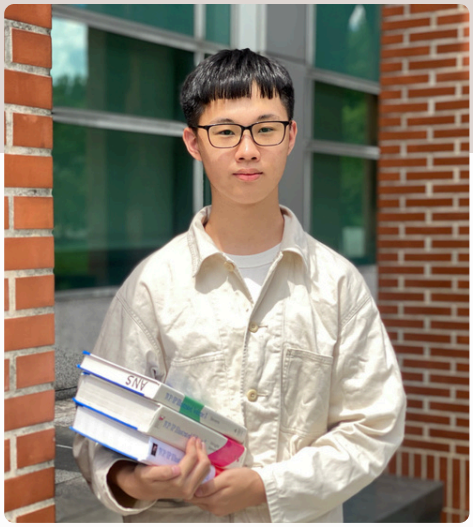


林宥熙(Raymond)

業餘漏洞研究員
kernel / 底層開發 愛好者

聯絡方式

linraymond2006@gmail.com
linraymond2006
新北市私立南山高中

核心技能

- C99
- x86 組合語言
- 逆向工程 / Ghidra 框架
- 漏洞挖掘 / 利用程式開發

漏洞回報

CVSS 6.5 CVE-2024-6044
CVSS 8.8 CVE-2024-6045 RCE
CVSS 9.8 CVE-2024-45694 RCE
CVSS 9.8 CVE-2024-45695 RCE
CVSS 8.8 CVE-2024-45696 RCE
CVSS 9.8 CVE-2024-45697 RCE
CVSS 8.8 CVE-2024-45698 RCE
中度風險 ZD-2024-00904

專案列表

- 實作 x86 MBR bootloader
- 摸索 x86 kernel

證照和檢定

- Certified Network Defender
- IELTS Academic Bandscore 6（CEFR B2）
- TOEIC 金色證書（925 / 990）

簡介

我是來自南山高中的林宥熙，是一位業餘的漏洞研究員。除了投入真實世界的漏洞研究，我也積極參與開源專案，貢獻軟體安全的知識，協助修復專案中安全相關的問題。

資安領域之外，我還是一名正在探索 kernel 和底層開發的學生，對作業系統的充滿興趣，摸索過 kernel 開發，並成功實作了一個開機程式。

我期望能成為一位有扎實學理背景的軟體工程師和專業漏洞研究員，投入資訊產業和社群發揮所學。因此我希望能夠進入資訊工程系學習。

活動經歷

- **AIS3 2022 最佳專題獎**
- **AIS3 EOF 2024 Finals #8**
- **MyFirst CTF 2022 #15**
- **台灣好厲駭第七屆（2022）結訓**
- **台灣好厲駭第八屆（2023）結訓**
- **台灣好厲駭第九屆（2024）學員**
- **NHNC CTF 2024 出題者**
- AIS3 EOF 2021、2022
- AIS3 Junior 第 1~3 屆（2022 ~ 2024）
- HITCON CMT 台灣駭客年會 2024

校內經歷和服務經驗

- 高中 1~3 年級 數理資優班
- 200 小時以上服務時數
- 多元選修：C語言 / TQC C+ 認證

技能組

- 可實際運用 / 持續精進中
- 有基本概念 / 正在學習
- 開始學習 / 正在探索
- 個人特質 / 軟實力

經驗 / 特質 / 軟技能

- 自學能力 / 耐挫力
- 技術文件閱讀能力
- 駭客道德 / 正面價值觀
- 學習動機 / 好奇心 / 求知慾
- 追根究底的精神
- 團隊協作能力

系統軟體 / kernel 開發 相關

- C99
- x86 家族組合語言
- Linux kernel 知識

資訊安全 / 軟體安全 相關

- 逆向工程 / Ghidra 框架
- binary exploiation（x86 / Arm / MIPS）
- 自動化 exploit 撰寫
- security code review
- 韌體分析

其他

- 密碼學
- 密碼學：數學原理
- TCP/IP 協定組

目錄

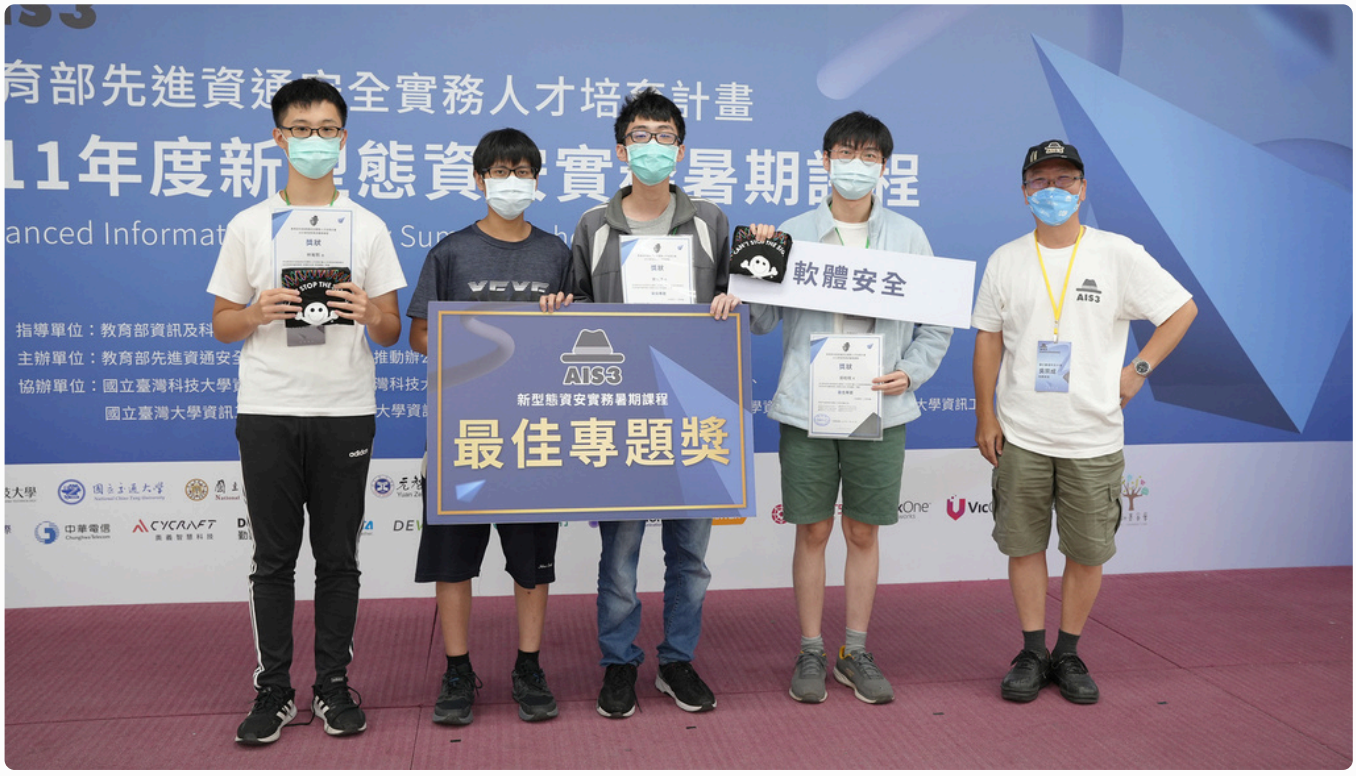
其他有利審查資料

AIS3 2022 最佳專題

透過 MyFirstCTF 的名次取得了進入為期七天的 AIS3 暑期營隊的資格。透過營隊的活動內容，我了解自己技術能力及未來努力的方向。

我們最後決定挖掘無線路由器的漏洞。在分組專題中，我擔任輔助角色，負責尋找目標、拆開韌體、架設模擬環境以降低組員的工作量。我們找到二個 buffer overflow 和 broken access control 漏洞，不僅獲得最佳專題獎，也讓我培養了團隊合作的能力。

我的習慣是每一次參加活動後都會把需要加強的主題紀錄起來，並且回家買書自我精進（或補救），回家後我繼續學習 binary exploitation，並且持續加快逆向工程的速度和準確度，目前我已經能夠自己進行 IoT 設備的漏洞挖掘，確實的見證了自己的成長和進步。



宗成教授（右一）在 AIS3 2022 向我的組員和我（左一）頒發最佳專題獎。

AIS3 2022：最佳專題獎

教育部先進資通安全實務人才培育計畫
AIS3新型態資安暑期課程

獎狀

林宥熙 君

參加教育部先進資通安全實務人才培育計畫111年度產業專題導向
新型態資安暑期課程 軟體安全組 表現優異，榮獲

最佳專題

特頒獎狀，以資鼓勵。

教育部先進資通安全實務人才培育計畫辦公室

吳宗成 Tzong-Chen Wu　鄭欣明 Shin-Ming Cheng
黃俊穎 Chun-Ying Huang　王銘宏 Ming-Hung Wang
蕭旭君 Hsu-Chun Hsiao　陳昱圻 Yu-Chi Chen

教育部 推動辦公室 先進資通安全實務人才培育計畫

中華民國 111 年 7 月 31 日

ISIP-AIS3 2022-獎-008

最佳專題獎

AIS3 2022：合格證明書

教育部先進資通安全實務人才培育計畫
AIS3新型態資安暑期課程

合格證明

林宥熙 君

111年7月25日至7月31日參加 教育部先進資通安全實務人才培育計畫
111年度產業專題導向新型態資安暑期線上課程共計40小時，
修習成績及格，特頒此證書。

教育部先進資通安全實務人才培育計畫辦公室

吳宗成 Tzong-Chen Wu　鄭欣明 Shin-Ming Cheng
黃俊穎 Chun-Ying Huang　王銘宏 Ming-Hung Wang
蕭旭君 Hsu-Chun Hsiao　陳昱圻 Yu-Chi Chen

教育部 推動辦公室 先進資通安全實務人才培育計畫

中華民國 111 年 7 月 31 日

ISIP-AIS3 2022-合-080

合格證明書

EOF 2024

經過三年後，我終於進入了 2024 年的 AIS3 EOF 的決賽。在決賽中，我負責 binary exploitation 和逆向工程相關題目，可惜在第一天晚上在被賽所以完全沒有睡覺，導致第二天表現失常，結果不盡人意。

我在這一次的比賽後深刻反省為什麼三年過去了，看到的攻擊面卻這麼少？我得到的結論是解題式的 CTF 比賽限制了想像，讓很類似真實世界的漏洞在眼前卻無法識別出來。

我在這一次的比賽後開始投入真實世界漏洞的研究，從今年初至現在，已經累積回報了 7 個 CVE，讓我知道那時候選擇的方向是正確的，而且正在那一條正確的道路上持續前進。

我（左一）與隊友們在 2024 年度 AIS3 EOF 決賽後合影

AIS3 EOF 2024：參加證明

教育部先進資通安全實務人才培育計畫
112年度 AIS3 EOF 進階資安攻防演練

參賽證明

UN1C0D3 H45H 隊，林宥熙 君

於113年2月3-4日參加 教育部先進資通安全實務人才培育計畫
112年度 AIS3 EOF 進階資安攻防演練，特頒此證書。

教育部先進資通安全實務人才培育計畫辦公室

吳宗成 Tzong-Chen Wu　　鄧惟中 Wei-Chung Teng
黃俊穎 Chun-Ying Huang　　王銘宏 Ming-Hung Wang
蕭旭君 Hsu-Chun Hsiao　　陳昱圻 Yu-Chi Chen

中華民國 113 年 2 月 4 日

ISIP-EOF 2024-參賽-067

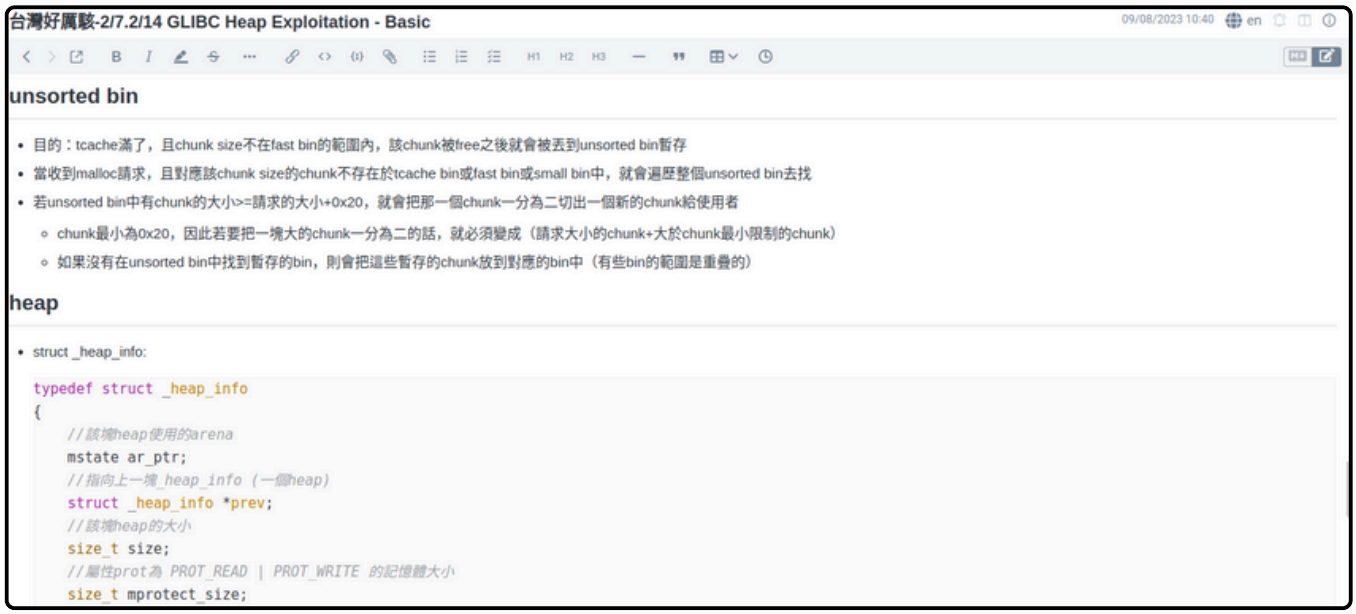
決賽參賽證明

台灣好厲駭

我在 AIS3 2022 之外還參加了三屆的台灣好厲駭。其中影響我最大的是好厲駭的培訓，在培訓中有各式的主題的講座和課程，這些課程除了學到了各種攻擊、防禦和管理技術外，也點明了之後學習的方向。而且每個學年都會有自評表填寫，也提供了追蹤自己變化的機會。

另外，我在這些課程中也看到了許多比我優秀的同齡人和學長，透過不斷的提高自己看到的上限，讓我可以訂定出更明確的目標。

我（前排左二）和「資安治理成熟度」講座參加者的大合照



GLibC heap heap exploitation 專題課程的筆記

台灣好厲駭

第七屆結訓證書

台灣好厲駭

第八屆結訓證書

NHNC CTF 出題經驗

題目原始碼

今年九月底在特殊選才群組認識許多資安同好，同時也被邀請加入了 ICEDTEA CTF 戰隊，那時戰隊正好在規劃一個名為 No Hack No CTF 的新手向比賽，我因此參加了出題的行列。

其中，我負責出逆向工程和 binary exploitation 題目（各 4 題），我認為比起一般 binary exploitation 題目，我更想向新手介紹一些不安全的程式範例。因此我用多種 C 語言函式庫的特性出題（例如：沒有檢查 malloc 回傳值導致的陣列界外寫、scanf matching failure 配合 CVE-2018-18778 的概念等）。

儘管比賽中出現了一些混亂情況，例如：題目出錯、flag 和解法外洩，以及因來自印度的 DDoS 攻擊導致服務中斷，但這次經歷所累積的寶貴經驗，是其他地方無法學到的。如果不是 ICEDTEA 戰隊的同學給予我這次出題的機會，我無法向社群中那些優秀的同齡人交流。

NHNC CTF 比賽平台，共計 287 人參加

AIS3 Junior

AIS3 Junior 2024 專題

我認為參加 AIS3 Junior 讓我認識同齡的資訊安全愛好者，也是一個互相切磋交流的好機會。在營隊的最後也都有專題發表，是展現分工合作的時候，也可以觀摩其他組別製作的簡報是否有可以學習之處。

每次參加營隊後，我會列出一張需要補強的清單，例如在 AIS3 Junior 2023 年，製作的專題主題是中間人攻擊，但是由於知識不足沒有辦法完整做出，於是我回家之後研讀了基礎的密碼學（當時看的是 Cryptography and Network Security: Principles and Practice）和 TCP/IP 協定組（當時看的是 TCP/IP Illustrated）等等，才知道當時的想法根本是天馬行空、缺少技術細節的空談。

我（左三）與助教（右二）、隊友們在 AIS3 Junior 2024 合影

AIS3 Junior

教育部先進資通安全實務人才培育計畫
AIS3 Juniors 新型態高中職資安課程

合格證明

林宥熙 君

111年8月23日至8月25日參加 教育部先進資通安全實務人才培育計畫
111年度新型態高中職資安課程共計25小時 ，
修習成績及格 ， 特頒此證書 。

教育部先進資通安全實務人才培育計畫辦公室

吳宗成 Tzong-Chen Wu　　鄭欣明 Shin-Ming Cheng
黃俊穎 Chun-Ying Huang　　王銘宏 Ming-Hung Wang
蕭旭君 Hsu-Chun Hsiao　　陳昱圻 Yu-Chi Chen

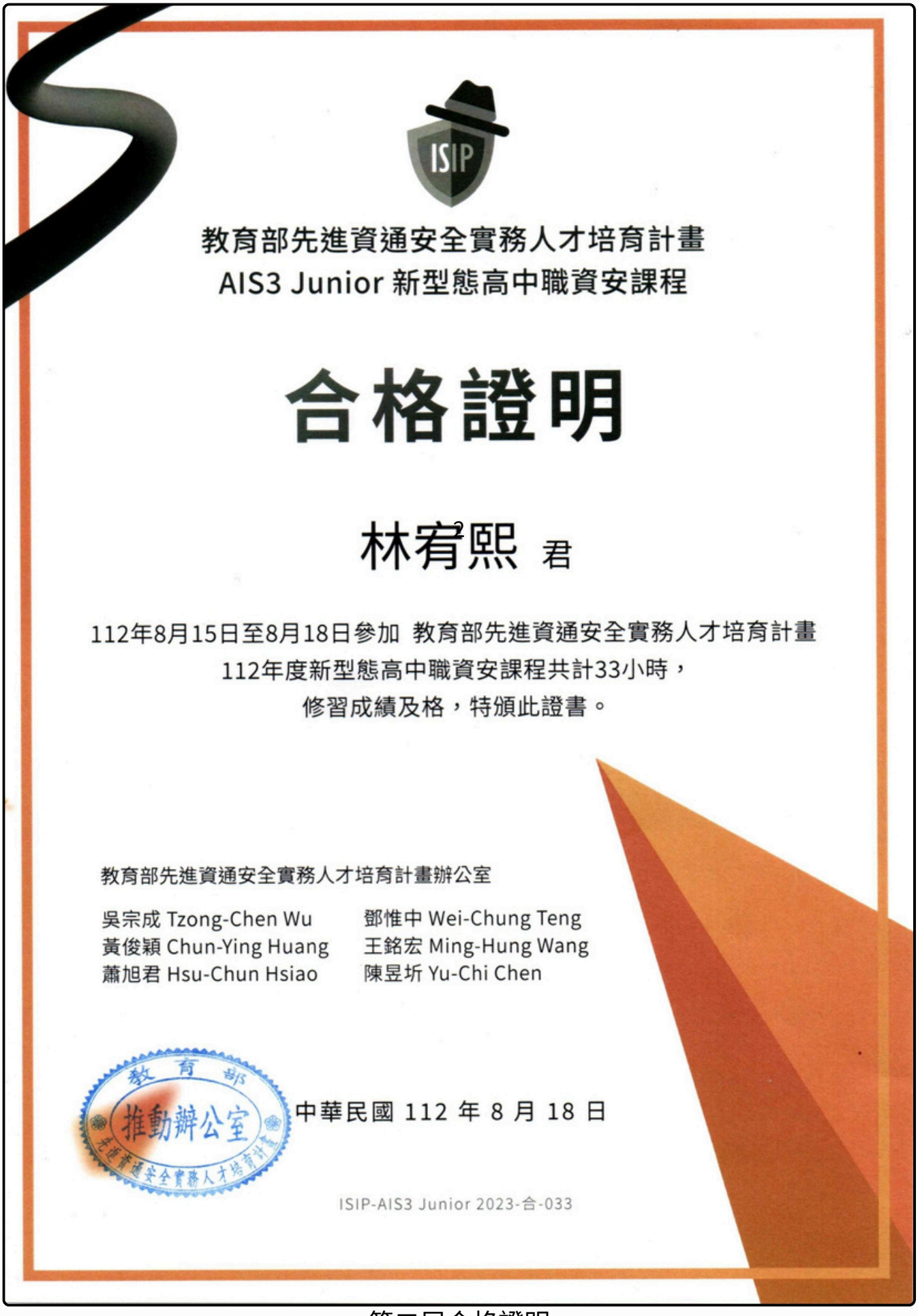
教育部 推動辦公室 先進資通安全實務人才培育計畫

中華民國 111 年 8 月 25 日

ISIP-AIS3 Juniors 2022-合-013

第一屆合格證明

AIS3 Junior



教育部先進資通安全實務人才培育計畫
AIS3 Junior 新型態高中職資安課程

合格證明

林宥熙 君

112年8月15日至8月18日參加 教育部先進資通安全實務人才培育計畫
112年度新型態高中職資安課程共計33小時，
修習成績及格，特頒此證書。

教育部先進資通安全實務人才培育計畫辦公室

吳宗成 Tzong-Chen Wu　　鄧惟中 Wei-Chung Teng
黃俊穎 Chun-Ying Huang　　王銘宏 Ming-Hung Wang
蕭旭君 Hsu-Chun Hsiao　　陳昱圻 Yu-Chi Chen

教育部 推動辦公室 先進資通安全實務人才培育計畫

中華民國 112 年 8 月 18 日

ISIP-AIS3 Junior 2023-合-033

第二屆合格證明

AIS3 Junior

教育部先進資通安全實務人才培育計畫
AIS3 Junior 新型態高中職資安課程

合格證明

林宥熙 君

113年8月15日至8月18日參加 教育部先進資通安全實務人才培育計畫
113年度新型態高中職資安課程共計33小時 ，
修習成績及格 ， 特頒此證書 。

教育部先進資通安全實務人才培育計畫辦公室

吳宗成 Tzong-Chen Wu　鄧惟中 Wei-Chung Teng
黃俊穎 Chun-Ying Huang　王銘宏 Ming-Hung Wang
蕭旭君 Hsu-Chun Hsiao　陳昱圻 Yu-Chi Chen

教育部 推動辦公室 先進資通安全實務人才培育計畫

中華民國 113 年 8 月 18 日

ISIP-AIS3 Junior 2024-合-47

第三屆合格證明

漏洞列表：簡述

我回報的漏洞中，有 3 個被歸類為 critical、3 個被歸類為 high、另一個則是 medium（FIRST CVSS 3.1）。除了 CVE-2024-6044 之外全部都是 pre-auth RCE，影響全球所有使用該機型的使用者。

為什麼會開始漏洞挖掘呢？主要因為在 AIS3 EOF 決賽的時候發現自己看到的攻擊面太少，更具體來說，很多顯而易見的漏洞就這樣子在比賽中和我擦身而過，這讓我反省自己的學習方式是否出了問題。

以我熟悉的逆向工程和 binary exploitation 來說，比賽題目範圍相當有限，而且會利用漏洞真的代表找得到漏洞嗎？我的答案是否定的。解題式 CTF 的 pwn 題可能只有幾百行，相對於編譯後有數 MB 的真實世界的程式來說真的很小。

為了挖掘漏洞，我在學校晚自習結束後回家，就馬上開始進行逆向工程。我藉由壓縮睡眠時間來投入漏洞研究、常常持續到凌晨兩、三點。這些不中斷的努力最後讓我成功踏入漏洞研究的領域。

除了技術上的進步，我也學會如何評估漏洞的嚴重性，撰寫完整的報告，並站在廠商的角度提供修補意見。我也遵循負責任的漏洞披露原則，避免在網路上公開發布 exploit 和細節，以免增加終端使用者被利用的風險。

我的研究成果登上 iThome 的資安新聞了！

漏洞列表

CVE-2024-{6044, 6045} 起源

破解 D-Link EAGLE PRO 系列韌體加密機制的故事

漏洞列表

CVE-2024-6044（Arbitrary file read）

path traversal / improper input validation

漏洞列表

CVE-2024-45694 / CVE-2024-45695（RCE）

stack-based buffer overflow

漏洞列表

CVE-2024-45697（RCE）

misconfigured ip6tables rule

漏洞列表

CVE-2024-45698（RCE）

command injection / hidden functionality

CVE-2024-6045 / CVE-2024-45696（RCE）

hard-coded credentials / b4ckd00r

漏洞列表

ZD-2024-00904

zerojudge.tw sandbox escape

Minidlna

Blind SSRF

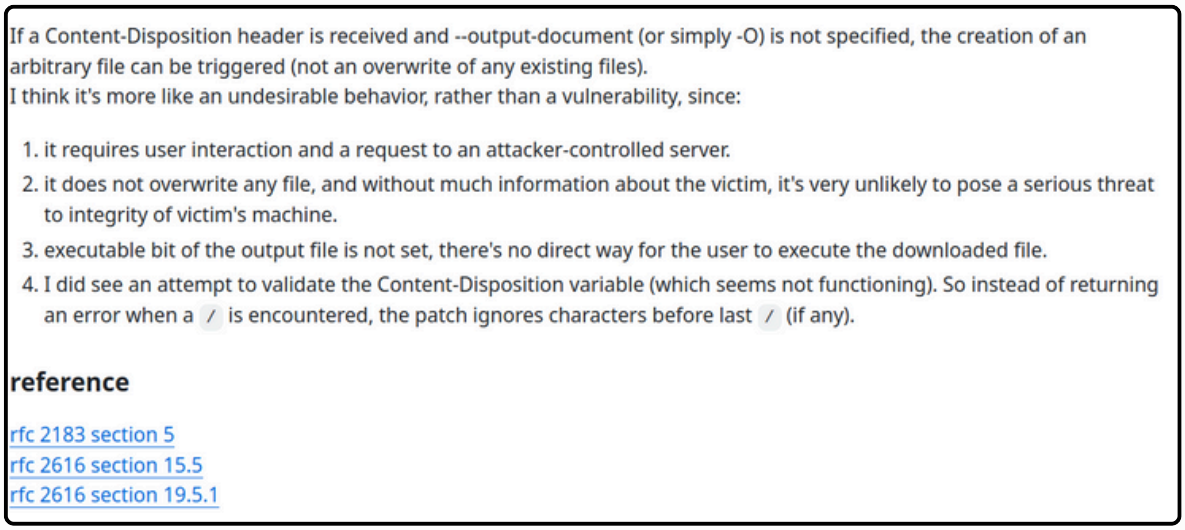
Toybox

pull request #516

path traversal（Arbitrary file creation）

由於簡化路徑的邏輯錯誤，導致用 wget 發送請求時，攻擊者如果傳送惡意的回應，可以建立任意檔案。

因為不是重大安全性問題，所以這一次回報用 pull request 的形式直接提供 patch，我也引用了多個 RFC 來說明不合規於協定的行為。



If a Content-Disposition header is received and --output-document (or simply -O) is not specified, the creation of an arbitrary file can be triggered (not an overwrite of any existing files).
I think it's more like an undesirable behavior, rather than a vulnerability, since:

1. it requires user interaction and a request to an attacker-controlled server.
2. it does not overwrite any file, and without much information about the victim, it's very unlikely to pose a serious threat to integrity of victim's machine.
3. executable bit of the output file is not set, there's no direct way for the user to execute the downloaded file.
4. I did see an attempt to validate the Content-Disposition variable (which seems not functioning). So instead of returning an error when a `/` is encountered, the patch ignores characters before last `/` (if any).

reference

rfc 2183 section 5
rfc 2616 section 15.5
rfc 2616 section 19.5.1

pull request 以攻擊者的角度分析可能的危害，並從開發者的角度提供修補

漏洞挖掘：下一步？

由於 IoT 設備程式碼過於鬆散，因此下一步我將嘗試不同的目標進行漏洞開發，藉由動手做的過程學習，計畫如下：

近期：間歇的 學習-練習-修正 循環

- 學習後練習，練習後學習：知識和經驗可以同時間增加
- 理解更多程式語言：熟悉更多程式語言，可以檢閱的弱點也會更多
- 站在不同角度看攻擊面：站在開發者或攻擊者的角度看攻擊面

近期至中期：嘗試大型開源專案

- 嘗試較大型的開源專案
  - 各種 service daemon（例如：IRC、FTP ...）
  - 日常使用的小工具
- 在學習之餘，也做出實質貢獻

中期：學習 kernel exploitation 技術

- 搭設漏洞復現環境，由已知漏洞學習
- 完成 pwn.college 的 system exploitation 類別
- 了解不同架構的 kernel exploitation

中期：了解各種主流平台利用手法

- 了解 Windows 系統和 API：*Windows via C/C++*, *Windows internals*
- 了解 OS X 系統架構：*Mac OS X internals*

中期至遠期：深入了解駭客文化

- 閱讀各種駭客文學作品，例如：
  - *PoC || GTFO*
  - *Underground: Tales of hacking, madness and obsession on the electronic frontier*
  - *Phrack Magazine*

專案列表

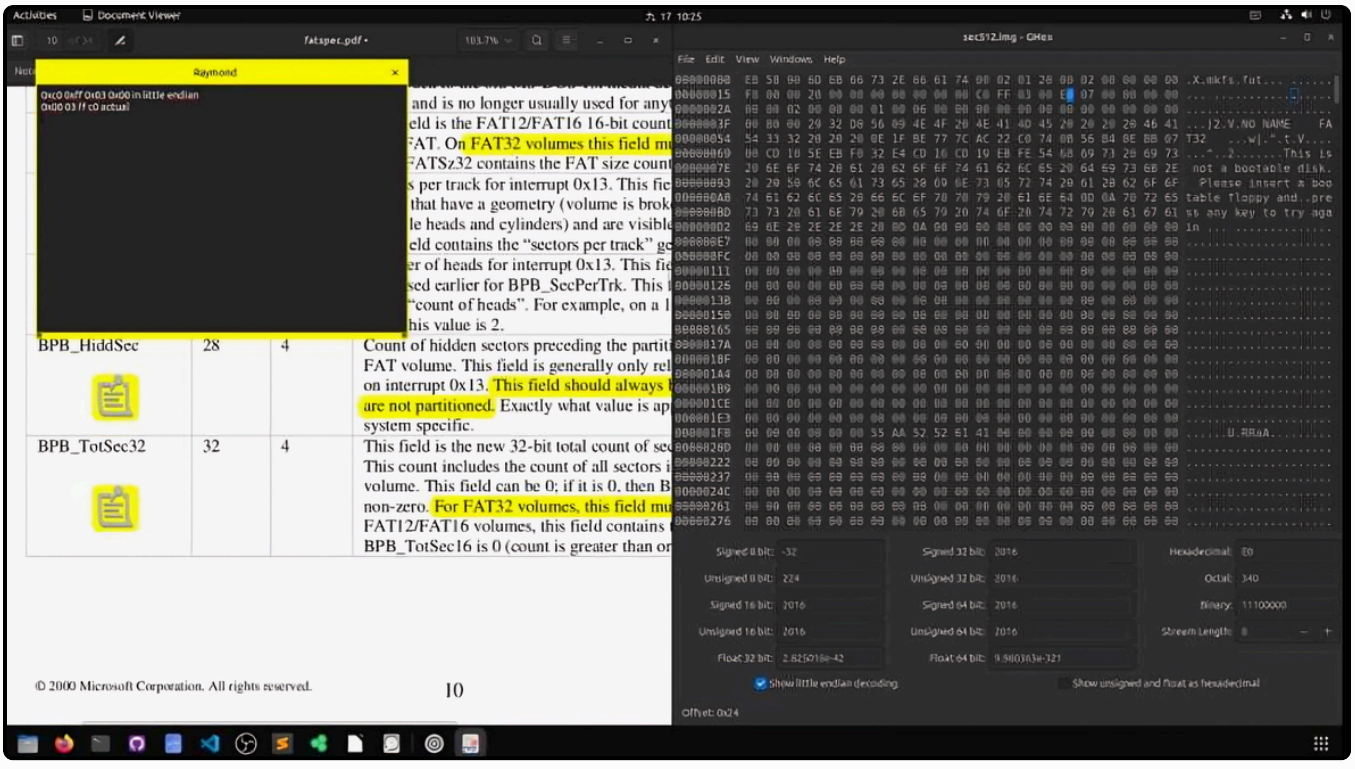
source code

可解析 FAT32 的 MBR bootstrap code

在 400+ bytes 的限制下用純組合語言寫成的 MBR

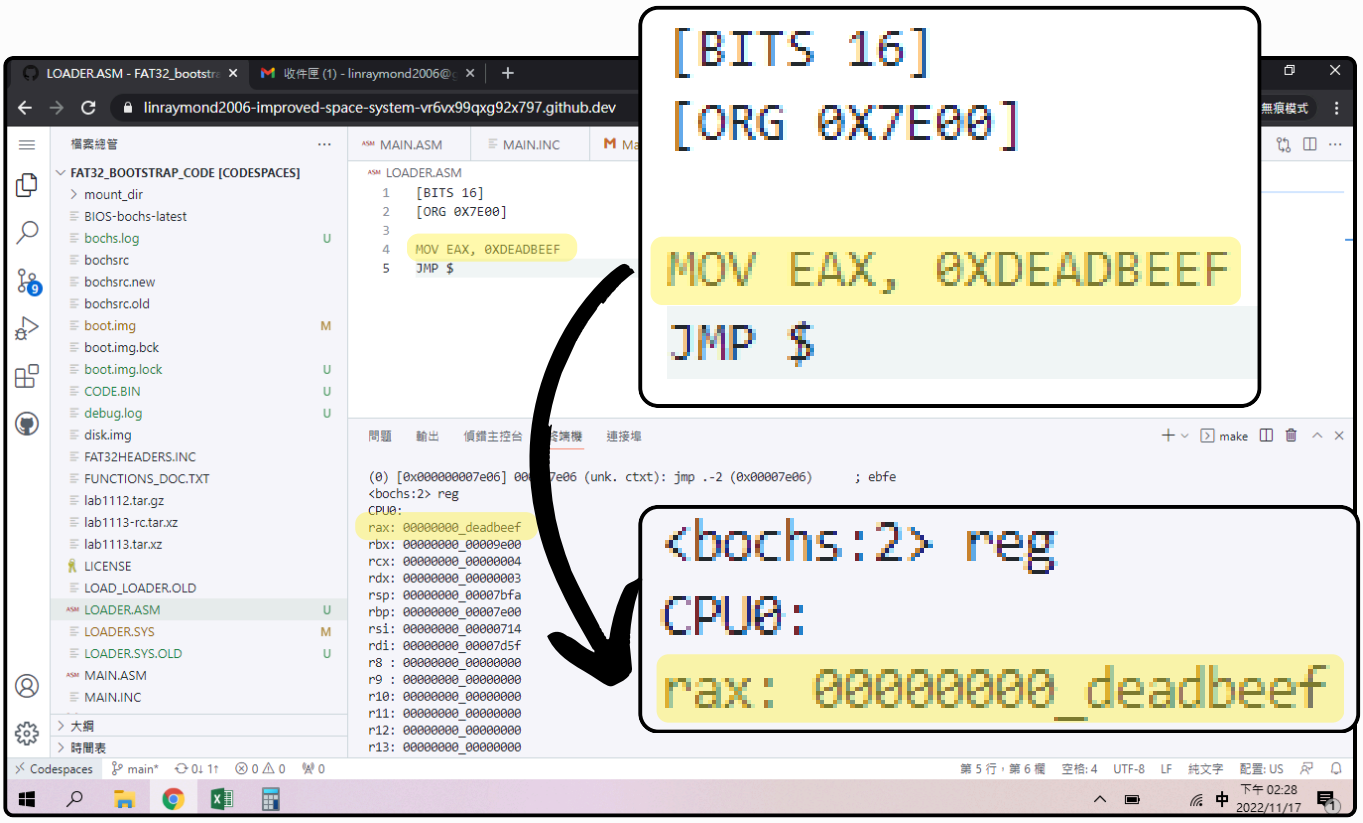
BIOS上電自檢（POST）後，便會把 sector #0 載入到 0x7c00 並轉交控制權，而 MBR 就是位於 sector 0 的開機程式（stage 0 loader）。此段程式雖然只有 500 上下個位元組，卻要完成載入 stage 1 loader 的任務（stage 1 loader 會再載入 kernel 執行）。

由於教學通常都是用 FAT 12/16 做範例，因此我挑戰可以解析 FAT32 的 MBR。為此，我查看了微軟對於 FAT32 規格的文件，並詳細了解 BIOS 資料區的記憶體布局。這一次的試驗不僅學到如何精簡組合語言，也強化了技術文件閱讀的能力，算是一次非常難得的嘗試！



藉由分析 metadata 和紀錄技術文件重點，我能更好的理解 FAT32 檔案系統

專案列表



第一次成功載入 second stage bootloader 至指定位址!

探索 kernel!

source code

費時兩年的摸索

從國中三年級到高中二年級的這段期間，我把大部分的時間投入在摸索 kernel，這是一個成長的過程。我摸索過的部份較多是硬體界面，包括:

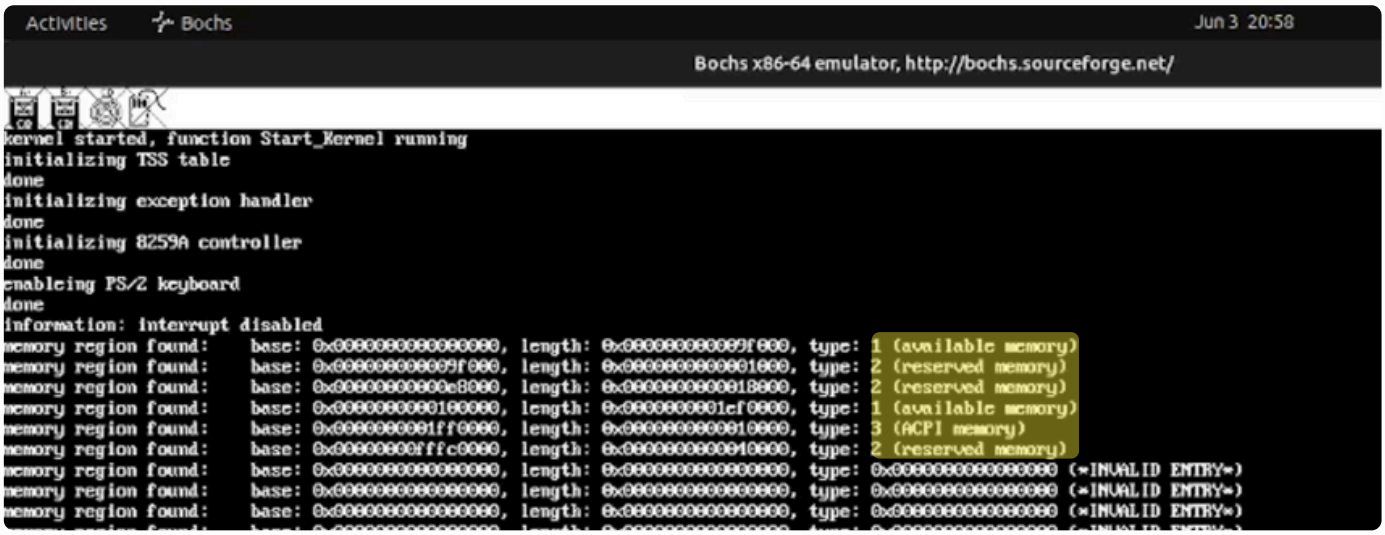
- 中斷處理
- 鍵盤解析程式
- SVGA 螢幕輸出
  - 類似 printk 的函式
  - 動手撰寫自製點陣字形的工具
- 記憶體區塊偵測

雖然失敗，但回顧過去所寫的程式，才發現一路走來所累積到的點滴，已將現在的我推到不同的高度！目前我已經轉成學習 Linux kernel module 開發和 Linux kernel 內部設計，還在摸索階段。我規劃之後將會融合我的軟體安全專長，投入 kernel 的軟體安全研究。

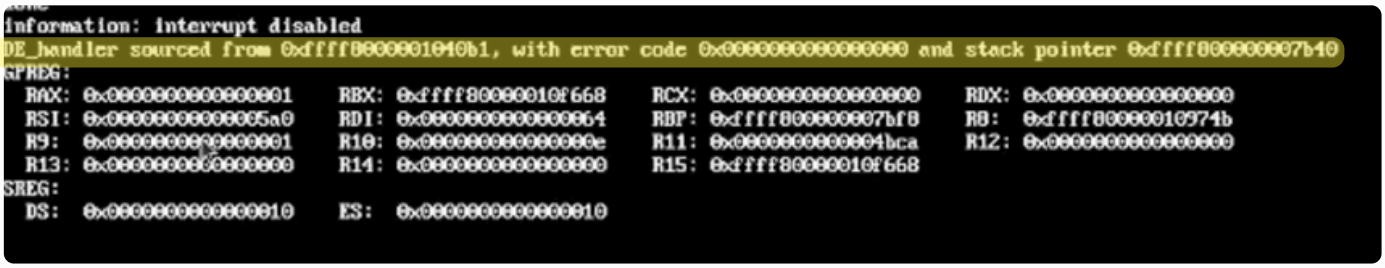
專案列表

影片

控制權轉交給 kernel



用 BIOS 提供的 e820 中斷偵測可用的記憶體區塊



Oops！除零錯誤

可以從鍵盤讀取輸入了，圖中正在輸入 Hello, World

專案：下一步?

研究 Linux kernel 並開發 kernel module

研究最被廣泛使用的核心

- 理解 Linux kernel 設計的巧思
- 了解 scalability 的各種考量
- 透過修改 kernel （kernel hacking）學習

研讀經典書籍和教材

按部就班的學習

向一些非概念性的經典 課程/書籍 學習

- xv6
- *Operating Systems Design and Implementation*
- *Operating System Design: The Xinu Approach*

設計 kernel 各部件

畫出藍圖

- 確定 kernel 的主要部件
- 設計各部件的交互方式
- 如何有效的管理資料結構

從 CISC 轉向 RISC

著重學習 kernel 設計，而非硬體界面

- x86 有一些歷史遺留的問題和極度複雜的硬體界面，學習門檻較高
- RISC 架構的硬體介面相對簡單，是適合學習 kernel 運作原理的平台
- 例如： Arm / AArch64 甚至更精簡的 RISC-V

研究 RTOS

除了 GPOS 之外的研究

- 了解如何把作業系統技術整合至各種對延遲有極高度要求的場景
- 學習 hard real-time OS 的設計巧思和真實應用

CND 網路防禦專家認證

我對於攻擊技術比較有興趣，但是以前從來都不知道「防禦」是怎樣的概念，這也是我為什麼選擇這一門課的主因。

對我來說，這一次的訓練只是一個開始，更細節的部份還要再繼續學習之後才會了解，藉由這一次的考試分析後發現我比較擅長技術面，而管理面的知識還要加強，畢竟人也是很大的攻擊面（ID-10T 問題）。

攻防本來就是一體兩面的事，攻擊者只需要找到一個點，而防禦者要防禦整個攻擊面，所以我現在如果能夠看到更多的攻擊面，增加自己的見識，就有機會更全面的檢閱攻擊者可能的進入點。

CND 網路防禦專家認證

語文檢定證明

IELTS™

Test Report Form — ACADEMIC

NOTE *Admission to undergraduate and post graduate courses should be based on the ACADEMIC Reading and Writing Modules. GENERAL TRAINING Reading and Writing Modules are **not** designed to test the full range of language skills required for academic purposes. It is recommended that the candidate's language ability as indicated in this Test Report Form be re-assessed **after two years** from the date of the test. To find out more about IELTS, IELTS band scores and the CEFR levels, please visit ielts.org/scores*

Centre Number	TW010	Date	21/SEP/2024	Candidate Number	505112

Candidate Details

Family Name	LIN
First Name(s)	YOU-SI
Candidate ID	361495909
Date of Birth	[redacted]
Sex (M/F)	M
Scheme Code	Private Candidate
Country or Region of Origin	
Country of Nationality	TAIWAN
First Language	CHINESE

Test Results

Listening	Reading	Writing	Speaking	Overall Band Score	CEFR Level
6.5	6.5	5.5	4.5	6.0	B2

IELTS 測驗成績單（學術組）：Band score 6（CEFR B2）

姓名 Name	出生年月日 Date of Birth
林宥熙 LIN, YOU SI	[redacted]
級數 Level	測驗日期 Test Date
中級 Intermediate	2022/04/23

聽力 Listening	閱讀 Reading	口說 Speaking	寫作 Writing
99	72	80	80
達通過標準 Pass (CEFR B1)		達通過標準 Pass (CEFR B1+)	達通過標準 Pass (CEFR B1+)

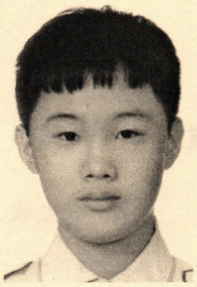
全民英檢中級初、複試通過證明

語文檢定證明

ETS TOEIC

LISTENING AND READING
OFFICIAL SCORE CERTIFICATE

TOEIC® 臺灣區總代理 忠欣股份有限公司
2F., No. 45, Sec. 2, Fuxing S. Rd., Da'an Dist.,
Taipei City 106472, Taiwan (R.O.C.)



林宥熙
LIN YOU-SI
Name

[redacted]
Date of Birth
(yyyy/mm/dd)

24045769
Registration Number

2024/09/29
Test Date
(yyyy/mm/dd)

LISTENING
Your Score 470
5 — 495

READING
Your Score 455
5 — 495

TOTAL SCORE
925

Individual (September 2024)
Client

- *TOEIC*® 臺灣區總代理 忠欣股份有限公司為讓成績使用單位辨識本成績單之真實性，提供智慧型手機使用之專屬應用程式服務。成績使用單位可在智慧型手機上下載右方之應用程式，並在網路連線下查閱本成績單之原始內容。
- TOEIC成績屬於考生本人之隱私與個人資料，使用本查驗應用程式之用戶，請確認已取得考生同意或具有查驗該成績單之權利，否則請勿使用本應用程式，以免違反個人資料保護法之相關規定。
- TOEIC成績保留兩年，可查驗期間為測驗日後兩年內。

TOEIC成績單查驗應用程式
Android版 iOS版

LISTENING

Your scaled score is between 400 and 495. Test takers who score around 400 typically have the following strengths:

- They can infer the central idea, purpose, and basic context of short spoken exchanges across a broad range of vocabulary, even when conversational responses are indirect or not easy to predict.
- They can infer the central idea, purpose, and basic context of extended spoken texts across a broad range of vocabulary. They can do this even when the information is not supported by repetition or paraphrase and when it is necessary to connect information across the text.
- They can understand details in short spoken exchanges, even when negative constructions are present, when the language is syntactically complex, or when difficult vocabulary is used.
- They can understand details in extended spoken texts, even when it is necessary to connect information across the text and when this information is not supported by repetition. They can understand details when the information is paraphrased or when negative constructions are present.

To see weaknesses typical of test takers who score around 400, see the *Proficiency Description Table.

ABILITIES MEASURED	PERCENT CORRECT OF ABILITIES MEASURED (Your Percentage)
Can infer gist, purpose and basic context based on information that is explicitly stated in short spoken texts	68
Can infer gist, purpose and basic context based on information that is explicitly stated in extended spoken texts	95
Can understand details in short spoken texts	93
Can understand details in extended spoken texts	95
Can understand a speaker's purpose or implied meaning in a phrase or sentence	75

READING

Your scaled score is close to 450. Test takers who score around 450 typically have the following strengths:

- They can infer the central idea and purpose of a written text, and they can make inferences about details.
- They can read for meaning. They can understand factual information, even when it is paraphrased.
- They can connect information across an entire text, and they can make connections between two related texts.
- They can understand a broad range of vocabulary, unusual meanings of common words, and idiomatic usage. They can also make distinctions between the meanings of closely related words.
- They can understand rule-based grammatical structures. They can also understand difficult, complex, and uncommon grammatical constructions.

To see weaknesses typical of test takers who score around 450, see the *Proficiency Description Table.

ABILITIES MEASURED	PERCENT CORRECT OF ABILITIES MEASURED (Your Percentage)
Can make inferences based on information in written texts	78
Can locate and understand specific information in written texts	88
Can connect information across multiple sentences in a single written text and across texts	89
Can understand vocabulary in written texts	91
Can understand grammar in written texts	95

※HOW TO READ YOUR SCORE REPORT:

Percent Correct of Abilities Measured:
Percentage of items you answered correctly on this test form for each one of the Abilities Measured. Your performance on questions testing these abilities cannot be compared to the performance of test-takers who take other forms or to your own performance on other test forms.

Note: TOEIC scores more than two years old cannot be reported or validated.

Copyright © 2024 by ETS. All rights reserved.
ETS, the ETS logos, and TOEIC are registered trademarks of ETS in the United States and other countries, used under license in Taiwan.

TOEIC 925/990 分（金色證書）

科學班證明

科 學 班 就 讀 證 明

茲證明本校學生 林宥熙（學號[redacted]，於111~113學年度就讀本校高中部編制之「科學班」無誤。

特此證明

新北市南山高級中學教務處

新北市南山高級中學 教務處 新北市中和區廣福路41號

中 華 民 國 113 年 10 月 08 日

科學班就讀證明