Network Security Laboratory – Lecture 8

SSL STRIP & PASSWORD CRACKING

Dott. Andrea Baffa
email: abaffa94@servizimicrosoft.unical.it

SSL Strip

- Allow the attacker to force victim at using HTTP, instaed of HTTPS
- Removing HTTPS an attacker can reduce the security of the connection given by SSL
- With HTTP all data is sent as plaintext, this allow the attacker to stole victim’s data
- It can be performed when an attacker is in a MITM positions

Password Storage

- On operative system, passwords are stored encrypted inside some special files
- These files usually contains the users and the passwords encrypted with an Hash function
- In Linux these files are called shadow
- In Windows are called SAM

Linux Shadow Files

- Shadow files usually can be read only from root users, 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 %Windows%/system32/config path

- These file are also mounted inside windows registry on path:
  - HKLM/SYSTEM
  - HKLM/SAM

- These path are useful if we want to attack the SAM database in order to decrypt passwords

Exercises

- On course Website there are two guides for password storage attack
    - Exercise for Shadow file attack (Linux)
    - Exercise for SAM file attack (Windows)
- Using these guide you must discover password of both operative system

Questions?

The lesson is over.

Thank you!