

Présentation

*Je répond au nom de **Diallo Mamadou Abdoulaye alias Threecubejr** je fais la 12eme Science Mathématiques à Conakry au groupe Scolaire **Hamas de Kissosso***

Découverte

En recherchant sur internet pour savoir s'il y avait un HACKER Guinean je suis tombé sur un post Facebook de **Nanamou** qui parlais d'une organisation d'un ctf qui aura lieu le 20 février et je me suis dis que ça sera la bonne manière pour moi de connaître les **Hackers ou défenseur Guinéens**. Alors j'ai pas hésité à m'inscrire même en tant que Débutant et attendre le jour de cet imminente **CTF**.

- **COMMENCEMENT**

Quelques heures avant le commencement du Défi on a été invité à assister à un live sur Facebook à 19h pour nous communiquer les conditions du défi et c'est bien terminé.

À 20h je reçois mes identifiant de connexion par e-mail.

Voici les challenge que j'ai pu faire et je vous explique comment je l'ai fait

Capture_Canada

*Pour ce challenge on avait devant nous un formulaire d'un site Web de la **CyberBadCorp** qui est en cours de construction et notre objectif était d'interagir avec leurs serveurs afin de trouver un usage à non sollicité.*

Procédure :

- **Lire l'énoncé**


Alors je ne sais pas pour vous mais moi quand j'ai un challenge ou un devoir qui m'est attribué la première chose que je fais est de bien lire l'énoncé et de savoir quels sont les mots et expressions qui me seront utiles pour ce devoir.

Dans cet énoncé j'ai remarqué deux (2) liens mais un (1) seul m'était utile alors j'ai vérifié ce que le liens me donnera comme réponse.

Mais en voyant ces erreurs je me suis pas limité laba car en tant que **HACKER** il faut toujours avoir l'**art** de fouiller dans différents morceaux de codes.

En fouillant un peu dans les **erreurs** que le serveur du **CyberBadCorp** m'a fourni je suis tombé directement sur le flag que je devrais fournir pour valider et avoir des points.

```
File "usr/local/lib/python3.8/dist-packages/flask/app.py", line 2518, in full_dispatch_request
    response = self.full_dispatch_request()
File "usr/local/lib/python3.8/dist-packages/flask/app.py", line 2518, in full_dispatch_request
    rv = self.handle_user_exception(e)
File "usr/local/lib/python3.8/dist-packages/flask/app.py", line 2516, in full_dispatch_request
    rv = self.dispatch_request()
File "usr/local/lib/python3.8/dist-packages/flask/app.py", line 2502, in dispatch_request
    return self.ensure_sync(self.view_functions[rule.endpoint])(**req.view_args)
File "app/app.py", line 32, in register
    r = requests.get('http://'+url+'/'+GCSC(UtillisseZ_t0uj0Ur$_c0ll4b0Rat0R}')
File "usr/local/lib/python3.8/dist-packages/requests/api.py", line 75, in get
    return request('get', url, params=params, **kwargs)
File "usr/local/lib/python3.8/dist-packages/requests/api.py", line 61, in request
    return session.request(method=method, url=url, **kwargs)
```



Threecubejr

Capture Brazil

Vous revoilà aussi dans ce challenge pour découvrir ensemble comment j'ai pu capturer ce flag en moins de quelques heures .

Dans cette challenge <<Les membres de la CyberBadCorp viennent d'avoir accès à une infrastructure critique de la Guinée.>> Nous savons que leurs logs ont été effacés mais l'ANSSI-Guinée avait pris des mesures en amont pour journaliser les actions des éventuels intrus dans ce système en répliquant le fichier de log au fur et à mesure dans l'image du Président.

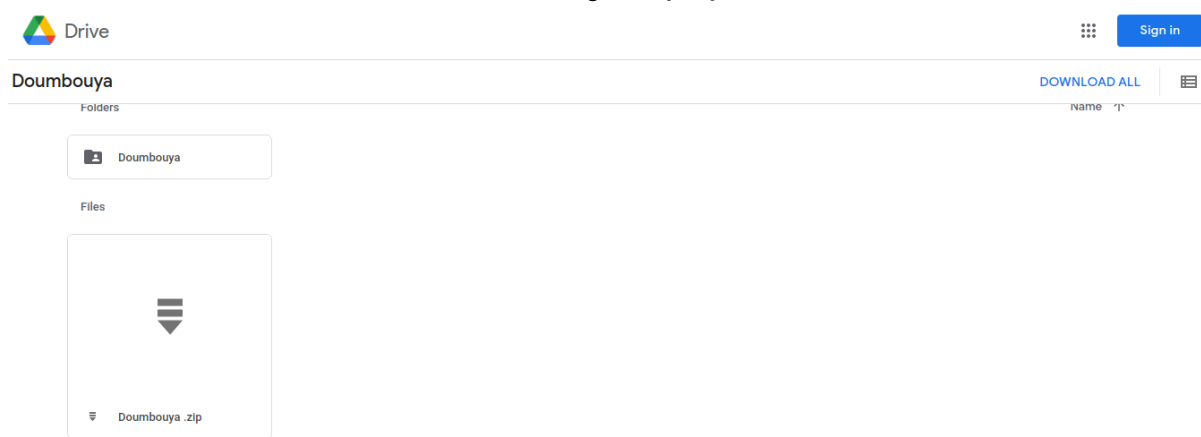
Procédures:

-Lire l'énoncé

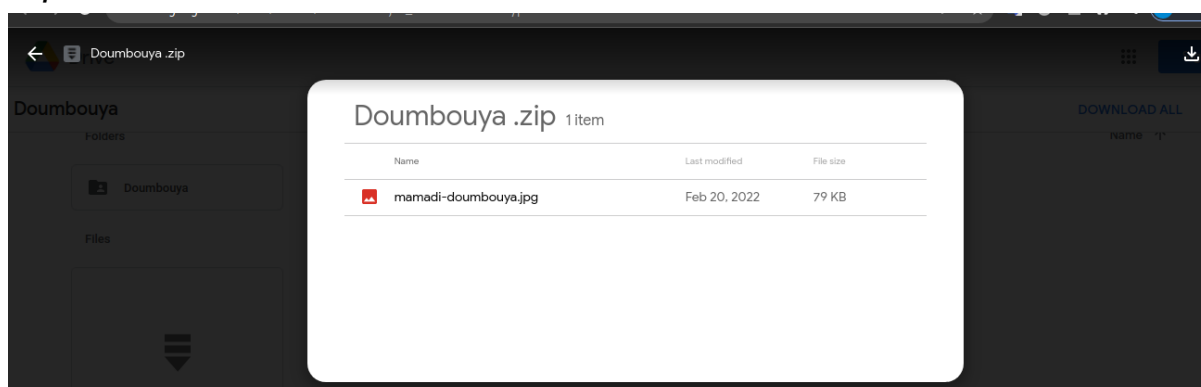
Comme je vous l'ai dit précédemment quand je suis confronté a un challenge je n'oublie jamais de lire et relire l'énoncé afin de bien me situer sur le sujet auquel je suis confronter. En tant que **Hacker Defenders** tout ce que nous avons en disposition est une image qui nous permettra de savoir ce qui a pu se passer tout au long de de cette cyber-attaque



En cliquant sur le lien dans l'énoncé j'ai été redirigée vers un document drive nommé **Doumbouya.zip** qui est ci-dessous.



Mais dans ce fichier Doumbouya.zip se trouve a l'interieur une photo aussi nomme mamadi-doumbouya.jpg que vous verrez en bas sur cette capture.



Pour nous, notre objectif est de savoir tout ce qui a pu se passer au moment de cette Cyber-attaque. Alors pour cela j'ai téléchargé le fichier zip afin de relever quelques informations sensibles pour mon enquête. Nous voila dans notre terminal Kali avec notre fichier zip Mais c'est un fichier zip alors pour la dézipper j'utilise la commande suivante:

\$ unzip Doumbouya.zip

```
(kali@kali)-[~/Downloads]
$ ls
app-debug.apk      blo.txt      hash.txt      note.zip      rsa.hash      ssh2john.py
BD_application_mobile.csv  burpsuite_pro_v2022.2.jar  id.hash      poeme-14fevrier.txt  script.py.txt  stegseek_0.6-1.deb
BD_application_mobile.db'  cacert.der  id_rsa      'renseignements-algerie (1).txt'  secrethash.txt  secrets.kdbx
bloman.txt         Doumbouya.zip  mamadi-doumbouya.jpg.out  renseignements-algerie.txt  secrets.kdbx  secret.zip
blomanvpn.pem

(kali@kali)-[~/Downloads]
$ unzip Doumbouya.zip
```

Comme vous pouvez le voir maintenant dans mon terminal que j'ai une photo appelé **mamadi-doumbouya.jpg**

```
(kali@kali)-[~/Downloads]
$ ls
app-debug.apk      blo.txt      hash.txt      note.zip      rsa.hash      ssh2john.py
BD_application_mobile.csv  burpsuite_pro_v2022.2.jar  id.hash      poeme-14fevrier.txt  script.py.txt  stegseek_0.6-1.deb
BD_application_mobile.db'  cacert.der  id_rsa      'renseignements-algerie (1).txt'  secrethash.txt  secrets.kdbx
bloman.txt         Doumbouya.zip  mamadi-doumbouya.jpg.out  renseignements-algerie.txt  secrets.kdbx  secret.zip
blomanvpn.pem

(kali@kali)-[~/Downloads]
```

Maintenant que j'ai la photo c'est pas fini car je dois avoir plus d'informations pour mon enquête mais pour ça je vais utiliser un outil tellement populaire appelé **exiftool**.

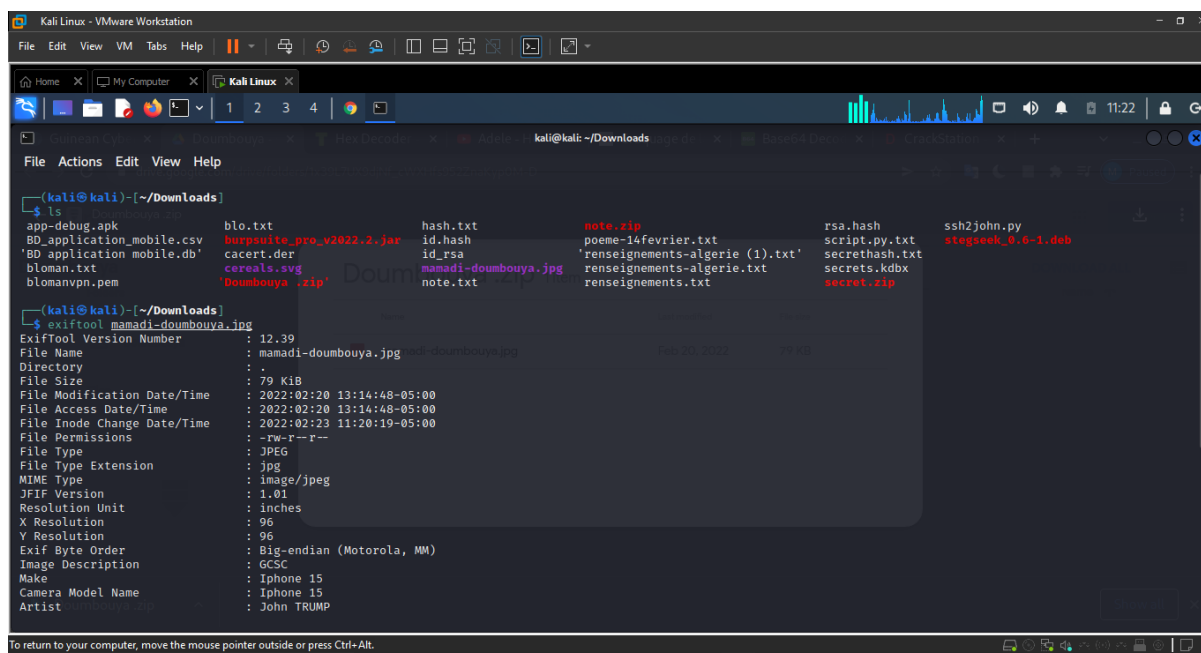
exiftool est une ligne de commande indépendante de la plate-forme et une application graphique pour la lecture, l'écriture et l'édition de métadonnées d'images et de fichiers multimédias.

pour l'installer sur Kali j'ai utiliser la commande suivante :

\$ sudo apt install libimage-exiftool-perl

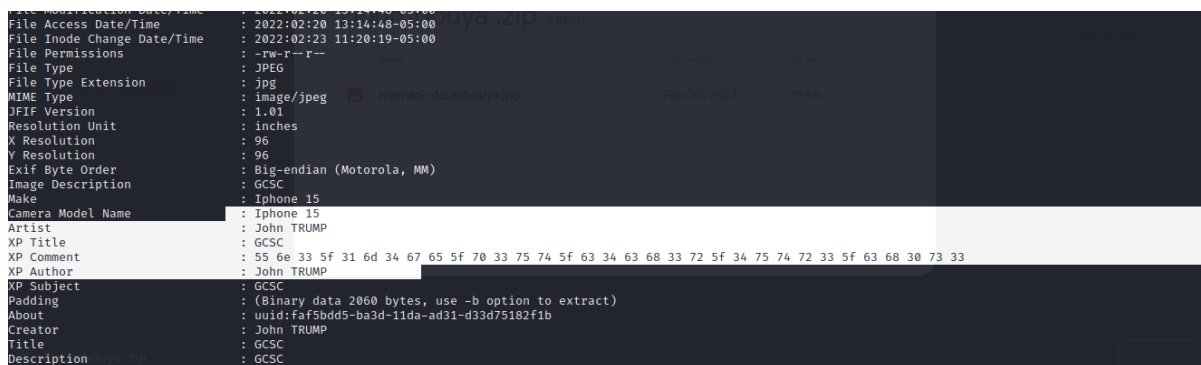
Après l'installation d'exiftool je commence la recherche d'informations sur la photo en faisant :

\$ exiftool mamadi-doumbouya.jpg

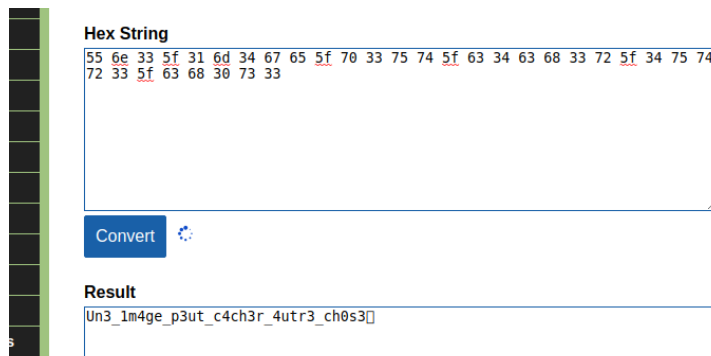


Et voilà seulement quelques secondes nous avons plusieurs informations utiles pour notre enquête.

*Dans ces informations je trouve un nom qui est sûrement le nom du Hacker de la **CyberBadCorp** et un commentaire qui est en Hexadécimal que je dois vraiment déchiffrer.*



*Pour déchiffrer un code Hexadécimal plusieurs outils sont disponible en ligne mais moi j'ai préféré utiliser un site disponible et gratuit en ligne qui est **online-toolz.com** qui m'a permis de déchiffrer le commentaire rapidement.*



En déchiffrant ce commentaire elle me dit qu'une image peut cacher autre chose mais à quoi ça serait cet autre chose alors je devrais fouiller aussi pour voir quelques infos cachées sur cette image. Pour ça aussi j'ai utilisé un outil formidable de la Stéganographie qui est steghide.

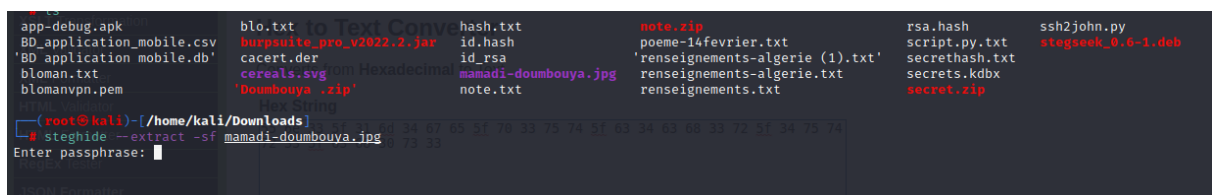
Steghide est un programme de stéganographie qui cache des bits d'un fichier de données dans certains des bits les moins significatifs d'un autre.

Pour l'installer sur kali j'ai fait :

\$ sudo apt-get install steghide

Ainsi pour extraire l'image j'ai utilisé la commande qui suis :

\$ steghide -extract -sf mamadi-doumbouya.jpg



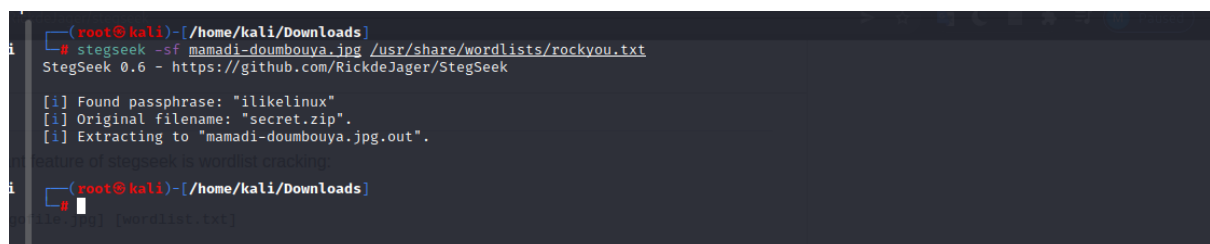
Mais oh la c'est pas gagné l'image me demande d'entrer des **passphrases** pour l'extraire mais je la connais pas alors je vais essayer de cracker ce passphrase en utilisant l'outil **stegseek** et mon wordlist **rockyou.txt**.

Pour ça j'ouvre un autre terminal et j'entre les commandes suivantes:

\$ stegseek -sf mamadi-doumbouya.jpg

/usr/share/wordlists/rockyou.txt

Comme vous pouvez voir sur mon écran en bas



On vient de cracker le passphrase qui est "ilikelinux" en moins de quelques secondes et on a aussi trouvé le fichier Original qui secret.zip. Alors sans tarder je me suis retourné dans mon terminal de là où il Y'a **steghide** pour fournir le passphrase que je viens de trouver.

```

root@kali: ~/home/kali/Downloads
ls
app-debug.apk  cacert.der  nanadi-dnoubouya.jpg.out  rsa.hash
80_application_mobile.csv  cernals.svg  note.txt  script.py.txt
80_application_mobile.db  cernals.svg  poeme-14fevrier.txt  secretchiph.txt
blomn.txt  hash.txt  renseignements-algerie (1).txt  secret.kdbx
blomanvpn.pem  id.hash  renseignements.txt  secret.zip
blo.txt  id_rsa  renseignements-algerie.txt  sha2john.py
baptiste_gre_v2022.2.jpg  nanadi-dnoubouya.jpg  renseignements.txt  steghide_0.6-1.deb

root@kali: ~/home/kali/Downloads
# unzip secret.zip
Archive: secret.zip
[secret.zip] flag.txt password:

```

En fournissant le passphrase j'obtiens un autre fichier appelée **flag.txt** que j'ai ouvert en utilisant la commande suivante :

\$ cat flag.txt

```

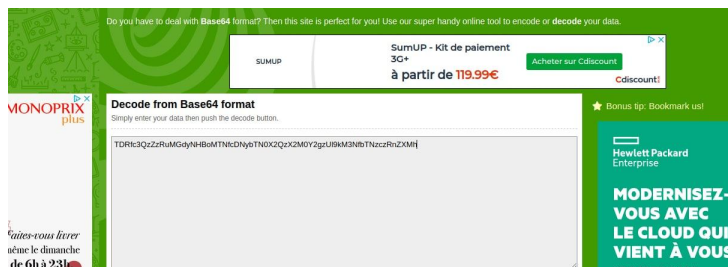
(root@kali)-[/home/kali/Downloads]
# cat flag.txt
Bravo, voici le flag : TDRfc3QzZzRuMGdyNHBoMTNfcDNybTN0X2QzX2M0Y2gzUl9kM3I=

(root@kali)-[/home/kali/Downloads]
#

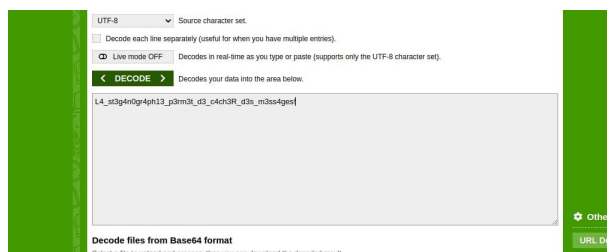
```

Comme vous voyez sur l'image on vient de me donner plusieurs mots crypté que je devrais décrypter pour avoir le flag

Je n'ai pas pu réfléchir trop quel outils je devrais utiliser mais j'ai utilisé le site **décode.org** pour le faire automatiquement



Vous voyez sûrement sur l'image que j'ai mis la phrase dans le site qui me donnera la réponse suivante:



La steganographie peut cacher des messages qui est le dernier mot que je devrais découvrir sur ce lien ensuite de les mettre au format :

GCSC2022{Reponse1_Reponse2_Reponse3_Reponse4_Reponse5}

Le flag était :
**GCSC2022{John
TRUMP_Un3_1m4ge_p3ut_c4ch3r_4utr3_ch0s3!_ilikelinux_secret.zip,
love2linux_L4_st3g4n0gr4ph13_p3rm3t_d3_c4ch3R_d3s_m3ss4ges!}**

Threecubejr

Capture_Madagascar

Pour ce challenge j'ai pas eu perdre plus de temps que les autres.
Ce challenge était si simple car le sujet était **d'accéder au serveur discord de la Guinean CyberSecurityTaskForce**.



Comme vous la voyez sur l'image si dessus on vois l'énoncé et un lien donné

- **Problème rencontré**

Le problème est que quand je cliquais sur le lien qui s'ouvre dans un autre onglet et que je le copie pour la mettre sous forme de flag sa prenais pas. Je me suis dit mais c'est le lien ça pourquoi ça prend pas 😞.

- **Comment j'ai fait**

Dans l'email que **Guinean CyberSecurity TaskForce** m'avais envoyé quand j'ai lu le contenu là où se trouvant la **communication tout au long de la compétition** y'avais le lien du serveur **discord**:

Communications tout au long de la compétition

L'une des philosophies derrière cette compétition est, avant tout, de t'apprendre de nouvelles choses en cybersécurité. Pour cette raison, toute l'équipe reste mobilisée pour te filer quelques pistes si tu bloques vraiment. Rejoins le serveur Discord ici <https://discord.gg/3gvtd8N6>

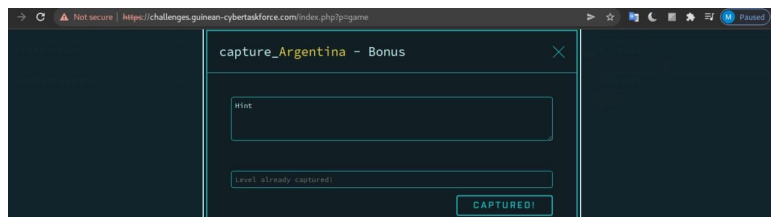
Donc j'ai copié le lien dans l'email et j'ai Collé sous formes de flag en mode
GCSC2022{https://discord.gg/3gvtd8N6}

Capture Argentine

Dans ce challenge c'était plus simple que le précédent car celui-ci était un bonus pour l'effort que nous avons fourni pour participer à cette compétition.

Comme je l'ai dis dans mes précédentes explications qu'il faut toujours lire l'énoncé alors ce challenge était basé sur ça.

Pour trouver ce flag il suffisais justement de lire cet énoncé qui est en bas



Alors pour le faire j'ai justement lus l'énoncé qui me disais << Hint >> et j'ai appliquer alors on m'a donné le flag que j'ai oublié de faire la capture.

Capture Congo Kinshasa

Dans ce challenge que j'ai eu la possibilité de faire est qu'un de nos agents du service contre-espionnage à mis la main sur un fichier crypté de la CyberBadCorp. Voir l'énoncé en bas sur la photo

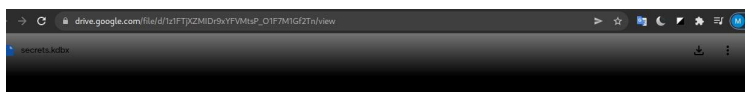


Comme chaque challenge on a toujours un objectif dans chaque challenge donné et ici notre objectif était d'aider le service du contre-espionnage à accéder à ce fichier crypté.

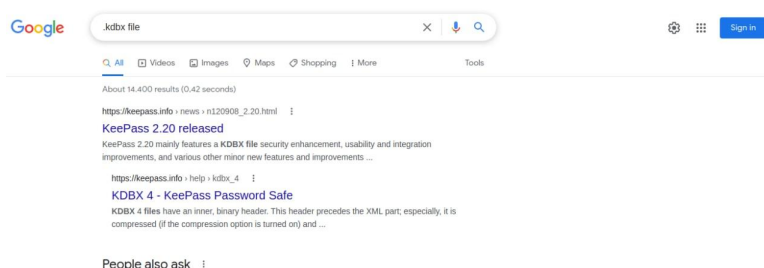
étape: vous le devinerez sûrement la première était de lire l'énoncé et bien comprendre le sujet.

En lisant l'énoncé se présente toujours un lien en bas que j'ai cliquer pour voir le résultat que ça me donne.

En cliquant sur ce lien j'apparais sur cet interface de Google drive avec un type de fichier rare que j'ai vu qui s'appelle **Secret.kdbx**



Voyant ce fichier, c'est ma première de voir un fichier du type **.kdbx**, alors comme tout autre hacker ma première à faire était de faire une recherche Google pour obtenir quelques informations.



Alors ici on me donne des résultats me disant **KeePass** qui a un outil de commande dans **kali**. J'ai téléchargé le fichier **secret.kdbx** pour pouvoir la déchiffrer et avoir des informations.



Vous pouvez le voir dans mon terminal **Kali** que j'ai téléchargé l'image et il restait plus que l'exploitation.

L'exploitation

*Pour déchiffrer mon fichier **secret.kdbx** j'ai utilisé un outil très populaire qui est **John the ripper** qui permet de casser des hashes ou d'autres etc...*

*Mais pour cracker un fichier avec **John the ripper** il faut la transformer en hash ce qui va nous permettre de le faire très vite.*

Ainsi pour la transformer en hash j'ai fait la commande suivante :

\$ ***KeePass2john*** ***secret.kdbx***

```
kali@kali:~/Downloads
# keepass2john --secret.kdbx
keepass2john --secret.kdbx
crackmapexec smb 10.10.10.10 --u 'Administrator' --H '5e10c7bb3429878544781997d481e91937738bba25d7584796417247c7666fb1b979932da0b55af55196e7a794829f9c4646e785149e721c077450ef959811fad57b12c3241b86359a330ae2647c630e437a3ab350b'
```

Je viens de mettre mon **secret.kdbx** en **hash** et la prochaine étape est de déchiffrer cette hash. Mais pour la déchiffrer j'ai utilisé **john**.

*vous la voyez sur l'image j'ai exécuté John puis j'ai défini le **fichier de hachage** ainsi avec le paramètre **—show** pour afficher le **mot de passe** qui sera donner.*

```
[kali@kali:~/Downloads]# cat john_ggcrthash.txt
secrets:rellK000

1 password hash cracked, 0 left

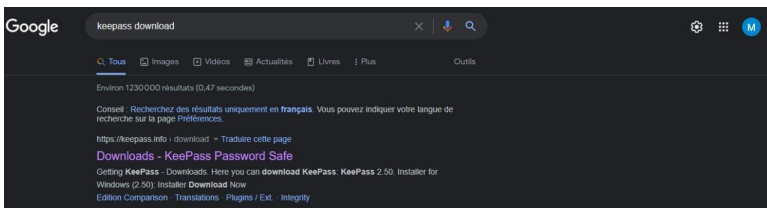
[kali@kali:~/Downloads]#
```

Seulement quelques secondes après j'ai obtenu un mot de passe qui est : **rellik000** et ce mot de passe m'aidera à ouvrir le dossier **secret.kdbx**.

*J'ai ouvert mon **navigateur Chrome** pour télécharger le logiciel **KeePass** et ensuite accéder au dossier secret.*

Il me suffisait justement d'écrire 2 mot pour la télécharger

KeePass Download



*Et enfin que j'ai obtenu le logiciel que je voulais alors il est temps d'ouvrir ce dossier secret de la **CyberBadCorp**.*

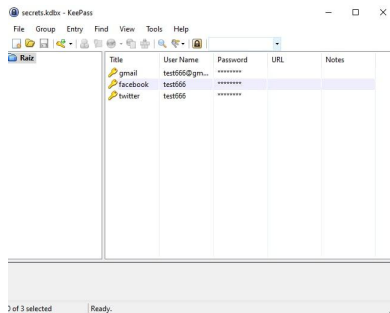


Et ben là il me demande d'entrer le mot de passe mais vous le savez bien que j'ai déjà le mot de passe qui est : **rellik000**

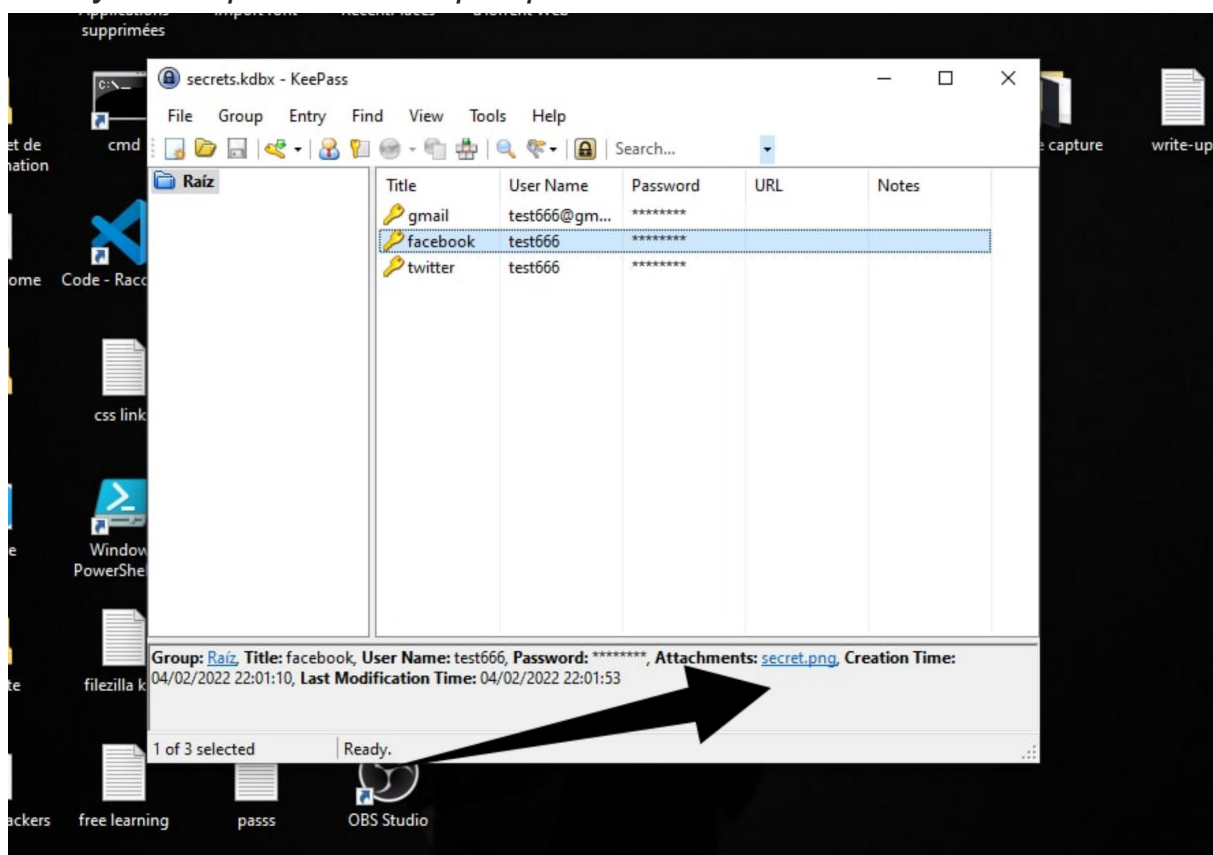
Le voir sur mon terminal

```
~(kali@kali) ~/Downloads
└─$ ./secretshashtest -p
secrets:rellik000
password hash cracked, 0 left
```

Alors c'est pas un problème il me suffisait juste de copier ce mot de passe et le coller dans le champ mot de passe et d'entrée OK qui me donnera ça.

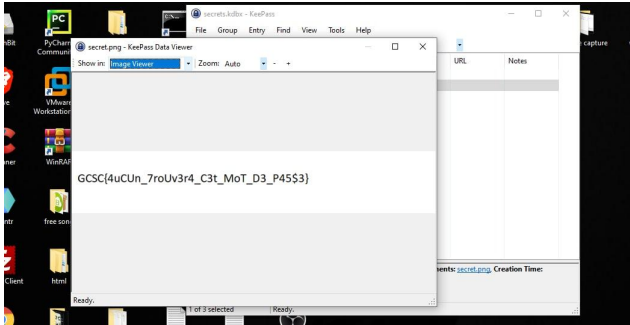


Mais j'ai regarder le mot de passe des comptes n'étais pas affichés mais y'avais quand même quelques choses en bas.



Je vois un lien d'une photo qui est **secret.png** et qui est vraiment une image alors je l'ouvre et devinez quoi je tombe direct sur le flag mais sous le format d'une photo.

Voici la flag



J'ai pris cette flag pour la valider et obtenir mes points.

Capture_Nigeria

On se retrouve enfin dans le dernier challenge que j'ai pu faire.

Dans ce challenge Les régions minières du pays attirent de plus en plus la CyberBadCorp.

Trois de leurs membres décident de s'installer dans la région de Kamsar afin de dépouiller le plus d'entreprises d'exploitation.

En cours de chemin, ils s'arrêtent un moment dans un village pour manger et se reposer avant de reprendre la route. Ils en profitent aussi pour recharger leurs appareils dans un télécentre.

Le gérant du télécentre, agent secret, dump le contenu de leurs téléphones qu'il te transmet à des fins d'analyse pour des questions de sécurité nationale.

Lors de tes analyses, tu remarques qu'à un moment donné, tous les trois ont utilisé le même téléphone pour se connecter à une application de messagerie instantanée étrange.

Tu as vite retrouvé la base de données reliée à cette application. Maintenant, trouver leurs mots de passe.

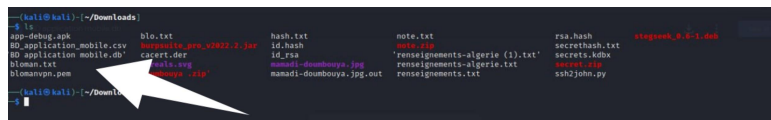
Objectif: trouver leurs mots de passe

Le lien donné dans l'énoncé que j'ai cliquer me donne la base de données d'une application mobile étrange.

Fichier : en bas



J'ai téléchargé le fichier de l'application que je vous montre à l'instant dans mon terminal



- **Exploitation du database**

Pour afficher cette base de donnée de l'application c'était pas trop difficile car le fichier était en **.db** et moi pour l'ouvrir j'ai utilisé un outil populaire en informatique appelée **sqlitebrowser** sur **Kali linux**

Pour l'installation de **sqlitebrowser**

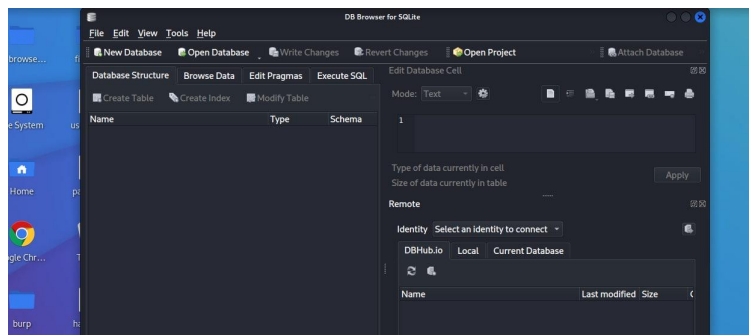
`$ sudo apt-get install sql browser`



Après l'installation pour l'ouvrir j'ai justement entré la commande

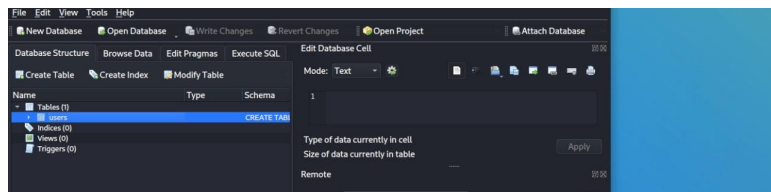
`$ sqlitebrowser`

Qui me donne l'interface de **sqlitebrowser** ci dessous

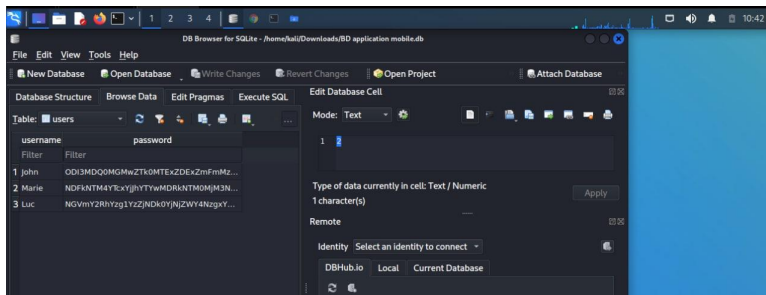


Maintenant que j'ai mon interface alors je dois ouvrir mon fichier **.db**

Comme vous la voyez sur l'image ci-dessus c'est écrit **open Database** j'ai cliquer laba pour importer le fichier

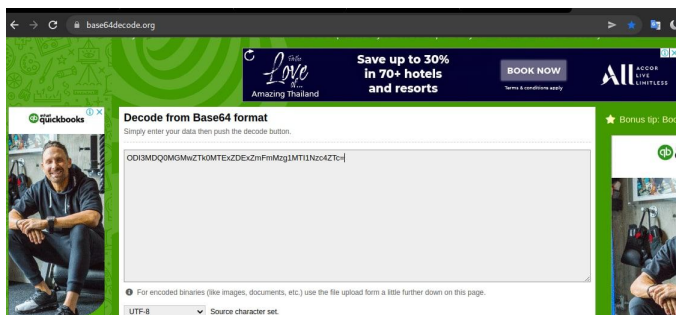


En ouvrant ce fichier je vois un column de nom **user** je dis Humm alors c'est **sensible** et je dois l'ouvrir et en cliquant dessus je tombe sur 3 mots de passe qui sont en **base64**.

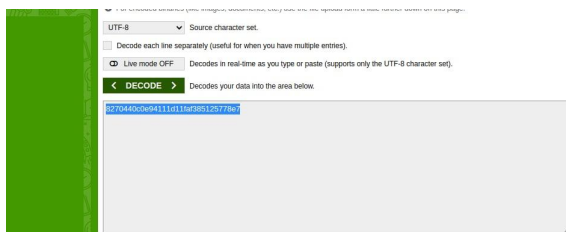


Alors pour les décrypter ça n'a pas été trop difficile car déjà j'ai précédemment déchiffrer quelques **base64** alors il me suffisais juste de rentrer dans le site de **base64.org** et ensuite copier chaque mot de passe et de la déchiffrer en **hash**.

Alors pour ça j'ai copier le Premier mot de passe et je l'ai coller dans **base64.org**



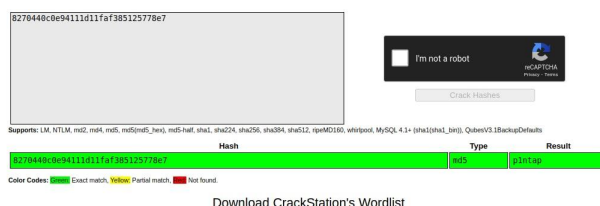
Celle ci me donne ce résultat en bas sur la photo



Mais je vous ai dit que ce **base64** nous retourne un mot de passe en **hash** qu'on doit encore déchiffrer pour obtenir le vrai mot de passe.

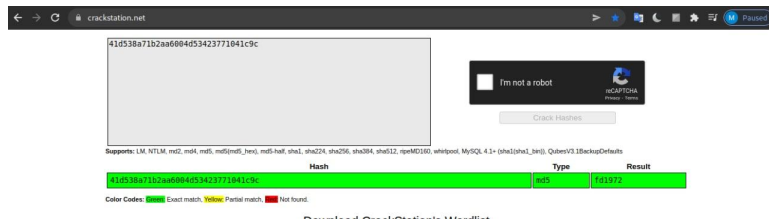
Pour la déchiffrer j'utilise aussi un outil en ligne très populaire au sein des **Hackers** appelées **Crackstation**.

Alors je copie le **hash** et je le colle sur **Crackstation** pour obtenir ce mot de passe sur cette photo.

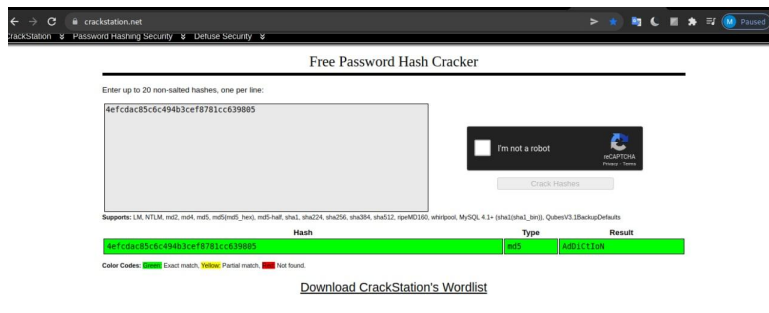


Vous pouvez voir que je viens de trouver le mot de passe **p1ntap**.

Ensuite pour trouver les autres j'ai fait la même méthodes et ça m'a donné les mots de passe.



Ceci est le deuxième mot de passe qui est : **fd1972**
Enfin pour le 3ème mot de passe



Ceci est le troisième mot de passe qui est : **AdDiCtloN**

Le flag du challenge est:
GCSC2022{p1ntap_fd1972_AdDiCtloN}
Threecubejr

-
- Si vous trouvez un challenge que j'ai terminer sans l'expliquer dans ce **write-up** sachez qu'alors que je l'ai oublier sinon j'ai rien laisser
-

Merci de m'avoir écouter jusqu'à la fin et je souhaite le mieux pour nous et à tous les **Guinéens**.

Que Dieu nous bénisse et bénisse la Guinée.