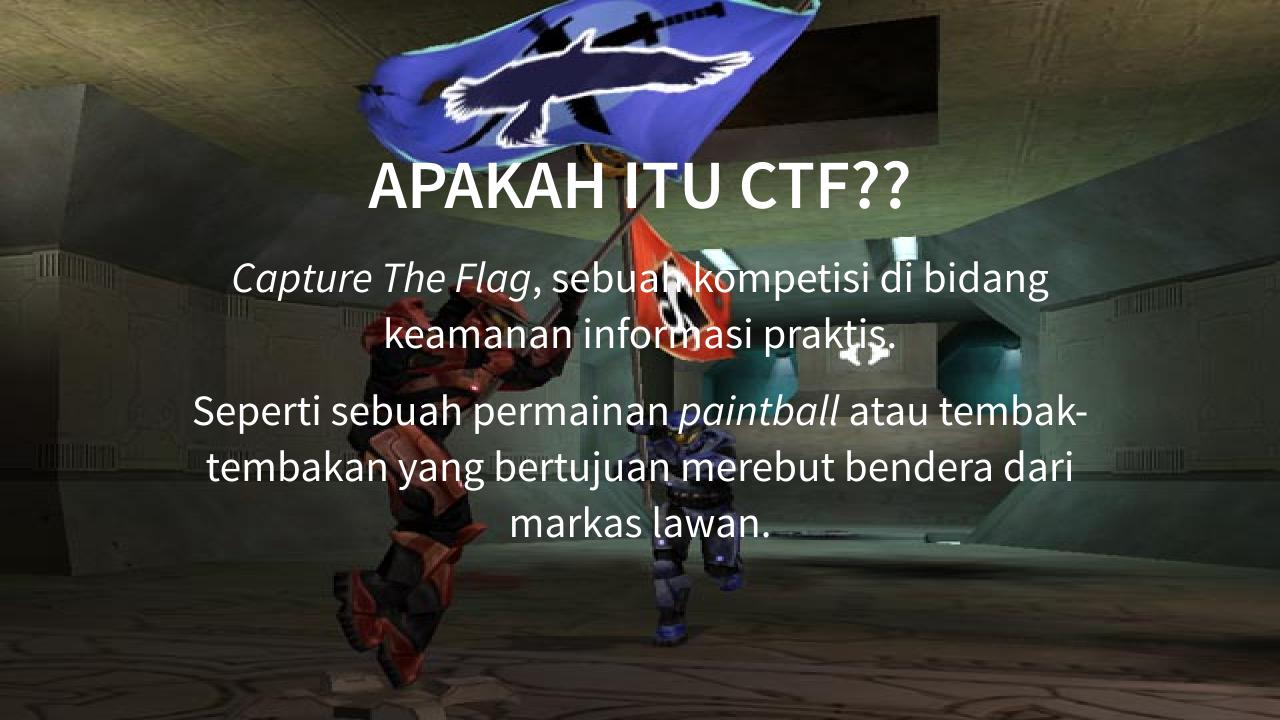
CTF: CAPTURE THE FLAG - AN INTRODUCTION

TENTANG SAYA

- Sukirno
- mblonyox@gmail.com
- mblonyox.com
- **y** @mblonyox
- mblonyox



FLAG??

Flag, biasanya berupa sebuah string sebagai bukti bahwa telah berhasil meretas sistem.

Format biasanya dibuat dengan format nama kompetisi dan deretan karakter acak yang sulit ditebak.

CTF{1ni_c0ntoh_Fl4g}

JENIS-JENIS CTF

ATTACK - DEFENSE

- Setiap tim mendapatkan mesin dengan service yang sudah dirancang dengan celah keamanan oleh penyelenggara
- Tim penyerang menyerang mesin lawan untuk mendapatkan *flag* sembari Tim yang bertahan memperbaiki celah keamanan di mesin tersebut.
- Biasanya bergantian

JEOPARDY

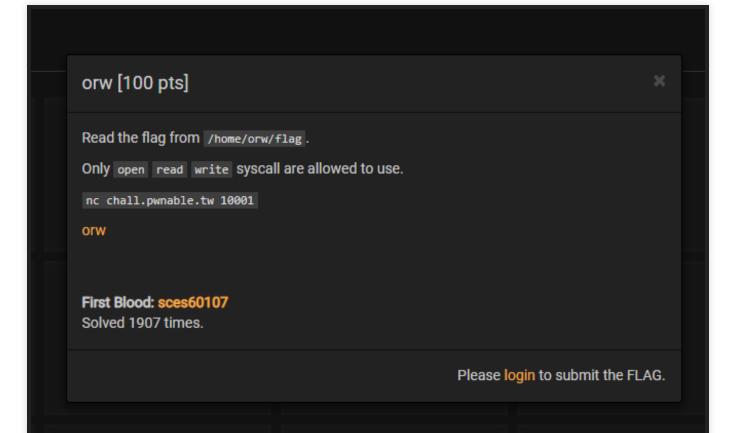
- Beberapa soal tantangan sudah disediakan dengan kategori-kategori tertentu
- Flag bisa ditemukan dalam file yang disediakan bersama dengan soal atau pada server yang telah disediakan
- Tiap flag memiliki bobot nilai tertentu sesuai tingkat kesulitan

KATEGORI TANTANGAN

- Reverse Engineering
- Pawning / Binary Exploit
- Crypto
- Web
- Forensic
- Misc

FORMAT SOAL/TANTANGAN (JEOPARDY STYLE)

- Memiliki Judul dan deskripsi yang bisa jadi petunjuk celah keamanan
- Kategori tantangan, tingkat kesulitan, nilai
- Statistik (solves, challenger)
- Lampiran *file* yang bisa diunduh (biasanya dalam bentuk zip dengan nama file sesuai hash)
- Alamat service pada server yang sudah disiapkan, beserta binary executable service tersebut (untuk kategori pawning/binary exploit)



CONTOH SOAL

RESOURCES

CTF>TIME

https://ctftime.org/ - CTF>TIME

WARGAME / CHALLENGES

- https://capturetheflag.withgoogle.com/ Google
 CTF
- https://2018game.picoctf.com/ PicoCTF 2018
- https://pwnable.tw/ (Pawning/Binary Exploit challenges)

YOUTUBE:

- LiveOverflow
 - What is CTF? An introduction to security Capture
 The Flag competitions
 - The Secret step-by-step Guide to learn Hacking
- Intro to CTFs Drew Miller
- Google CTF 2018 Beginners Quest

WRITEUPS

- https://ctftime.org/writeups
- https://github.com/pcchou/ctf-writeups

TERIMA KASIH~