

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

Nom d'utilisateur : takeoff

E-mail : robertohoungbo@gmail.com

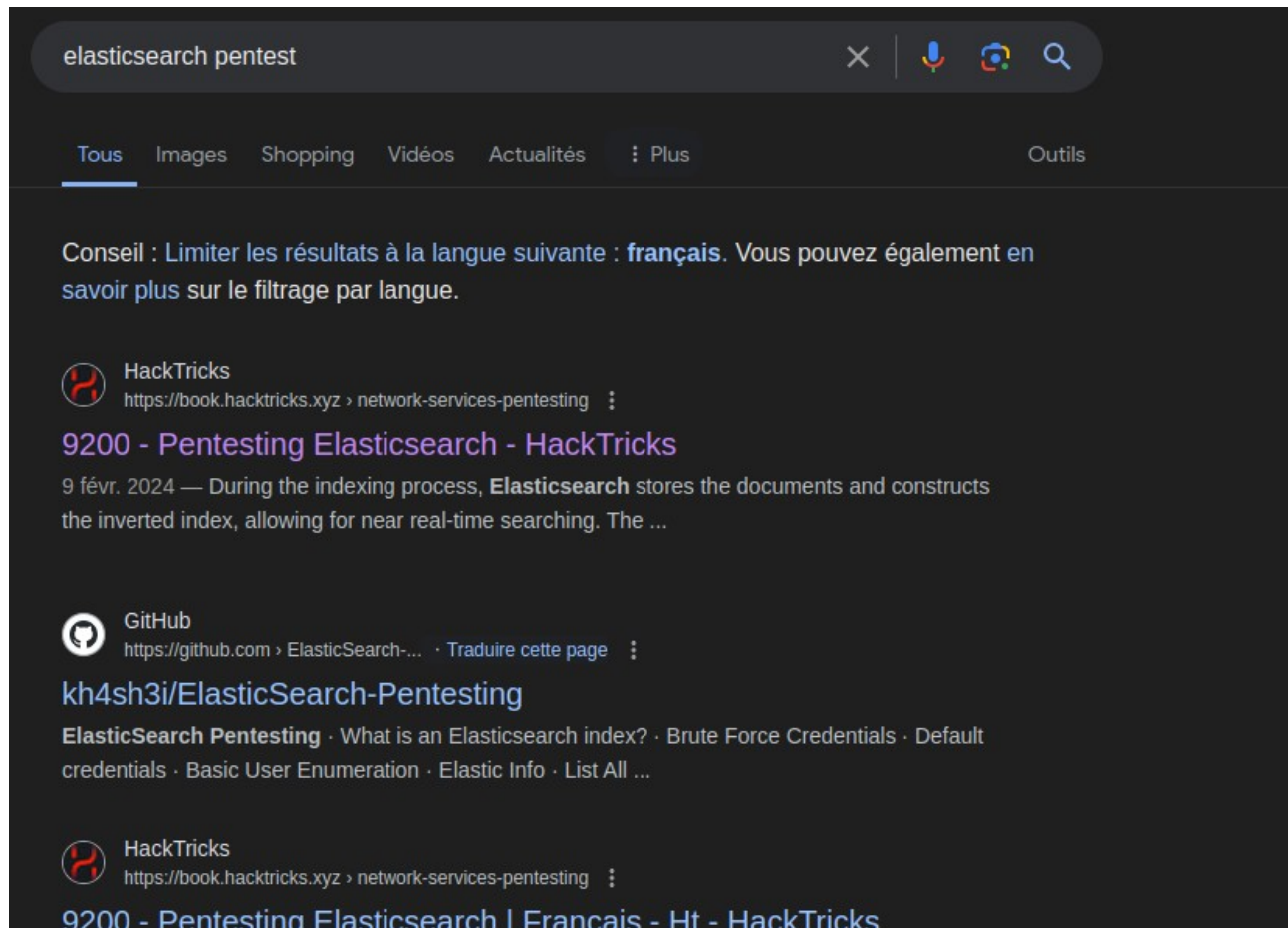
Affiliation : IFRI

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'Elasticsearch 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 suivants : elasticsearch, pentest.



Le premier résultat de la recherche m'a mené vers un article sur le pentest d'Elasticsearch proposé par Hacktricks. 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 :

```
← → ↻ ⚠ Non sécurisé qualif.hackerlab.bj:9200
YouTube Maps
Impression élégante ☐
{
  "name" : "6522275d032a",
  "cluster_name" : "docker-cluster",
  "cluster_uuid" : "kQ00cV63RV61dwJELtGANA",
  "version" : {
    "number" : "7.15.2",
    "build_flavor" : "default",
    "build_type" : "docker",
    "build_hash" : "93d5a7f6192e8a1a12e154a2b81bf6fa7309da0c",
    "build_date" : "2021-11-04T14:04:42.515624022Z",
    "build_snapshot" : false,
    "lucene_version" : "8.9.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Toujours en lisant l'article, j'ai appris que les données dans elasticsearch 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.

health	status	index	uuid	pri	rep	docs.count	docs.deleted	store.size	pri.store.size
green	open	.geopip_databases	Us1B0LwwRKmewITNa13rRg	1	0	33	0	30.6mb	30.6mb
yellow	open	index_1	4tvUBgiKTSyb8zfB5AzzSg	1	1	100	0	81.1kb	81.1kb
yellow	open	index_2	RKXE2vn-S_uhTSwTAvEHSA	1	1	100	0	86kb	86kb
yellow	open	index_3	TsvnQNe2Q4meR3yx-T0_wQ	1	1	100	0	86.2kb	86.2kb
yellow	open	index_4	NJwyKQBLRRiALPpteBZvqg	1	1	100	0	79.6kb	79.6kb
green	open	.apm-custom-link	LuyjEDQbRauf3p00CQdphQ	1	0	0	0	208b	208b
green	open	index_0	y1wOG1IwQ3qmfJH9a_zlEA	1	1	100	0	88.4kb	88.4kb
green	open	.kibana-event-log-7.15.2-000001	ANK-TdnhSwSTwOpFXeM0wQ	1	0	1	0	6kb	6kb
green	open	.apm-agent-configuration	qG0GeKG5TLA80twVWZWfdg	1	0	0	0	208b	208b
green	open	.async-search	l9lKs-wo55u62dHW5ozrrg	1	0	8	0	101.4kb	101.4kb
green	open	.kibana_7.15.2_001	pF9l7a3ZTEiEaUX0G-A9pQ	1	0	224	81	4.8mb	4.8mb
green	open	.kibana_task_manager_7.15.2_001	HPXavaHFS4eNYdgNdF4qqQ	1	0	15	37680	3.4mb	3.4mb

Ensuite j'ai cherché un outil pour faire le dump des données de chaque index. Je suis tombé sur l'outil elasticsearch-dump. Et pour dumper les données de chaque index j'ai utilisé la commande suivante : `elasticsearch-dump --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
```

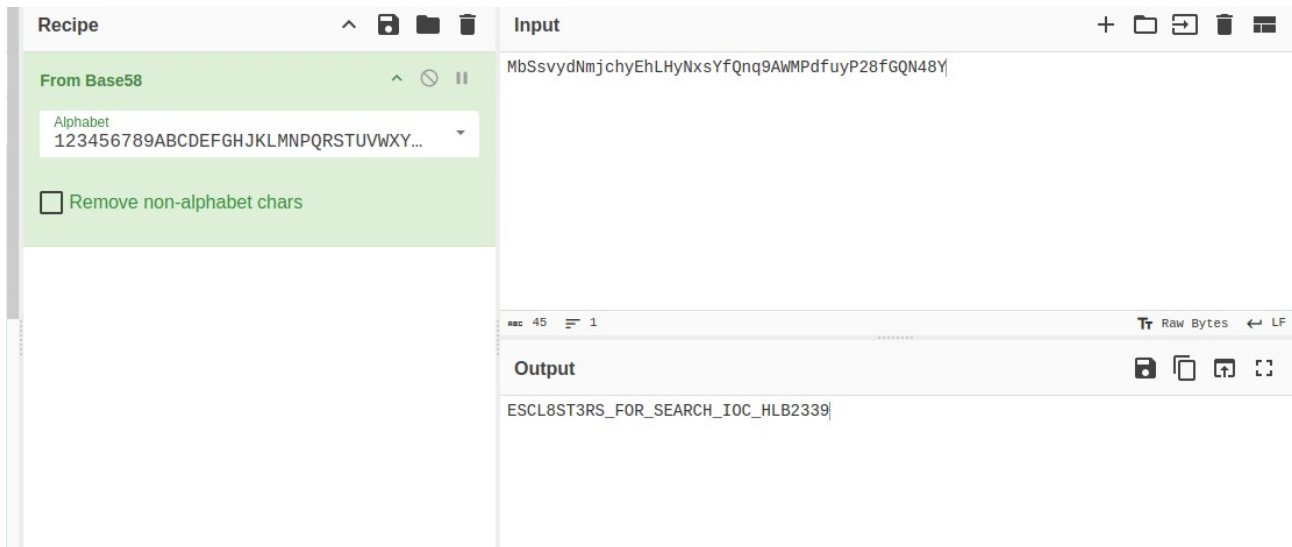
J'ai exécuté la même commande pour récupérer toutes les données de chaque index dans différents fichiers portant le nom de l'index correspondant.

J'ai analysé 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 SearchLoC.

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 loC encodé en base64 (SW9D)). J'ai ensuite décodé la valeur du champ sur cyberchef et j'ai eu le résultat suivant :

The screenshot shows the CyberChef web interface. On the left, a 'Recipe' panel contains a 'From Base64' recipe. The 'Alphabet' dropdown is set to 'A-Za-z0-9+/' and the 'Remove non-alphabet chars' checkbox is checked. The 'Input' panel on the right contains a single line of base64 text: "SW9D": "SExCMjAyNHtNYlNzdnlkTm1qY2h5RWhMSHl0eHNZZlFucTlBV01QZGZ1eVAyOGZHUU400Fl9". Below the input, the 'Output' panel displays the decoded result: [IoCHLB2024{MbSsvydNmjchyEhLHyNxsYfQnq9AWMPdfuyP28fGQN48Y}].

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 !