Soal Terkait

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

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\nTarget address : 0x%p\nInput 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>
```

```c
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 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)

```
PS C:\Users\Muhamad\Desktop\seleksisister\b\cheat>  & 'c:\Users\Muhamad\.vscode\extensions\ms-vscode.cp
ptools-1.17.2-win32-x64\debugAdapters\bin\WindowsDebugLauncher.exe' '--stdin=Microsoft-MIEngine-In-yiuk
rcbk.u04' '--stdout=Microsoft-MIEngine-Out-xxg5adgu.o1l' '--stderr=Microsoft-MIEngine-Error-4vzamy50.vy
0' '--pid=Microsoft-MIEngine-Pid-vk5ip2bg.bfd' '--dbgExe=C:\msys64\mingw64\bin\gdb.exe' '--interpreter=
mi'
Target value : 0xdeadbeef
Target address : 0x00000075af7ff90c
Input any number to continue
```

Eksekusi program cheat

```
PS C:\Users\Muhamad\Desktop\seleksisister\b\cheat>  & 'c:\Users\Muhamad\.vscode\extensions\ms-vscode.cp
ptools-1.17.2-win32-x64\debugAdapters\bin\WindowsDebugLauncher.exe' '--stdin=Microsoft-MIEngine-In-vfvv
rpzk.1ut' '--stdout=Microsoft-MIEngine-Out-qsnc45in.skb' '--stderr=Microsoft-MIEngine-Error-zeeje3u0.ma
j' '--pid=Microsoft-MIEngine-Pid-pxqxjljn.cf0' '--dbgExe=C:\msys64\mingw64\bin\gdb.exe' '--interpreter=
mi'
problem.exe (PID 12392)
pid is: 12392
Scanning memory
Read 4 bytes
Content: -559038737
Written 4 bytes
Memory after writing:
Read 4 bytes
Content: 0
```

Hasil program setelah dicheat

```
PS C:\Users\Muhamad\Desktop\seleksisister\b\cheat>  & 'c:\Users\Muhamad\.vscode\extensions\ms-vscode.cp
ptools-1.17.2-win32-x64\debugAdapters\bin\WindowsDebugLauncher.exe' '--stdin=Microsoft-MIEngine-In-yiuk
rcbk.u04' '--stdout=Microsoft-MIEngine-Out-xxg5adgu.o1l' '--stderr=Microsoft-MIEngine-Error-4vzamy50.vy
0' '--pid=Microsoft-MIEngine-Pid-vk5ip2bg.bfd' '--dbgExe=C:\msys64\mingw64\bin\gdb.exe' '--interpreter=
mi'
Target value : 0xdeadbeef
Target address : 0x00000075af7ff90c
Input any number to continue
a
Target value : 0x0
PS C:\Users\Muhamad\Desktop\seleksisister\b\cheat>
```