

INTRODUCTION TO CYBER-DRILLS & CTFS

KANSIIME JOEL

passionate penetration Tester
soc analyst & threat hunter

CTF Developer that crafts solvable challenges to sharpen skills
of cybersecurity enthusiasts

co-founder Uguntu infosec community

CTF-PLAYER

Mentored 1000+ cyber security passionate people, this year

Introduced 1000+ people into the infosec community,

Inspired From

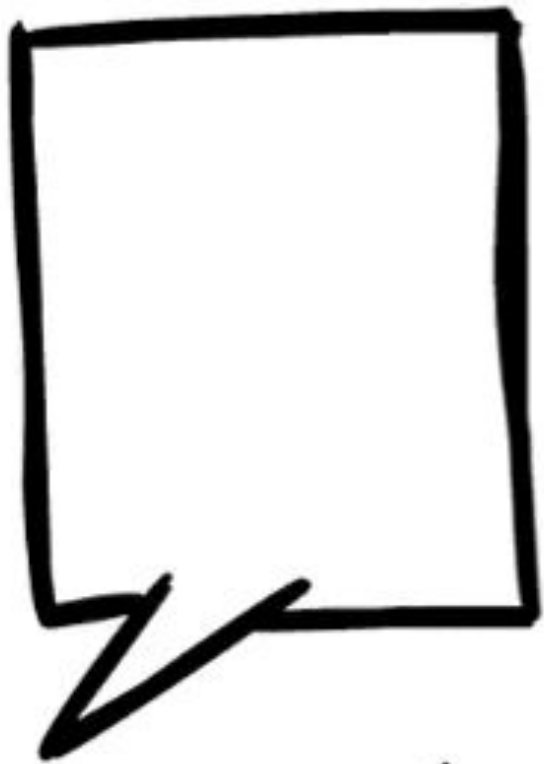
Offsec, DEFCON, YCN, PENTESTERLABS, HTB,
MyHardwork, Failures, My journey

`\xd`

Introduction to CTFs & cyber Drills



START YOUR ENGINES!



Linda

CTF/cyber-drill

- Capture the Flag (CTF) is a cybersecurity competition that is used test and develop computer security skills.

- CTFs have been shown to be an effective way to improve cybersecurity education through gamification.

Government-supported competitions

- Governmentally supported CTF competitions include the **DARPA** Cyber Grand Challenge and **ENISA** European Cybersecurity Challenge. In 2023, the **US Space Force**-sponsored **Hack-a-Sat** CTF competition included, for the first time, a live orbital satellite for participants to exploit

These 3 teams just hacked a US Air Force satellite in space ... and won big cash prizes

By Brett Tingley published August 16, 2023

The issue of satellite cybersecurity has taken center stage in recent years.

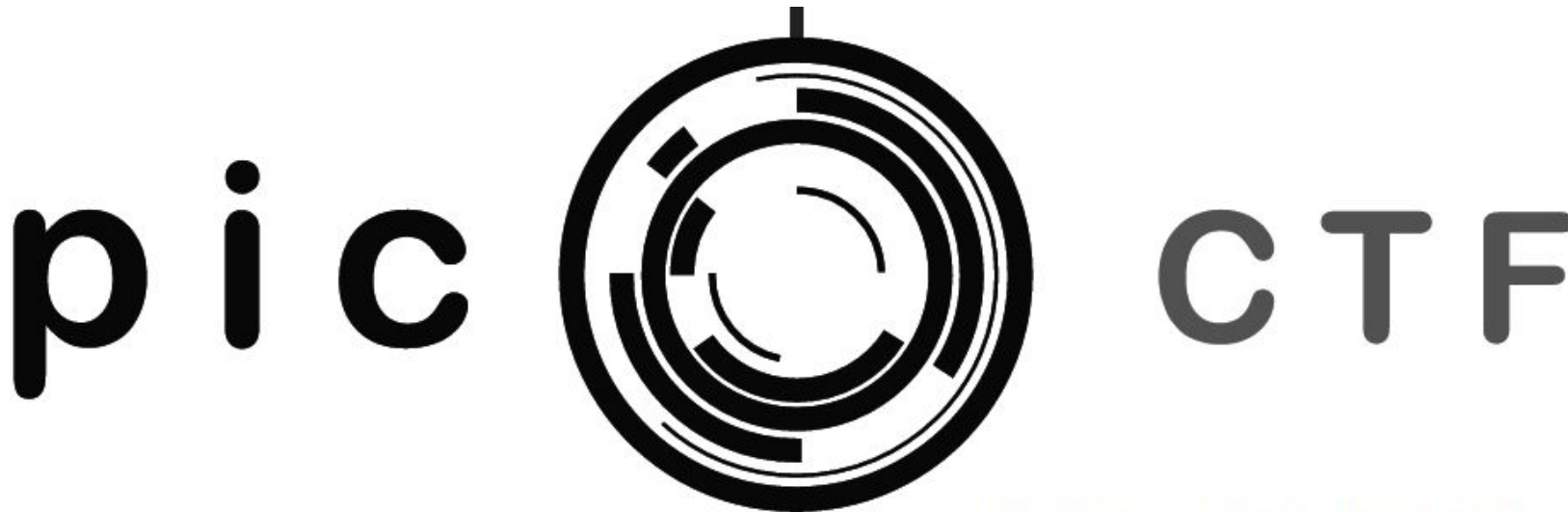
[f](#) [t](#) [e](#) [p](#) [r](#) [m](#) [Comments \(0\)](#)



CTF/cyber-drill

Educational-supported competitions

There are many examples of CTFs designed to teach cybersecurity skills to a wide variety of audiences, including **PicoCTF, organized by the Carnegie Mellon CyLab**, which is oriented towards high school students, and Arizona State University supported pwn.college.



CMU CYBERSECURITY COMPETITION

CTFS HISTORY

- ▣ **Starting from Defcon 4 in 1996**
- ▣ **Format is a mystery...**
- ▣ **Held every year since 1996**
- ▣ **The most important CTF now**



CTFS HISTORY

- ▣ **UCSB iCTF first held in 2001**

- ▣ **The first CTF be held by academic organization[University Of Carlifonia]**



Traditional Course Practice

- **More theory and basic concept, but less practice and lab**
- **Offensive Thinking**
 - **Think like a hacker**
-

CTF TYPES



Jeopardy

- **Problems are classified into different disciplines**
 - Most Jeopardy CTF contain 20~30 problems
 - Pwn, Reverse Engineering, Web security, Forensics and Cryptography
 - More difficult problem worth more score
- **About 90% CTFs are in Jeopardy style**
 - Can be held online and hundred of teams can involve

Attack & Defense

The competitors are put into the closed environment and try to attack each other's.

The server with vulnerable programs running



Competitor needed to patch(fix) the vulnerability and exploit(attack) the other teams

Need good support of networking environment

Less CTFs are in Attack & Defense style

Can do many interesting things

Attack & Defense

- ▣ **Skills needed**

- ▣ **Vulnerability discovery and patching**
- ▣ **Network flow analysis**
- ▣ **System administrator**
- ▣ **Backdoor**

King of Hill

- ▣ **There are several servers provided**
 - ▣ **Competitors should compromise and keep control to the server**
- ▣ **The more time you own the machine, the more score can be got**
 - ▣ **Just like real-world cyber war**
- ▣ **Attackers not only need to attack, but also need to prevent other exploit server you owned**

Real World Attack

- **Overall attack life cycle**
 - **Reconnaissance**
 - **Gaining Access**
 - **Maintain Access**
 - **Clearing Tracks**

The other way for security training

▣ CTF as the training for offensive security

- ▣ Spread security techniques

- ▣ Measure security skill

- ▣ Practice, practice and more practice

- ▣ Emulate real world problems

 - Environment close to real environment

 - Eliminate the boring task and focus on advanced security skill

- ▣

- ▣

THE ART OF PROBLEM SOLVING



$$a$$
$$S=a \cdot h_1$$
$$S=b \cdot h_2$$

CYBER DRILLS

- **The competition to steal data, a.k.a flag, from other computers**
- **EX. Steal admin password from a web server,**
- **Most problems are related to information security**

THE ROOK | STARZ



WHY YOU?

Why you Should try drills

- Practice your hacking skills
- Compete with top hackers among the world
- Grow your critical thinking capabilities
- Earn
- certify
- Network

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i x \xi} dx$$



CTFs around the world

- To enhance education of offensive security, CTFs are held in many country
 - U.S: DEFCON, Ghost In the Shellcode, PlaidCTF

The image shows a screenshot of a CTF scoreboard and a challenge card. The scoreboard is titled "Plaid CTF5" and lists various categories and their scores. The challenge card is titled "HACK THE PLANET" and is worth 20 points. It contains a question about a mysterious message and a note that the flag does not have a flag.

Plaid CTF5

DEFKOR	41
PPP	41
Gallopsled	35
9447	35
blue-lotus	32
Odaysober	30
SpamAndHex	30
Oops	30
Shellphish	30
LC BC	28
HITCON	28
binja	28
Eat, Sleep, Pwn, Repeat	28
Dragon Sector	28
Samurai	26
WhatTheBird	26
CORNDUMP	26
tasteless	26
Routards	25
Mostly Inexperienced Beginner	25
Hackers	25
Alternatives	23
KAIST GoN	22
Blunt Instrument	21
Hello World	21
int3pids	20
BambooFox	15

Baby's First 1 1 1 1
Coding Challenge 1
Pwnable 2 2 3 3 4 4 4 5 5 6
Reverse Engineering 1 1 2 3 3 3
Web 2
Miscellaneous 2 3

HACK THE PLANET
Misc (20 pts)
What kind of mysterious message is this??
.....
Note: This flag does not have flag()

CTFs around the world

- Japan: SECCON, TMCTF, MMACTF

MMA CTF 1st 2015

- Top
- Announcement
- Problem
- Ranking

Team Name
BambooFox

Score
1150

Rank
2

Remain
1 day

- Update Profile
- Log out
- Switch to Japanese

Current Server Time
2015/09/05 10:24:37 UTC

Ranking

Rank	Team	Score	Last submission
1	Plaid Parliament of Pwning	1400	2015/09/05 08:56:25 UTC
2	BambooFox	1150	2015/09/05 10:23:32 UTC
3	Shellphish	1050	2015/09/05 09:24:02 UTC
4	samurai		
5	tomcr00se		
6	9447		
7	BXB		
8	dcua		
9	shinh		
10	nkfust		
11	mage		
12	Qdaysober		
13	KaSec		
14	BatmansKitchen		

CTFs around the world

- Korea: CodeGate, SECUINSIDE
- China: XCTF, BCTF, OCTF,
- Russia: RuCTF
- France: Nuit du HackCTF

CodeGate 2013 YUT

BIOS (India)

Vulnerab	Binary
100 41/580	100 159/580
200 49/580	200 57/580
300 41/580	300 25/580
400 13/580	400 10/580
500 12/580	500 3/580

SECUINSIDE 2012

Trading
Hacking

HACKING CONTEST

PROBLEMS

Ranking

weibo.com/u/3695251881

CTFs around the world

**AFRICA: CYBER TALENTS, URCHINSEC, BUG PWN
CTF ETC**

**Africa has less involvement in the cyber drills
competitions**

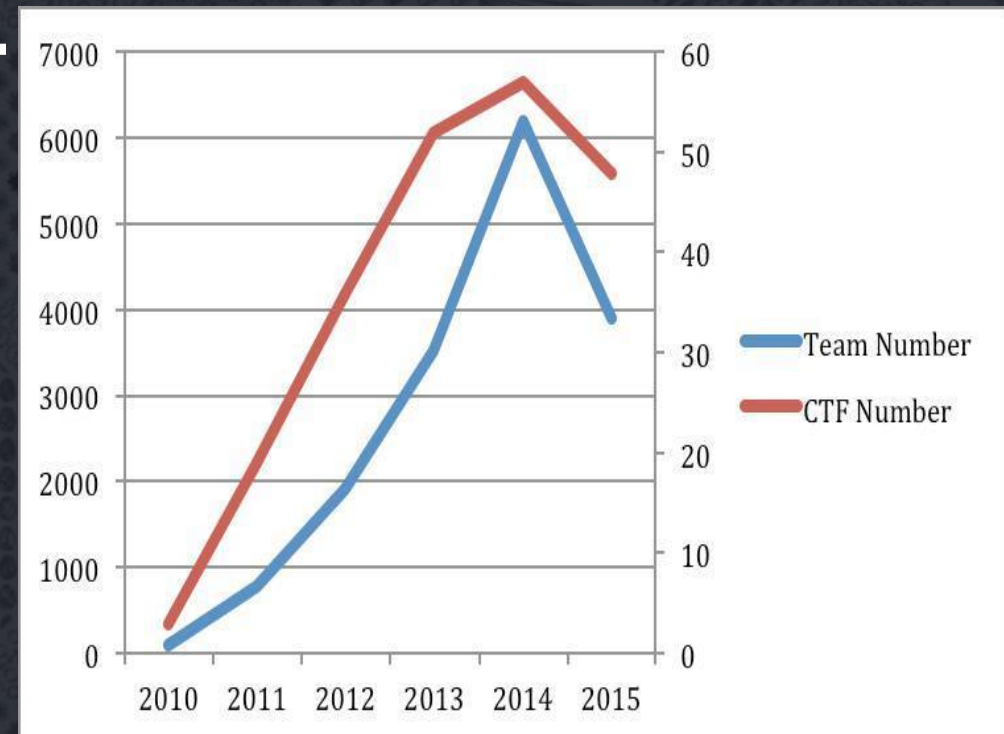


SO UNIQUE

AR

Trend of CTFs

- **CTF contest**
 - **Less than 10 in 2010**
 - **More than 50 CTFs in 2014**
 - **More than 1 million CTFs 2020**
- **CTF teams**
 - **More than 6000 teams in 2014**
 - **1 million+ 2023**



CTFS TO PLAY

More than 100 CTF's each year, you can find the proper CTF

Beginner CTFs

PICOCTF

- ▣ **Backdoor**
- ▣ **CSAW Qualification**
- ▣ **ASIS**

CTFS TO PLAY

More than 100 CTF's each year, you can find the proper

CTF

Advanced CTFs

- ▣ **DEFCON**
- ▣ **PlaidCTF**
- ▣ **CodeGate**
- ▣ **SECCON**
- ▣ **PHD Qals**

▣

EXPERIENCE SHARING



Focus !

When you start to CTF/DRILLS, it is best to focus on one type of problem.

- **E.g. Pwn, Reverse, Web....**

When playing CTF, keep up with 1 problem in the same time

Following New Techniques

- ▣ **Hackers like new techniques**
- ▣ **CTF organizer often proposes problem with these new techniques**
- ▣ **Follow up new technique**
 - ▣ **Freebuf**
 - ▣ **ippsec**
 - ▣ **johnhammond**
 - ▣ **liveoverflow**

Reddit Hacking, NetSec and Reverse Engineering Channel

Customize Your CTF Toolset

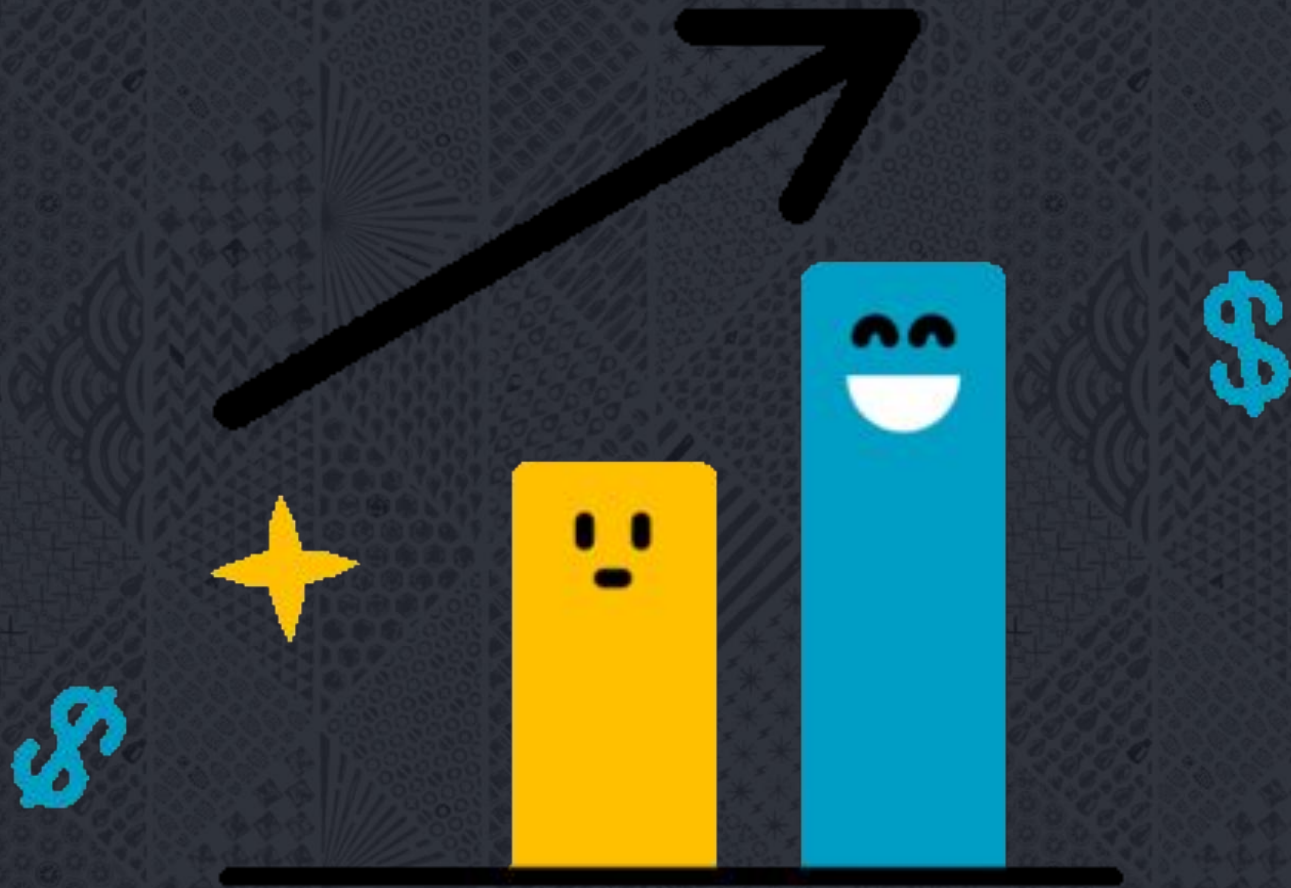
- **Prepare your own environment**
 - **With your favorite tools**

Customize it. Make your operation more efficient.

Keep and refine the toolset and program after every CTF

- **Even better to come up with the writeup**

Tools/Hacks



Review the Problems

- ▣ **Review the problem you are unable to solve during CTF**



- Read the writeup**



Practice, practice and practice

□

□ **Experience and proficiency play the important role in CTF**

□ **Experience make you find the right way earlier**

□ **Proficiency make you try more approaches than others**

□ **Practice, practice ,practice , practice**

□

□

STUDY HARD & MAKE RESEARCH



Enjoy the Game

- **Don't panic. Keep calm and carry on.**



Thanks
Good Luck

CONTACT ME

TWITTER/X: @Khanzjoel

EMAIL: khanzjoel55@gmail.com

LINKEDIN: Kansiime Joel

DISCORD: @J_PWN