**BYPASSING HTTPS AND HSTS**

**to bypass it we must spoof and sniff the target first**

**secondly we need to run caplet from bettercap:**

hstshijack/hstshijack

**Now everytime our target accesses HTTPS site it will load HTTP instead**

**That way we can see the usernames, passwords, URLs and so on**

**! This wont work on HSTS sites !**

**In order to bypass HSTS we must use fake sites that work exactly the same way as the main site but are slightly different but the target most of the time wont even notice**

**Example:**

**facebook.com == facebook.corn**

**twitter.com == twiter.com**

**We load facebook.coRN not coM and its hard to notice**

**And we load twiter.com instead of twiTTer.com which is hard to notice too**

We can modify the hstshijack caplet and make more sites fake the way we want to

**!! If the target tries to load facebook from the HSTS google.com site it would load the main HSTS facebook.com but if the target tries to click on facebook.com through HTTP google.ie then it would load HTTP facebook.coRN !!**