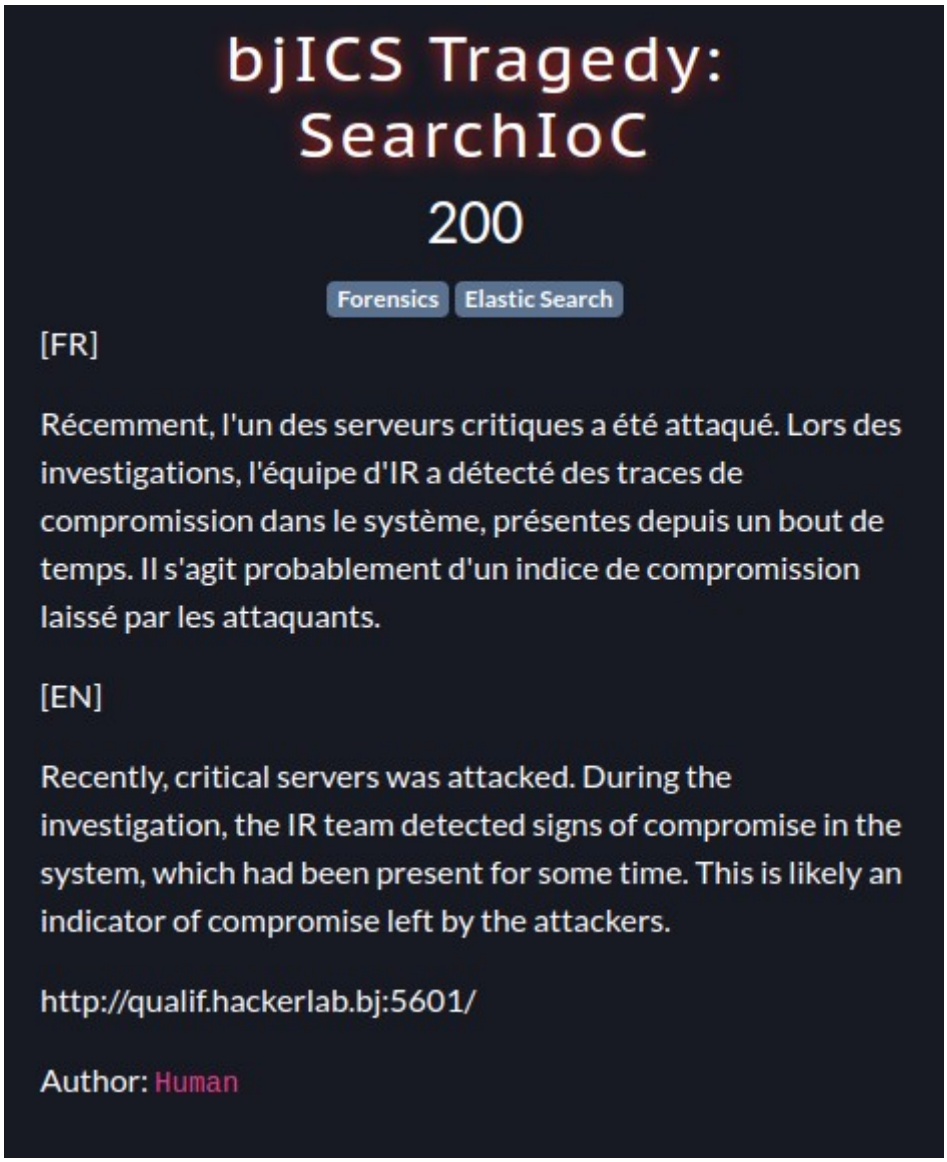
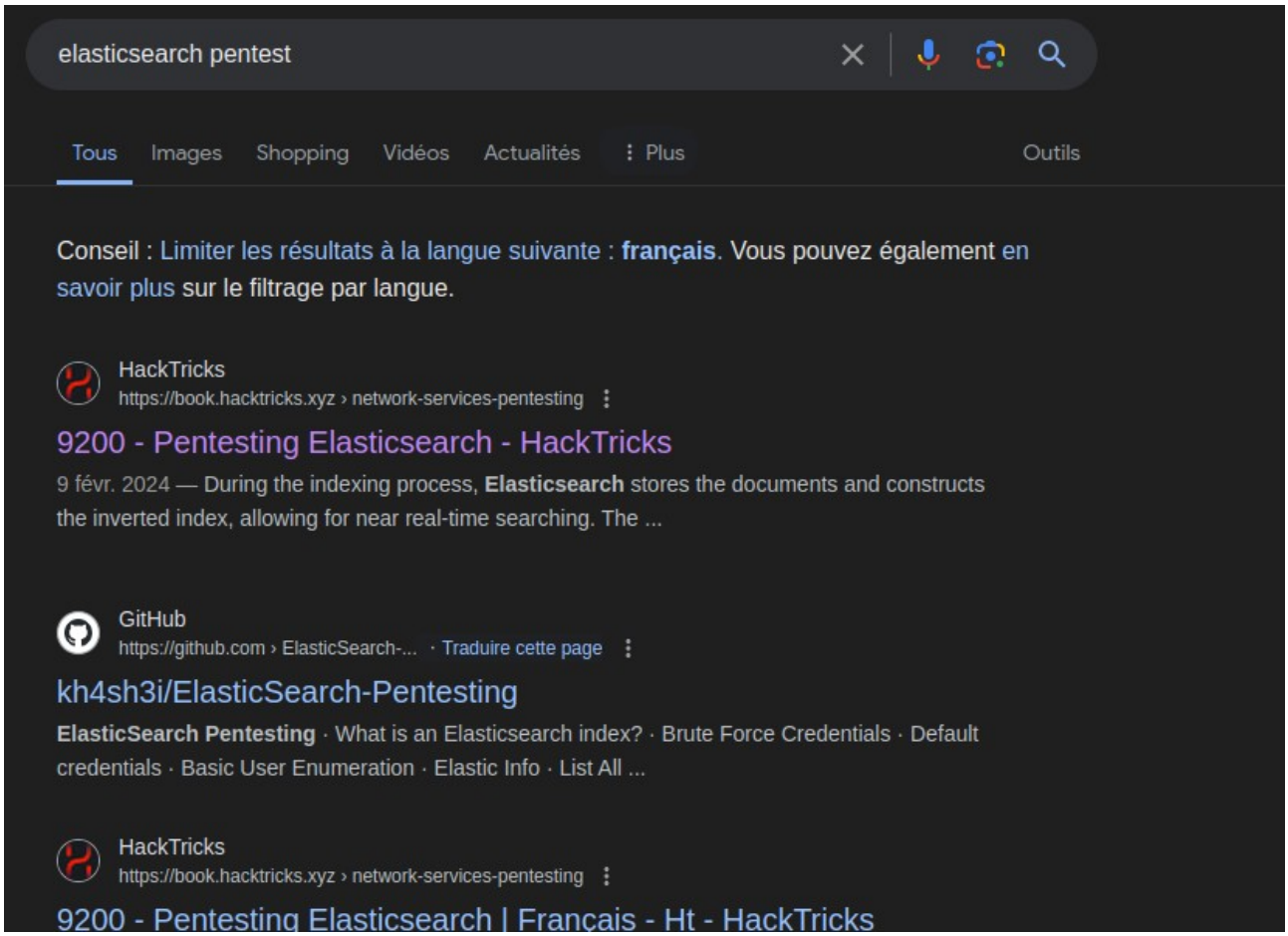
Writeup pour le challenge bjICS Tragedy: SearchIoc de la phase de qualification pour le HackerLab2024

Nom d'utilisateur : takeoff
E-mail : robertohoungbo@gmail.com
Affiliation : IFRI
Pays : Bénin

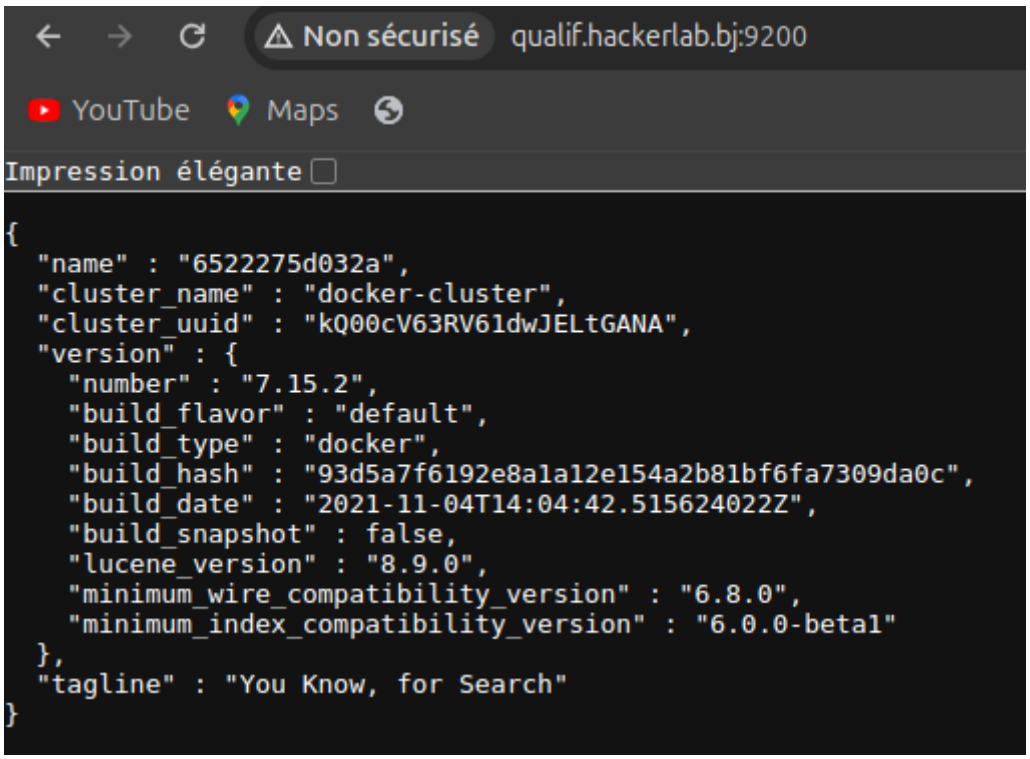


Le but du challenge est de trouver un indice de compromission laissé par les attaquants.

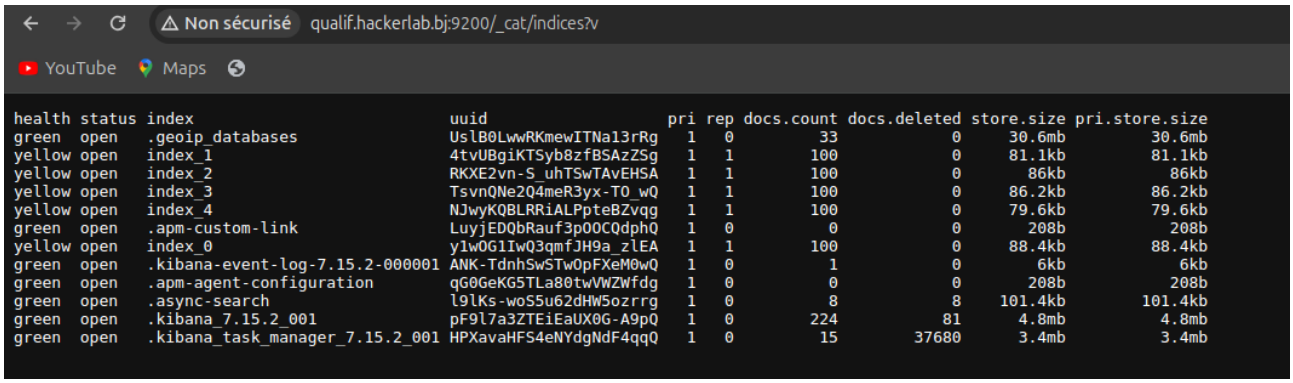
Le lien du challenge m'a mené vers le dashboard d'elasticearch à l'url http://qualif.hackerlab.bj:5601/app/home#/ . J'ai ensuite cherché des données à exploiter au niveau des différents onglets de navigation mais rien de concluant après 1h de recherche. J'ai alors décidé de faire une petite recherche sur internet avec les mots clés suivant : elasticsearch, pentest.



Le premier résultat de la recherche m'a mené vers un article sur le pentest d'elasticsearch proposé par Hactricks. En lisant l'article je me suis rendu compte que je pouvais accéder à elasticsearch par un autre port , le port 9200. Je m'y suis donc rendu et j'ai eu le rendu suivant :



Toujours en lisant l'article, j'ai appris que les données dans elastisearch sont stockées sur des index et que je pouvais faire un dump pour les récupérer. Avant tout j'ai d'abord essayé de voir si dans mon cas, il existait des index. J'ai accédé à l'url http://qualif.hackerlab.bj:9200/_cat/indices?v, ce qui m'a affiché les index nommés index_0, index_1, index_2, index_3, et index_4.



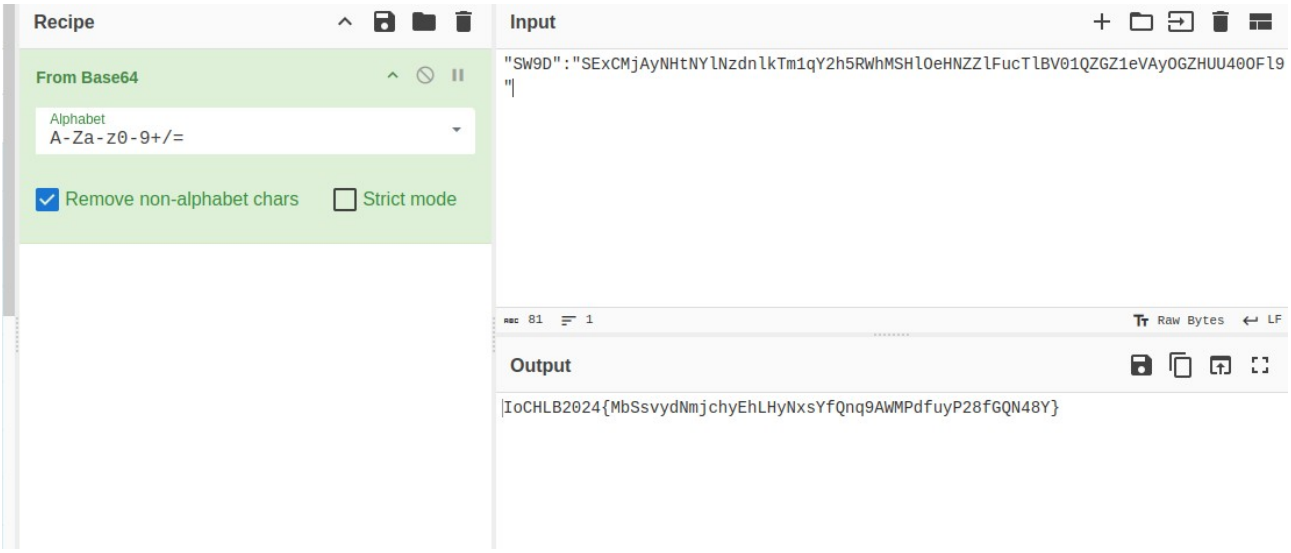
Ensuite j'ai cherché un outil pour faire le dump des données de chaque index. Je suis tombé sur l'outil elasticdump. Et pour dumper les données de chaque index j'ai utilisé la commande suivante : elasticdump --input=http://qualif.hackerlab.bj:9200/index_0 --output=index_0 --type=data

```
roberto@roberto-HP-Pavilion-x360-Convertible:~/JSshell$ elasticdump --input=http://qualif.hackerlab.bj:9200/index_0 --output=index_0 --
type=data
Mon, 03 Jun 2024 12:04:52 GMT | starting dump
Mon, 03 Jun 2024 12:04:53 GMT | got 100 objects from source elasticsearch (offset: 0)
Mon, 03 Jun 2024 12:04:53 GMT | sent 100 objects to destination file, wrote 100
Mon, 03 Jun 2024 12:04:53 GMT | got 0 objects from source elasticsearch (offset: 100)
Mon, 03 Jun 2024 12:04:53 GMT | Total Writes: 100
Mon, 03 Jun 2024 12:04:53 GMT | dump complete
```

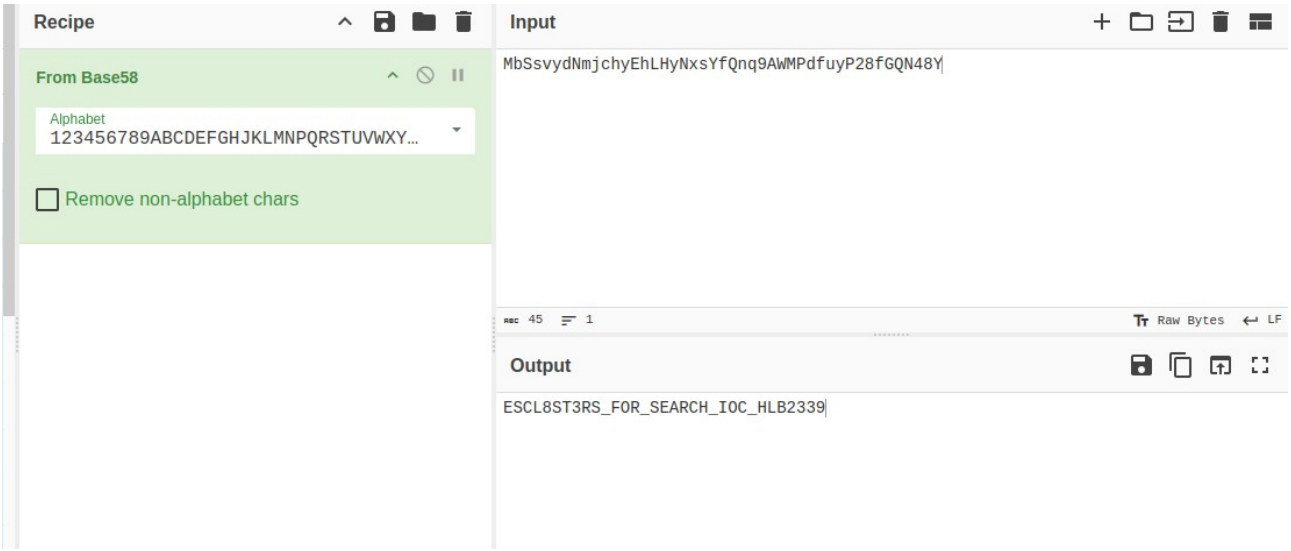
J'ai exécuté la même commande pour récupérer toutes les données de chaque index dans différents fichiers portant le nom de l'index correspondant.

J'ai analyser ces données pendant un long moment en vain, sans rien trouver de concret. Je me suis alors retourné vers l'énoncé du challenge puis je me suis demandé ce à quoi servait l'indication SearchIoC.

J'ai cogité pendant un moment et j'ai recommencé l'analyse des données en inspectant scrupuleusement les noms des champs de chaque index puis au niveau de l'index_3, j'ai constaté un champ qui portait le nom IoC encodé en base64 (SW9D)). J'ai ensuite décodé la valeur du champ sur cyberchef et j'ai eu le résultat suivant :



A ce moment je me suis dit que j'avais trouvé le flag, je l'ai soumis mais il était erroné. J'ai compris que l'intérieur était encodé en base 58 en le décodant sur cyberchef :



Flag : HLB2024{ESCL8ST3RS_FOR_SEARCH_IOC_HLB2339}

Merci !