

Forum: [Hack Forums](#)

Thread: [Handles in Window](#)

Abathur - April 23, 2016, 5:09 pm

Is there another way of getting a handle on an application other than the method of using the FindWindow function?

I do it this way: `HWND hWnd = FindWindow(0, Calculator);`

Is there another way of doing this.

EwilDave - April 23, 2016, 11:06 pm

What about using [EnumDesktopWindows\(\)](#)?

You'd have to define a callback function, and then use [GetWindowText\(\)](#) to search for a specific window

This method seems a bit more complex than just using FindWindow()

Abathur - April 23, 2016, 11:21 pm

(Apr 23, 2016 11:06 PM)EwilDave Wrote: [\[CITE\]](#) What about using [EnumDesktopWindows\(\)](#)?

You'd have to define a callback function, and then use [GetWindowText\(\)](#) to search for a specific window

This method seems a bit more complex than just using FindWindow()

Yes you are right the other method is more preferable. Also what's up? been a while.

Irritable - April 24, 2016, 1:19 am

(Apr 23, 2016 05:09 PM)Beacon Wrote: [\[CITE\]](#) Is there another way of getting a handle on an application other than the method of using the FindWindow function?

I do it this way: `HWND hWnd = FindWindow(0, Calculator);`

Is there another way of doing this.

[https://msdn.microsoft.com/en-us/library/windows/desktop/ms633515\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms633515(v=vs.85).aspx)

Tons of functions for accomplishing that task.

Phizo - April 25, 2016, 6:07 am

I like to use CreateToolhelp32Snapshot to find the PID and then call OpenProcess.

Here is a function I use for getting a process handle from it's name:

PHP Code

```
<?php
```

```
#include <Windows.h>
```

```
#include <TlHelp32.h>
```

```
HANDLE GetProcessByName(LPCWSTR ProcName, DWORD dwDesiredAccess)
```

```

{
    HANDLE hProcess = NULL;
    PROCESSENTRY32 pe = {0};
    pe.dwSize = sizeof(pe);

    HANDLE hSnapshot = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0);
    if (hSnapshot == INVALID_HANDLE_VALUE)
    {
        return NULL;
    }

    if (Process32First(hSnapshot, &pe) == TRUE)
    {
        do
        {
            if (lstrcmpW(ProcName, pe.szExeFile) == 0)
            {
                hProcess = OpenProcess(dwDesiredAccess, FALSE, pe.th32ProcessID);
                break;
            }
        } while (Process32Next(hSnapshot, &pe));
    }

    CloseHandle(hSnapshot);
    return hProcess;
}

```

dwDesiredAccess is passed straight to OpenProcess, so it'd pay to read the MSDN page for that to know the possible flags, here's the setup I use for DLL injection:

PHP Code

```
<?php
```

```

HANDLE hProcess = GetProcessByName(L"calc.exe", PROCESS_QUERY_INFORMATION |
PROCESS_VM_OPERATION | PROCESS_VM_WRITE | PROCESS_VM_READ);

```

Note: If there is more than one instance of a process (IE: You open calc.exe twice), this function will only return the first instance it encounters, likely the one with the lowest PID.

#HackedByKubrickian

Mouse? - April 25, 2016, 7:14 am

(Apr 25, 2016 06:07 AM)Phizo Wrote: [\[CITE\]](#) I like to use CreateToolhelp32Snapshot to find the PID and then call OpenProcess.

Here is a function I use for getting a process handle from it's name:

PHP Code

```
<?php
```

```
#include <Windows.h>
```

```
#include <TIHelp32.h>
```

```

HANDLE GetProcessByName(LPCWSTR ProcName, DWORD dwDesiredAccess)
{
    HANDLE hProcess = NULL;
    PROCESSENTRY32 pe = {0};

```

```

pe.dwSize = sizeof(pe);

HANDLE hSnapshot = CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0);
if (hSnapshot == INVALID_HANDLE_VALUE)
{
    return NULL;
}

if (Process32First(hSnapshot, &pe) == TRUE)
{
    do
    {
        if (lstrcmpW(ProcName, pe.szExeFile) == 0)
        {
            hProcess = OpenProcess(dwDesiredAccess, FALSE, pe.th32ProcessID);
            break;
        }
    } while (Process32Next(hSnapshot, &pe));
}

CloseHandle(hSnapshot);
return hProcess;
}

```

dwDesiredAccess is passed straight to OpenProcess, so it'd pay to read the MSDN page for that to know the possible flags, here's the setup I use for DLL injection:

PHP Code

```
<?php
```

```

HANDLE hProcess = GetProcessByName(L"calc.exe", PROCESS_QUERY_INFORMATION |
PROCESS_VM_OPERATION | PROCESS_VM_WRITE | PROCESS_VM_READ);

```

Note: If there is more than one instance of a process (IE: You open calc.exe twice), this function will only return the first instance it encounters, likely the one with the lowest PID.

#HackedByKubrickianThat's not getting window handles at all. That's enumerating processes. Please read the thread and stay on topic.

(Unless OP's example of FindWindow was misplaced)

Abathur - May 13, 2016, 11:59 pm

Phizo that is what I was looking for thanks

0xDEAD10CC - May 14, 2016, 1:35 pm

(May 13, 2016 11:59 PM)NullObject Wrote: [\[CITE\]](#) Phizo that is what I was looking for thanks

In that case you don't know how to properly ask the question in regards to what you're looking for. A process HANDLE has nothing to do with a window handle.

Aker15 - May 14, 2016, 5:59 pm

(May 13, 2016 11:59 PM)NullObject Wrote: [\[CITE\]](#) Phizo that is what I was looking for thanks

I don't know why you would even say that as I sent you that exact code before anyone even posted on this thread, as I knew that's what you were looking for, now you either lost it, or I don't get it..... Except my code had the terminate process API call in it, which is what you were looking for, now this very simple code you could've googled as it is posted over 500,000 times everywhere from google.

Abathur - May 15, 2016, 11:16 am

(May 14, 2016 05:59 PM)Aker15 Wrote: [\[CITE\]](#) I don't know why you would even say that as I sent you that exact code before anyone even posted on this thread, as I knew that's what you were looking for, now you either lost it, or I don't get it..... Except my code had the terminate process API call in it, which is what you were looking for, now this very simple code you could've googled as it is posted over 500,000 times everywhere from google.

Questions maybe simple for a lot of people here. Just started really learning the winapi, so I can understand people on the C forum would look at this question and laugh. I have done my research just for the record. Want to verify with others that's all. I have told you Aker15 that I use Python and just started getting back into C.

We need more people like some on this thread that just answers the question (or not) and move on. Can't hate on someone for asking or learning, because this is the way I get better.

Aker15 - May 15, 2016, 3:49 pm

(May 15, 2016 11:16 AM)NullObject Wrote: [\[CITE\]](#) Questions maybe simple for a lot of people here. Just started really learning the winapi, so I can understand people on the C forum would look at this question and laugh. I have done my research just for the record. Want to verify with others that's all. I have told you Aker15 that I use Python and just started getting back into C.

We need more people like some on this thread that just answers the question (or not) and move on. Can't hate on someone for asking or learning, because this is the way I get better. But I sent you this code and told you how it worked weeks ago, that is my point.

Abathur - May 15, 2016, 3:53 pm

(May 15, 2016 03:49 PM)Aker15 Wrote: [\[CITE\]](#) But I sent you this code and told you how it worked weeks ago, that is my point.

That's fine but the rating you gave me was a little mean don't you think =/