

硬體安全導論 – Fall 2019

Lab01 Exercise HW1

Homework Description :

在Lab01的 password example當中，破解密碼。藉由capture software當中的 set_cwlite_password.py (名字以software 裡的為主 這裡是示意)，此script直接執行的話會破解出aaaaa的密碼，並不是真正的密碼 h0px3。需更改script中的參數與程式碼達到真正的破解效果，此次homework請更改script且破解出正確密碼。

Inputs

1. Lab01 裡的設定包括包含 h0px3 的 password firmware
2. set_cwlite_password.py (名字以 software 裡的為主 這裡是示意)

Outputs

1. 利用 set_cwlite_password.py (名字以 software 裡的為主 這裡是示意)破解出 Lab01 的密碼
2. 撰寫簡易的 report 說明調整了 script 裡的那些參數與程式碼。

Grading Policy

function correct 50%
Report 50%

Note

1. Lab01 Document https://hackmd.io/s/SJHfXGJT702_SYN/
2. Lab00 Document <https://hackmd.io/s/S1EEanA2X>
3. 目前最新版本為 ChipWhisperer 4.0.1 (有 vim 可以用)
<https://github.com/newaetech/chipwhisperer/releases/tag/v4.0.1?fbclid=IwAR0vqTAI7Vz-Q6y7pJIvf1d1VucCwHcEZLJdd-TXcg7lZiyG6M-VP2qiEo4>
這本版本內的 預設 chipwhisper 路徑為 Desktop 內記得要 git pull，其他的相對路徑皆保持不變。(所以路徑會跟投影片內的路徑不一樣)