Vacaciones

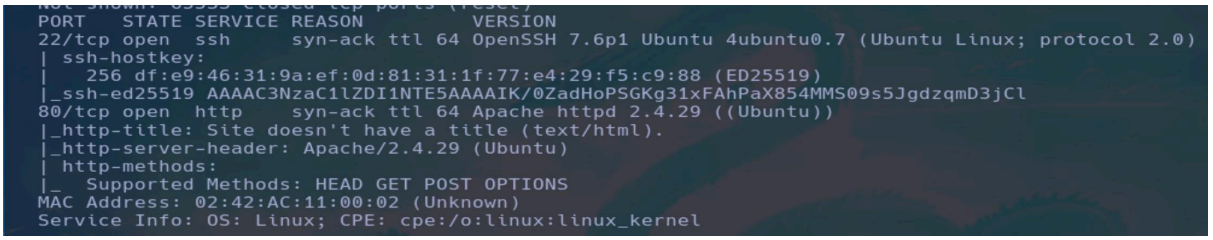
Una vez desplegada la máquina haremos un escaneo de puertos abiertos con nmap.

En mi casa utilizo el siguiente comando:

nmap -p- -sS -sC -sV --min-rate 5000 -n -vvv -Pn (ip objetivo)

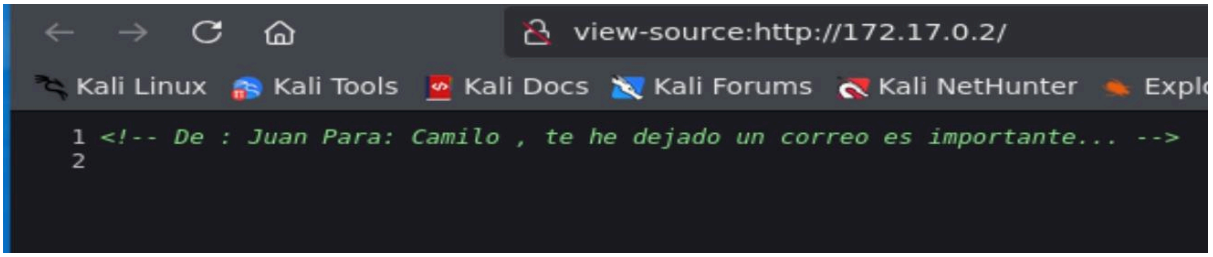
- **-p-**: Escanea todos los puertos .
- **-sS**: Realiza un escaneo sigiloso (SYN Scan) para detectar puertos abiertos.
- **-sC**: Ejecuta scripts predeterminados para recopilar más información del sistema.
- **-sV**: Detecta las versiones de los servicios en ejecución.
- **--min-rate 5000**: Acelera el escaneo enviando al menos 5000 paquetes por segundo.
- **-n**: No realiza resolución DNS, trabaja directamente con direcciones IP.
- **-vvv**: Muestra información detallada y actualizaciones constantes durante el escaneo.
- **-Pn**: Salta el "ping" previo y fuerza el escaneo, incluso si el objetivo no responde.

una vez realizado el escaneo vemos que tenemos dos puertos abiertos

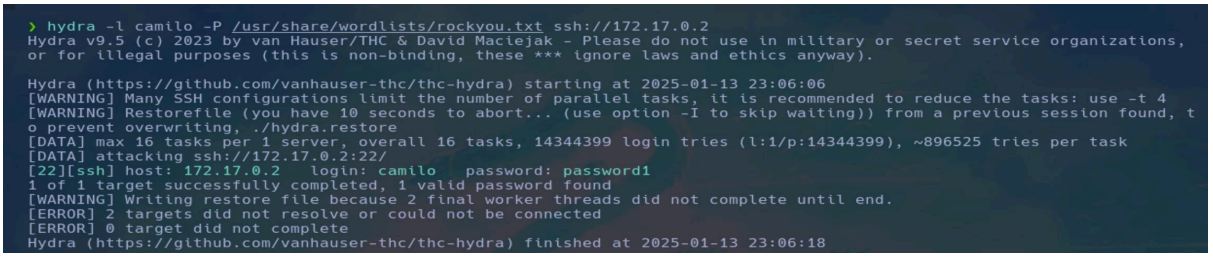


el puerto 22 corre un openSSH en un version <7.7 pero no se puede enumerar los usuarios con metasploit por lo que al tener el puerto 80 nos inidica que hay una pagina wed

La página no nos dice nada por lo que intento buscar subdominios ocultos con gobuster pero no encuentra nada, por lo que me quedaría mirar el codigo fuente de la pagina



Dos posibles usuarios podrían ser juan o camilo por lo que intentamos sacar la contraseña de los dos por fuerza bruta utilizando hydra y este solo nos encuentra la contraseña de camilo.



Nos contectamos por el puerto ssh con el siguiente comando : ssh camilo@172.17.0.2 y vemos que no somos root así que habrá que escalar privilegios.

Una forma sencilla es buscar binarios SUID que podamos aprovechar para escalar privilegios con el comando : find / -perm -4000 2>/dev/null

o binarios Sudo con sudo -l

No encontramos ningún binario pero recordemos el mensaje de juan a camilo, decía que le había enviado un email por lo que vamos a la carpeta donde se encuentran los email: cd /var/mail entramos a la carpeta camilo y vemos un archivo correo.txt hacemos un cat para visualizarlo y tenemos que

Tenemos la contraseña de juan asi que nos conectaremos por ssh con: ssh juan@172.17.0.2 y de la misma manera buscamos escalar privilegios con algun binario. con sudo -l encontramos el binario ruby,para encontrar las vulnerabilidades recomiendo esta pagina: https://gtfobins.github.io/

En nuestro caso buscamos el binario ruby nos aparece la opción de Sudo

ruby

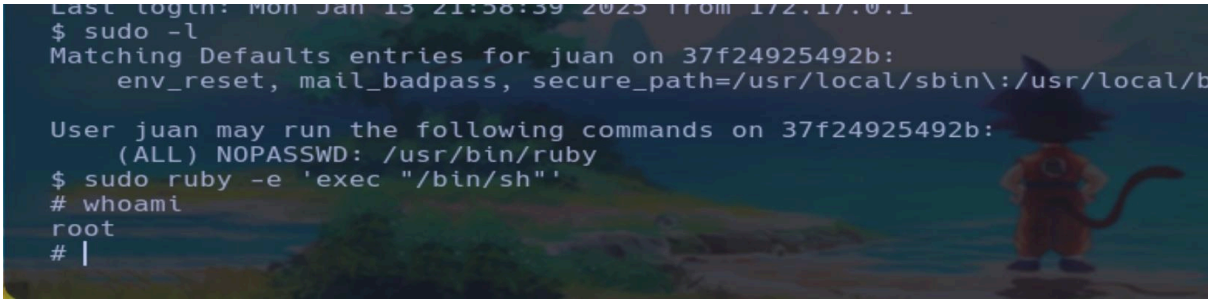
Binary	Functions
ruby	Shell, Reverse shell, File upload, File download, File write, File read, Library load, Sudo, Capabilities

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo ruby -e 'exec "/bin/sh"'
```

Ahora simplemente copiamos y pegamos el comando:sudo ruby -e 'exec "/bin/sh"'



Y ya somos usuario root.