Captura de pantalla de un celular con texto e imagen

Descripción generada automáticamente

We start deploying the machine:

Una captura de pantalla de un celular con texto e imagen

Descripción generada automáticamente con confianza media

After we deploy the machine, we proceed with a ping to check the connection, and the scan of open ports to check for vulnerabilities.

Texto

Descripción generada automáticamente

As we can appreciate the only two open ports available are number 22, in charge of ssh service and port 80, in charge of http. Since port 80 is open, we open the browser and check the page.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

As we can see, there’s an image, so we just download it using wget.

Texto

Descripción generada automáticamente

(We know that it’s name is imagen.jpeg, using ctrl + u)

Texto

Descripción generada automáticamente

You can also click on the image and do it. But using the command line seems more professional. After we got the image, we just use exiftool.

Texto

Descripción generada automáticamente

We got an user, let’s try by brute force.

Texto

Descripción generada automáticamente

We found a password, let’s enter by the port 22, with that user and password.

Texto

Descripción generada automáticamente

We’re in, so let’s escalate privileges to be user root.

Texto

Descripción generada automáticamente