周聖倫 SHENG LUN CHOU

國立暨南國際大學 資訊管理學系

參與專案 2023 - 至今

- 2025 - 架設資安教育網站
  我們開發結合資安知識與遊戲化互動的數位學習平台，以 OWASP Top 10 漏洞與 CEH 知識為核心，設計理論、實作與挑戰模組，透過教材與小遊戲引導初學者快速建立資安概念。
- 2025 - Linux 系統管理實務 CSF-POC 資安架構概念驗證 - 專案負責人
  團隊設計一套專為資訊安全教學設計的 CTF 題目，能夠模擬從偵查、滲透、橫向移動、提權到資料外洩等完整攻擊流程，並結合多層次的內建監控與備份機制，持續記錄並保存學生的每一步攻擊行為（包含系統日誌、網路流量、進程／系統呼叫與檔案變動等痕跡）。我負責監控系統的架構設計與部署、日誌收集與警示規則的設定（Prometheus、Loki、Grafana），以及對攻擊紀錄進行彙整、關聯分析與產出可供教學與改進的技術報告。
- 2024 - 資安管理與實務 Honey Pot - 專案負責人
  採用開源誘捕系統（honeypot）模擬多種服務，讓團隊能察覺並偵測真實攻擊手法；同時整合 ELK（Elasticsearch、Logstash、Kibana）進行日誌收集、解析與索引，建立可視化儀表板並設定警示以加速異常回應。負責架構分解、系統部署與監控線建置。
- 2024 - Linux 系統管理實務 AI-IDS-SystemLog 分析工具 - 專案負責人
  針對 Linux 系統初學者在操作、實務階段遇到的種種相關問題提供分析工具。主要負責系統內服務撰寫 (Corntab) 以及 API 調用。
- 2024 - 軟體工程 外送系統 & 競標系統
- 2023 - SAD 金融業務保單系統 - 專案負責人
  為金融業務人員設計一套符合流程的保單批准系統。負責每組負責人再次分析保險業者使用者需求，針對問題設計出系統架構，確保設計能兼顧使用便利性、流程合規性與後續維運的可擴充性且定期與各組代表討論解決方案。
- 2023 - WordPress 偏鄉教學企劃 - 專案負責人
  負責系統設計架構以及維護，同時向組員定期開會討論進度。
- 2023 - 計算機概論 影像辨識

教材製作

- 資訊安全
  從建立扎實的資安基礎知識帶入，接著從攻擊者角度看侵入性檢測，再開始講述如何規劃並執行組織層級防護措施，確保資訊系統安全穩定運行。
- FHS 檔案系統階層標準
  從電腦的歷史講述最初使用系統的進化，以及為何採用檔案系統階層標準，再將結構拆解簡化讓初學者容易理解。
- Linux 基礎指令
  講述使用 Linux 時基本會使用到的指令，並且其中會不定時帶入實作，讓參與者能夠更好理解其中用途。

課程教學助理 國立暨南國際大學 2025

- 針對精選的 Linux 主題進行授課，指導學生進行實作練習，並提供課後技術支援。
- 上課內容
  FHS 檔案系統階層標準、Linux 基礎指令

技能

- Python / C#
- JavaScript / PHP
- Docker / Swarm
- Loki / Prometheus / ELK

開源貢獻

- AI-IDS
- SCF-POC

參賽經歷

- ITSA全國大專程式設計極客挑戰賽

技能

1. 擅長的程式語言：Python、JavaScript、PHP、SQL、C#
2. Web 後端框架：Node.js
3. Web 前端框架：React.js、Vue.js
4. 雲端虛擬化：Docker、Swarm
5. Linux 架設 Server：Web (Nginx、Apache2)
6. 監控與可觀測性：ELK Stack (Elasticsearch、Logstash、Kibana)、Grafana、Prometheus、Loki、eBPF

實務應用-開源以及教材

我參與開源開發，不僅希望藉由協作來提升程式開發與系統架構能力，也希望能在資安教育上留下實際貢獻。

開源專案

- LSA2_CSF_POC：以 NIST CSF 資安框架為基礎，設計一個專為資訊安全教學的 CTF 概念驗證專案，能模擬從偵查、滲透、橫向移動、提權到資料外洩等完整攻擊流程，並透過多層次的監控與事件紀錄機制，完整保存系統日誌、網路流量、進程呼叫與檔案變動等痕跡，協助教學中觀察與分析攻防行為。我負責監控系統的架構設計與部署，整合 Prometheus、Loki、Grafana 進行日誌收集與警示規則設定，並針對攻擊紀錄進行彙整、關聯分析與報告產出，以提供教學改進與案例研討的依據。
- LSA_Ai_Ids：結合 AI 與日誌分析的入侵偵測系統，探索以機器學習輔助事件監控與異常偵測的可行性。

教材

- FHS 檔案系統階層標準：從電腦的歷史講述最初使用系統的進化，以及為何採用檔案系統階層標準，再將結構拆解簡化讓初學者容易理解。
- Linux 基礎指令：講述使用 Linux 時基本會使用到的指令，並且其中會不定時帶入實作，讓參與者能夠更好理解其中用途。
- 資安書籍式教材彙編：從建立扎實的資安基礎知識帶入，接著從攻擊者角度看侵入性檢測，再開始講述如何規劃並執行組織層級防護措施，確保資訊系統安全穩定運行。

其他有利

大學專題 - 資安築城記

指導教授 : 陳彥錚教授
組員 : 周聖倫 劉姵岑 陳厚駪 李宗霖 楊璇蓁 黃子恩 黃子懿

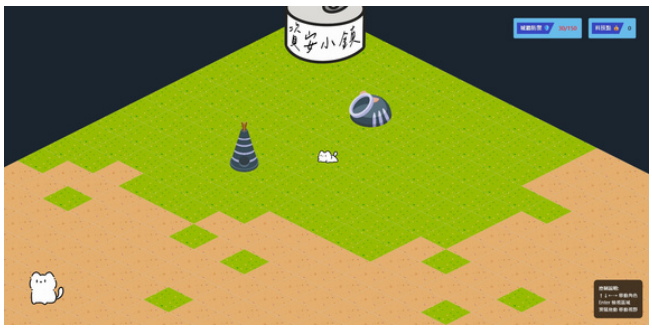
專題簡介:
近期常出現的勒索病毒到釣魚簡訊，資安威脅已經深入台灣社會日常，但多數人仍缺乏基本防護意識。為降低學習門檻並提升參與意願，我們開發了一個結合資訊安全知識與遊戲化互動的數位學習平台。課程以 OWASP Top 10 常見漏洞為核心，搭配 CEH（道德駭客認證）相關知識，設計兼具理論、實作與挑戰的學習模組，透過教材、練習題與小遊戲，引導初學者快速建立資安概念，將艱澀的專業轉化為有趣且具成就感的學習體驗。

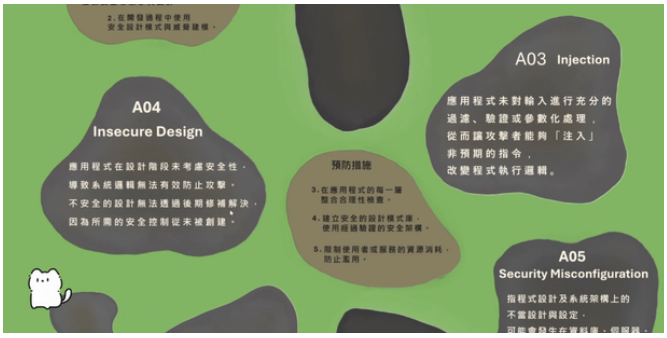
規劃階段（需求與教材設計）
為了打造不會造成使用者困惑且正確的網頁，需要學習並掌握必要的資安知識，並深化對系統運作的認識。

- 負責研究並整理部分 OWASP Top 10 漏洞、CEH 重點項目、各式滲透或是網頁安全掃描工具、使用題庫、遊戲事件。

開發階段（系統設計與前/後端開發）
每周與組員開會跟著手開發網頁，調整並思考使用者學習效果以及體驗。

- 負責設計網頁架構、前端部分 UI 及功能 (Vue)、後端 (Node.js) 及資料庫 (FireBase) API 串接、完整前後端整合、刷題區、測試。





其他有利

開源專案內容

CSF-POC

cybersecurity Framork - Proof of Concept 資安架構概念驗證

簡介：

設計並實作針對資訊安全教學的 CTF 平台：模擬完整攻擊流程、內建行為監控並記錄學生攻擊手法；系統依 NIST SP 800-53 Rev.5 與 NIST SP 800-63 系列之參考與驗證原則規劃，以協助教師分析學生解題策略並作為課堂教學回饋依據。

題目設計：

- 攻擊流程：SQLi → LFI → Reverse Shell → 提權
- 任務：取得帳號密碼、上傳 Webshell、進行 RCE、讀取 FLAG

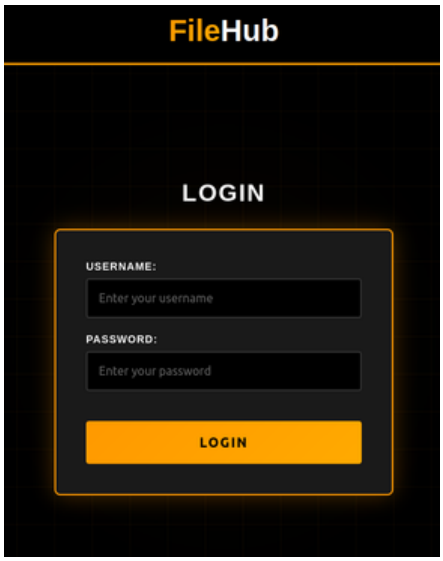
監控系統架構 ：

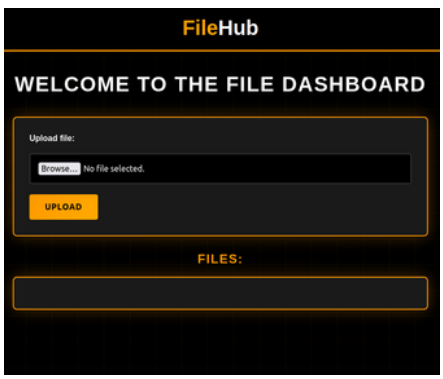
組件

- Nginx + Promtail + Loki + Grafana：收集、儲存、展示容器內 log、
- Prometheus：收集系統 metric（CPU、記憶體、HTTP 分佈）
- eBPF (bpftace)：攔截 syscall（execve, open, connect 等），補足 log 無法追蹤的行為

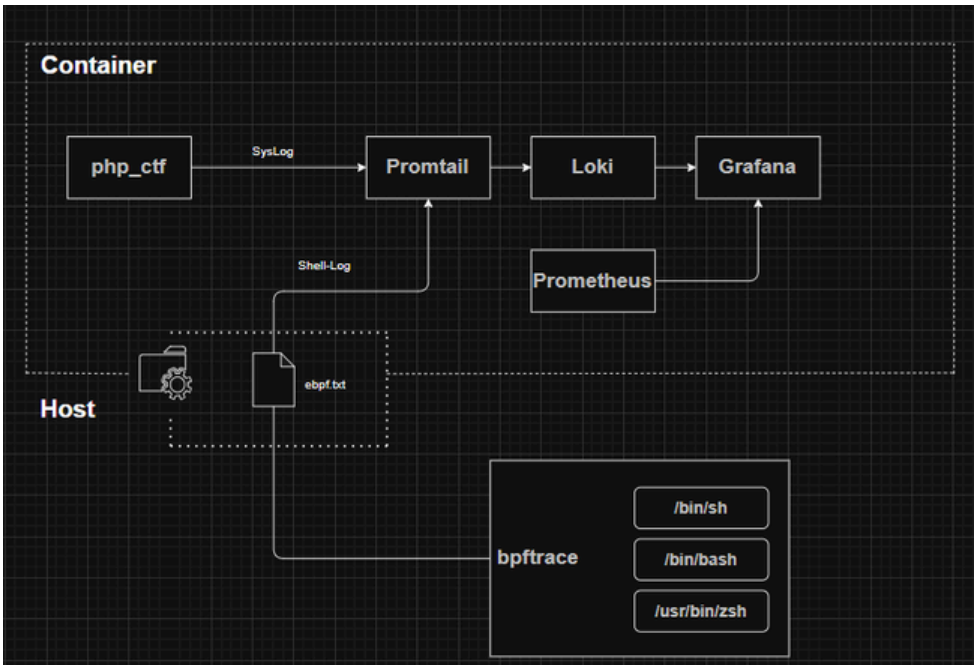
特色

- Loki/Prometheus 主要看 log 與 metric
- eBPF 能捕捉到「誰開了哪個 process、連了什麼 IP」等底層細節





- 登入介面以及上傳介面



- 整體架構圖

其他有利

遇到的問題與解決方式：

我負責的部分是架構設計以及監控部分，一開始天真地以為只要安裝 Grafana / Loki / Prometheus，就能完整觀測容器內的所有細節。但實際操作後發現後並不是。

問題

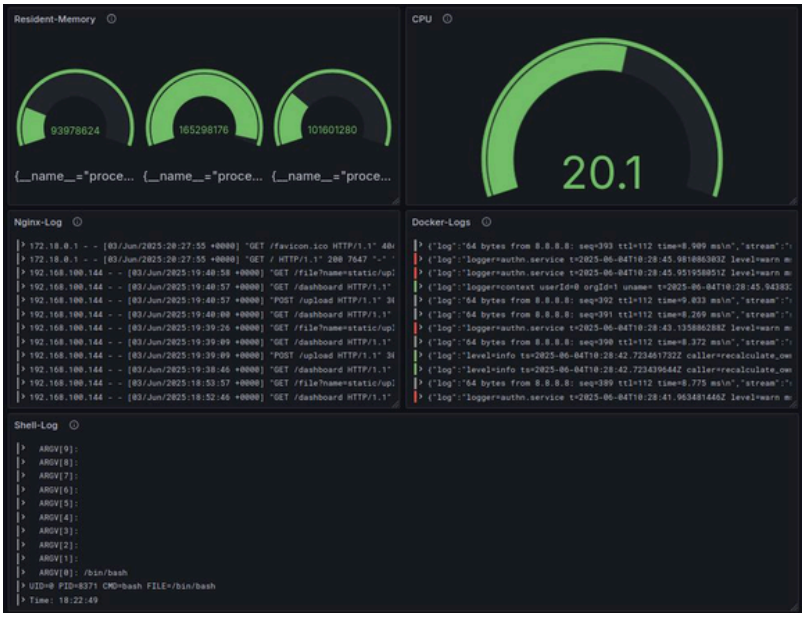
- 反彈 shell 行為是透過 系統呼叫（execve, socket, connect 等）觸發的，Grafana/Loki/Prometheus 並不會 hook OS syscall，因此根本無法得知「誰在容器裡開了什麼 process、往哪個 IP 發了連線」。
- 反彈 shell 使用 交互式 TTY，輸入/輸出並不會寫進容器 stdout，所以 Loki 也抓不到任何 log。

解法

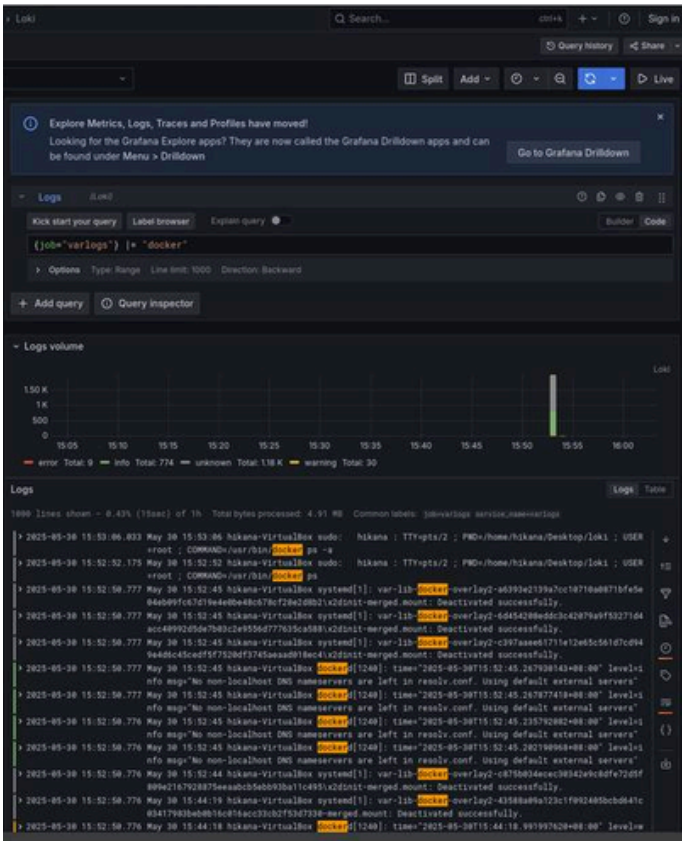
- 透過 eBPF 技術監控 syscall
- 在 kernel 層即時偵測可疑行為（如非法檔案存取或外部連線）

收穫：

- 學到光看 log 不夠，必須深入 Syscall / Kernel / eBPF 層
- 反彈 shell 與隱蔽攻擊需要更底層的監控
- eBPF 是往後可擴展的安全可觀測性核心



- 監控內容



- 監控內容

其他有利

AI-IDS

Artificial Intelligence-based Intrusion Detection System 人工智慧式入侵偵測系統

簡介 :

設計一套自動化 AI 輔助診斷系統，透過 Flask 平台收集伺服器 log，並呼叫 GPT 模型分析錯誤訊息，回傳建議解法，降低人工 Debug 成本。

架構 :

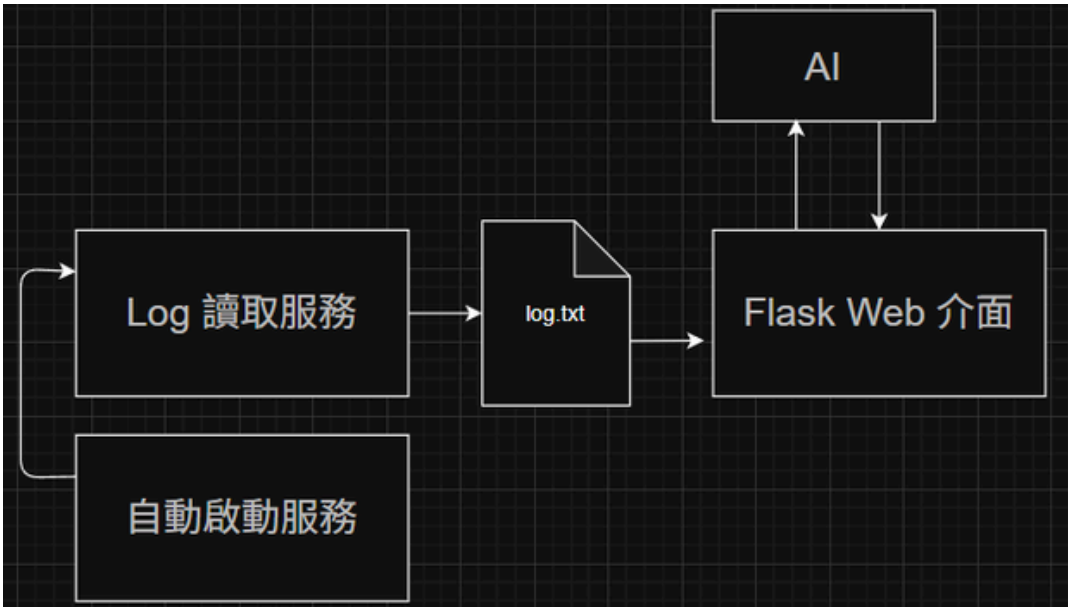
- Log Collector：systemd 服務定時監控 Linux 系統 log，將錯誤輸出成文字檔。
- Flask Web：提供介面與 API，顯示 AI 分析回覆。
- AI/LLM：將 log 傳給 GPT API，回傳對應修復建議。

遇到問題 :

- Log Collector：systemd 服務定時監控 Linux 系統 log，將錯誤輸出成文字檔。
- Flask Web：提供介面與 API，顯示 AI 分析回覆。
- AI/LLM：將 log 傳給 GPT API，回傳對應修復建議。

收穫 :

- Log 分析限制：目前為了便利，只用關鍵字篩選錯誤，但真實情境需要 模型或資料庫 去判斷哪些訊息才是真正的問題。
- 介面不足：現有介面偏向工程師使用，設計單調，未來應該增加 更友善的視覺化，像是分級告警、歷史比對。



- 整體架構圖

OXFORD PLACEMENT TEST

Test taker name: 周聖倫 周聖倫

Organisation name: National Chi Nan University

Date taken: 7th September 2022

Results	Score	CEFR	Time taken
Overall result	**84**	**C1**	00:45

	Score	CEFR	Time taken	Communicative competencies
Use of English	78	B2	00:14	Learners at this level can typically... • use a good range of vocabulary for most general topics • use the appropriate collocations of many words fairly systematically in most contexts • demonstrate a relatively high degree of grammatical control; occasional errors in sentence structure may still occur, but these can often be corrected • demonstrate a good command of simple language structures and some complex grammatical forms.
Listening	90	C1	00:31	Learners at this level can typically ... • recognise a wide range of idiomatic expressions and colloquialisms • follow speech that is not clearly structured and requires inference to make connections between ideas • follow interactions on abstract, complex topics that are both familiar and unfamiliar • identify finer points of detail, including implicit attitudes and relationships between speakers.

Score guide

The Oxford Placement Test measures a test taker's ability in English on the Common European Framework of Reference (CEFR).

Pre-A1			A1		A2		B1		B2		C1		C2	
low	mid	high	A1.1	A1.2	A2.1	A2.2	B1.1	B1.2	B2.1	B2.2	C1.1	C1.2	C2.1	C2.2
0.1	0.4	0.7	1	11	21	31	41	51	61	71	81	91	101	111	120

Please note that the result from the Oxford Placement Test is intended to help place learners in the right level class with appropriate learning materials. As the test does not cover the full range of language skills, it is recommended that a language proficiency test should be taken for evidence of overall proficiency.

OXFORD UNIVERSITY PRESS