Les fichiers sont disponibles sur le serveur http://labo971.fr/CTF

CYBERSECURITE, DEVIENS UN DETECTIVE DU NUMERIQUE
Ateliers CTF (Capture The Flag)

*(Sécurité web : failles, cryptographie, réseaux, systèmes. Chaque défi résolu fourni un **flag**)*

Activité 1 : Peut-on faire confiance à tout le monde sur les réseaux sociaux ?

☐ Oui ☐ Non

Activité 2 : Une photo peut-elle révéler des informations ?

https://jimpl.com/

Answer : _____

Activité 3 : Les mots de passe !

Un mot de passe « 123456 » est-il sécurisé ? ☐ Oui ☐ Non

Comparer les mots de passe suivants : azerty, Collège2026, T !g3r-92+Bleu

https://www.security.org/how-secure-is-my-password/

https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe

Activité 4 : Can you decode the following?

VEhNe2p1NTdfZDNjMGQzXzdoM19iNDUzfQ==

https://www.base64decode.org/fr/ *ou* *https://gchq.github.io/CyberChef/*

Answer : _____

Activité 5 : Meta meta. Find the flag.

Find_me_1577975566801.jpg

https://jimpl.com/

Answer (OwnerName) : _____

Les fichiers sont disponibles sur le serveur http://labo971.fr/CTF

Activité 6 : Something is hiding. That's all you need to know.

Extinction_1577976250757.jpg

#steghide extract -sf Extinction.jpg (avec Kali Linux)
Où
https://futureboy.us/stegano/decinput.html
Answer : THM{******_**_*****_**_**_***_****}

Activité 7 : QRrrrr. Find the flag.


QR_1577976698747.png

https://zxing.org/w/decode.jspx

Answer : _____

Activité 8 : Lire le fichier exécutable (binaire) suivant : hello_1577977122465.hello
Ce fichier est au format ELF 64 bits.
Sous Linux, ELF (Executable and Linkable Format) est le format le plus courant de fichiers binaires.

https://gchq.github.io/CyberChef/
Answer : _____

#strings hello_1577977122465.hello (Kali Linux)
#file hello_1577977122465.hello (Kali Linux)

*La commande « **strings** » permet d'extraire et afficher toutes les chaînes de caractères incluses dans un exécutable.*

*La commande « **file** » affiche les caractéristiques de l'exécutable passé en paramètre.*

*Le « **reverse engineering** » consiste à étudier le comportement d'un système afin d'en comprendre son fonctionnement interne. Il permet de :*

- *analyser des programmes malveillants*
- *améliorer la sécurité / rechercher des failles*
- *contourner des protections logicielles*
- *altérer le comportement d'un programme*

Référence : https://blog.maxds.fr/reverse-engineering-intro-radare2/

Les fichiers sont disponibles sur le serveur http://labo971.fr/CTF

Activité 9 : Gauche, droite, gauche, droite… Rot 13 est trop banal. Résolvez ce problème.

MAF{atbe_max_vtxltk}

https://www.dcode.fr/chiffre-cesar

Answer : _____

Activité 10 :

[redacted] dark_1578020060816.png

https://www.aperisolve.com/

ou

#/home/kali/tools/stegsolve.jar (Kali Linux)

Answer : _____

Activité 11 :

 QRCTF_1579095601577.png

https://zxing.org/w/decode.jspx

Answer : _____

Références :

https://tryhackme.com/room/ctfcollectionvol1

[FR] TryHackMe - Plein de petits challenges sympas - CTF collection Vol.1 - EASY - YouTube