

# Introduction to CTF

Ice1187

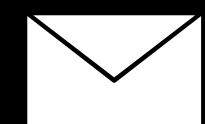
# Speaker

黃俊嘉 (Ice1187)

- ▶ Master's student at NTU CSIE NSLab
- ▶ Member of Balsn CTF Team
- ▶ Member of UNDEFINED
- ▶ Intern Researcher at CyCraft
- ▶ Speaker of CyberSec, SECCON



<https://github.com/Ice1187>



[hcc001202@gmail.com](mailto:hcc001202@gmail.com)

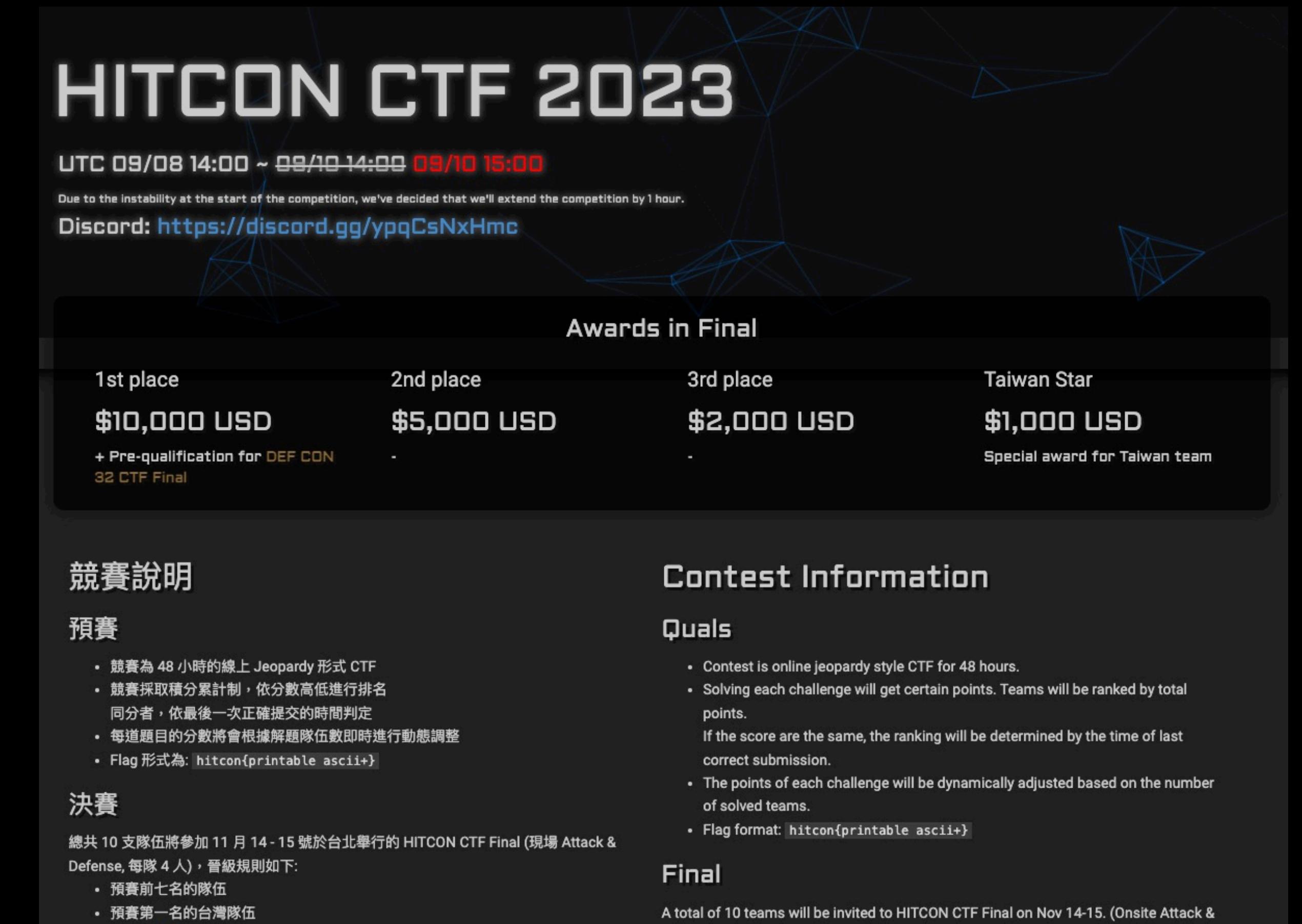


# Course Info

- 簡報連結：<https://github.com/lce1187/My-Slides>
- 練習平台：<https://github.com/lce1187/My-CTF-Challenges>

# 大綱

- 什麼是 CTF
- CTF 五大領域
- 自主學習資源介紹
- 從 CTF 學習資安的優點與缺點
- CTF 與資安實務的關係
  - 資安實務概...概覽



**HITCON CTF 2023**

UTC 09/08 14:00 ~ 09/10 14:00 **09/10 15:00**

Due to the instability at the start of the competition, we've decided that we'll extend the competition by 1 hour.

Discord: <https://discord.gg/ypqCsNxHmc>

**Awards in Final**

| 1st place                                    | 2nd place   | 3rd place   | Taiwan Star                   |
|--|-------------|-------------|-------------------------------|
| \$10,000 USD                                 | \$5,000 USD | \$2,000 USD | \$1,000 USD                   |
| + Pre-qualification for DEF CON 32 CTF Final | -           | -           | Special award for Taiwan team |

**Contest Information**

**Quals**

- Contest is online jeopardy style CTF for 48 hours.
- Solving each challenge will get certain points. Teams will be ranked by total points.
- If the scores are the same, the ranking will be determined by the time of last correct submission.
- The points of each challenge will be dynamically adjusted based on the number of solved teams.
- Flag format: hitcon{printable ascii+}

**Final**

A total of 10 teams will be invited to HITCON CTF Final on Nov 14-15. (Onsite Attack &

**競賽說明**

**預賽**

- 競賽為 48 小時的線上 Jeopardy 形式 CTF
- 競賽採取積分累計制，依分數高低進行排名  
同分者，依最後一次正確提交的時間判定
- 每道題目的分數將會根據解題隊伍數即時進行動態調整
- Flag 形式為: hitcon{printable ascii+}

**決賽**

總共 10 支隊伍將參加 11 月 14 - 15 號於台北舉行的 HITCON CTF Final (現場 Attack & Defense, 每隊 4 人)，晉級規則如下:

- 預賽前七名的隊伍
- 預賽第一名的台灣隊伍

# 聲明

本課程目的在提升學員對資安產業之認識及資安實務能力。本課程所授與的知識和技巧僅做為資安實務教育訓練目的。

所有課程學習內容應於雙方知情、同意且合法的情況下進行實作和練習，並且不得從事非法攻擊或違法行為，以免受到法律制裁。請勿利用所習得之技術從事非法或惡意的攻擊及入侵行為！

# 刑法：妨礙電腦使用罪

## 第三十六 章 妨害電腦使用罪

**第 358 條** 無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

**第 359 條** 無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

**第 360 條** 無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

**第 361 條** 對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。

**第 362 條** 製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

**第 363 條** 第三百五十八條至第三百六十條之罪，須告訴乃論。

## 不滿分手後被刪好友 竟變更前女友IG、FB密碼判拘役30日



A+



不滿分手後被刪好友，男子竟換掉前女友IG、FB、email密碼讓她無法登入。圖為苗栗地院。（資料照）

2023/08/20 13:58

〔記者蔡政珉／苗栗報導〕男女感情糾紛鬧上法院又一樁！苗栗縣曾姓女子與前男友鮑男分手後，曾女刪除鮑男臉書好友，但引發鮑男不滿，竟在家中使用電腦變更曾女常使用的社群軟體IG、FB與電子信箱密碼，導致曾女無法登入使用。而鮑男也曾於通訊軟體恐嚇曾女，經苗栗地院法官審理後，認定鮑男涉妨害電腦使用罪處拘役30日，如易科罰金，以1000元折算1日；涉恐嚇危害安全罪，處罰金6000元，如易服勞役，以1000元折算1日。

Src: <https://news.ltn.com.tw/news/society/breakingnews/4401911>

## 搶太妍門票僅須4秒！警破獲首宗AI搶票黃牛 逮30歲台大畢業工程師



A+



周嫌被移送法辦。（記者邱俊福翻攝）

2023/09/06 16:00

〔記者邱俊福／台北報導〕刑事局偵九大隊第二隊在文創產業發展法上路後，破獲首宗AI搶票黃牛案，發現嫌犯30歲周姓男子為台大資訊工程研究所高材生，自己撰寫搶票的AI程式，接訂單搶熱門演唱會門票牟利，已長達5年之久，修法後仍持續搶票，以「太妍演唱會」最夯。落網後，周嫌則表達知道有修法，但認為只是代購，自己並無不法。

Src: <https://news.ltn.com.tw/news/society/breakingnews/4419771>

# 什麼是 CTF？

# CTF (Capture The Flag)

- Capture The Flag 名稱源自西方傳統運動
- 資訊安全領域的攻防競賽多被稱為 CTF
- 多數 CTF 目標在於攻陷有漏洞的系統，  
取得系統中的 flag
- 象徵取得機密資訊或系統控制權

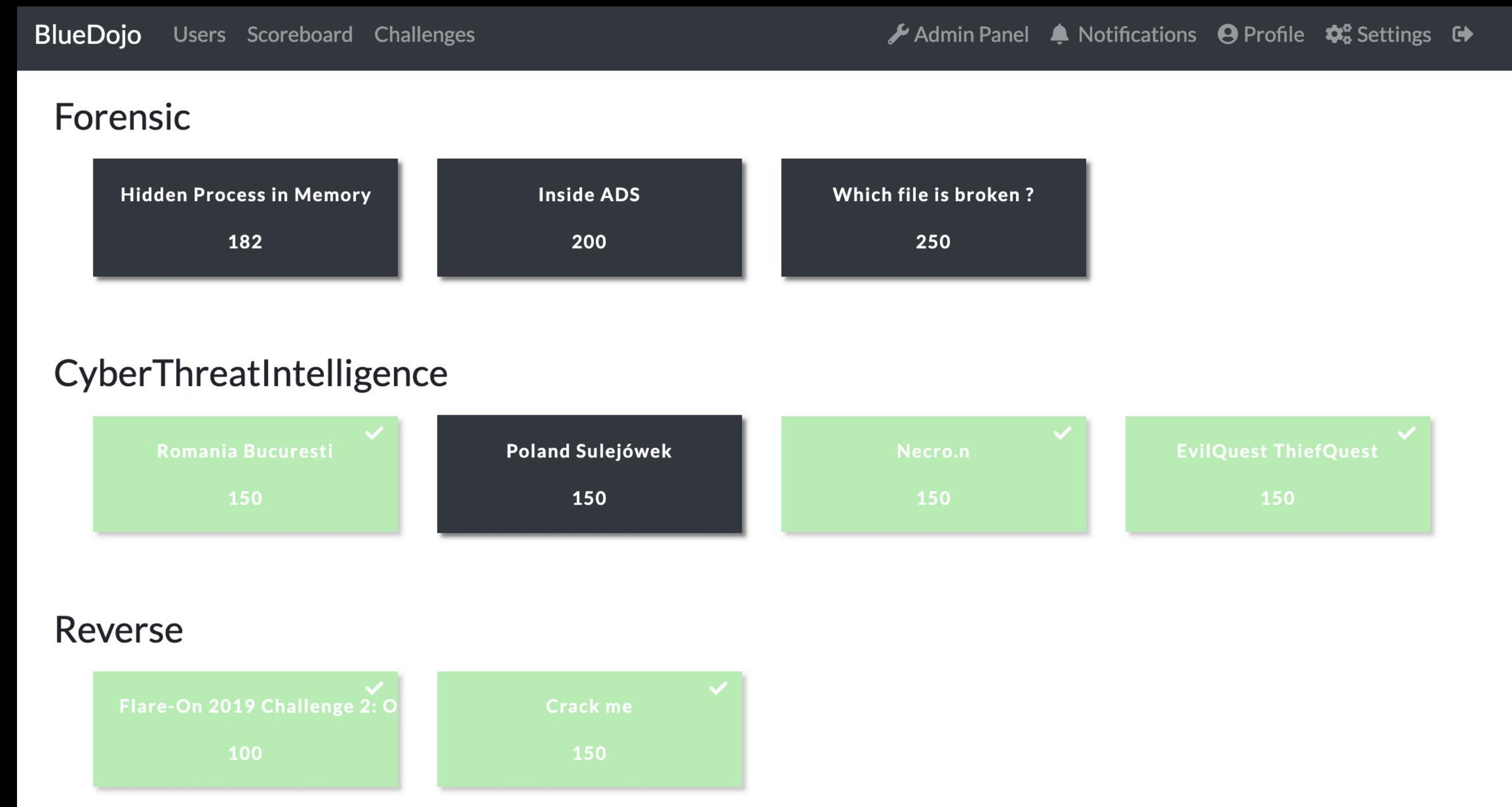


Image Src: <https://www.topendsports.com/sport/list/capture-the-flag.htm>

FLAG{Ld\_Pr3L0aD\_15\_E4sy!!!}

# CTF 的類型

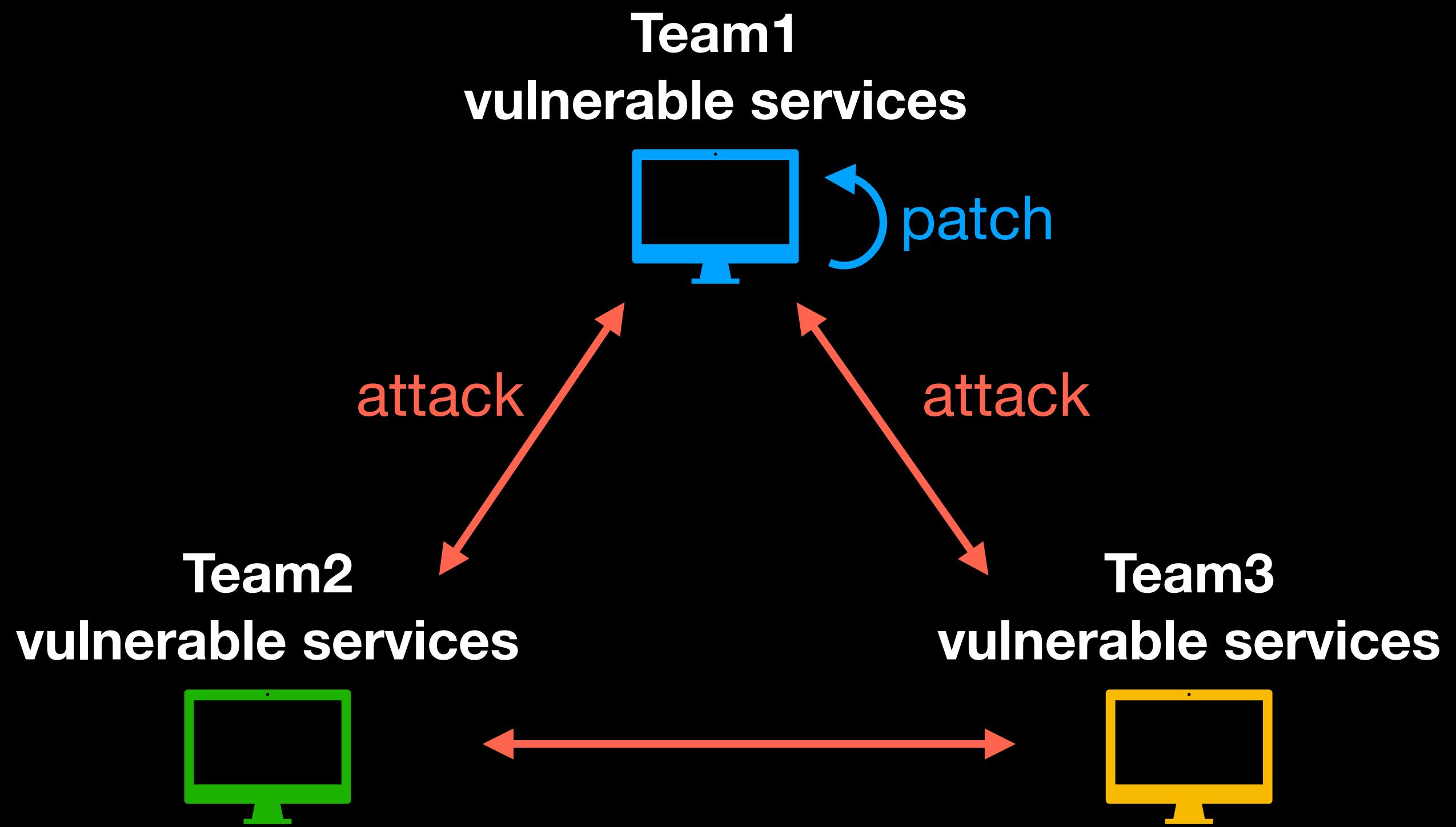
- Jeopardy 解題
- Attack & Defense
- King of Hill
- Live CTF



Img Src: <http://bluedojo.tw/challenges>

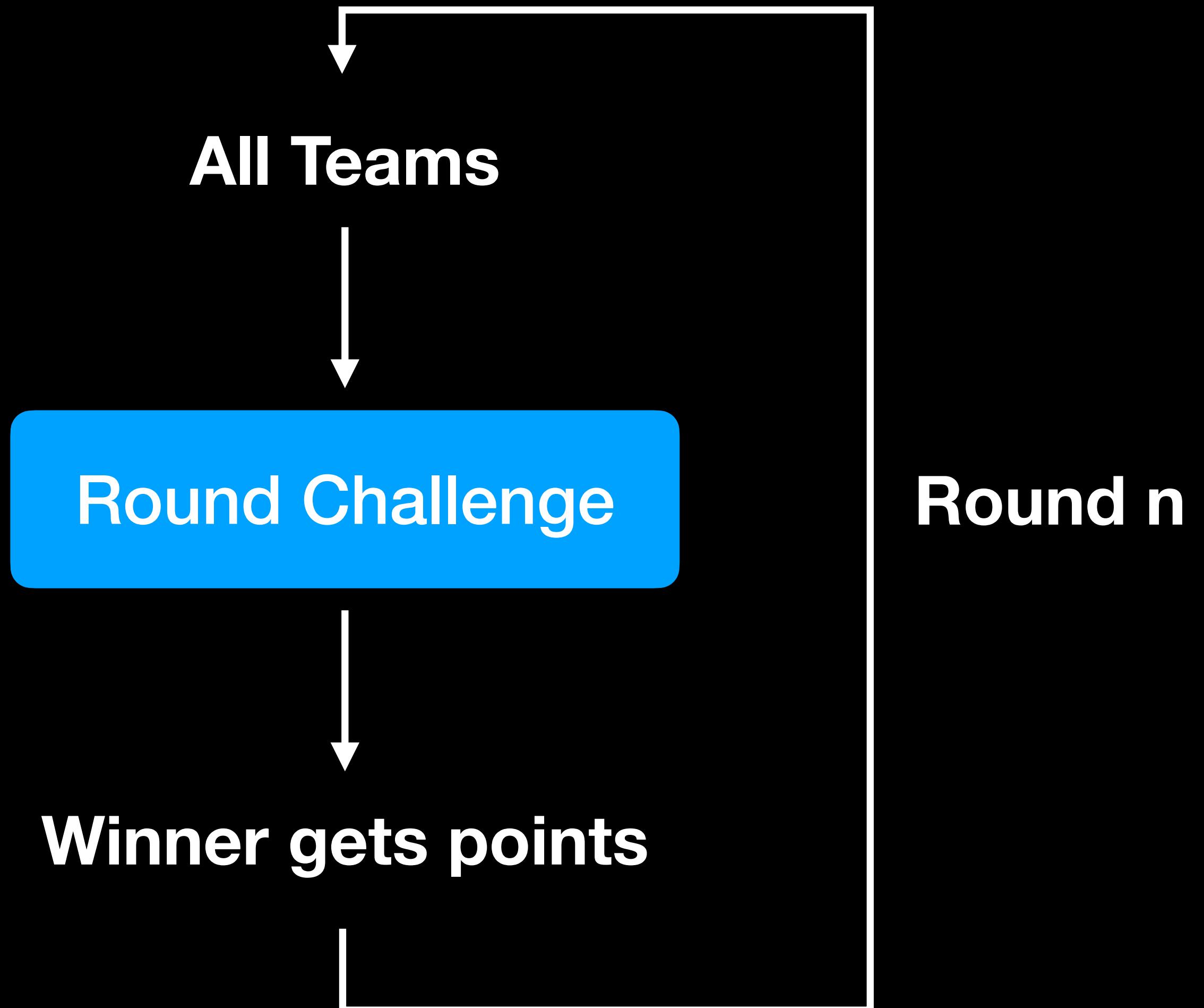
# CTF 的類型

- Jeopardy
- **Attack & Defense 攻防**
- King of Hill
- Live CTF



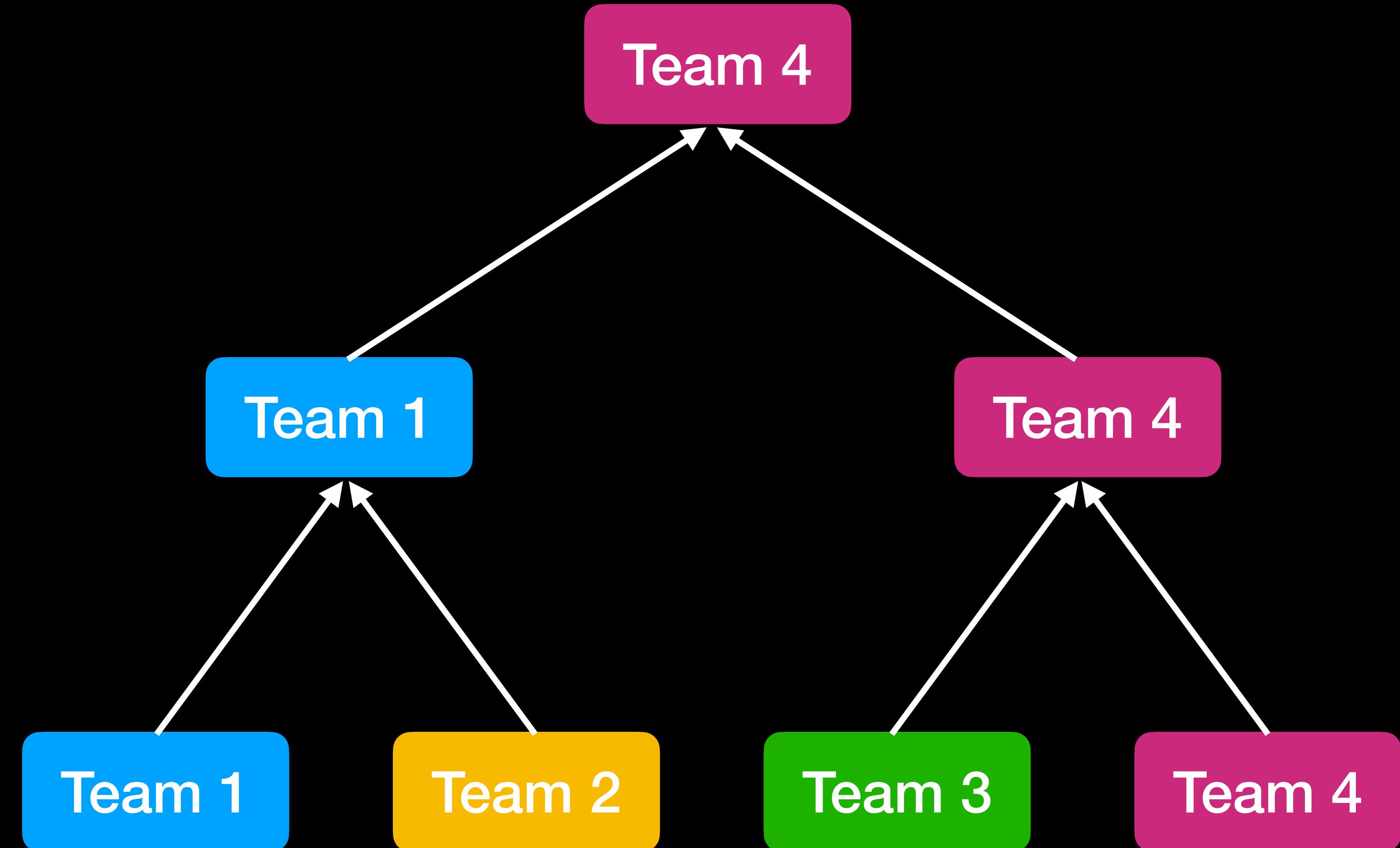
# CTF 的類型

- Jeopardy
- Attack & Defense
- King of Hill 爭奪
- Live CTF



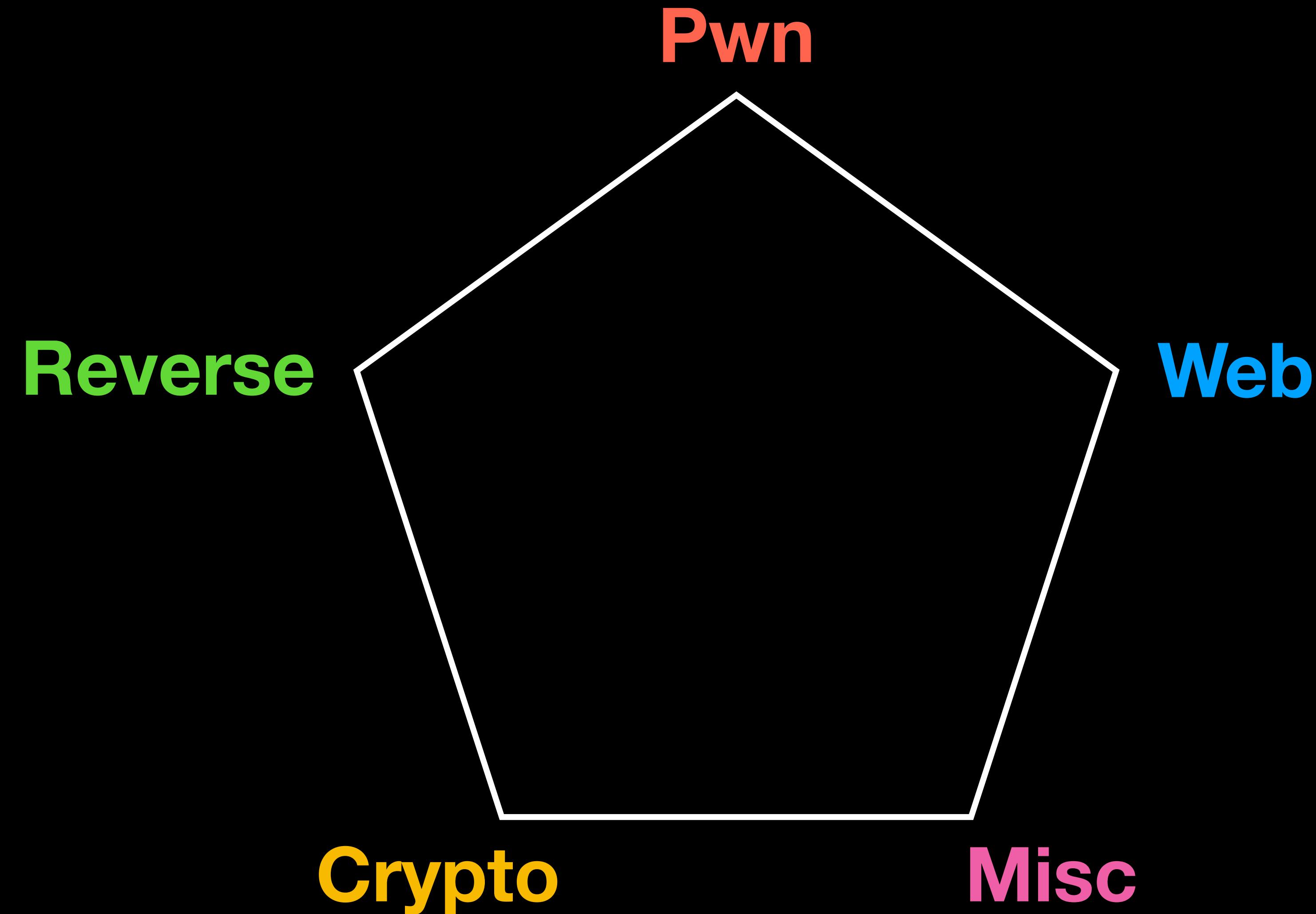
# CTF 的類型

- Jeopardy
- Attack & Defense
- King of Hill
- Live CTF 淘汰



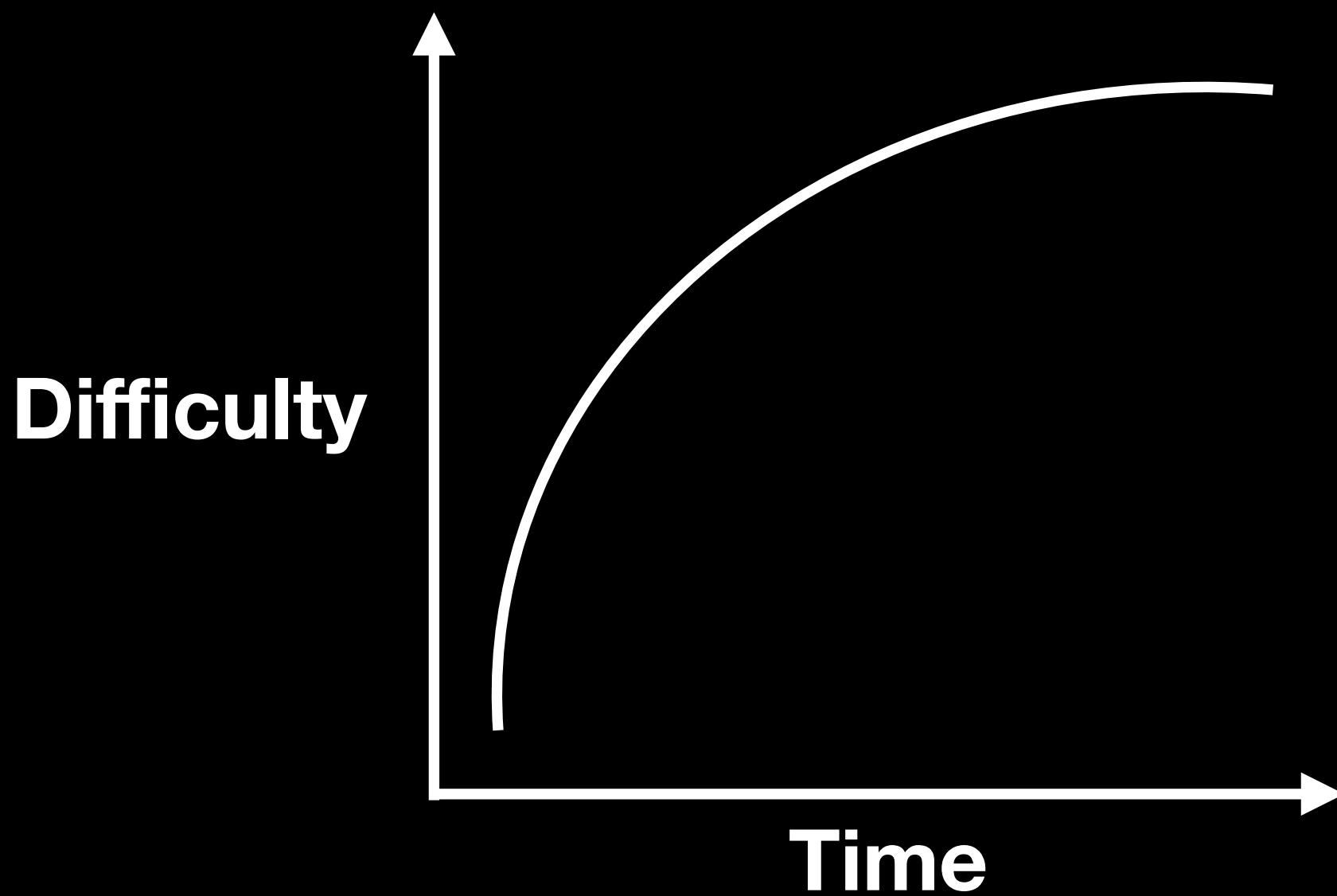
# CTF 五大領域

# CTF 五大領域



# Pwn 漏洞利用

- 題目：具有漏洞的程式 (執行檔、Android app、kernel driver、firmware)
- 目標：找到並利用漏洞，最終取得任意程式碼執行
- 背景知識：組合語言、作業系統運作原理、檔案格式、記憶體管理機制...

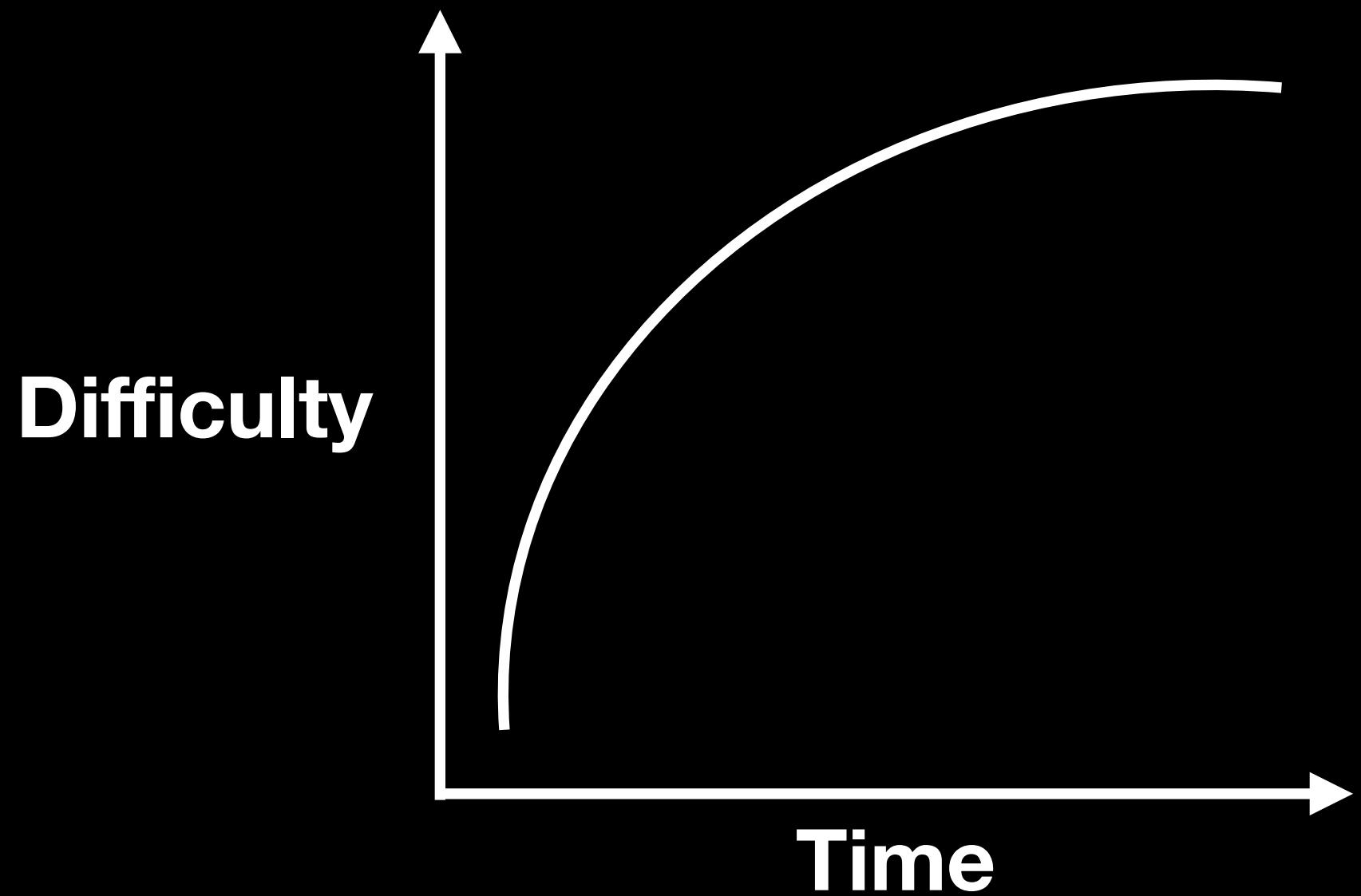


```
1 #include <stdio.h>$
2 #include <stdlib.h>$
3 #include <string.h>$
4 $  
5 #define FLAG "FLAG{gets_is_not_safe_at_all!!!}"$  
6 $  
7 int main(void) {$
8     char msg[40];$  
9 $  
10    scanf("%s", msg);$  
△    gets(msg);$  
12    printf("Echo: %s\n", msg);$  
13 $  
14    printf("Get good. Try harder.\n");$  
15 $  
16    return 0;$  
17 }$  
18 $  
19 void win() { printf("Flag: %s\n", FLAG); }$
```

```
ice1187@ice1187-lab:/tmp$ cat solve.py
with open('payload', 'wb') as f:
    f.write(b'A'*48 +
            b'B'*8 +
            (0x4011f6).to_bytes(8, 'little'))
ice1187@ice1187-lab:/tmp$ python3 solve.py ; ./pwn < payload
Echo: AAAAAAAAAAAAAAAAAAAAAAAAABBBBBBBB?@
Get good. Try harder.
Flag: FLAG{gets_is_not_safe_at_all!!!}
Segmentation fault (core dumped)
```

# Reverse 逆向分析

- 題目：具有惡意/複雜行為的程式
- 目標：了解程式的行為，並根據其行為取得 flag
- 背景知識：組合語言、加解殼、反混淆、anti-debug、檔案格式...



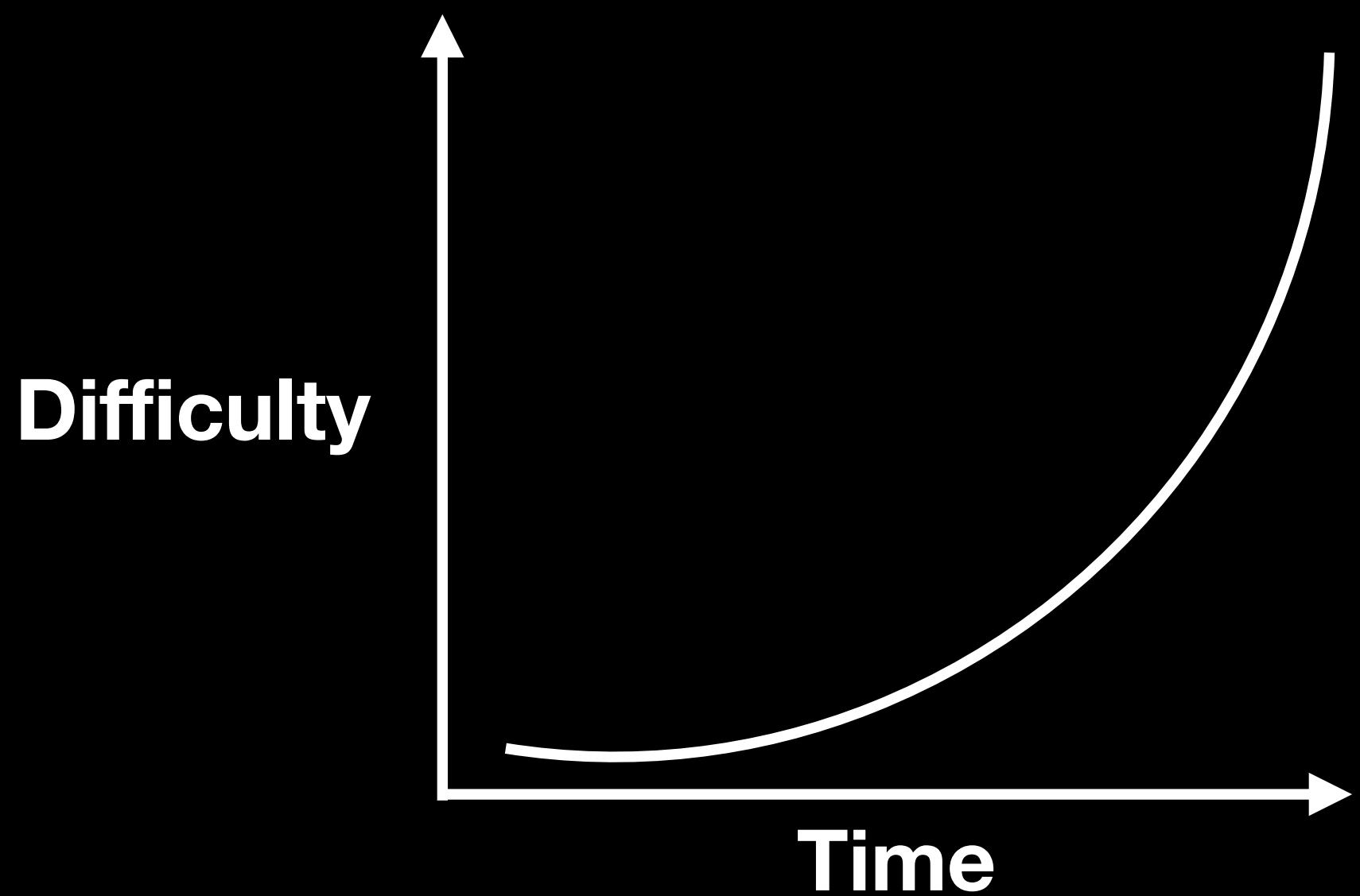
```
lea    rax, byte_20F0
mov    [rbp+enc_flag], rax
lea    rax, a127001 ; "127.0.0.1"
mov    [rbp+host], rax
mov    [rbp+port], 2BB3h
mov    edx, [rbp+port]
mov    rax, [rbp+host]
mov    esi, edx      ; port
mov    rdi, rax      ; host
call   socket_connect
mov    [rbp+sockfd], eax
mov    rdx, [rbp+enc_flag]
lea    rax, [rbp+flag]
mov    rsi, rdx      ; flag
mov    rdi, rax      ; buf
call   decode_flag
mov    rdx, [rbp+flag]
mov    eax, [rbp+sockfd]
mov    rsi, rdx      ; msg
mov    edi, eax      ; sockfd
call   send_msg
lea    rdi, s         ; "Message sent."
call   _puts
mov    edi, 1         ; seconds
call   _sleep
mov    rax, [rbp+flag]
mov    rdi, rax      ; ptr
call   _free
mov    eax, [rbp+sockfd]
mov    edi, eax      ; fd
call   _close
```



```
1 int __cdecl main(int argc, const char **argv, co
2 {
3     int sockfd; // [rsp+1Ch] [rbp-24h]
4     char *flag; // [rsp+20h] [rbp-20h] BYREF
5     char *enc_flag; // [rsp+28h] [rbp-18h]
6     char *host; // [rsp+30h] [rbp-10h]
7     unsigned __int64 v8; // [rsp+38h] [rbp-8h]
8
9     v8 = __readfsqword(0x28u);
10    enc_flag = byte_20F0;
11    host = "127.0.0.1";
12    sockfd = socket_connect("127.0.0.1", 11187);
13    decode_flag(&flag, byte_20F0);
14    send_msg(sockfd, flag);
15    puts("Message sent.");
16    sleep(1u);
17    free(flag);
18    close(sockfd);
19    return 0;
20 }
```

# Web 網站

- 題目：具有漏洞的網站
- 目標：找到並利用漏洞，最終取得網站管理權限 / 任意程式碼執行
- 背景知識：前/後端框架運作原理、資料庫管理系統、通訊協定...





Connect with friends and the world around you on Facebook.

please\_help\_me\_to\_hack\_fb\_account

Password

Log In

[Forgot password?](#)

[Create new account](#)

[Create a Page](#) for a celebrity, brand or business.

# SQL Injection 101

1. 登入檢查程式碼

```
SELECT * FROM users where name="{USER}" and pswd="{PASSWORD}"
```

2. 駭客輸入

```
USER=admin, PASSWORD=" OR "1"="1
```

3. 登入檢查程式碼

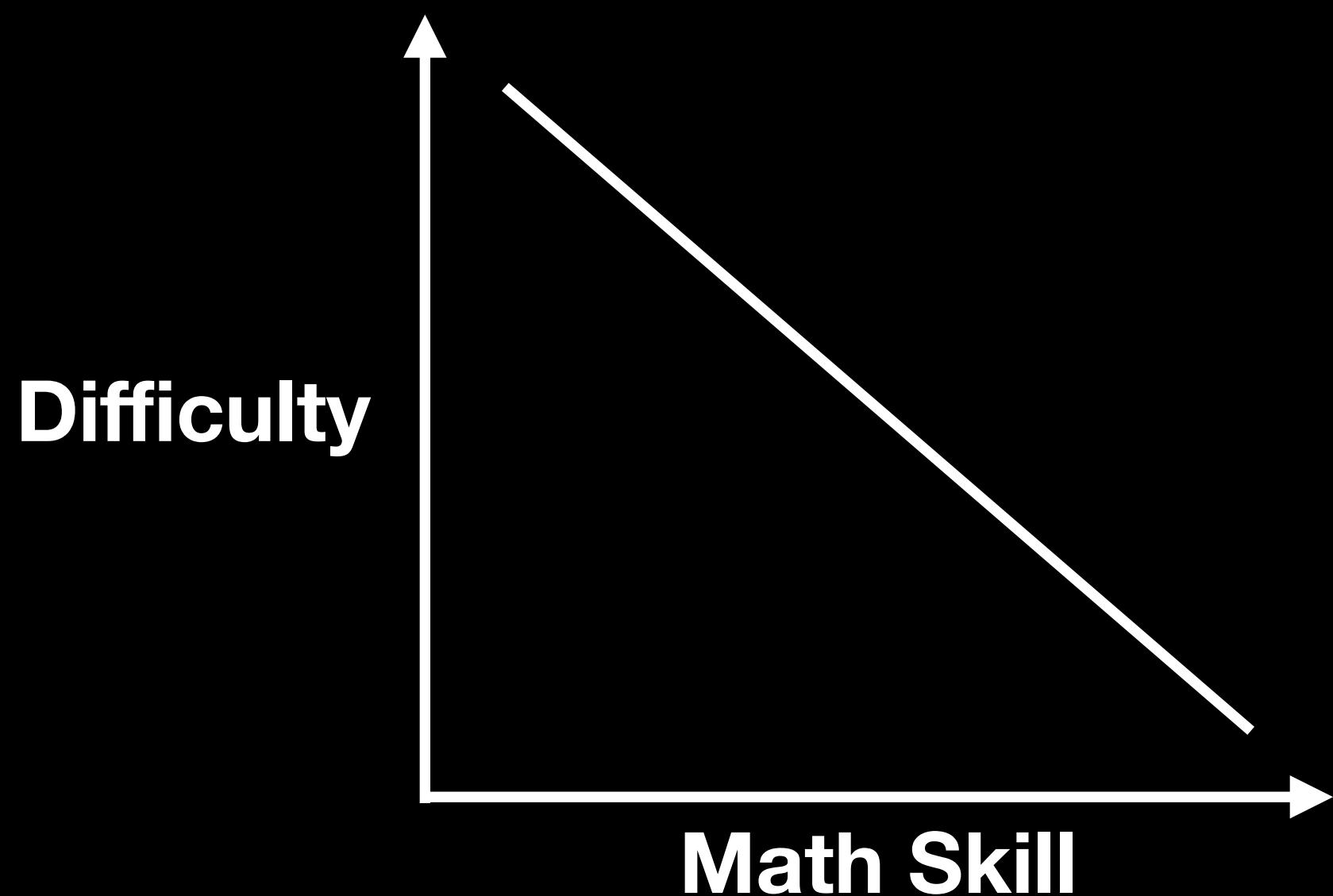
```
SELECT * FROM users where name="admin" and pswd="" OR "1"="1"
```

4. 成功登入 

```
pswd="" OR "1"="1"
```

# Crypto 密碼學

- 題目：不安全的密碼學加密系統實作
- 目標：找到加密機制的弱點，解密訊息
- 背景知識：密碼學原理、離散數學、程式語言行為、硬體運作機制...



|     |         |                       |
|-----|---------|-----------------------|
| "a" | decrypt | Failed, time: 0.00257 |
| "b" | decrypt | Failed, time: 0.00231 |
| "c" | decrypt | Failed, time: 0.00242 |
| "d" | decrypt | Failed, time: 0.00198 |
| "e" | decrypt | Failed, time: 0.00235 |
| "f" | decrypt | Failed, time: 0.00267 |

|     |         |   |
|-----|---------|---|
| "a" | decrypt | Failed, time: 0.00257                       |
| "b" | decrypt | Failed, time: 0.00231                       |
| "c" | decrypt | Failed, time: 0.00242                       |
| "d" | decrypt | Failed, time: 0.00198 (significant smaller) |
| "e" | decrypt | Failed, time: 0.00235                       |
| "f" | decrypt | Failed, time: 0.00267                       |

# Misc 其他

- 鑑識 Forensics
- 硬體 Hardware
- 區塊鏈 Blockchain
- 隱寫術 Stegnography
- 演算法 Algorithm
- ...

# 自主學習資源介紹

# 台灣資安 / CTF 學習資源整理

- Better to have: English reading, a little C/C++ programming、a little Python
- [Ice1187/TW-Security-and-CTF-Resource](https://github.com/Ice1187/TW-Security-and-CTF-Resource)
  - 線上自學教材
  - CTF 競賽 & Wargame
  - 營隊與培訓課程
  - 活動
  - 社團、社群、獎學金、實習...



<https://github.com/Ice1187/TW-Security-and-CTF-Resource>

# 線上自學教材

- Pwn : 臺大 計算機安全 – Pwn by Yuawn
- Web : How to Hack Websites by splitline
- Reverse : 交大 程式安全 – Rev by LJP-TW
- Crypto : Crypto Course by oalieno
- 大學課程 : 台師大 資安攻防演練

# CTF 競賽 & Wargame

簡單

## CTF 競賽 (每年一次)

1. MyFirstCTF / 寻找資安女婕思
2. AIS3 pre-exam
3. AIS3 EOF
4. Balsn CTF / TSJ CTF
5. HITCON CTF
6. DEFCON CTF

困難

## Wargame (常駐)

- picoCTF / picoGym
- LoTux CTF
- SCIST CTF
- CTFTime
- pwnable.tw
- Hackme CTF

# 營隊與培訓課程

入門

教育部資安人才培育計畫

社群

- 高中職生資安研習營
- AIS3 Junior 新型態高中職資安課程
- AIS3 新型態資安實務主題課程
- 臺灣好厲駭 高階資安人才培訓計畫
- SCIST 資訊安全課程
- TeamT5 Security Camp 資安培訓營
- TDOH 資安功德院

高階

# 活動

- SITCON 學生資訊年會
  - 學生分享的資安議程
  - 認識社群、同好
  - 加入 / 組成社群
  - 投稿分享！
- HITCON 臺灣駭客年會
  - 專家分享最新漏洞、APT 追蹤、攻防技術
  - Hacking 101
  - 認識同好、加入社群
  - 大地遊戲
  - 投稿

# 每月活動整理

- TDOHacker 每月資安、社群活動整理

## 2023年 9月份資安、社群活動分享



2023年 9月份資安、社群活動分享

Product Manager Happy Hour & Networking Event 2023/9/2  
<https://www.meetup.com/international-product-management-meetup-group/events/295580305/>

Just a chat - with no Expectations 2023/9/2  
<https://www.meetup.com/taipei-%E6%9A%97%E5%8F%B7%E9%80%9A%E8%B2%A8-cryptocurrency-meetup/events/295419679/>

PyCon TW 2023 2023/9/2 ~ 2023/9/3  
<https://tw.pycon.org/2023/zh-hant/registration/tickets>

Coffee & Code 2023/9/3  
<https://www.meetup.com/innovate-taiwan/events/295754118/>

SHALLOW - 2023 Summer Workshop 2023/9/4  
<https://project4by55.kktix.cc/events/shallow-2023summer>

Hugging Face : Feature Extraction 2023/9/5  
<https://www.meetup.com/tensorflow-user-group-taipei/events/295006101/>

IR系列課程：惡意程式獵捕與網路封包探索 | ACW SOUTH數位產業署沙崙資安服務基地  
2023/9/6  
<https://ievents.iii.org.tw/EventS.aspx?t=0&id=2191>

**著作人**

- TDOHacker
- Unknown
- Unknown
- 爆肝網管

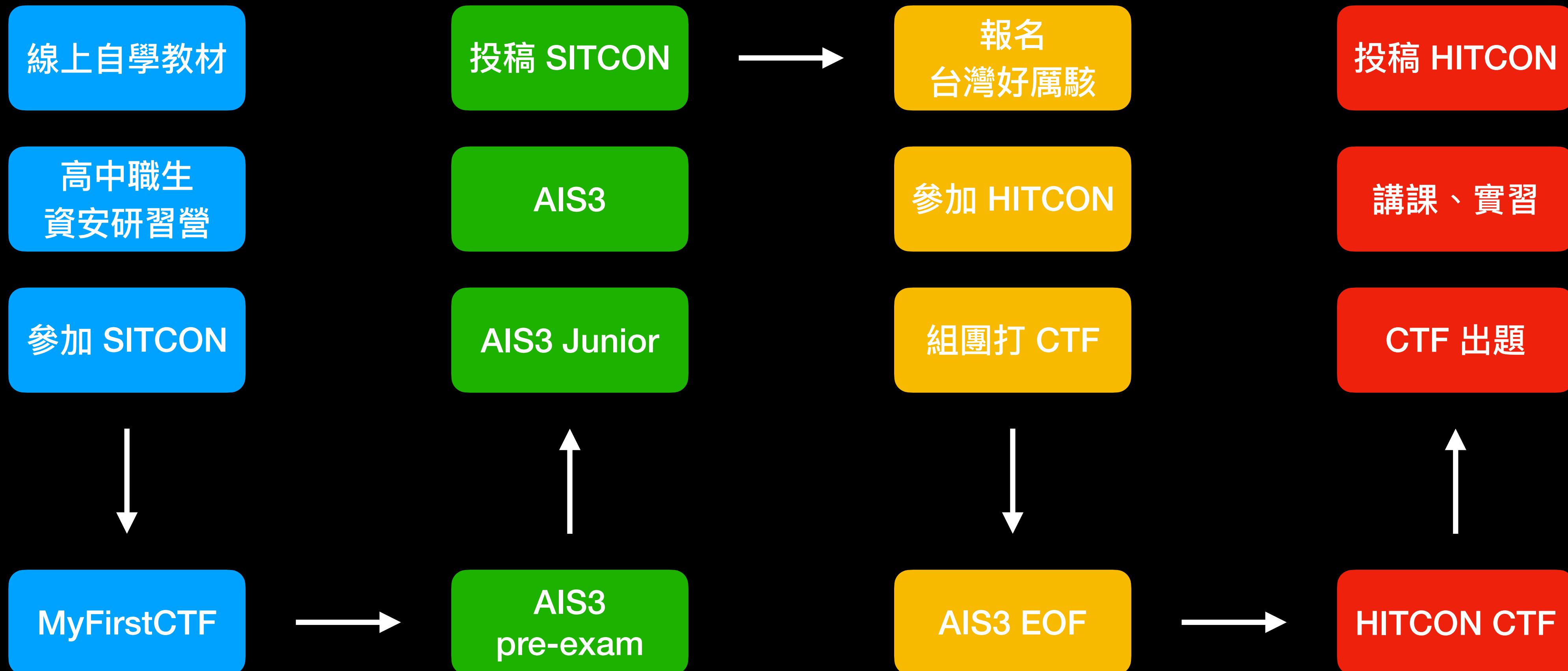
**文章列表**

- ▼ 2023 (8)
  - ▼ 9月 2023 (1)
    - 2023年 9月份資安、社群活動分享
  - 7月 2023 (1)
  - 6月 2023 (2)
  - 4月 2023 (1)
  - 3月 2023 (1)
  - 2月 2023 (1)
  - 1月 2023 (1)
- 2022 (12)
- 2021 (64)
- 2020 (64)
- 2019 (63)
- 2018 (81)
- 2017 (73)
- 2016 (44)
- 2015 (16)
- 2014 (28)

**標籤**

技術交流 (18) 活動分享 (120) 活動紀錄 (2) 資安新聞及事件週報 (282) About US (1) TDOH - PIPE (16)

# 其中一種可能的參與順序



# picoGym

- 由卡內基美濃大學和國際 CTF 戰隊 PPP 成立
- 給新手的入門 Wargame
- 線上學習資源 (英文)
- Teacher + Classroom 功能



# picoGym for Teacher

I am a:

 Learner    Teacher

**1 Get Started**   **2 Create a Classroom**   **3 Track Student Progress**

**Sign Up**

1. Sign up for an account for picoCTF.org. You will receive a confirmation email with a verification link.

[Sign Up](#)

2. Verify your account via the confirmation email.

**Get Connected**

**Discord Chat**

We welcome you to join our picoCTF community Discord server. This server is intended for general conversation around picoCTF, team recruitment for competitors, discussion about picoCTF open-source development, or casual chat. This server is **not** intended for competition challenge help, and will not be monitored by problem developers. Spoilers or flag sharing during competition will be grounds for removal.

We have a dedicated **#teachers-and-educators** channel to exchange ideas, share stories and collaborate in any other manner towards teaching cybersecurity more effectively to the next generation

[Request Discord invite](#)

[https://picoctf.org/get\\_started.html](https://picoctf.org/get_started.html)

# picoGym

picoGym Practice Challenges 總分 picoGym Score: 7440

Progress Tracker 各領域進度

Filters

Hide Solved  
 Show Bookmarked  
 Show Assigned

Search by Name

Category Filter 領域

- All Categories (330)
- Web Exploitation (52)
- Cryptography (57)
- Reverse Engineering (76)
- Forensics (57)
- General Skills (42)
- Binary Exploitation (46)
- Uncategorized

題目

| General Skills      | 5 points  | Cryptography        | 10 points | General Skills   | 10 points |
|---------------------|-----------|---------------------|-----------|------------------|-----------|
| Obedient Cat        |           | Mod 26              |           | Python Wrangling |           |
| 202,025 solves      | 89% ↗     | 168,661 solves      | 90% ↗     | 105,025 solves   | 62% ↗     |
| General Skills      | 10 points | Forensics           | 10 points | General Skills   | 15 points |
| Wave a flag         |           | information         |           | Nice netcat...   |           |
| 120,818 solves      | 88% ↗     | 81,473 solves       | 41% ↗     | 98,671 solves    | 88% ↗     |
| Reverse Engineering | 20 points | Binary Exploitation | 20 points | Web Exploitation | 20 points |
| Transformation      |           | Stonks              |           | GET aHEAD        |           |
| 39,079 solves       | 54% ↗     | 22,454 solves       | 57% ↗     | 61,459 solves    | 81% ↗     |
| Cryptography        | 20 points | General Skills      | 20 points | General Skills   | 20 points |

# 從 CTF 學習資安的優缺點

CTF 只是學習資安的其中一種方式，並不一定適合所有人。  
除了 CTF 之外，還有很多入門資安的方式。

*- Ice1187, 2023*

# 其他入門資安的方式

- 讀書會
- 遊戲外掛
- 軟體破解
- 自主研究
- 二轉



# CTF 的優點

- 實際動手操作
- 加深印象
- 培養實作能力
- 競賽形式
- 有趣
- 競爭強化自主學習動機
- 獎勵、回饋
- 好的題目
- 認識真實漏洞的發生
- 學習系統運作原理
- 許多知識來自解題過程
- 閱讀程式碼
- 學習使用、開發工具

|                           |                       |     |                        |
|---------------------------|-----------------------|-----|------------------------|
| Malicious File            | EndpointThreatHunting | 172 | July 31st, 2:13:53 AM  |
| RTLO Malware              | EndpointThreatHunting | 50  | July 31st, 2:08:32 AM  |
| Start Attack              | EndpointThreatHunting | 195 | July 31st, 1:51:32 AM  |
| Decode PowerShell Command | EndpointThreatHunting | 50  | July 30th, 10:28:39 PM |
| knock knock               | EndpointThreatHunting | 120 | July 30th, 9:27:47 PM  |
| The Uninvited             | EndpointThreatHunting | 50  | July 30th, 8:24:04 PM  |
| APT3 Password             | EndpointThreatHunting | 50  | July 30th, 6:31:39 PM  |
| Process 0xf18             | EndpointThreatHunting | 50  | July 30th, 6:26:46 PM  |

為了分數從 18 點解到凌晨 2 點

# CTF 的缺點

- 無法涵蓋所有面向
  - 多過於注重攻擊
  - 物理限制
  - 競賽形式
  - 競爭意識過強
  - 熬夜解題有礙身心健康
  - 有時間限制
- 壞的題目
  - 重複、無意義的編碼或隱寫術
  - 通靈
  - 不合理的設定
  - 必須使用特定、不知名工具
  - 與現實情況相去甚遠

# CTFs are Awesome/Terrible!



<https://youtu.be/L2C8rVO2lAg?si=LlnXZN0QZcIISTLH>

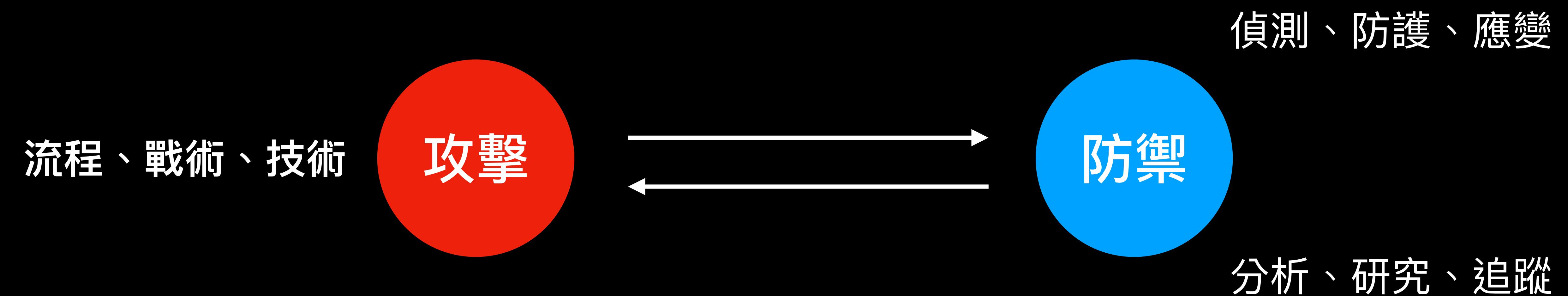


# 好題目 v.s. 糟題目

🚧 Working in Progress... 🚧

# CTF 與資安實務的關係

# 資安實務概覽



# 攻擊戰術與技術 – ATT&CK Matrix

- 由 MITRE 所提出的攻擊戰術與技術框架
- 建立具體、統一、實務、泛用的攻擊行為描述
- 相較 Cyber Kill Chain 更具體與實務導向
- 參考自 ATT&CK 101 blog post

ATT&CK®

Img Src: <https://attack.mitre.org/>

各種平台

# Windows Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the Windows platform.

[View on the ATT&CK® Navigator](#)
[Version Permalink](#)
[layout: side ▾](#)
[show sub-techniques](#)
[hide sub-techniques](#)
[help](#)
**戰術 Tactic**

| Initial Access                      | Execution                             | Persistence                              | Privilege Escalation                    | Defense Evasion                       | Credential Access            | Discovery                                 | Lateral Movement                     | Collection                             | Command and Control                        | Exfiltration                               |
|-------------------------------------|---------------------------------------|--|---|---------------------------------------|------------------------------|---|--------------------------------------|--|--|--|
| 9 techniques                        | 10 techniques                         | 18 techniques                            | 13 techniques                           | 34 techniques                         | 16 techniques                | 26 techniques                             | 9 techniques                         | 15 techniques                          | 16 techniques                              | 8 techniques                               |
| Drive-by Compromise                 | Command and Scripting Interpreter (5) | Account Manipulation (2)                 | Abuse Elevation Control Mechanism (1)   | Abuse Elevation Control Mechanism (1) | Adversary-in-the-Middle (3)  | Account Discovery (3)                     | Exploitation of Remote Services      | Adversary-in-the-Middle (3)            | Application Layer Protocol (4)             | Automated Exfiltration                     |
| Exploit Public-Facing Application   | Exploitation for Client Execution     | BITS Jobs                                | Access Token Manipulation (5)           | Access Token Manipulation (5)         | Brute Force (4)              | Application Window Discovery              | Internal Spearphishing               | Archive Collected Data (3)             | Communication Through Removable Media      | Data Transfer Size Limits                  |
| External Remote Services            | Inter-Process Communication (2)       | Boot or Logon Autostart Execution (10)   | BITS Jobs                               | Credentials from Password Stores (3)  | Debugger Evasion             | Browser Information Discovery             | Lateral Tool Transfer                | Audio Capture                          | Exfiltration Over Alternative Protocol (3) | Exfiltration                               |
| Hardware Additions                  | Native API                            | Boot or Logon Initialization Scripts (2) | Deobfuscate/Decode Files or Information | Exploitation for Credential Access    | Device Driver Discovery      | Domain Trust Discovery                    | Remote Service Session Hijacking (1) | Automated Collection                   | Data Encoding (2)                          | Exfiltration Over C2 Channel               |
| Phishing (3)                        | Scheduled Task/Job (2)                | Boot or Logon Initialization Scripts (2) | Direct Volume Access                    | Forced Authentication                 | File and Directory Discovery | File and Directory Discovery              | Remote Services (5)                  | Clipboard Data                         | Data Obfuscation (3)                       | Exfiltration Over Other Network Medium (1) |
| Replication Through Removable Media | Shared Modules                        | Browser Extensions                       | Domain Policy Modification (2)          | Forge Web Credentials (2)             | Group Policy Discovery       | Group Policy Discovery                    | Replication Through Removable Media  | Data from Information Repositories (1) | Dynamic Resolution (3)                     | Fallback Channels                          |
| Supply Chain Compromise (3)         | Software Deployment Tools             | Compromise Client Software Binary        | Create or Modify System Process (1)     | Execution Guardrails (1)              | Network Service Discovery    | Network Service Discovery                 | Data from Local System               | Encrypted Channel (2)                  | Exfiltration Over Physical Medium (1)      | Ingress Tool Transfer                      |
| Trusted Relationship                | System Services (1)                   | Create Account (2)                       | Domain Policy Modification (2)          | Exploitation for Defense Evasion      | Network Share Discovery      | Network Share Discovery                   | Data from Network Shared Drive       | Non-Application Layer Protocol         | Exfiltration Over Web Service (3)          | Multi-Stage Channels                       |
| Valid Accounts (3)                  | User Execution (2)                    | Create or Modify System Process (1)      | Escape to Host                          | Event Triggered Execution (12)        | Network Sniffing             | Network Sniffing                          | Data from Removable Media            | Scheduled Transfer                     | Scheduled Transfer                         |  |
|                                     | Windows Management Instrumentation    | Event Triggered Execution (12)           | Event Triggered Execution (12)          | Exploitation for Privilege Escalation | Hide Artifacts (9)           | Passport Policy Discovery                 |                                      |  |  |  |
|                                     |                                       | External Remote Services                 | Hijack                                  | Hijack Execution Flow (10)            | Hijack Execution Flow (10)   | Use Alternate Authentication Material (2) |                                      |  |  |  |

**技術 Technique**

# 駭客攻擊行動的一生



Src: [YouTube - 山道猴子的一生（上集）](#)

# 攻擊行動的一生：初始存取 & 執行

Dear Linda,

I hope this message finds you well. I have attached the Q3 accounting report for the IT department, which requires your prompt attention.

[Attachment: IT\_Q3\_Accounting\_Report.pdf]

Your timely review would be greatly appreciated.

Thank you kindly.

Sincerely,

| Initial Access                      | Execution                               |
|-------------------------------------|---|
| 9 techniques                        | 10 techniques                           |
| Drive-by Compromise                 | Command and Scripting Interpreter (0/5) |
| Exploit Public-Facing Application   | Exploitation for Client Execution       |
| External Remote Services            | Inter-Process Communication (0/2)       |
| Hardware Additions                  | Native API                              |
| Phishing (1/3)                      | Scheduled Task/Job (0/2)                |
| Spearphishing Attachment            |   |
| Spearphishing Link                  |   |
| Spearphishing via Service           |   |
| Replication Through Removable Media | Shared Modules                          |
| Supply Chain Compromise (0/3)       | Software Deployment Tools               |
| Trusted Relationship                | System Services (0/1)                   |
| Valid Accounts (0/3)                | Malicious File (1/2)                    |
| User Execution (1/2)                |   |
| Malicious Link                      |   |
| Windows Management Instrumentation  |   |

# 攻擊行動的一生：維持 & 提權

- 維持 Persistence

1. 註冊 scheduled task，定期執行惡意程式

2. 建立後門帳號

- 權限提升 Privilege Escalation

3. 利用漏洞將使用者提權至 Administrator

| Persistence<br>18 techniques          | Privilege<br>Escalation<br>13 techniques |
|---------------------------------------|--|
| Compromise                            | System Process (0/1)                     |
| Client Software                       |  |
| Binary                                |  |
| Create Account (0/2)                  |  |
| Create or Modify System Process (0/1) |  |
| Event Triggered Execution (0/12)      |  |
| Event Triggered Execution (0/12)      |  |
| External Remote Services              |  |
| Hijack Execution Flow (0/10)          |  |
| Hijack Execution Flow (0/10)          |  |
| Modify Authentication Process (0/6)   |  |
| Scheduled Task/Job (0/2)              |  |
| Office Application Startup (0/6)      |  |
| Pre-OS Boot (0/3)                     |  |
| Scheduled Task/Job (0/2)              |  |
| Valid Accounts (0/3)                  |  |

# 攻擊行動的一生：防禦規避

- 防禦規避 Defense Evasion

4. 將惡意程式設為隱藏檔案

5. 執行後刪除惡意程式

6. 關閉防毒軟體

7. 清除 Windows Event Log

| Defense Evasion<br>34 techniques     |                                |
|--------------------------------------|--------------------------------|
| Email Hiding Rules                   |                                |
| Hidden File System                   |                                |
| Hidden Files and Directories         |                                |
| Hidden Users                         |                                |
| Hide Artifacts (1/9)                 |                                |
| II                                   | Hidden Window                  |
| NTFS File Attributes                 |                                |
| Process Argument Spoofing            |                                |
| Disable or Modify System Firewall    |                                |
| Disable or Modify Tools              |                                |
| Disable Windows Event Logging        |                                |
| Downgrade Attack                     |                                |
| Impair Defenses (1/8)                |                                |
| II                                   | Impair Command History Logging |
| Indicator Blocking                   |                                |
| Safe Mode Boot                       |                                |
| Spoof Security Alerting              |                                |
| Clear Command History                |                                |
| Clear Mailbox Data                   |                                |
| Clear Network Connection History and |                                |
| Clear Persistence                    |                                |
| Indicator Removal (2/8)              |                                |
| II                                   | Clear Windows Event Logs       |
| File Deletion                        |                                |
| Network Share Connection Removal     |                                |
| Timestamp                            |                                |

# 攻擊行動的一生：憑證存取 & 橫向移動

- 憑證存取 Credential Access

8. 從作業系統取得密碼明文 / hash

- 探索 Discovery

9. 掃描系統上的帳號，內網中的網路服務、  
芳鄰、其他機器

- 橫向移動 Lateral Movement

10. 透過 RDP、WinRM，利用已取得的  
credential 移動至其他機器

| Credential Access<br>16 techniques             | Discovery<br>26 techniques        | Lateral Movement<br>9 techniques            |
|--|-----------------------------------|---|
| Adversary-in-the-Middle (0/3)                  | Account Discovery (0/3)           | Exploitation of Remote Services             |
| Brute Force (0/4)                              | Application Window Discovery      | Internal Spearphishing                      |
| Credentials from Password Stores (0/3)         | Browser Information Discovery     | Lateral Tool Transfer                       |
| Exploitation for Credential Access             | Debugger Evasion                  | Remote Service Session Hijacking (0/1)      |
| Forced Authentication                          | Device Driver Discovery           | Distributed Component Object M              |
| Forge Web Credentials (0/2)                    | Domain Trust Discovery            | Remote Desktop Protocol                     |
| Input Capture (0/4)                            | File and Directory Discovery      | SMB/Windows Admin Shares                    |
| Modify Authentication Process (0/6)            | Group Policy Discovery            | VNC   |
| Multi-Factor Authentication Interception       | Network Service Discovery         | Windows Remote Management                   |
| Network Sniffing                               | Network Share Discovery           | Replication Through Removable Media         |
| Multi-Factor Authentication Request Generation | Network Sniffing                  | Software Deployment Tools                   |
| Network Sniffing                               | Password Policy Discovery         | Taint Shared Content                        |
| OS Credential Dumping (0/6)                    | Peripheral Device Discovery       | Use Alternate Authentication Material (0/2) |
| Steal or Forge Authentication Certificates     | Permission Groups Discovery (0/2) |   |
| Steal or Forge                                 | Process Discovery                 |   |
|  | Query Registry                    |   |
|  | Remote System Discovery           |   |
|  | Steal or Forge                    |   |

# 攻擊行動的一生：蒐集 & 滲出

- 蒯集 Collection

11. 蒯集系統、SMB、Email、剪貼簿等資料

- 指揮與控制 Command & Control

12. 與攻擊者 server 連線，取得後續攻擊指令

- 滲出 Exfiltration

13. 將資料透過加密連線傳回攻擊者 server

| Collection<br>15 techniques              | Command and Control<br>16 techniques  | Exfiltration<br>8 techniques                 |
|--|---------------------------------------|--|
| Adversary-in-the-Middle (0/3)            | Application Layer Protocol (0/4)      | Automated Exfiltration (0/0)                 |
| Archive Collected Data (0/3)             | Communication Through Removable Media | Data Transfer Size Limits                    |
| Audio Capture                            | Data Encoding (0/2)                   | Exfiltration Over Alternative Protocol (0/3) |
| Automated Collection                     | Data Obfuscation (0/3)                | Exfiltration Over C2 Channel                 |
| Browser Session Hijacking                | Dynamic Resolution (0/3)              | Exfiltration Over Other Network Medium (0/1) |
| Clipboard Data                           | Encrypted Channel (0/2)               | Exfiltration Over Physical Medium (0/1)      |
| Data from Information Repositories (0/1) | Fallback Channels                     | Exfiltration Over Web Service (0/3)          |
| Data from Local System                   | Ingress Tool Transfer                 | Scheduled Transfer                           |
| Data from Network Shared Drive           | Multi-Stage Channels                  |  |
| Data from Removable Media                | Non-Application Layer Protocol        |  |
| Data Staged (0/2)                        | Non-Standard Port                     |  |
| Email Collection (0/3)                   | Protocol Tunneling                    |  |
| Input Capture (0/4)                      | Proxy (0/4)                           |  |
| Screen Capture                           | Remote Access Software                |  |
| Video Capture                            | Traffic Signaling (0/2)               |  |
|  | Bidirectional Communication           |  |
|  | Dead Drop Resolver                    |  |
|  | One-Way Communication                 |  |



Src: YouTube - 山道猴子的一生 (下集)



Working In Progress...

# Q & A