CTF Workshop

Mustakimur Rahman Khandaker
09/01/2021 @ 4:00 - 5:30 PM

Capture The Flag

Capture the Flag (CTF) is a special kind of information security competitions.

- Players use real hacking tools to break into the system, detect vulnerabilities, and exploit them to capture an encoded string.
  - This string is known as a flag i.e. is evidence that a player has discovered the weakness in the systems.

There are three common types of CTFs:

- Jeopardy
- Attack-Defence
- Mixed.

Why should you consider playing CTF?

- Learning new skills is one of the most essential things to get ahead in your career. Especially if you are working in a field such as Cybersecurity, where new challenges keep arising on a regular basis. Continuous learning and upgrading your skills is the only way to keep yourself in the game.
- Also, it is fun to break systems, develop team spirit, and boost your confidence.
- But, foremost, secure a well-paid job in information security.

Types of CTFs

Jeopardy:

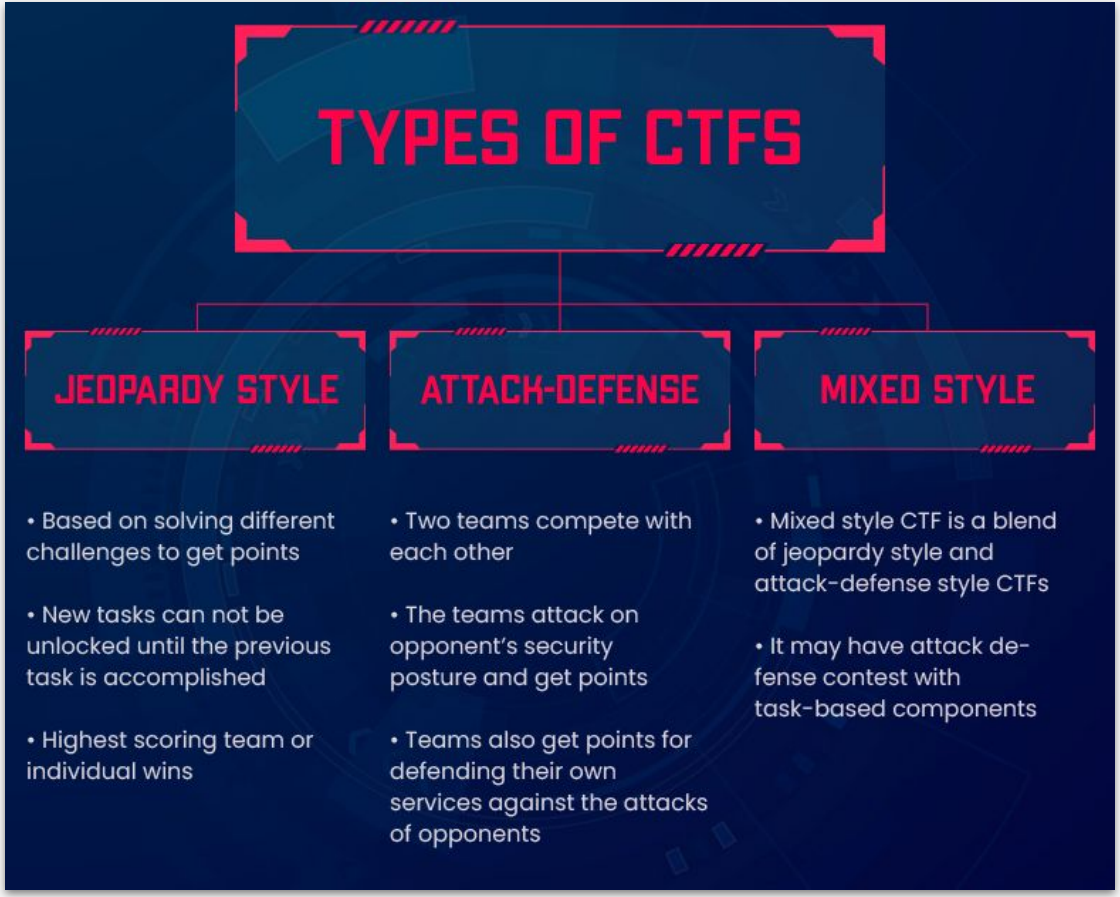
- Cryptography.
- Binary Exploitation.
- Web Exploitation.
- Forensics.
- Reverse Engineering.
- Programming.
- Packet Analysis.
- Miscellaneous.

Attack-Defense (wargame):

- Finding out vulnerabilities.
  - Generate exploit.
  - Patch the vulnerabilities.

Mixed:

- Wargame with special time for task-based elements.



Online Resources

Jeopardy Practice:

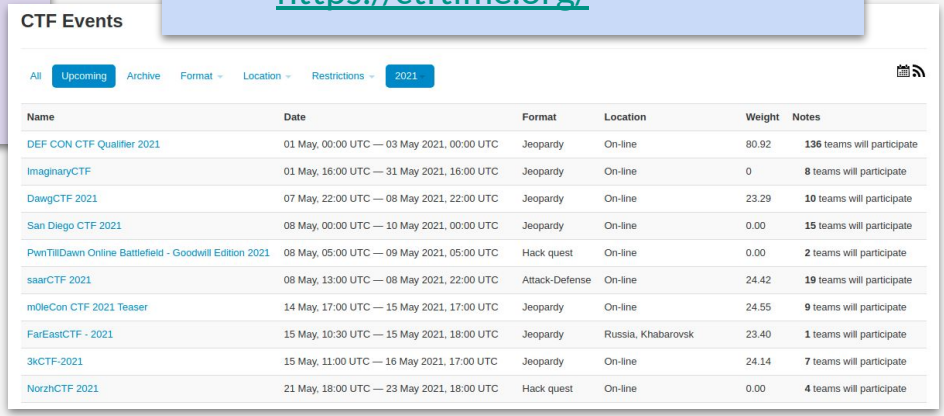
- Pwnable.kr
- pwnable.tw
- Reversing.Kr
- picoCTF - CMU Cybersecurity Competition
- CTF Challenge - Web App Security Challenges
- The Cryptopals Crypto Challenges
- Welcome to pwn.college! | pwn.college
- Web Security Academy: Free Online Training from PortSwiggerportswigger.net
- Home - CTFlearn - CTF Practice - CTF Problems - CTF Challenges

Attack-defense Practice:

- https://ctf365.com/
- http://smashthestack.org/
- https://legitbs.net/

Check for upcoming CTF competition:

- https://ctftime.org/



CTF Events

All | Upcoming | Archive | Format | Location | Restrictions | 2021

Name	Date	Format	Location	Weight	Notes
DEF CON CTF Qualifier 2021	01 May, 00:00 UTC — 03 May 2021, 00:00 UTC	Jeopardy	On-line	80.92	**136** teams will participate
ImaginaryCTF	01 May, 16:00 UTC — 31 May 2021, 16:00 UTC	Jeopardy	On-line	0	**8** teams will participate
DawgCTF 2021	07 May, 22:00 UTC — 08 May 2021, 22:00 UTC	Jeopardy	On-line	23.29	**10** teams will participate
San Diego CTF 2021	08 May, 00:00 UTC — 10 May 2021, 00:00 UTC	Jeopardy	On-line	0.00	**15** teams will participate
PwnTillDawn Online Battlefield - Goodwill Edition 2021	08 May, 05:00 UTC — 09 May 2021, 05:00 UTC	Hack quest	On-line	0.00	**2** teams will participate
saarCTF 2021	08 May, 13:00 UTC — 08 May 2021, 22:00 UTC	Attack-Defense	On-line	24.42	**19** teams will participate
m0leCon CTF 2021 Teaser	14 May, 17:00 UTC — 15 May 2021, 17:00 UTC	Jeopardy	On-line	24.55	**9** teams will participate
FarEastCTF - 2021	15 May, 10:30 UTC — 15 May 2021, 18:00 UTC	Jeopardy	Russia, Khabarovsk	23.40	**1** teams will participate
3kCTF-2021	15 May, 11:00 UTC — 16 May 2021, 17:00 UTC	Jeopardy	On-line	24.14	**7** teams will participate
NorzhCTF 2021	21 May, 18:00 UTC — 23 May 2021, 18:00 UTC	Hack quest	On-line	0.00	**4** teams will participate

Workshop Purpose

Introduce students (undergraduate and graduate) to CTF competition.

Regular workshop presentation on problem solving of different categories.

- Starting with ICSP faculty members and gradually transferring the presentation to the experienced students.
- ICSP faculty members will be always there for advising.

Assigning students CTF problems to solve and discuss the problems in next workshop session.

- A website will be maintained to help students on track and observing their progress.
- ICSP will also invite external CTF expertise for specialized talk (e.g. tutoring about their invented tool).

Ultimate goal is to build 2-3 strong teams from the department students.

- ICSP will organize online CTF competition to help students find out their teams.
- ICSP will sponsor top student teams to participate in flagship CTF competitions (e.g. Defcon CTF).

ICSP will invite federal agencies and industries who will be interested to see the activities.

- CTF workshop participants will be able to engage that will benefit them on job hunting.

Fall 2021 Workshop Schedule

Date	Category	Presentation	Exercise
09/01/2021	Bin Exploit	Buffer overflow.	
09/15/2021	Bin Exploit	Passcode.	
09/22/2021	Rev Eng		
09/29/2021	Web Exploit		
10/06/2021	Rev Eng		
10/20/2021	Crypto		
10/27/2021	Packet Analysis		
11/10/2021	Web Exploit		
11/17/2021	Misc		
12/01/2021	Bin Exploit		

Spring 2022 Plan

Continue the workshop (specially for new students willing to join).
- But, preferably presenting by students participated in Fall 2021.

Invite at least 2 external presenters to give talks.
- Someone experienced with CTF competition and invented tools well-known in the arena.

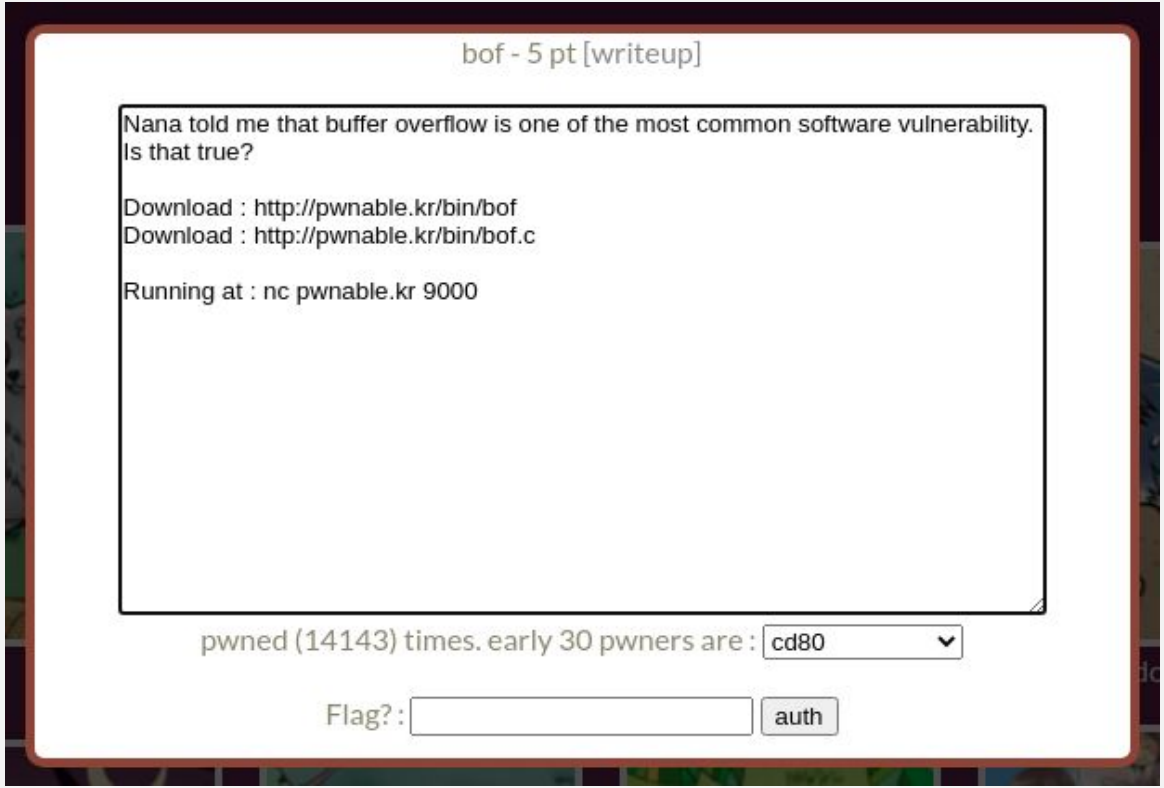
By mid semester, arrange a local CTF competition for the UGA students.
- It will be a good time to build teams to participate in flagship CTF competition.

Selecting top UGA team/s to sponsor in participating in flagship CTF competition.
- Specially, DefCon 2022 (probably will held on May).

Invite representative from federal agencies and industries to tour our activities and meet with students.
- Hopefully, collaborate with UGA Career Center.

Stack overflow exploitation

Problem Statement




```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

void func(int key) {
 char overflowme[80];
 printf("overflow me : ");
 gets(overflowme); // smash me!
 if (key == 0xaaefabca) {
   system("/bin/sh");
 } else {
   printf("Nah..\n");
 }
}
int main(int argc, char *argv[]) {
 func(0xeeaacaae);
 return 0;
}
```

Exercise

1. Create an account on pwnable.kr.
2. Go to http://pwnable.kr/play.php.
3. Look for the problem **bof**.
4. Download the code and binary to exploit locally.
   a. Use a VM with Linux setup.
   b. Disable the ASLR of the system.
   c. Compile the code with `-fno-stack-protector`.
5. Then use the exploit to get the flag from exploit server (`nc pwnable.kr 9000`).
6. Submit the flag to pwnable.kr.
7. Take a screenshot of the exploit is being successful and submit it on the UGA-CTF website.

See you on 09/15/2021
@ 4:00 – 5:30 PM
@ Boyd – 201