

INTRODUCTION AUX CTF



@Becode Melissa ben abdelkader

C'EST QUOI UN CTF ?

LES DIFFÉRENTS TYPES DE CTF.

Qu'est-ce qu'on
flag ?



COMMENCER LES CTF.

POURQUOI CTF ?

Qu'est-ce que le Ctf ?

MODÈLE BASIQUE

- En équipe
- Challenges de sécurité qui donnent des « flags »
- Flags qui rapportent des points
- L'équipe ayant le plus de points gagne

GÉNÉRALEMENT ENTRE 24 ET 48H

- On échange du sommeil contre des flags
- Moins long pour les CTF sur place

DES PRIX POUR LES PREMIERS

- Des places pour la conf, qualification pour une finale

Les différents types de CTF.

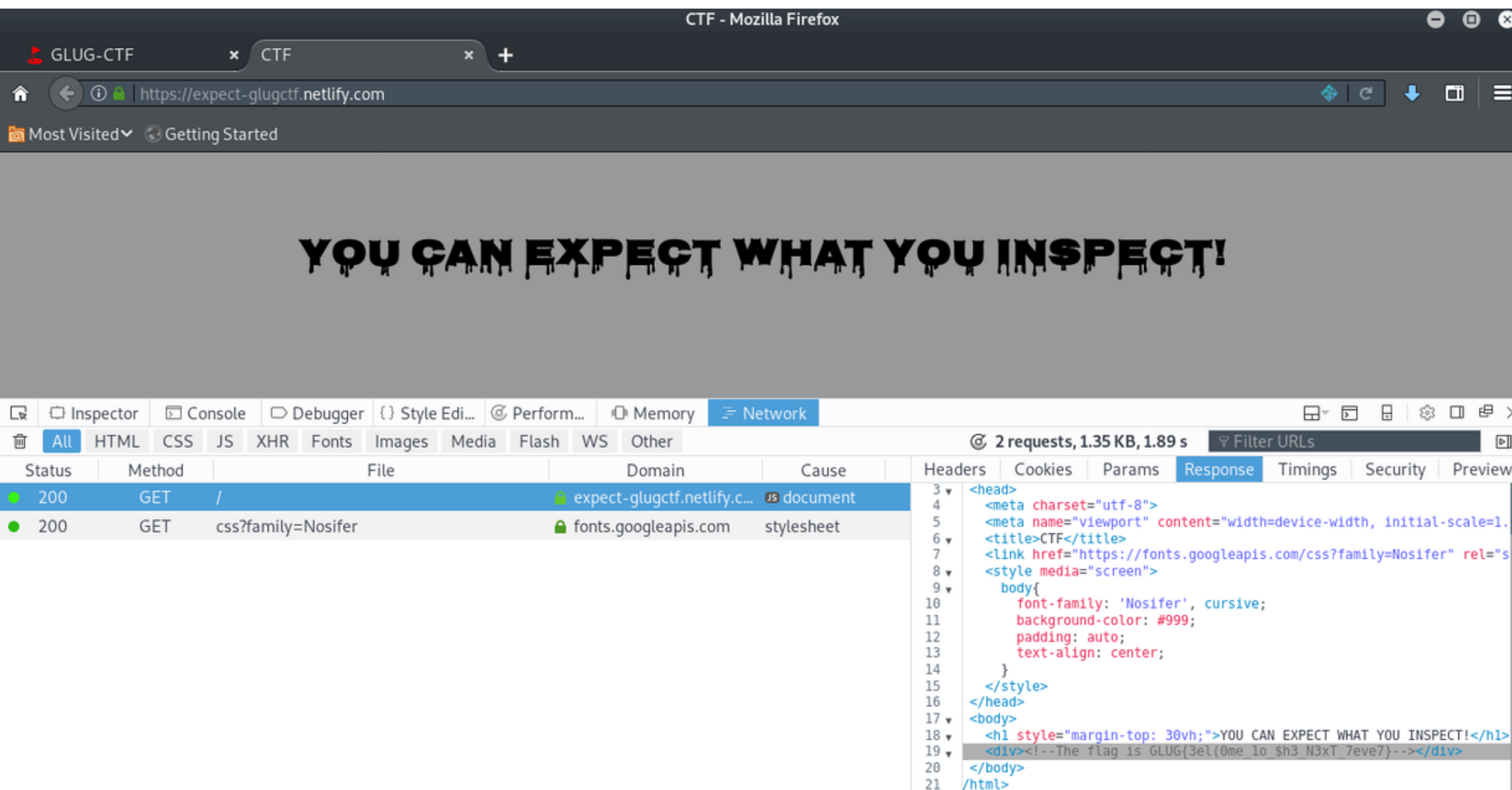
STYLE JEOPARDY

Dans cette variante, les joueurs résolvent certains problèmes pour acquérir des « drapeaux » (une string de texte spécifique) pour gagner.

ATTAQUE-DÉFENSE

Dans ce type, deux équipes sont créés : l'équipe **rouge** (qui tente de percer le système) et l'équipe **bleue** (qui tente de défendre le système).

Exploitation Web



- UNE APPLICATION WEB EST MISE À DISPOSITION
- UNE OU PLUSIEURS VULNÉRABILITÉ(S) « WEB »

On est en souvent « blackbox »

- LE BUT DE L'ÉPREUVE EST VARIABLE :

Devenir administrateur de l'application

Obtenir de l'exécution de code

Lire un fichier

Lire une base de données

Cryptographie

Alphabet shift

-4 ▼

Cipher text:

PDA LWOOSKNZ BKN PDA YDWHHAJCA LWCA EO: YNULPK

decrypt

Clear text:

THE PASSWORD FOR THE CHALLENGE PAGE IS: CRYPTO

encrypt

- EXPLOITATION D'UNE VULNÉRABILITÉ DE CRYPTOGRAPHIE
- ON NOUS DONNE UN MESSAGE CHIFFRÉ
- INPUT TRÈS VARIABLE POUR NOUS DONNER L'ALGORITHME :

Binaire

Scripts

Spécifications de l'algorithme

Forensics

①

- recherche d'information et de traces

②

- Validation de la preuve numérique

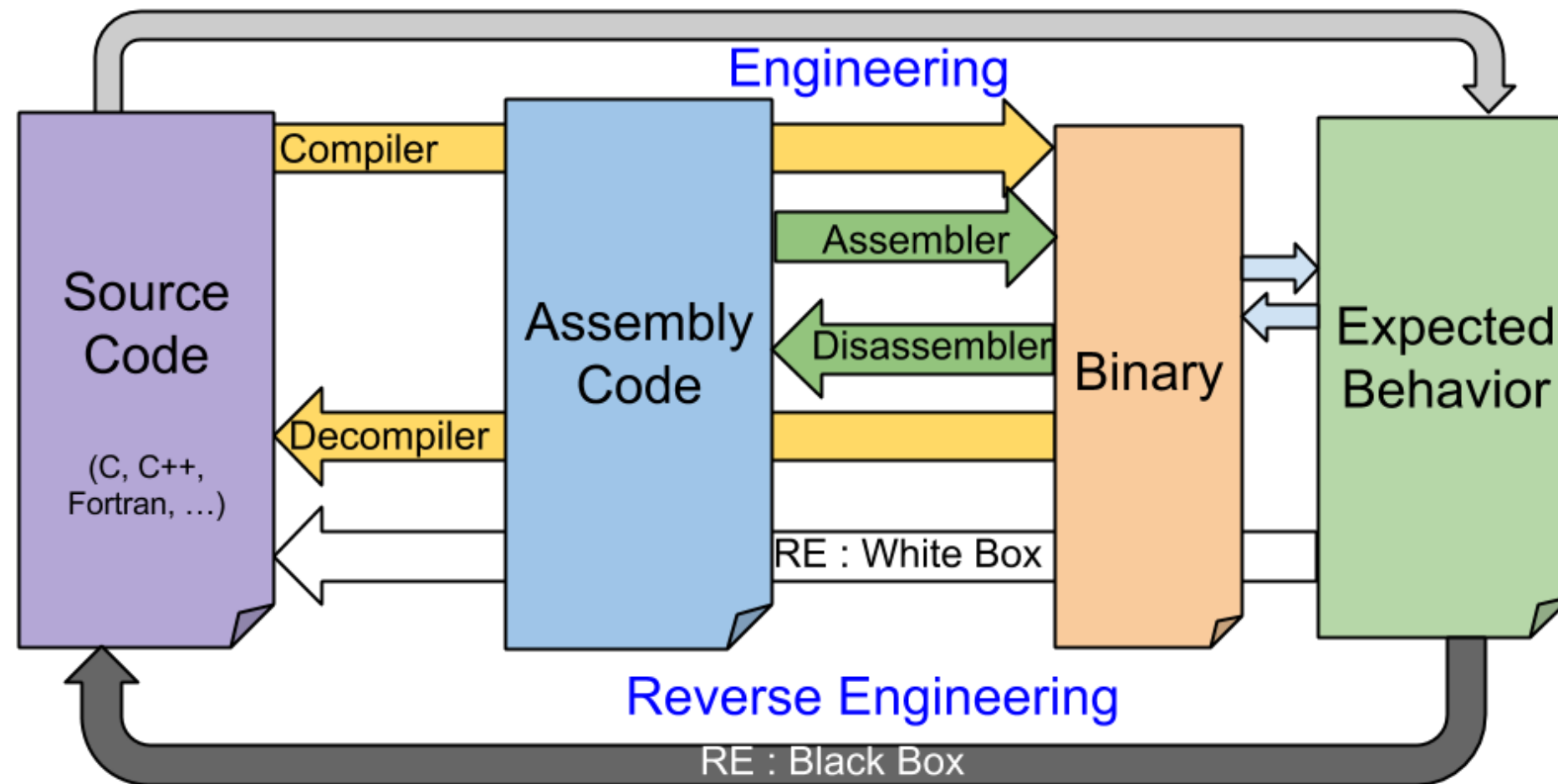
③

- Exploitation des traces

- **CHALLENGE D'INVESTIGATION NUMÉRIQUE:**

Traces mémoires
Fichiers de journalisation
Captures réseaux (rejoint le réseau)

Reverse engineering



- UN FLAG CACHÉ DANS UN BINAIRE
- IL FAUT LE « REVERSE » AFIN DE LE TROUVER

Keygen
CrackMe

Blue team-Red team (Attaque/Défense.)

1

Des services vulnérables sont exposés:

- Si ils ne répondent plus, l'équipe perd des points
- Exploiter les services sur les serveurs des autres équipes pour récupérer des flags
- Patcher les services sur son propre serveur

2

Généralement sur place:

- Infrastructure compliquée à mettre en ligne (mais ça existe : iCTF)
- Format classique de finale

3

La rapidité est très importante:

- On doit gagner le maximum de temps

4

Être malin :

- Voler les exploits des autres
- Denis de Service (dans le respect des règles)

5

Savoir ce qu'on fait:

- On peut facilement briser une règle sans le vouloir
- Bien connaître les règles, pour mieux les contourner

Let's play !

POUR COMMENCER...

- Pas besoin de compétences, c'est là qu'on apprend
- Besoin de personne

POUR PROGRESSER...

- Une équipe c'est mieux !
- BrainStorming
- Partage de connaissances
- Lire des write-ups
- ÉCRIRE des write-ups

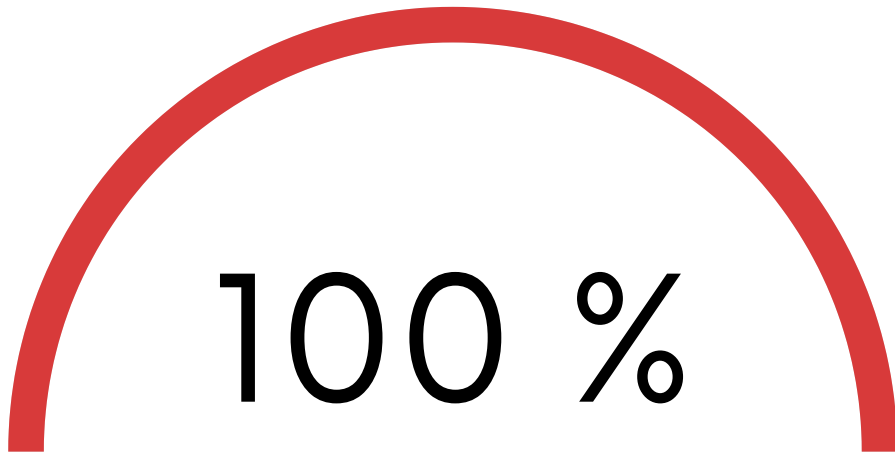
POUR FINIR...

- Se qualifier / déplacer en CTF sur place
- Amusez vous !



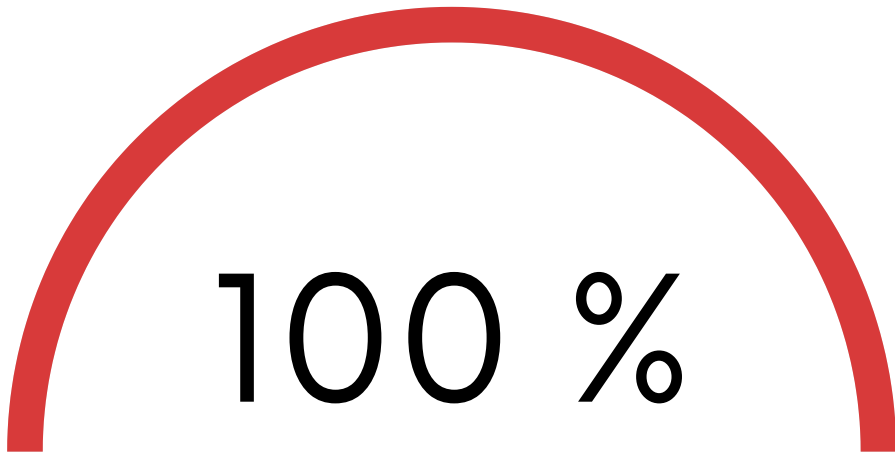
Pourquoi CTF ?

CTF est un passe-temps idéal pour ceux qui s'intéressent à la résolution de problèmes ou à la cybersécurité.



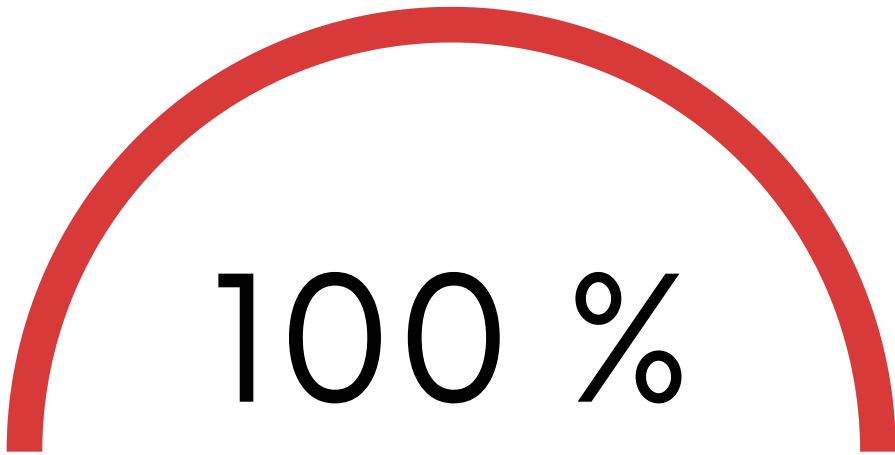
100 %

PROGRESSER EN SÉCURITÉ



100 %

FAIRE DE LA COMPÉTITION !



100 %

S'AMUSER!



<<N'OUBLIEZ
JAMAIS ils y a un
secret DANS tout
ceci
Ils faut
ESSAYE>>

Useful CTF tools

Reverse

GDB	ILSpy (.NET)
IDA Pro	JD-GUI (Java)
Immunity Debugger	FFDec (Flash)
OllyDbg	dex2jar (Android)
Radare2	uncompyle2 (Python)
nm	Any hex editor
objdump	Exe unpackers
strace	Resource unpackers
	Compilers

Stegano

OpenStego	Gimp
OutGuess	Audacity
Steghide	MP3Stego
StegFS	ffmpeg
pngcheck	Own tools

Forensics

dd	ExifTool
strings	Any hex editor
scalpel	DFF
TrID	CAINE
binwalk	The Sleuth Kit
foremost	Volatility

Networking

Wireshark, tshark	tcpdump
OpenVPN	netcat, telnet
OpenSSL	nmap

Scripting

Any text editor or IDE
Programming language for quick scripting
e.g. python (with modules)

Crypto

Cryptool	John the Ripper
hashpump	Online tools
Sage	Modules for python

Ressource

Apprentissage

<http://ctfs.github.io/resources/> - Introduction aux techniques CTF courantes telles que la cryptographie, la stéganographie, les exploitsWeb (incomplet)

<https://trailofbits.github.io/ctf/forensics/> - Trucs et astuces relatifs aux défis/scénarios CTF typiques

<https://ctftime.org/writeups> - Explications des solutions aux défis passés du CTF

Pratique

<https://ctflearn.com> - Une collection de divers défis soumis par les utilisateurs destinés aux nouveaux arrivants

<https://overthewire.org/wargames/> - Une série de défis de style pwn de plus en plus difficiles. (Commencez par la série des bandits)

<https://2018game.picoctf.com/> - CTF annuel limité dans le temps désormais disponible pour s'entraîner

<https://capturetheflag.withgoogle.com/beginners-quest>

Ressource en plus

<https://ctftime.org> - Suivi des événements CTF

<https://github.com/apsdehal/awesome-ctf> - Liste complète d'outils et lectures complémentaires

Repo github d'outils :

<https://github.com/sbilly/awesome-security>

<https://github.com/Laxa/HackingTools>