2025/11/29 20:17 1/3 Metasploit para novatos

Metasploit para novatos

Estos ejemplos son para una versión de Metasploit preinstalada en sistemas kali linux.

1. Inicialización de la base de datos y primer arranque de metasploit

Para el uso de metasploit se recomienda inicializar la base de datos la primera vez que se arranque con el comando:

```
msfdb init
```

Una vez que se inicialice la base de datos, cada vez que se quiera usar metasploit se puede arrancar con el siguiente comando:

msfdb run

2. Escaneo de máquina objetivo

Lo primero que debemos hacer es escanear los puertos de la máquina objetivo para identificar que servicios tiene arrancados y si alguno de estos es vulnerable.

2.1 NMAP

Primero se puede comenzar realizando un escaneo de namp desde metasploit con el siguiente comando:

```
db_nmap <ip_maquina_objetivo>
```

Como resultado deberíamos recibir un listado de puertos abiertos indicando que servicio provee cada uno:

```
msf6 > db_nmap 192.168.56.9
    Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-02 11:03 EDT
[*] Nmap: Nmap scan report for 192.168.56.9
[*] Nmap: Host is up (0.0011s latency).
[*] Nmap: Not shown: 977 closed tcp ports (reset)
[*] Nmap: PORT STATE SERVICE
[*] Nmap: 21/tcp open ftp
[*] Nmap: 22/tcp open ssh
[*] Nmap: 23/tcp open telnet
[*] Nmap: 25/tcp open smtp
[*] Nmap: 53/tcp open domain
[*] Nmap: 80/tcp open http
[*] Nmap: 111/tcp open rpcbin
                          rpcbind
[*] Nmap: 139/tcp open
                          netbios-ssn
[*] Nmap: 445/tcp open microsoft-ds
[*] Nmap: 512/tcp open exec
[*] Nmap: 513/tcp open login
[*] Nmap: 514/tcp open shell
[*] Nmap: 1099/tcp open rmiregistry
[*] Nmap: 1524/tcp open ingreslock
[*] Nmap: 2049/tcp open nfs
[*] Nmap: 2121/tcp open ccproxy-ftp
[*] Nmap: 3306/tcp open mysql
[*] Nmap: 5432/tcp open postgresql
[*] Nmap: 5900/tcp open vnc
[*] Nmap: 6000/tcp open X11
[*] Nmap: 6667/tcp open irc
[*] Nmap: 8009/tcp open ajp13
[*] Nmap: 8180/tcp open unknown
[*] Nmap: MAC Address: 08:00:27:22:00:BD (Oracle VirtualBox virtual NIC)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 13.45 seconds
<u>msf6</u> >
```

2.2 Metasploit port scanner

Alternativamente también se puede usar el módulo de escaneo de metasploit, para ello podemos seleccionarlo con el siguiente comando:

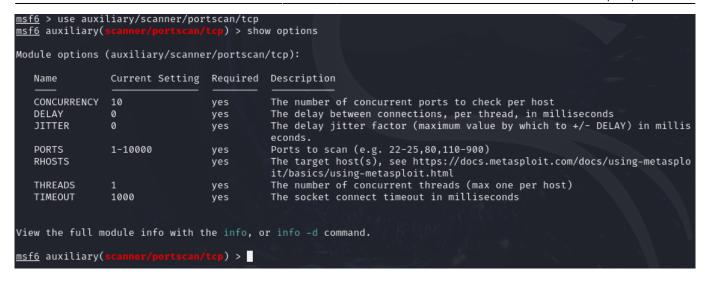
```
use auxiliary/scanner/portscan/tcp
```

Una vez seleccionado el módulo, hay que configurar sus parámetros, podemos ver los parámetros disponibles con el siguiente comando.

```
show options
```

http://knoppia.net/ Printed on 2025/11/29 20:17

2025/11/29 20:17 3/3 Metasploit para novatos



From:

http://knoppia.net/ - Knoppia

Permanent link:

http://knoppia.net/doku.php?id=metasploit:ms_dummies&rev=1746198657

Last update: **2025/05/02 15:10**

