Network Security Laboratory Session 8

SSL STRIP & PASSWORD CRACKING

SSL Strip

- Allows the attacker to force victim at using HTTP, instead of HTTPS
- The attacker can reduce the security of the connection given by SSL
- With HTTP all data are sent as plaintext, allowing the attacker to stole victim's data
- It can be performed when an attacker is in a MITM positions

Password Storage

- Passwords are stored in an encrypted text inside some special files
- These files usually contains the users and the passwords encrypted with an Hash function
- In Linux these files are called **passwd** and **shadow**
- In Windows the file is called **SAM**

Linux Shadow Files

- Shadow files can be only **read** from the root user, to protect it
- In the shadow password mechanism the data are split in two differents file:
- Passwd file, that contains users
- Shadow file, that contains hashed password

Windows Security Account Manager (SAM) Files

- Security Account Manager (SAM) is an encrypted DataBase that contains users and passwords of windows
- SAM and SYSTEM file, useful for decrypting and obtain password for windows, are located in the **%Windows%/system32/config** path
- These files are also mounted inside windows registry on path:
  - HKLM/SYSTEM
  - HKLM/SAM
- These paths are useful if we want to attack the SAM database in order to decrypt passwords

Exercises

- Perform an **ssl strip** attack using **Bettercap**
- Discover Linux password
- Discover Windows password