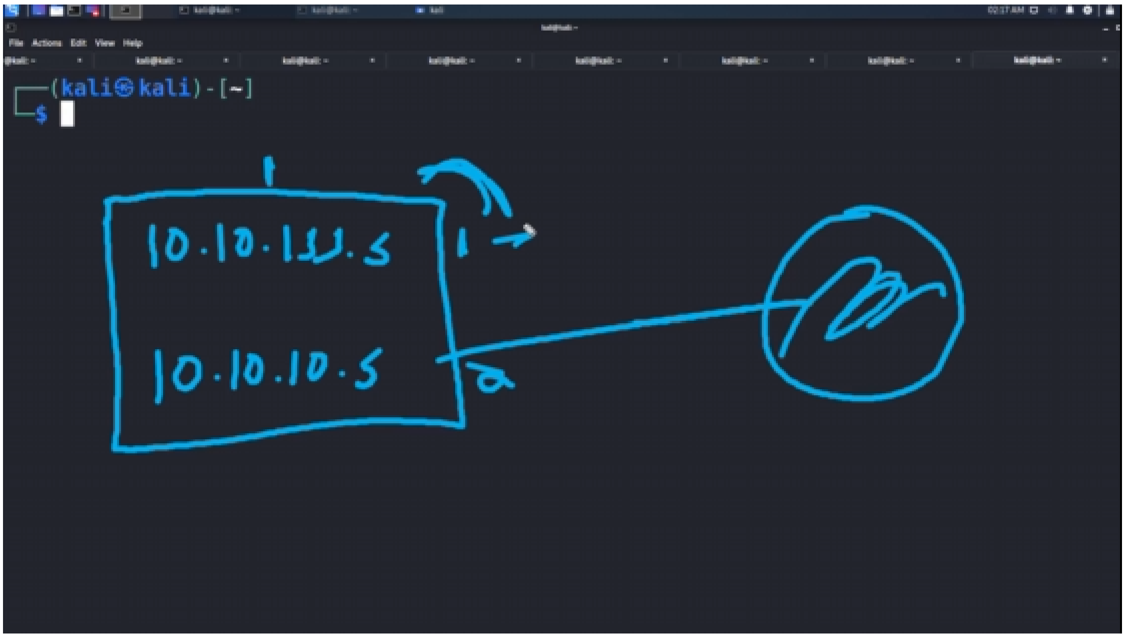
03 - Pivoting Overview

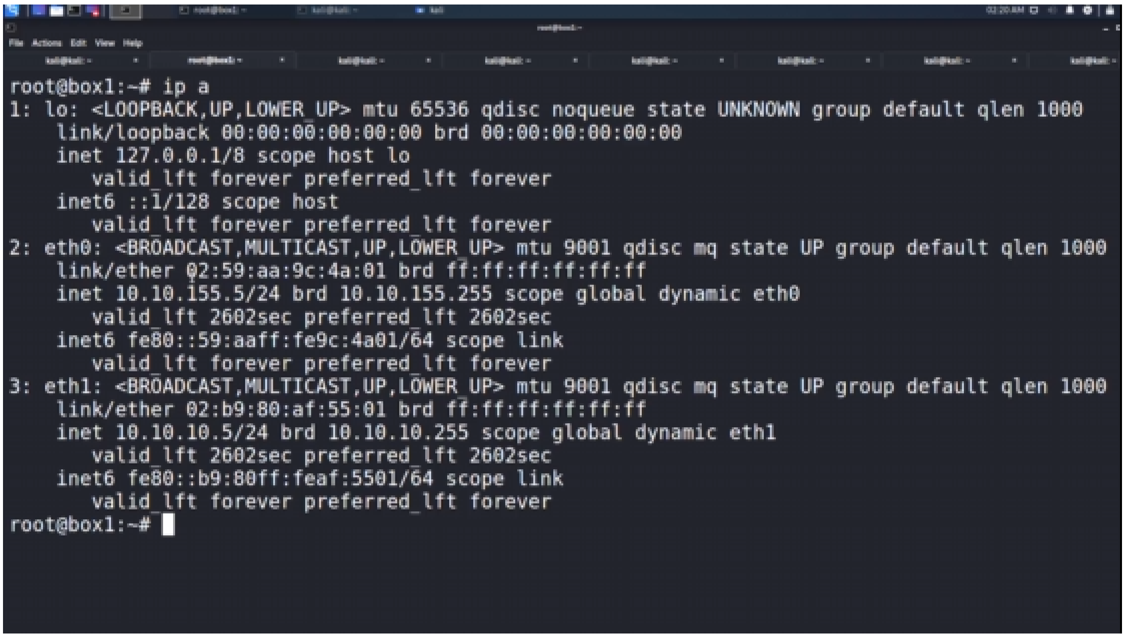
Image we have compromised a machine, and that machine allows access to two Network Interfaces. And those Network Interfaces share a new network that was originally not available to us.



```
┌──(kali㉿kali)-[~]
└─$ 
```

We were first pentesting 1010.155.5 network, and on this particular machine, we saw that we also had this 10.10.10.5 network connected to it. So now, if we want to "move"(pivot) to the other network and starting attacking it, we can do the following.

The scenario is going to look something like this, if we are on an ubuntu machine.



```
root@box1:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 02:59:aa:9c:4a:01 brd ff:ff:ff:ff:ff:ff
    inet 10.10.155.5/24 brd 10.10.155.255 scope global dynamic eth0
       valid_lft 2602sec preferred_lft 2602sec
    inet6 fe80::59:aaff:fe9c:4a01/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 02:b9:80:af:55:01 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.5/24 brd 10.10.10.255 scope global dynamic eth1
       valid_lft 2602sec preferred_lft 2602sec
    inet6 fe80::b9:80ff:feaf:5501/64 scope link
       valid_lft forever preferred_lft forever
root@box1:~# 
```

We can see eth0 and eth1 are ip addresses.

At this moment, we do not have any access to the eth1 network (10.10.10.5/24). We do not have a route to that network.

Now, we need to install a pivot in this machine, so we can access this new network.

There are a couple of ways of doing so, the next lesson is going to show the tools we can use, and how to use them.