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, Texto, Aplicación

Descripción generada automáticamente

We see that is a blank page, so we press ctrl + u to check if there’s something hidden.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

We found a message. Since in the message is saying that Juan has left a important mail to Camilo, we can assume that those two names could be valid usernames, so we try with Camilo by brute force, using hydra and rockyou dictionary.

Texto

Descripción generada automáticamente

We found the password for that username, so we just enter through the ssh.

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 not as root, so we just need to escalate privileges.

Texto

Descripción generada automáticamente

As we can see, there’s other users as Juan and Pedro, since we weren’t able to escalate using Camilo, we will check that mail that Juan sent, to see if there’s something that we can use.

Texto

Descripción generada automáticamente

We have found a password for Juan here, so let’s try with that user.

Texto

Descripción generada automáticamente

We have found that Juan can execute a binary, so we go to gtfobins on the browser to check what we can do with that binary.

Imagen que contiene Diagrama

Descripción generada automáticamente

As we can execute sudo, we can escalate to be user root with this bin.

Texto

Descripción generada automáticamente con confianza media

We execute the command, and as we can see, we escalated privileges to user root.

