# [Intrusión Extra] Metasploit para dummies

Para arrancar metasploit usamos el comando:

```
msfconsole
```

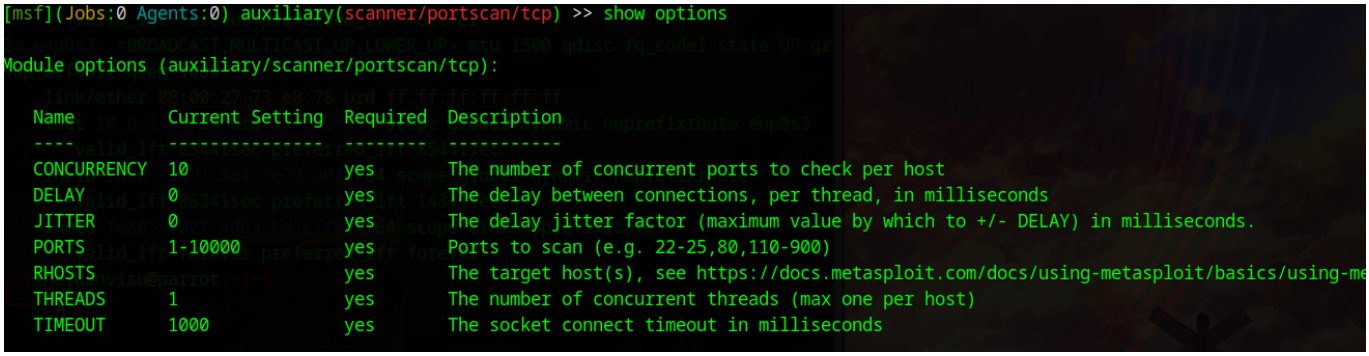
## Escaneo de puertos

Para escanear los puertos de una máquina a la que llamaremos RHOST debemos cargar primero el módulo de escaneo con el siguiente comando:

```
use auxiliary/scanner/portscan/tcp
```

Una vez cargamos el módulo podemos ver que opciones hay disponibles para su configuración con el comando:

```
show options
```



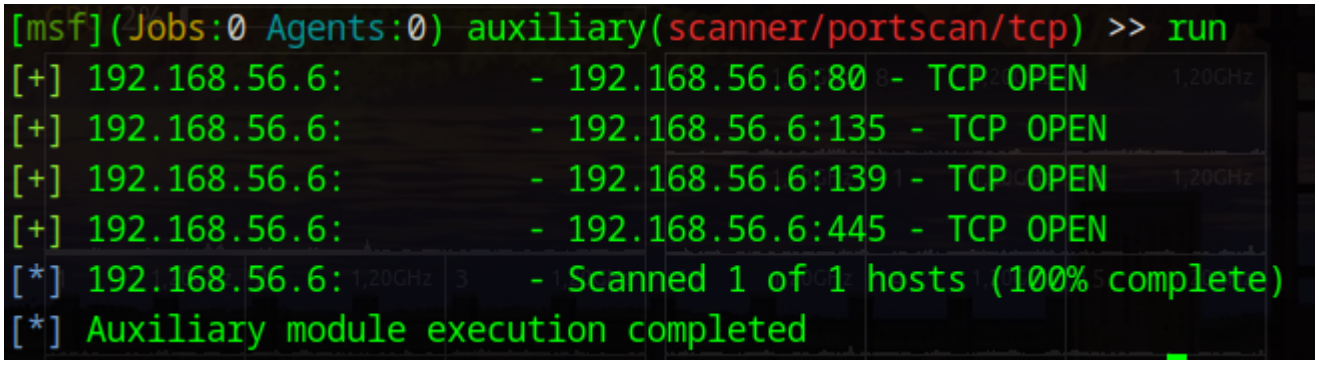

Como se puede obervar la ip de la máquina que se va a escanear está vacía, por lo que la establecemos con el siguiente comando:

```
set RHOSTS <IP del objetivo>
```

Finalmente podemos ejecutar el escaneo de puertos con el comando:

```
run
```

Tras la ejecución del módulo se pueden ver los puertos abiertos que se van localizando:




## Escaneo en profundidad de los puertos abiertos

Ahora que sabemos que puertos están abiertos, procedemos a realizar un escaneo en profundidad de estos para ver que servicios tienen corriendo dentro con el comando:

```
db_nmap -sV -p <puerto1,puerto2, ... ,puerto3> <IP del objetivo>
```