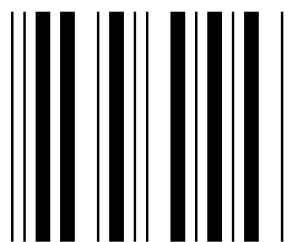
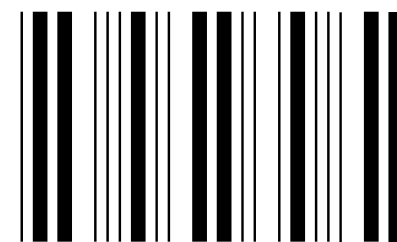


C A P T U R E



T H E



F L A G



C'est quoi un CTF ?

- Une compétition
- Basée sur des failles de sécurité réelles
- Une ambiance fun
- Vous êtes le Hacker (le quoi ?)

Apprendre mains
sur le clavier



Qui fait des CTF ?

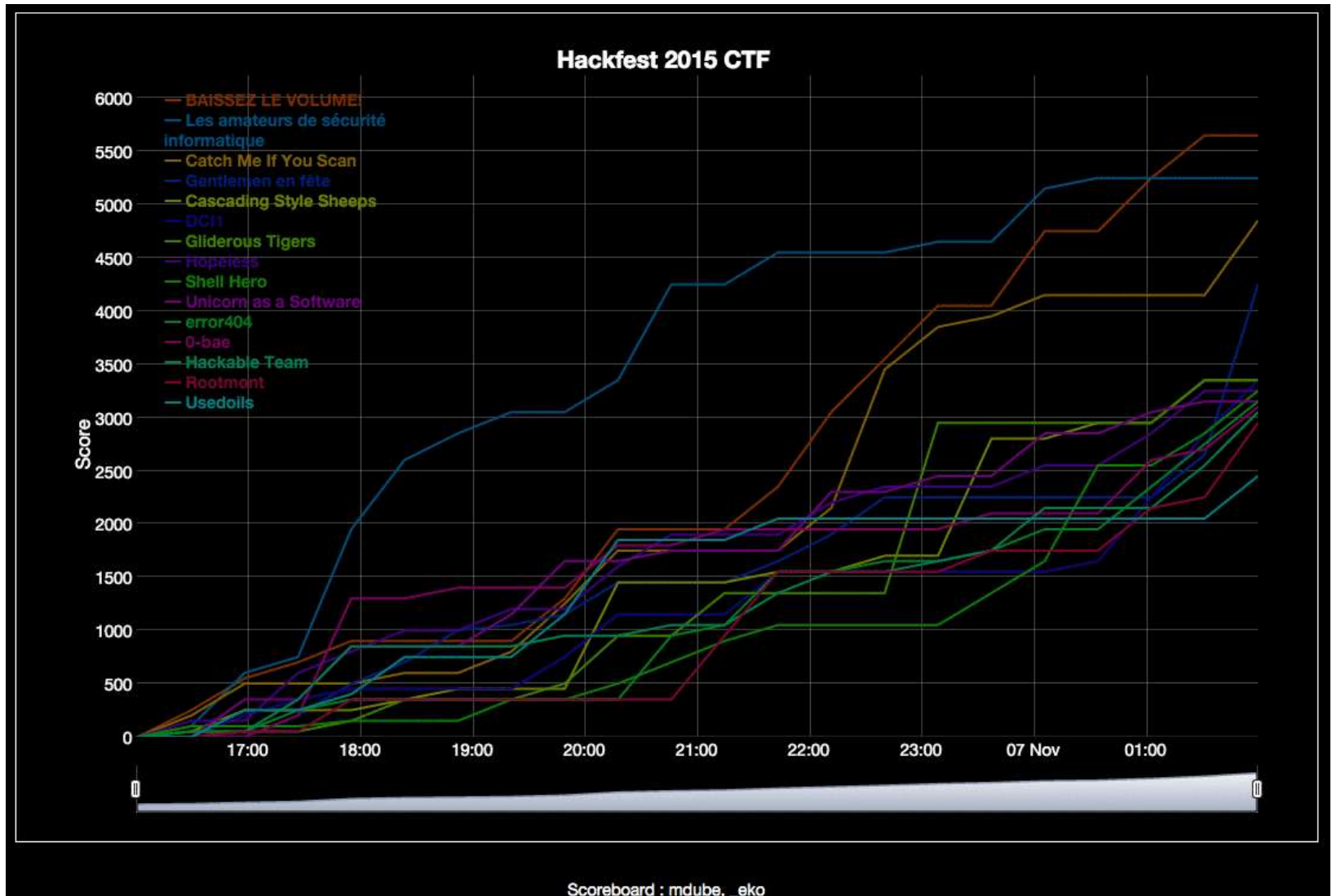
- Les pro de la Sécurité
- Les amateurs
- Les étudiants
- Les débutants
- Les curieux
- ...



Des Challenges en temps limité

<i>Vulnerab</i>	<i>Binary</i>	<i>Network</i>	<i>Forensics</i>	<i>Misc</i>
100 66/472	100 128/472	100 74/472	100 151/472	100 136/472
200 64/472	200 48/472	200 35/472	200 95/472	200 72/472
300 40/472	300 31/472	300 28/472	300 61/472	300 56/472
400 20/472	400 17/472	400 16/472	400 30/472	300 108/472
500 9/472	500 14/472	500 5/472	500 12/472	100 87/472

Un classement en temps Réel



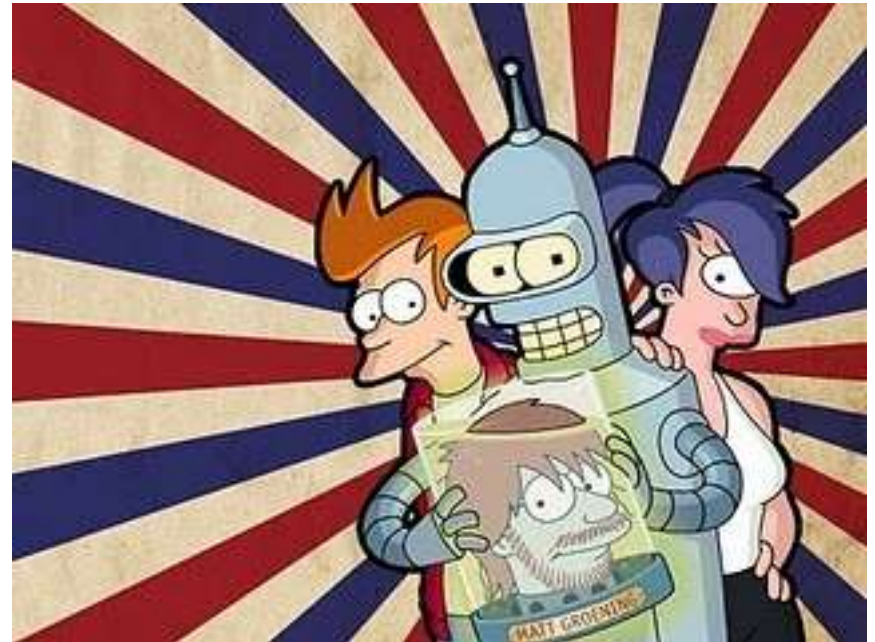
Deux types de CTF

- Jeopardy : Participants vs Server
- Attack-Defense :
 - Defendre ses Flags
 - Capturer les autres



Quelles thématiques ?

- Tout ce qui peut être mal configuré ou présenter une vulnérabilité exploitable
- Chiffrement
- Reverse engineering
- Analyse de Code
- Site Web
- Protocole Réseau
- Hardware/IoT
- VMs



C'est quoi un Flag ?

- Un Flag rapporte des points



- `Flag_A{y0l0_l3s_p0t0s}`
- `d9cad5b8fe41e6dd9cad5b8fe41e6d`
- `$flag$ebe85184bd9cad5b8fe41e6d5ee99f89`

Un exemple de Flag pour débutant

- dpef qbs efdbmbhf ef mfuusf gmbh{z0m0_m3t_q0u0t}
- <https://cryptii.com/pipes/caesar-cipher>
- code par decalage de lettre
flag{y0l0_l3s_p0t0s}



Un exemple de Flag type CTF

Winter is coming

Vm0wd2QyVkZOVWhTYmxKV1YwZDRXRmxVUum5kVlJscHpXa2M1VjFKdGVGWlZNbmhQWVd4S2MxTnNXbGRTTTFKUVdWY3hTMUI4WkhGUmJGWNbVbXh3VVZkV1pEUIRNazE0Vkc1T1dHSkdjSEJXTUdSdlpWWmtWMWR0ZEZSTIZUVkpWbTEwYTFkSFNrZGpSVGxYWWxoU00xVXhXbXRXTVZaeVpFWINUbFp0ZHpcV2EyUTBWakZWZVZOclpHcFNiV2hvVm1wT2IyRkdXWGhYYIhSWFRWZFNlbfI5TVRCVWJVCehZMFZzVjJFeVRYaFdha1pyVTBaT2NtSkdTbWxTTW1ob1YxZDBZVlI3TIVkVmJrcFIZbGhTV1ZWc1VrZFdiRlpZVFZoa1ZXSkdjRnBWVm1oclZqSkZIVIZZWkZwbGExcHIWVEJhVDJNeVJraGxSazVzWWxob1dsWXhaREJaVm14V1RVaG9XR0pzU25OVmFrNVRWMVpXYzFWclpGUmlSMUo1Vm14U1YxWXdNVmRqUldSV1RWWktTRlpxU2tkamJVbzJV3hhYkdFeGNGbFdiWEJIWVRKT2MxZHVUbFJpUjFKVVZGUkJKMDFSUFQwSw==

<http://www.utilities-online.info/base64/>

Vm0wd2VFNUhSblJWV0d4WFIURndVRlpzWkc5V1JteFZVMnhPYWxKc1NsWldSM1JQWVcxS1lxZHFRbFZpUmxwUVdWZDRTMk14VG5OWGJGcHBWMGRvZVZkV1dtdFRNVTVJVM10a1dHSkdjRTIXYlhSM1UxWmtWMVZyZEZSTIZtdzBWa2Q0VjFVeVNrZGpSbWhoVmpOb2FGWXhXbXRXTVdSelYyMTBUBUpHY0VsV2EyTXhWakZrU0ZOcmJGSmlSMmhoV1d0YVYwNUdVbkpYYIhSWVVsUkdWbFZYTVhkVWJGcFpVVMhrVjJFeVYyZFlpY1pyVTBaT2MyRkhlRk5sYlhOwIYxZDBZVmxWTUhoWGJsSnNVak5TV1ZWc1VrZFRiR1J5VmxSV1YwMVdjRWRWTVZKSfZqSkdjbUo2UWxabGExcFIWbXBHYTJOc1duTIRiR1JUVFRBd01RPTOK

Flag{You know nothing Jon Snow}



La Def Con

- 1993
- Badges
- Black Badge



Une équipe

- Personne ne sait tout faire



- Plus fun



La boîte à outil pour débuter

Outils

- Google
- nmap
- Exploit_db
- Msfconsole
- Burp Suite
- Python

Connaissances

- HTTP
- Cookies
- XSS
- SQLi
- LFI
- Buffer Overflow



Comment P0wner un serveur ?

- Analyse du système
 - Masscan, nmap
- Identifications de vulnérabilités
 - Nmap, wpscan, dirbuster
- Exploitation de vulnérabilité
 - Hydra, sqlmap, metasploit
- Post Exploitation



www.root-me.org

Root Me

HOME / CAPTURE THE FLAG / CTF ALL THE DAY

CTF all the day

Improve your hacking skills
root » the host !

You are facing a vulnerable environment
security system for penetrating it.

Games act as follow:

- VMs
- Challenges
- Docs
- Tools

Root Me

HOME / CHALLENGES

- App - Script
- App - System
- Cracking
- Cryptanalysis
- Forensic
- Network
- Programming
- Realist
- Steganography
- Web - Client
- Web - Server

357 visitors now

Newest members :

Chemical_Algorithm ulquiore
omg Dre Hid ongobab
Franky666

Casino Royale: 1



Will you gain your status as a

- Difficulty: Intermediate
- Flag is /root/flag/flag.sh
- DHCP enabled, tested on V

SHA1: B93AD21074619C860B6976C38BB78684B5C297D9

Stack Overflows for Beginners: 1

```
File Edit View Search Terminal Help
level0kali:~$ id
uid=1000(level0) gid=1000(level0) groups=
level0kali:~$ ./level0ne
buf is:
key is: 0x42424242
$ id
uid=1001(level1) gid=1000(level0) groups=
```

A series of challenges to test basic stack

Starting as level0 exploit a binary owned

There are 5 flags to collect:

- /home/level1/level1.txt
- /home/level2/level2.txt
- /home/level3/level3.txt
- /home/level4/level4.txt
- /root/root.txt

Each flag is the corresponding users password on the next challenge

To start boot the machine and login as:

SHA1: EDB2C5A38FF256C3291735E8C3C249271A5C1F42

- Download VMs
- Check SHA1
- Lisez les Walkthrough

CTFTime.org

CTF TIME[CTFs](#)[Upcoming](#)[Archive](#)[Calendar](#)[Teams](#)[FAQ](#)[Contact us](#)[About](#)[Sign in](#)

Team rating

[2019](#) [2018](#) [2017](#) [2016](#) [2015](#) [2014](#) [2013](#) [2012](#) [2011](#)

Place	Team	Country	Rating
1	dcua		344,692
2	OpenToAll		266,765
3	voidka		249,201
4	WreckTheLine		245,277
5	p4		236,376
6	0daysober		225,120
7	LC+BC		188,144
8	bi0s		179,673
9	FireShell		166,730
10	Dragon Sector		166,397

[Full rating](#) | [Rating formula](#)

Upcoming events

[Open](#) [High-School](#) [Academic](#)

Format	Name	Date	Duration
	VolgaCTF 2019 Qualifier On-line	ven, mars 29, 15:00 — dim, mars 31, 15:00 UTC	2d 0h 92 teams
	b00t2root '19 On-line	ven, mars 29, 17:30 — sam, mars 30, 17:30 UTC	1d 0h 26 teams

Past events

[With scoreboard](#) [All](#)

Securinets CTF Quals 2019

mars 24, 2019 16:00 UTC | On-line | [Weight voting in progress](#)

Place	Team	Country	Points
1	dcua		46,120*
2	zer0pts		33,645
3	Sudo_root		28,874

[435 teams total](#) | [Tasks and writeups](#)

Insomni'hack 2019

mars 23, 2019 03:00 UTC | Switzerland, Geneva | [Weight voting in progress](#)

Place	Team	Country	Points
1	LC+BC		142,000*
2	p4		103,356
3	Dragon Sector		84,343

[20 teams total](#) | [Tasks and writeups](#)

Teaser CONFidence CTF 2019

mars 17, 2019 11:00 UTC | On-line

Place	Team	Country	Points
1	hxp		49,900
2	Balsn		34,153
3	Dranon Sector		27 712

A vos claviers

