**EXPERIMENT NO. 6**

|  |
| --- |
| **Student Name and Roll Number: Harshit Parashar 18CSU081** |
| **Semester /Section:5th semester CS-V-CSA1** |
| **Link to Code:** |
| **Date:** 24/9/2020 |
| **Faculty Signature:** |
| **Marks:** |

|  |
| --- |
| **Objective:** To practice writing and running basic x86 assembly code, using the Jasmin interpreter. |
| **Outcome:** Students will understand language that can be reliably recovered from malware when source code is unavailable |
| **Problem Statement:**  In the Code section, type in these instructions.  mov eax, 1  mov ebx, 9  mov ecx, 49  push eax  push ebx  push eax  push ecx  push ebx  push eax  pop eax  pop ebx  pop ecx  add eax, ebx (1)  pop ecx  add eax, ecx  pop ebx (2)  pop ecx (3)  add eax, ebx  Load and run this program. Find the value of eax in (1), ebx in (2) and ecx in (3) |
| **Background Study:** 3 coding levels involved in malware analysis. Reverse engineer use a disassembler to generate assembly code and figure out how a pgm operates. Assembly is the highest level language that can reliably and consistently recovered from machine code when high-Level language source code is not available. Assembly language is actually a class of languages. Different versions of assembly language for each type of processor |
| **Algorithm/Flowchart:** |
| **Code(Solution):** |
| **Sample Outputs:**  After downloading jasmin,open the new file and write the commands and press play button to execute it,do it after every command:  1:screenshot after executing **add eax, ebx** command  **EAX=10,EBX=9,ECX=49,ESP=4084,EBP=4096,EIP=13**    2:screenshot after executing **pop ebx** command  **EAX=11,EBX=9,ECX=1,ESP=4092,EBP=4096,EIP=16**    3:screenshot after executing **pop ecx** command  **EAX=11,EBX=9,ECX=1,ESP=4096,EBP=4096,EIP=17**    Final screenshot after the execution of command **add eax,ebx**  **EAX=20,EBX=9,ECX=1,ESP=4096,EBP=4096,EIP=18** |
| **Question Bank:**  Q1. Compilers, assemblers and interpreters are examples of this.   1. **Translator** 2. Run time environment 3. Editor 4. Error diagnostics   Q2. Which type of code is assembly language?   1. High level code 2. **Low level code**   Q3. Examples of this include binary machine code and assembly language   1. High level code 2. **Low level code**   Q4. This translator is used to translate all of the source code at the same time and creates one executable file   1. Interpreter 2. **Compiler** 3. Assembler   Q5. Uses Mnemonics as command words (for example LDA, STA and ADD)   1. High level code 2. Low level code 3. **Assembly language** |