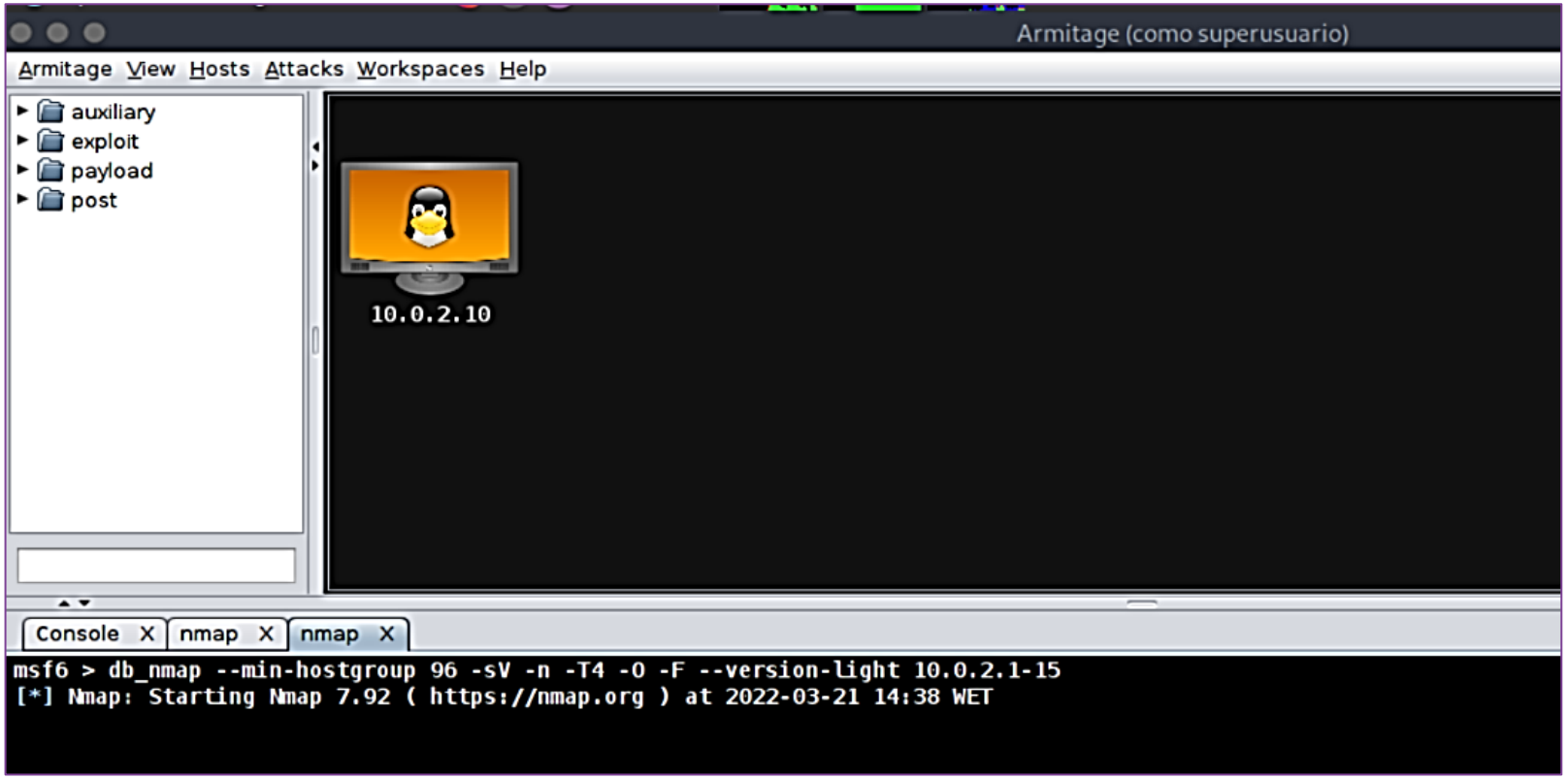
Actividad 01. Uso de Armitage

Armitage es una herramienta gráfica de gestión de ataques cibernéticos para el Proyecto **Metasploit** que visualiza objetivos y recomienda exploits . Es la forma de ejecutar los exploit de **Metaslploit** de una forma gráfica y sencilla.



En el siguiente artículo se habla sobre la herramienta Armitage:

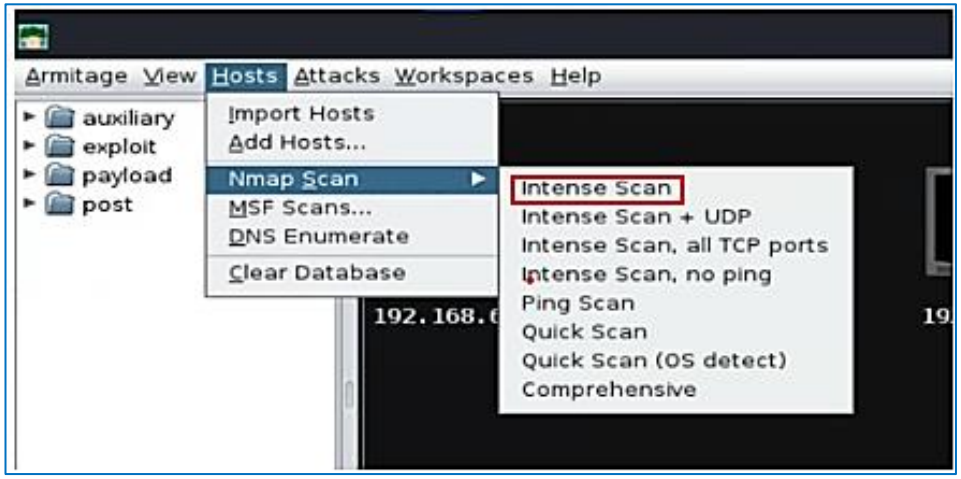
[Manual de Armitage en Español]

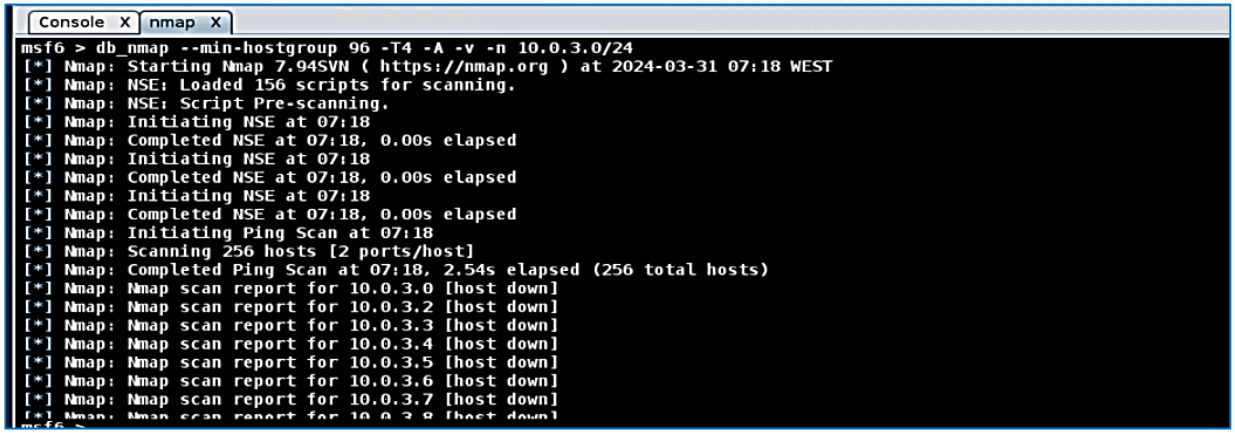
1. Instalamos Armitage

```
sudo apt install armitage
```

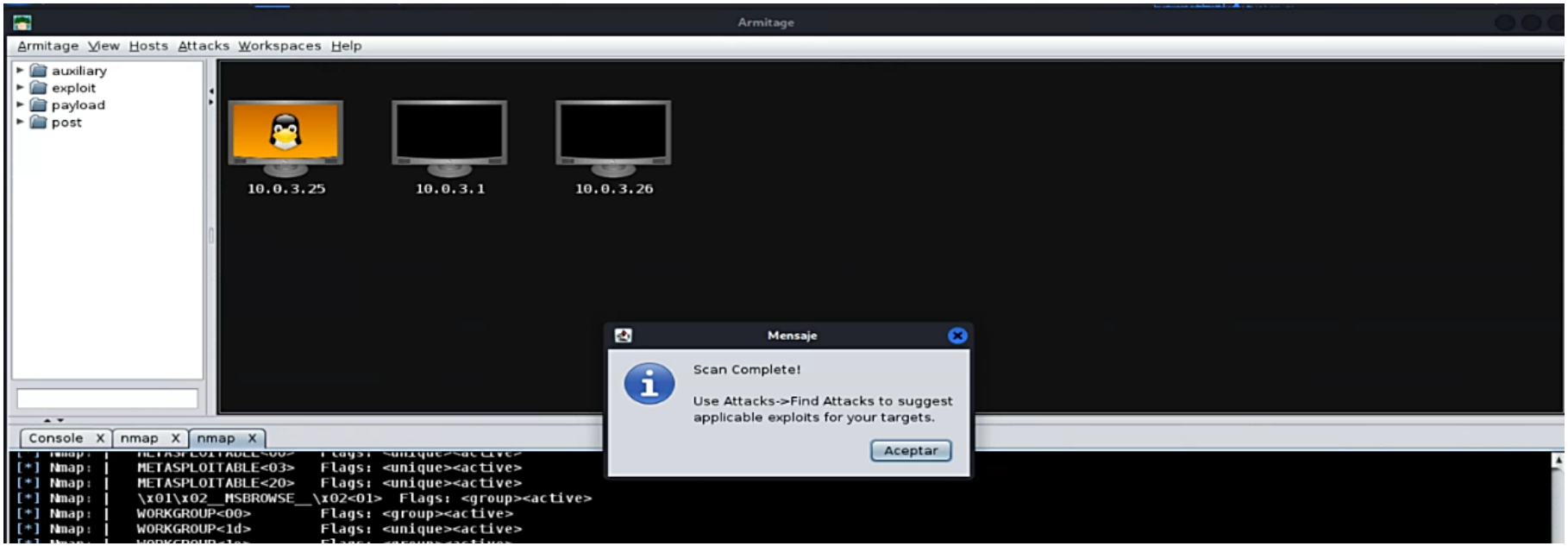
Si falla Armitage, seguimos los siguientes pasos:
Desinstalamos Postgresql
`sudo apt purge postgresql`
Volvemos a instalarlo
`sudo apt install postgresql-contrib`
Volvemos a instalarl Armitage
`sudo apt install armitage`
Habilitamos e iniciamos el servicio postgresql
`sudo systemctl enable postgresql --now`
Habilitamos e iniciamos el servicio postgresql
`sudo systemctl status postgresql`
Reiniciamos la base de datos de Metasploit
`sudo msfdb reinit`
Ejecutamos Armitage
`armitage`

2. Explorar la red
    1. Una vez cargado **Armitage**, ejecutar escaneo de la red con **Nmap**:

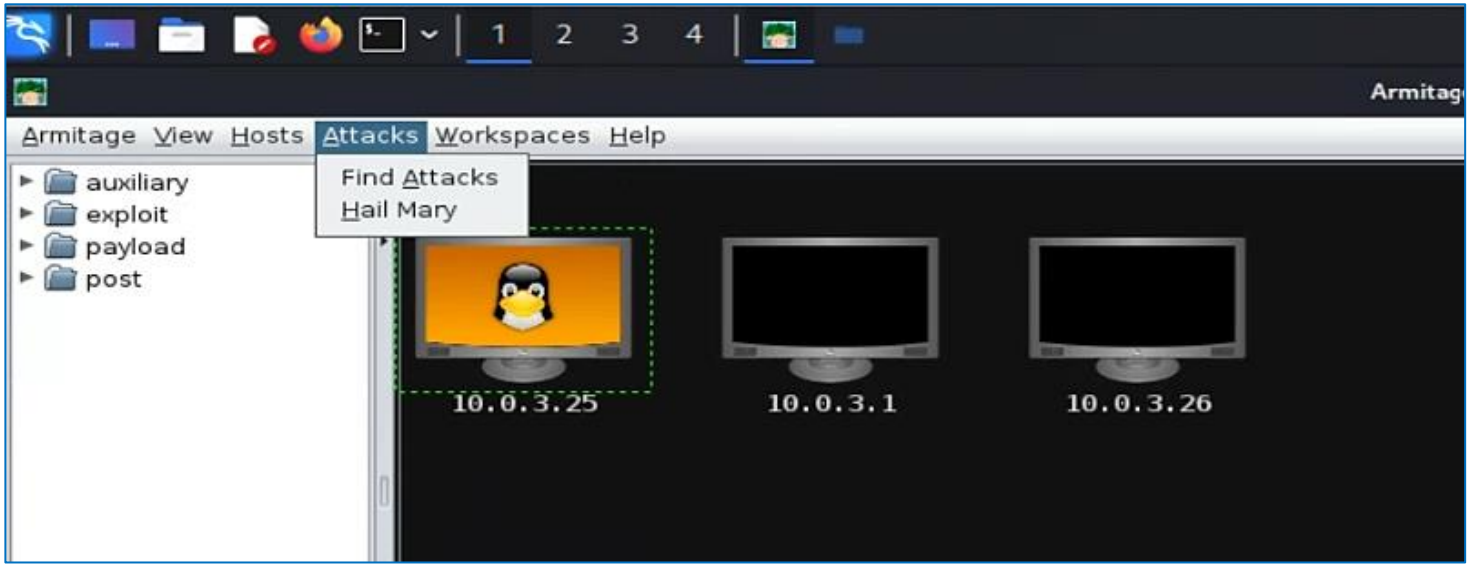




Al finalizar, mostrará los equipos encontrados:



3. Vamos a buscar vulnerabilidades en la máquina **metasploitable2**.
    i. Seleccionamos la máquina y seleccionamos la opción **Find Attacks**:



ii. Seleccionamos el **exploit**

Seleccionamos **exploit/multi/samba/usermap_script**

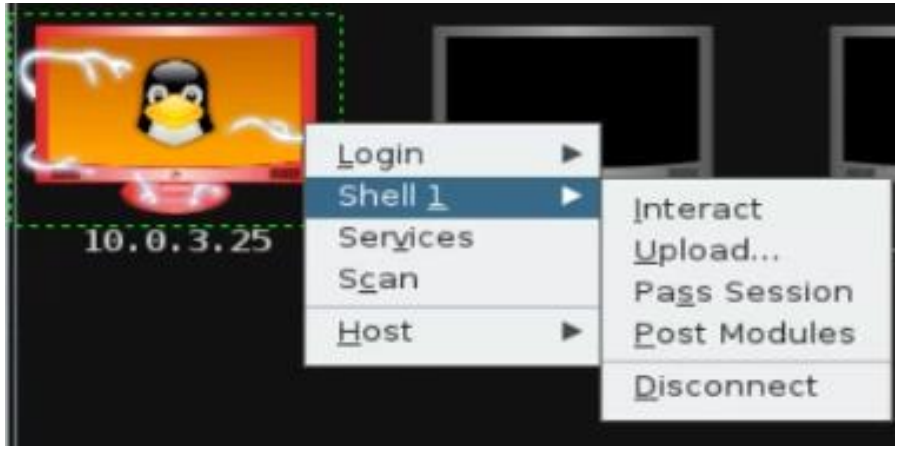
Hacemos doble clic y aparecen los valore por defecto del exploit

iii. Lanzamos el **exploit**

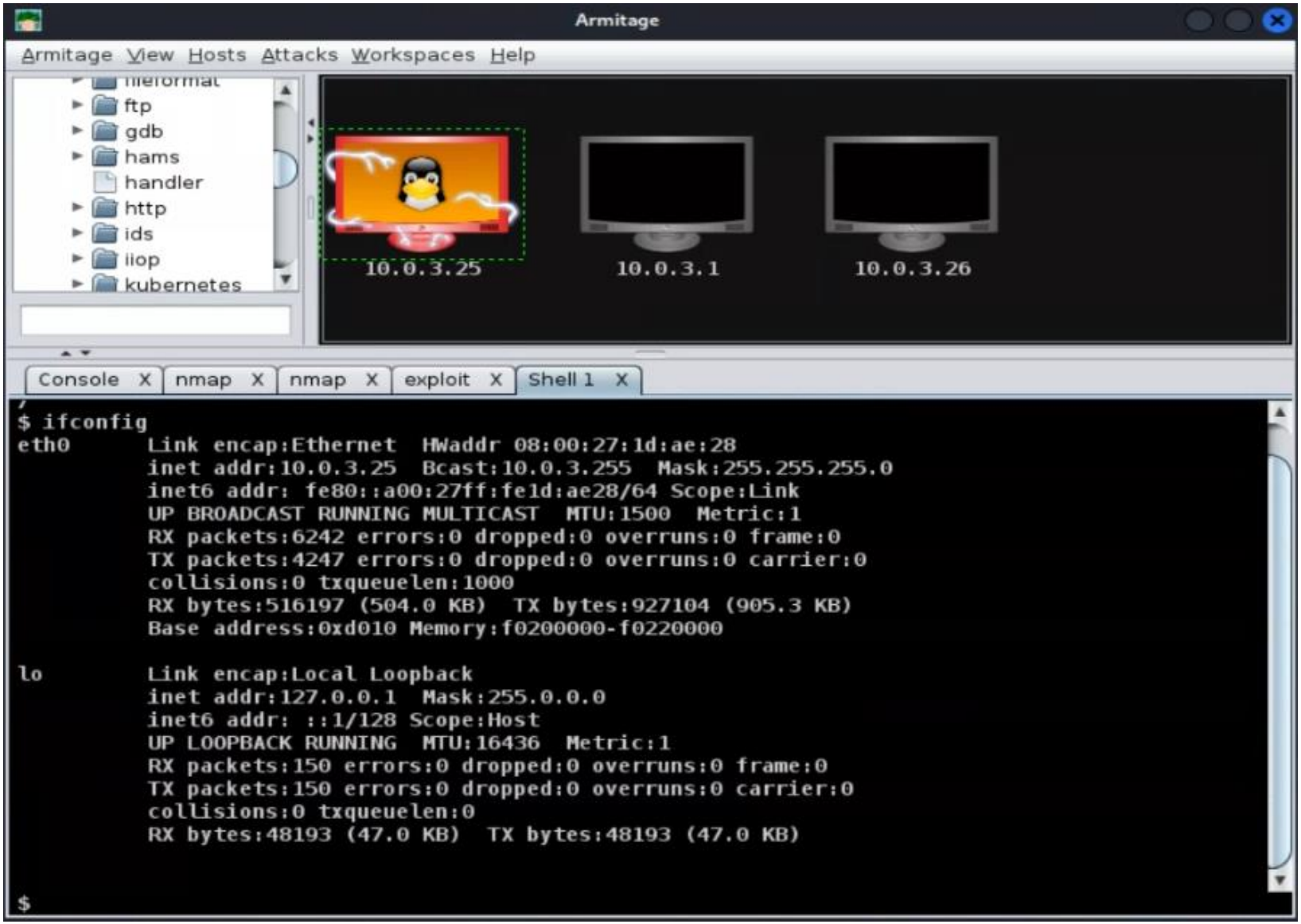
Hacemos clic en **launch**

La máquina ha sido vulnerada:

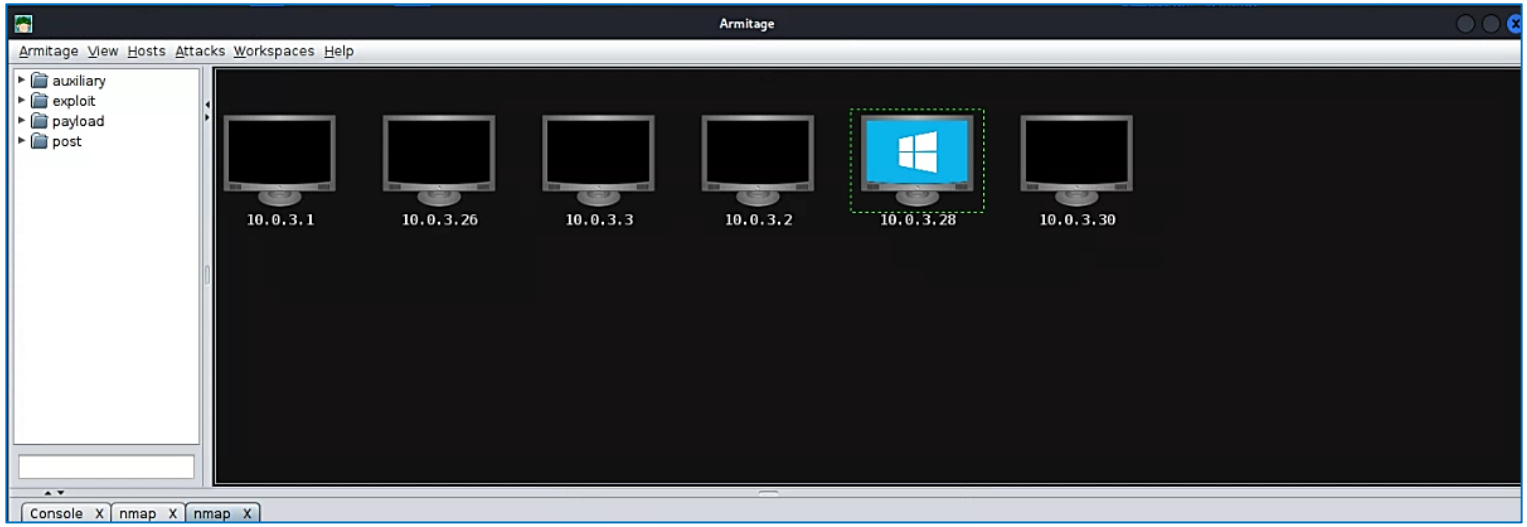
Pulsamos **shell/interact**



Y podemos interactuar con la máquina:



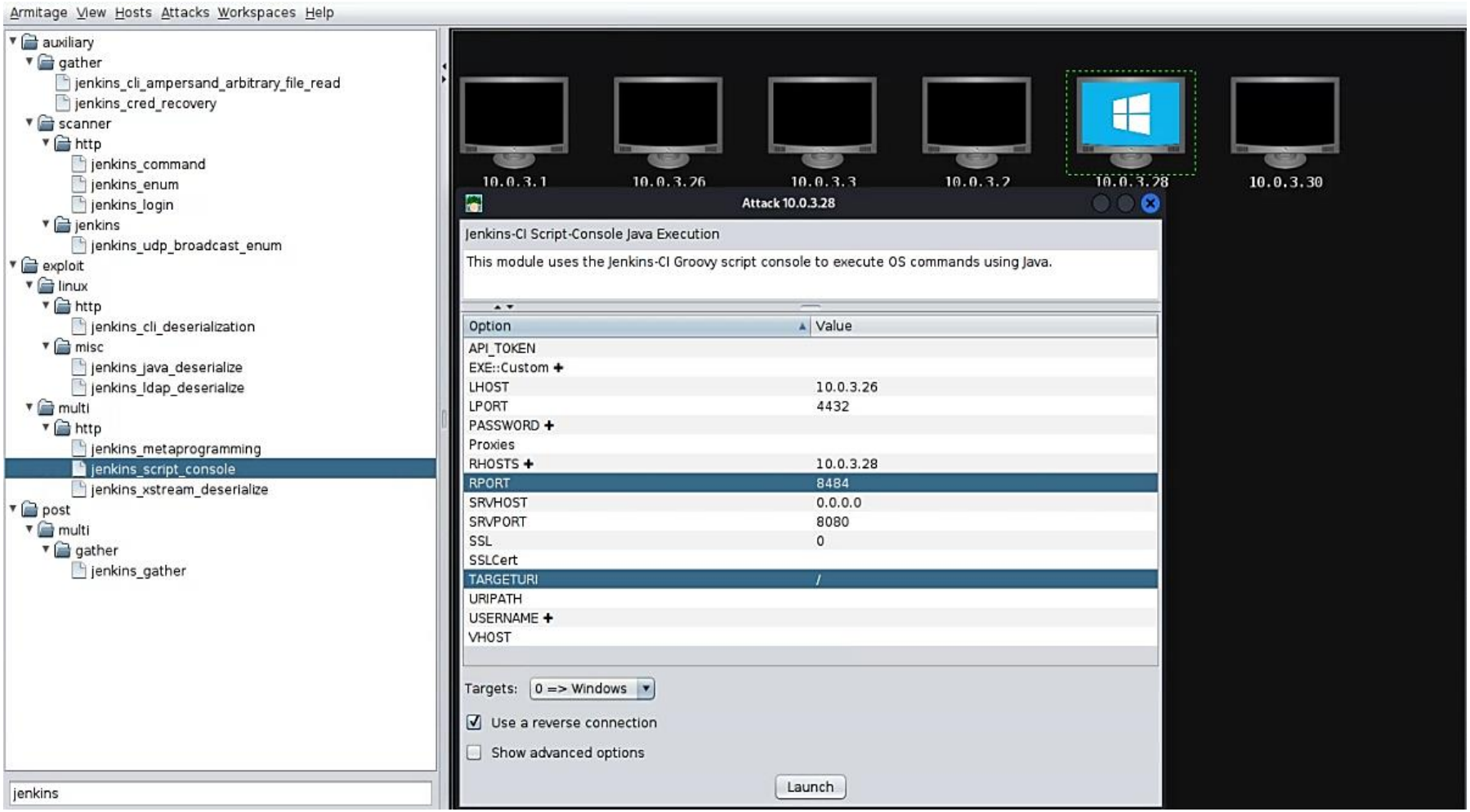
4. Vamos a buscar vulnerabilidades en la máquina **metasploitable3 WINDOWS**
    i. Seleccionamos la máquina y seleccionamos la opción **Find Attacks**:



ii. Seleccionamos el **exploit**

Seleccionamos **exploit/multi/http/jenkins_script_console**

Hacemos doble clic y aparecen los valore por defecto del exploit. Ponemos los correctos

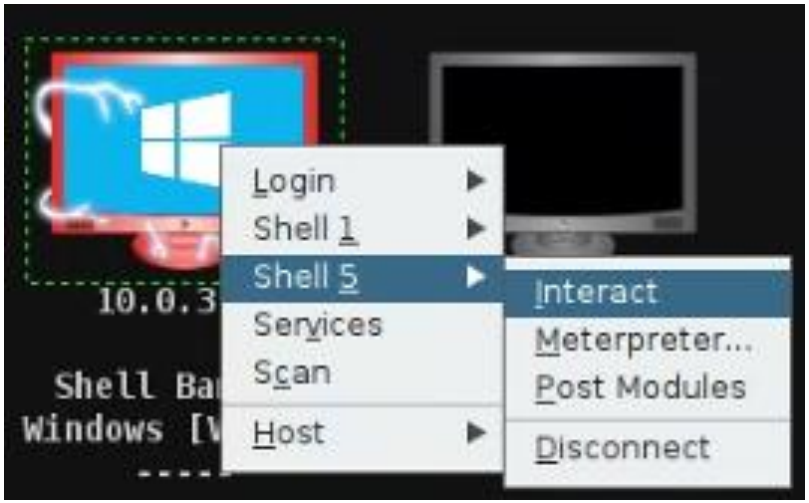


iii. Lanzamos el **exploit**

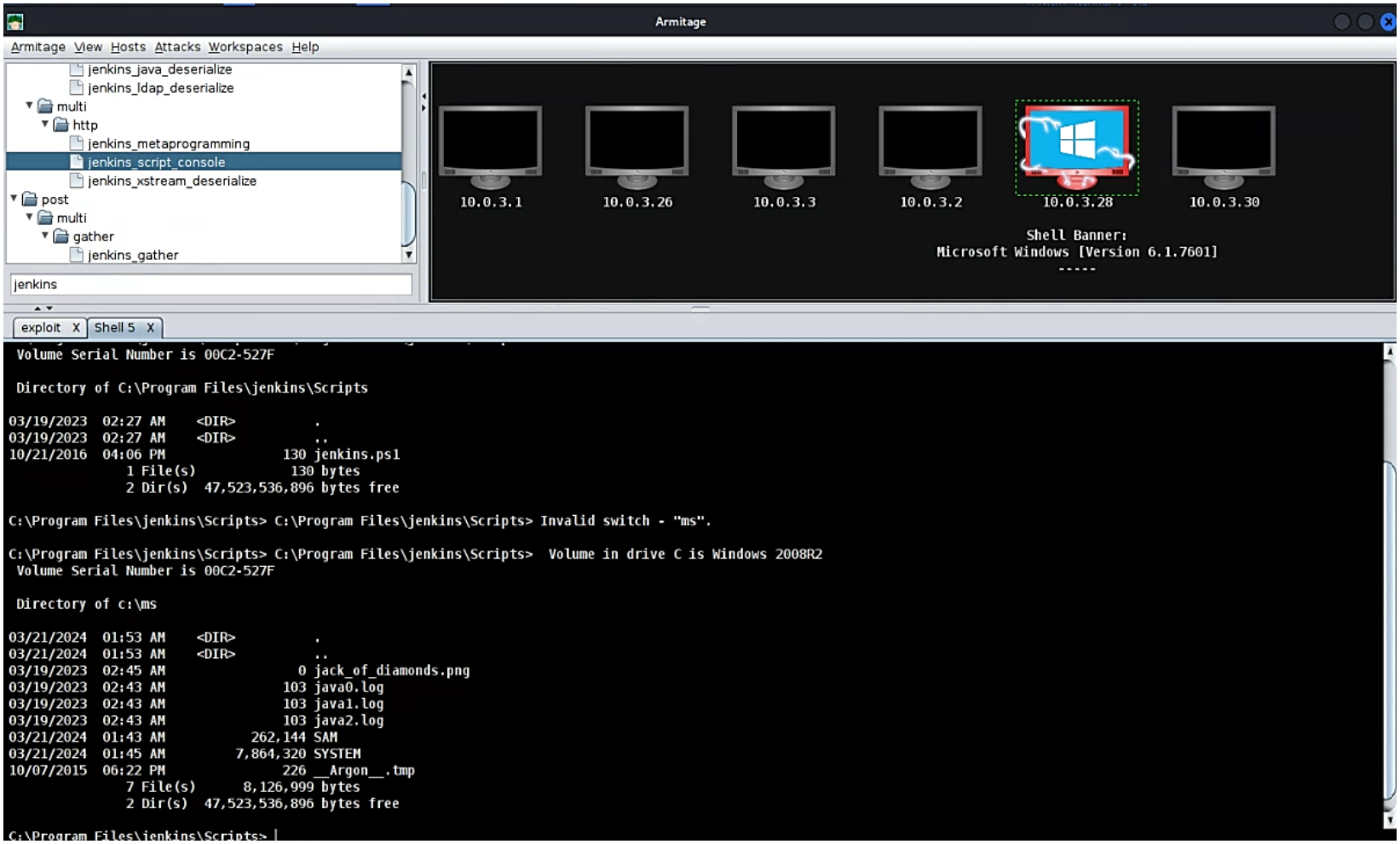
Hacemos clic en **launch**

La máquina ha sido vulnerada:

Pulsamos **Shell 1/interact**



Y podemos interactuar con la máquina:



Se pide:

Realiza la actividad y sube una memoria con capturas de pantallas y explicación de las actividades realizadas.