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 three open ports available are number 21, in charge of file transfer protocol, number 22, in charge of ssh service and port 80, in charge of http. Let’s get more information about those ports.

Texto

Descripción generada automáticamente

With this information, we can see that there’s a website in port 80, let’s look.

Interfaz de usuario gráfica

Descripción generada automáticamente

We saw a fitness web, in which one guy is promoting his services. If we take a close look at the page, there’s a form and contact information.

Texto

Descripción generada automáticamente

We can start thinking about how to upload a file that will let us enter or maybe about an injection SQL if there’s a login page, or even try to make a brute force attack with the contact information. But let’s keep looking at it, in this case pressing ctrl + u.



We found this message, that it’s a hint, saying that he’s using the same username for everything. So let’s try with the brute force.

Texto

Descripción generada automáticamente

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

Texto

Descripción generada automáticamente

We found an error, but in the same error, we have how to solve it, let’s solve it and try again.

Texto

Descripción generada automáticamente

We’re in, so let’s escalate privileges.



After we find that russoski can execute that binary as root, we go to GTFObins to check what we can do.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

We just execute what says in the page, and we’re root.

Un conjunto de letras blancas en un fondo blanco

Descripción generada automáticamente con confianza media