

[Intrusión Extra] Metasploit para dummies

Para arrancar metasploit usamos el comando:

```
msfconsole
```

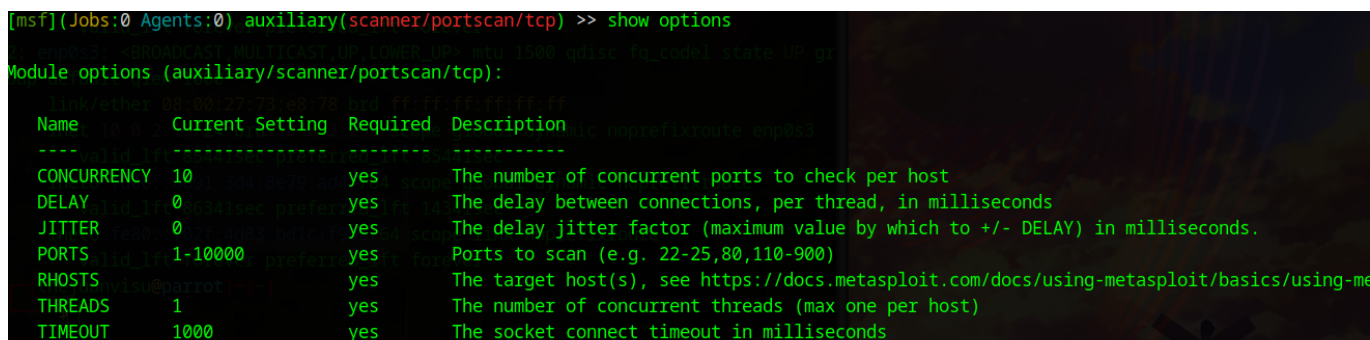
Escaneo de puertos

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:29:25:48:20 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     [unspecified]    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 - TCP OPEN
[+] 192.168.56.6: - 192.168.56.6:135 - TCP OPEN
[+] 192.168.56.6: - 192.168.56.6:139 - TCP OPEN
[+] 192.168.56.6: - 192.168.56.6:445 - TCP OPEN
[*] 192.168.56.6: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

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>
```

From:

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

Permanent link:

https://knoppia.net/doku.php?id=master_cs:int:ms&rev=1744208559

Last update: **2025/04/09 14:22**

