Soal Terkait

**Cheat ~~Pekalongan~~ Labtek V** (2 poin + 2 point)

A video game with an object and people

Description automatically generated

*Lah kok tembus!?*

Ketentuan

Buatlah sebuah program memory editor sederhana yang akan mengedit memory target program dengan value yang lain. Berikut adalah contoh program yang menjadi target:

|  |
| --- |
| **targetprogram.cpp** |
| #include <iostream>  #include <stdio.h>  **int** **main**() {  **int** buf = **0xDEADBEEF**;      printf("Target value : 0x%x**\n**Target address : 0x%p**\n**Input any number to continue**\n**", buf, &buf);  **int** prompt\_buf;      std::cin >> prompt\_buf;      printf("Target value : 0x%x**\n**", buf);  **return** **0**;  } |

Berikut template program editor untuk Win32

|  |
| --- |
| **memoryeditor.cpp** |
| #include <iostream>  #include <windows.h>  #include <stdio.h>  #include <tchar.h>  #include <psapi.h>  **void** **print\_ps\_name**(DWORD pid) {      TCHAR pname[MAX\_PATH] = TEXT("<unknown>");      HANDLE phandle = OpenProcess(PROCESS\_QUERY\_INFORMATION | PROCESS\_VM\_READ, FALSE, pid);  **if** (phandle != NULL) {          HMODULE pmod;          DWORD temp;  **if** (EnumProcessModules(phandle, &pmod, **sizeof**(pmod), &temp))              GetModuleBaseName(phandle, pmod, pname, **sizeof**(pname) / **sizeof**(TCHAR));      }      \_tprintf(TEXT("%s (PID %u)**\n**"), pname, pid);      CloseHandle(phandle);  }  **void** **print\_ps**() {      DWORD ps\_list[**1024**], ps\_memctr, ps\_ctr;  **if** (!EnumProcesses(ps\_list, **sizeof**(ps\_list), &ps\_memctr))  **return**;      ps\_ctr = ps\_memctr / **sizeof**(DWORD);  **for** (**int** i = **0**; i < ps\_ctr; i++)  **if** (ps\_list[i] != **0**)              print\_ps\_name(ps\_list[i]);  }  **int** **main**() {      print\_ps();      // TODO : Add memory editor    **return** **0**;  } |

*Environment* target dibebaskan, tetapi template diatas hanya dapat digunakan untuk *environment* Win32. *API Process & Virtual Memory* setiap *environment* dapat berbeda-beda.

Untuk target Win32, gunakan *Visual Studio Community C++ Console Project* untuk mempermudah *development*.

Bonus

(Poin 2)  Download, Compile, dan mainkan game pada [tautan ini](https://drive.google.com/file/d/1AZC-OeyqrwFTj43Uzwf2A-LNNrEkmvUA/view?usp=sharing)  hingga menang menggunakan program yang anda buat, serta dokumentasikan proses tersebut dalam sebuah video yang kemudian diunggah ke google drive/youtube yang menampilkan:

* Proses Download
* Source code game
* Proses kompilasi
* Proses penyelesaian permainan menggunakan cheat yang sudah kalian buat
* Tampilan hasil akhir permainan ketika sudah berhasil memenangkan game ini.

Note: boleh untuk mengunduh dan mencoba program terlebih dahulu untuk memikirkan cara menyelesaikannya. Namun saat pembuatan video, tetap dimulai dari proses *download* dan *compile* program terlebih dahulu.

Tujuan

* Menjadi *citer* handal hingga membuat *cheater* professional ketar ketir
* Mengetahui *API Process & Virtual memory*
* Belajar nge-hack game

Berkas

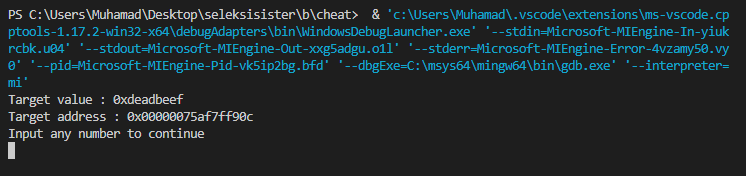
* Source code
* Dokumen berisikan eksekusi program memory editor
* Tautan (*link*) menuju link video jika mengerjakan spek bonus. *Link* boleh ditulis dalam file .txt tersendiri atau digabung dengan dokumen program memori editor.

Referensi

* <https://docs.microsoft.com/en-us/windows/win32/api/memoryapi/nf-memoryapi-readprocessmemory>
* <https://docs.microsoft.com/en-us/windows/win32/api/memoryapi/nf-memoryapi-writeprocessmemory>
* <https://github.com/cheat-engine/cheat-engine>
* <https://docs.microsoft.com/en-us/windows/win32/procthread/process-enumeration>

<https://www.linuxquestions.org/questions/programming-9/reading-proc-pid-mem-462646/>  

Eksekusi awal program (buat ngambil addressnya)



Eksekusi program cheat

A computer screen shot of a computer program

Description automatically generated

Hasil program setelah dicheat

