



키보드..
너의 마음을 후킹하겠어 !-!



AGENDA

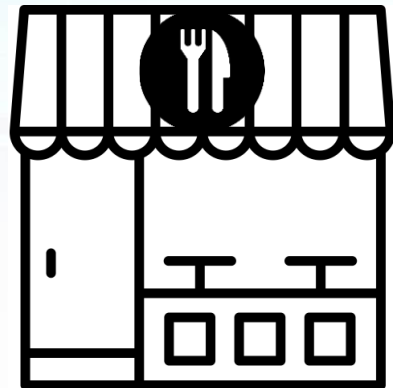
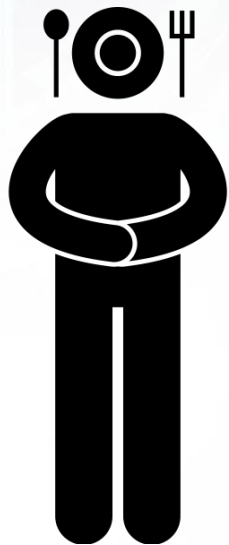
- Hooking이란?
- 기본지식?
- KeyLogging이란?
- KeyLogging 시연

Hooking이란?

Hooking

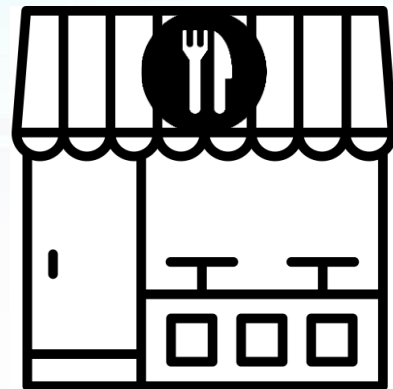
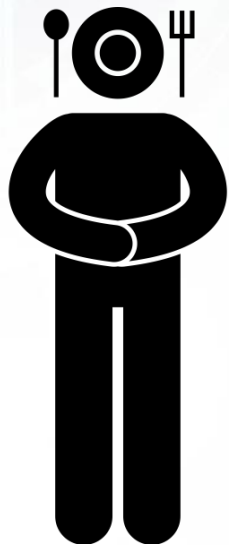
Hooking이란?

치킨 한 마리
주세요



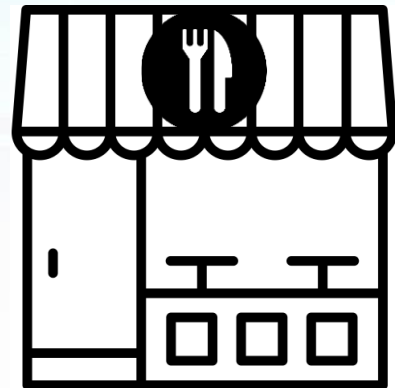
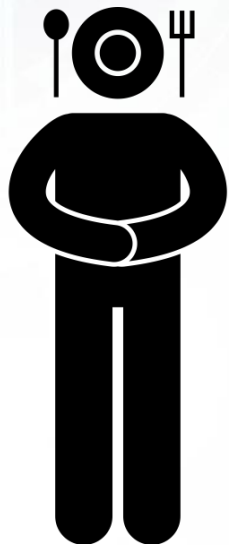
Hooking이란?

피자 한 판
주세요



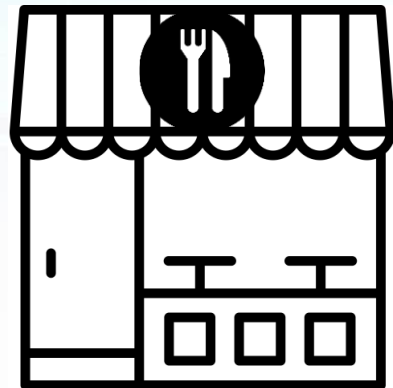
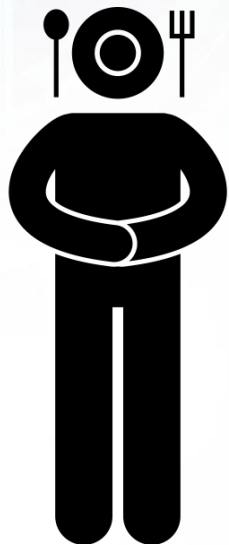
Hooking이란?

치킨 한 마리
주세요



Hooking이란?

으엑
이거 아닌데;;

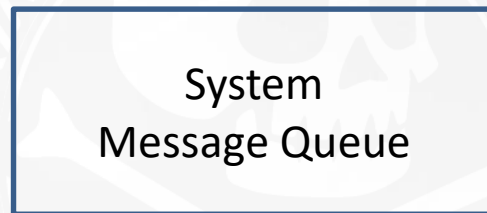
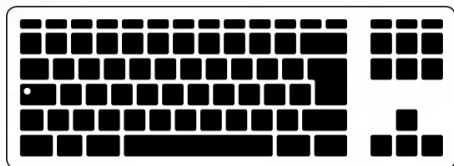


Key input



Chrome
Message Queue

Notepad
Message Queue





Message Queue

Message Queue

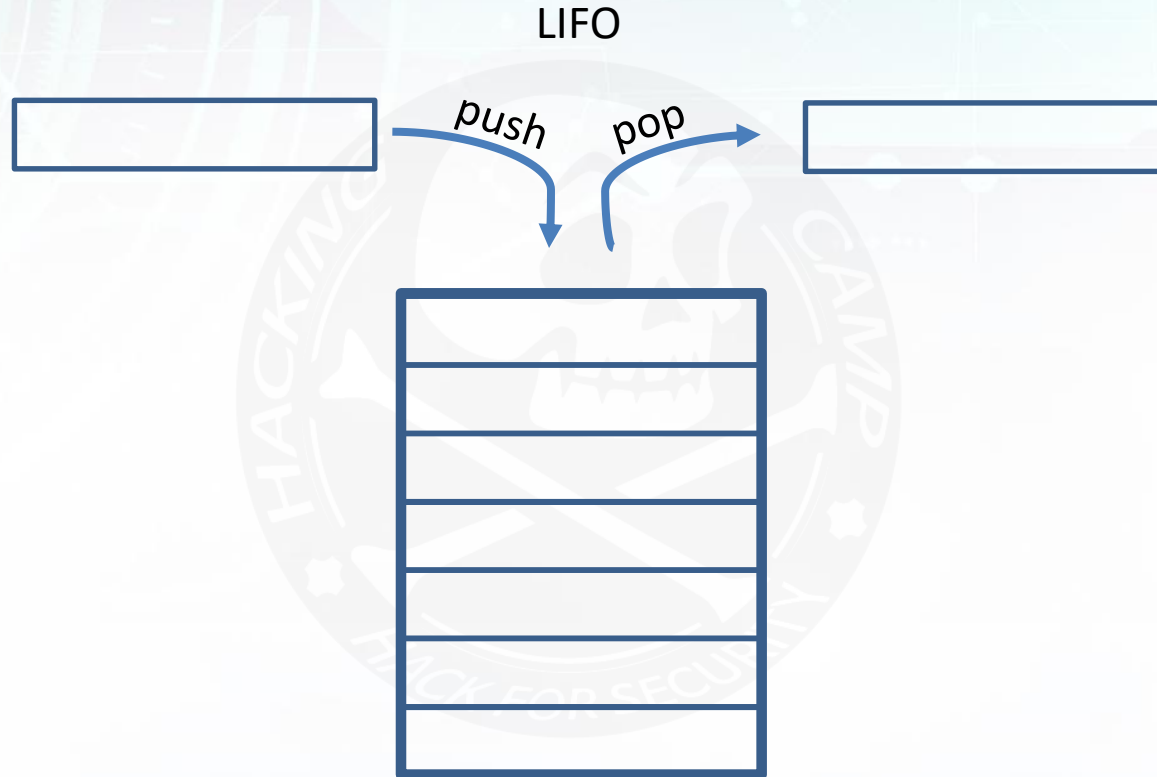


Message Queue

Queue
Stack

Message Queue

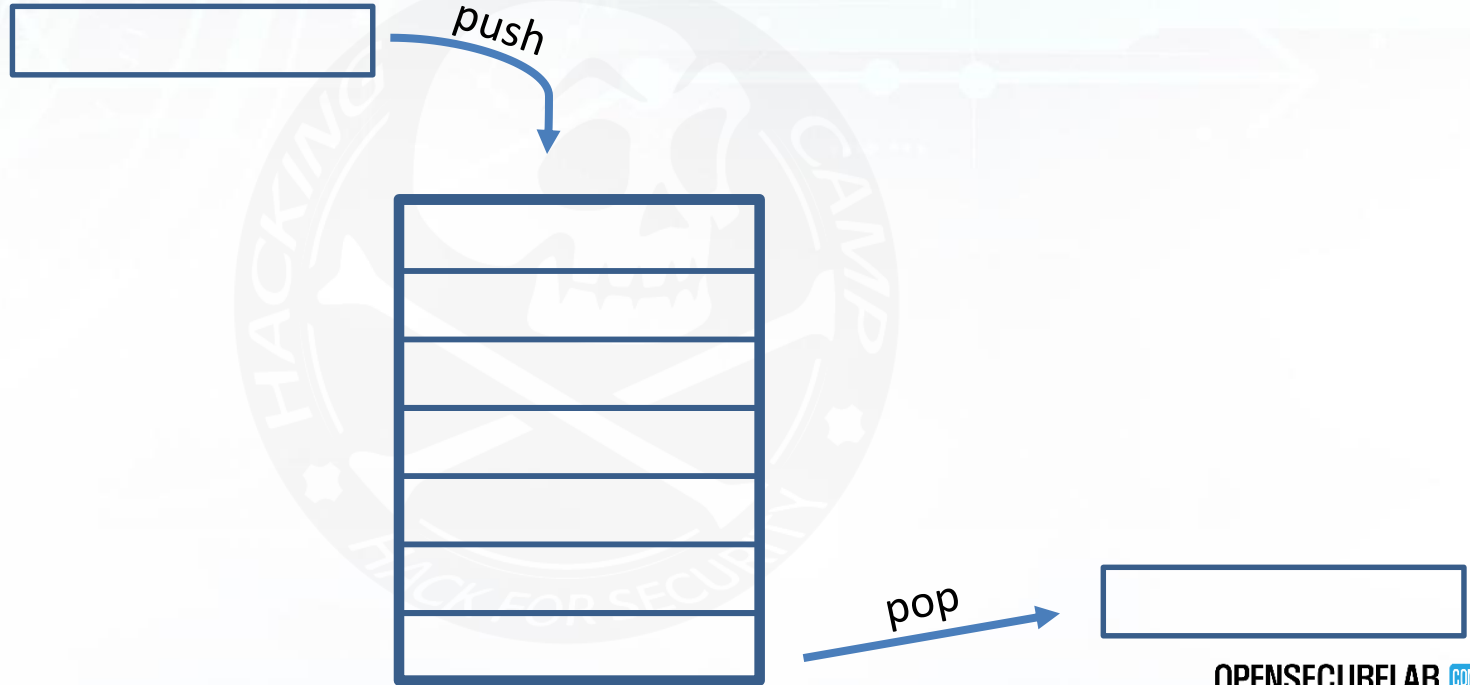
- Stack



Message Queue

- Queue

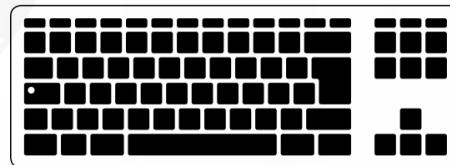
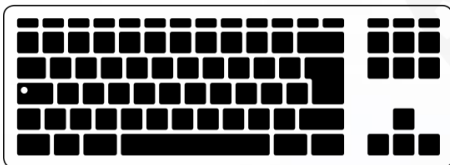
FIFO



Message Queue

Hle olrl!Wdo

Hello World!



SetWindowsHookEx

```
HHOOK WINAPI SetWindowsHookEx(  
    _In_ int idHook,  
    _In_ HOOKPROC lpfn,  
    _In_ HINSTANCE hMod,  
    _In_ DWORD dwThreadId  
);
```

```
HHOOK WINAPI SetWindowsHookEx(  
    _In_ int WH_KEYBOARD,  
    _In_ HOOKPROC keylog,  
    _In_ HINSTANCE hIns,  
    _In_ DWORD 0  
);
```

SetWindowsHookEx

Main Program

```
int main(void){  
    LoadLibraryA(DLL);  
    DLL.Hooking();  
    DLL.UnHooking();  
    FreeLibrary(DLL);  
    return 0;  
}
```

DLL

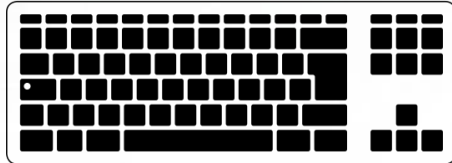
```
LRESULT CALLBACK keylog(...){...}  
extern void Hooking(void){  
    SetWindowsHookEx();  
}  
extern void UnHooking(void){  
    UnhookWindowsHookEx();  
}
```

KeyLogging 시연



Chrome
Message Queue

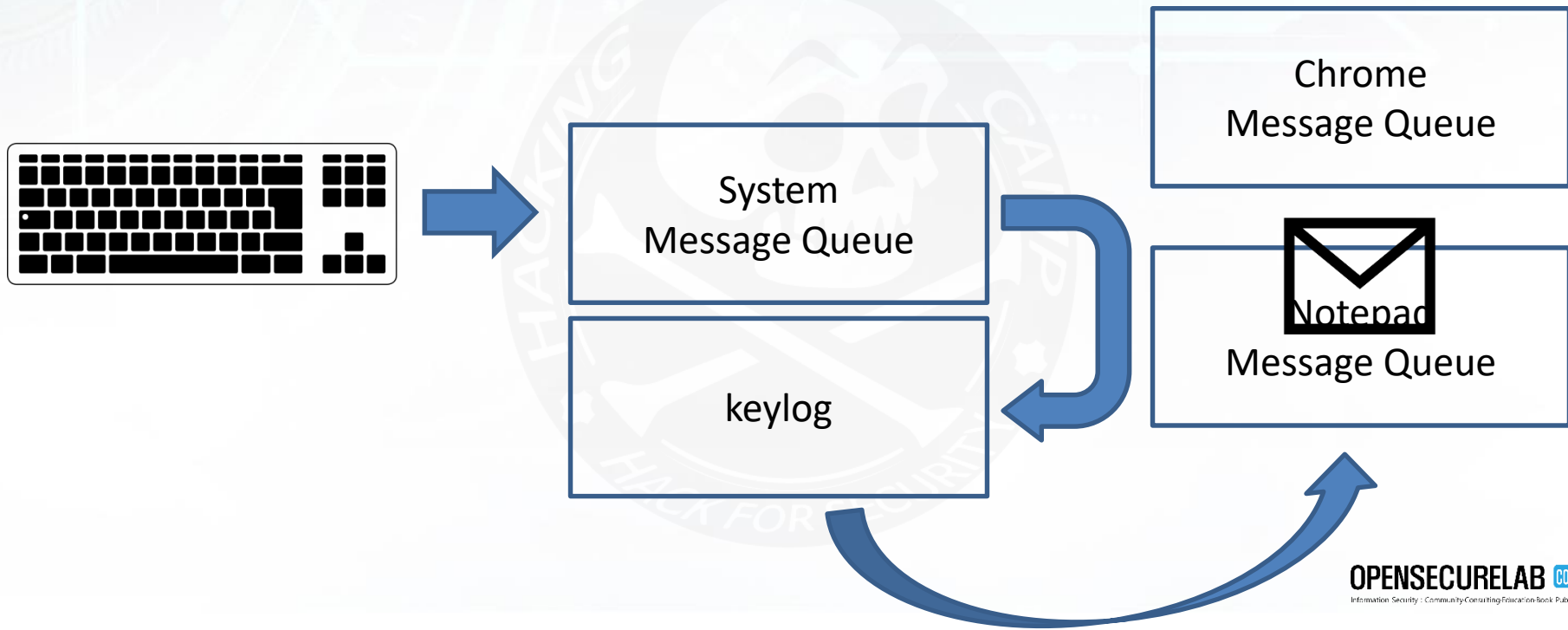
Notepad
Message Queue



System
Message Queue



KeyLogging 시연





KeyLogging 시연



KeyLogging 시연



김민석

Kakao ID: minjk1213

Mail: minjk1213@gmail.com