



Challenging from the Hacker's  
Perspective:

Penetration Testing Revealing  
Enterprise Security Vulnerabilities

Byron Wai



## \$ gonjk --help

- ~~Snacks Provider of BlackB6a~~
- Founding Member of BlackB6a
- Founding Member of HKUST Firebird CTF Team
- HITCON 2020 Speaker
- CISSP
- Pentester



```
$ blackb6a --help
```


Black Bauhinia (blackb6a)

- Best CTF team in Hong Kong (self-proclaimed)
- Top 20 CTF Team in CTFTIME

<https://b6a.black>

 @blackb6a

 @blackb6a

 /team/83678

[Home](#) / [Teams](#) / [Black Bauhinia](#)

## Black Bauhinia

### Also known as

- BlackBauhinia
- blackb6a

Website: <https://b6a.black>

Twitter: [blackb6a](#)

[Sign in](#) to join the team.

# CTFTime Record (11 Dec 2023)



A team based in Hong Kong.  
(We are NOT affiliated with any associations.)

### Participated in CTF events

[2023](#) [2022](#) [2021](#) [2020](#) [2019](#)

Overall rating place: **18** with **584.425** pts in 2023

Country place: **1**

Place	Event	CTF points	Rating points
24	<a href="#">Hack.lu CTF 2023</a>	1236.0000	26.425

# Quick Introduction to CTF



## \$ ctf -help



CSAW CTF, a Jeopardy CTF, has some of the best collegiate hackers in the nation



DEFCON CTF Finals, an Attack & Defense CTF, is widely considered the world cup of hacking

## \$ CTF --help

- A cybersecurity game where participants compete to solve challenges and get the hidden strings or files (flags)
- Participants have to submit flag to platform to score points.
- Participants have to accumulate the highest score within a given time limit (usually 48 hrs)



## Challenges

\* Challenges are from previous

LockPickDuck v3 (I)

SD Card

Echo

Catch-22

### SD Card

#### Info 基本資料

GonJK forensics ★☆☆☆☆

#### Description 描述

I have accidentally format my SD card. Please help me to recover the photo inside 🙏.

Attachment: [sdcards\\_f88edd62fb9d6f66b9bcab4497ca23b9.zip](#)

Solution: <https://hackmd.io/@blackb6a/hkcert-ctf-2022-i-en-3f8a9ef6>

hkcert22{funfunfunfunlookinforwardtotheweekend}

## \$ CTF --real-life-correlation

- Gain hands-on experience in identifying vulnerabilities, securing systems, and defending against various types of attacks
- Helping participants stay up to date with emerging threats and countermeasures

\$ blackb6a --hosting-experience



## ORGANISERS .



## CO-ORGANISERS .



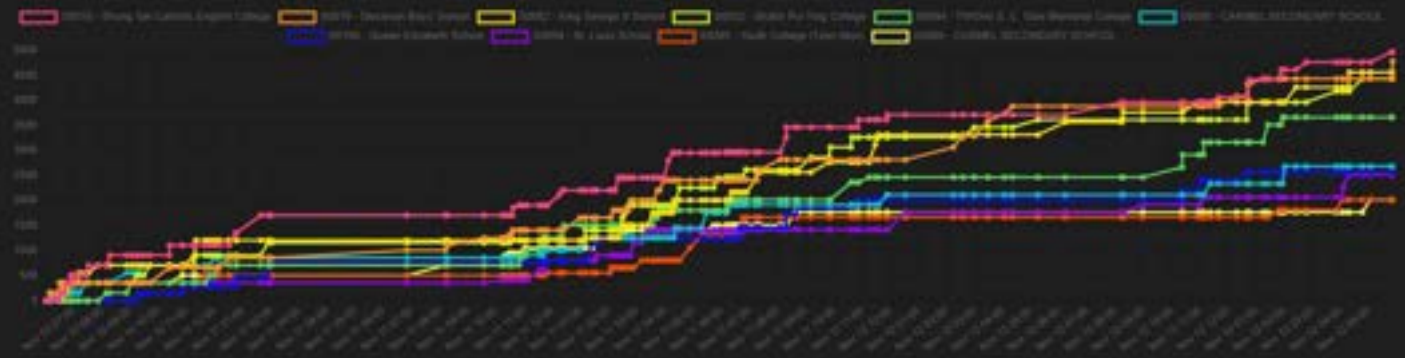
# Summary of HKCERT 2023?

**TF2023 challenge**

 Information  
**Scoreboard**

OVERALL SCOREBOARD

- #1 00010 - Shung Tak Cath... 4970 points
- #2 00019 - Diocesan Boys' ... 4790 points
- #3 00052 - King George V S... 4570 points
- #4 00032 - Sha Tin Pui Ying ... 4440 points
- #5 00094 - TWDH S. C. Ga... 3670 points
- #6 00098 - CARMEL SECO... 2690 points
- #7 00106 - Queen Elizabeth... 2570 points
- #8 00054 - St. Louis School 2530 points
- #9 00063 - Youth College (... 2030 points
- #10 00099 - CARMEL SECO... 2030 points

**SECONDARY DIVISION**


Rank	Name	Score
#1	00010 - Shung Tak Catholic English College	4970
#2	00019 - Diocesan Boys' School	4790
#3	00052 - King George V School	4570
#4	00032 - Sha Tin Pui Ying College	4440
#5	00094 - TWDH S. C. Gaw Memorial College	3670
#6	00098 - CARMEL SECONDARY SCHOOL	2690
#7	00106 - Queen Elizabeth School	2570
#8	00054 - St. Louis School	2530

**CTF2023 challenge**

- Information
- Scoreboard**

**OVERALL SCOREBOARD**

- #1 00044 - Jane Street Am... 11400 points
- #2 Tower of Hanoi 11399 points
- #3 aboutMarkets 10499 points
- #4 00128 - Black Bacon 8499 points
- #5 thehackerscrew 8399 points
- #6 Kalmarankoneen 8199 points
- #7 00034 - Mystic's Fan Club 8000 points
- #8 00104 - FireDuck 7599 points
- #9 T0091 - NattyShell 6399 points
- #10 00123 - NattyShell People 6299 points



Rank	Team Name	Points
#1	00044 - Jane Street Amateurs	11400
#2	Tower of Hanoi	11399
#3	aboutMarkets	10499
#4	00128 - Black Bacon	8499
#5	thehackerscrew	8399
#6	Kalmarankoneen	8199
#7	00034 - Mystic's Fan Club	8000
#8	00104 - FireDuck	7599

- ~ TICKET +
- # open-ticket
  - # ticket-40
  - # ticket-93
  - # ticket-289
  - # ticket-322
  - # ticket-330
  - # ticket-340
  - # ticket-341
  - # ticket-346
  - # ticket-348
  - # ticket-349
  - # ticket-350
  - # ticket-351
  - # ticket-352
  - # ticket-354
  - # ticket-355
  - # ticket-356





# From CTF to Pentester?

# Recent Cybersecurity News in HK

即時新聞

主頁 · 即時新聞 · 本地

## 數碼港上月中被黑客入侵 「暗網」可查員工資料

2023-09-12 HKT 22:41

介紹 · 分享工具



即時新聞

主頁 · 即時新聞 · 本地

## 消委會電腦系統遭黑客入侵 員工及月刊訂戶資料或被盜

2023-09-22 HKT 10:18

介紹 · 分享工具



凝聚香港 - 黑客入侵 盜取資料

RTHK  
香港電台

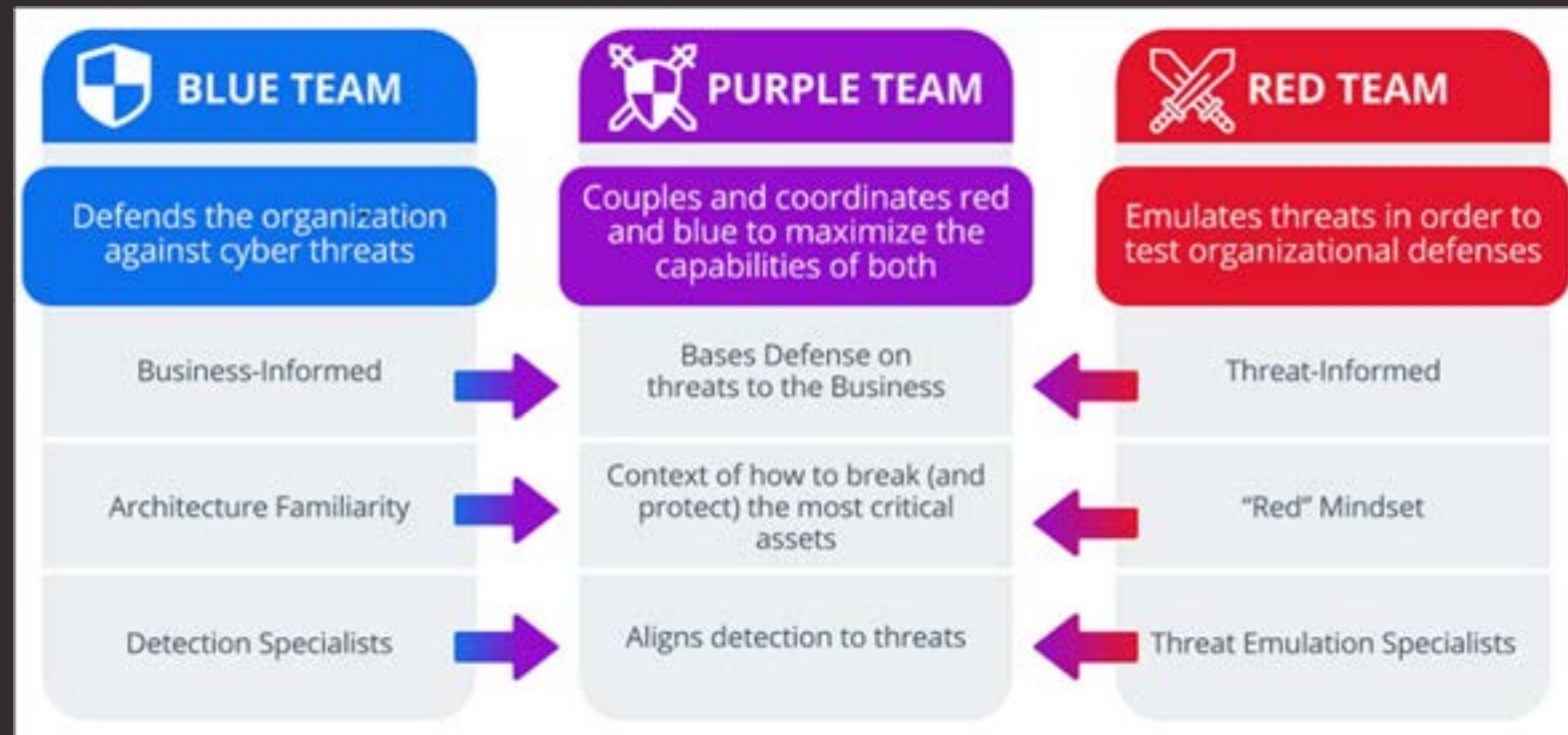
港式速遞  
講你知



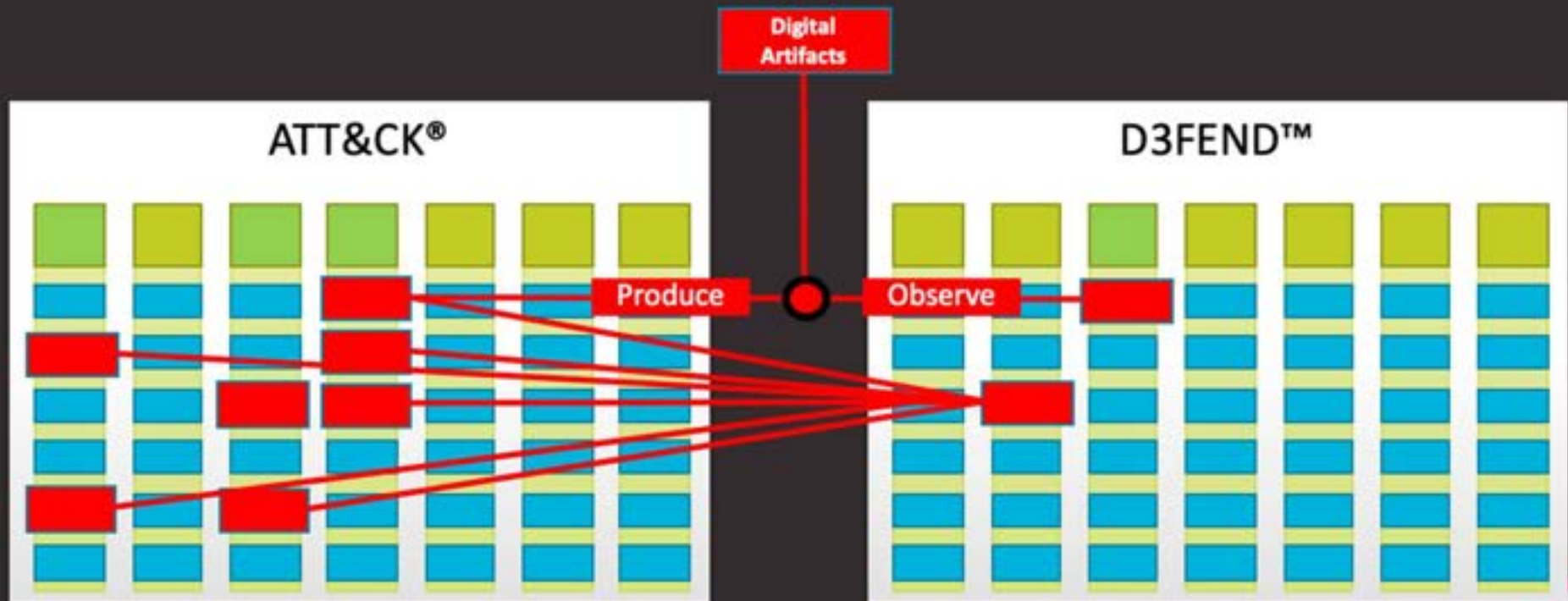
# Hacker Attack Flow



# Protection?



# MITRE ATT&CK, MITRE D3FEND



# Cyber Defense Matrix

	Identify	Protect	Detect	Respond	Recover
<b>Devices</b>	Configuration and Systems Management	IAM AV, HIPS	Endpoint Visibility and Control / Endpoint Threat Detection & Response		
<b>Applications</b>		App Sec (SAST, DAST, IAST, RASP), WAFS			
<b>Network</b>	Netflow	Network Security (FW, IPS)	DDoS Mitigation		
			IDS	Full PCAP	
<b>Data</b>	Data Labeling	Data Encryption, DLP	Deep Web, Brian Krebs, FBI	DRM	Restore Backup
<b>Users</b>	Phishing Simulations	Phishing Awareness	Insider Threat / Behavioral Analytics		
<b>Dependency</b>	Technology			People	
	Process				

# Penetration Test

**PEN TESTER**

**CORE SECURITY**  
A HelpSystems Company



What my friends think I do



What my mom thinks I do



What society thinks I do



What hackers think I do



What I think I do



What I actually do





ZERO KNOWLEDGE

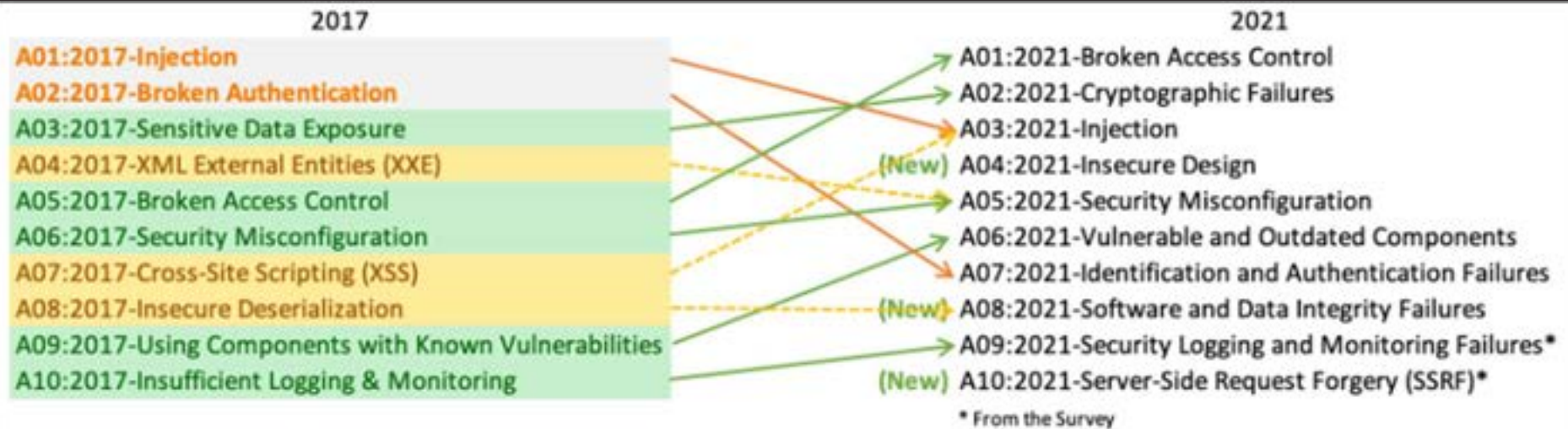


SOME KNOWLEDGE

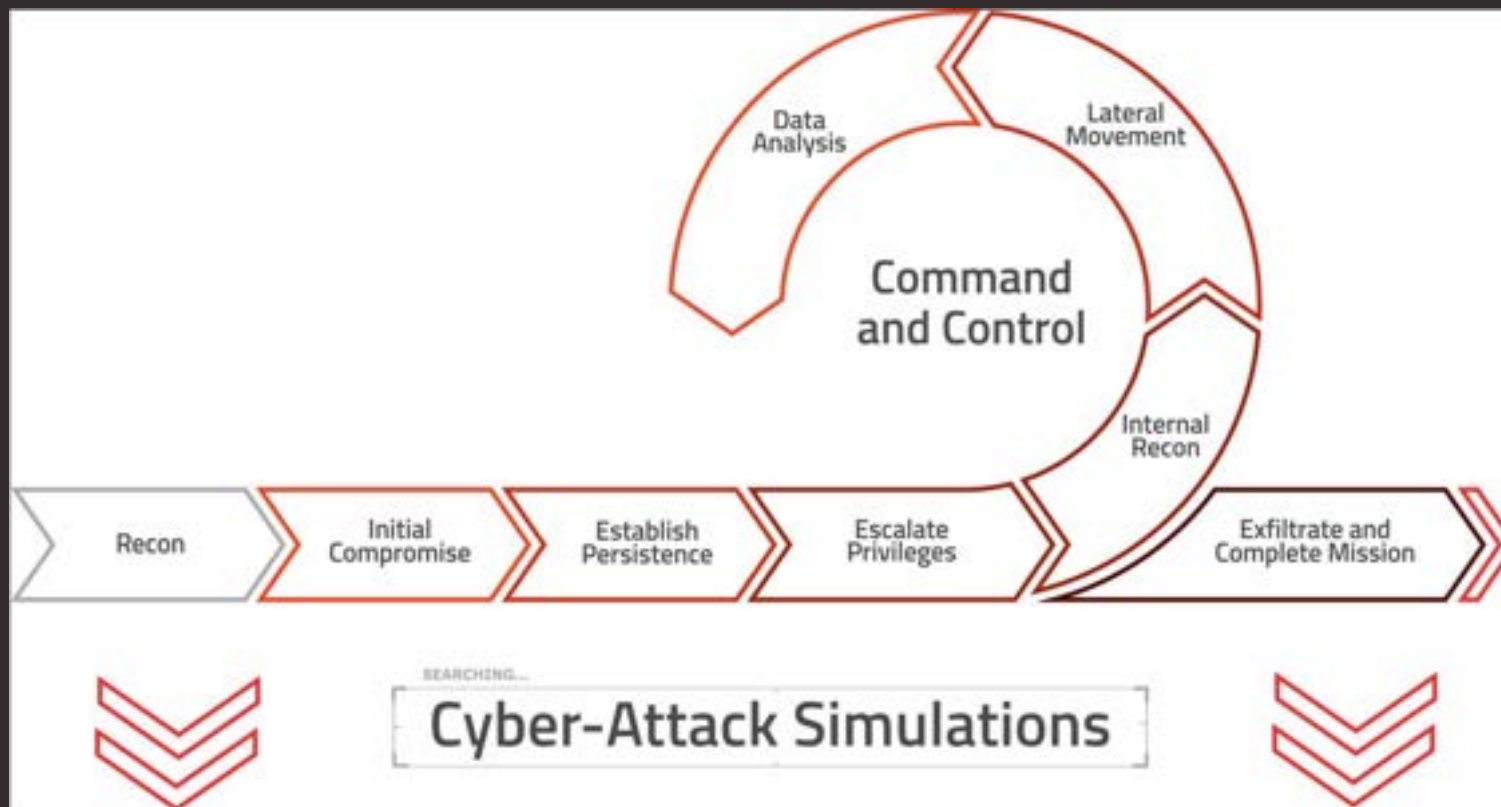


FULL KNOWLEDGE

# OWASP Top 10



# Red Team Operation



## Similarity between CTF and Pentest

- **Cybersecurity Focus:**  
Both CTF and Penetration Testing are focused on identifying and addressing vulnerabilities in computer systems, networks, and applications.
- **Skill Requirement:**  
Both activities require a strong understanding of cybersecurity concepts, programming, and various hacking techniques.
- **Ethical Hacking:**  
CTF and Penetration Testing are forms of ethical hacking, where professionals use their skills to improve security rather than exploit vulnerabilities for malicious purposes.

How playing CTF helps?

## Improved knowledge & skills in cyber security

- Require players to use a wide range of cyber security skills
  - Reverse engineering
  - Cryptography
  - Exploitation (pwn)
  - Web
  - Forensic
  - ...
- Become more knowledgeable and proficient in cyber security

## Enhanced problem-solving abilities

- Require creative thinking to solve
- Think outside the box and come up with creative solutions

## Increased teamwork and collaboration

- Team-based, requiring players to work together to solve challenges
- Develop strong teamwork and collaboration skills
- Essential in the cyber security field (but not limited)



## Opportunities to network and learn from others

- CTF competitions often attract a wide range of participants
- Network with others in the field
- Learn from others experiences, and potentially even find job opportunities

## Fun and engaging way to learn

- Fun and engaging way to learn about cyber security
- Rewarding and enjoyable way to spend their time
- Challenges can be a great way to stay motivated and engaged in learning

# Difference between CTF and Pentest

## Purpose

- CTF: Primarily designed as a competitive game or training exercise. Participants solve challenges and capture flags to score points. The goal is to enhance skills and knowledge in a gamified environment.
- Penetration Testing: Conducted to identify and mitigate security vulnerabilities in a specific system, network, or application. The primary objective is to simulate a real-world attack and provide recommendations for improving security.

## Environment

- CTF: Often has a specific timeframe, such as a few hours to a few days, during which participants attempt to solve challenges and accumulate points.
- Penetration Testing: The duration varies based on the scope and complexity of the engagement. It could last from a few days to several weeks, depending on the goals and objectives.

## Scope

- CTF: Broad and may cover a wide range of security topics, including cryptography, reverse engineering, web security, and more.
- Penetration Testing: Usually has a defined scope, such as testing specific applications, networks, or systems. The scope is agreed upon with the client to focus efforts on critical areas of concern.

## Reporting

- CTF: Participants may not necessarily produce formal reports. The emphasis is on learning and solving challenges.
- Penetration Testing: Involves the creation of detailed reports outlining the identified vulnerabilities, their potential impact, and recommendations for remediation.