

NoBrackets CTF



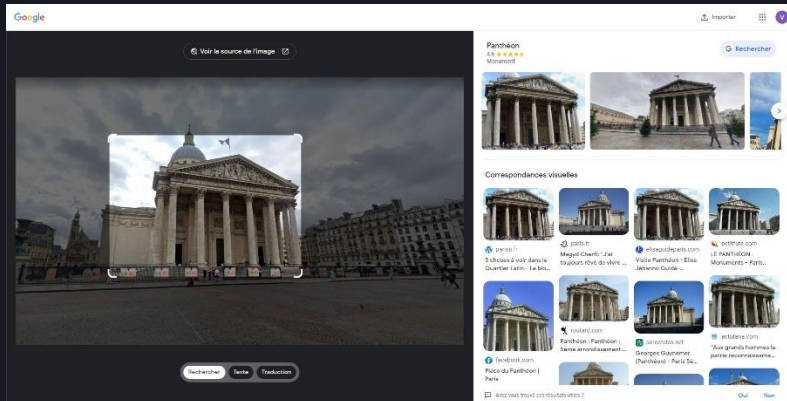
WriteUp by val74k

OSINT

Geosint 1/2 :

Après avoir téléchargé l'image lieu_rdv.png, je remarque un drapeau français sur le bâtiment et des bâtiments au style Haussmannien, ce qui me fait fortement penser à Paris.

L'énoncé indique qu'il faut trouver une place, donc pour retrouver le lieu d'où la photo a été prise, j'utilise un outil de reconnaissance d'image : le plus connu Google Image qui arrive facilement à identifier le nom du bâtiment présent sur l'image : Le Panthéon



Le Panthéon est à Paris, qui est cohérent avec ma supposition.

Maintenant pour la place où est situé le Panthéon, je fais tout simplement la recherche Panthéon sur Google Maps : Place du Panthéon.

Donc pour valider le challenge, j'en déduis que le flag est :
NBCTF{place_du_pentheon}

Carte d'invitation :

D'après l'énoncé, je dois rechercher le pseudonyme secret20 (anciennement Marguerite Cleenewerck de Crayencour). Pour cela, j'utilise l'outil [Osint Framework](#) , je clique sur la première allitération : Username puis sur Username Search Engines.

Parmi les sites proposés, je choisis avec l'expérience, [WhatsMyName](#) qui va me permettre de retrouver tous les sites où le pseudo secret20 est présent (54/508).

Après avoir essayé plusieurs sites où le profile secret20 est présent, je tombe sur le profile Github de secret20 dont son deuxième pseudo est 0xMarg_Cleenewer_ ce qui est fortement correspondant à l'ancien pseudo de secret20. Sur son Github un repository est présent : « my_super_project » qui contient « flag.txt » mais le flag n'est pas dedans... Je remarque alors qu'il est écrit « Latest commit ... on Sep 22 » ce qui signifie qu'il y a eu d'autres versions de projet, je vérifie donc les commits et je remarque les commits « don't touch ». La plus vieille version de ce commit contient le fichier .secret.txt qui contient le flag : NBCTF{OSInt_W!th_\$h€rL0ck_!S_Th€_B€\$T}

FORENSIQUE

Pong :

Pour commencer, je télécharge le fichier pong.pcapng dont l'exercice .pcapng m'est familière : c'est un format utilisé pour enregistrer une capture de paquets sur un réseau. Avec mon expérience je sais très bien que ce type de fichier est ouvrable avec le logiciel Wireshark, ce qui est cohérent avec la question posée à la fin de l'énoncé.

Donc j'ouvre ce fichier dans Wireshark et il me suffit de cliquer sur le 5^{ème} paquet et je remarque le flag en bas de l'écran : NBCTF{pIng_P0nG}

(Qui était aussi présent sur tous les paquets en Protocol ICMP).

The screenshot shows the Wireshark interface with a packet capture of a Pong game. The 5th packet is selected, and the packet details pane shows an ICMP Echo (ping) request. The packet bytes pane shows the raw data, with a red box highlighting the flag NBCTF{pIng_P0nG}.

Packet 5 details:

- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0xdf26 [correct]
- [Checksum Status: Good]
- Identifier (BE): 6608 (0x19d0)
- Identifier (LE): 53273 (0xd019)
- Sequence Number (BE): 1 (0x0001)
- Sequence Number (LE): 256 (0x0100)
- [Response frame: 6]
- Timestamp from icmp data: Sep 22, 2022 13:03:35.000000000 Paris, Madrid (heure d'été)
- [Timestamp from icmp data (relative): 0.068520139 seconds]
- Data (48 bytes)
- Data: 660b0100000000004e424354467b70496e675f50306e477d4e424354467b70496e675f50...
- [Length: 48]

Packet bytes (hex and ASCII):

```
0000 02 42 ac 11 00 02 02 42 dc 04 b8 6e 08 00 45 00  .B....B...n..E..
0010 00 54 7f 9e 40 00 40 01 62 e5 ac 11 00 01 ac 11  .T..@.@b.....
0020 00 02 08 00 df 26 19 d0 00 01 07 41 2c 63 00 00  .8.....A.c...
0030 00 00 66 0b 01 00 00 00 00 00 4e 42 43 54 46 7b  .f.....NBCTF{
0040 70 49 6e 67 5f 50 30 6e 47 7d 4e 42 43 54 46 7b  pIng_P0n G}NBCTF{
0050 70 49 6e 67 5f 50 30 6e 47 7d 4e 42 43 54 46 7b  pIng_P0n G}NBCTF{
0060 70 49                                     pI
```

SYSTÈME

La fin des systèmes d'exploitation propriétaires 1/10 :

Pour valider ce challenge, j'ai utilisé le logiciel PuTTY pour me connecter en SSH à l'adresse challenge.nobrackets.fr avec comme port 1026 et comme login « gcc ».

J'ai ensuite mis le mot de passe « e4kpNeYj5J1yKMz2avmj » qui est écrit dans l'énoncé puis j'ai fait la commande `ls` pour lister le contenu du répertoire où je me trouve. J'ai trouvé le fichier `flag.txt` et j'ai finalement fait la commande `cat flag.txt` pour afficher le contenu du fichier qui est le flag :
NBCTF{GNU_Linux_power}

La fin des systèmes d'exploitation propriétaires 2/10 :

Même chose que pour le challenge précédent mais cette fois si, lorsque je fais la commande `ls`, rien ne s'affiche donc par réflexe j'ai tout simplement fait la commande `ls -la` qui me permet de lister également les fichiers cachés, ce qui est bien le cas : un fichier `.flag.txt` est bien présent. Donc il me suffit de faire la commande `cat .flag.txt` pour recevoir le flag : NBCTF{M3ss4g3_s3cr3t}

La fin des systèmes d'exploitation propriétaires 3/10 :

Cette fois si, même processus que les deux derniers challenges, mais aucun fichier ainsi qu'aucun fichier caché. A la fin de l'énoncé une aide est présente « Commande : find » donc j'en déduis qu'il faut faire cette commande.

Donc pour rechercher correctement dans la machine, je fais la commande `cd /` qui me permet de me retrouver à la racine et alors comme dans les deux derniers challenges le fichier se nommait « flag.txt » je fais donc la commande : `find -name flag.txt` et cela me renvoie pleins de `flag.txt` trouvé mais en permission denied sauf un seul qui se trouve dans le répertoire `var/log`.

Je fais alors la commande `cd var/log` puis `cat flag.txt` et je retrouve le flag :
NBCTF{man_linux_great_again}

STÉGANOGRAPHIE

Toutes les couleurs méritent la même attention :

Ce challenge m'a pris un peu plus de temps que les autres car je suis allé beaucoup trop loin jusqu'à que je trouve par hasard la solution à force de chercher :

Lorsque j'ai passé ma souris un peu plus bas dans le document, mon curseur a changé et c'est là que j'ai découvert que le flag était présent mais coloré en texte blanc.

J'ai donc sélectionné aveuglement le texte puis je l'ai copier-coller :

NBCTF{Wh1te_is_discreet7}

L'oreiller d'un enfant

*Cher petit oreiller, doux et chaud sous ma tête,
Plein de plume choisie, et blanc ! et fait pour moi !
Quand on a peur du vent, des loups, de la tempête,
Cher petit oreiller, que je dors bien sur toi !*

*Beaucoup, beaucoup d'enfants pauvres et nus, sans mère,
Sans maison, n'ont jamais d'oreiller pour dormir ;
Ils ont toujours sommeil. Ô destinée amère !
Maman ! douce maman ! cela me fait gémir.*

*Et quand j'ai prié Dieu pour tous ces petits anges
Qui n'ont pas d'oreiller, moi j'embrasse le mien.
Seule, dans mon doux nid qu'à tes pieds tu m'arranges,
Je te bénis, ma mère, et je touche le tien !*

*Je ne m'éveillerai qu'à la lueur première
De l'aube ; au rideau bleu c'est si gai de la voir !
Je vais dire tout bas ma plus tendre prière :
Donne encore un baiser, douce maman ! Bonsoir !*

Marceline Desbordes-Valmore.

████████████████████I

CRYPTOGRAPHIE

Connaissez-vous la substitution ? :

Après avoir téléchargé le fichier « message_encore.txt » j'ai découvert un string ressemblant fortement au format du flag mais sans être le flag :

AOPGS{Ebg13_vf_a0g_p0zcy1p4g3q}

A première vue je dirais que c'est du code César, et pour vérifier cela je suis allé sur le site dcode.fr, dans la catégorie code césar et j'ai inséré le string, Dcode m'a ensuite renvoyé le flag : NBCTF{Rot13_is_n0t_c0mpl1c4t3d}

Décode ton monde 1/6 :

Après avoir téléchargé le fichier j'ai directement reconnu du binaire, j'ai donc cherché sur google « binaire to text » et j'ai entré le binaire sur convertbinary.com qui m'a donné le flag : NBCTF{pas_a_la_mano_la_crypto}

Décode ton monde 2/6 :

Pour celui-ci, comme pour le challenge précédent sauf que cette fois-ci, j'ai repéré du hexadécimal, j'ai donc cherché sur google « hex to text » et le site.unit-conversion.info m'a donné le flag : NBCTF{le_binaire_ca_va_deux_minutes}

WEB

L'envol d'Hélène 1/4 :

Après avoir fouillé le [site](#), j'ai découvert que vers la fin du [code source](#) (CTRL+U) de la page /histoire il y a le flag commenté : NBCTF{h313n3_b0uch3r_vole_avec_le_flag}

Le fan club 1 :

Pour ce [site](#) là, il suffit d'aller dans la partie /admin.html et de regarder également le code source (CTRL+U) pour voir :

l'email : fanclubmariecurie@gmail.com et le mot de passe : mysuperstrongpswd123!!

A la fin du [code source](#). Il suffit donc de rentrer cela dans le login sur la page /admin pour avoir le flag : NBCTF{js-cest-pas-secure}