Basic Crackme by xxdepelxx

Requirements: OllyDbg

Open the crackme with OllyDbg, go to 0x00402506 which represent the onLoad handler, go down, and stop at the address 0x00402606.

Has you can see, in this snippet of code, the crackme will compare the actual name of the crackme, with “Crackme.exe”, and if they are different we can't go forward, so don't rename the crackme. Next we will reach another validation which uses the api “IsDebuggerPresent” to avoid debug.

Step into 0x004026D9, a you will see IsDebuggerPresent api call.

So just, patch the JNE located at the address 00x4026F1 with a JMP, and resume the process.

Set your data like this!

So, now we just have to locate the “Yes” button click handler, and get the correct serial. Set a breakpoint at the address 0x004027C0 and press on the “Yes” button.

At the address 0x0040297D the crackme retrieve the first 3 chars our username, with the api “rtcLeftCharVar”.

iamjuza [at] gmail [dot] com
Basic Crackme by xxdepelxx

And at the address 0x004029B8 the crackme will call the api “rtcRightCharVal” to get the last 3 chars of our username.

Next, our username last 3 chars will be added to the string “SCT-”, which means that one of our serials will be at this time “SCT-cde”.

Next, the crackme will get the length of our username, and add it to the serial, which is now “SCT-cde5”.

And at last the serial is finished by adding the first 3 chars to the end of it. “SCT-cde5abc”.

At the address 0x00402A37, the second serial will be compared to “Shooter”, so now we can assume that:

Username: abcde
Serial1: SCT-cde5abc
Serial2: Shooter

Go see the keygen source!