

HIT



社團法人台灣駭客協會
ASSOCIATION OF
HACKERS IN TAIWAN

hacker.org.tw

駭客的鬥法大賽 - 從 HITCON
CTF 到 HITCON Cyber Range
CK & Kyo

HIT

台灣駭客協會 2025 計畫



Community



CTF



CISO Summit



Enterprise



Cyber Range



Training



FreeTalk



人才媒合活動



社群補助



HITCON GIRLS



ZeroDay



KnowledgeBase

HIT

五大活動介紹



HITCON Community
台灣駭客年會 - 社群場

全台技術含量最高、最具駭客文化的資安研討會，齊聚上千海內外資安技術人員，進行深度技術交流及社群互動。



HITCON CISO Summit
資安長高峰會

全閉門邀請制的資安長高峰會，邀請超過百位來自全球的資安決策者與政府代表親臨現場，針對資安策略、時事議題與政策進行深度與廣度兼具的會議。



HITCON Enterprise
台灣駭客年會 - 企業場

針對企業資安議題的研討會，百位企業資安管理代表出席，從資安管理及實務技術相互交流，促進並推動國際產官學研交流，提升資安成熟度。



HITCON CTF
CTF 競賽

一場挖掘資安明星的現場即時攻防競賽，由國內知名戰隊出題，將邀請來自世界各地的頂尖駭客隊伍到場進行世界級的巔峰技術對決。



HITCON Cyber Range
企業藍隊競賽

專為企業資安人員量身打造的資安攻防賽，以面對資安威脅的事件處理能力為主要競賽項目，透過實戰打造更健全和強韌的企業環境。

HIT_

HITCON CTF

社團法人台灣駭客協會
ASSOCIATION OF
HACKERS IN TAIWAN

HIT_

當有個程



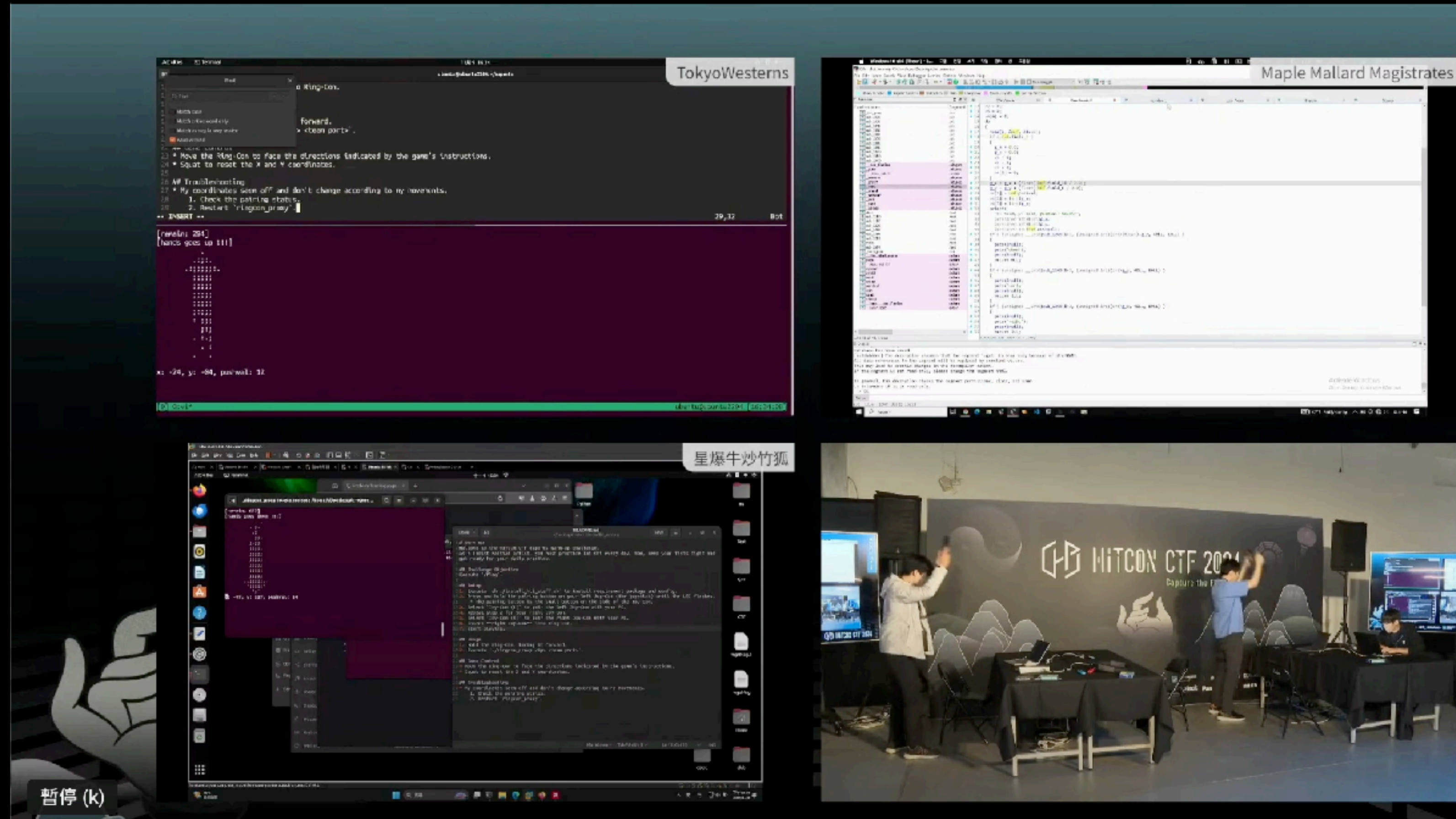
下健身環



JAKE-CLARK.TUMBLR

HIT_

Bytes to Thrive



TokyoWesterns 告訴我們，健身也可以解 CTF



HITCON CTF

頂尖駭客的全球性技術競技

One of Most Important Global Hacker
Competition for Top Hackers

HIT

HITCON CTF 2024 年活動亮點

- **競賽規模參與度擴大：吸引更多國家、頂尖駭客參與 HITCON CTF**
為了鼓勵更多駭客參與競賽，今年特別將 HITCON CTF 出賽時間提前至 DEFCON 決賽前，並與 DeFiHackLabs 合作，提供 Web3 新興題型額外解題獎勵，將競賽方向多元化
- **提升競賽趣味性與視覺化：題目與主題結合，視覺化讓會眾體驗**
今年競賽將以 Capture The FengShui 為主題，題目不僅承襲以往頂尖水準與多元方向，並將與中華文化主題緊密結合，提升題目趣味性。並與現場視覺化結合，透過導覽讓更多會眾體驗 CTF
- **同場舉辦精英人才交流：會提各項資安競賽，提供學子導引**
首次舉辦精英人才交流活動，邀請台灣各大資安競賽得獎者擺攤演講，透過不同階層、不同面向的競賽者互相交流，讓學生了解發展方向，選擇適合的發展方向，為台灣資安發展奠定人才基礎



HIT

來自世界各國的駭客明星隊



Blue Water

- 2023 世界積分第一名戰隊
- DEFCON 2024 2nd



MMM

- DEFCON 2023, 2024 冠軍



Friendly Maltese Citizens

- 世界大聯隊
- HITCON 2023 冠軍
- 九隻常勝軍聯合
- 英國、芬蘭、越南、中國



TokyoWesterns

- 日本最強戰隊

HIT

來自世界各國的駭客明星隊



thehackerscrew

- 來自超過 15 個國家的聯隊
- 去年在七場 CTF 中奪冠



RePokemonCollections

- 今年新興戰隊
- DEFCON 2024 第四名
- r3kapiG, C4T BuT S4D, Bushwhackers, dtl, More Smoked Leet Chicken



Superflat

- 來自荷蘭的新戰隊



Defunqt

- A team of formerly retired CTF players looking to make a comeback

HIT

來自世界各國的駭客明星隊



Cold Fusion

- The Cold Fusion Team is a union comprised of Korean people.



SuperDiceCode

- SuperDiceCode is the combination of SuperGuesser, DiceGang, and CodeRed.



星爆牛炒竹狐

- 台灣第一名晉級
- 星爆牛炒竹狐結合星爆吉娃娃、牛肉湯和竹狐三隊，以星爆、煮牛肉湯、cosplay 狐狸聞名。他們用各自的頂尖技術，成為台灣新一代資安界的強大勢力。



YAATN

- AIS3 推薦團隊
- 星爆牛炒竹狐結合星爆吉娃娃、牛肉湯和竹狐三隊，以星爆、煮牛肉湯、cosplay 狐狸聞名。他們用各自的頂尖技術，成為台灣新一代資安界的強大勢力。

HIT 台灣首創全新 Esports 一對一擂台賽



今年比賽新增了全台首創的 CTF Esports 一對一擂台賽項目，並首次引入 LiveCTF 賽制。該賽制將比賽過程同步直播，並由賽事主播與賽評全程解說，四場精采對戰的直播促進了全球資安愛好者之間的互動，讓無法親臨現場的觀眾也能即時觀戰

HIT

合作單位/社團



尋找資安女婕思
Girls in CyberSecurity

GiCS 尋找資安女婕思



ISIP 教育部資訊安全
人才培育計畫



THJCC 臺灣
高中聯合資安競賽



Balsn



Taiwan Security
-Club (TSC)



技能競賽 - 網路安全

HIT

HITCON CTF 頒獎典禮



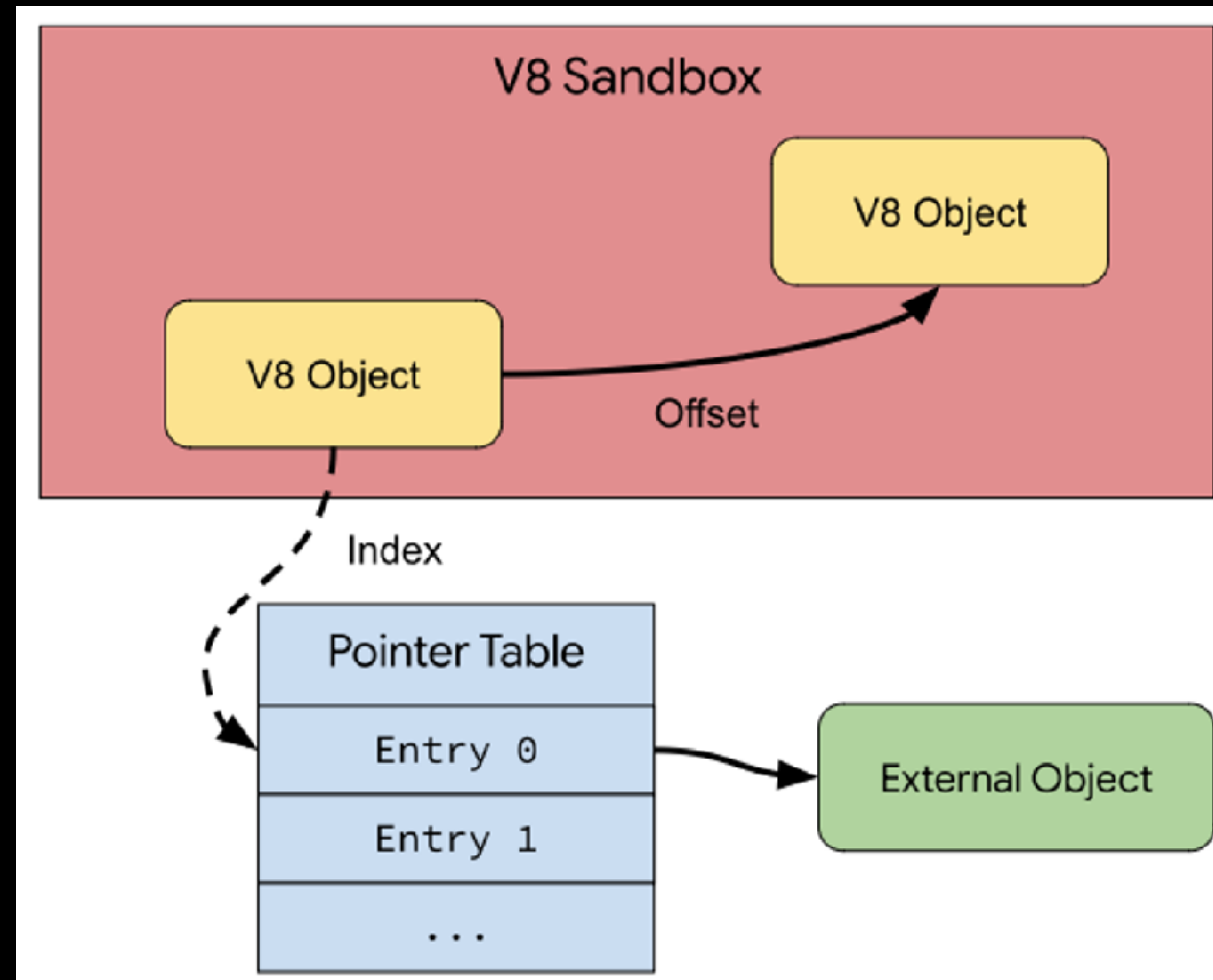
最終由國際聯隊「Friendly Maltese Citizens」獲得了第一名的寶座，並取得參與 2025 DEFCON CTF 決賽的資格

HIT_

V8 SBX—一段關於 Thinking Outside The Box 的故事

By ljp_tw

- V8 Sandbox Escape 題
- Chrome 底層運行的 Javascript engine
- V8 中有替記憶體管理機制加上 Sandbox 保護
- 直接給了 Sandbox 內的任意讀寫
 - V8 SBX 額外提供一個可以改 Trusted Pointer Table 的 primitive
- 輸入一段 javascript, 然後跑一跑要 RCE



- 先創立一個 function, 呼叫一次, 產生它對應的 bytecode array
- 修改 Trusted Pointer Table, 讓原先指向 bytecode array 的 pointer 指向我們偽造的 bytecode array
- 將 bytecode 修改為會洩漏 stack 上的 return address
- 執行 function 做到 leak d8 address
- 再將 bytecode 修改為會將傳入的參數放到 stack 上覆蓋掉某一層 function call 的 old rbp
- 準備含有 ROP chain 的物件
- 將該物件傳入執行 function, 進而執行 ROP → Get Shell

Breaking V8 Sandbox with Trusted Pointer Table

Jul 14, 2024

Recently, I have submitted my academic paper to NDSS 2025. Now it's time to take a break. Following the deadline is the HITCON CTF 2024, so as the break, why not take a look? I really haven't played CTF for quite a long time. :)

During the two days, I spent my efforts on the V8 Sandbox challenge. Actually I haven't worked on V8 for a while. It seems that the sandbox feature now has already been enabled and incorporated into the bug bounty program. This is also a chance for me to catch up to the new progress on the V8 security. :)

0x00 Abstract

The challenge provides two exploitation primitives: writing a 64-bit value to the entry of the trusted pointer table and leaking the base address of PIE. We can use the first primitive to fake a

value in the trusted memory
number arguments of the
the immediate numbers in the



2019
@r3tr0spect2019

Haven't played CTF and V8 for a while, but recently solved the V8 SBX challenge in the HITCON CTF. This is my write-up:

mem2019.github.io/jekyll/update/...

ポストを翻訳

午前9:01 · 2024年7月15日 · 1.1万 件の表示

15 リポスト 1 件の引用 132 件のいいね 52 ブックマーク

HIT

預期解題流程

- 先創立一個 function, 呼叫一次, 產生它對應的 bytecode array
- 修改 Trusted Pointer Table, 讓原先指向 bytecode array 的 pointer 指向我們偽造的

Breaking V8 Sandbox with Trusted Pointer Table

Jul 14, 2024



LJP 2024/07/13 01:10

First Blood - 星爆牛炒竹狐 solved v8 SBX by thinking outside the box, congratulations 100



1



2



1



1



1

- 執行 function 做到 leak to address
- 再將 bytecode 修改為會將傳入的參數放到 stack 上覆蓋掉某一層 function call 的 old rbp
- 準備含有 ROP chain 的物件
- 將該物件傳入執行 function, 進而執行 ROP → Get Shell

0x00 Abstract

The challenge provides two exploitation primitives: writing a 64-bit value to the entry of the trusted pointer table and leaking the base address of PIE. We can use the first primitive to fake a



2019
@r3tr0spect2019

Haven't played CTF and V8 for a while, but recently solved the V8 SBX challenge in the HITCON CTF. This is my write-up:

mem2019.github.io/jekyll/update/...

ポストを翻訳

午前9:01 · 2024年7月15日 · 1.1万 件の表示

15 リポスト 1 件の引用 132 件のいいね 52 ブックマーク

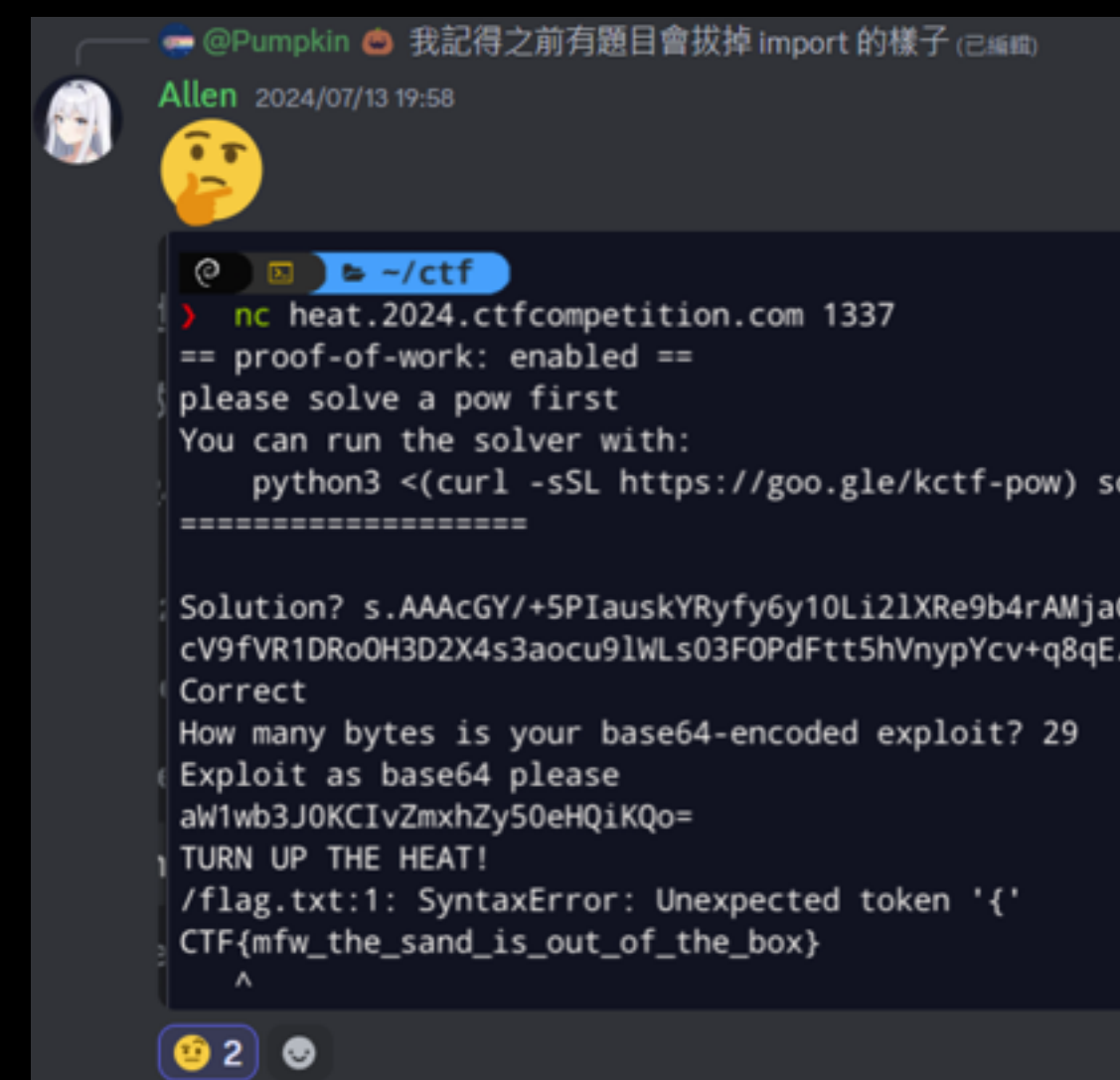
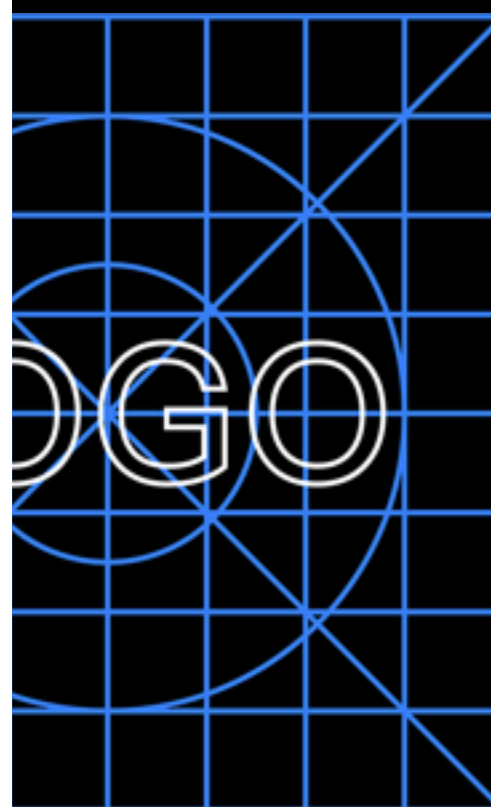
HIT

非預期解

```
Length:
24
JS script:
import("/home/ctf/flag")
/home/ctf/flag:1: SyntaxError: Unexpected token '{'
hitcon{Modifying_TPT_A1l0w5_u_t0_easily_escape_the_sandb0x}
^
SyntaxError: Unexpected token '{'

/home/ctf/flag:1: SyntaxError: Unexpected token '{'
hitcon{Modifying_TPT_A1l0w5_u_t0_easily_escape_the_sandb0x}
^
SyntaxError: Unexpected token '{'

1 pending unhandled Promise rejection(s) detected.
```



- 最終 35 solves, 是除了 welcome 題以外, 第三名最多人解的題目
- 比賽當天晚上 10 點開始, 這題 11 點 40 分左右就被台灣隊伍「星爆牛炒竹狐」取得首殺
- 隨著首殺出現, 解題隊伍開始如雨後春筍湧現 預想難度不應該這麼快就被解

HIT

V8 SBX

題目培養的能力

- 對現代瀏覽器架構的深入了解
- JavaScript 的架構，以及如何 Escape Sandbox
- 實作 Exploit 的能力

戰隊 LJP_TW 花費了當兵寶貴的休假來刻這題，
感謝他的辛勞！

V8 SBX Revenge [315pts]

```
nc v8sbx.chal.hitconctf.com 1338
```

https://storage.googleapis.com/hitcon-ctf-2024-qual-attachment/v8sbx_revenge/v8sbx_revenge-772b4668c5867082df541cfcecaa0f81caaf36e8.tar.gz

Author: ljp_tw
13 Teams solved.

#	Team	Submit Time
1	defunqt2	2024-07-12 23:00:16 UTC
2	Maple Mallard Magistrates	2024-07-12 23:51:08 UTC
3	Blue Water	2024-07-13 00:49:20 UTC

Contest is over.

HIT_

**將駭客思維用在藍隊！
讓藍隊的英雄有發揮的舞台！**



HIT_

HITCON Cyber Range

社團法人台灣駭客協會
ASSOCIATION OF
HACKERS IN TAIWAN



HITCON Cyber Range

挑戰極限的企業藍隊資安 調查x應變 競賽

**An elite Enterprise Cybersecurity Investigation
and Response Competition for Blue Team**

HIT 企業藍隊 / Blue Team, GPT 說...

常見工作	說明
🛡️ 防禦建置	設計並實施防禦機制，如防火牆、入侵偵測系統（IDS）、端點防護（EDR）等。
👁️ 監控與偵測	使用 SIEM、SOC 等工具，持續監控網路與系統異常行為。
🔍 威脅分析與回應	分析惡意行為、可疑流量，進行資安事件調查（Forensics）與應變（Incident Response）。
🧰 弱點掃描與修補	定期掃描漏洞、管理修補流程，降低攻擊面。
📖 資安教育與政策制定	執行資安意識訓練、撰寫資安政策與流程。



HITCON Cyber Range 是一場以資安事件調查及應變為主的企業藍隊競賽。模擬企業遭受網路攻擊，參賽隊伍扮演資安應變團隊，從威脅告警資料及系統日誌中找出攻擊者的足跡，攻擊事件應變，增強企業面對資安威脅的防禦能力。

HITCON Cyber Range 為臺灣難度最高的藍隊 (防禦) 資安競賽之一，透過競賽不僅考驗參賽隊伍的技術實力及團隊默契，更重要的是培養參賽隊伍的實戰經驗與防禦技巧，從中熟悉資安事件的調查流程與技術，提升面對資安威脅的實戰解決能力，培育企業及政府迫切需要的防禦性資安人才。

TRAPA Security

- 2020 年於台灣成立
- 由五位 **HITCON CTF** 戰隊成員創辦
- 具有豐富紅藍隊經驗
 - Cybersecurity Firm, PSIRT, SOC Team, etc.
- 專精於漏洞研究、藍隊團隊養成

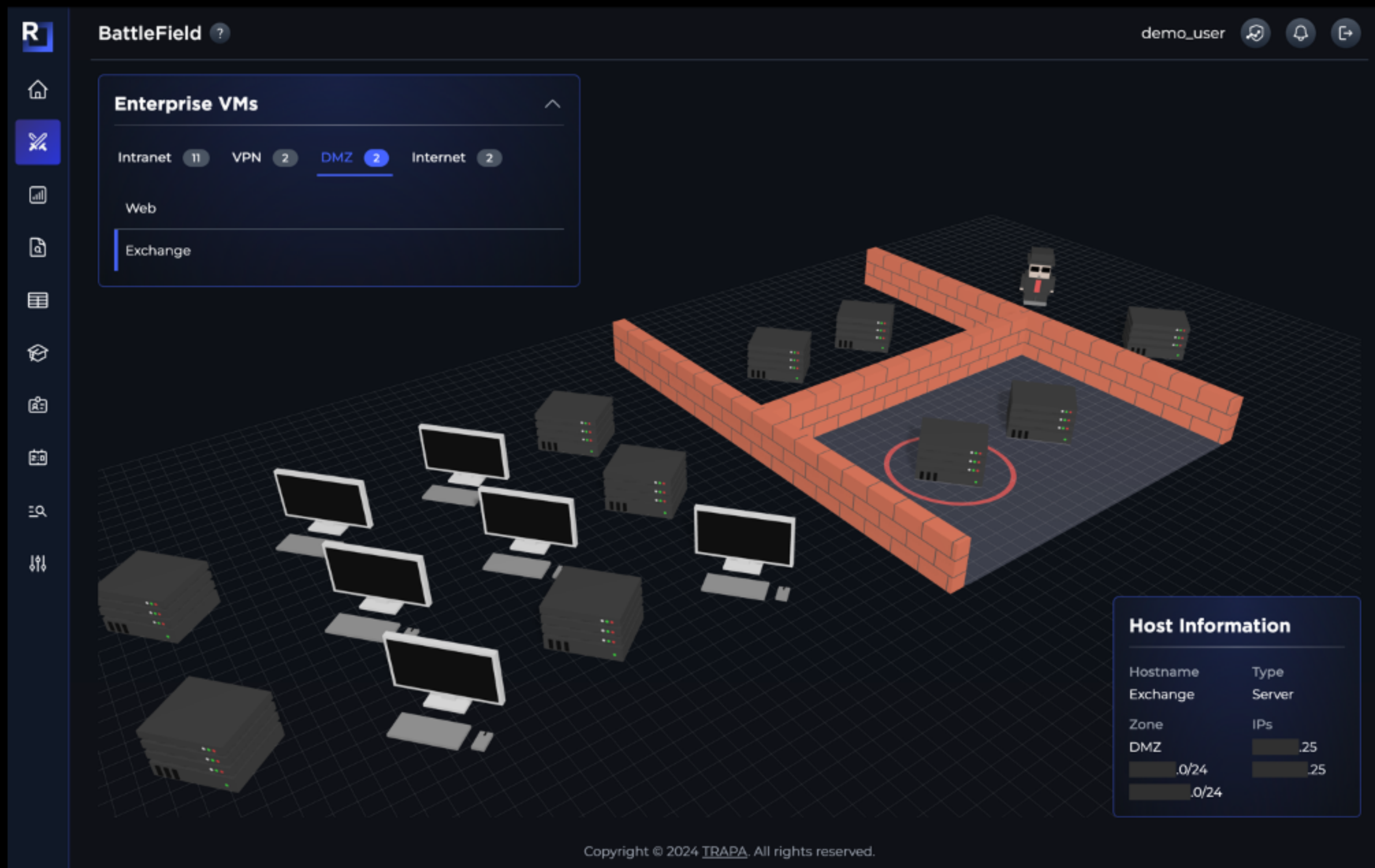
漏洞挖掘能力、CTF 參賽/舉辦經驗、
企業藍隊服務經歷

- **DEFCON CTF**、**PWN2OWN** 戰績
- 頂尖企業 SOC Team、PSIRT 服務經歷



HIT

HITCON Cyber Range 競賽情境



HIT HITCON Cyber Range 競賽情境

Action Timeline

✓

Weird Connection Detected Investigation
2024-05-03 18:19:22

🔍

Abnormal Logging Session Investigation
Score: 100

⌚

Something went wrong Investigation
Score: 100 Penalty Time: 78 seconds

✓

Credential Dump Investigation
2024-05-03 18:20:35

🔍

Phishing Mail Investigation
Score: 60

Action Timeline

Alerts from built-in real-time rules

Investigate Action

Something went wrong

• T1046

Score: 100 pts

We detected an abnormal traffic from DMZ to intranet, please find it.
Related dashboard: [Firewall Status](#)

Notice: There may be more than one answer. You can submit any of it.

Max Port The maximum port which attacker tried	Min Port The minimum port which attacker tried

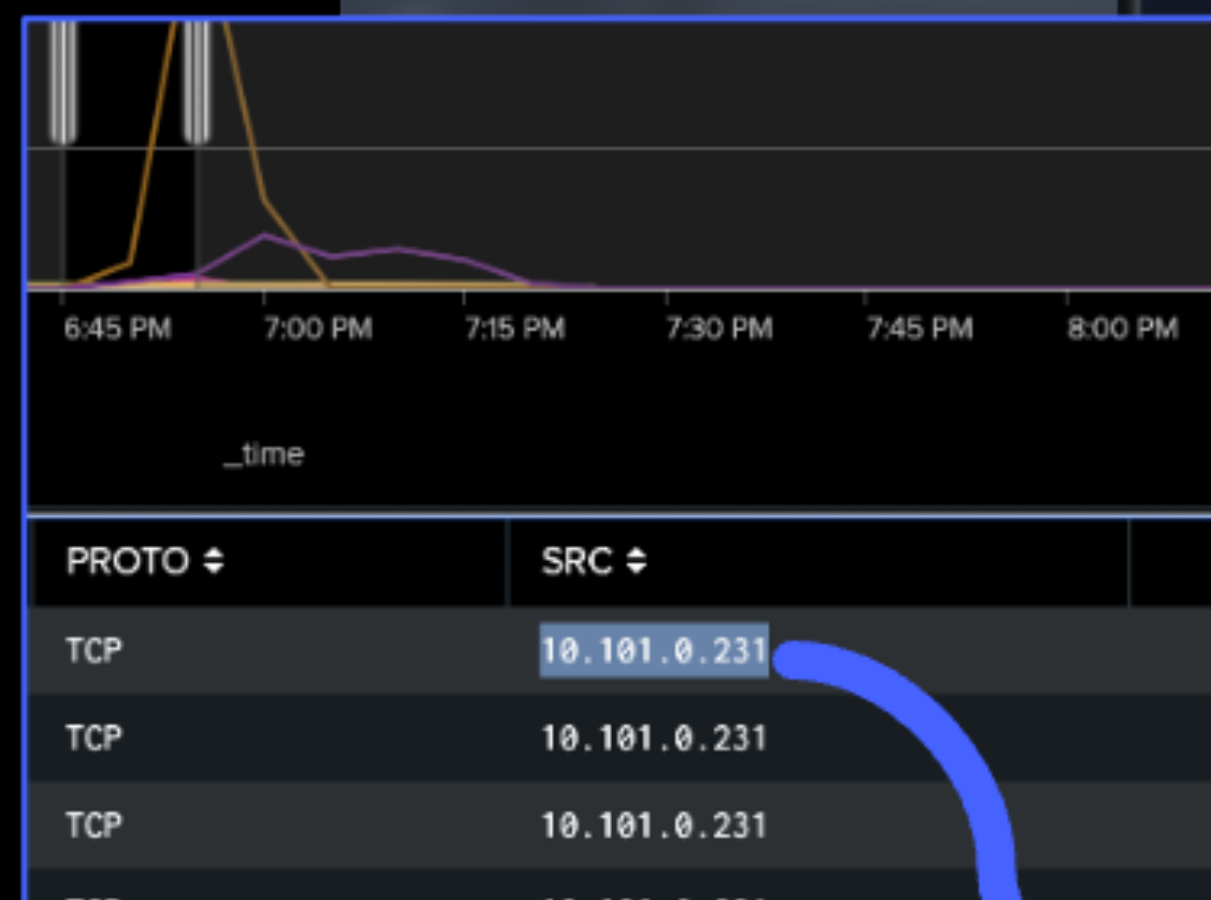
Source IP
The source IP address

Submit

Investigation Form

Fill-in Questions for critical information

HIT HITCON Cyber Range 競賽情境



Something Went Wrong

T1046

Details Tickets 2

We detected an abnormal traffic from Intranet to

Related dashboard: [Firewall Status](#)

Notice: There may be more than one answer. You can submit any o

Max Port

The maximum port which attacker tried

Source IP

The source IP address

Something Went Wrong

T1046

Score: 100 pts

Details Tickets 2

We detected an abnormal traffic from Intranet to VPN, please find it.

Related dashboard: [Firewall Status](#)

Notice: There may be more than one answer. You can submit any of it.

Max Port

The maximum port which attacker tried

Min Port

The minimum port which attacker tried

Source IP

The source IP address

Submit

HIT

HITCON Cyber Range 題目設計

實務性

採用企業事件應變時的流程進行比賽。
於 **SIEM** 中發現攻擊行為並分配資源進行調查及應對。

真實性

攻擊鏈根據 APT 組織攻擊特徵及 **MITRE ATT&CK** 攻擊技術設計。

複雜性

模擬企業環境中內部員工操作電腦、製造常見網路服務事件。不單只有使用**特定工具**就可以解決所有的問題。

完整性

演練將套用完整的攻擊鍊 - **漏洞掃描、伺服器入侵、寄送釣魚郵件、水平滲透、權限提升、資料竊取**。挑戰參賽者的**資安應變思維**。

HIT — HITCON Cyber Range 題目範例

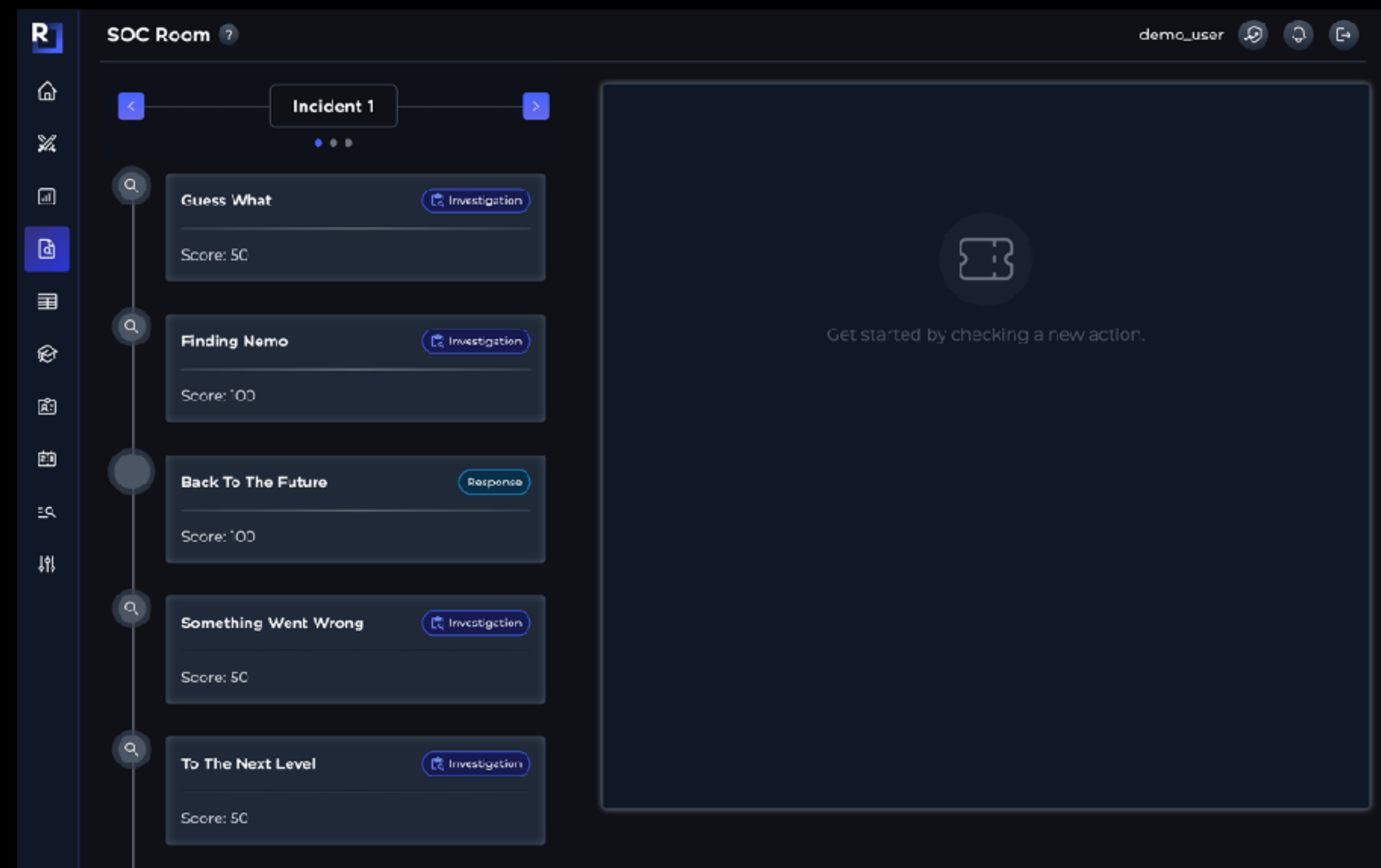
調查類 Investigation 題目範例 (2023)

考驗資安事件發生時的調查能力

攻擊者藉由 系統管理服務 的漏洞進入 Linux server

- 側錄封包 嘗試取得敏感資訊
- 植入 Rootkit

1. 參賽者從紀錄分析入侵軌跡, 使用的漏洞, 入侵後的行為
2. 透過 **Disk Forensics** 還原被刪除的檔案, 竊取的資訊
3. 透過 **Memory Forensics** 找出 Rootkit
4. 透過 **Reverse Engineering** 分析 Rootkit 運作方式及密碼



HIT HITCON Cyber Range 題目範例

應變類 Response 題目範例 (2024)

考驗資安事件發生後的應變及復原能力

參賽者透過調查發現 Misconfigure 事件後，為避免未來發生類似情況，撰寫 script 在重要設備的設定檔更動時，檢查此更動是否跟申請一致。

- 網路設定檔判讀
- 防火牆申請單判讀
- 規則比對

Audit Inconsistency

• T1595

Score: 125 pts

Details

Tickets 0

Due to the previous event, we have to ensure the firewall configuration in the firewall application accurately reflects and implements the organization's security policies and intended network access controls.

You are given a firewall application database and current active firewall configuration file. All firewall entries should be applied through firewall application. As the current active firewall configuration might be tampered by attacker, your task is to list out all inconsistent entries which are different from firewall application database in 2024-10-30.

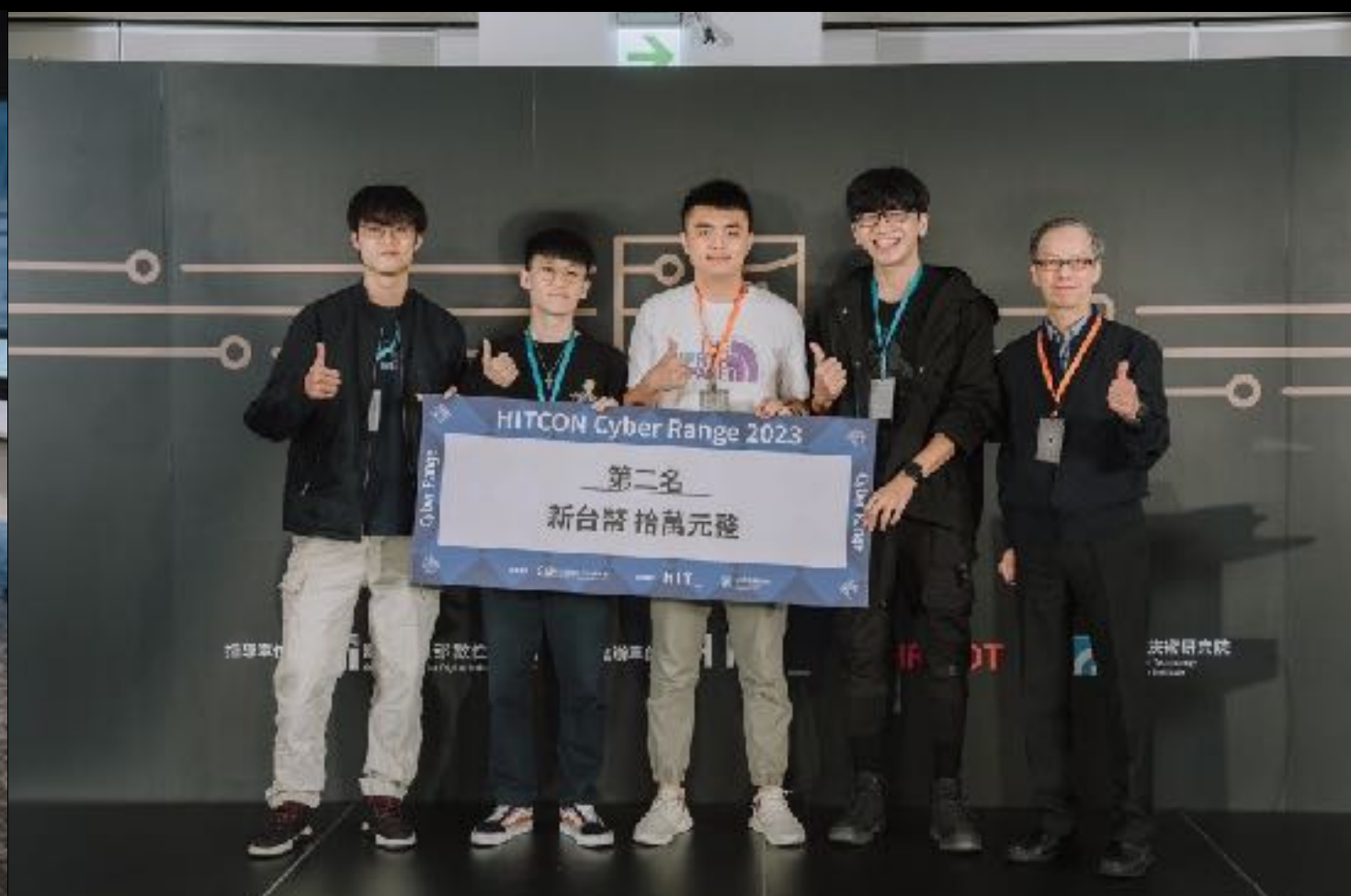
Firewall configuration entry should follow this format (one entry per line): `add chain=forward src-address=<src_address> dst-address=<dst_address> protocol=<protocol> src-port=<sorted_src_ports> dst-port=<sorted_dst_ports> action=<action> comment=<reason>`

Attachment: [hcr_2024_audit_inconsistency.tgz](#)

Attachment SHA256:

`b8e170fc30abd721c5309a09a6efc170e5c48810ebdb06ec5dc4f6e72b988eeb`

HITCON Cyber Range 2023



Rank	Team	Score	Last Solved Time
1	Con Ranger	0	
2	新創博覽會	0	
3	One4All	0	
4	綠巨人	0	
5	石壁守護者	0	
6	how2root (X)	0	
7	DefThreat	0	
8	loggol	0	
9	Armed Security	0	
10	GH team	0	
11	OTS	0	
12	無想不到隊	0	
13	Blue MURPHY	0	

HIT

HITCON Cyber Range 2024



- **更多元的資安事件，真實的模擬駭客入侵的情境**

物聯網產品的管理，往往是企業資安的重要破口，本屆競賽首次加入物聯網資安事件類題目，將資安事件模擬地更完整及多元。

- **提升國際影響力：促進國際與臺灣資安人才的交流與競爭機會**

全面開放國際企業參與，大幅提升台灣在全球資安領域的能見度和影響力。透過此競賽吸引全球資安人才和企業的關注，並為未來的國際合作奠定基礎。

- **參賽條件限縮，提升企業能掌握的務實藍隊技能**

瞄準企業內部的資訊安全團隊，讓企業更重視培養有能力的資安人才，並能及時應對企業層級的資安事件。



HITCON 2025 CYBER RANGE

角逐企業藍隊最強稱號！

QUAL

2025.07.18 FRI.
10:00 ~ 23:59, ONLINE

FINAL

2025.10.17 FRI.
10:00 ~ 16:00, ONSITE

ADVISOR

di 數位發展部 數位產業署
Administration for Digital Industries, moda

ORGANIZERS

HIT



工業技術研究院
Industrial Technology
Research Institute

READY?



HIT

產業資安

資安產業

學術研究

專家

參與實戰演練

持續了解最新的安全威脅

紮實基本技能

新手

HITCON CISO Summit

PWN2OWN

DEFCON 發表

ACM CCS

S&P

Bug Bounty Program

HITCON CTF 戰隊

BlackHat 發表

HITCON 發表

USENIX

HITCON Cyber Range

資安公司實習

DEFCON Village

國際會議發表

DEVCORE

T5

TRAPA

TXOne

奧義學院

Kernel CTF

SECCON CTF

Google CTF

頂尖 CTF

DEFCON CTF

HITCON CTF

ICC / ACSC CTF

HITCON Defense

HITCON Enterprise

CYBERSEC

HITCON Community

HITCON Defense

OSCP

Pwn.College

Pwnable.tw

資安相關科系

國家資通安全研究院培訓課程

全國技能競賽

金盾獎

神盾盃

HITCON Training

HITCON ZeroDay

TWCERT/CC
台灣漏洞揭露平台 (TVN)

AIS3 EOF

中山資安所

台大資安所

台科資安所

交大資安所

清大資安所

CyberDefenders

台灣好厲駭

AIS3

HITCON Hackdoor

My First CTF

TSC CTF

HITCON KB

HITCON Girls

AIS3 Junior

女媧思

THJCC CTF

學生社團

逢甲黑客社

Balsn

BambooFox

Beef Soup

NISRA

THJCC

TSC

AIS3社團補助

HITCON 社群補助

HIT_

工商時間

社團法人台灣駭客協會
ASSOCIATION OF
HACKERS IN TAIWAN

HIT

HITCON 2025

2025 年 08 月 15 日 - 2025 年 08 月 16 日 @ 中央研究院

Perimeter Security is Dead, Long Live Resilience

自 HITCON 2018 「Transforming: Cybersecurity and Resilience」以來，Resilience 再次成為焦點。近年來，俄烏戰爭、海底電纜破壞等事件不斷發生，顯示除了資訊安全，**通訊安全** 亦至關重要，特別是海底電纜、低軌衛星等基礎設施，這些議題為 Resilience 帶來了新的挑戰與討論方向。

此外，這一主題也與歐盟推動的《Cyber Resilience Act》相呼應。對於大量生產消費電子產品的台灣而言，如何在產品開發流程中導入 **Secure-by-Default** 的概念，將資安內建於設計之中，而非事後補救，將是值得深入探討的關鍵課題。



HITCON 2025 Call for Paper

Perimeter Security is Dead, Long Live Resilience

徵稿截止：2025 年 6 月 8 日 任意時區

審稿完成：2025 年 6 月 22 日（AI 審稿助理流程將優先進行審稿），2025 年 6 月 29 日

**HITCON X
COSCUP 資安軌**

AI 審稿助理



	7 月	8 月		9 月	10 月		11 月	12 月
會議活動		Community 台灣駭客年會社群場 8/15-8/16	Enterprise 台灣駭客年會企業場 8/15-8/16		CISO Summit 資安長高峰會			
競賽	HITCON CTF	Cyber Range Quals			Cyber Range 企業藍隊競賽 10/17	CTF 交流 賽 10/17, 10/18		
教育訓練	Training							
社群	HITCON GIRLS、社群補助計畫、海外補助計畫							
平台	ZeroDay, KnowledgeBase							

HIT_

社團法人台灣駭客協會
ASSOCIATION OF
HACKERS IN TAIWAN

會員招募中！



Q&A

謝謝聆聽！歡迎聯繫我們

+886-2-2700-0073
hacker.org.tw