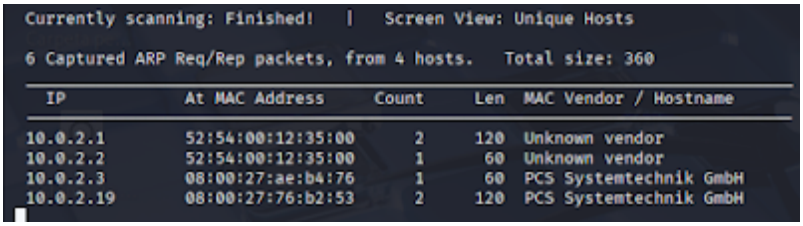
Máquina Build (Vulnyx)

De Ignacio Millán Ledesma Publicado el: 04 octubre

Comenzamos con averiguar la dirección IP de la Máquina Victima, para ello primeramente utilizaremos la herramienta **netdiscover**, para ello ejecutamos el siguiente comando:

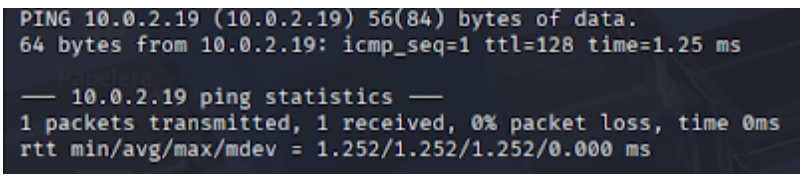
$ netdiscover -i eth1 -r 10.0.2.0/24



- **Kali (Máquina Atacante):** 10.0.2.4
- **Máquina Victima:** 10.0.2.19

Comprobamos si tenemos conexión con la Máquina Victima, para ello ejecutamos el siguiente comando:

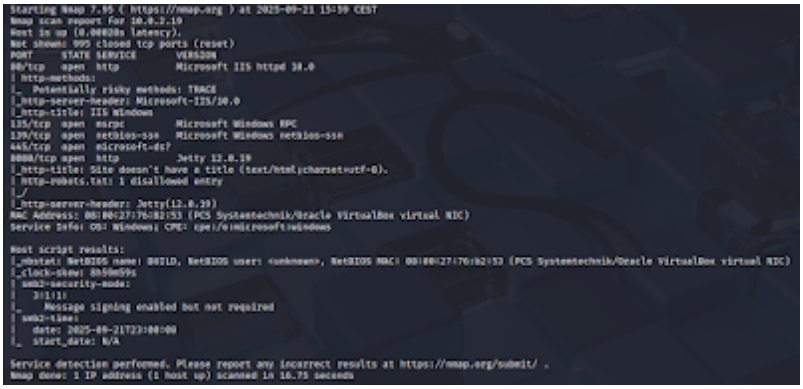
$ ping -c 1 10.0.2.19



Como se puede comprobar por el TTL nos enfrentamos a una Máquina **Windows**.

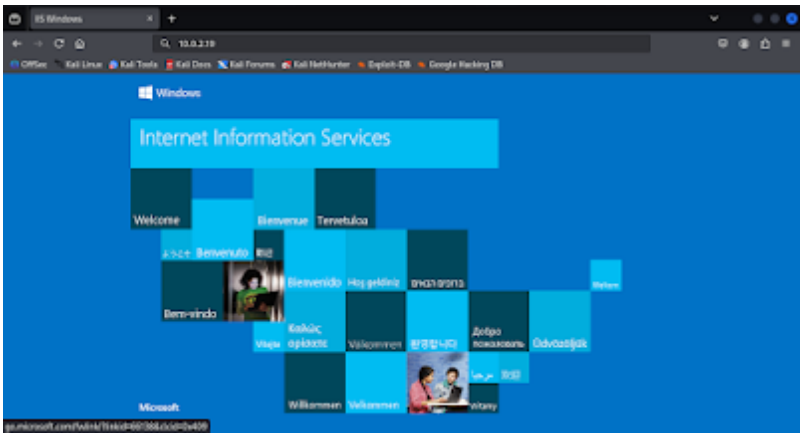
A continuación, realizamos con la herramienta **nmap** un reconocimiento de los servicios, para ello ejecutamos el siguiente comando:

$ nmap -Pn 10.0.2.19 -sVC



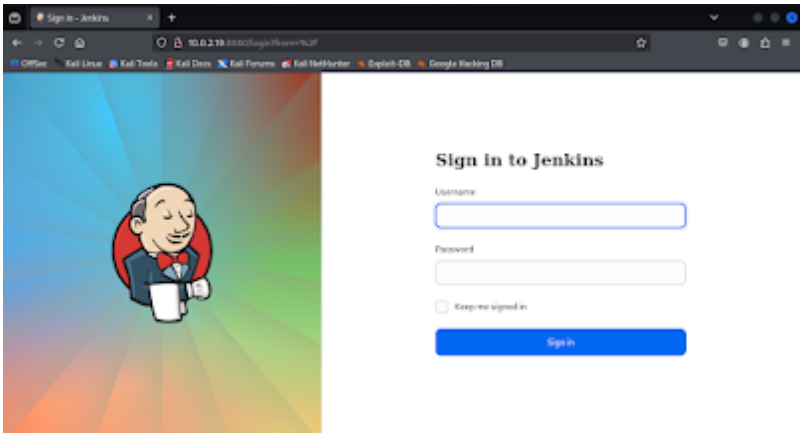
Como podemos comprobar la Máquina Victima tiene abiertos los puertos **80**, **135**, **139**, **445** y **8080**.

Comprobamos que es lo que corre por el puerto 80.



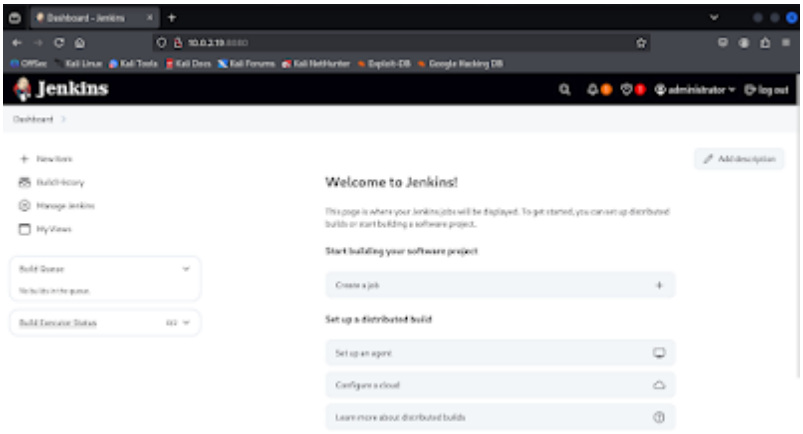
Nos encontramos con la pagina por defecto del servicio **IIS**, si realizamos con la herramienta **gobuster** un fuzzing web, no encontramos nada.

Comprobamos que es lo que corre por el puerto 8080.

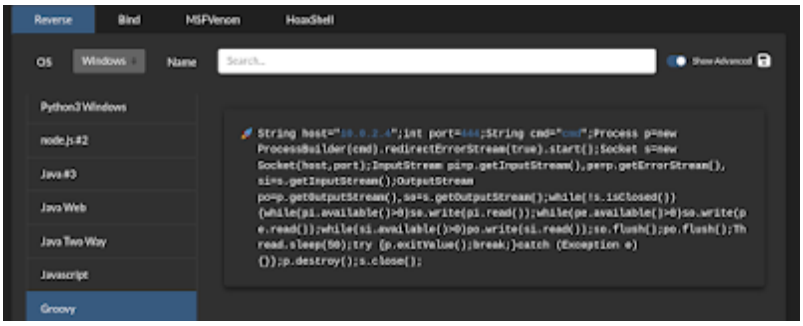


Nos encontramos con un panel de login de un **Jenkins**.

Probamos diferentes contraseñas por defecto, siendo posible acceder con las credenciales **admin:admin**.

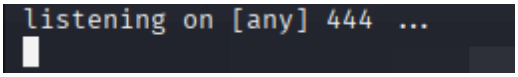


Investigando un poco en hacktricks cloud nos encontramos con que podemos obtener **RCE** ejecutando un *script* en **Groovy**, siendo este más sigiloso que crear un nuevo proyecto, por lo tanto, nos creamos una reverse shell en Groovy.

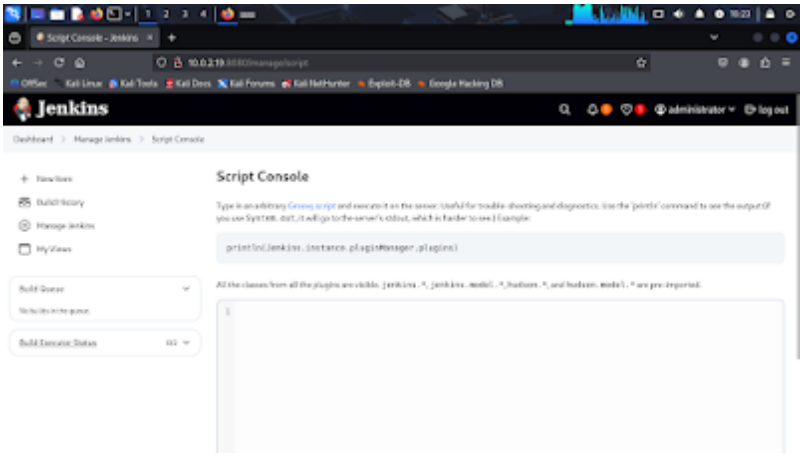


En nuestra Máquina Atacante con la ayuda de la herramienta **netcat** (**nc**) nos ponemos a la escucha por el puerto **444** por donde vamos a recibir la conexión, para ello ejecutamos el siguiente comando:

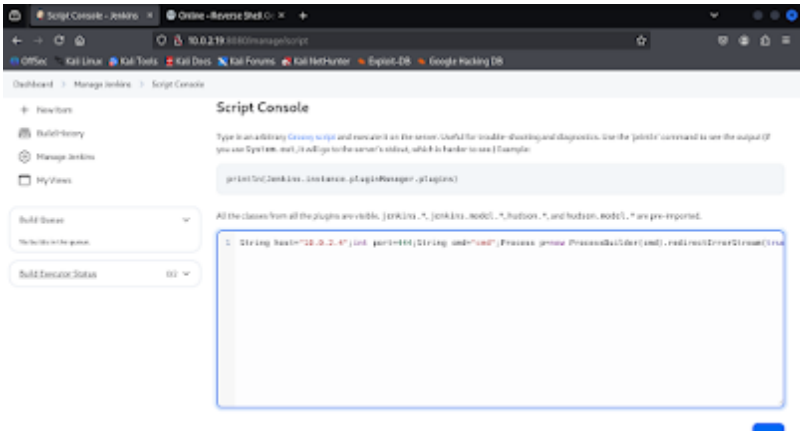
$ nc -lvnp 444



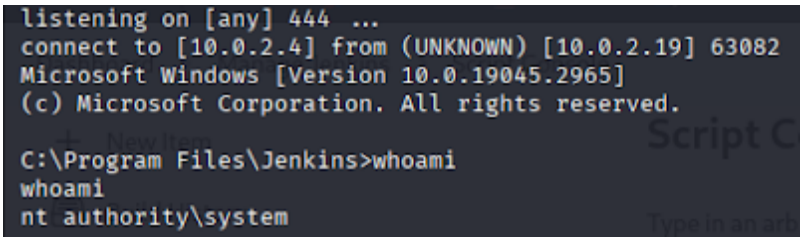
En el Jenkins nos dirigimos a *Manage Jenkins* > *Script Console*.



Pegamos nuestra reverse shell y pulsamos *Run*.



Y recibimos la conexión como ¡¡¡**Administrador**!!!.



También pudiendo leer las flags de **user** y **root**.