WRITE UP « DigiCarross » - Partie 2

NORZHCTF 2K19

ENSIBS CYBERDEFENSE

par @y0r3l

Date	Acteur	Mail de contact	Version
10/12/2018	@y0r3l	y0r3l@protonmail.com	1.0
07/08/2019	@y0r3l	y0r3l@protonmail.com	2.0

INTRODUCTION

Ce challenge a été réalisé dans le cadre du NORZHCTF se tenant à Lille le 22 janvier 2019. Ce dernier est un événement de type Capture The Flag (CTF) et est orgnaisé par les étudiants de la formation Cyberdéfense de L'ENSIBS (Ecole Nationale Supérieur d'Ingénieurs de Bretagne Sud).

C'est dans le but d'alimenter cet événement en épreuves que j'ai créé le challenge « DigiCarross ».

Ce challenge étant découpé en deux parties, ce document a pour but de vous présenter la démarche afin de résoudre l'étape finale du challenge.

Toute ressemblance avec des faits réels ne serait que pure et fortuite coïncidence.

Certaines ressources de ce challenge sont hébergées sur des plateformes tierces. La disponibilité dans le temps des données hébergées chez ces tiers n'est donc pas assurées. Ainsi, les informations présentes au sein de ce document peuvent s'avérées différentes de la réalité.

Catégorie

OSINT (Open Source INTelligence)

Niveau de difficulté

Moyen

Énonce

Le but de ce challenge est d'obtenir un mot de passe utilisé par votre cible.

Pour rappel, le challengeur n'a pas besoin d'utiliser une vulnérabilité d'un langage de programmation pour résoudre ce challenge.

En effet, il devra analyser les activités de la victime sur Internet.

Matériel nécessaire pour le résoudre

Accès à Internet
Un compte Facebook

Matériel nécessaire pour le rejouer

Navigateur internet

Indices

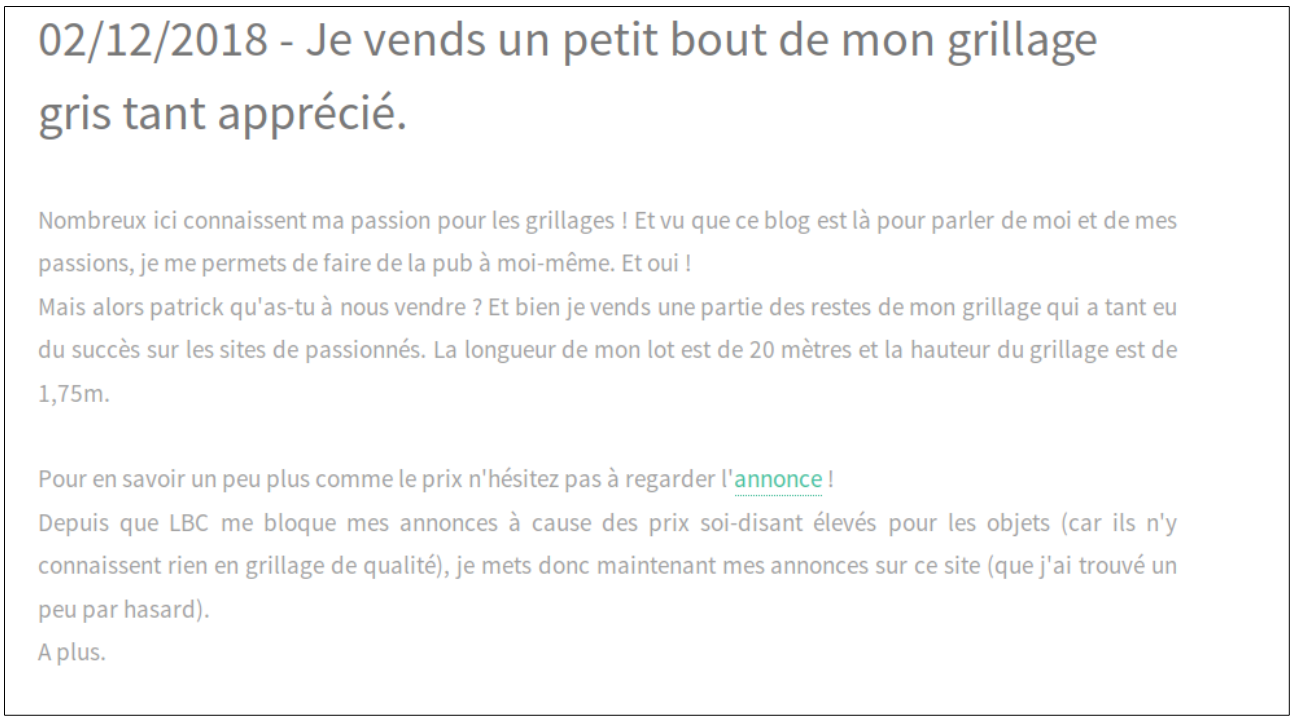
Les indices peuvent être donnés tout au long du challenge à intervalle espacé.

1. « Ah oui ce fameux grillage ! »
2. « C'est très pratique pour retrouver sa page. »

Explication détaillée du challenge :

Pour rappel, à la fin de la première partie du challenge, nous avions découvert, via GitHub, le blog personnel de notre cible Patrick Dubois.

Patrick Dubois a écrit de nombreux articles sur différents thèmes : le développement, les animaux et les grillages. Oui, vous avez bien lu, des articles sur les grillages. D'après l'article « Je vends un petit bout de mon grillage tant apprécié » daté du 2 décembre 2018, notre cible est passionnée par les grillages.



02/12/2018 - Je vends un petit bout de mon grillage gris tant apprécié.

Nombreux ici connaissent ma passion pour les grillages ! Et vu que ce blog est là pour parler de moi et de mes passions, je me permets de faire de la pub à moi-même. Et oui !
Mais alors patrick qu'as-tu à nous vendre ? Et bien je vends une partie des restes de mon grillage qui a tant eu du succès sur les sites de passionnés. La longueur de mon lot est de 20 mètres et la hauteur du grillage est de 1,75m.

Pour en savoir un peu plus comme le prix n'hésitez pas à regarder l'annonce !
Depuis que LBC me bloque mes annonces à cause des prix soi-disant élevés pour les objets (car ils n'y connaissent rien en grillage de qualité), je mets donc maintenant mes annonces sur ce site (que j'ai trouvé un peu par hasard).
A plus.

Illustration 1: article "Je vends un petit bout de mon grillage tant apprécié" du blog personnel de Patrick Dubois

Hormis cet article, les autres articles semblent être des impasses. En effet, M. Dubois mentionne une petite annonce qu'il aurait déposé sur un site dédié à ce genre de service.

En cliquant sur l'annonce dont il fait mention, nous arrivons sur la petite annonce suivante du site « marche.fr » :

Grillage rare — Répondre

Annonce	bonjour, je vends ce maginifique grillage gris bien connu des amateurs de grillage. n'hésitez pas à me contacter pour plus d'informations.
Prix	**72 €**
Ville	LA DEFENSE (92 - Hauts de Seine) nouveau Localiser l'annonce sur une carte
vues	18
	L'annonceur ne souhaite pas être contacté par téléphone Vous pouvez le joindre par mail en cliquant ici
Rubrique	Jardin - Nature - Matériels
Type	Offre passée le 02/12/2018
N° Annonce	61340808
Annonceur	**trickpatpat** (Voir toutes ses annonces)
Site web	NC

Agrandir l'image

Illustration 2: petite annonce "Grillage rare" de l'utilisateur "trickpatpat" présente sur le site "marche.fr"

Cette annonce a été déposée le 2 décembre 2018 par l'utilisateur « trickpatpat ». En cliquant sur « Voir toutes ses annonces » à droite du pseudonyme de l'annonceur, nous arrivons sur une page présentant toutes les annonces déposées par notre cible :

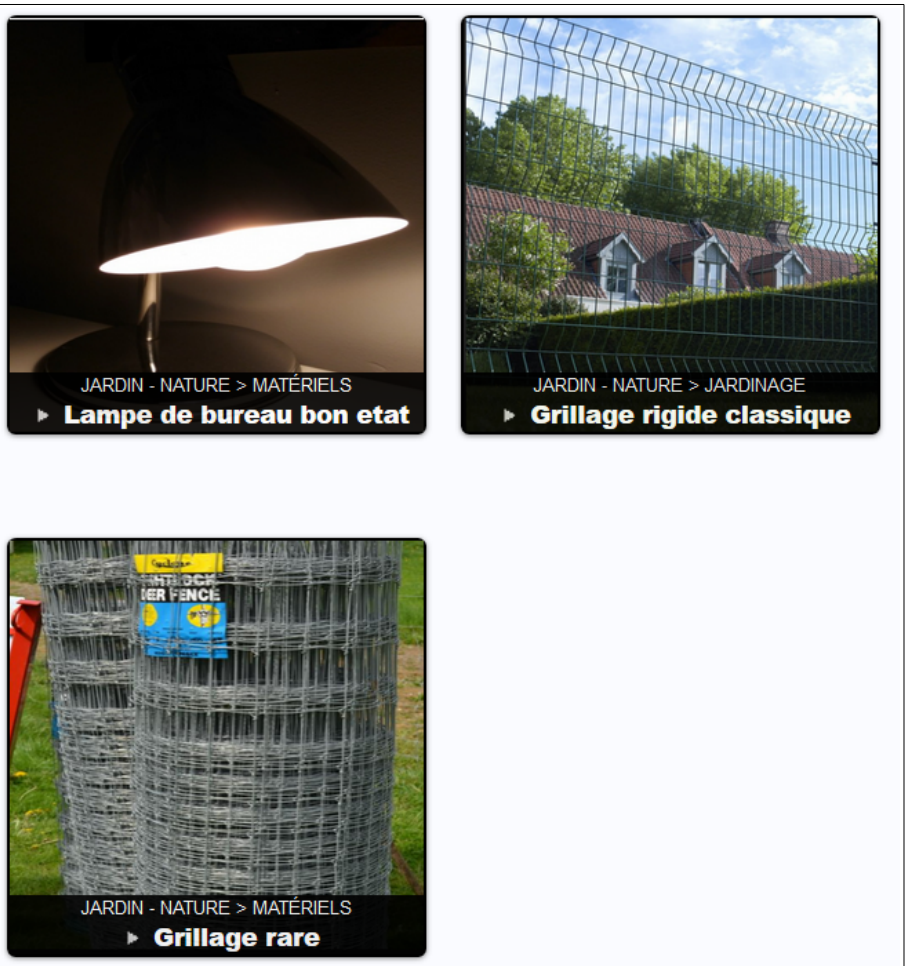


Illustration 3: annonces déposées par l'utilisateur "trickpatpat" sur le site "marche.fr"

En fouillant toutes les annonces déposées par Patrick Dubois, nous découvrons une image très intéressante. En effet, l'annonce portant le titre «LAMPE DE BUREAU BON ETAT» possède trois images. Parmi ces dernières, nous découvrons un bout d'écran affichant la page d'accueil de Facebook :

Illustration 4: deuxième photo de l'annonce "LAMPE DE BUREAU BON ETAT"

En zoomant sur l'écran présent dans cette photographie, nous apercevons la photo d'un compte Facebook et le prénom utilisé par ce compte. La photo est un petit chat blanc et le prénom est identique au pseudo utilisée par notre cible sur le site de petites annonces : trickpatpat ».

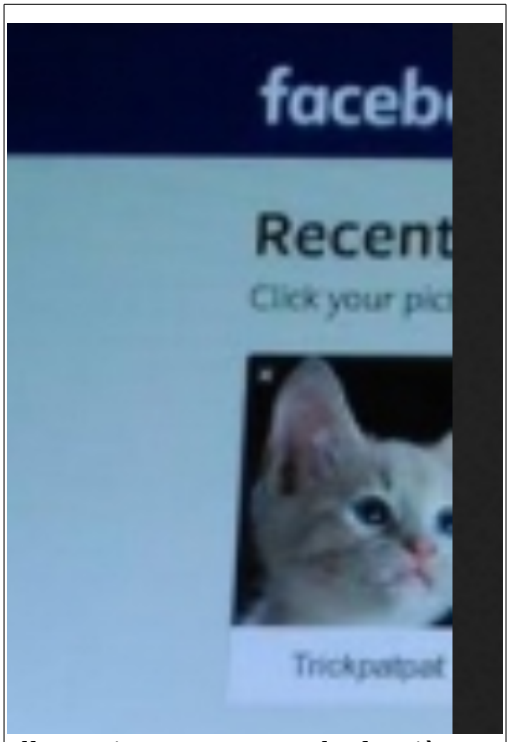


Illustration 5: zoom sur la deuxième photo de l'annonce "LAMPE DE BUREAU BON ETAT"

En effectuant une recherche de ce pseudonyme sur Facebook, nous obtenons seulement deux résultats :

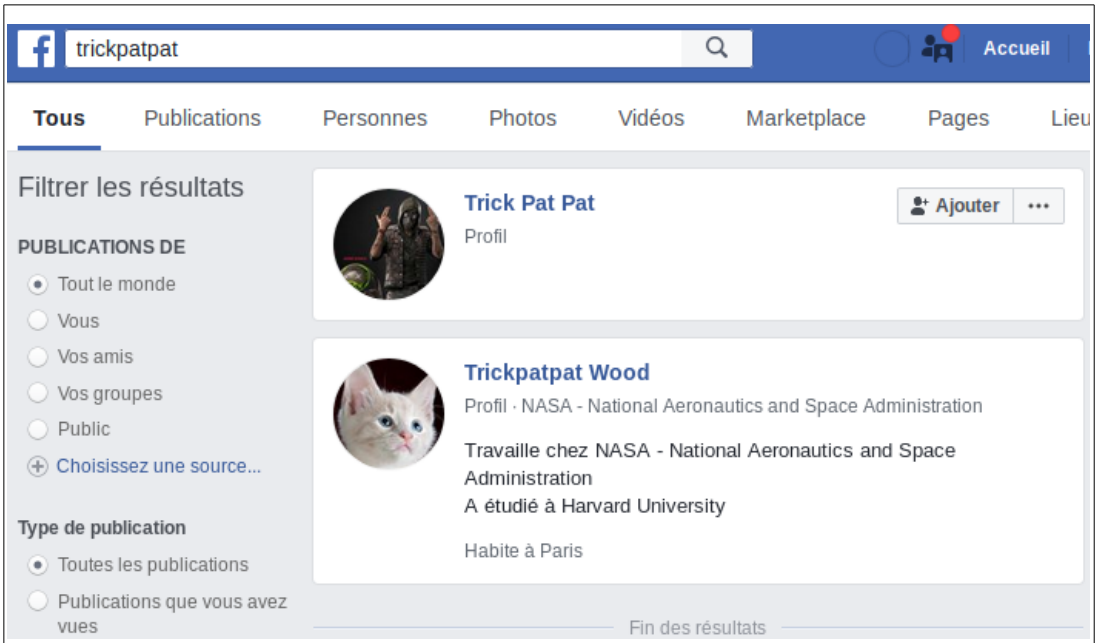


Illustration 6: résultat de la recherche "trickpatpat" sur Facebook

En outre, grâce à la photo de profil identifiée précédemment grâce à l'annonce, nous en déduisons que le compte Facebook de M. Dubois est « Trickpatpat Wood ».

Ce compte est plutôt fournit grâce à de nombreuses publications partagées par notre cible. Cependant, parmi ces dernières, une publication d'une page nous interpelle. Le nom de cette page est « Mongrillagemavie ».

Illustration 7: page Facebook "Mongrillagemavie"

Au vu de la photo de profil utilisée par la page ainsi que par son nom, nous pouvons en déduire que M. Dubois fait référence à « Mongrillagemavie » en utilisant l'acronyme MGMV.

En parcourant les quelques publications présentes sur la plage, nous apprenons que cette dernière est la page officielle du site mongrillagemavie.com, site dédié aux passionnés de grillage.

La dernière publication a pour but d'informer tous les fans de la page « Mongrillagemavie » que suite à une faille de sécurité dans la base de données, l'ensemble des comptes utilisateurs de MGMV sont potentiellement tombés dans les mains d'une personne mal intentionnée. Cependant, l'administrateur de la page rassure les passionnés de grillage en précisant que les mots de passe étaient protégés par une technologie fiable :

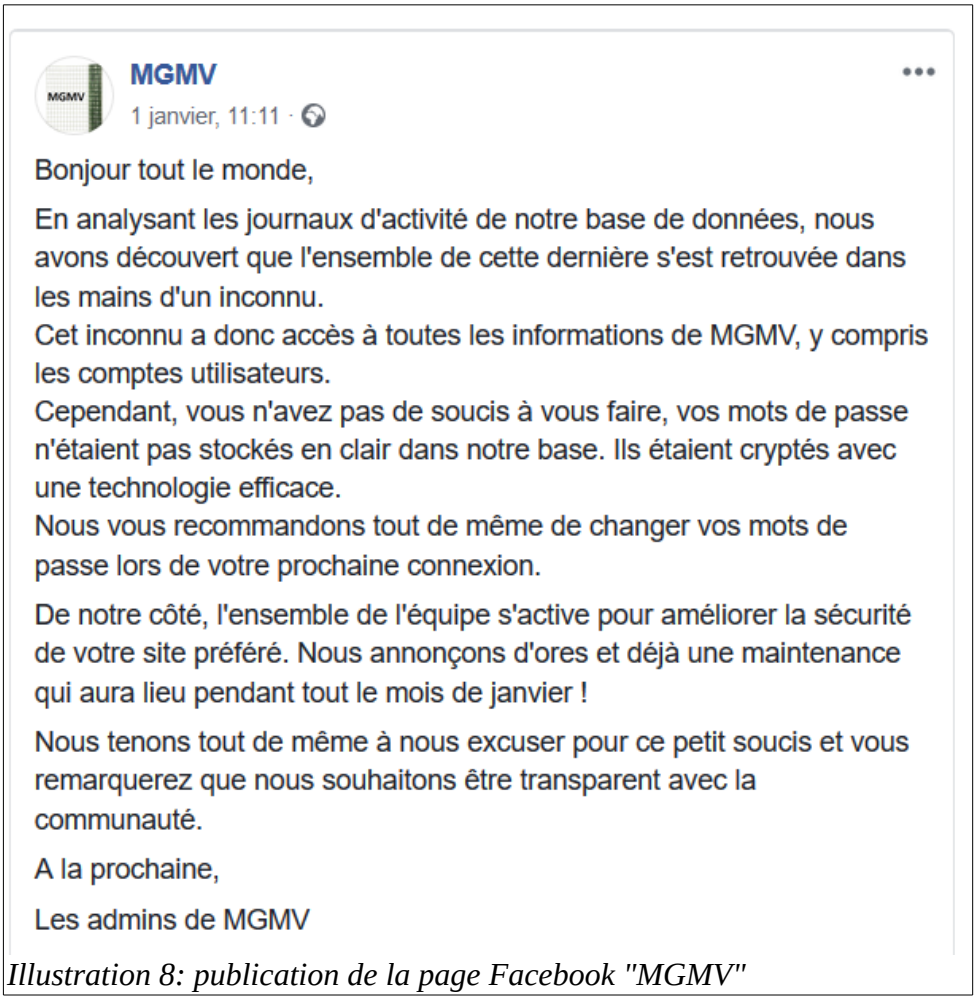


Illustration 8: publication de la page Facebook "MGMV"

La publication précise également que le site ne sera pas disponible tout au long du mois de janvier.

Pour de diverses raisons, de nombreuses bases de données compromises se retrouvent sur Internet. Les pirates utilisent notamment des outils connus pour partager les base de données piratées. C'est le cas du site « pastebin.com ». Ce site permet de mettre à disposition du texte facilement et rapidement : une fois le texte à partager renseigné sur le site, ce dernier va générer un lien. Lien qui va permettre à d'autres internautes d'accéder au texte.

Il peut alors être intéressant de rechercher le terme « mongrillagemavie » sur certains moteurs de recherche.

Ainsi, en utilisant le moteur de recherche le plus utilisé au monde, Google, et un de ses « dork » connu pour rechercher sur le site pastebin.com, nous obtenons un résultat :

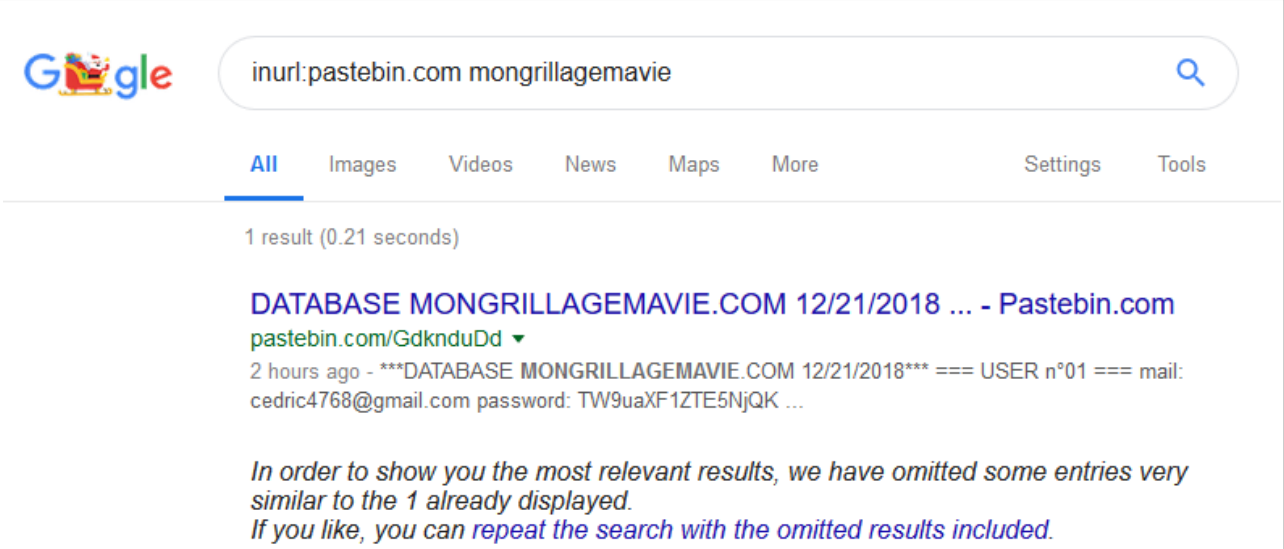


Illustration 9: résultat de la recherche Google "inurl:pastebin.com mongrillagemavie"

Ce « pastebin » semble bel et bien être la base de données du site mongrillagemavie.com. En inspectant ce dernier, nous découvrons 13 couples mail/password appartenant certainement à des membres de MGMV :

Illustration 10: extrait du pastebin contenant la base de données de MGMV

Parmi ces 13 utilisateurs, un compte retient notre attention. L'utilisateur numéro 11 utilise l'adresse mail « patpat.dubois@gmail.com » pour se connecter à MGMV :

```
43. === USER n°11 ===
44. mail: patpat.dubois@gmail.com
45. password: RU5TSUJTe0RpZ2lDYXJyb3NzX3BhcnQyX01kcF9Qcm9fRWdhbGVfTWRwX1BlcnNvfSA=
46.
```

Illustration 11: utilisateur numéro 11 présent sur le pastebin

En outre, les mots de passe ne sont pas en clairs mais ne sont pas non plus protégés. Les chaînes de caractère contenu dans les champs « password » sont les base64 des mots de passe.

La base64 d'une valeur est son encodage en 64 caractères. Cette base est notamment utilisée pour rendre l'information disponible sur une grande majorité des systèmes.

De nombreux outils permettent de décoder ou d'encoder une chaîne de caractère en base64. Si nous prenons par exemple l'outil « www.base64decode.org» et que nous décodons la chaîne présente dans le champ « password » pour l'utilisateur numéro 11, nous obtenons le résultat suivant :

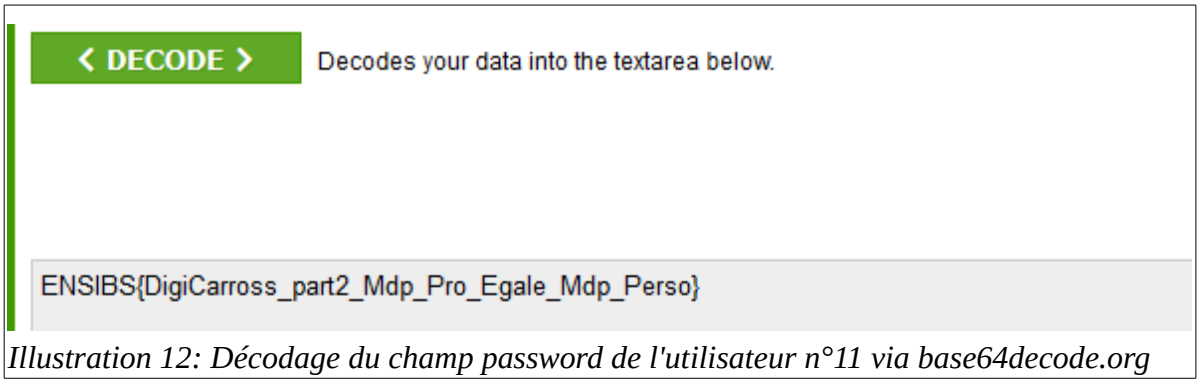


Illustration 12: Décodage du champ password de l'utilisateur n°11 via base64decode.org

Bingo ! La base64 décodée nous donne le second flag :

ENSIBS{DigiCarross_part2_Mdp_Pro_Egale_Mdp_Perso}

Ce flag annonce la fin du challenge DigiCarross.

Conclusion

Patrick Dubois aurait pu facilement éviter de se retrouver dans une telle situation. Tout d'abord, il aurait dû utiliser, pour ses activités professionnelles, des mots de passe différents que ceux qu'il utilise dans ses activités personnelles. Encore faut-il que M. Dubois n'utilise pas qu'un seul mot de passe pour l'ensemble de ses activités.

Ce genre d'habitude peut facilement être évitée en utilisant un manager de mots de passe tel que KeePass.

De plus, il est vital de vérifier et contrôler les informations que nous mettons à disposition sur Internet. Ceci est surtout valable pour les réseaux sociaux et les blogs personnels. Il n'est pas rare de voir des personnes publiées sur les réseaux sociaux leur colis reçu sans prêter attention à l'enveloppe laissée en arrière plan dévoilant leur adresse.

Dans le cas de Patrick Dubois, nous avons pu, grâce à une erreur d'inattention sur une photo d'une petite annonce, découvrir une page Facebook directement liée à l'une des passions de notre cible. Malheureusement, la base de donnée du site lié à la page Facebook a été compromise et l'ensemble des couples login/mot de passe sont présents sur un pastebin. Cet exemple semble tiré par les cheveux mais il est parfois possible de compromettre l'ensemble d'une entreprise à cause de ce genre de comportement.

En outre, une adresse mail est également présente sur le blog de Patrick afin de le contacter directement. On retrouve ce principe dans de nombreux blogs, pages personnelles ou CV en lignes. Il est important ne pas indiquer son adresse mail quotidienne sur ce genre de support. Il faut donc créer une adresse mail dédiée à cette utilisation.

En effet, si vous indiquez votre adresse mail principale sur un blog personnel par exemple, une personne mal intentionnée ira directement rechercher sur des sites spécialisés si cette adresse mail est présente au sein d'un « leak » de base de données (ex : haveibeenpwned.com). Si c'est le cas, il trouvera généralement sans difficulté (ex :ghostproject.fr) le mot de passe en clair rattaché à cette adresse mail dans un des « leak ».