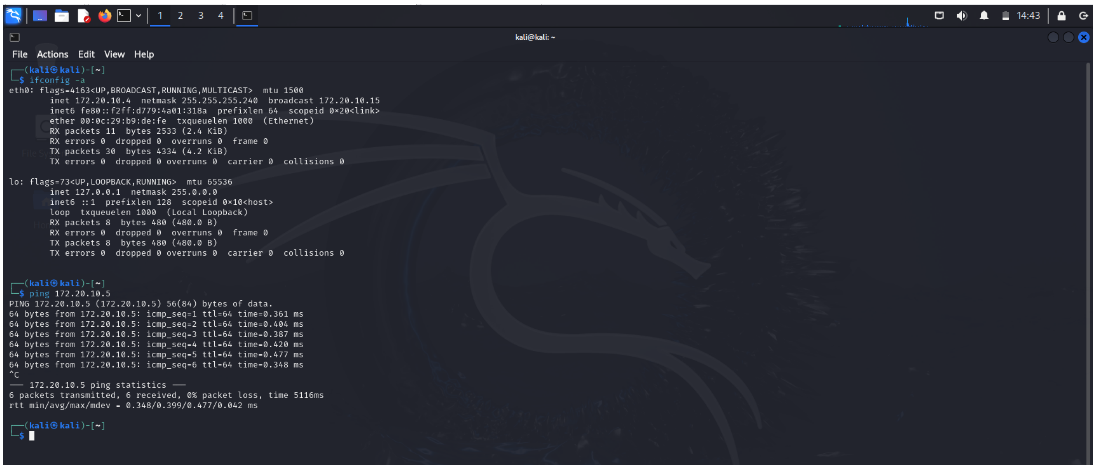
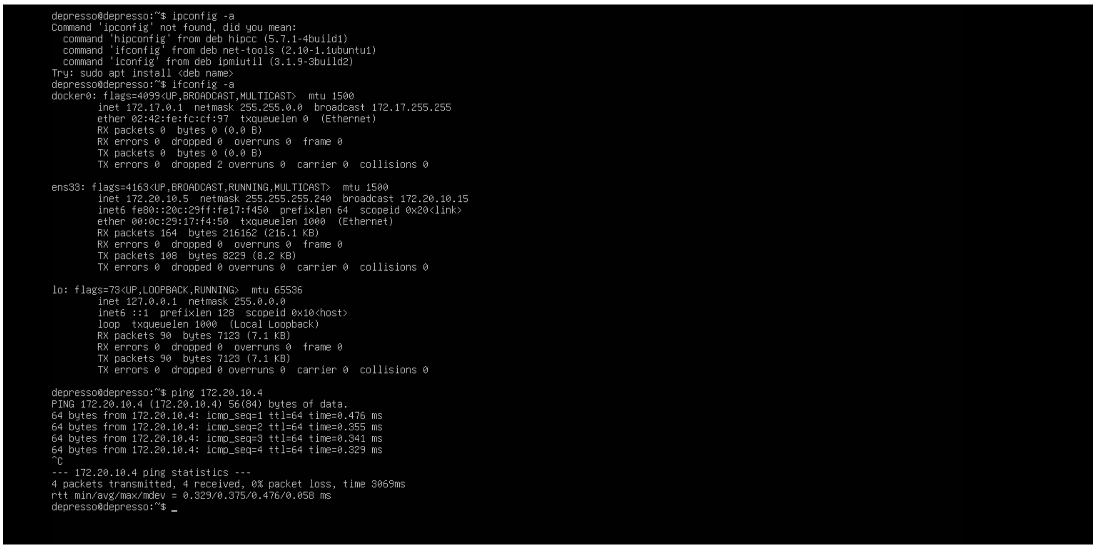
# TP N° 3

## 1 Connectivité Des Machines Virtuelles



```
┌──(kali㉿kali)-[~]
└─$ ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.10.4  netmask 255.255.255.240  broadcast 172.20.10.15
        inet6 fe80::f2ff:d779:4a01:318a  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:b9:de:fe  txqueuelen 1000  (Ethernet)
        RX packets 11  bytes 2533 (2.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30  bytes 4334 (4.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ ping 172.20.10.5
PING 172.20.10.5 (172.20.10.5) 56(84) bytes of data.
64 bytes from 172.20.10.5: icmp_seq=1 ttl=64 time=0.361 ms
64 bytes from 172.20.10.5: icmp_seq=2 ttl=64 time=0.404 ms
64 bytes from 172.20.10.5: icmp_seq=3 ttl=64 time=0.387 ms
64 bytes from 172.20.10.5: icmp_seq=4 ttl=64 time=0.420 ms
64 bytes from 172.20.10.5: icmp_seq=5 ttl=64 time=0.477 ms
64 bytes from 172.20.10.5: icmp_seq=6 ttl=64 time=0.348 ms
^C
── 172.20.10.5 ping statistics ──
6 packets transmitted, 6 received, 0% packet loss, time 5116ms
rtt min/avg/max/mdev = 0.348/0.399/0.477/0.042 ms

┌──(kali㉿kali)-[~]
└─$ 
```



```
depresso@depresso:~$ ipconfig -a
Command 'ipconfig' not found, did you mean:
  command 'hipconfig' from deb hipcc (5.7.1-4build1)
  command 'ifconfig' from deb net-tools (2.10-1.1ubuntu1)
  command 'iconfig' from deb ipmiutil (3.1.9-3build2)
Try: sudo apt install <deb name>
depresso@depresso:~$ ifconfig -a
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:fe:fc:cf:97  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 2 overruns 0  carrier 0  collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.10.5  netmask 255.255.255.240  broadcast 172.20.10.15
        inet6 fe80::20c:29ff:fe17:f450  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:17:f4:50  txqueuelen 1000  (Ethernet)
        RX packets 164  bytes 216162 (216.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 108  bytes 8229 (8.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 90  bytes 7123 (7.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 90  bytes 7123 (7.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

depresso@depresso:~$ ping 172.20.10.4
PING 172.20.10.4 (172.20.10.4) 56(84) bytes of data.
64 bytes from 172.20.10.4: icmp_seq=1 ttl=64 time=0.476 ms
64 bytes from 172.20.10.4: icmp_seq=2 ttl=64 time=0.355 ms
64 bytes from 172.20.10.4: icmp_seq=3 ttl=64 time=0.341 ms
64 bytes from 172.20.10.4: icmp_seq=4 ttl=64 time=0.329 ms
^C
--- 172.20.10.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3069ms
rtt min/avg/max/mdev = 0.329/0.375/0.476/0.058 ms
depresso@depresso:~$ _
```

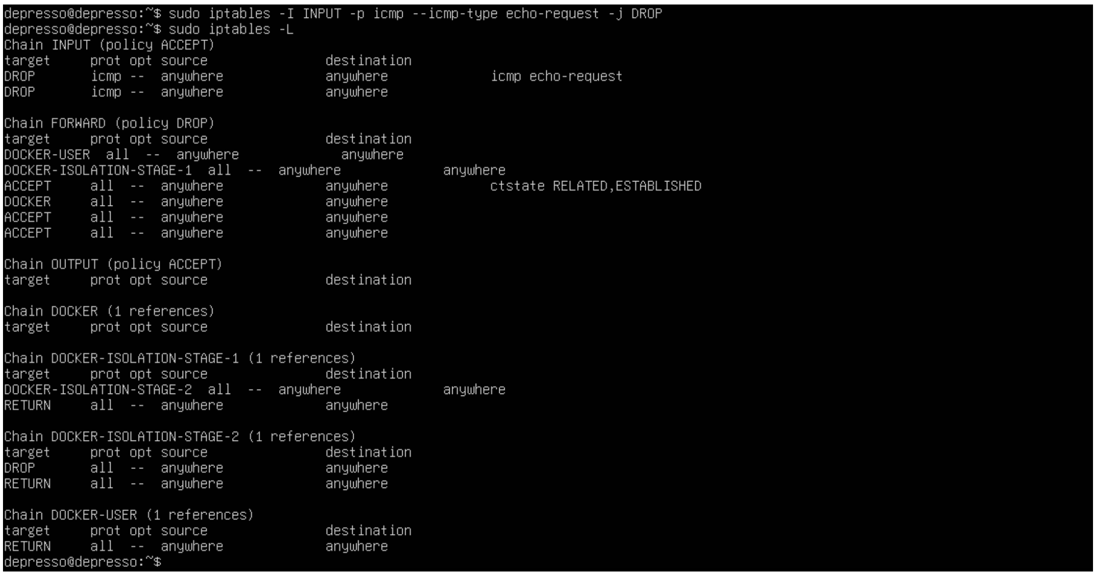
### Connectivité

D'après les captures d'écran, on remarque que les adresses IP des machines sont :

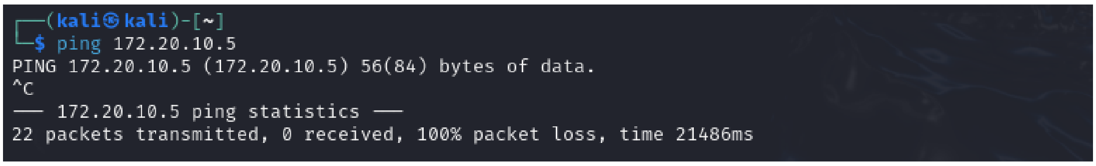
- **Ubuntu :** `172.20.10.5`
- **Kali Linux :** `172.20.10.4`

Et le ping est réussi, donc il y a une connectivité.

# 2 Restriction Des Paquets Entrants Vers Ubuntu



```
depresso@depresso:~$ sudo iptables -I INPUT -p icmp --icmp-type echo-request -j DROP
depresso@depresso:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere             icmp echo-request
DROP       icmp --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
DOCKER-USER  all  --  anywhere             anywhere
DOCKER-ISOLATION-STAGE-1  all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
DOCKER     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain DOCKER (1 references)
target     prot opt source               destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
target     prot opt source               destination
DOCKER-ISOLATION-STAGE-2  all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere

Chain DOCKER-ISOLATION-STAGE-2 (1 references)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere

Chain DOCKER-USER (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere
depresso@depresso:~$
```

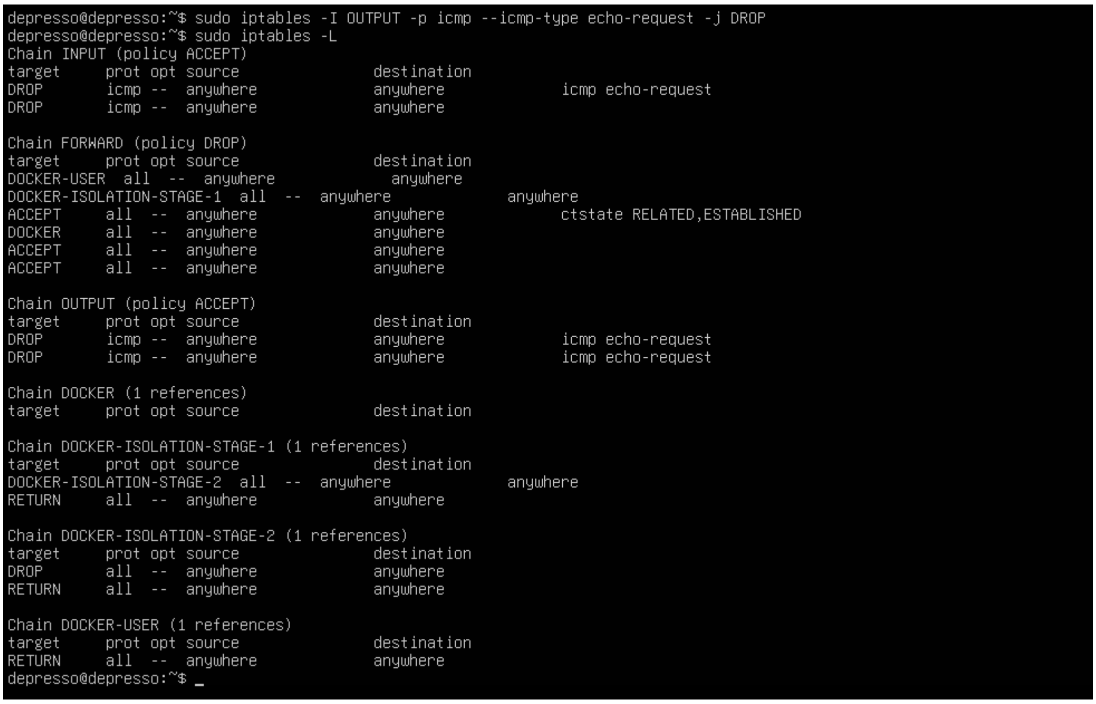


```
┌──(kali㉿kali)-[~]
└─$ ping 172.20.10.5
PING 172.20.10.5 (172.20.10.5) 56(84) bytes of data.
^C
─── 172.20.10.5 ping statistics ───
22 packets transmitted, 0 received, 100% packet loss, time 21486ms
```

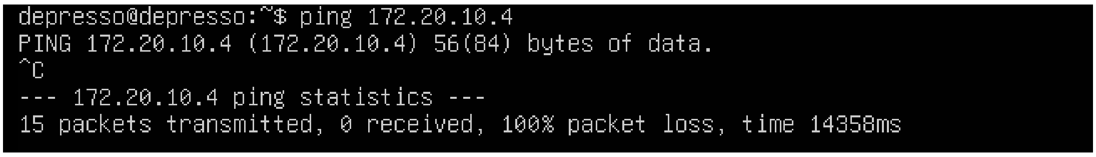
## Remarque

- On constate que `iptables` d'Ubuntu n'accepte plus les ping entrants (chain **INPUT** policy **DROP**).
- Kali Linux ne peut plus envoyer de requêtes ping vers la machine Ubuntu.

# 3 Restriction Des Paquets Sortants Depuis Ubuntu



```
depresso@depresso:~$ sudo iptables -I OUTPUT -p icmp --icmp-type echo-request -j DROP
depresso@depresso:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere             icmp echo-request
DROP       icmp --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
DOCKER-USER  all  --  anywhere             anywhere
DOCKER-ISOLATION-STAGE-1  all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
DOCKER     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere             icmp echo-request
DROP       icmp --  anywhere             anywhere             icmp echo-request

Chain DOCKER (1 references)
target     prot opt source               destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
target     prot opt source               destination
DOCKER-ISOLATION-STAGE-2  all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere

Chain DOCKER-ISOLATION-STAGE-2 (1 references)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere

Chain DOCKER-USER (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere
depresso@depresso:~$ _
```



```
depresso@depresso:~$ ping 172.20.10.4
PING 172.20.10.4 (172.20.10.4) 56(84) bytes of data.
^C
--- 172.20.10.4 ping statistics ---
15 packets transmitted, 0 received, 100% packet loss, time 14358ms
```

## Remarque

- On constate que `iptables` d'Ubuntu n'accepte plus les ping sortants (chain **OUTPUT** policy **DROP**).
- Ubuntu ne peut plus envoyer de requêtes ping vers la machine Kali Linux.