

HTB SİLENTİUM

Herkese merhaba!!!! Bugün HACKTHEBOX' dan SİLENTİUM makinesini çözeceğiz.

Öncelikle bir nmap taraması ve devamına dir taraması atıyorum.

```
root@kali:~# nmap 10.129.31.196
Starting Nmap 7.95 ( https://nmap.org ) at 2026-04-19 13:46 +03
Nmap scan report for silentium.htb (10.129.31.196)
Host is up (0.15s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 2.58 seconds

root@kali:~# dir 10.129.31.196
dir: '10.129.31.196' ögesine erişilemedi: Böyle bir dosya ya da dizin yok

root@kali:~# gobuster dir -u http://10.129.31.196 \
-w /usr/share/wordlists/dirb/common.txt \
-x php,txt,html \
-t 50

gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

+ ] Url: http://10.129.31.196
```

Dir taramasında staging i görüyorum ve bu beni login sayfasına atıyor.

File	Status	Size	Words	Lines	Duration
staff	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 145ms]	8753	1866	252	145ms
stackdump.txt	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 145ms]	8753	1866	252	145ms
staff.php	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 144ms]	8753	1866	252	144ms
staff.html	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 145ms]	8753	1866	252	145ms
ssl.txt	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 146ms]	8753	1866	252	146ms
staff.txt	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 146ms]	8753	1866	252	146ms
staff.js	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 146ms]	8753	1866	252	146ms
ssl_check.php	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 144ms]	8753	1866	252	144ms
staff_directory	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 144ms]	8753	1866	252	144ms
staff_directory.php	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 145ms]	8753	1866	252	145ms
staff_directory.txt	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 147ms]	8753	1866	252	147ms
staff_directory.html	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 148ms]	8753	1866	252	148ms
staff_directory.js	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 147ms]	8753	1866	252	147ms
staffs	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 146ms]	8753	1866	252	146ms
staffs.txt	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 145ms]	8753	1866	252	145ms
staffs.js	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 146ms]	8753	1866	252	146ms
stage	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 145ms]	8753	1866	252	145ms
staging	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 145ms]	8753	1866	252	145ms
staffs.php	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 147ms]	8753	1866	252	147ms
stage.html	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 146ms]	8753	1866	252	146ms
stage.php	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 145ms]	8753	1866	252	145ms
staffs.html	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 145ms]	8753	1866	252	145ms
stage.js	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 146ms]	8753	1866	252	146ms
stage.txt	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 146ms]	8753	1866	252	146ms
staging.php	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 146ms]	8753	1866	252	146ms
staging.html	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 146ms]	8753	1866	252	146ms
staging.txt	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 145ms]	8753	1866	252	145ms
stale	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 144ms]	8753	1866	252	144ms
staging.js	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 144ms]	8753	1866	252	144ms
stale.php	[Status: 200, Size: 8753, Words: 1866, Lines: 252, Duration: 145ms]	8753	1866	252	145ms

Artık login sayfasını görünüyoruz.

Sign In

Email *

Password *

[Forgot password?](#)

Login

Forget passwd kısmına bakıyoruz.

Reset Password

[Back to Login.](#)

Email *

Reset Token *

Please copy the token you received in your email.

New Password *

Password must be at least 8 characters long and contain at least one lowercase letter, one uppercase letter, one digit, and one special character.

Confirm Password *

Confirm your new password. Must match the password typed above.

Update Password

Token ile işlem yapıldığını görüyoruz bu şekilde giriş yapmaya çalışmalıyız.


```
0::/
/ # cat /proc/1/environ | tr '\0' '\n'
FLOWISE_PASSWORD=F1l3_d0ck3r
ALLOW_UNAUTHORIZED_CERTS=true
NODE_VERSION=20.19.4
HOSTNAME=c78c3cceb7ba
YARN_VERSION=1.22.22
SMTP_PORT=1025
SHLV=1
PORT=3000
HOME=/root
SENDER_EMAIL=ben@silentium.htb
PUPPETEER_EXECUTABLE_PATH=/usr/bin/chromium-browser
JWT_ISSUER=ISSUER
JWT_AUTH_TOKEN_SECRET=AABBCCDDAABBCCDDAABBCCDDAABBCCDDAABBCCDD
SMTP_USERNAME=test
SMTP_SECURE=false
JWT_REFRESH_TOKEN_EXPIRY_IN_MINUTES=43200
FLOWISE_USERNAME=ben
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
DATABASE_PATH=/root/.flowise
JWT_TOKEN_EXPIRY_IN_MINUTES=360
JWT_AUDIENCE=AUDIENCE
SECRETKEY_PATH=/root/.flowise
PWD=/
SMTP_PASSWORD=r04D!!_R4ge
SMTP_HOST=mailhog
JWT_REFRESH_TOKEN_SECRET=AABBCCDDAABBCCDDAABBCCDDAABBCCDDAABBCCDD
SMTP_USER=test
/ #
```

Ve bu shellden şifreyi çekiyoruz.

Bu şifre ile ssh bağlantısı alıp user.txt yi çekiyoruz.

Şimdi root olmak için araştırma yapacağız ss -tulnp ile socket bilgilerine bakıyoruz

```
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

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: Sun Apr 19 19:45:46 2026 from 10.10.15.170
ben@silentium:~$ 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:*	
udp	UNCONN	0	0	0.0.0.0:68	0.0.0.0:*	
tcp	LISTEN	0	4096	127.0.0.1:3000	0.0.0.0:*	
tcp	LISTEN	0	4096	127.0.0.1:3001	0.0.0.0:*	
tcp	LISTEN	0	4096	127.0.0.53%lo:53	0.0.0.0:*	
tcp	LISTEN	0	4096	127.0.0.54:53	0.0.0.0:*	
tcp	LISTEN	0	4096	0.0.0.0:22	0.0.0.0:*	
tcp	LISTEN	0	511	0.0.0.0:80	0.0.0.0:*	
tcp	LISTEN	0	4096	127.0.0.1:8025	0.0.0.0:*	
tcp	LISTEN	0	4096	127.0.0.1:38661	0.0.0.0:*	
tcp	LISTEN	0	4096	127.0.0.1:1025	0.0.0.0:*	
tcp	LISTEN	0	4096	[::]:22	[::]:*	
tcp	LISTEN	0	511	[::]:80	[::]:*	

Buradan bu servislerin sadece localhost a çalıştığını görüyoruz.

http analizinde gogs un çalıştığını görüyoruz ve 3000 ile bir ssh açıp o ssh a dokunmuyoruz yani ssh tunneling yapıyoruz.

Araştırma sonucu bu zafiyetin CVE-2025-8110 olduğunu görüyoruz.

Gogs a girip kullanıcı açıyoruz. Ve scripti doğru bir şekilde çalıştırarak root flagi çekiyoruz.

