

WRITE-UP MALHOMME POUR LA COMETITION
<https://challenges.guinean-cybertaskforce.com/index.php?p=game>

AFRIQUE DU SUD

capture_South Africa - Au super-maché 

Tu fais de la filature depuis plusieurs semaines sur un membre actif de la CyberBadCorp.
Tous les jours, il se rend dans cette même enseigne pour faire ses courses.
Tu as remarqué qu'il prend assez de temps dans le rayon des céréales.
Pointilleux sur les détails, tu décides de prendre une séquence photos des produits de ce rayon pour les analyser.
Sans surprise, tu trouves que cette image est un peu particulière à vue d'œil.
Arriveras-tu à trouver des informations qui feront avancer ta mission?
Flag: GCSC2022{flag_ici}

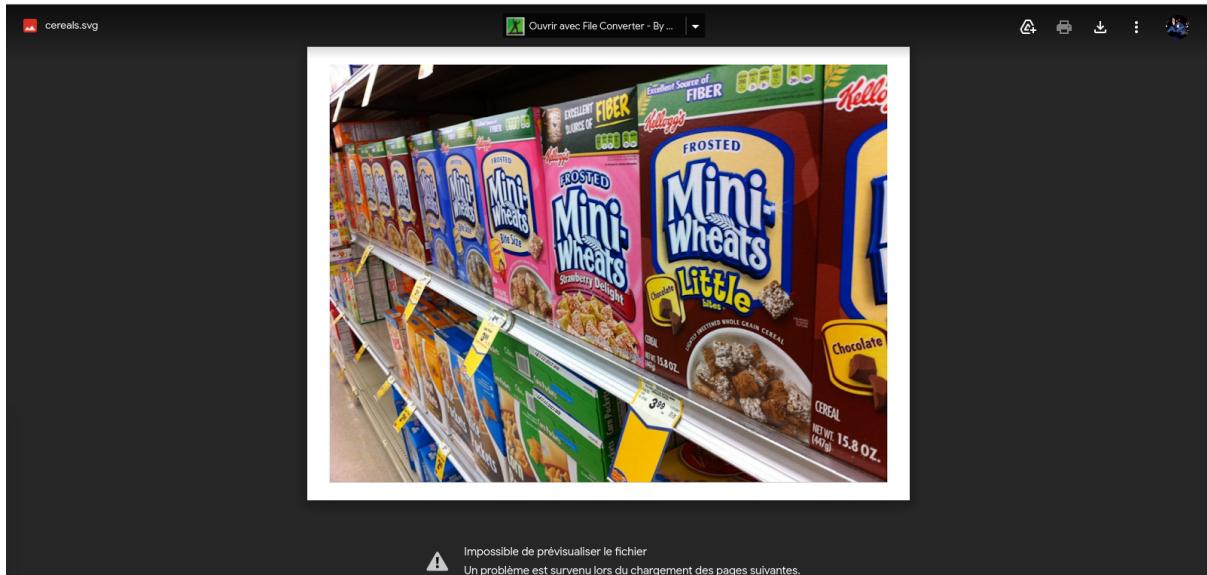
[Link 1]

Level already captured!

CAPTURED!

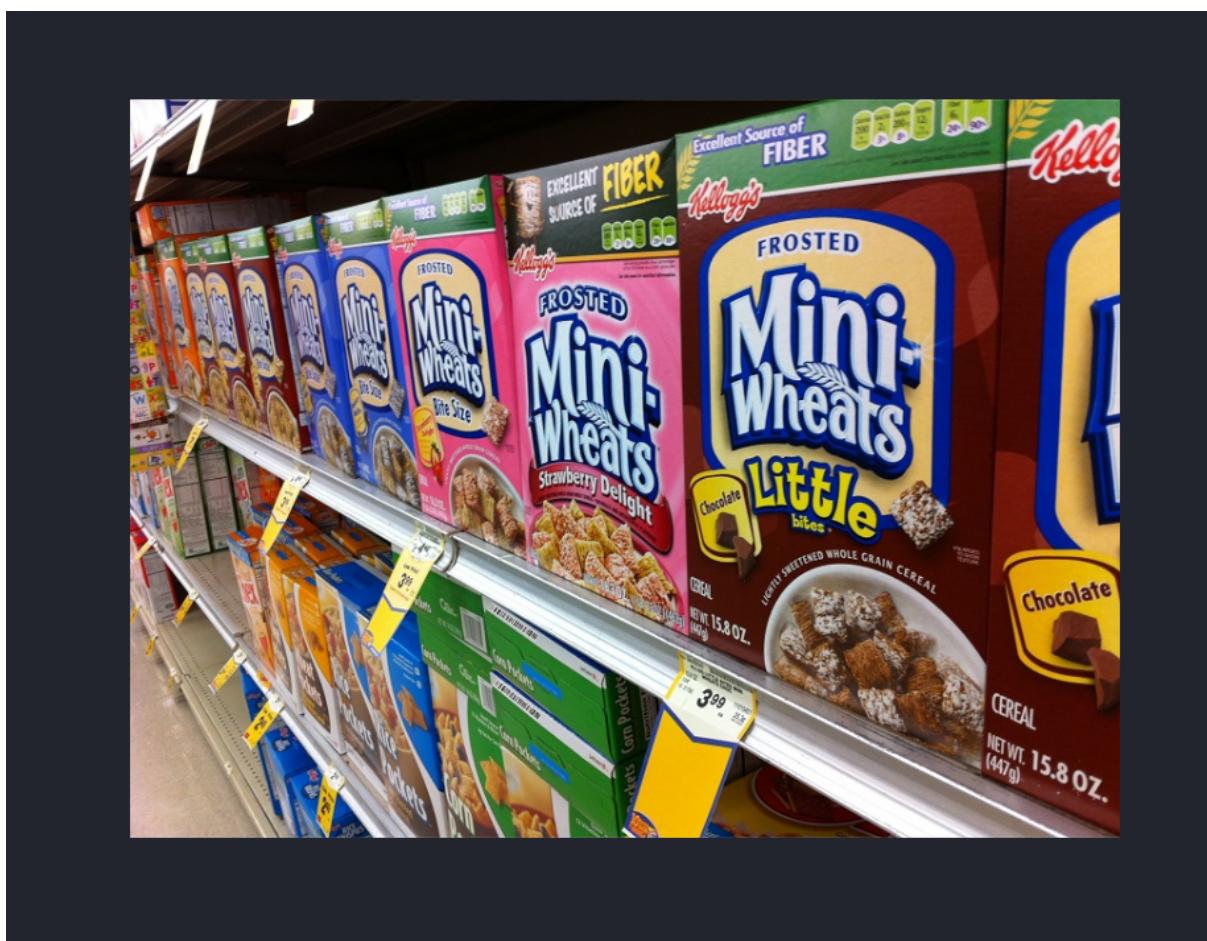
20 PTS	type flag category Steganalysis first_capture PwnProphecy	completed_by > PWNPROPHECY INSIDERBLAST IDEK WORTY PROJECT SEKAI LEOX
------------------	---	--

Lorsque que vous cliquez sur Link 1 vous obtenez la page qui est à l'image suivante.
A ce niveau vous téléchargez le fichier image.



⚠ Impossible de prévisualiser le fichier
Un problème est survenu lors du chargement des pages suivantes.

Après le téléchargement vous obtiendrez l'image suivante.



Je suis rentré dans mon terminal linux pour faire le travail. Là je suis dans le répertoire qui contient les fichiers concernant le challenge.

```
(Malhomme💀 kali) -[~/Images/WRITE-UP GCSC2022/AFRIQUE DU SUD] $ ls  
afriqueDuSud0.png afriqueDuSud3.png afriqueDuSud7.png téléchargement1.png  
afriqueDuSud1_2.png afriqueDuSud4.png afriqueDuSud8.png téléchargement2.png  
afriqueDuSud1.png afriqueDuSud5.png afriqueDuSud9.png  
afriqueDuSud2.png afriqueDuSud6.png cereals.svg  
  
re le travail. Là je suis dans le  
e ch [Malhomme💀 kali) -[~/Images/WRITE-UP GCSC2022/AFRIQUE DU SUD]  
$ strings cereals.svg |  
$ ls -l  
1 févr. 13:08 afriqueDuSud1.png  
1 févr. 13:11 afriqueDuSud2.png
```

Après avoir effectué la fonction strings sur le fichier image au format svg, j'obtiens le résultat suivant.

A ce niveau je remarque deux liens à la fin de ma sortir qui peuvent être lisible par mon navigateur.

Donc voici les deux liens en gras qui m'intéressent, je les mets dans bar d'URL et je tape entre.

```
<image
    width="12.062613"
    height="1.5402763"
    preserveAspectRatio="none"
```

xlink:href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAARkAAABZCAYAAAA6hTwfAAAABHNCSVQICAgIfAhkiAAAAnxJREFUeJzt3EFuwjAUQM
Gm6v2v7K5YFMyTCigp5Idk+D8Khg9seAYY4wvAAAI+X73AAAA8GwiFwCAHJ
ELAECoYAUAIefkAgCQ8zM7cRzHn79vP8JwO37/owyz41fXPbv+s87P5lodn51/9
7yr+XaPv+q53x+fvX73frPrHn2uq/I35929bnWfs/Pdv/7RdVfzzu7/6H1X/8fZOXB32
Wqe/34/7O7z3X30qfvi0c/j2bqz6161b67uo9lcn/bcVsdnr5/NO5vj6nO7ut5q3tX53f2
42xtn5919P8zWm12/O+eVzzPf5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA5IhcAg
ByRCwBAjsgFACBH5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA5IhcAg
AjsgFACBH5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA5IhcAg
BH5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA5IhcAg
CNyAQDIEbkAAOSIXAAAckQuAAA5IhcAg
EbkAAOSIXAAAckQuAAA5IhcAg
SIXAAAckQuAAA5IhcAg
kQuAAA5IhcAg
COyAUAIefkAgCQI3IBAMgRuQAA5IhcAABfgFRxiK6XYCKsAAAAABJRU5Erk
Jggg==

 id="image29"
 x="150.91969"
 y="70.401352"
 transform="rotate(38.524062)" />

<image
 width="12.062613"
 height="1.5402763"
 preserveAspectRatio="none"

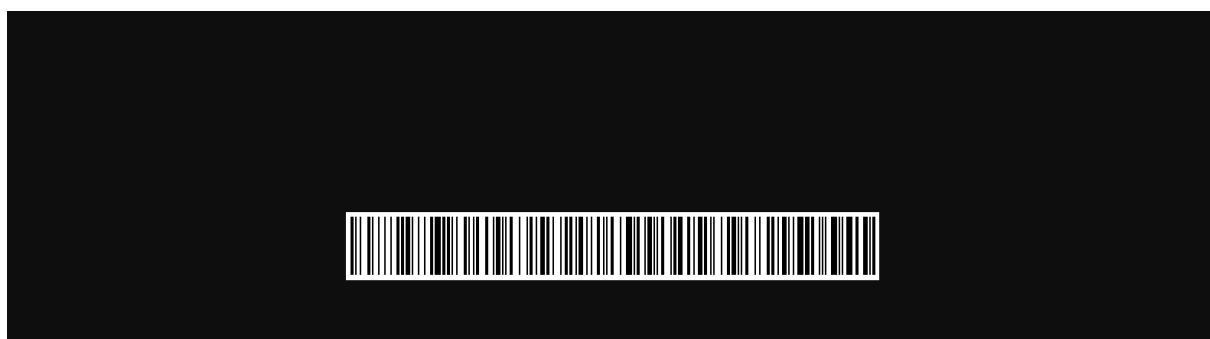
xlink:href="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAARkAAABZCAYAAAA6hTwfAAAABHNCSVQICAgIfAhkiAAAAnxJREFUeJzt3EFuwjAUQM
Gm6v2v7K5YFMyTCigp5Idk+D8Khg9seAYY4wvAAAI+X73AAAA8GwiFwCAHJ
ELAECoYAUAIefkAgCQ8zM7cRzHn79vP8JwO37/owyz41fXPbv+s87P5lodn51/9
7yr+XaPv+q53x+fvX73frPrHn2uq/I35929bnWfs/Pdv/7RdVfzzu7/6H1X/8fZOXB32
Wqe/34/7O7z3X30qfvi0c/j2bqz6161b67uo9lcn/bcVsdnr5/NO5vj6nO7ut5q3tX53f2
42xtn5919P8zWm12/O+eVzzPf5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA5IhcAg
ByRCwBAjsgFACBH5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA5IhcAg
AjsgFACBH5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA5IhcAg
BH5AIAkCNyAQDIEbkAAOSIXAAAckQuAAA5IhcAg
CNyAQDIEbkAAOSIXAAAckQuAAA5IhcAg
EbkAAOSIXAAAckQuAAA5IhcAg
SIXAAAckQuAAA5IhcAg
kQuAAA5IhcAg
COyAUAIefkAgCQI3IBAMgRuQAA5IhcAABfgFRxiK6XYCKsAAAAABJRU5Erk

**C0yAUAIEfkAgCQI3IBAMgRuQAA5lh
AAByfgFRxiK6XYCKsAAAAABJRU5ErkJgg== "**

id="image29-2"
x="134.73402"
y="69.453888"
transform="rotate(33.907631)" />

On obtient les deux résultats suivant respectivement selon chaque lien:

← → ⌂ G | ➤ ⋆



Je remarque que c'est du code bar.



Je les télécharge puis j'utilise l'outil lecteur de code bar en ligne Free Online Barcode reader.



408.737.7092

Free Online Barcode Reader

1. Select barcode types

1D: Code 39, Code 128...

PDF417

Postal: IMB, 4state ...



QR code

DataMatrix

Driver License, ID cards



2. Select Image File (PDF, TIFF, JPEG, BMP, GIF, PNG, WMF, WEBP)

téléchar...ent1.png

Maximum file size: 12 Mb.

3.

Et j'obtiens le flag. C'est facile n'est ce pas !



408.737.7092

Free Online Barcode Reader

To get such results using [ClearImage SDK](#) use TBR Code 103.

If your **business** application needs barcode recognition capabilities,
email your technical questions to support@inliteresearch.com
email your sales inquiries to sales@inliteresearch.com

File: [téléchargement1.png](#)

Pages: 1

Barcodes: 1

Barcode: 1 of 1

Type: [Code128](#)

Page 1 of 1

Length: 28

Rotation: none



Module: 2.0pix

Rectangle: {X=6,Y=6,Width=685,Height=75}

GCSC{baR_c0d3\$_oR_J41L_b4rZ}

ALGERIE

capture_Algeria - Des points tirés (tirets)?

X

La CyberBadCorp vient de recruter un stagiaire débutant pour développer son malware.

Ce dernier ayant appris la cryptographie sur le tas, il pense bien dissimuler les informations sur la prochaine attaque.

Retrouve le nom de l'opération dans le fichier ou lien joint et préviens tes collègues.

Flag : GCSC2022{minuscule(nom_de_loperation)}

[Link 1]

Level already captured!

CAPTURED!

10
PTS

type
flag
category
Cryptanalysis
first_capture
idek

completed_by > IDEK
WORTY
RMD723
PROJECT
SEKAI
PWNPROPHECY

Lorsque je clique sur Link 1, j'obtiens le résultat sur l'image suivante.

C'est du code Morse.

Dot = .

Dash = -

Donc j'ai converti tout le code en code morse.

J'ai utilisé sublime texte et vite remplacé ce qui est par ce qui convient.

```
1 DashDotDashDot DotDotDotDot Dot DotDashDot DotDotDot
2 DashDotDashDot DashDashDash DotDashDotDot DotDashDotDot Dot DashDashDot DotDotDash Dot DotDotDot
3 DashDotDot Dot
4 DotDashDotDot DotDash
5 DashDotDashDot DashDotDashDash DashDotDotDot Dot DotDashDot DashDotDotDot DotDash DashDotDashDot DashDotDashDot DashDashDash DotDashDot
6 DotDashDotDash DotDashDotDashDash
7 DotDashDotDot DotDashDash DashDot DashDotDashDot Dot DashDashDotDot
8 DotDashDotDot DashDashDashDot DashDashDashDot DashDashDashDot DotDashDot DotDash Dash DotDot DashDashDash DashDot
9 DotDashDotDashDot DashDashDashDotDashDash
10 DotDashDotDot Dot
11 DotDashDotDot DashDash Dot DashDotDot DotDot
12 DotDashDashDashDot DotDotDashDashDash DashDot DashDotDashDot DashDashDashDashDot DashDotDashDashDashDot DotDotDashDashDashDash
13 DashDashDashDashDot DashDotDashDashDot DashDotDashDashDot DashDotDashDashDash
14 DotDashDotDashDash DotDotDashDashDot DashDashDashDotDot DotDotDashDot DotDashDotDashDashDot DashDotDashDashDot DashDotDashDashDash
```

```
1 Dot.Dot DotDotDotDot Dot Dot.Dot DotDotDot
2 Dot.pot ||| Dot.DotDot Dot | DotDot Dot | Dot DotDot-| Dot DotDotDot
3 .dotDot Dot
4 Dot.DotDot Dot |
5 Dot.pot Dot-| .DotDotDot Dot Dot.Dot | DotDotDot Dot | DotDot -Dot Dot -||| Dot.Dot Dot-|Dot | DotDot-|
6 Dot.DotDot Dot-| .Dot Dot Dot | DotDot
7 Dot.DotDot Dot-||| Dot | Dot Dot Dot | -| DotDot -||| -Dot
8 Dot.DotDot Dot Dot Dot Dot | | Dot.pot DotDotDot Dot Dot.DotDot DotDotDot Dot-|DotDot | Dot -|DotDot-|
9 Dot.Dot Dot
10 DotDotDot Dot-| .-| Dot -DotDot DotDot
11 Dot | | DotDot-| | DotDot Dot | | DotDot | | DotDot Dot DotDot | | DotDot | | DotDot-|
12 DotDot | | DotDotDot | | DotDotDot DotDotDotDotDot -||| Dot
13 Dot-|Dot-Dot -|Dot -Dot DotDotDot | DotDot | Dot Dot-Dot-Dot | -| Dot Dot-| -|
```

```
1 .Dot Dot DotDotDot Dot Dot Dot DotDotDot  
2 .Dot-Dot -- Dot-DotDot Dot-DotDot Dot -Dot DotDot- Dot DotDotDot  
3 .DotDot Dot  
4 DotDotDot Dot.  
5 .Dot-Dot - .DotDotDot Dot-Dot-Dot .DotDotDot Dot - .DotDot -Dot Dot ... Dot Dot Dot - Dot - DotDot ..  
6 Dot DotDot Dot - Dot .Dot-Dot Dot - DotDot  
7 DotDotDot Dot --- Dot --- Dot Dot-Dot Dot. - DotDot --- -Dot  
8 DotDotDot Dot Dot Dot --- DotDot DotDotDot Dot DotDot Dot DotDotDot DotDotDot Dot DotDot Dot - DotDot ..  
9 DotDotDot Dot  
10 DotDotDot Dot - - Dot - DotDot DotDot  
11 Dot... DotDot... DotDotDot Dot ... DotDot ... DotDot Dot DotDot - - - - DotDot - - DotDot - -  
12 DotDot... DotDotDot... DotDotDot DotDotDotDotDotDot ... Dot  
13 Dot-Dot Dot - Dot - Dot DotDotDotDot. DotDot Dot Dot Dot Dot - Dot Dot - -
```

Après avoir remplacé chaque chose.
J'obtiens la ligne suivante. Et c'est ça du code morse.

J'utilise l'utilitaire cyberchef en ligne pour convertir le codage morse en compréhensible, pour obtenir le flag.

```
14
15 CHERS COLLEGUES DE LA CYBERBADCORP, LANCEZ L'OPRATION "REMORSELESS", LE SAMEDI 12/02/2022 23:59 @GCSTF.TEAM
16
17 Flag : GCSC2022{minuscule(nom_de_loperation)}
18
19
20
21
22 | le final flag - GCSC2022{remorseless}
23
24
```

Après cela je suis les instructions du contexte et j'obtiens mon flag.

```
| le final flag - GCSC2022{remorseless}
```

ANGOLA

capture_Angola - Quelle audace ! X

Les membres de la CyberBadCorp décident de célébrer leur dernier coup qui a permis l'arrêt de nombreux SI de l'administration guinéenne.

Sur la mission depuis plusieurs semaines, tu sais qu'ils communiquent par tous les moyens.

Alors tu tentes le coup par le coup : tu t'y invites et enregistres toutes les musiques jouées à cette soirée.

Tu as vu combien ils étaient en feu particulièrement sur cette musique. Analyse-la et dis-nous ce que tu trouves.

Flag: GCSC2022{flag_ici}

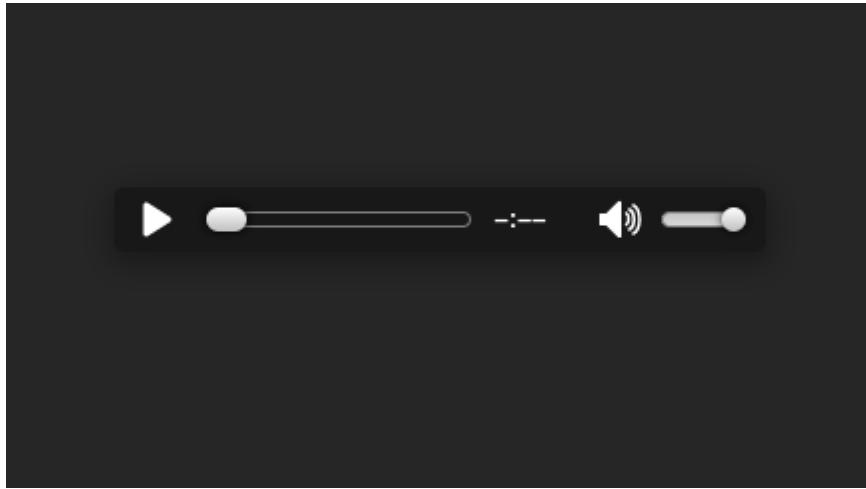
[Link 1]

Level already captured!

CAPTURED!

20 PTS	type flag category Steganalysis first_capture Leox	completed_by > LEOX IOEK PROJECT SEKAI OFSH1LL PWNPROPHECY SETKAT
------------------	---	--

Je clique sur Link 1
J'obtiens l'audio suivante:



J'upload dans Morse Decoder audio online

INTERNATIONAL MORSE DECODERS

Morse Decoder

This is an experimental tool for listening to, analysing and decoding [International Morse code](#) all done in Javascript using the [Web Audio API](#). I know it works in the latest Chrome and Firefox browsers on Windows, it might work in Safari and it just can't work in Internet Explorer. No information from the microphone is transmitted to the server, but the connection to the server is encrypted nonetheless.

If you cannot produce your own Morse code sounds then try using my [Morse code translator](#) to play or download some.

Use the microphone:

Listen Stop

Or analyse an audio file containing Morse code:

Upload Play Stop Filename: "enregistrement vocal.mp3"

Je patiente un peu et à la fin de l'audio j'obtiens le flag suivant qui valide le challenge.

IINEIEIDIE&EIDHTRIESRTTNHIISTIDSEEEEERTKHNEWESMIEWETNETHZ3WESG2ILNEKETOISNTTLE6WTUNLIT-E15YSSSETV
EOMTVUERETEITEIEENOMSBTTYHISMIE'EEEIDTINEMIAEITIEDEEBETINTELENAENINITNTEENTNIEEETONTEEE
MEM E IEE

BECOME A PATIENT
MD Anderson
Cancer Center

[Clear message](#)

WPM

132

Farnsworth WPM

20

Frequency (Hz)

2412

Minimum volume

-60

Maximum volume

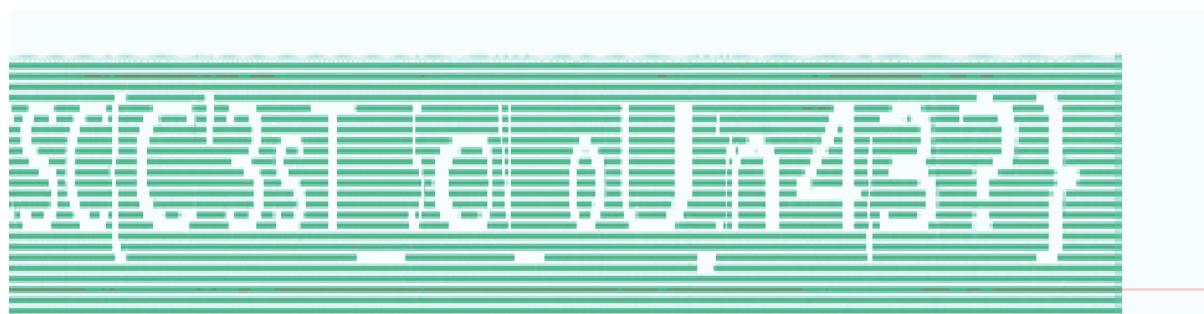
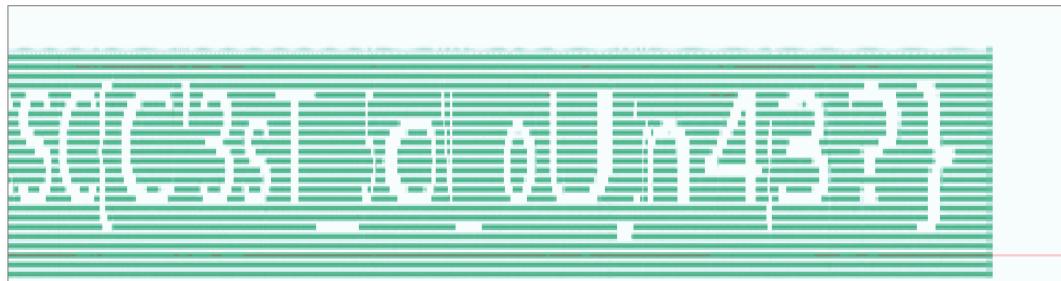
-30

Volume threshold

200

Manual

Manual



CAMEROON

capture_Cameroon - Voler des informations avec classe. Quel art ! 

Cette nuit encore, un nouvel incident de sécurité s'est produit du côté de la préfecture de Kankan.

Après avoir eu un accès au SI, le malveillant tente d'exfiltrer des informations par l'envoi d'une image d'apparence anodine.

Il semble que c'est la technique utilisée par la CyberBadCorp avant que tu ne rejoignes le rang des cybercombattants guinéens.

Analyse attentivement cette image et trouve l'information exfiltrée.

Flag: GCSC2022{flag_ici}

[Link 1]

Level already captured!

CAPTURED!

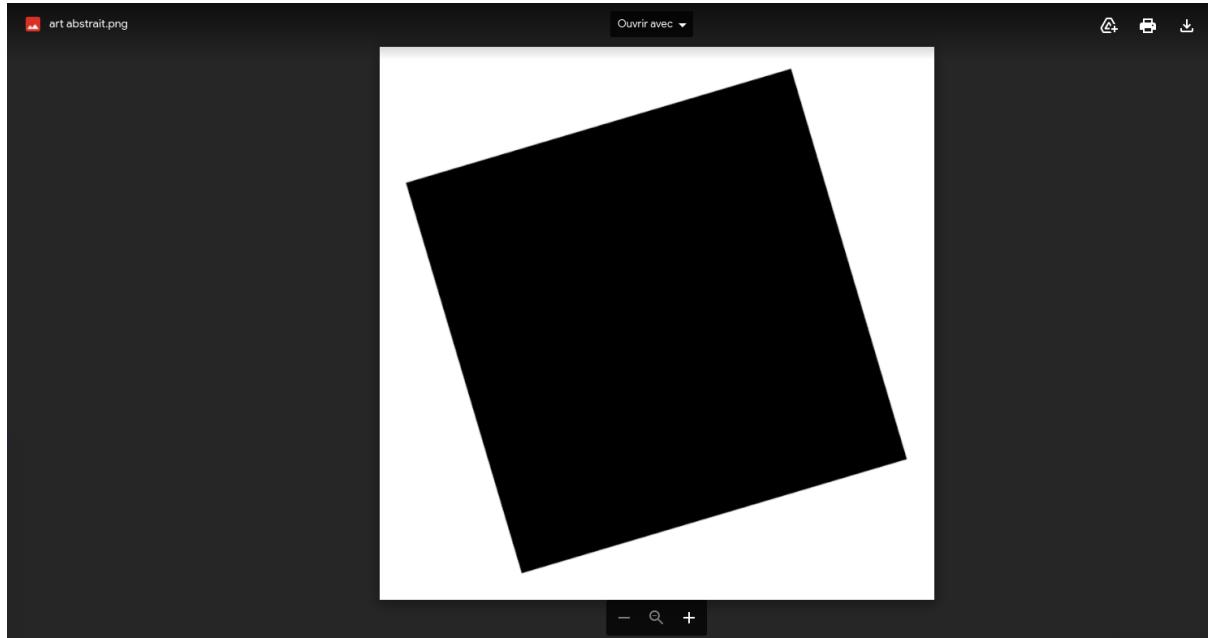
10
PTS

type
flag
category
Steganalysis

first_capture
idek

completed_by > IDEK
WORTY
PROJECT
SEKAI
ABDULSEC
BLACKSNOW229
POULLO

Je clique sur Link 1 et je télécharge l'image, puis je strings dans le terminal.



```
Malhomme@kali:~/Téléchargements/CAMEROON$ ls
'art abstrait.png'
Malhomme@kali:~/Téléchargements/CAMEROON$ strings 'art abstrait.png'
IHDR Malhomme
sRGB Bureau
gAMA
pHYs eille
IDATx^ocuments
,0tE Musique
PDTTL
O&," mages
0::1 vidéos
0::1 Téléchargements
0::1 périphériques
0::1 Système de fichiers
0::1 Volume de 179 Go
0::1 Volume de 124 Go
0::1
WkjJJJ
4'''3S6 courrir le réseau
ruuuQQ
kjjd
SWWWQQ
$'''//O68
>utt
    ggg
UUU%
<(33
W_{u
```

String me donne pas grand chose, alors j'ouvre avec Aperi'Solve

Aperi'Solve

What is this ?

Aperi'Solve is an online platform which performs layer analysis on image. The platform also uses zsteg, steghide, outguess, exiftool, binwalk, foremost and strings for deeper steganography analysis. The platform supports the following images format: .png, .jpg, .gif, .bmp, .jpeg, .jfif, .jpe, .tiff...



Select a file or drag here

SELECT A FILE

SUBMIT

DISABLE

DISABLE

DISABLE

Extract all zsteg files (--extract) ?

Test all options of zsteg (--all) ?

I've got a password !

Aperi'Solve

What is this ?

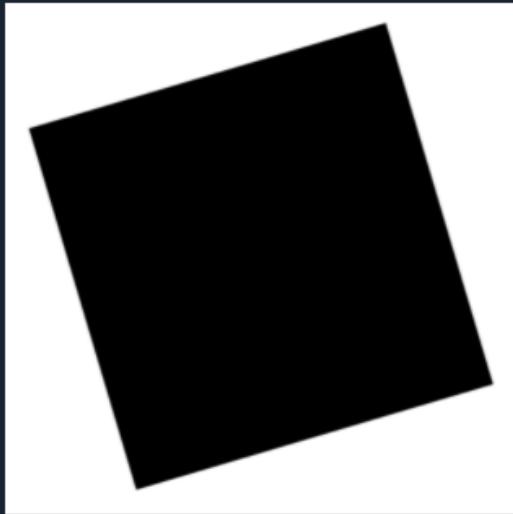
Aperi'Solve is an online platform which performs layer analysis on image. The platform also uses zsteg, steghide, outguess, exiftool, binwalk, foremost and strings for deeper steganography analysis. The platform supports the following images format: .png, .jpg, .gif, .bmp, .jpeg, .jfif, .jpe, .tiff...



art%20abstrait.png

SUBMIT

Informations



[+] NAME(S) : art abstrait.png, artabstrait.png, abstract.png

[+] SIZE : 27.28 ko

[+] FIRST UPLOAD : 20/02/2022 03:44:05

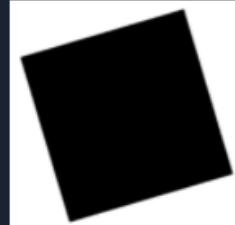
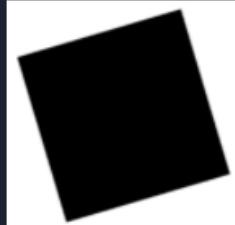
[+] LAST UPLOAD : 21/02/2022 11:35:06

[+] UPLOAD COUNT : 11

[+] COMMON PASSWORD(S) :

View

[+] Superimposed



Et j'obtiens le flag.



GCSC{4bs7r4ct_4rT_i\$_woRtHL3\$\$}

CHAD

capture_Chad - Clé de déchiffrement ou décryptage?

X

Mon Dieu! Le pire est arrivé.

Déterminé à faire tomber la CyberBadCorp, à tout prix, tu as malencontreusement cliqué sur un lien laissé exprès dans le téléphone que tu as analysé.

Cela a crypté uniquement ton rapport d'avancement sur ladite mission.

Retrouve vite la clef de déchiffrement et continue a les traquer.

Flag: GCSC2022{flag_ici}

[Link 1]

Level already captured!

CAPTURED!

50

PTS

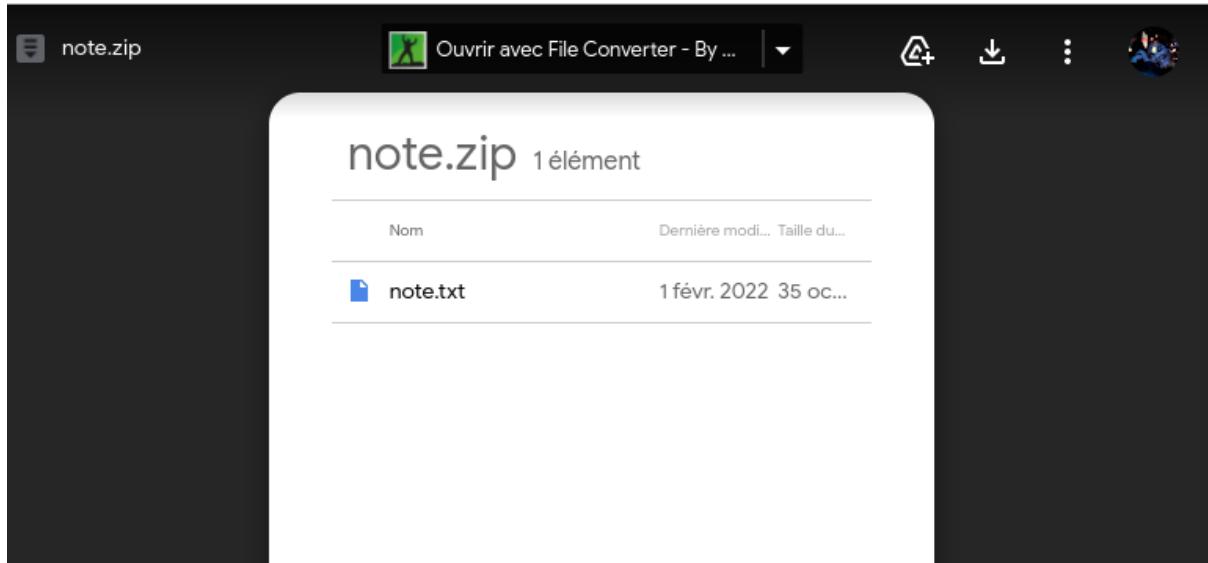
type
flag

category
Cryptanalysis

first_capture
Worty

completed_by > WORTY
OFSH1LL
INSIDERBLAST
IDEK
RMD723
PROJECT
SEKAI

Je télécharge le note.zip puis je j'applique zip2john puis du hashcat avec la liste rockyou.txt et j'obtiens la clé qui me permet d'ouvrir le fichier note.txt.



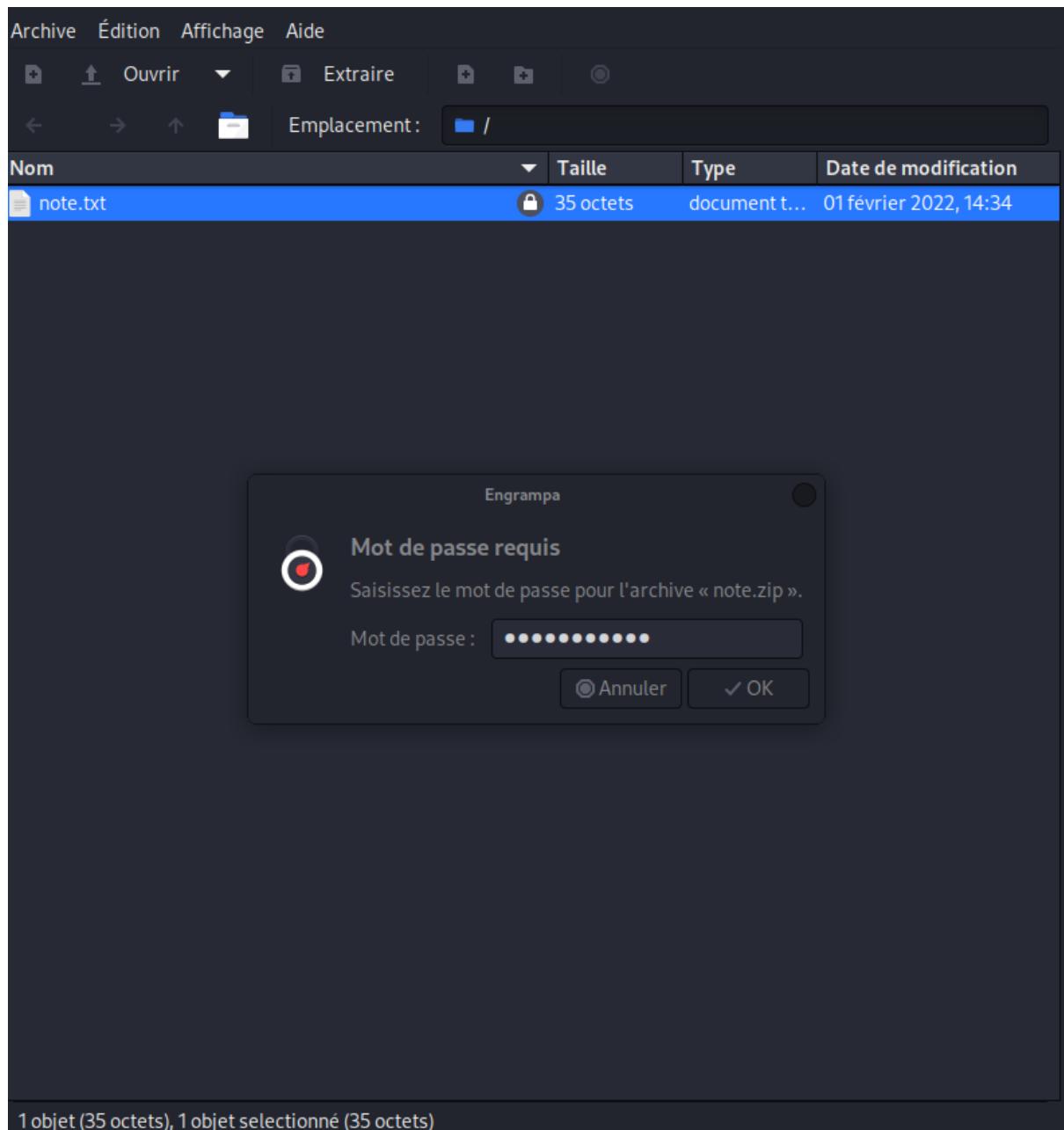
```
Malhomme@...022/TCHAD$ ls
note.zip
Malhomme@kal:~/Images/WRITE-UP GCSC2022/TCHAD$ strings note.zip
ZtAT
note.txt
CZ]
[~/PK
ZtAT
note.txt
Malhomme@kal:~/Images/WRITE-UP GCSC2022/TCHAD$ zip2john note.zip > crack.hash
ver 2.0 note.zip/note.txt PKZIP Encr: cmplen=47, decmplen=35, crc=D4124615 ts=745A cs=d412 type
=0
Malhomme@kal:~/Images/WRITE-UP GCSC2022/TCHAD$ ls
crack.hash
Malhomme@kal:~/Images/WRITE-UP GCSC2022/TCHAD$ cat crack.hash
note.zip/note.txt:$pkzip$1*1*2*0*2f*23*d4124615*0*26*0*2f*d412*Off07062b8da65181bef4b45fc92eb57
472f113ac911676100ab435a5d2f951791cd2aa52db3459b1524cce55b7e2f*$:note.txt:note.zip::note
.zip
Malhomme@kal:~/Images/WRITE-UP GCSC2022/TCHAD$ nano crack.hash
Malhomme@kal:~/Images/WRITE-UP GCSC2022/TCHAD$ cat crack.hash
$pkzip$1*1*2*0*2f*23*d4124615*0*26*0*2f*d412*Off07062b8da65181bef4b45fc92eb57472f113ac911676100
ab435a5d2f951791cd2aa52db3459b1524cce55b7e2f*$:note.txt:note.zip::note.zip
```

```
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHA$ ls
ch3.png cha1.png cha2.png crack.hash flag.png note.zip zip.hash
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHA$ cat crack.hash
$pkzip$1*1*2*0*2f*23*d4124615*0*26*0*2f*d412*0ff07062b8da65181bef4b45fc92eb57472f113ac911676100
ab435a5d2f951791cd2aa52db3459b1524cce55b7e2f*$pkzip$
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHA$ hashcat --help | grep -i "$pkzip$1*1*2*"
 3200 | bcrypt $2*$, Blowfish (Unix)          | Operating System
 s | !"#$%&'()*+,.-/:<=>?@[{}]^_`{|}~
* https://hashcat.net/wiki/#howtos_videos_papers_articles_etc_in_the_wild
* https://hashcat.net/faq/
* https://hashcat.net/discord
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHA$ hashcat --help | grep -i "pkzip"
17220 | PKZIP (Compressed Multi-File)        | Archive
17200 | PKZIP (Compressed)                   | Archive
17225 | PKZIP (Mixed Multi-File)             | Archive
17230 | PKZIP (Mixed Multi-File Checksum-Only)| Archive
17210 | PKZIP (Uncompressed)                 | Archive
20500 | PKZIP Master Key                  | Archive
20510 | PKZIP Master Key (6 byte optimization)| Archive
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHA$ ;|
```

```
Malhomme@kali:~/Images/WRITE-UP GCSC2022/TCHA$ hashcat -a 0 -m 17210 crack.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.5) starting
[...]
Je ne pouvais pas savoir qu'on serais comme ça.
[...]
/sys/class/hwmon/hwmon2/temp1_input: No such file or directory
[...]
Pourquoi tu me hais et je me hais pour la haine et de la haine à
OpenCL API (OpenCL 2.0 pocl 1.8 Linux, None+Asserts, RELOC, LLVM 11.0, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: pthread-Intel(R) Core(TM) i7 CPU M 620 @ 2.67GHz, 2112/4288 MB (1024 MB allocatable), 4MCU
[...]
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
[...]
Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
[...]
Optimizers applied:
* Not-Iterated
* Single-Hash
* Single-Salt
[...]
Je l'aime, je le cache pas.
Tu m'aimes et tu le cache pas.
[...]
I arrive pas vraiment a comprendre ma désicion mais je
sais qu'avec toi je suis heureux pour la vie.
[...]
Watchdog: Temperature abort trigger set to 90c
[...]
Host memory required for this attack: 1MB
[...]
Dictionary cache hit:
* Filename.: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
```

```
Dictionary cache hit:  
*Filename.: /usr/share/wordlists/rockyou.txt  
*Passwords.: 14344385  
*Bytes.....: 139921507  
*Keyspace.: 14344385  
  
S'Amour Réussir?  
Cracking performance lower than expected?  
  
* Append -w 3 to the commandline. Je l'aimais, elle m'aimait.  
This can cause your screen to lag. Ont s'aimais.  
  
* Append -S to the commandline. Je ne pouvais pas savoir qu'on serait comme ça.  
This has a drastic speed impact but can be better for specific attacks. Et on se gueule.  
Typical scenarios are a small wordlist but a large ruleset. L'amour à la haine et de la haine à  
l'amour.  
* Update your backend API runtime / dr suis le right way: amoureux d'elle  
https://hashcat.net/faq/wrongdriver et elle est vraiment amoureuse de moi.  
* Create more work items to make use of our parallelization power: le de temps à temps, juste  
https://hashcat.net/faq/morework pour se rappeler combien de fois, l'un tiens à l'autre.  
  
$pkzip$1*1*2*0*2*23*d4124615*0*26*0*2f*d412*0ff07062b8da65181bef4b45fc92eb57472f13ac911676100ab435a5d2f951791cd2aa52db3459b1524cce55b7e2*f$pkzip$:Catsandcows  
  
Session..... hashcat  
Status.....: Cracked  
Hash.....: $pkzip$1*1*2*0*23*d4124615*0*26*0*2f*d412*0ff070...pkzip$  
Hash.Mode.....: 17210 (PKZIP (Uncompressed))  
Hash.Target.....: $pkzip$1*1*2*0*23*d4124615*0*26*0*2f*d412*0ff070...pkzip$  
Time.Started....: Mon Feb 21 17:40:18 2022 (7 secs)  
Time.Estimated....: Mon Feb 21 17:40:25 2022 (0 secs)  
Kernel.Feature...: Pure Kernel  
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)  
Guess.Queue.....: 1/1 (100.00%)  
Speed.#1.....: 1746.2 kH/s (0.40ms) @ Accel:512 Loops:1 Thr:1 Vec:4  
Recovered.....: 1/1 (100.00%) Digests  
Progress.....: 11296768/14344385 (78.75%)  
Rejected.....: 0/11296768 (0.00%)  
Restore.Point....: 11294720/14344385 (78.74%)
```

2f*\$pkzip\$:Catsandcows



Et j'obtiens le flag pour valider.

```
1  
2  
3  
4 |GCS{p4$sw0rD_cr4ck1nG_br34kZ_GPUs}
```

CONGO-KINSHASA

capture_Congo - Kinshasa - Hasher, c'est crypter? X

Un de nos agents du service de contre-espionnage a mis la main sur un fichier crypté de la CyberBadCorp.

Aide-le à accéder à son contenu.

Flag: GCSC2022{flag_ici}

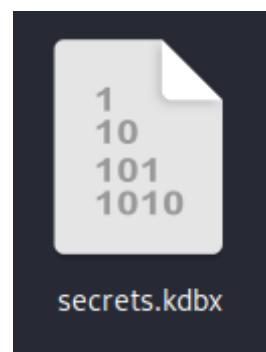
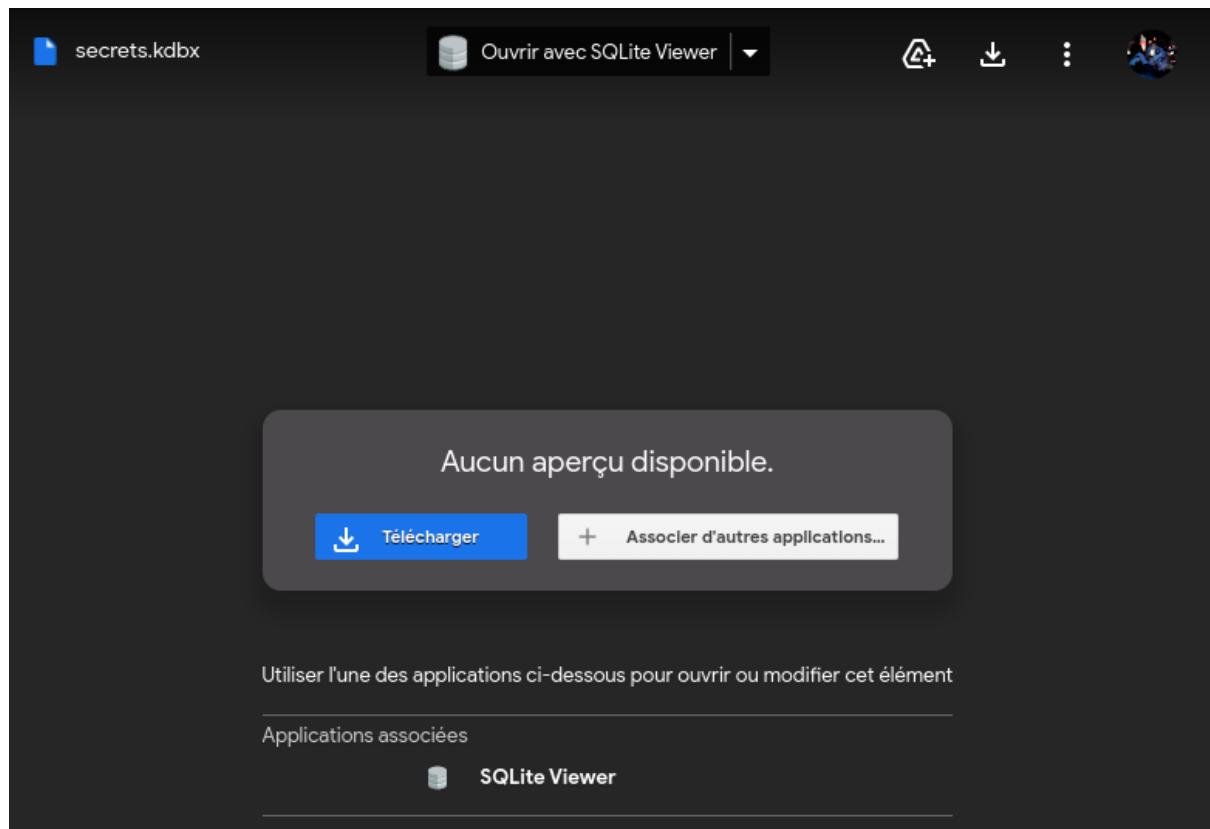
[Link 1]

Level already captured!

CAPTURED!

50 PTS	type flag category Cryptanalysis first_capture Worty	completed_by > WORTY PROJECT SEKAI LEOX PWNPROPHECY RMD723 GCSTF-TEAM NOYORI
------------------	--	---

Je télécharge le fichier secret.kdbx et j'y applique du keepass2john puis du hashcat pour obtenir le mot de passe situé dans le fichier rockyou.txt



```

Fichier Actions Editer Vue Aide
Malhomme@.../KINSHASA $ ls
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ LS
LS: command not found
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ ls
secrets.kdbx
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ keepass2john
Usage: keepass2john [-k <keyfile>] <.kdbx database(s)>
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ keepass2john secrets.kdbx > crack.hash
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ ls
crack.hash secrets.kdbx
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ cat crack.hash
secrets:$keepass$*2*30*0*baeaaca143ecac0a48c76109f1af109db2e1e2c27cc02e59a57317854ba71fb*4b76a
74e00b23ed3ffe5c3a10afcfc8bf0944500c32eda170cd900afad2e5e7*2d244191935a0738bba52abb75844796*4
7247c7668f1b979932dad055a5fd15196e77a948929fca646e785149e721c*0774501ef9598111fad57b12c32411b
863593430aae2647cb30e437a3ab350b
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ nano crack.hash
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ cat crack.hash
$keepass$*2*30*0*baeaaca143ecac0a48c76109f1af109db2e1e2c27cc02e59a57317854ba71fb*4b76a74e00b23
ed3ffe5c3a10afcfc8bf0944500c32eda170cd900afad2e5e7*2d244191935a0738bba52abb75844796*417247c766
8f1b979932dad055a5fd15196e77a948929fca646e785149e721c*0774501ef9598111fad57b12c32411b86359343
Oaae2647cb30e437a3ab350b
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ |
```

Autres questions posées

Comment reconnaître signe Inférieur-superieur ?

If you think you need help by a real human come to the hashcat Discord:

* <https://hashcat.net/discord> est le sigle de supérieur ?

```

Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep keepass
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep Keepass
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep "Keepass"
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep -e "Keepass"
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep -r* "Keepass"
grep : option invalide -- '*'
Usage : grep [OPTION]... MOTIFS [FICHIER]...
Exécutez « grep --help » pour obtenir des renseignements complémentaires.
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep -i "Keepass"
13400 | KeePass 1 (AES/Twofish) and KeePass 2 (AES) | Password Manager
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ |
```

```

Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep -e "Keepass"
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep -r* "Keepass"
grep : option invalide -- '*'
Usage : grep [OPTION]... MOTIFS [FICHIER]...
Exécutez « grep --help » pour obtenir des renseignements complémentaires.
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat --help | grep -i "Keepass"
13400 | KeePass 1 (AES/Twofish) and KeePass 2 (AES) | Password Manager
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ ls /usr/share/wordlists/
dirb/ fasttrack.txt metasploit/ rockyou.txt
dirbuster/ fern-wifi/ nmap.lst wfuzz/
Malhomme@kali:~/Images/WRITE-UP GCSC2022/KINSHAS$ hashcat -a 0 -m13400 crack.hash /usr/share/wordlists/rockyou.txt|
secrets (!).kdbx
```

```
[dirbuster] fern-wif1 mmap.lst -wuzz
Malhome@kal-: /images/WRITE-UP/GCSC2022/KINSHAS$ hashcat -a 0 -m13400 crack.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.5) starting

/sys/class/hwmon/hwmon2/temp1_input: No such file or directory

OpenCL API [OpenCL 2.0 pocl 1.8 Linux, None+Asserts, RELOC, LLVM 11.0, SLEEP, DISTRO, POCL_DEBUG] - Platform #1 [The pocl project]
-----
```

* Device #1: pthread-Intel(R) Core(TM) i7 CPU M 620 @ 2.67GHz, 2112/4288 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0

Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts

Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Rules: 1

Optimizers applied:

- * Zero-Byte
- * Single-Hash
- * Single-Salt

Autres questions posées

Comment recommander signe inférieur supérieur ?

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

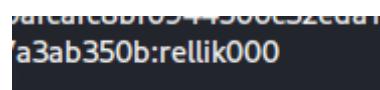
Dictionary cache built:

- * Filename.: /usr/share/wordlists/rockyou.txt
- * Passwords: 14344392
- * Bytes...: 139971507
- * Keypairs.: 143444385
- * Runtime...: 3 secs

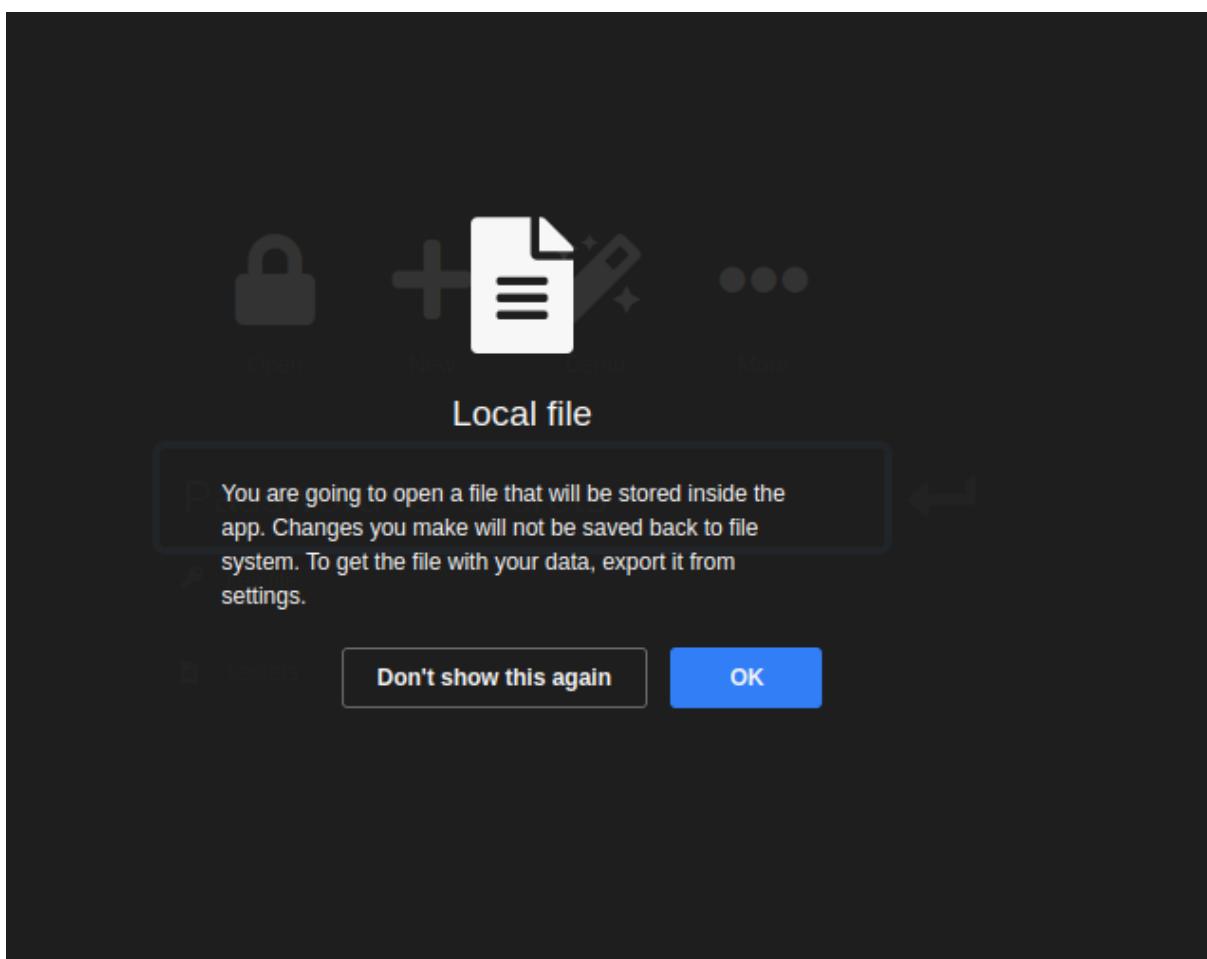
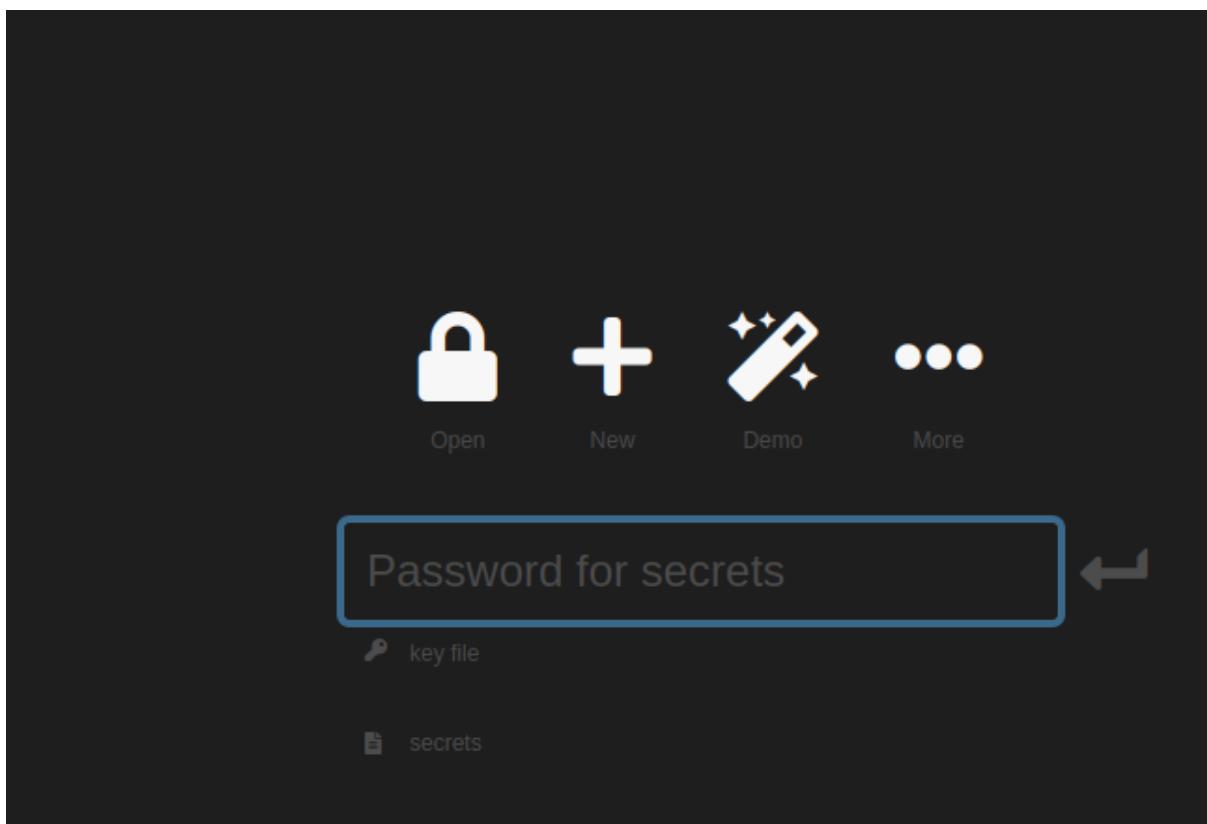
\$keypass*2**0baeaca143ceca048f76109f1af09db2e1e2c7cc02e59a57317854ba7fb*4b76a74e00b23ed3ff5c3a10afcacf8bf0944500c32eda170cd900afad2e5e*2d244191935a0738bba52abb75844796*417247c7668fb97
9932dab055a5fd15196e77a948929fc646e785149e721c*0774501ef959811ffadcf57b17c3241b863593430aae2647cb30e437a3ab350b:rellik000

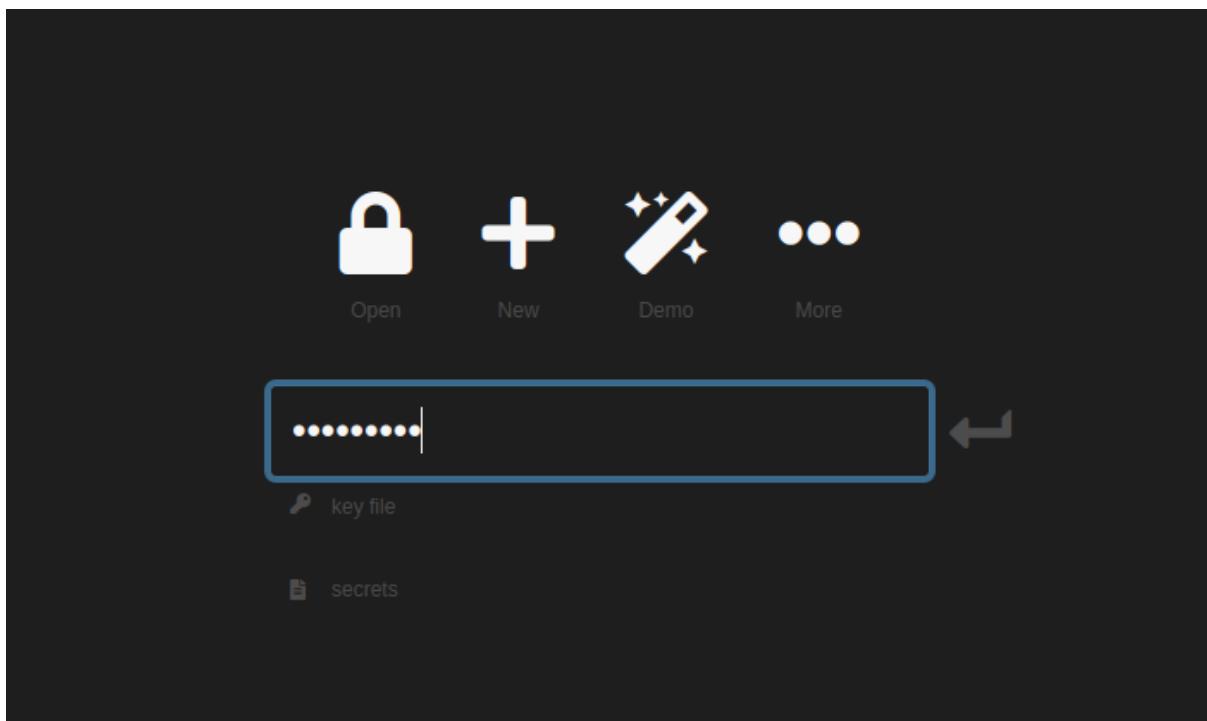
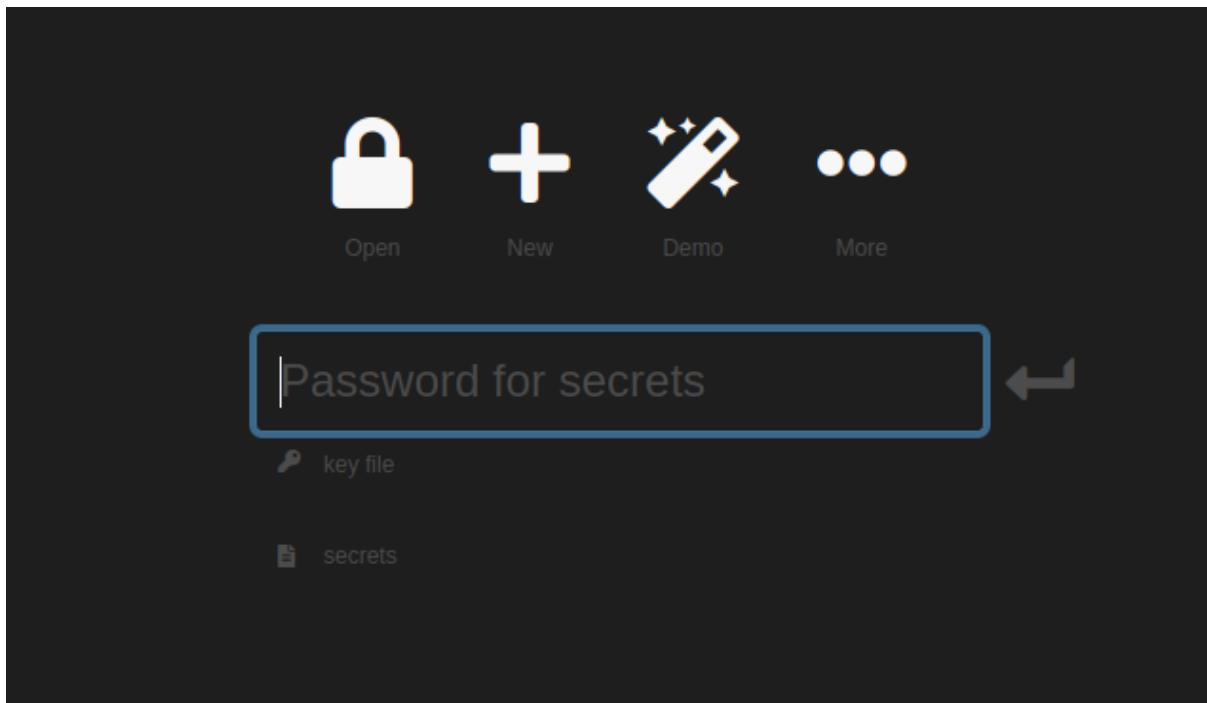
```
$ KeePassPS#*2^30*0`baeaca143ecac0a48c76109lfaf109db2e12c27cc02e59a57317854ba7fb74b76a74e0b23ed3ffe5c3a10acfcbf0944500c32eda170cd900afad2e5e7*2d244191935a0738bb52abb75844796*417247c7668fb97  
99322ad055a5d15196e77948929fc646e785149e721c0774501ef959811fadc57b12c32411b863593430a0aa2647cb30e437a3ab350b.relik000  
  
Session.....: hashcat  
Status.....: Cracked  
Hash.Mode....: 13400 (KeePass1 (AES/Twofish) and KeePass 2 (AES))  
Hash.Target....: KeePassPS#*2^30*0`baeaca143ecac0a48c76109lfaf109db2...ab350b  
Time.Started...: Mon Feb 21 15:56:41 2022 (5 secs)  
Time.Estimated...: Mon Feb 21 15:56:46 2022 (0 secs)  
Kernel.Feature...: Pure Kernel  
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)  
Guess.Queue....: 1/1 (100.00%)  
Speed.#1.....: 14.04 kH/s (8.98ms) @ Accel:512 Loops:30 Thr:1 Vec:4  
Recovered.....: 1/1 (100.00%) Digest:  
Progress.....: 813056/14344385 (5.67%)  
Rejected.....: 0/813056 (0.00%)  
Restore.Point...: 811008/14344385 (5.56%)  
Restore.Sub.#1...: Salt0 Amplifier:0 Iteration:0-30  
Candidate.Engine.: Device Generator  
Candidates.#1...: reynaline -> red616  
Hardware.Mon.#1..: Util: 95%  
  
Cracking performance lower than expected? See our troubleshooting page  
  
* Append -w 3 to the commandline.  
This can cause your screen to lag.  
  
* Append -S to the commandline.  
This has a drastic speed impact but can be better for specific attacks.  
Typical scenarios are a small wordlist but a large ruleset.  
  
* Update your backend API runtime / dr  
    > right way:  
https://hashcat.net/faq/wrongdriver  
  
* Create more work items to make us  
    our parallelization power:  
https://hashcat.net/faq/morework
```

Et voici le mot de passe.



J'utilise app.keeweb.info pour uploader le fichier secret.kdbx et j'y applique le mot de passe trouver dans la liste. Et j'obtiens le flag situé dans le fichier image dans l'angle droit bas.





The screenshot shows a password manager interface with a dark theme. On the left sidebar, there are buttons for 'All Items', 'Colors', 'Tags', and 'secrets'. Below these is a 'Trash' button. The main area has a search bar at the top. A blue-highlighted entry for 'facebook' is selected, showing the following details:

	facebook
User	test666
Password	*****
Website	
Notes	
Tags	
Expires	
more...	
File	secrets
Group	secrets
Created	Feb 4, 2022, 9:01:10 PM
Updated	Feb 4, 2022, 9:01:53 PM
History	2 records

At the bottom right, there is a file icon labeled 'secret.png'.

This screenshot shows the same password manager interface after the password has been decrypted. The 'facebook' entry now displays its full password value in the 'Password' field:

	facebook
User	test666
Password	45DiJ_RmAEYFeu+Fe8,A
Website	
Notes	
Tags	
Expires	
more...	
File	secrets
Group	secrets
Created	Feb 4, 2022, 9:01:10 PM
Updated	Feb 4, 2022, 9:01:53 PM
History	2 records

At the bottom right, there is a file icon labeled 'secret.png'.

The screenshot shows a password manager application with a dark theme. On the left, a sidebar lists categories: All Items, Colors, Tags, secrets, and Trash. The main area displays a list of entries:

- facebook**
test666
- gmail**
test666@gmail.com
- twitter**
test666

The 'facebook' entry is selected and expanded. The right panel shows the details for this entry:

facebook key icon

return to entry link icon

GCSC{4uCUn_7roUv3r4_C3t_MoT_D3_P45\$3}

Shift-click the attachment button to download it or ctrl+Delete to remove

trash bin icon link icon secret.png

Et voici le flag pour valider.

GCSC{4uCUn_7roUv3r4_C3t_MoT_D3_P45\$3}

GUINEA

capture_Guinea - B.A. - BA v1 X

En tant que Agent de terrain, tu dois connaître au bout des doigts les empreintes numériques de notre pays.

Les malveillants que tu seras amené à traquer pourraient les utiliser en remplacement de son nom officiel "Guinée".

1. Quel est le ccTLD de la Guinée ?
2. Quel est la codification de la loi relative à la Cybersécurité et la Protection des Données à Caractère Personnel en Guinée?
3. Quel est le fuseau horaire de la Guinée?

- Le format attendu est :

Réponse1: tout en minuscule

Réponse2: tout en majuscule

Réponse3: tout en majuscule et n'oublie pas le petit +

Flag: GCSC2022{Réponse1_Réponse2_Réponse3}

[Link 1]

Level already captured!

CAPTURED!

30
PTS

type
flag
category
Quizz

first_capture
Project Sekai

completed_by > PROJECT
SEKAI
WORTY
PERCE
JOB007
KITRONGHD
IDEK

J'utilise google et trouve le flag.



En tant que Agent de terrain, tu dois connaître au bout des doigts les empreintes numériques de notre pays.
Les malveillants que tu seras amené à traquer pourraient les utiliser en remplacement de son nom officiel "Guinée".
1. Quel est le ccTLD de la Guinée ?
2. Quel est la codification de la loi relative à la Cybersécurité et la Protection des Données à Caractère Personnel en Guinée?
3. Quel est le fuseau horaire de la Guinée?
- Le format attendu est :
Réponse1: tout en minuscule
Réponse2: tout en majuscule
Réponse3: tout en majuscule et n'oublie pas le petit +
Flag: GCSC2022{Reponse1_Reponse2_Reponse3}

REPONSE 1: .gn
REPONSE 2: L/2016/037/AN ||| L-2016-037-AN
REPONSE 3: GMT+0
.gn_L/2016/037/AN_GMT+0

le flag ::::::| GCSC2022{.gn_L-2016-037-AN_GMT+0}

KENYA

capture_Kenya - Tout le monde est la bienvenue à la #GCSC2022 X

Wow, quel acharnement contre notre pays!

Les membres de la CyberBadCorp se sont aussi inscrits à la compétition "Guinean Cyber Security Task Force" pour la saboter.

Très malheureusement pour eux, l'équipe "Guinean Cyber Task Force" a mis en place toutes les mesures pour les empêcher.

Nous avons identifié un compte et te transmettons quelques informations pour deviner son mot de passe.

- pseudonyme : CyberBadCorp
- email : cyberbadcorp@gmail.com
- token d'inscription : 20022022

Flag: GCSC2022{mot_de_passe})

Level already captured!

CAPTURED!

10
PTS

type
flag
category
OSINT

first_capture
Project Sekai

completed_by > PROJECT
SEKAI
POULLO
RMD723
KITRONGHO
WHITEHORSE224
SOUL2MANE

Je regarde mon mot de passe de connexion et je construit le flag puis je remplace le parenthèse de la fin par un accolade.

Wow, quel acharnement contre notre pays!

Les membres de la CyberBadCorp se sont aussi inscrits à la compétition "Guinean Cyber Security Task Force" pour la saboter.

Très malheureusement pour eux, l'équipe "Guinean Cyber Task Force" a mis en place toutes les mesures pour les empêcher.

Nous avons identifié un compte et te transmettons quelques informations pour deviner son mot de passe.

- pseudonyme : CyberBadCorp
- email : cyberbadcorp@gmail.com
- token d'inscription : 20022022

Flag: GCSC2022{GCSC2022_CyberBadCorp20022022cyberbadcorp@gmail.com20022022}

|-----La difference c'est la parenthèse)

Flag: GCSC2022{GCSC2022_CyberBadCorp20022022cyberbadcorp@gmail.com20022022}

MADAGASCAR

capture_Madagascar - Accès au serveur discord! X

N'oublie pas d'accéder au serveur Discord!
Flag : GCSC2022{lien_serveur_discord}

[Link 1]

Level already captured!

CAPTURED!

10 PTS	type flag category OSINT first_capture Project Sekai	completed_by > PROJECT SEKAI WORTY KIFILI KITRONGHD BLACKSNOW229
------------------	--	--

```
1 N'oublie pas d'accéder au serveur Discord!
2 Flag : GCSC2022{lien_serveur_discord}
3
4
5
6 https://discord.gg/3gvtd8N6
7
8 |
9
10
11 Flag: GCSC2022{https://discord.gg/3gvtd8N6}
12
13
```

```
10
11 Flag: GCSC2022{https://discord.gg/3gvt8N6}
12
13
```

MALI

capture_Mali - B.A. - BA v2 X

Lors des missions qui te seront confiées, tu seras amené à tenir un rapport journalier rigoureux et détaillé de tes avancements.

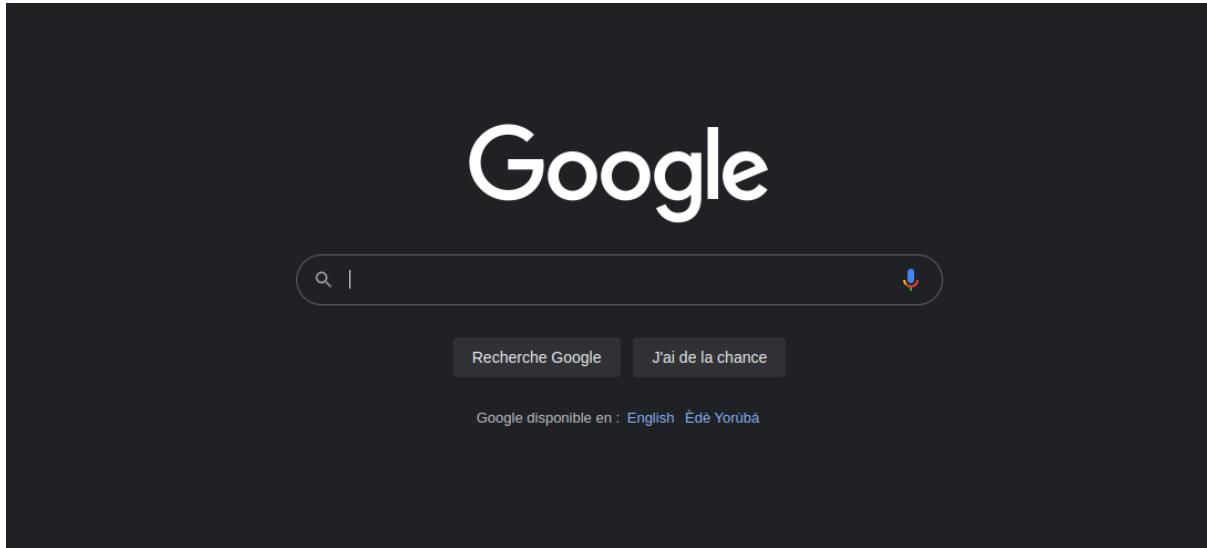
Afin de t'y préparer, nous voulons être sûrs que tu maîtrises le jargon

[Link 1]

Level already captured!

CAPTURED!

50 PTS	type flag	completed_by >
	category Quizz	IDEK BLACKSNOW229 PROJECT SEKAI WORTY KITRONGHO PERCE
	first_capture idek	



```
1 Lors des missions qui te seront confiées, tu seras amené à tenir un rapport journalier rigoureux et détaillé de tes avancements.
2 Afin de t'y préparer, nous voulons être sûrs que tu maîtrises le jargon des hommes en capuches et surtout, que tu as un sens élevé des
3 détails (recherches) !
4 Applique-toi.
5
6 1- Quels sont les trois éléments qui composent la triade CIA ?
7 -Réponse attendue : Cite-les dans cet ordre en Anglais, séparé par des tirets (-), première lettre de mot en majuscule et sans espace
8
9 2- On s'intéresse à la norme de télécommunication fonctionnant sur la fréquence 2.4 GHz dont le nom est inspiré du roi des Vikings.
10 Donne-le nom suivi de sa dernière version.
11 - Réponse attendue sous la forme: LoRaWAN v1.1
12
13 3- Parmi les technologies suivantes, laquelle est la plus appropriée pour sécuriser son accès Wifi : WEP, WPA, WPA2? La réponse est
14 sa norme IEEE.
15 - Réponse attendue sous la forme: IEEE 802.11X
16
17 4- Que signifie chacun des sigles suivants: AV, FW, IDS, IPS, SIMS, SOC et VPN?
18 - Réponse attendue : définition séparée par des tirets (-), un espace avant et après le tiret (-), majuscule en début de mot, mot au
19 signulier.
20 5- J'utilise un laptop MacBook pour mes activités quotidiennes. J'utilise Linux pour naviguer sur des sites douteux. J'utilise le réseau
21 social LinkedIn. Dans ce cas, je ne peux pas du tout subir de piratage. Vrai ou Faux?
22
23 Confidentiality-Integrity-Availability
24 Bluetooth v5.2
25 IEEE 802.11i
26 Antivirus - Firewall - Intrusion Detection System - Intrusion Prevention System - Security Information Management System - Security
27 Operation Center - Virtual Private Network
28 _Faux
29
30
31 flag : GCSC2022{md5(Confidentiality-Integrity-Availability_Bluetooth v5.2_IEEE 802.11i_Antivirus - Firewall - Intrusion Detection System -
Intrusion Prevention System - Security Information Management System - Security Operation Center - Virtual Private Network_Faux)}
```

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

Confidentiality-Integrity-Availability_Bluetooth v5.2_IEEE 802.11i_Antivirus - Firewall - Intrusion Detection System - Intrusion Prevention System - Security Information Management System - Security Operation Center - Virtual Private Network_Faux

Generate →

Your String	Confidentiality-Integrity-Availability_Bluetooth v5.2_IEEE 802.11i_Antivirus - Firewall - Intrusion Detection System - Intrusion Prevention System - Security Information Management System - Security Operation Center - Virtual Private Network_Faux
MD5 Hash	bcd079cae36b60dc8071a18ea491290 <button>Copy</button>
SHA1 Hash	b255611d27f0e46ab7172d6e5a140cb64d50b726 <button>Copy</button>

```
0: flag : GCSC2022{md5(Confidentiality-Integrity-Availability_Bluetooth v5.2_IEEE 802.11i_Antivirus - Firewall - Intrusion Detection System - Intrusion Prevention System - Security Information Management System - Security Operation Center - Virtual Private Network_Faux)}
1:
2:
3: |
4:
5: flag : GCSC2022{bcd079cae36b60dc8071a18ea491290}
```

NIGERIA

capture_Nigeria - Mots de passe d'une application étrange X

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

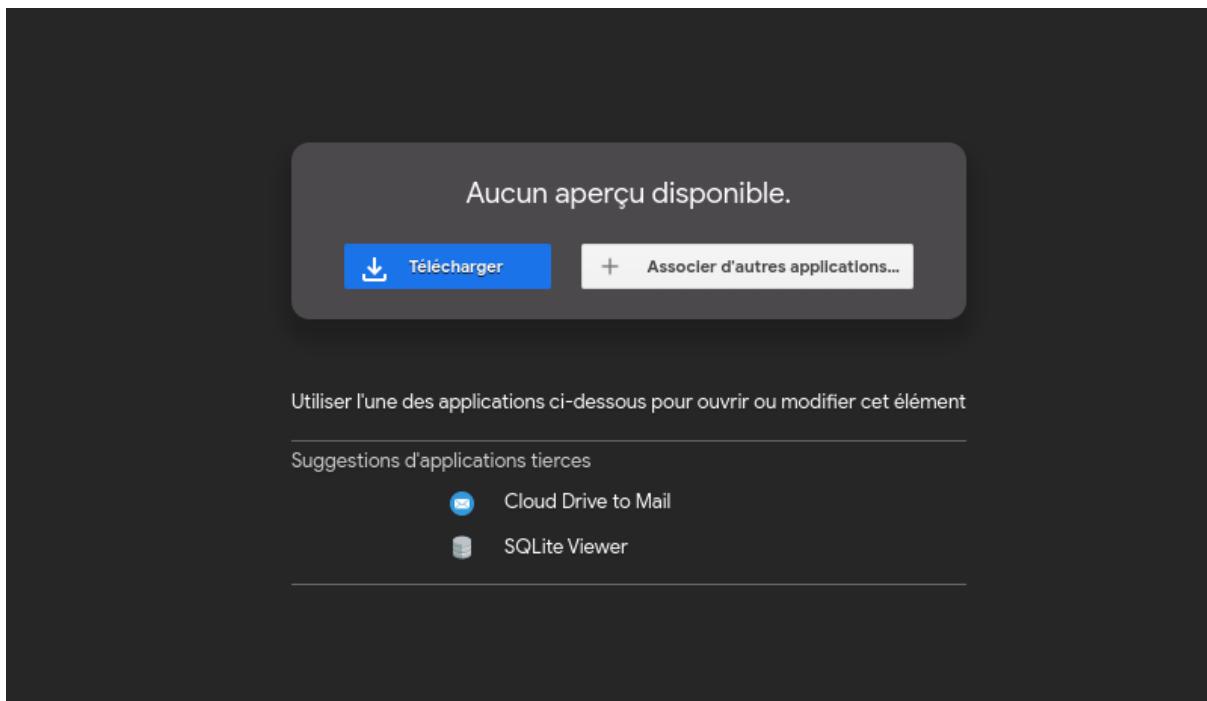
Flag: GCSC2022>Password1_Password2_Password3)

[Link 1]

Level already captured!

CAPTURED!

30 PTS	type flag category Miscellaneous first_capture idek	completed_by > IDEK OFSH1LL RMD723 PROJECT SEKAI BLACKSNOW229 LEOX
------------------	---	---



Screenshot of the SQLite Viewer with Google Drive interface. The title bar shows "SQLite Viewer with Google Drive" and "Memo". Below the title, it says "FileName: BD application mobile.db" and has a "Save to Computer" button. The main area has a search bar with placeholder "Search For Owner Full Name, Full Address, Relatives & More!" and a "Powered By BeenVerified" logo. A "TYPE PHONE NUMBER" input field with a placeholder "Example: (123) 456-7890" and a "Search" button are also present. A dashed box allows users to "Drop a file here" or open a file dialog. Below this, a table named "users" is displayed with 3 rows. The table has columns "username" and "password". The data is as follows:

username	password
John	ODI3MDQ0MGwZTk0MTEzDExZmFmMzg1MTI1Nzc4ZTc=
Marie	NDFkNTM4YTcxYjJhYTYwMDRkNTM0MjM3NzEwNDFjOWMK
Luc	NGVmY2RhYzg1YzZjNDk0YjNjZWY4NzgxY2M2Mzk4MDUK

Below the table, there is a SQL query input field containing "SELECT * FROM 'users' LIMIT 0,30" and an "Execute (Ctrl+Enter)" button.

Decode from Base64 format

Simply enter your data then push the decode button.

```
ODI3MDQ0MGMwZTk0MTEzDExZmFmMzg1MTI1Nzc4ZTc=
```

 For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
8270440c0e94111d11faf385125778e7
```

NDFkNTM4YTcxYjJhYTYwMDRkNTM0MjM3NzEwNDFjOWMK

For encoded binaries (like images, documents, etc.) use the file upload form a little further down.

Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

41d538a71b2aa6004d53423771041c9c

Decode from Base64 format

Simply enter your data then push the decode button.

NGVmY2RhYzg1YzZjNDk0YjNjZWY4NzgxY2M2Mzk4MDUK

For encoded binaries (like images, documents, etc.) use the file upload form a little further down.

Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

4efcdac85c6c494b3cef8781cc639805

8270440c0e94111d11faf385125778e7 : p1ntap

Trouvé en 0.41s

41d538a71b2aa6004d53423771041c9c : fd1972

Trouvé en 0.269s

4efcdac85c6c494b3cef8781cc639805 : AdDiCtIoN

Trouvé en 0.453s

ODI3MDQ0MGMwZTk0MTEzDExZmFmMzg1MTI1Nzc4ZTc=	8270440c0e94111d11faf385125778e7	p1ntap
NDFkNTM4YTcxYjJhYTYwMDRkNTM0MjM3NzEwNDFjOWMK	41d538a71b2aa6004d53423771041c9c	fd1972
NGVmY2RhYzg1YzZjNDk0YjNjZWY4NzgxY2M2Mzk4MDUK	4efcdac85c6c494b3cef8781cc639805	AdDiCtIoN

|le flag ::::::: GCSC2022{p1ntap_fd1972_AdDiCtIoN}

UNITED STATE

capture_United States - Ils vivent avec le RSA en France? 

On te donne le crytosystème utilisé : message, clé privée et clé publique.

Indice: -5 points
Flag: GCSC2022{flag_ici}

[Link 1]

Level already captured!

CAPTURED!

20
PTS

type
flag
category
Cryptanalysis
first_capture
idek

completed_by > IDEK
PWNPROPHECY
POULLO
SCOR7
INSIDERBLAST
WORTY
BLACKSNOW229

Fichiers



-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQC3Coz02BrFQ42/fNEfHyls569Z0olFZVy+Y6ppnV5/LqUol/OU
TSYBLSPI1Gi2HTikYu/Z9Rng59gkftbaxVXk/bz5NHiEAKaXdGWrW9QIdGGJ1doQ
8IQiMcZebQ3xmhJ05Uo5SFs1Fwa7mpR55e+EinNcgT+1BqibAcLljX18IQIDAQAB
AoGATZrRjHWbVAuCK6+10iYaICxSshilTrurdCX0kKscn63BRYdaa1U0oW1NSGrHD
+4KEI143Jwe+AxcJEuAcJAEKmyYqdjfZn8Xbg/PN+PqZhVSc/pulJhfxvN5z3EsG
tAJh8qXFhPu0cfgioFk/ygOXqCer2wrJGrEfuiyx6TUPOqkCQQDhoGZLdqph+41e
eMg0aRcqjm6SvvLbhhdEIhFU/57+6tdsUbEwzh5dwVdInVn9sXI8c0i+Bi7vUk5i
wNKZpzsvAkEAz66QWJTX1Eg4NquFabGEUANRSGo+VjlQOpDfaTc4VpcH7N9MeOKq
WqnCVWQyufVAm16LzaccfIzd5GIdnQaprwJBAJl3gbz4pSHqeZj1rK/Bf4lpwh08
mXHp/i9QwNtA18PqtsattklNGeiJlrYEmW5u4RXtctG14PzVzg1rvJPY508CQDe1
r+rTIeEYXlvr7sHHaKK+ARPXzBj9DtRnAEcNFQPFR872p2DSDLR9TS/yzNitPUMr
kXz9EtsmPm+BEiyj00kCQHgQWr+oUXQ/mhZ9mG2jZeJxhfmPSOf58SxG4KwFYvmX
MPT06kbikZ4/CLPiNqgliR1zu0i3quKaS48w4dWVz+4=

-----END RSA PRIVATE KEY-----

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC3Coz02BrFQ42/fNEfHyls569Z
0olFZVy+Y6ppnV5/LqUol/OUTSYBLSPI1Gi2HTikYu/Z9Rng59gkftbaxVXk/bz5
NHiEAKaXdGWrW9QIdGGJ1doQ8IQiMcZebQ3xmhJ05Uo5SFs1Fwa7mpR55e+EinNc
gT+1BqibAcLljX18IQIDAQAB

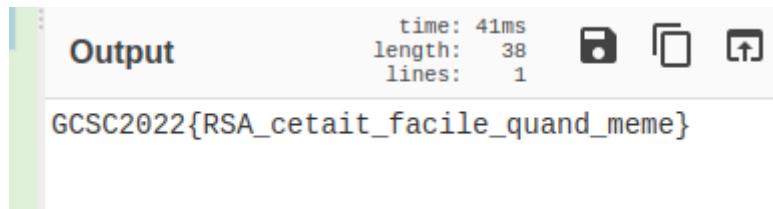
-----END PUBLIC KEY-----



J'utilise cyberchef online pour décoder le texte.

The CyberChef interface shows the following configuration:

- Input:** A long Base64 encoded string:
UxL8XXqLetXJ0h7RTifRCiKBv7zJw7siJ7ZEkw90+XcXqb9cezj9Ps3LFyZSjqUVlIwS01+i2oqgkYTaSVH6NnP0of1B/4u1EoZfxQ8S9oSx32/2R39ZKjN5App1MY63AvV4U9+yV7wC1su0p9A2LMRpRc21v090+FNTLhkfb7c=
- RSA Decrypt:** RSA Private Key (PEM) is pasted into the input field:
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKbQ0C3Coz02BrF042/fNEfHy1s569Z0o1FZVv+Y6ppnV5/LqUo1/OU
TSYBLSPt1G1zHTikYu/z9Rng59gkftbaxVXk/bz5NHxEKAxdGMrW9QIdGGJ1dQ
8IQ1McZebQ3xmhJ05Uo5SFs1Fwa7mpR55e+EinNcgT+18qibAc1ljX18IQIDAQAB
AoGATZrRjHwbVAUck6+101YaICxSsh1LTrrdCX0Kscn63BRYdaa1UooW1NSGrHD
+4KEI143Jwe+AxcJEuAcJAEKmyYqdjfZn8Xbq/PN+PqZhVSc/pulJhfxvN5z3Esg
- Key Password:** The input field is empty.
- Encryption Scheme:** RSAES-PKCS1-V1_5
- Output:** The decrypted text is displayed:
GCSC2022{RSA_cetait_facile_quand_meme}



ZAMBIA

capture_Zambia - Cybertalent! Il faut mettre le paquet... 2/2 X

Tu décides de continuer l'analyse des captures réseaux des cybercafés de la capitale que tu as commencé dans le Challenge Somalie.

Cette fois-ci, tu remarques qu'un membre de la CyberBadCorp présent dans ce cybercafé ce jour-là, s'est rendu sur le darkweb où il a passé la commande de nombreuses armes de guerre.

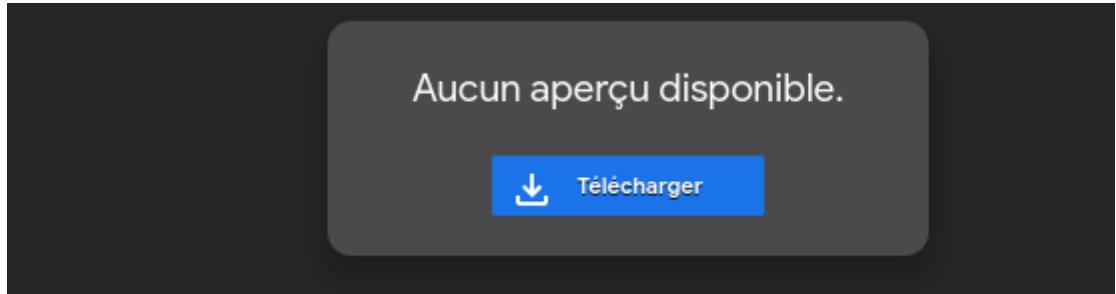
Retrouve son nom d'utilisateur, son mot de passe et surtout le message de la commande.

[Link 1]

Level already captured!

CAPTURED!

20 PTS	type flag category Network Security first_capture Worty	completed_by > WORTY IDEK PERCE PROJECT SEKAI PWNPROPHECY GCSTF-TEAM
------------------	--	--



Après avoir téléchargé le fichier, j'ai ouvert avec Ettercap.
Et puis filtrer les paquets http et tcp.

connexion-non-securisee.pcap						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	74	54214 → 34001 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSeq=252143462 TSecr=0 WS=
2	0.000012	127.0.0.1	127.0.0.1	TCP	74	34001 → 54214 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSeq=252143462 TSecr=0
3	0.000020	127.0.0.1	127.0.0.1	TCP	66	54214 → 34001 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSeq=252143462 TSecr=252143462
4	0.000069	127.0.0.1	127.0.0.1	HTTP	459	GET /action_page.php HTTP/1.1
5	0.000079	127.0.0.1	127.0.0.1	TCP	66	34001 → 54214 [ACK] Seq=1 Ack=394 Win=65536 Len=0 TSeq=252143462 TSecr=252143462
6	0.001836	127.0.0.1	127.0.0.1	HTTP	1286	HTTP/1.1 200 OK (text/html)
7	0.001845	127.0.0.1	127.0.0.1	TCP	66	54214 → 34001 [ACK] Seq=394 Ack=1221 Win=64512 Len=0 TSeq=252143463 TSecr=252143463
8	0.079055	127.0.0.1	127.0.0.1	HTTP	428	GET /css/bootstrap.min.css HTTP/1.1
9	0.079073	127.0.0.1	127.0.0.1	TCP	66	34001 → 54214 [ACK] Seq=1221 Ack=756 Win=65536 Len=0 TSeq=252143541 TSecr=252143541
10	0.079260	127.0.0.1	127.0.0.1	HTTP	556	HTTP/1.1 404 Not Found (text/html)
11	0.079268	127.0.0.1	127.0.0.1	TCP	66	54214 → 34001 [ACK] Seq=756 Ack=1711 Win=65536 Len=0 TSeq=252143541 TSecr=252143541
12	0.081624	127.0.0.1	127.0.0.1	TCP	66	34001 → 54214 [ACK] Seq=1711 Ack=786 Win=65536 Len=0 TSeq=252143541 TSecr=252143541
13	0.081629	127.0.0.1	127.0.0.1	TCP	66	54214 → 34001 [FIN, ACK] Seq=1786 Ack=1712 Win=65536 Len=0 TSeq=252148543 TSecr=252148543
14	5.081632	127.0.0.1	127.0.0.1	TCP	66	34001 → 54214 [ACK] Seq=1712 Ack=1757 Win=65536 Len=0 TSeq=252148543 TSecr=252148543
15	59.669718	127.0.0.1	127.0.0.1	TCP	74	54210 → 34001 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSeq=252203131 TSecr=0 WS=
16	59.669720	127.0.0.1	127.0.0.1	TCP	74	34001 → 54210 [SYN, ACK] Seq=0 Ack=1 Win=65492 Len=0 MSS=65495 SACK_PERM=1 TSeq=252203131 TSecr=0

> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 54214, Dst Port: 34001, Seq: 0, Len: 0

Fichier Editer Vue Aller Capture Analyser Statistiques Téléphonie Wireless Outils Aide

http

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000069	127.0.0.1	127.0.0.1	HTTP	459	GET /action_page.php HTTP/1.1
6	0.001836	127.0.0.1	127.0.0.1	HTTP	1286	HTTP/1.1 200 OK (text/html)
8	0.079055	127.0.0.1	127.0.0.1	HTTP	428	GET /css/bootstrap.min.css HTTP/1.1
10	0.079260	127.0.0.1	127.0.0.1	HTTP	556	HTTP/1.1 404 Not Found (text/html)
18	59.669816	127.0.0.1	127.0.0.1	HTTP	678	POST /action_page.php HTTP/1.1 (application/x-www-form-urlencoded)
20	59.671389	127.0.0.1	127.0.0.1	HTTP	1294	HTTP/1.1 200 OK (text/html)
22	59.725783	127.0.0.1	127.0.0.1	HTTP	428	GET /css/bootstrap.min.css HTTP/1.1
24	59.726648	127.0.0.1	127.0.0.1	HTTP	556	HTTP/1.1 404 Not Found (text/html)

```

> Frame 4: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits)
> Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 54214, Dst Port: 34001, Seq: 1, Ack: 1, Len: 393
> Hypertext Transfer Protocol

```

Fichier Editer Vue Aller Capture Analyser Statistiques Téléphonie Wireless Outils Aide

http

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000069	127.0.0.1	127.0.0.1	HTTP	459	GET /action_page.php HTTP/1.1
6	0.001836	127.0.0.1	127.0.0.1	HTTP	1286	HTTP/1.1 200 OK (text/html)
8	0.079055	127.0.0.1	127.0.0.1	HTTP	428	GET /css/bootstrap.min.css HTTP/1.1
10	0.079260	127.0.0.1	127.0.0.1	HTTP	556	HTTP/1.1 404 Not Found (text/html)
18	59.669816	127.0.0.1	127.0.0.1	HTTP	678	POST /action_page.php HTTP/1.1 (application/x-www-form-urlencoded)
20	59.671389	127.0.0.1	127.0.0.1	HTTP	1294	HTTP/1.1 200 OK (text/html)
22	59.725783	127.0.0.1	127.0.0.1	HTTP	428	GET /css/bootstrap.min.css HTTP/1.1
24	59.726048	127.0.0.1	127.0.0.1	HTTP	556	HTTP/1.1 404 Not Found (text/html)

```

> Frame 18: 678 bytes on wire (5424 bits), 678 bytes captured (5424 bits)
> Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 54216, Dst Port: 34001, Seq: 1, Ack: 1, Len: 612
> Hypertext Transfer Protocol
  > HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "username" = "GCSC"
    > Form item: "password" = "{Ut1l1$3z_70uJoUR$_H77P$!}"
    > Form item: "login" = ""

```

Puis dans une protocole Http, j'ai où la méthode POST est utilisée j'ai trouvé le flag.

```

HyperText Transfer Protocol
  - HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "username" = "GCSC"
    > Form item: "password" = "{Ut1l1$3z_70uJoUR$_H77P$!}"
    > Form item: "login" = ""

```

SOMALI

capture_Somalia - Cybertalent! Il faut mettre le paquet... 1/2 

Les membres de la CyberBadCorp en sont conscients. Alors, ils font souvent recours aux cybercafés.

Or, l'ANSSI-Guinée a récemment exigé aux cybercafés opérant sur toute l'étendue du territoire Guinéen de mettre en place des mesures garantissant l'authentification, la traçabilité, l'imputabilité/la non-répudiation de l'usage des appareils de leurs parcs informatiques.

Plus concrètement, il s'agit d'identifier les utilisateurs, de journaliser les actions et superviser l'ensemble des flux entrants et sortants de chaque poste.

En charge de l'analyse des captures réseaux bimensuels de certains cybercafés de la capitale, tu décides de commencer ta journée par celle-ci.

Y a t'il quelque chose dans ces paquets qui mettraient en péril la sécurité nationale?

[Link 1]

Level already captured!

CAPTURED!

10
PTS

type
flag

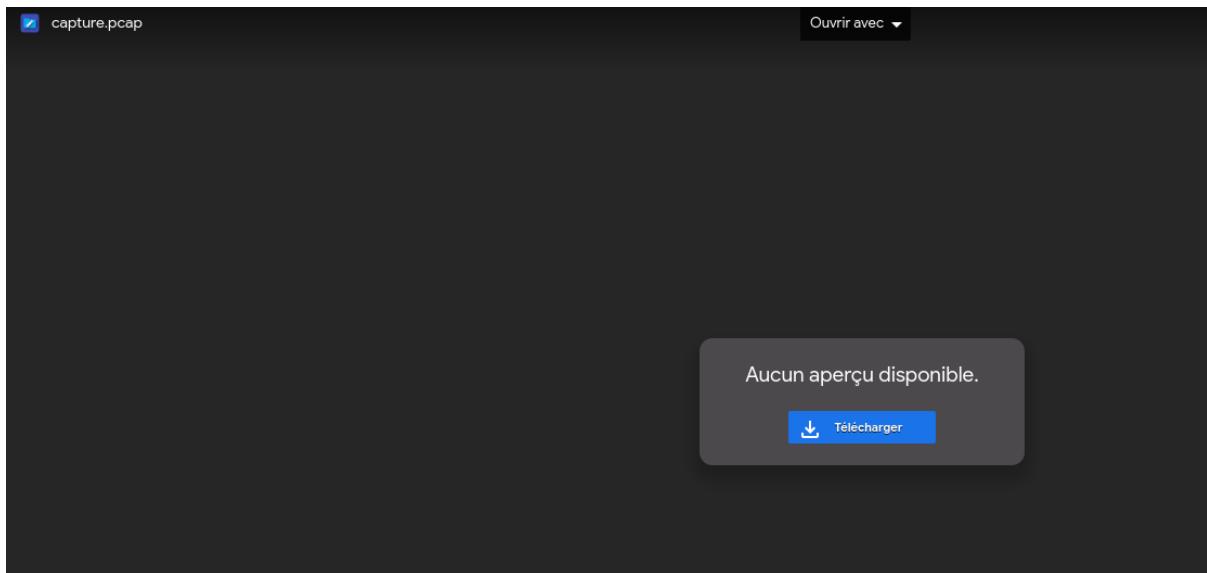
category
Network Security

first_capture
Worty

completed_by > WORTY
PERCE
IDEK
PROJECT
SEKAI
BABYSAYMYNAME

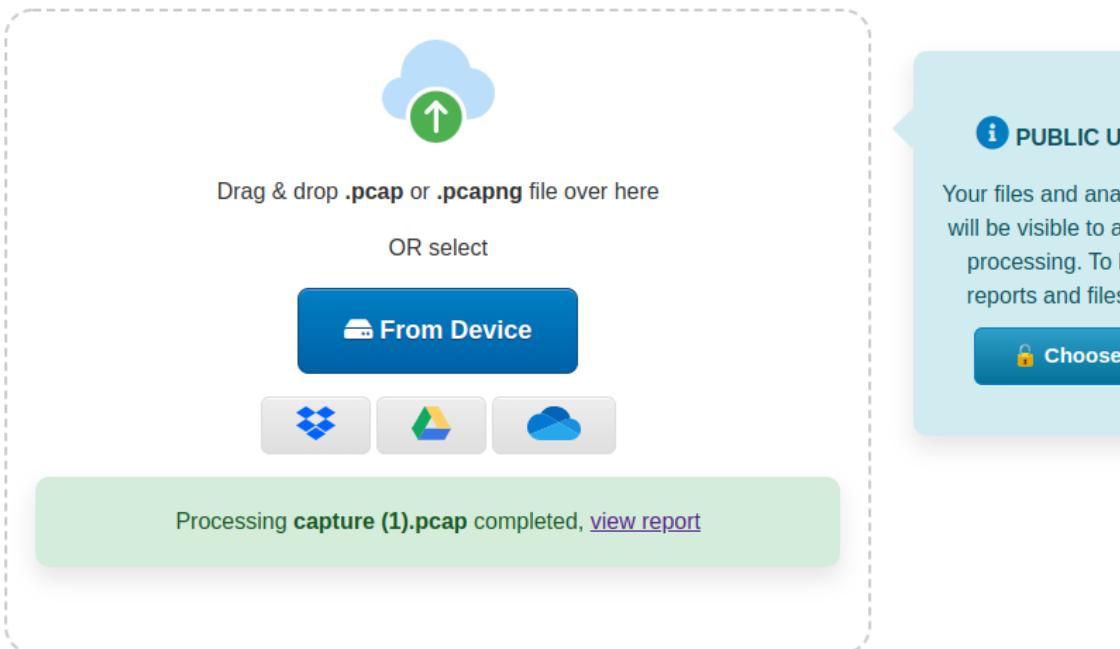
Je clique sur Link 1.

Puis je télécharge le fichier capture pcap.



Après je l'ouvre avec l'utilitaire online A-Packets

A screenshot of the A-Packets website. The header includes the logo 'A-Packets' and navigation links for 'Features', 'FAQ', 'Upload', 'Price', 'View Pcaps', 'My Pcaps', and 'Sign In'. The main section features the heading 'A-Packets' and 'Online pcap file analyzer'. It describes the tool's capabilities: reading and viewing pcap files, analyzing IPv4/IPv6, HTTP, Telnet, FTP, DNS, SSDP, WPA protocols, building network maps, sniffing, and extracting data. Below this is a 'View analyzed pcaps' button and an 'Upload pcap file' button. To the right is a screenshot of the analysis interface showing network traffic maps and data tables. At the bottom, there is a 'FEATURES' section and a note about bringing intellectual network traffic analysis into the cloud.



Upload pcap file on Windows

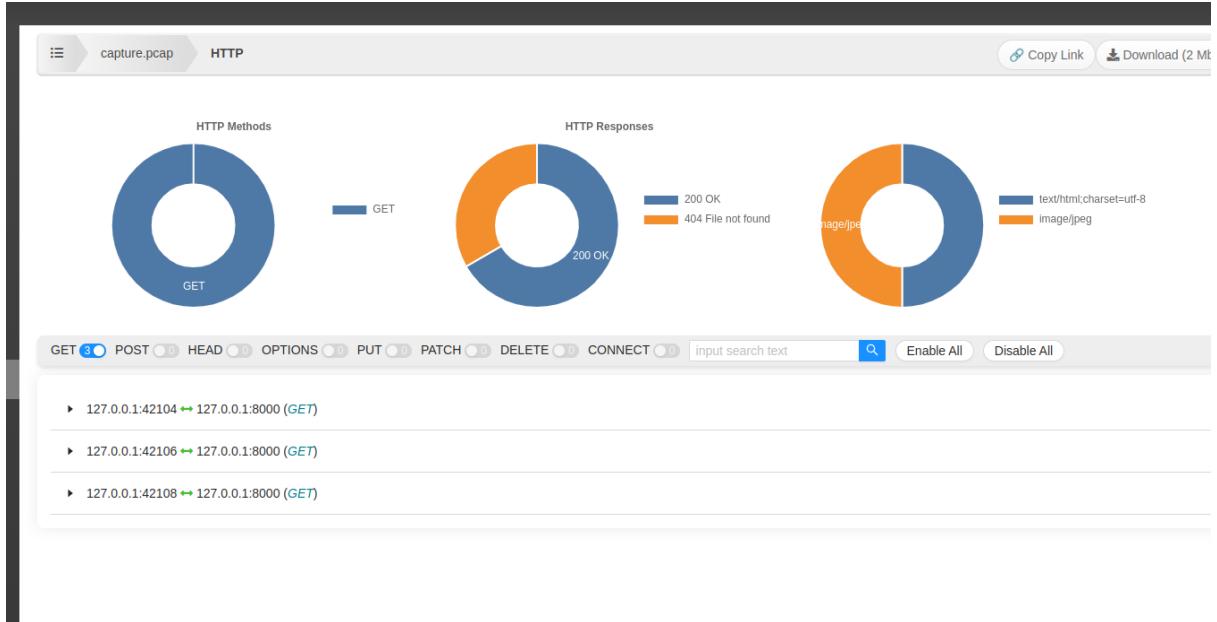
J'upload le fichier et A-Packet se charge de faire l'analyse puis je clique sur view report.

Pour voir le rapport.

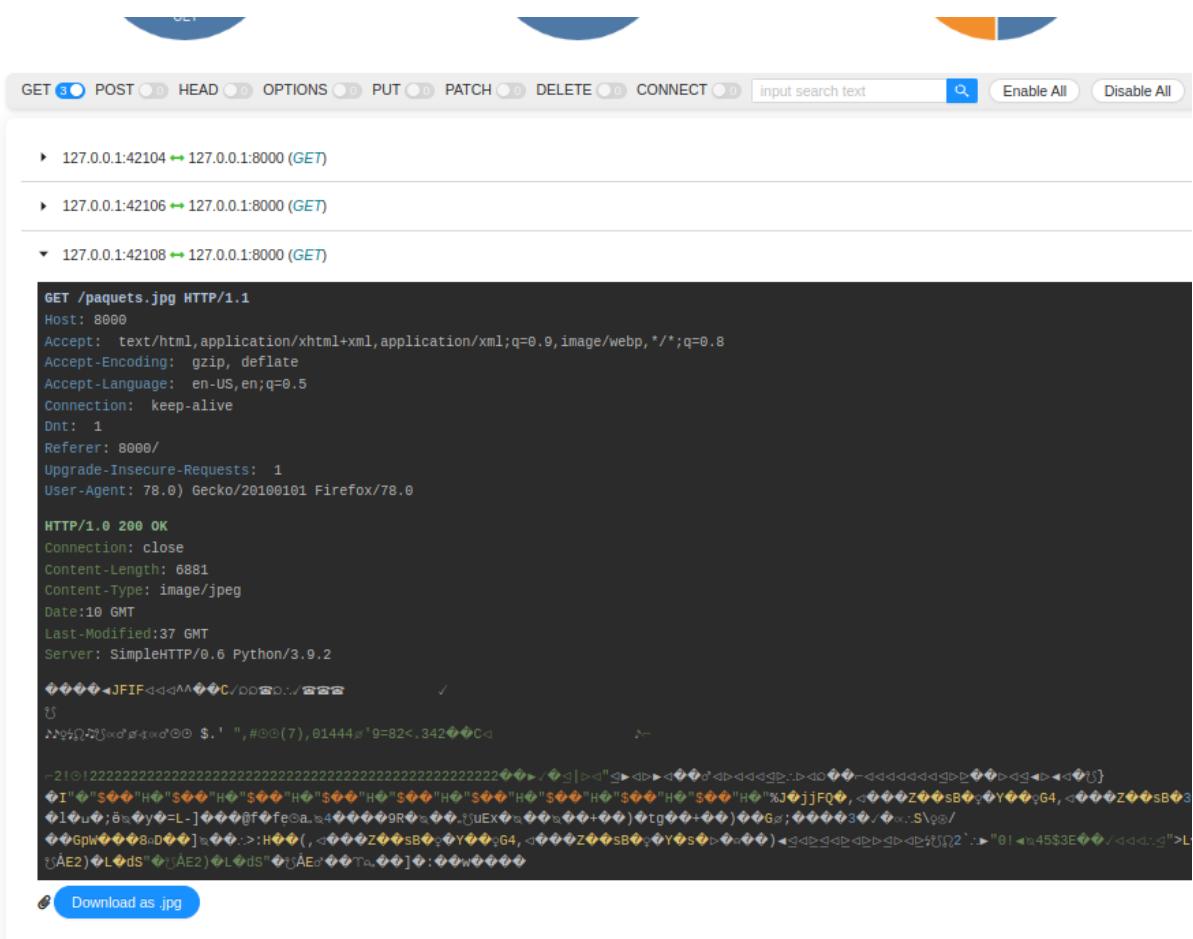
Section	Description
Found credentials	View found plain text passwords or hashes for various authentication protocols.
DNS Queries	Explore DNS/NBNS/mDNS queries to DNS servers on world map.
HTTP Communication	Display HTTP requests, responses and transferring data.
SMB Sniffer	Explore SMB announces and information about installed OS features. Found NTLMv1/v2 hashes.
ARP	Contains link layer information about network communications. Help detect network routers and ARP spoofing attackers.
Network Map	Analyze IP communications between devices and used protocols. Found fingerprints like OS/installed software.
Open Ports	Open TCP ports fingerprints found in the captured traffic.
Images	Images found in HTTP data.
Telnet	Show Telnet sessions data.
FTP	Show FTP sessions data.
SSDP announces	Contains announces of services running on network devices using protocol SSDP.
Connections	Visualize IP connections, display endpoints and transferring data volume on world map.
DNS, DHCP and LDAP Servers	Detect DNS, DHCP and LDAP servers from intercept.
Ethernet Devices	Find fingerprints of ethernet devices and detect used ethernet broadcast addresses.
WiFi	View information about access points, clients, connection requests and found WPA2 handshakes.

Je vois tous les services et protocoles utilisés et qui sont stockés dans le fichier pcap sur mon board.

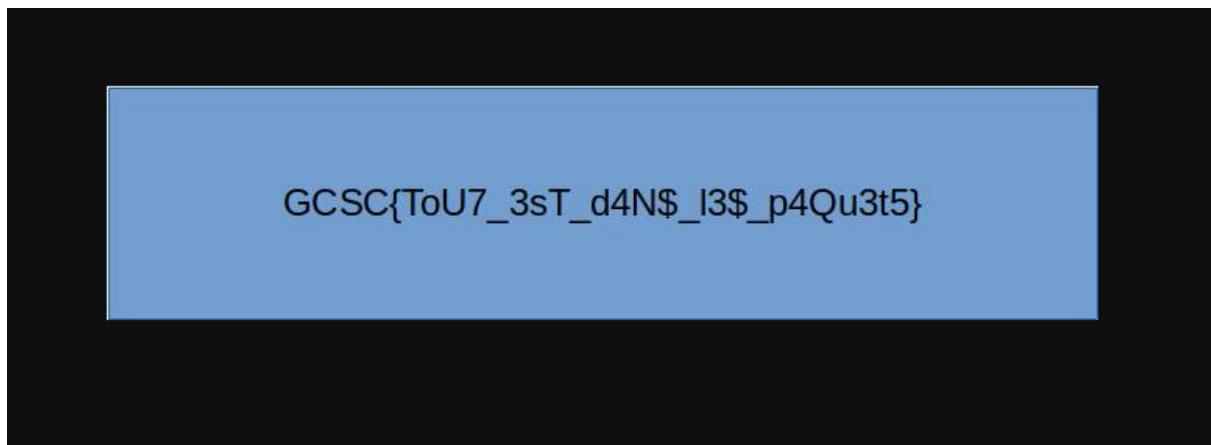
Comme c'est le trafic qui me concerne. Je regarde dans HTTP Communication pour voir les échanges.



Ici le trouves les échanges entre différentes adresses IP.



Je visualise le tout. Et je vois que dans la dernière communication entre les ip, il y un fichier image qui est joint. Je l'ouvre pour voir.



Et c'est le flag.

CANADA

capture_Canada - IP_publique x Collaborer x Interagir

X

Houhou!

On te présente ce formulaire du site web en cours de construction.

Interagit avec le serveur de la CyberBadCorp et trouve-lui un usage non sollicité.

Indice: -5 points

Flag: GCSC2022{flag_ici}

[Link 1]

[Link 2]

Level already captured!

CAPTURED!

150
PTS

type
flag
category
Web Security

first_capture
PwnProphecy

completed_by > PWNPROPHECY
WORTY
LEOX
IDEK
MAO_BERRY
TERMINATOR
PERCE

Je clique sur Link 1.

Link 2 c'est de la Fouine. Pour vous dire, ne stressez pas.

Please, register a new user to continue

Kante
password
kante@gmail.com
test.com
<input type="button" value="Envoyer"/>

J'ai une page où je remplir le formulaire.
Essayons juste de remplir ce formulaire. Et j'ai eu la réponse.

← → C 🔍 Non sécurisé | challenges.guinean-cybertaskforce.com:5000/register?user=Kante&passwd=password&email=

Applications Acheter sur A... eBay - Discoun... Téléchargeme... Demande d'ad... Commerce

```
File "/usr/local/lib/python3.8/dist-packages/urllib3/connectionpool.py", line 785, in urlopen
    retries = retries.increment()

File "/usr/local/lib/python3.8/dist-packages/urllib3/util/retry.py", line 592, in increment
    raise MaxRetryError(_pool, url, error or ResponseError(cause))

During handling of the above exception, another exception occurred:

File "/usr/local/lib/python3.8/dist-packages/flask/app.py", line 2091, in __call__
    return self.wsgi_app(environ, start_response)

File "/usr/local/lib/python3.8/dist-packages/flask/app.py", line 2076, in wsgi_app
    response = self.handle_exception(e)

File "/usr/local/lib/python3.8/dist-packages/flask/app.py", line 2073, in wsgi_app
    response = self.full_dispatch_request()

File "/usr/local/lib/python3.8/dist-packages/flask/app.py", line 1518, in full_dispatch_request
    rv = self.handle_user_exception(e)

File "/usr/local/lib/python3.8/dist-packages/flask/app.py", line 1516, in full_dispatch_request
    rv = self.dispatch_request()

File "/usr/local/lib/python3.8/dist-packages/flask/app.py", line 1502, 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{Ut1llisseZ_t0uj0Ur$c0ll4boRat0R}')

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)

File "/usr/local/lib/python3.8/dist-packages/requests/sessions.py", line 529, in request
    resp = self.send(prep, **send_kwargs)

File "/usr/local/lib/python3.8/dist-packages/requests/sessions.py", line 667, in send
    history = [resp for resp in gen]

File "/usr/local/lib/python3.8/dist-packages/requests/sessions.py", line 667, in <listcomp>
    history = [resp for resp in gen]
```

voici le flag parmis toute la sortie.

```
File "/app/app.py", line 32, in register
    r = requests.get('http://'+url+'/GCSC{Ut1llisseZ_t0uj0Ur$c0ll4boRat0R}')
```

Trouvez. J'ai trop bien aimé cette compétition.
Merci à GCSC2022.