[Intrusión Extra] Metasploit para dummies

Para arrancar metasploit usamos el comando:

```
msfconsole
```

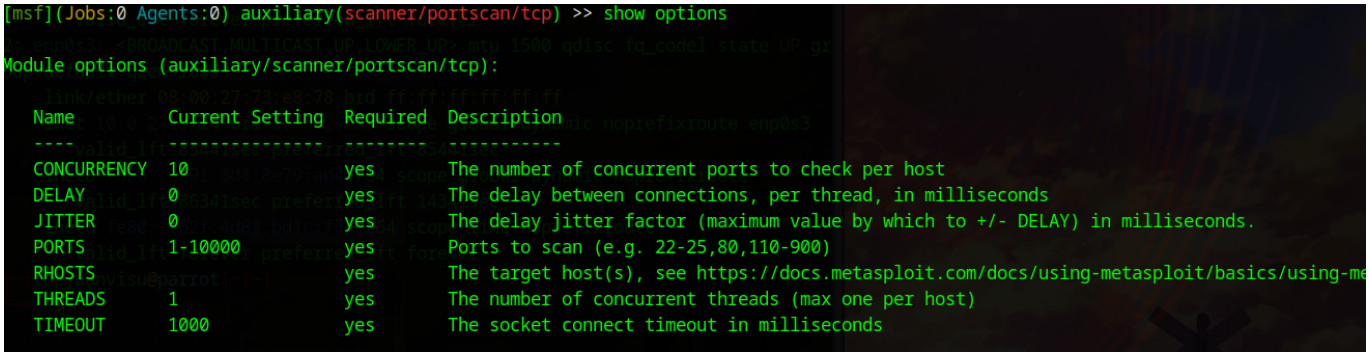
Escaneo de puertos

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:

```
[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>
```

```
[msf](Jobs:0 Agents:0) >> db_nmap -sV -P 80,135,139,445 192.168.56.6
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-09 16:33 CEST
[*] Nmap: 'Failed to resolve "80,135,139,445".'
[*] Nmap: Nmap scan report for 192.168.56.6
[*] Nmap: Host is up (0.0067s latency).
[*] Nmap: Not shown: 994 filtered tcp ports (no-response)
[*] Nmap: PORT     STATE SERVICE     VERSION
[*] Nmap: 80/tcp   open  http        Microsoft IIS httpd 7.5
[*] Nmap: 135/tcp  open  msrpc       Microsoft Windows RPC
[*] Nmap: 139/tcp  open  netbios-ssn Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp  open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: MUNICS)
[*] Nmap: 49154/tcp open msrpc       Microsoft Windows RPC
[*] Nmap: 49156/tcp open msrpc       Microsoft Windows RPC
[*] Nmap: Service Info: Host: META-FLAVOUR2; OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 59.75 seconds
```

NOTA: Si sale un mensaje diciendo que no se puede conectar con la base de datos ejecuta los siguientes comandos:

```
sudo msfdb reinit
sudo msfdb run
```

Y debería iniciarse una nueva instancia de mestasploit en la que funcione la base de datos.

From:
https://www.knoppia.net/ - **Knoppia**

Permanent link:
https://www.knoppia.net/doku.php?id=master_cs:int:ms&rev=1744209547

Last update: **2025/04/09 14:39**