

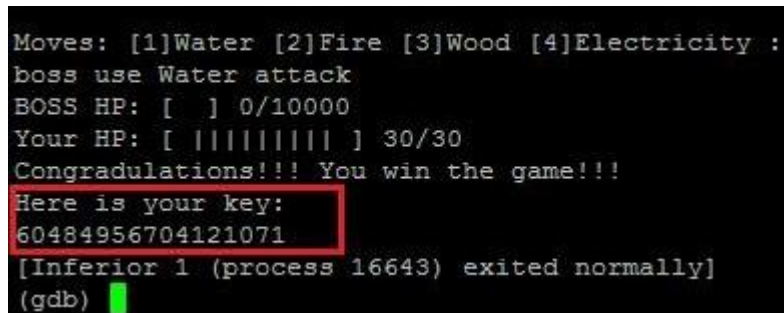
Network Security Project 2-2 Report

Q. If you are the game downloader, how will you verify certificates?

A. 確認 certificate 裡的 issuer，並取得該 issuer 的 public key，對 certificate 上的簽名做驗證。

Q. Your key in the game

A. 60484956704121071



```
Moves: [1]Water [2]Fire [3]Wood [4]Electricity :
boss use Water attack
BOSS HP: [ ] 0/10000
Your HP: [ ||||| ] 30/30
Congradulations!!! You win the game!!!
Here is your key:
60484956704121071
[Inferior 1 (process 16643) exited normally]
(gdb)
```

Q. The logic error:

A. 製造亂數使用的 seed 太容易被找出來。要防止被預測行動應該用 server 回傳亂數。

Q. The way that you defeat the boss

A. 首先用 GDB 開啟遊戲，並把 breakpoint 設在 srand 函數的地方，進入遊戲輸完 ID 之後在第一回合前會呼叫一次 srand，也就是 breakpoint。在這邊用 info all-register 把所有的 register 值印出來，確認\$eax 的值，也就是 srand 函數裏頭的參數，也就是這一局遊戲的 seed。接著開啟另外寫的 rand_peeker(code 也有附在 zip 裡)，把 seed 代入 srand，算出一千次 rand 出來的結果，用跟 boss_next_move 函式中操作 rand()回傳的值同樣的方式操作這一千次 rand 出來的結果，並且根據遊戲相剋的關係印出連續一千個相剋的魔法代號(這部分必須同樣在 linux 系統上執行，不然算出來的 rand 值會不一樣)。把這一千個數字直接複製，回到遊戲繼續用 continue 進行遊戲，把一千個數字直接貼上輸入，就可以打贏 Boss 了。

要執行 Part(1)，只需要在可以執行 python 的環境下輸入 python A022029.py 就可以了。