

# On prend le contrôle de la Cible 1 ( Metasploit ) en étant sur l'attaquant

```
root@kali: /home/kali/Downloads/SAE304/Scans
Session Actions Edit View Help
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 100
    link/ether 08:00:27:88:f7:4e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.3/24 brd 10.0.2.255 scope global eth0
        inet6 fe80::a00:27ff:fe88:f74e/64 scope link
            valid_lft forever preferred_lft forever
echo "Dans le cadre de la SAE304, moi, Sami HAMEG, ai choisis la vulnérabilité backdoor ID 46882" > SAE304.txt
ls
SAE304.txt
hello
vulnerable
ls -l
total 12
-rw——— 1 root      root      94 Jan 29 10:59 SAE304.txt
drwxr-xr-x 2 msfadmin msfadmin 4096 Jan 29 10:31 hello
drwxr-xr-x 6 msfadmin msfadmin 4096 Apr 27 2010 vulnerable
whoami
root
```

- On affiche l'adresse ip actuelle, on voit qu'on a celle de la cible 1
- On créer un fichier preuve SAE304.txt.

On se rend sur notre machine virtuelle Metasploit ( non plus via Kali )

- On affiche l'adresse ip actuelle, c'est la même que celle d'en haut
- On retrouve le fichier SAE304.txt, créé à la même date que celui plus haut

```
msfadmin@metasploitable:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:88:f7:4e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.3/24 brd 10.0.2.255 scope global eth0
        inet6 fe80::a00:27ff:fe88:f74e/64 scope link
            valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ pzd
-bash: pzd: command not found
msfadmin@metasploitable:~$ pud
/home/msfadmin
msfadmin@metasploitable:~$ ls 61
ls: cannot access 61: No such file or directory
msfadmin@metasploitable:~$ ls -l
total 12
drwxr-xr-x 2 msfadmin msfadmin 4096 2026-01-29 10:31 hello
-rw----- 1 root      root      94 2026-01-29 10:59 SAE304.txt
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
msfadmin@metasploitable:~$ whoami
msfadmin
```