- (3) (8%) (*CTF*) Chiffon 學長寫了一個 sorting 的服務，想要把狗派們依編號排序，方便他把他們做成派。被發配去勞改的 AnJ 仍在默默抗爭，你能協助他來拖慢這個服務嗎。請用上面提供的資訊連上 server，解決 PoW (md5 hash 問題) 之後，輸入選項 1。請設計適當的 input data 來達到 DoS 的效果。
- (4) (8%) (*CTF*) Chiffon 學長為了在日後進行思想控制，他寫了一個小函數，來挑出任何帶有狗派思想的郵件。被發配去勞改的 AnJ 仍在默默抗爭，你能協助他來拖慢這個服務嗎。請用上面提供的資訊連上 server，解決 PoW (md5 hash 問題) 之後，輸入選項 2。請設計適當的郵件，來達到 DoS 的效果。(hint: what is ReDoS?)
- (5) (7%) (*CTF*) AnJ 的小把戲全部都被 Chiffon 學長看在眼裡，他決定加大 AnJ 的工作量，讓他用更多的工作證明自己。善良的你於心不忍，決定替他承擔工作！請用上面提供的資訊連上 server，解決 PoW (md5 hash 問題) 之後，輸入選項 3。請快速地解決 10 份 PoW，並將 server 給你的證明寫在作業 report 當中。

hint: Chiffon：喜歡做甜點其實不是要把狗派做成派，是因為要幫全世界的狗做巧克力蛋糕。

5. Linux Q&A (20 points)

- (1) (5%) 承 3.(1) 題，在仔細研究 `/etc/shadow` 這個檔案之後，你會發現只有 `root` 有權限進行讀寫，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？
- (2) (5%) 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 ≥ 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。



```
➤ ~ ssh [redacted]@[redacted]
Last login: Mon Mar 29 14:38:08 2021 from [redacted]
[redacted@localhost ~]$ sudo su -
[sudo] password for [redacted]:
Last login: Mon Mar 29 14:32:12 CST 2021 on pts/0
Last failed login: Thu Apr 15 10:15:18 CST 2021 from 27.69.246.77 on ssh:notty
There were 13995 failed login attempts since the last successful login.
[root@localhost ~]#
```

Figure 1: 很多人來敲門

- (3) (5%) 承上題，請問我們可以如何防範密碼被多次 `ssh` 暴力破解，請舉出 3 種方式
- (4) (5%) 在一台 `Linux` 電腦上，存在著非常多我們從來就不知道的使用者，不信的話連上工作站執行 `cat /etc/passwd` 就可以看到了。例如說 `http` 這個使用者，就是用來處理跟網頁伺服器有關的工作；`systemd-network` 這個使用者，就是用來處理跟電腦網路有關的工作。請說明為什麼這些工作需要額外創建專門的使用者來處理，並舉出如果全部都用 `root` 使用者來執行的話會有什麼安全問題。

6. TLS (30 points)

AnJ 很喜歡三個字的東西，像是 `CIA`、`PoW`、`CTF`、`DSA`、`ADA`、`CNS`、`APO`..... 其中他最喜歡 `TLS` 了，因為 `TLS` 就是 `Three Letter Sequences` 的縮寫，代表了他喜歡的這些三個字序列。於是他決定來傳教，讓你知道 `TLS` 的美好！

- (1) (5%) 你知道 `TLS` 的憑證是什麼嗎？請簡述一個 `TLS` 的 `certificate` 裡會有什麼內容跟什麼是 `CA`(certificate authority)。
- (2) (7%) (*CTF*) AnJ 架了一個網站，並且自己幫它產生了一個憑證。大家都知道 `http` 是赤裸裸的協定，但這是 `https` 欸！肯定是按下去「進階 > 知道風險並繼續」啊～就算他的 `server key` 掉在 這裡 應該也沒有關係吧？這是他連上自家網站的 紀錄，聰明的你登的進去嗎？
- (3) (10%) (*CTF*) AnJ 發現自己太大意了，他又架了一個網站，而且這次他有好好的把自己 `server` 的 `private key` 收起來。這樣總可以了吧！這是他連上自家網站的 紀錄，聰明的你登的進去嗎？(hint: 這個 `public key` 看起來不行喔..... `p` 跟 `q` 看起來太接近了.....)
- (4) (8%) AnJ 死不認錯，他覺得上面那個只是他又太大意了，如果他產生一個足夠強的 `key`，並且好好保管，就算沒有給 `CA` 簽憑證，也不會讓你們有機可趁！但事實真的是這樣嗎？請敘述一下，在 `server key` 足夠強的情況下（`private key` 無法從 `public key` 解出來）的情況下，`self-signed certificate` 還會遇到怎麼樣的問題（可以舉出一些實際的攻擊手法）？

7. Steganography (15 points)

doge 很害羞，所以只能把他想說的話藏在自拍照裡面，但是藏的過程太麻煩了，於是 doge 寫了一個 python 程式來隱匿秘密。你能發現 doge 的小祕密嗎？

- doge 使用的 python 程式 [hide.py](#)
- doge 的秘密自拍照 [informative_doge.png](#)

- (1) (7%) 請觀察 doge 使用的 python 程式，解釋 doge 如何將秘密藏在自拍照中
- (2) (8%) 寫一個 python 程式來解出秘密，並且取得 flag

NFS & Fix VM

Fix VM

- 在 Init 和 Authorized? 這兩題，請詳細寫下你解決問題的步驟。
- Pacman 這題沒有對應的 VM image，所以請盡可能詳細的寫下你認為發生問題的地方是什麼，還有你是怎麼得到這樣的結論的。也可以附上參考資料（例如你搜尋到類似的錯誤訊息）或自己嘗試復現這些錯誤。
- 請不要重新安裝 Arch Linux，如果不確定自己想做的事情算不算重新安裝，歡迎來信詢問。

Init (10 points)

NASA 助教 titusjgr 第一次安裝 Arch Linux，但是他不小心漏掉了一些步驟，導致拔掉 ISO 之後就沒辦法開機了。請你幫忙 titusjgr 修好他的 VM，讓他能夠正常開機。

- 下載 VM：
 - CSIE Workstation: linux1[1-5].csie.ntu.edu.tw 的 /tmp2/nasa-hw5-fixvm
 - Google Drive: https://drive.google.com/file/d/1gCULAbEa7Gfon6h8Z8doXUHapSHkp2XL/view?usp=share_link
 - b2sum:
c7b8383e0f8b8b136f755f3b6da98206b40c6608d07c1e8d609ad66e
6f8838f837a0922b1b7996c171e9a2fc6ad966cf39bdef10284a1417
3cd7fd355126dac9
- root 使用者的密碼：root

如果你使用工作站的 qemu 可以使用以下的指令開啟 VM：

```
$ qemu-system-x86_64 -enable-kvm -m 2048\  
-bios /usr/share/ovmf/x64/OVMF.fd\  
-hda hda.qcow2 -hdb hdb.qcow2\  
-vnc :[port number],password=on -monitor stdio
```

並使用 VNC 來連線。建議使用 snapshot 節省備份空間，例如：

```
$ qemu-img create -b hda.qcow2 -F qcow2 -f qcow2 recover-hda.qcow2
```

Authorized? (7 points)

順利開機之後，titusjgr 發現他雖然有把他的 ssh private key 對應的 public key 傳給 VM 了，但是用 ssh 連線時卻還是需要輸入密碼。請找出問題，讓 titusjgr 可以不用輸入密碼就用 ssh 登入 VM，並附上在 VM 中輸入以下指令並成功登入的截圖。

```
# ssh root@localhost
```

本題只要求在 guest VM 中使用 ssh key 登入 localhost 可以不用輸入密碼，你不需要設定 NAT 或讓 host 可以連到 guest VM。不過如果你想使用 NAT 的話，可以使用以下的指令並連到 host 的 port number 2。


```
$ qemu-system-x86_64 -enable-kvm -m 2048\  
-bios /usr/share/ovmf/x64/OVMF.fd\  
-hda hda.qcow2 -hdb hdb.qcow2\  
-vnc :[port number 1],password=on -monitor stdio  
-nic user,hostfwd=tcp::[port number 2]-:22
```

Pacman (8 points)

1. (4 points) titusjgr 在用

```
# pacman -Sy openssh
```

更新 ssh 之後，想要連上他的工作站來寫 HW5 Fix VM 的前兩題，但是卻出現了以下的錯誤：

```
# ssh titusjgr@oasis1  
ssh: error while loading shared libraries:  
libcrypto.so.3: cannot open shared object file:  
No such file or directory
```

請指出這個問題的原因，並提出修復的方法。

2. (4 points) titusjgr 還是比較熟悉 VirtualBox，於是他在他的全新的 Arch Linux 上用以下的指令安裝了 VirtualBox：

```
# pacman -S virtualbox virtualbox-host-modules-arch
```

但是啟動卻失敗了，而且出現以下的警告：

```
# VirtualBox  
WARNING: The vbox drv kernel module is not loaded.  
Either there is no module available for the  
current kernel (6.2.8-arch1-1) or it failed to  
load. Please recompile the kernel module and  
install it by  
  
sudo /sbin/vboxconfig  
  
You will not be able to start VMs until this  
problem is fixed.
```

請解釋這個警告出現的原因，並說明應該做什麼才能讓 VirtualBox 正常啟動。

NFS

這題需要同學們實作 NFS server & client，請詳細寫下每一個步驟，可用截圖輔助。
請使用提供的兩台 VM，server-nasahw5 及 client-nasahw5，相關資訊如下：

- server-nasahw5: NFS server
 - CSIE Workstation:
linux1[1-5].csie.ntu.edu.tw 的 /tmp2/nasa-hw5-nfs/nasahw5-server.ova

- Google Drive: [nasahw5-server.ova](#)
- SHA256 checksum:
c04b0f5873b691ae7a8ac9cd720d883b9f375fc2d296aee0b5b579595bf06c0e
- 對內網卡 ip: 192.168.30.1
- client-nasahw5: NFS client
 - CSIE Workstation:
linux1[1-5].csie.ntu.edu.tw 的 /tmp2/nasa-hw5-nfs/nasahw5-client.ova
 - Google Drive: [nasahw5-client.ova](#)
 - SHA256 checksum:
ad9d6aa17e223f502577daab3eecd7be21d37116b3aaaefb906a8891c0f6770
 - 對內網卡 ip: 192.168.30.2

兩台 VM 中都已建好兩個 user : nasahw5 (有 sudo 權限) 和 alice , password 皆為 nasa2023 。無特別指定時可用 nasahw5 這個 user 進行操作。

Mount-ain't hard! (5 points)

- server 中的 /mnt/share 為共享的目錄，請設定讓 client 中的 /mnt/share 能夠開機自動掛載到 server 的 /mnt/share 。
- 請在 client 端對 /mnt/share 做任一操作 (e.g. 創建一個檔案)，檢查 server 端是否有相對應的結果，並附上截圖。

Not a Fair System. (14 points)

1. (1 point) 請在 server 中創建 /mnt/share/alice，限制除了 alice 外的使用者不能存取 (i.e. 不能對這個目錄進行任何操作)。
2. (2 point) 在 server 和 client 中新增一個 user 名為 bob，password 為 nasa2023。以 bob 身分登入後，確認他不能存取 alice 的目錄。
關於新增 user 有幾個限制:
 - 因為 alice 沒有 sudo 權限，為求公平 bob 也不能有
 - 請勿刪除任何已存在的 user
3. (0 point) 如 1.，在 server 中創建 /mnt/share/bob，限制除了 bob 外的使用者不能存取。
4. (1 point) 在 client 中以 bob 身分登入，試著存取 /mnt/share/bob，附上截圖。
5. (10 points) bob 表示怎麼可以這樣，果然世界是不公平的...QQQ...
 - (3 points) 如果你發現 bob 在步驟 4. 沒有權限，請說明可能的原因。反之，請說明什麼情況下 bob 可能沒有權限。
 - (5 points) 呈上，說明你如何修正這個問題。
 - (2 points) 附上以下三張截圖:
 - 以 bob 的身分在 /mnt/share/bob 中新增一個檔案
 - 在 server 端 `cat /etc/passwd | grep bob`
 - 在 client 端 `cat /etc/passwd | grep bob`

Now You See Me. (6 points)

1. (3 points) 經過前面的設置，alice 和 bob 現在無法存取對方的目錄，BUT！這個讓人又愛又恨的 BUT，Leterrier 偷偷告訴 bob，他其實能在 alice 更改檔案的時候... 讓一切公平 (?) 一點...
 - 在 server 端登入 bob，打開 Wireshark，開始監聽 NFS 封包。
 - 在 client 端登入 alice，並對 /mnt/share/alice 目錄下的檔案做修改。此時 Wireshark 應會收到含有 alice 修改內容的封包，請附上截圖。
2. (3 points) 寫到這邊同學們應該了解，本題 NFS 架構還有很多不完善的地方，無法直接套用在現實生活中。針對前面 Wireshark 的監聽，請提出一個防禦方法。

Leterrier 其實還想請同學們實作加密，BUT bob 想繼續偷看 alice 的檔案... :D