Interfaz de usuario gráfica

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

We see that there’s a word wrote that says tails. We assume that tails is a valid username so we just try to break it using brute force with hydra and the dictionary rockyou.

Texto

Descripción generada automáticamente

As we see, we are not getting an immediate response, and we will not get it because there’s a trick. As the proper name says, you’ll need to start by the tail of the dictionary to arrive to the password faster. To do that, we use

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

After checking the passwords list, we see that there exists a space in them. (To check use nano invertido.txt).

To solve this, we use Imagen que contiene objeto, medidor, pelota, reloj

Descripción generada automáticamente

which will change the spaces for a non-space there. And then we just run the brute force method but with this dictionary.

After almost no time we find the password for that username.

Texto

Descripción generada automáticamente

So, we just try to enter.

Texto

Descripción generada automáticamente

We encounter an error, but it says also how to remove it that is using the command ssh-keygen -f “/root/.ssh/known\_hosts” -R “172-17.0.2”

Texto

Descripción generada automáticamente

As we can see, we are in but as tails, so we want to escalate privileges to gain access as root.

Texto

Descripción generada automáticamente