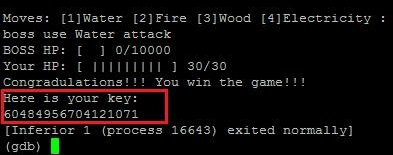
Network Security Project 2-2 Report

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



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\_peeper(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。