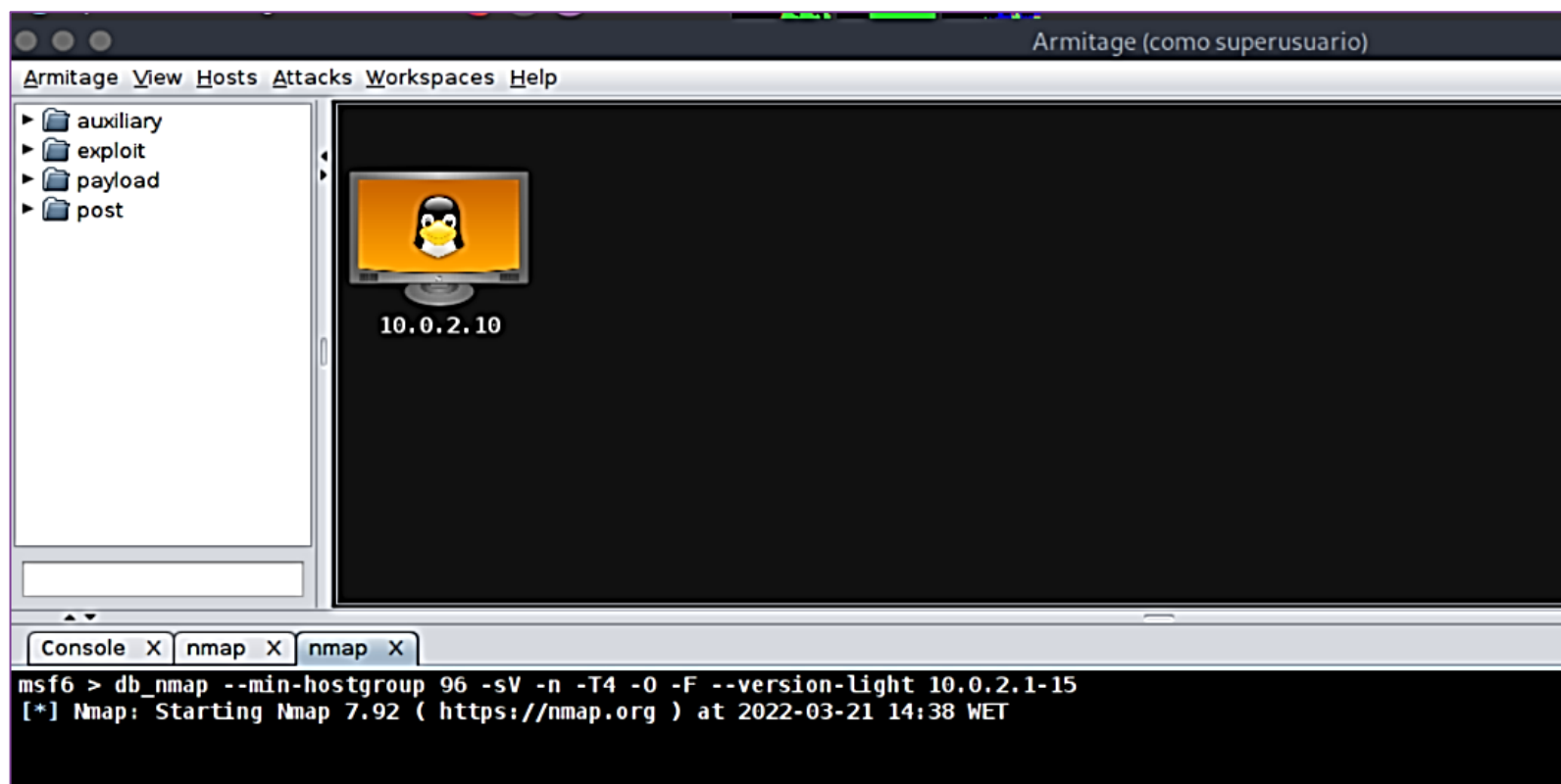


Actividad 01. Uso de Armitage

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 **Metasploit** 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 instalar 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

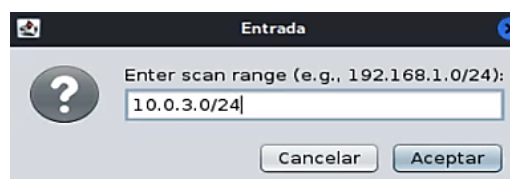
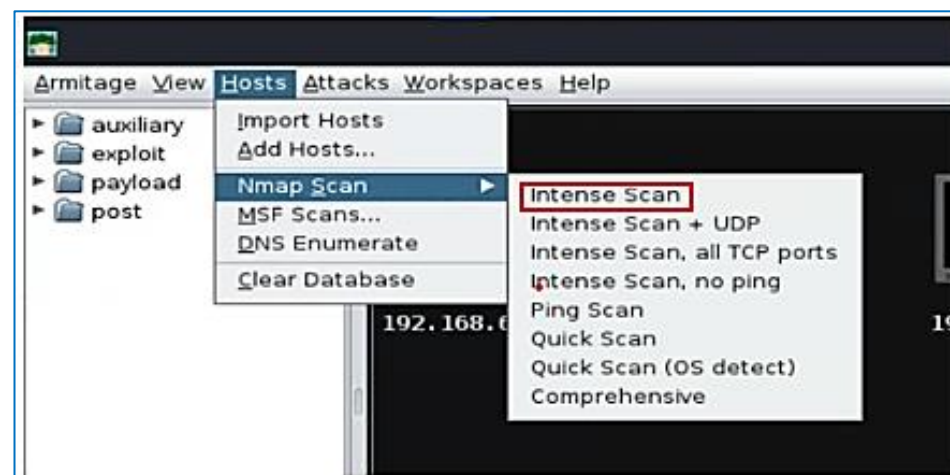
```
sudo msfdb reinit
```

Ejecutamos Armitage

```
armitage
```

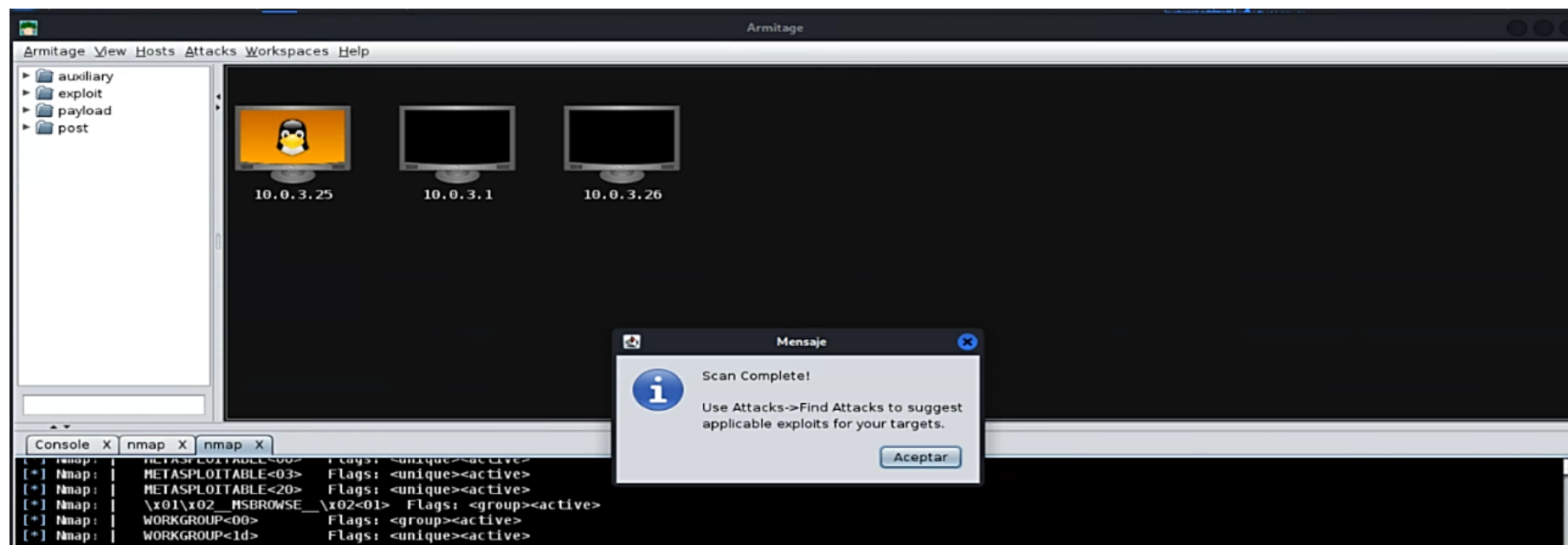
2. Explorar la red

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

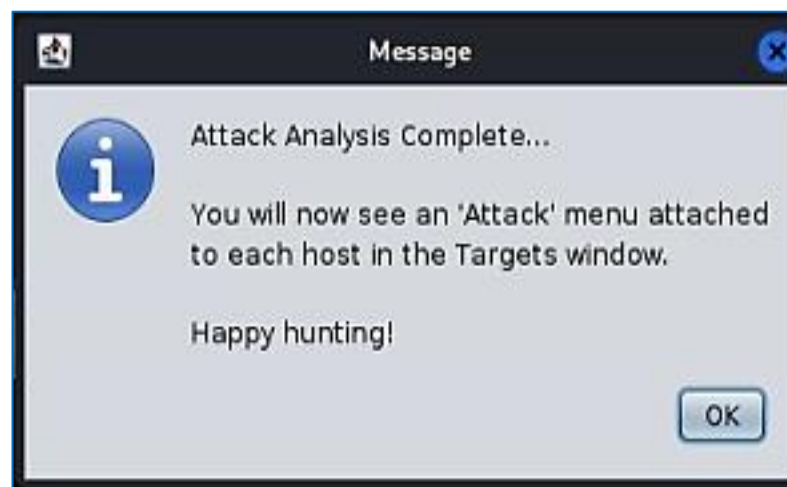
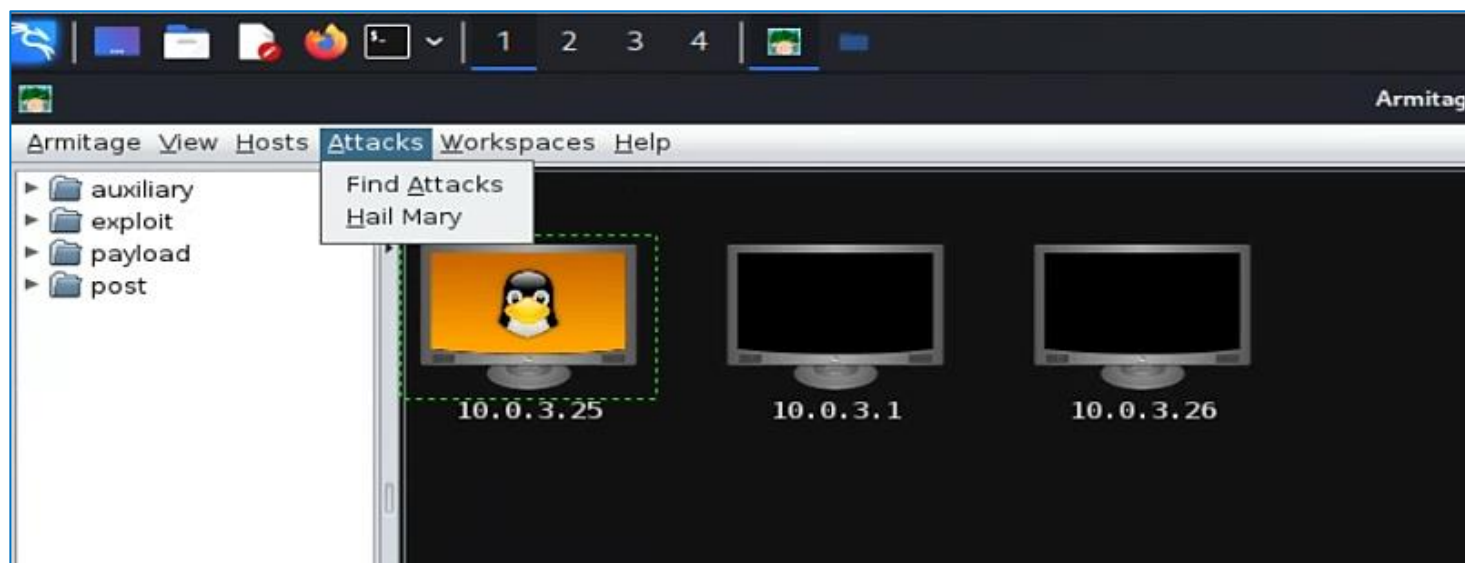


```
msf6 > db nmap --min-hostgroup 96 -T4 -A -v -n 10.0.3.0/24
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-31 07:18 WEST
[*] Nmap: NSE: Loaded 156 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: Initiating NSE at 07:18
[*] Nmap: Completed NSE at 07:18, 0.00s elapsed
[*] Nmap: Initiating NSE at 07:18
[*] Nmap: Completed NSE at 07:18, 0.00s elapsed
[*] Nmap: Initiating NSE at 07:18
[*] Nmap: Completed NSE at 07:18, 0.00s elapsed
[*] Nmap: Initiating Ping Scan at 07:18
[*] Nmap: Scanning 256 hosts [2 ports/host]
[*] Nmap: Completed Ping Scan at 07:18, 2.54s elapsed (256 total hosts)
[*] Nmap: Nmap scan report for 10.0.3.0 [host down]
[*] Nmap: Nmap scan report for 10.0.3.2 [host down]
[*] Nmap: Nmap scan report for 10.0.3.3 [host down]
[*] Nmap: Nmap scan report for 10.0.3.4 [host down]
[*] Nmap: Nmap scan report for 10.0.3.5 [host down]
[*] Nmap: Nmap scan report for 10.0.3.6 [host down]
[*] Nmap: Nmap scan report for 10.0.3.7 [host down]
[*] Nmap: Nmap scan report for 10.0.3.8 [host down]
```

Al finalizar, mostrará los equipos encontrados:



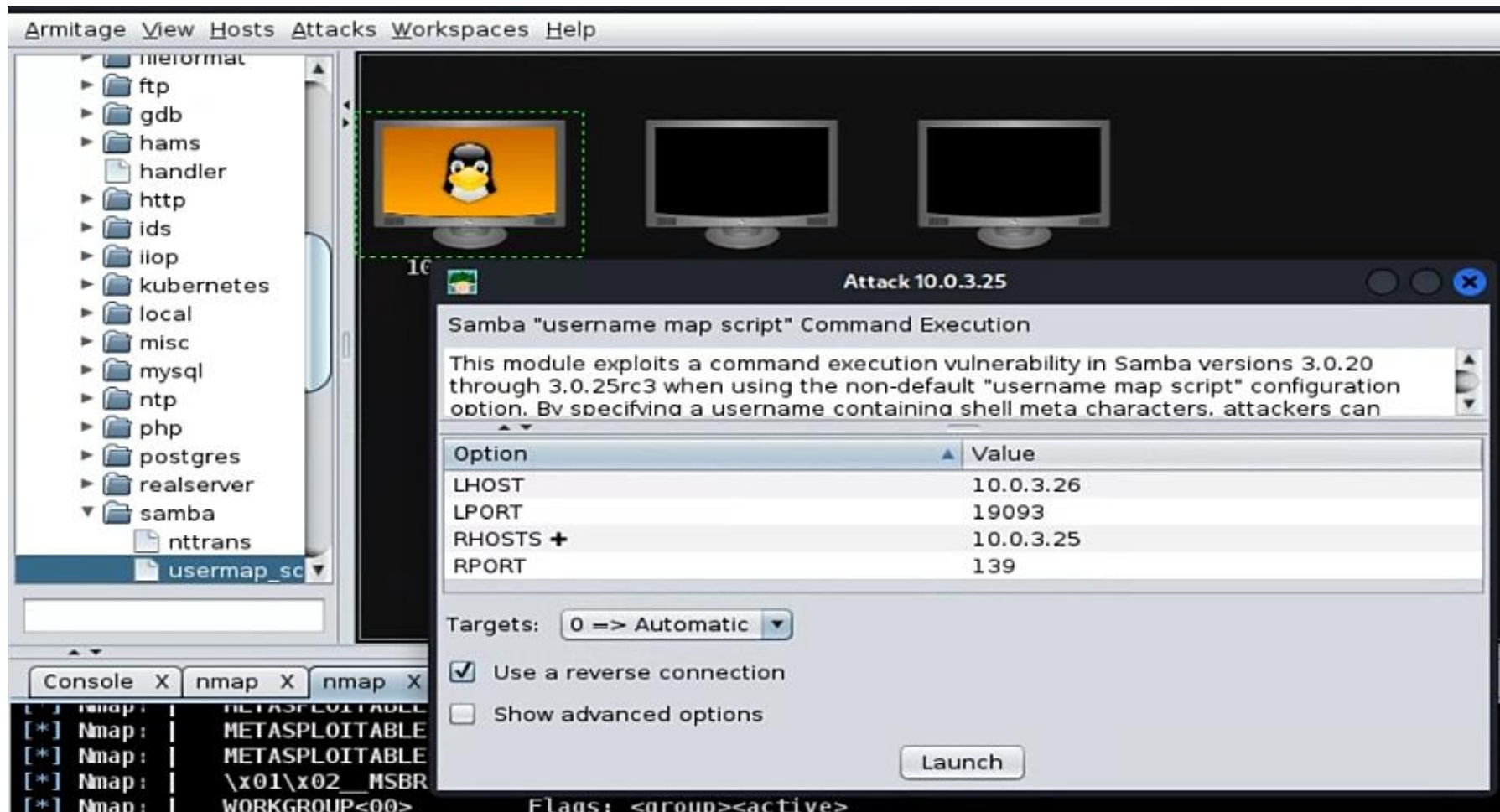
3. Vamos a buscar vulnerabilidades en la máquina **metasploitable2**.
- i. Seleccionamos la máquina y seleccionamos la opción **Find Attacks**:



ii. Seleccionamos el **exploit**

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

Hacemos doble clic y aparecen los valores por defecto del exploit



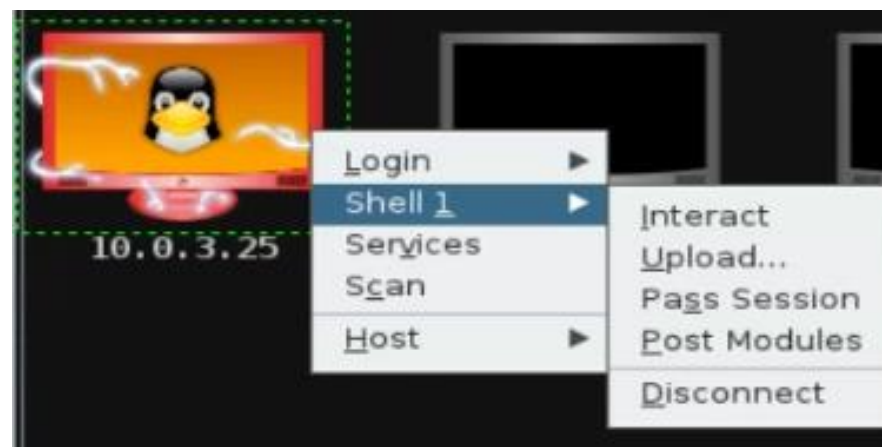
iii. Lanzamos el **exploit**

Hacemos clic en **launch**

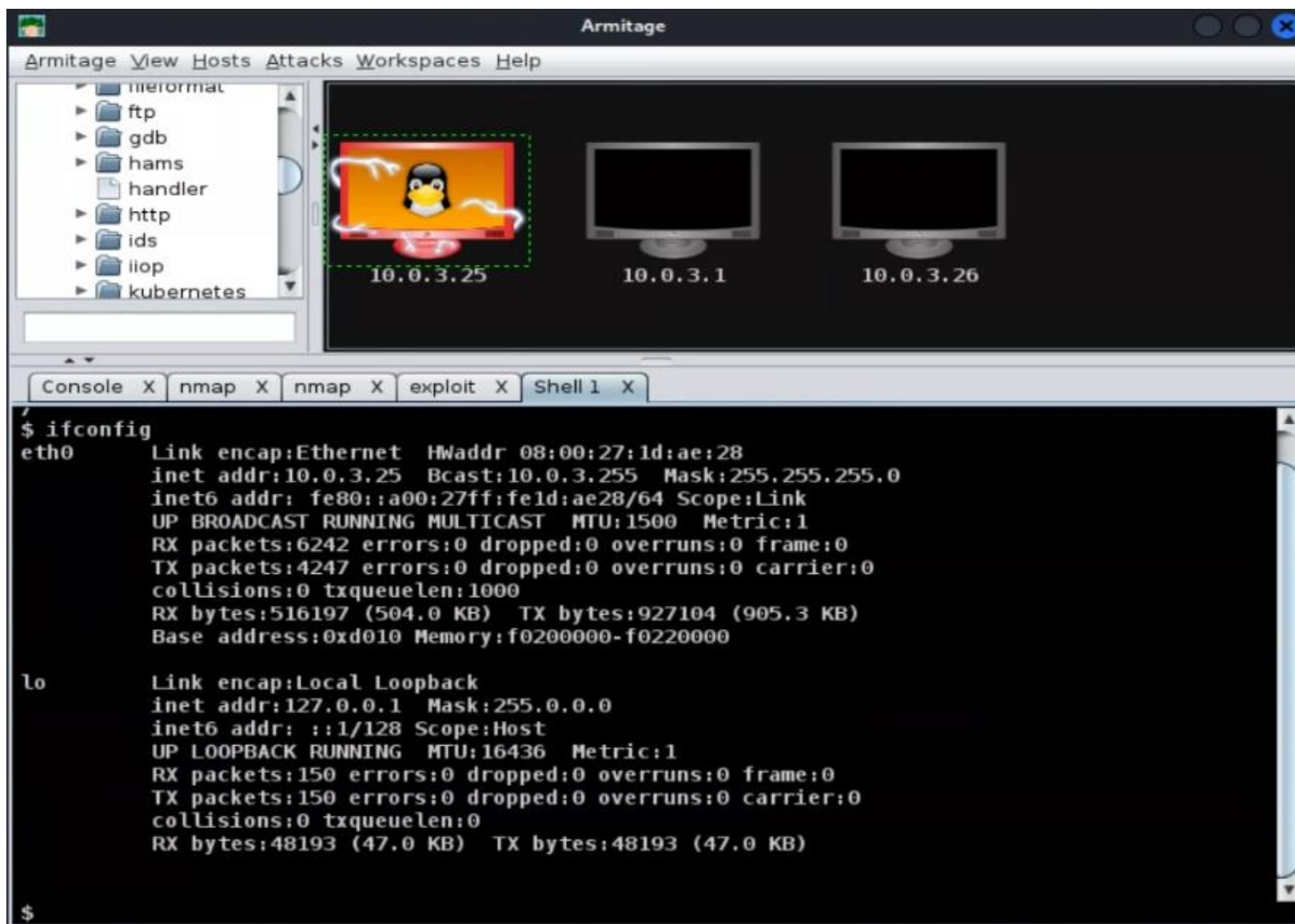
La máquina ha sido vulnerada:



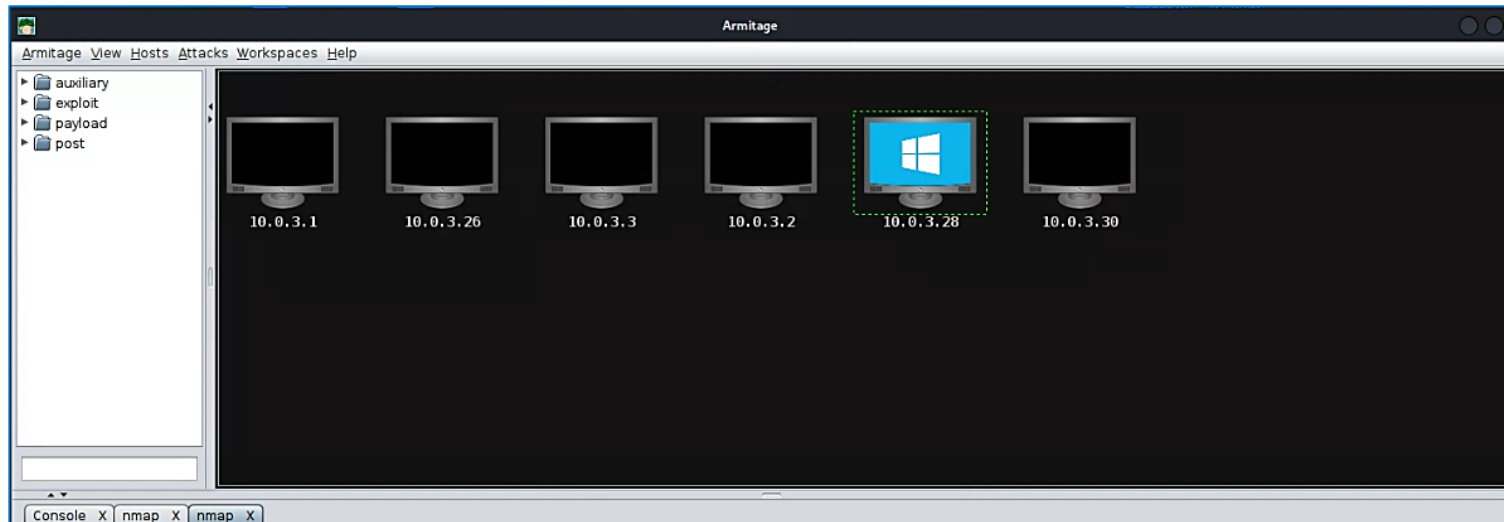
Pulsamos **shell/interact**



Y podemos interactuar con la máquina:



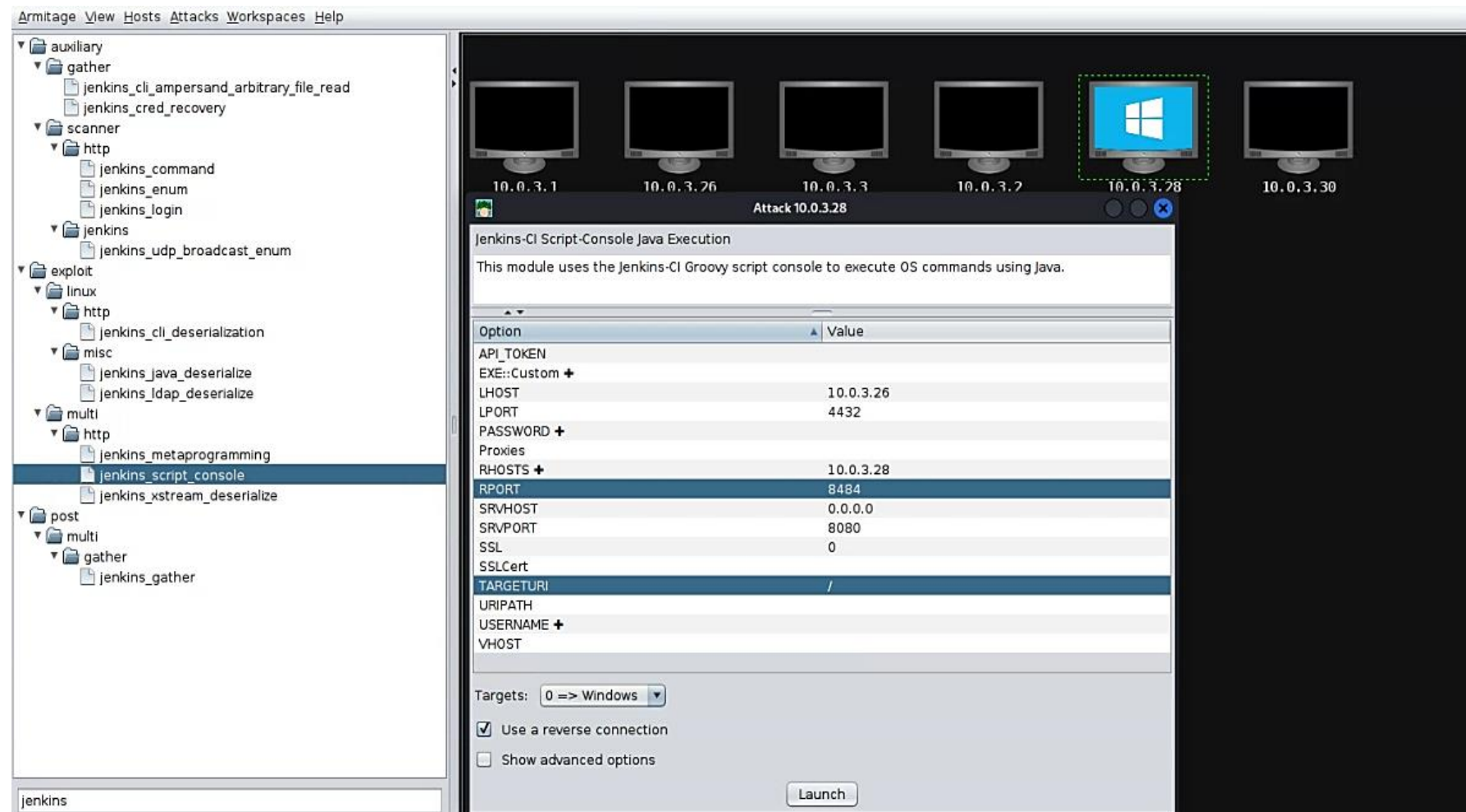
4. Vamos a buscar vulnerabilidades en la máquina **metasploitable3 WINDOWS**
- i. Seleccionamos la máquina y seleccionamos la opción **Find Attacks**:



ii. Seleccionamos el **exploit**

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

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



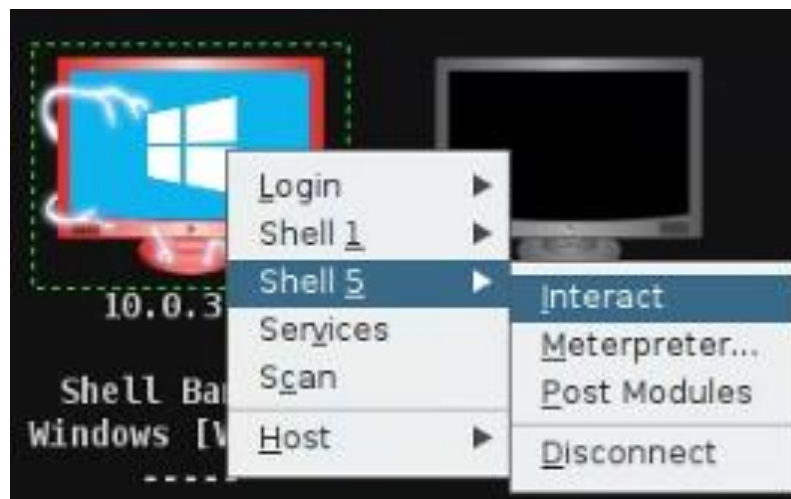
iii. Lanzamos el **exploit**

Hacemos clic en **launch**

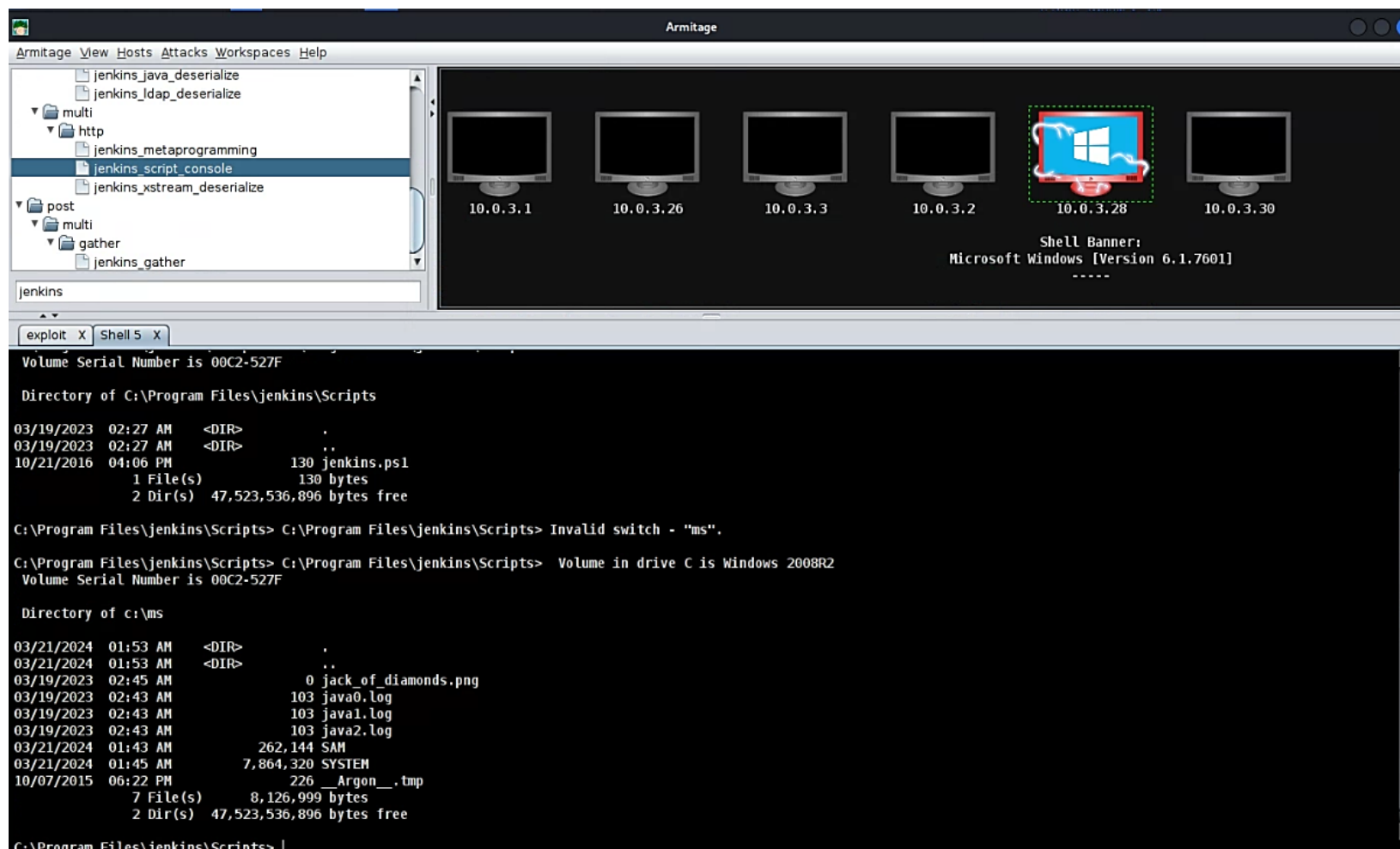
La máquina ha sido vulnerada:



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.