

[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
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       RHOST            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 1.20GHz
[+] 192.168.56.6: - 192.168.56.6:135 - TCP OPEN
[+] 192.168.56.6: - 192.168.56.6:139 - TCP OPEN 1.20GHz
[+] 192.168.56.6: - 192.168.56.6:445 - TCP OPEN
[*] 192.168.56.6: 1.20GHz 3 - 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".' (192.168.56.6) indicated by SMB reply
[*] Nmap: Nmap scan report for 192.168.56.6 (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 metasploit en la que funcione la base de datos.

Escaneo de vulnerabilidades de los servicios detectados

Para realizar un escaneo de vulnerabilidades usamos el comando:

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

```
[msf](Jobs: 0 Agents: 0) >> db_nmap -sV -A -P 80,135,139,445 192.168.56.6
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-09 16:43 CEST
[*] Nmap: 'Failed to resolve "80,135,139,445".'
[*] Nmap: Nmap scan report for 192.168.56.6
[*] Nmap: Host is up (0.0058s 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: |_http-title: Site doesn't have a title.
[*] Nmap: |_http-server-header: Microsoft-IIS/7.5
[*] Nmap: |_http-methods:
[*] Nmap: |_ Potentially risky methods: TRACE
[*] Nmap: 135/tcp   open  msrpc       Microsoft Windows RPC
[*] Nmap: 139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds Windows Server 2008 R2 Enterprise 7601 Service Pack 1 microsoft-ds (workgroup: MUNICS)
[*] Nmap: 49154/tcp open  msrpc       Microsoft Windows RPC
[*] Nmap: 49156/tcp open  msrpc       Microsoft Windows RPC
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[*] Nmap: Device type: bridge|general purpose
[*] Nmap: Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (94%)
[*] Nmap: OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
[*] Nmap: Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (94%)
[*] Nmap: No exact OS matches for host (test conditions non-ideal).
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Host: META-FLAVOUR2; OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Host script results:
[*] Nmap: | smb2-time:
[*] Nmap: |   date: 2025-04-09T23:44:48
[*] Nmap: |   start_date: 2025-04-09T23:29:17
[*] Nmap: | smb-os-discovery:
[*] Nmap: |   OS: Windows Server 2008 R2 Enterprise 7601 Service Pack 1 (Windows Server 2008 R2 Enterprise 6.1)
```

From:
<http://knoppia.net/> - Knoppia

Permanent link:
http://knoppia.net/doku.php?id=master_cs:int:ms

Last update: **2025/04/09 14:49**

