Network Administration/System Administration Homework #12

B10202012 劉仲楷

1 Linux 大小事

ref: Linux man page、askubuntu: How do I keep track of failed SSH log-in attempts?

1. 存在 `/etc/shadow`，打開可以看到類似 `username:$6$saltvalue$hashedpassword:...`，其中 6 代表用 SHA-512 hash。
2. 因為 passwd 程式是 setuid root，透過 `ls -l /usr/bin/passwd`，就可以看到 `-rwsr-xr-x 1 root root ...`
3. 這些登入嘗試被存放再 `/var/log/auth.log`，例如
   `2025-12-08T14:19:19.139769+00:00 nfs-server sshd[844]: Failed password for invalid user from 10.0.2.2 port 34568 ssh2`
   檔案會存放 timestamp、server name、驗證失敗訊息、src IP、port 等等。
4. - 監控 `/var/log/auth.log`，若偵測同一 IP 多次登入失敗，就封鎖一段時間，累進制。如果忘記密碼導致永久封鎖，則需要 admin 手動解鎖，重設密碼。
   - 不要使用密碼認證，改用 public key。剛開始需要先塞 public key 進 server。Disable 密碼後，就都用 public key authentication 登入。

2 畫中有話

1. 程式將要寫的訊息轉成二進位，一次處理三個 pixels 的三個 channels，將 8 bits（1 byte）的資料放入。放入的方法是將一個 pixel channel 的最後一個 bit 轉換奇偶數。如果要放入的 bit 是 1 就放奇數，0 就放偶數。由於只有 8 個 bit，所以第三個 pixel 的第三個 channel 不會用到。利用微小肉眼不易察覺的改變，將訊息隱寫入圖片。
2. `HW12{S4KiCh4n_sakiCHAN_S4k1ChaN}`
   如上所說，所以只要依序判斷各 pixel channel 的奇偶數，就能還原回訊息。詳細見 `code/P2.py`。

3 Alya Judge

1. `HW12{r3MeM8eR_To_s3t_S7RONg_PAS5WOrds}`
   用 `http://140.112.187.51:45588/submissions/..%2faccounts/accounts` 可以看到 hash 後的密碼，再利用 wordlist brute force 出密碼即可。密碼是 mortis00。詳細見 `code/P3_a.py`。

2. `HW12{8rok3N_PrO8LeM}`
   `special_judge` 做的就是比對最長 substring，越長則回傳分數越高。且只要直接連線到 `http://140.112.187.51:45588/submit/3` 沒擋也沒限次數，所以就能作為一個 oracle，一直依序猜，直到分數變高，再猜下一個 byte。此外 flag 有限制字元共 $d = 63$，我們只要猜到 accept 即可。本來 brute force 複雜度是 $O(d^n)$，有了 oracle 後變成 $O(nd)$，n 是 flag 長度。詳細見 `code/P3_b.py`。

3. `HW12{i_l1KE_a15CR3am_MoRE_7H4n_Co0Ki3s}`
   直接從公佈的 `app.py` 找到明文 secret key `A_super_SecUrE_$eCR37_keY`。再利用 `flask.sessions.SecureCookieSessionInterface` 偽造一個假的 cookie，接在連線到 `http://127.0.0.1:45588/submissions/admin` 時一起送去。詳細見 `code/P3_c.py`

4 Introduction to gnireenignE esreveR

1. `HW12{hW0_8UT_WiTH_r3V3Rse_eN91NE3rinG}`
   將 exe 檔上傳至 Dogbolt。觀察 Hex-Rays decompiler，找到 key、pattern，發現 flag 是 key xor pattern，因此直接還原即可。詳細見 `code/P4.c`。