**EXPERIMENT NO. 7**

|  |
| --- |
| **Student Name and Roll Number: Harshit Parashar 18csu081** |
| **Semester /Section:5th semester CS-V-CSA1** |
| **Link to Code:** |
| **Date: 01/10/2020** |
| **Faculty Signature:** |
| **Marks:** |

|  |
| --- |
| **Objective:** Use IDA Pro Free to disassemble and analyze Windows executable files |
| **Outcome:** Students will be able to solve challenges |
| **Problem Statement:** Analyze crackme-121-3 in IDA. Find the correct command line. Use IDA Pro to find the password, and run the program with the correct password, so you see a "Congratulations" message. |
| **Background Study:** The Interactive Disassembler is a disassembler for computer software. It generates assembly language source code from machine-executable code. It supports a variety of executable formats for different processors and operating systems. It is the dissembler of choice for many Malware analysts, Reverse engineers and Vulnerability analysts |
| **Algorithm/Flowchart:** |
| **Code(Solution):** |
| **Sample Outputs:**  **Step#1: we will download and copy the crackme 121-3 and dll file in the IDA freeware folder**    **Step#2 now we will open the terminal and try to run the file,as we see,it is asking for two passwords I.e password1 and password2 now we don’t know the password so we try to enter some random passwords as a result it is showing that Fail! First word was wrong,to crack the passwords we need to disassemble the file**    **Strep3 : now we will open the IDA freeware and search crackme in the search>text>”crackme”,also we directly open the file**    **Step4: in this screenshot we can see the graphical representation of the file i.e how code is functioning**  **To zoom we right click and select fit window size,this will fit the whole graphical representation in the window**  **After observation we see the last two lines of first block then we find that it is cmp that is comparing some argument and making two decision ,jz ,if flag is set to zero it will jump ,now here are two green and red ,it will move to red arrowed box if comparison is wrong.**  **Now here are conditions if password 1 and password 2 both are right then these green arrow will take to the box where it is written “congratulation ! you found the passwords”**  **If first password is wrong then it will take to the box with red arrow and say”first word is wrong “ similary with the second password.**        **Now we can see that password 1 is “suffering” and password2 is “succotash”**      **After finding the passwords now we will again run the file and insert the above mentioned passwords**  **>>Congratulations! You found the passwords!** |
| **Question Bank:**  1. Which of the following is not a disassembler tool?  a) IDA Pro  b) PE Explorer  c) **Turbo C**  d) W32DASM  2. What is the difference between IDA Pro and Ghidra?   * IDA has a debugger whereas Ghidra does not. * Ghidra is free and open source including the decompiler. While IDA is very expensive, particularly when you start adding the decompiler licenses. * Ghidra has an undo button while ida does not if we mess up then we have to do all over again * Ghidra has collaborative disassembly/decompiler projects built in by design, whereas IDA requires plugins to do collaboration and the IDA database files are not designed to be shared * Since IDA is a more mature and ubiquitous product, there are a lot of open-source tools built around it.   3. Explain the features available in Ghidra  Answer : Ghidra appears to have better support for very large (1GB+) firmware images with decent performance  It also doesn't have problems with analysing firmware images that declare large memory regions.   Ghidra has collaborative disassembly/decompiler projects built in by design.  Ghidra's disassembler has data flow analysis built in, showing you where data can come from when you click a register or variable |