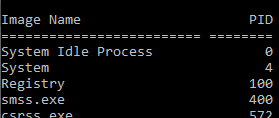
CODE:

*Process:*

-không thể có một process và một thread có cùng một ID

-1 process không bao giờ được gán ID =0



- thực sự không có "System Idle Process",Task Manager tạo process hư cấu này as a placeholder cho Idle thread chạy khi không có gì khác đang chạy.

-Số threads trong System Idle Process luôn luôn bằng số lượng CPU trong máy tính, hay nói cách khác System Idle Process đại diện cho số CPU chưa dùng.

Process32First(hProcessSnap, &pe32);

Lấy thông tin process đầu tiên trong danh sách hProcessSnap truyền vào biến pe32

Process32Next(hProcessSnap, &pe32)

Tương tự như trên nhưng là lấy process tiếp theo từ vị trí con trỏ hiện tại, dịch luôn con trỏ 1 đơn vị.

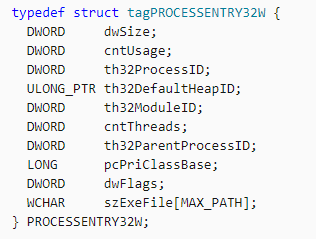
HANDLE hProcessSnap = CreateToolhelp32Snapshot(TH32CS\_SNAPPROCESS,0);

Chụp danh sách process xong bỏ vào biến hProcessSnap

HANDLE hProcess = OpenProcess(PROCESS\_TERMINATE, 0, (DWORD)pe32.th32ProcessID);

Mở process đang tồn tại, giành quyền truy cập.

PROCESSENTRY32 pe32;



CloseHandle(hProcessSnap);

Đóng tiến trình để tránh rò rỉ tài nguyên trong khi ứng dụng đang chạy. (không phải là kill tiến trình). chỉ đơn giản là cho system biết bạn không quan tâm đến process. process sẽ tiếp tục thực thi cho đến khi nó tự kết thúc

TerminateProcess(hProcess, 9);

Kill process, với đầu vào là biến process và exit code là 9

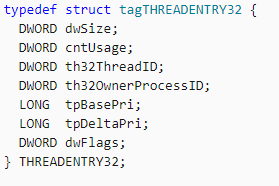
*Thread:*

HANDLE hThreadSnap = CreateToolhelp32Snapshot(TH32CS\_SNAPTHREAD, 0);

Thread32First(hThreadSnap, &te32);

Thread32Next(hThreadSnap, &te32);

THREADENTRY32



CreateThread(NULL, 0, Thread, (PVOID)&ThreadInput[i], 0, &dwThreadID[i]);

Thread: tên hàm thread

(PVOID)&ThreadInput[i]: biến truyền vào

WaitForSingleObject(hThread[i], INFINITE);

Đợi 1 thread

WaitForMultipleObjects(MAX\_THREADS, hThread, TRUE, INFINITE);

Đợi nhiều thread

SYSTEMTIME

FILETIME

GetThreadTimes(thread, &ftCreationTime, &ftExitTime, &ftKernelTime, &ftUserTime);

Lấy thời gian bắt đầu và kết thúc của thread bỏ vào biến CreationTime và exittime

FileTimeToSystemTime(&ftCreationTime, &CreationTime);

Convert filetime sang systemtime

EP:entry point :con trỏ đến lệnh đầu tiên

EIP:e instruction point:con trỏ hướng dẫn chạy các lệnh tiếp theo