Systems Security

Exercise 6 & 7

Password cracking in Windows 2000

1. Login as an administrator, run *regedit* and change the value of the key HKEY_USERS\.DEFAULT\Control Panel\Desktop\ScreenSaveTimeOut to 30 (sec) and ScreenSaveActive to 1.
2. Create 3 accounts: u1, u2, u3 settings their passwords as 3, 5 and 8 characters long, respectively.
3. Try an unauthorized access to your computer using the standard screen saver *logon.scr*:
   - Log on to your computer
   - Change *logon.scr* to *logon.scr.old* and *cmd.exe* to *logon.scr*
   - logout and wait 30 sec.

   When the console appears do the following:
   - Find out current user context using *whoami* from resource kit
   - Run lusrmgr.msc and try a) administrator password change, b) creation of a new user account c) administrator group membership change
   - Run *explorer.exe* and try to use administrative tools
   - Close the console window
4. Install password auditing program – LC4 (lc4setup.exe)
5. Using LC4 do the following:
   - Get passwords from the local computer.

   Run dictionary attack and combined attack (custom options). When not successful modify the dictionary. Try the possibility of password acquisition in the context of an ordinary user and without authorization (as in p. 2). Measure the time taken. Restore the original files (from p. 2).
   - Try to get password from a remote computer
     a. In the console window on your machine run *PWDUMP3*, then give the password for the chosen account on the remote machine. If using a user account is not successful, use the admin account.

    b. Locally run LC4, do not use the wizard. Create a new session choosing **Import|Import from PWDUMP file ...** Use the file created by PWDUMP3. Try password cracking with any method.

6. Prepare a floppy disk for off-line password change.
   - Create another administrator account
   - Run rawwrite2.exe to create the floppy using image bd011022.bin
   - Check what number your disk partition ha
   - Boot the computer from the prepared floppy
     a. choose your partition
     b. point the directory with SAM database (\winnt\system32\config)
     c. do not switch off password hashing (SYSKEY)
     d. type the new admin password
     e. answer yes to the following questions
   - Boot the computer again, check what is the current password
7. Install program *Iris*. Sniff and decode 2 chosen sessions (pop3, http, ftp, ...). Use port filtering.

During the exercise everyone must prepare a report, describing all the performed activities and obtained information. Indicate which programs you have used and with what parameters/options. Attach 2 most interesting screenshots. In the report you should mention failures, too. Reasons of a failure should be explained.

The report must be stored in a location given by the teacher **before leaving** the classroom.

Prepared by Zbigniew Zieliński, translated by Janusz Borkowski