

# [Intrusión Extra] Metasploit para dummies

Para arrancar metasploit usamos el comando:

```
msfconsole
```

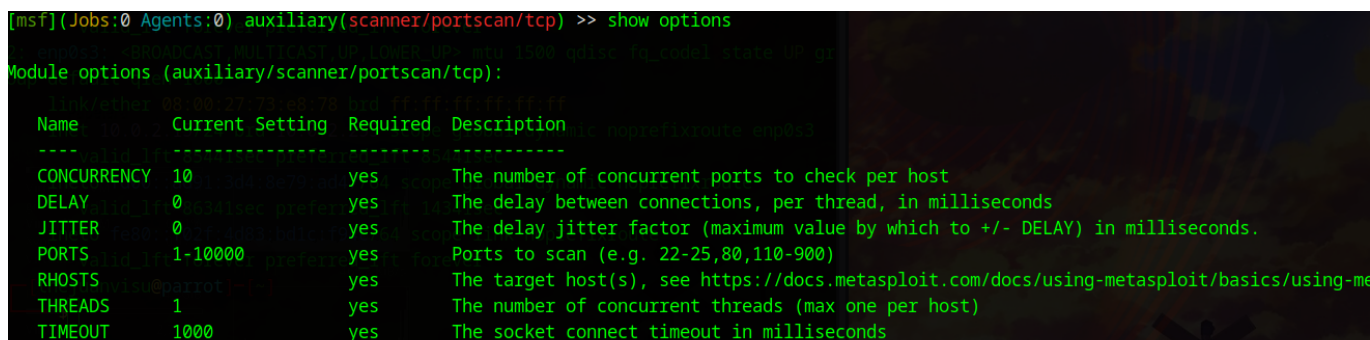
## Escaneo de puertos

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
```



```
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/tcp) >> show options
Link/Ether 00:0c:29:2a:00:20 bin FF FF FF FF FF
Module options (auxiliary/scanner/portscan/tcp):
  Name      Current Setting  Required  Description
  ----
  CONCURRENCY 10               yes       The number of concurrent ports to check per host
  DELAY       0                yes       The delay between connections, per thread, in milliseconds
  JITTER      0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
  PORTS       1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
  RHOSTS      nil              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-me
  THREADS     1                yes       The number of concurrent threads (max one per host)
  TIMEOUT     1000             yes       The socket connect timeout in milliseconds
```

Como se puede observar 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:

```
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/tcp) >> run
[+] 192.168.56.6: - 192.168.56.6:80 1- TCP OPEN 2- 2,40GHz
[+] 192.168.56.6: - 192.168.56.6:135 - TCP OPEN
[+] 192.168.56.6: 2,40GHz 3 - 192.168.56.6:139 4- TCP OPEN 2,40GHz
[+] 192.168.56.6: - 192.168.56.6:445 - TCP OPEN
```

From:

<https://www.knoppia.net/> - Knoppia

Permanent link:

[https://www.knoppia.net/doku.php?id=master\\_cs:int:ms&rev=1744206866](https://www.knoppia.net/doku.php?id=master_cs:int:ms&rev=1744206866)

Last update: **2025/04/09 13:54**

