1110111011011

1001100

110011001100

10101010101010

00011001001

DOS , DDOS

ataki sieciowe

Hacking i Cyberbezpieczeństwo | Giganci Programowania

Opracowanie: Michał Suchoń

Przypomnienie

1. Co to **file floading**, jak działa?
2. W jakim celu stosuje się **tryb invisible** przy tworzeniu wirusów?

Przypomnienie

1. Co to **file floading**, jak działa?
   rodzaj wirusa, który tworzy nieskończenie wiele plików bądź folderów na dysku, powodując zapełnienie pamięci niepotrzebnymi danymi

2. W jakim celu stosuje się **tryb invisible** przy tworzeniu wirusów?

Przypomnienie

1. Co to **file floading**, jak działa?
   rodzaj wirusa, który tworzy nieskończenie wiele plików bądź folderów na dysku, powodując zapełnienie pamięci niepotrzebnymi danymi

2. W jakim celu stosuje się **tryb invisible** przy tworzeniu wirusów?
   aby ukryć działanie wirusa, uniemożliwić jego wyłączenie

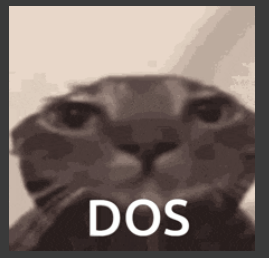
W hackowaniu nie tylko włamywanie się do systemów jest ważne, ale też utrudnianie działania

Dlaczego?

Blokada usług [DoS]

denial of service

atak na system komputerowy lub usługę sieciową celem uniemożliwienia działania, np. przez zatrzymanie jej




flooding pakietów do sieci, przeciążając pasmo hosta
wyczerpanie wolnych portów na serwerze WWW / FTP
DoS
przykłady
wykorzystanie błędu, który zablokuje działanie aplikacji
zapełnienie systemu plików, aby dalsze dodawanie informacji było niemożliwe

Zdalny DoS?

https://webstresser.org/

WYZWANIE NR 1

Spróbujmy zDoS'ować następujące strony:

a) **wp.pl**
b) **testsite.cytr.us**
c) **gov.pl**

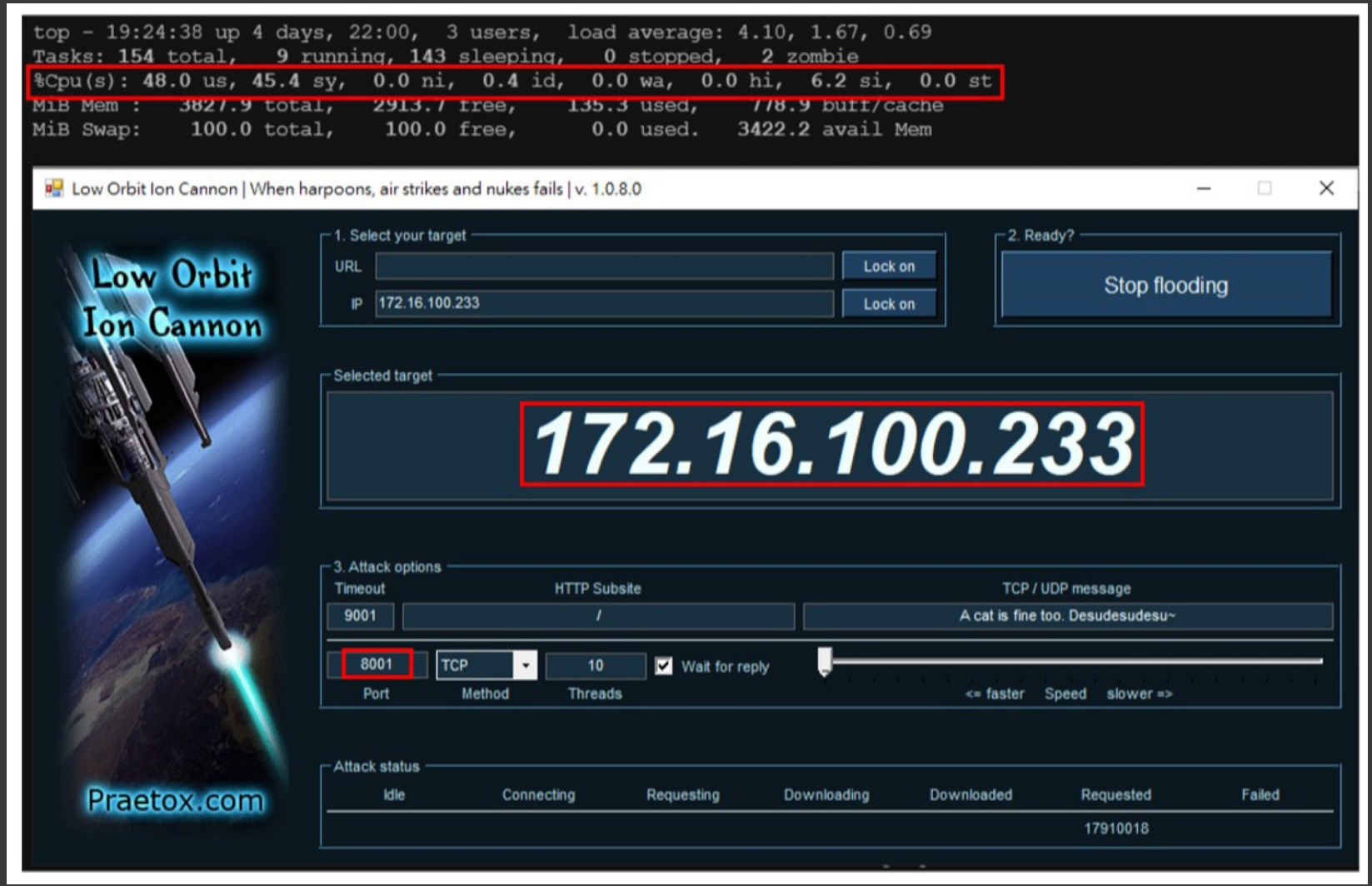
Jakie były rezultaty? Czy w każdym przypadku DoS przebiegł pomyślnie? Jeśli nie, dlaczego?

Czy istnieją gotowe programy do DoS’owania?

Low Orbit Ion Cannon (LOIC)

Niskoorbitalne Działo Jonowe

narzędzie scriptkiddy



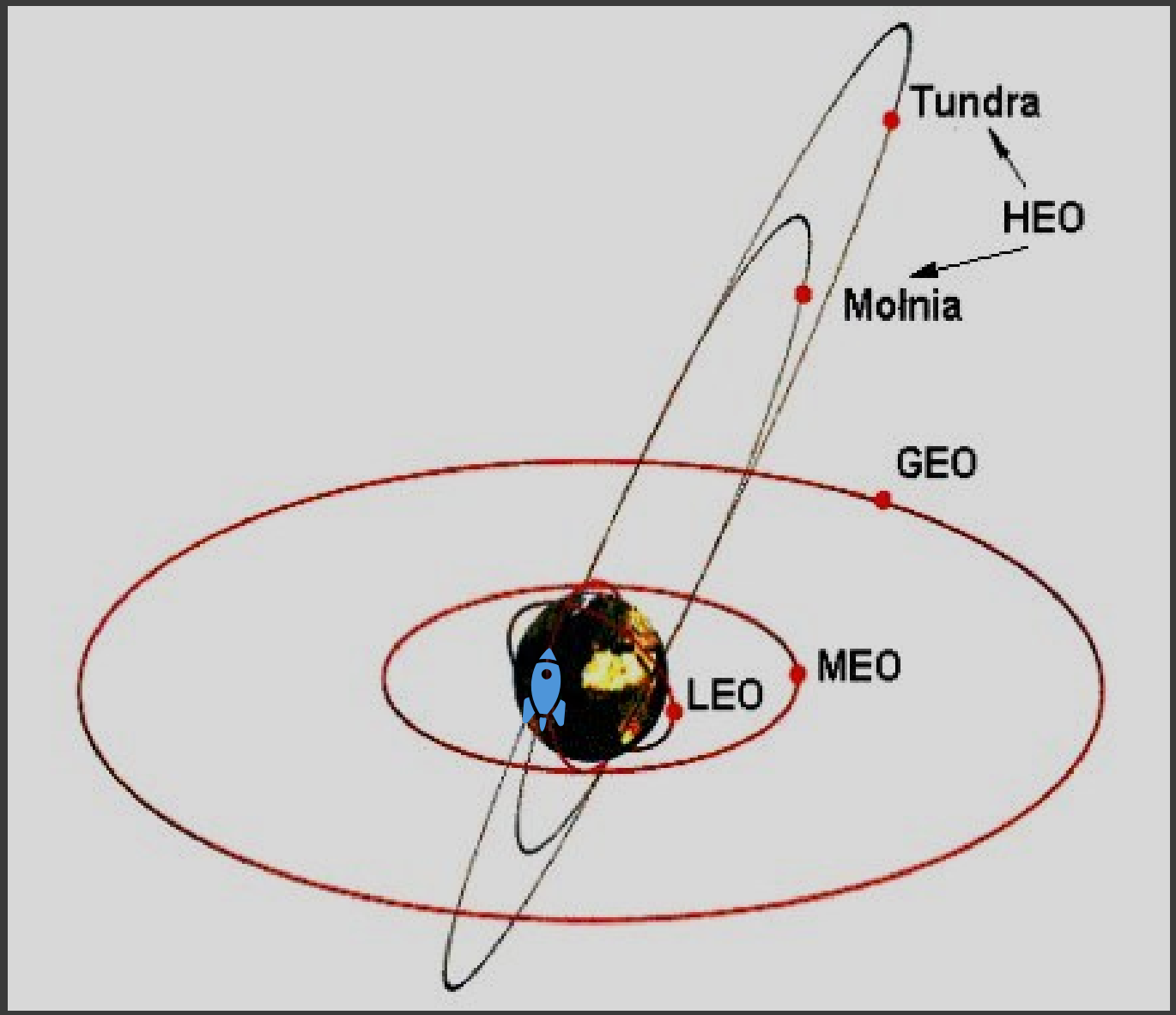
https://github.com/NewEraCracker/LOIC

Skąd ta nazwa?

Coś dla fanów **Sci-Fi**!

Cechy LOIC:

- napisany w c#
- na licencji open source
- interfejs aplikacji pozwala na szeroką konfigurację i atak zarówno przez IP jak i adres domenowy, również z uwzględnieniem konkretnego protokołu i portu
- pozwala na zarządzanie, ile wątków procesora chcemy przeznaczyć na atak
- był często używany na „chanach” dla zabawy lub złośliwego atakowania stron



Rozwinięciem ataku DoS jest DDoS. Czym się różni?

DDoS

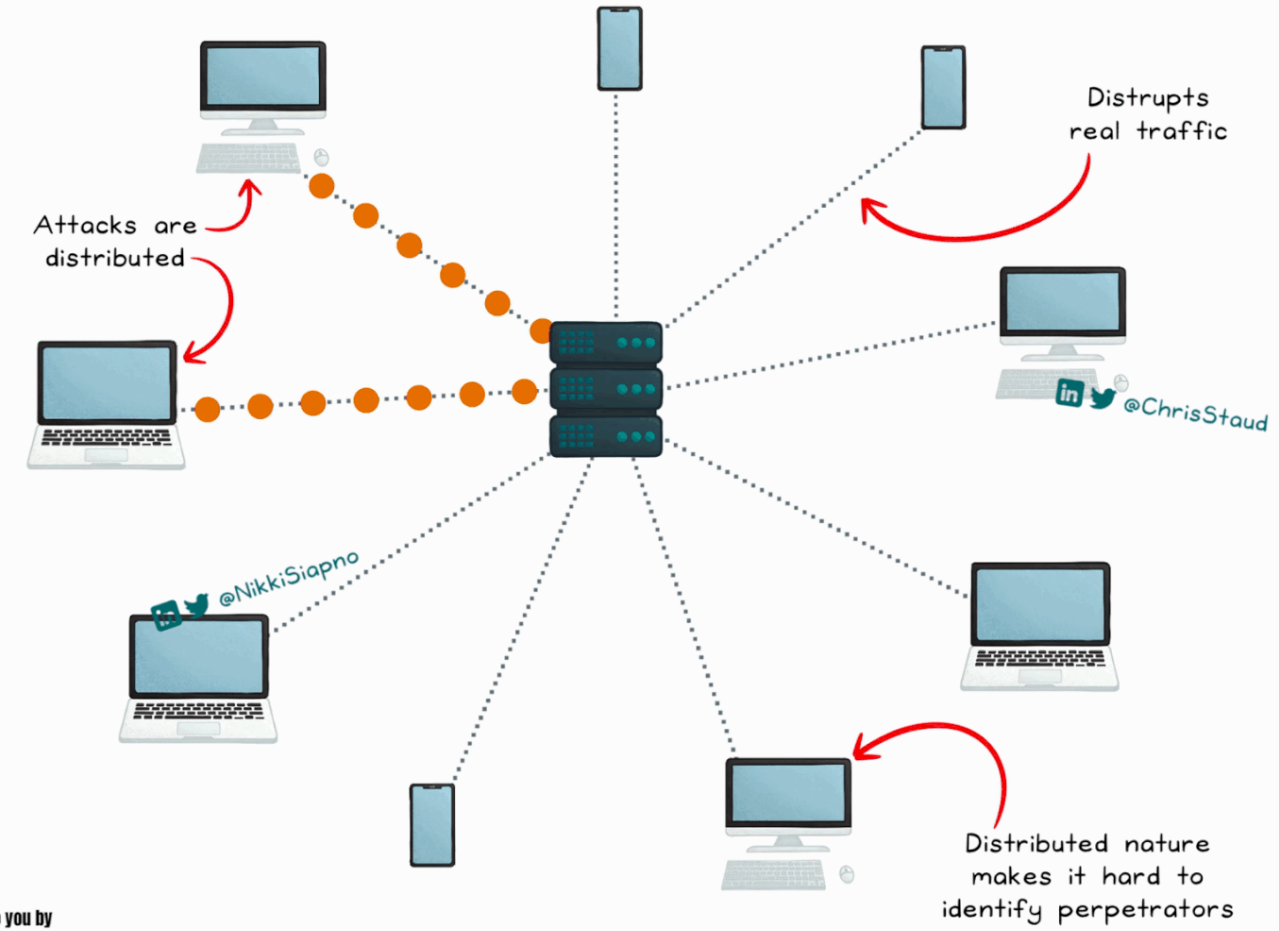
distributed denial of service

rozproszona blokada usługi, atak działający na zasadzie DoS z tą różnicą, że wykorzystuje się do tego wiele komputerów „zombie” – najczęściej zhackowane, bez wiedzy ich właścicieli -> tzw. **farmy urządzeń (zombie)**

DDoS Attacks

by levelupcoding.com

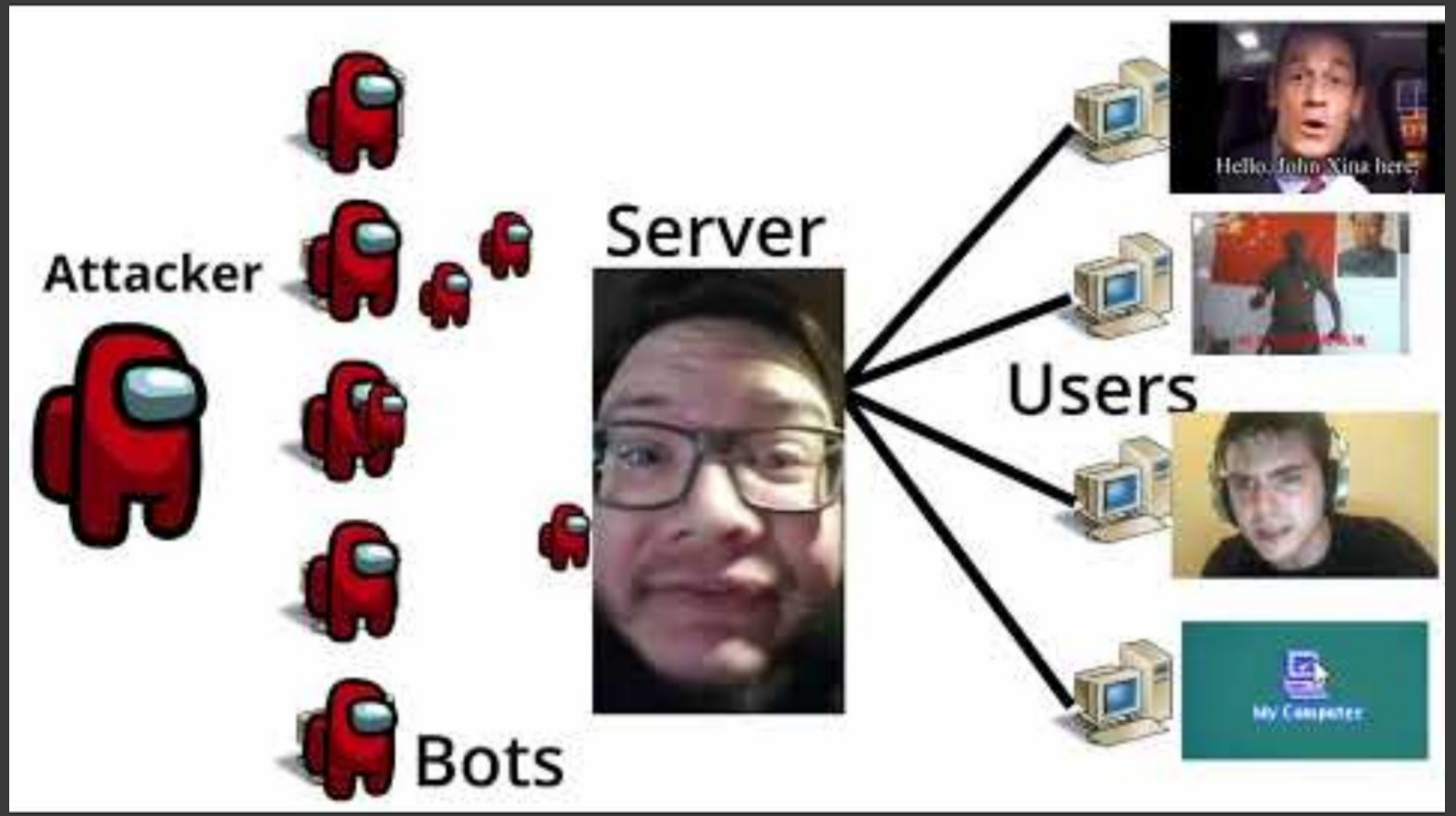
Explained



Brought to you by

LEVEL UP CODING

@NikkiSiapno @ChrisStaud



ŹRÓDŁO:
YouTube: https://www.youtube.com/watch?v=r3bEjsv9JFw

Masowy DDoS na Dyn za pomocą IoT -> 2016

https://www.youtube.com/watch?v=GUeeR4B6V_A https://thehackernews.com/2016/10/iot-dyn-ddos-attack.html

„Mądra lodówka” exploitem?

https://www.shodan.io/search?query=iot

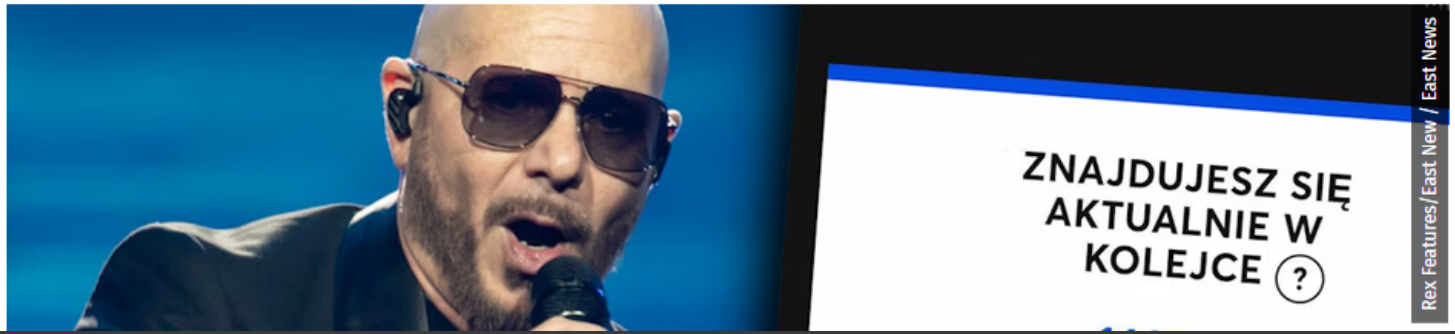
Czy za DDoS zawsze odpowiedzialni są hackerzy?

Gigantyczne zainteresowanie koncertem Pitbulla w Polsce. "Powinni przenieść na stadion"

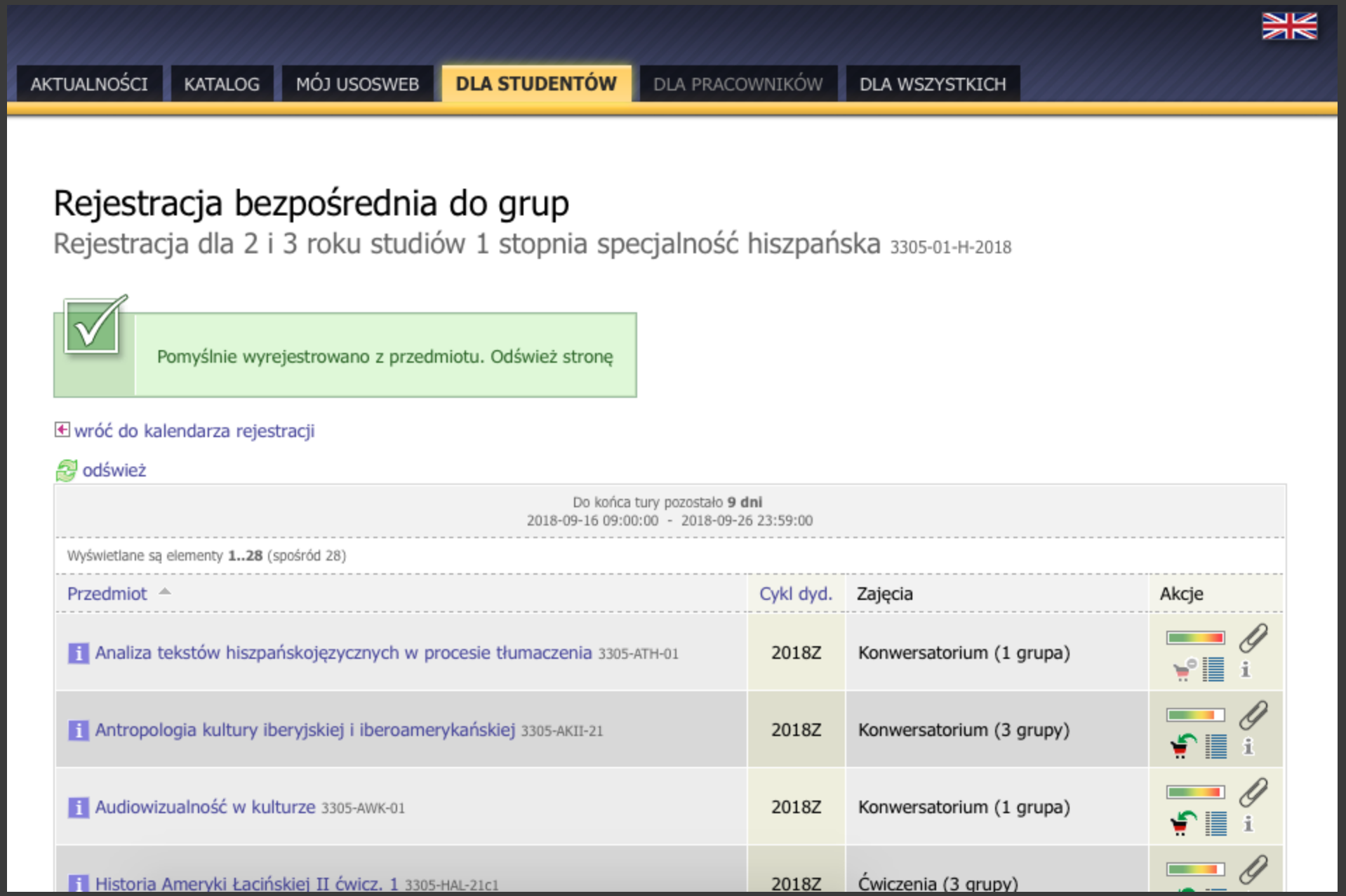
Dziennikarze Onet Kultura

27 lutego 2025, 12:10

Polacy czekali na ten koncert od ponad dekady. Dzisiaj oficjalnie ruszyła sprzedaż biletów na krakowski występ Pitbulla. W wirtualnej kolejce tysiące fanów walczyło o wejściówki. Wielu z nich wiedziało, że może im się to nie udać. "Takiego zamieszania już dawno nie było. Na szczęście złapałem do koszyka wymarzone trybuny" — mówi w rozmowie z Onetem jeden z zainteresowanych.



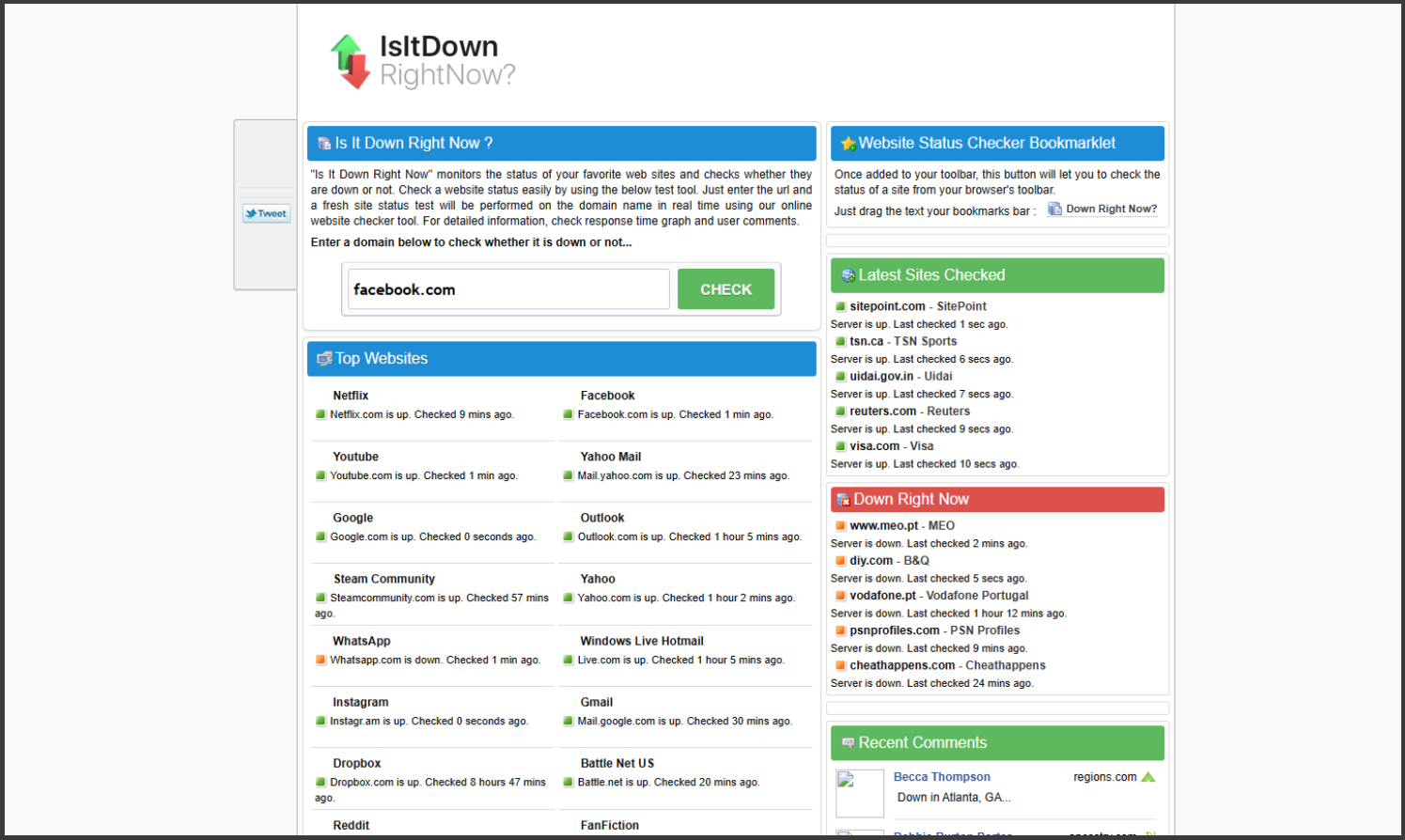
https://kultura.onet.pl/muzyka/wiadomosci/gigantyczne-zainteresowanie-koncertem-pitbulla-w-polsce-powinni-przeniesc-na-stadion/9qehtrb


AKTUALNOŚCI
KATALOG
MÓJ USOSWEB
DLA STUDENTÓW
DLA PRACOWNIKÓW
DLA WSZYSTKICH
Rejestracja bezpośrednia do grup
Rejestracja dla 2 i 3 roku studiów 1 stopnia specjalność hiszpańska 3305-01-H-2018
Pomyślnie wyrejestrowano z przedmiotu. Odśwież stronę
wróć do kalendarza rejestracji
odśwież
Do końca tury pozostało 9 dni
2018-09-16 09:00:00 - 2018-09-26 23:59:00
Wyświetlane są elementy 1..28 (spośród 28)
Przedmiot
Cykl dyd.
Zajęcia
Akcje
Analiza tekstów hiszpańskojęzycznych w procesie tłumaczenia 3305-ATH-01
2018Z
Konwersatorium (1 grupa)
Antropologia kultury iberyjskiej i iberoamerykańskiej 3305-AKII-21
2018Z
Konwersatorium (3 grupy)
Audiowizualność w kulturze 3305-AWK-01
2018Z
Konwersatorium (1 grupa)
Historia Ameryki Łacińskiej II ćwicz. 1 3305-HAL-21c1
2018Z
Ćwiczenia (3 grupy)

Jakie sytuacje są „korzystne” na DDoS?

Czy DDoS się udał?

https://www.isitdownrightnow.com/



WYZWANIE NR 2 i 3

Napiszmy własnego DDoS'a!

a) Za pomocą C# - wyzwanie nr 2
b) Za pomocą C++ - wyzwanie nr 3

wyzwanie nr 2

DDoS cz. 1- C++

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

KROK 2: Wprowadzamy następujący **kod:**

https://pastebin.com/0K6JCDJ6

```cpp
#include <iostream>
#include <thread>
#include <chrono>

#pragma comment(lib, "ws2_32.lib")


int main() {
    WSADATA wsaData;

    if (WSAStartup(MAKEWORD(2, 2), &wsaData) != 0) {
        std::cerr << "WSAStartup failed.\n";
        return 1;
    }

    sockaddr_in serverAddr;
    serverAddr.sin_family = AF_INET;
    serverAddr.sin_port = htons(11000);
    serverAddr.sin_addr.s_addr = inet_addr("192.168.2.255");

    const char* text = "Hello";
    int textLen = strlen(text);

    while (true) {
        SOCKET sock = socket(AF_INET, SOCK_DGRAM, IPPROTO_UDP);
        if (sock == INVALID_SOCKET) {
            std::cerr << "Socket creation failed.\n";
            break;
        }

        BOOL broadcast = TRUE;
        if (setsockopt(sock, SOL_SOCKET, SO_BROADCAST, (char*)&broadcast, sizeof(broadcast)) < 0) {
            std::cerr << "setsockopt failed.\n";
            closesocket(sock);
            break;
        }

        int sent = sendto(sock, text, textLen, 0, (sockaddr*)&serverAddr, sizeof(serverAddr));
        if (sent == SOCKET_ERROR) {
            std::cerr << "sendto failed. Error: " << WSAGetLastError() << "\n";
        }
        else {
            std::cout << "Sent: " << text << "\n";
        }

        closesocket(sock);
        std::this_thread::sleep_for(std::chrono::seconds(1));
    }

    WSACleanup();
    return 0;
```

wyzwanie nr 3

DDoS cz. 2- C#

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

KROK 2: Wprowadzamy następujący **kod:**

https://pastebin.com/Yqe94gV7

```
using System;
using System.Net;
using System.Net.Sockets;
using System.Text;

namespace ConsoleApp1
{
    class Program
    {
        static void Main(string[] args)
        {
            int counter = 0;
            while (true)
            {
                try
                {
                    Socket sock = new Socket(
                        AddressFamily.InterNetwork,
                        SocketType.Dgram,
                        ProtocolType.Udp);

                    IPAddress serverAddr = IPAddress.Parse("192.168.2.255");
                    IPEndPoint endPoint = new IPEndPoint(serverAddr, 11000);

                    string text = "Hello " + counter;
                    byte[] send_buffer = Encoding.ASCII.GetBytes(text);

                    sock.SetSocketOption(SocketOptionLevel.Socket, SocketOptionName.Broadcast, true);
                    sock.SendTo(send_buffer, endPoint);

                    Console.WriteLine($"Wysłano: {text}");
                    sock.Close();

                    counter++;
                    System.Threading.Thread.Sleep(1000);
                }
                catch (Exception ex)
                {
                    Console.WriteLine($"Błąd: {ex.Message}");
                }
            }
        }
    }
}
```

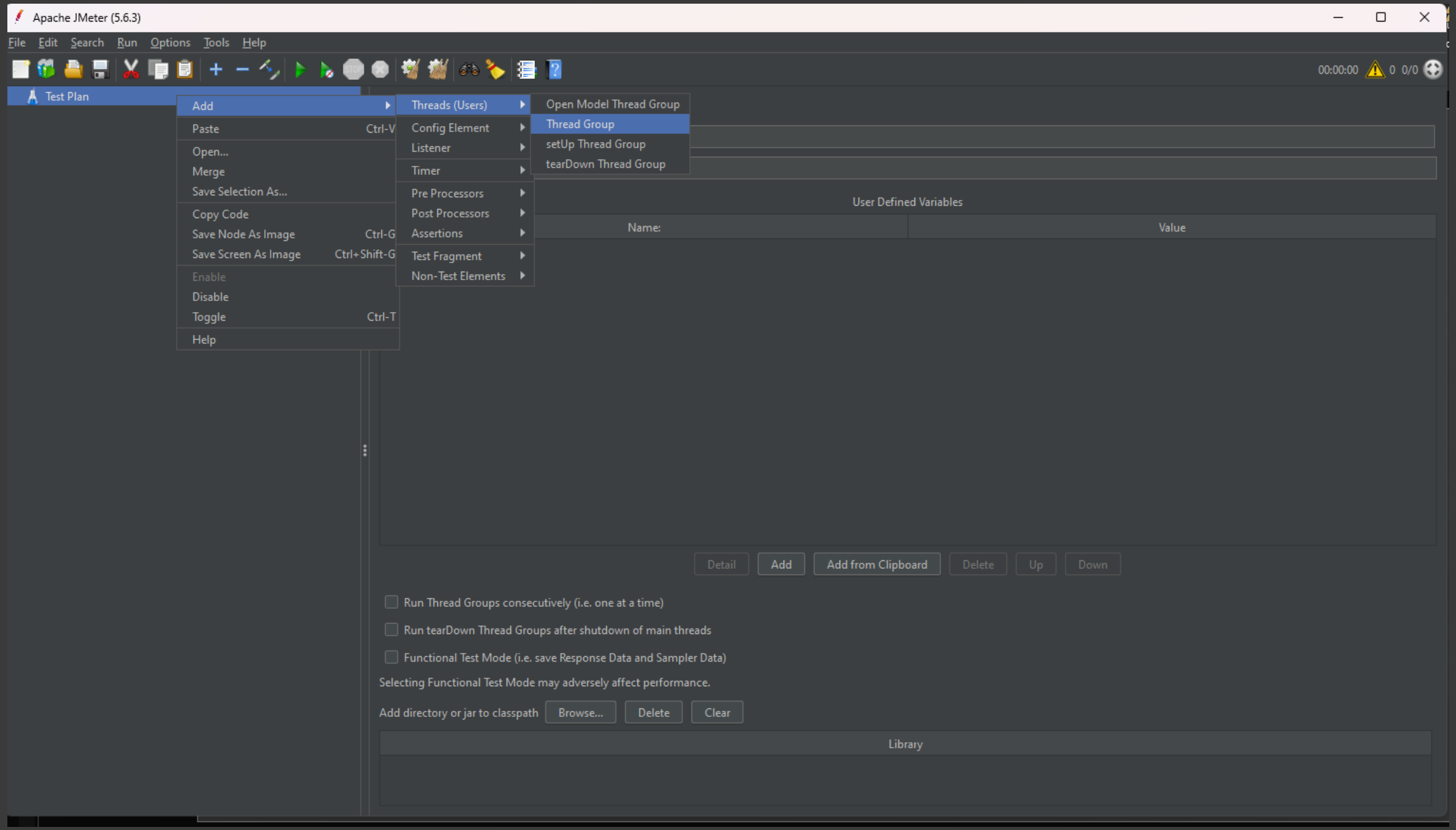
Czy ważne jest testowanie aplikacji przez twórców?

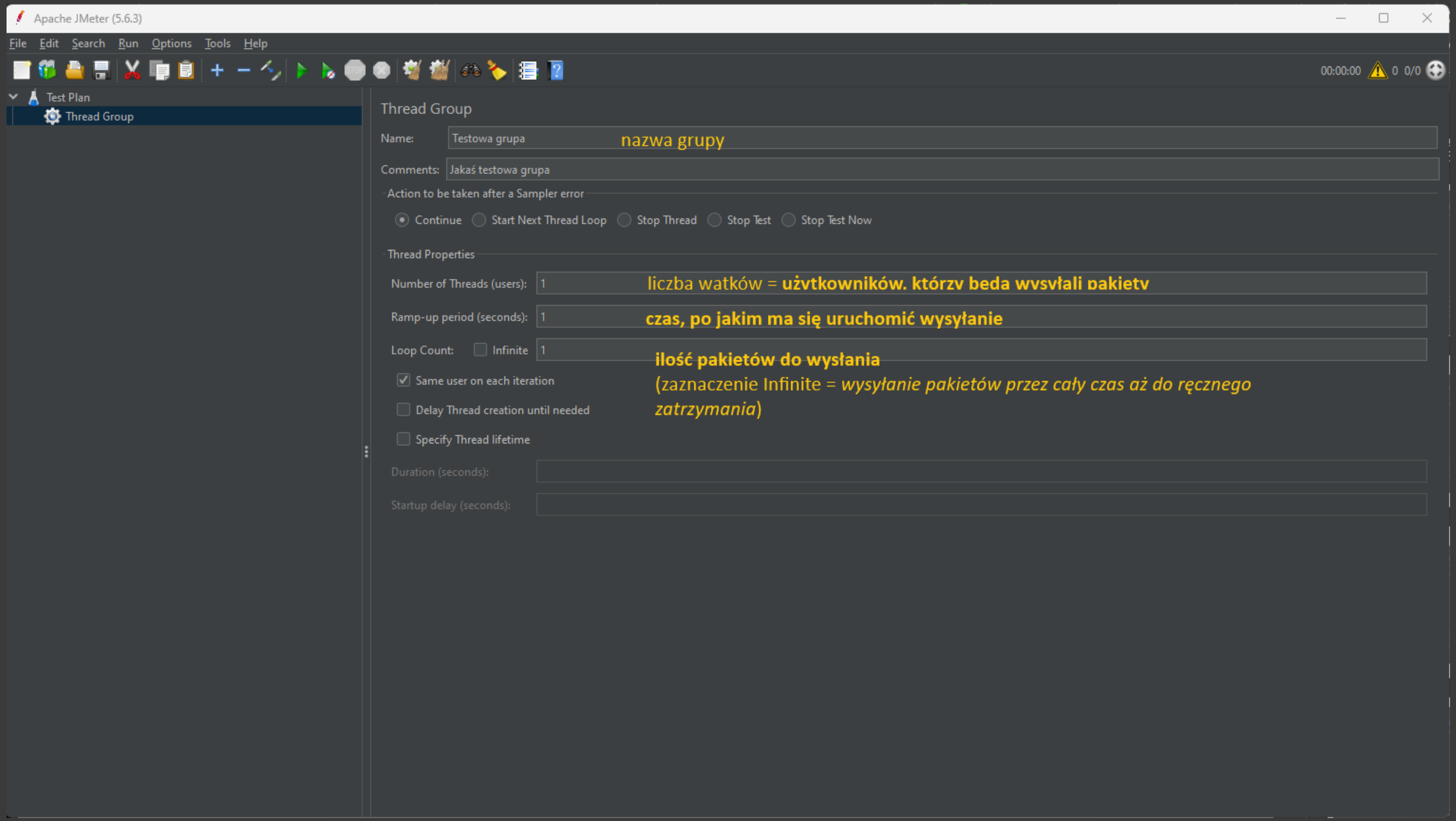
WYZWANIE NR 4

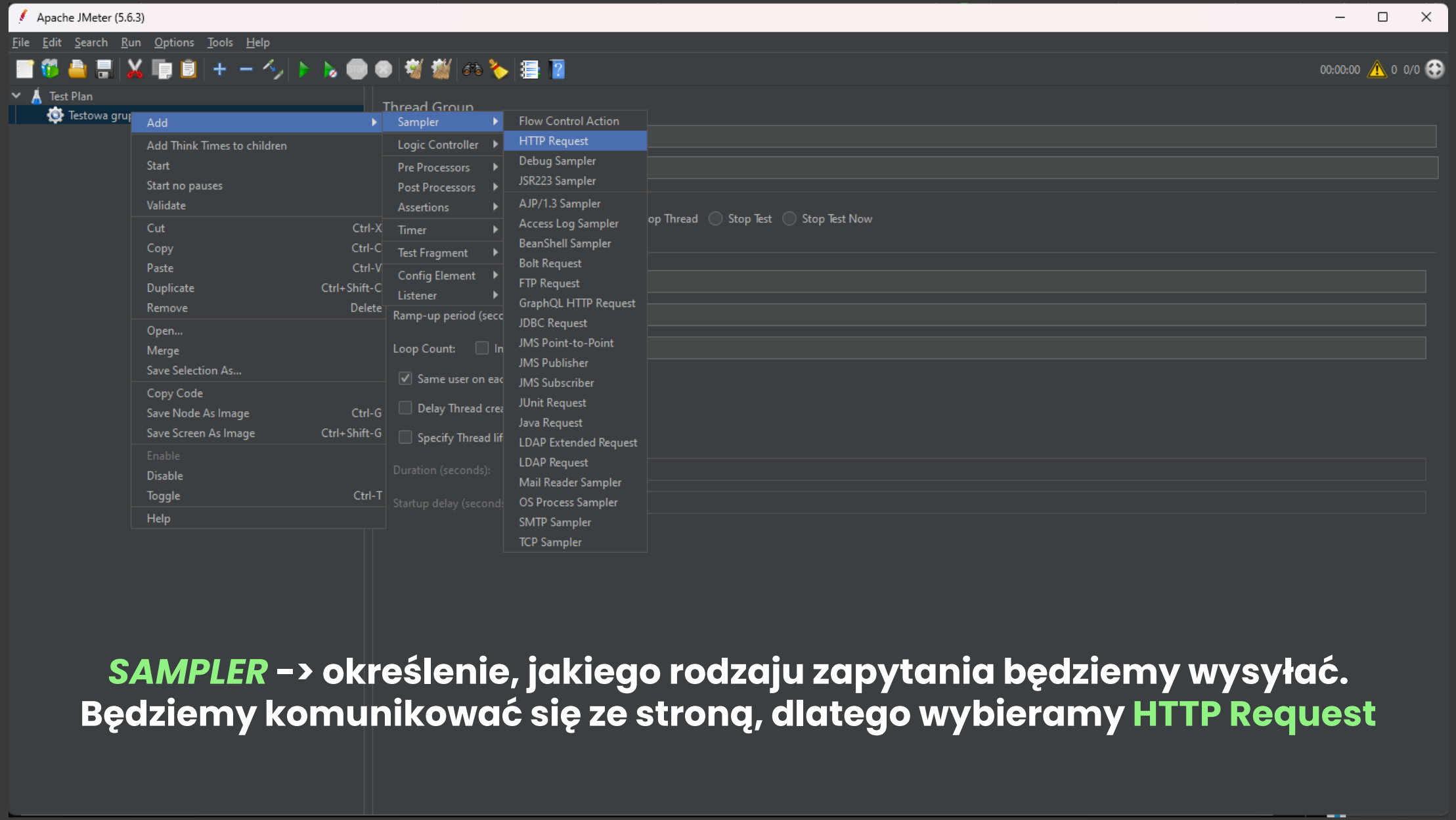
Przeprowadźmy atak DDoS za pomocą aplikacji Apache JMeter

Do ataku potrzebujemy mieć zainstalowaną na komputerze Javę oraz sam wypakowany folder z aplikacją.

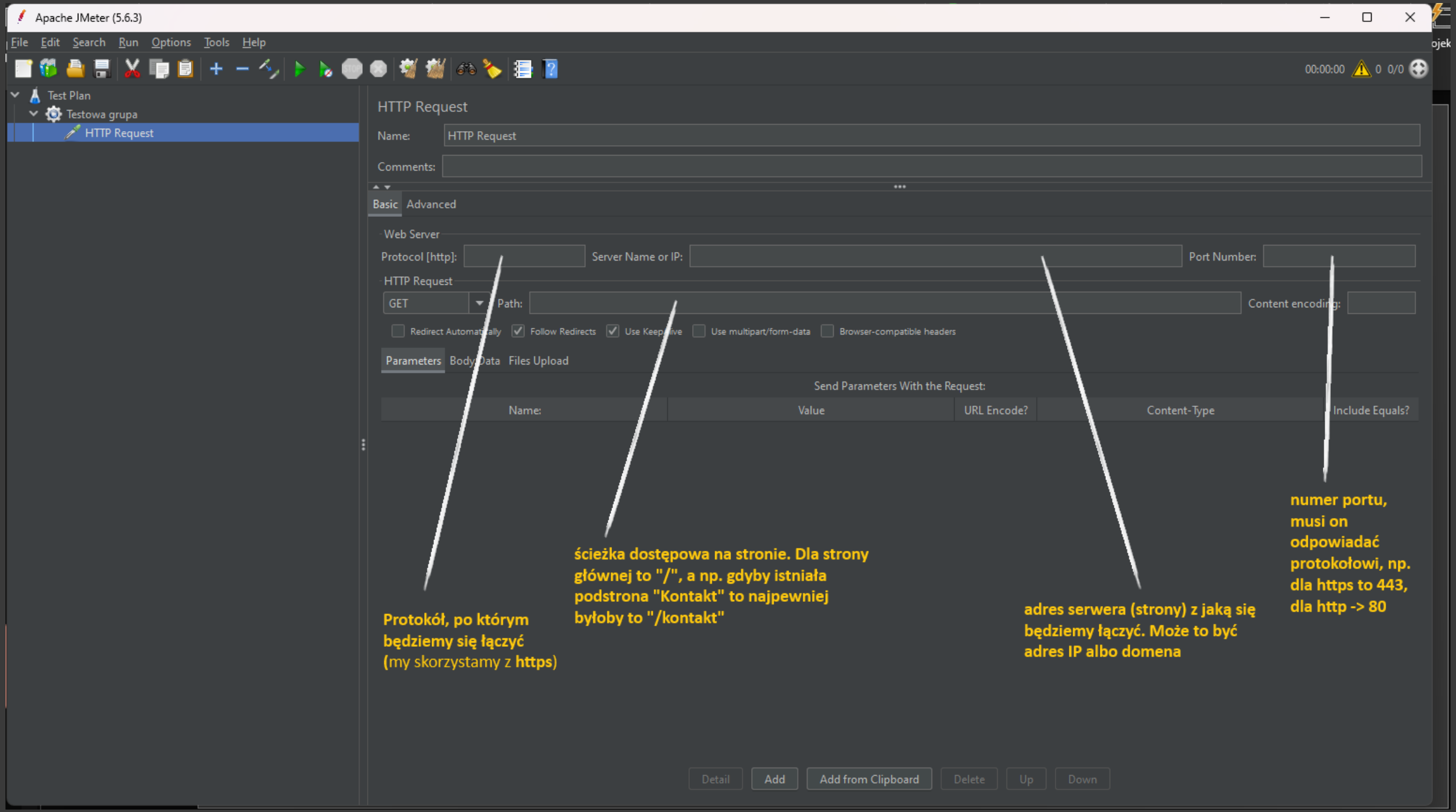
Uruchomienie: folder *bin* > uruchamiamy jmeter.bat
(uruchomi się początkowo wiersz poleceń, którego nie zamykamy!)

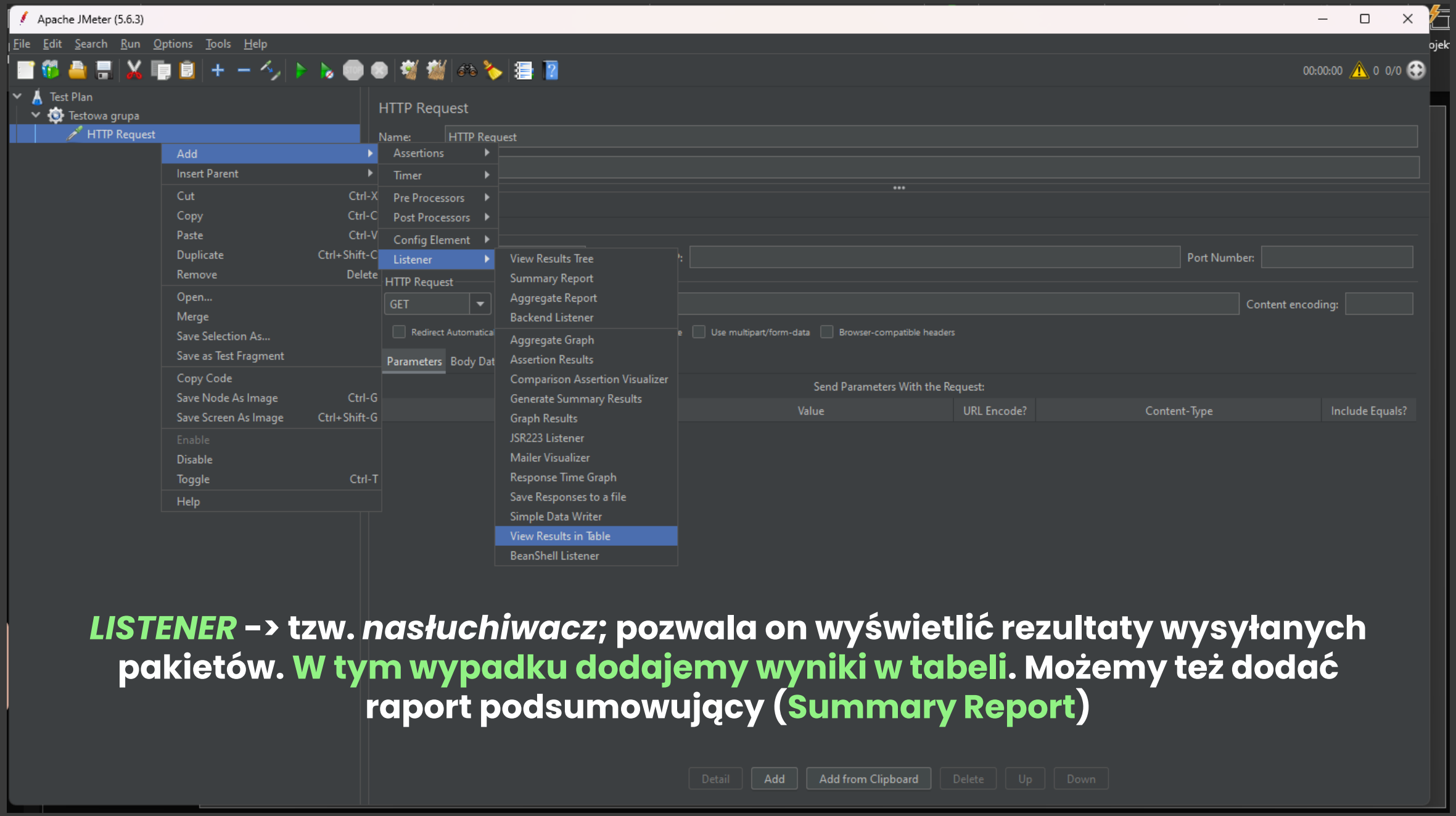

Apache JMeter (5.6.3)
File Edit Search Run Options Tools Help
00:00:00 0 0/0
Test Plan
Add
Paste Ctrl-V
Open...
Merge
Save Selection As...
Copy Code
Save Node As Image Ctrl-G
Save Screen As Image Ctrl+Shift-G
Enable
Disable
Toggle Ctrl-T
Help
Threads (Users)
Config Element
Listener
Timer
Pre Processors
Post Processors
Assertions
Test Fragment
Non-Test Elements
Open Model Thread Group
Thread Group
setUp Thread Group
tearDown Thread Group
User Defined Variables
Name:
Value
Detail
Add
Add from Clipboard
Delete
Up
Down
Run Thread Groups consecutively (i.e. one at a time)
Run tearDown Thread Groups after shutdown of main threads
Functional Test Mode (i.e. save Response Data and Sampler Data)
Selecting Functional Test Mode may adversely affect performance.
Add directory or jar to classpath
Browse...
Delete
Clear
Library


Apache JMeter (5.6.3)
File Edit Search Run Options Tools Help
00:00:00 0 0/0
Test Plan
Thread Group
Thread Group
Name: Testowa grupa
nazwa grupy
Comments: Jakaś testowa grupa
Action to be taken after a Sampler error
Continue Start Next Thread Loop Stop Thread Stop Test Stop Test Now
Thread Properties
Number of Threads (users): 1
liczba watków = użytkowników, którzy beda wysyłali pakiety
Ramp-up period (seconds): 1
czas, po jakim ma się uruchomić wysyłanie
Loop Count: Infinite 1
ilość pakietów do wysłania
(zaznaczenie Infinite = wysyłanie pakietów przez cały czas aż do ręcznego zatrzymania)
Same user on each iteration
Delay Thread creation until needed
Specify Thread lifetime
Duration (seconds):
Startup delay (seconds):

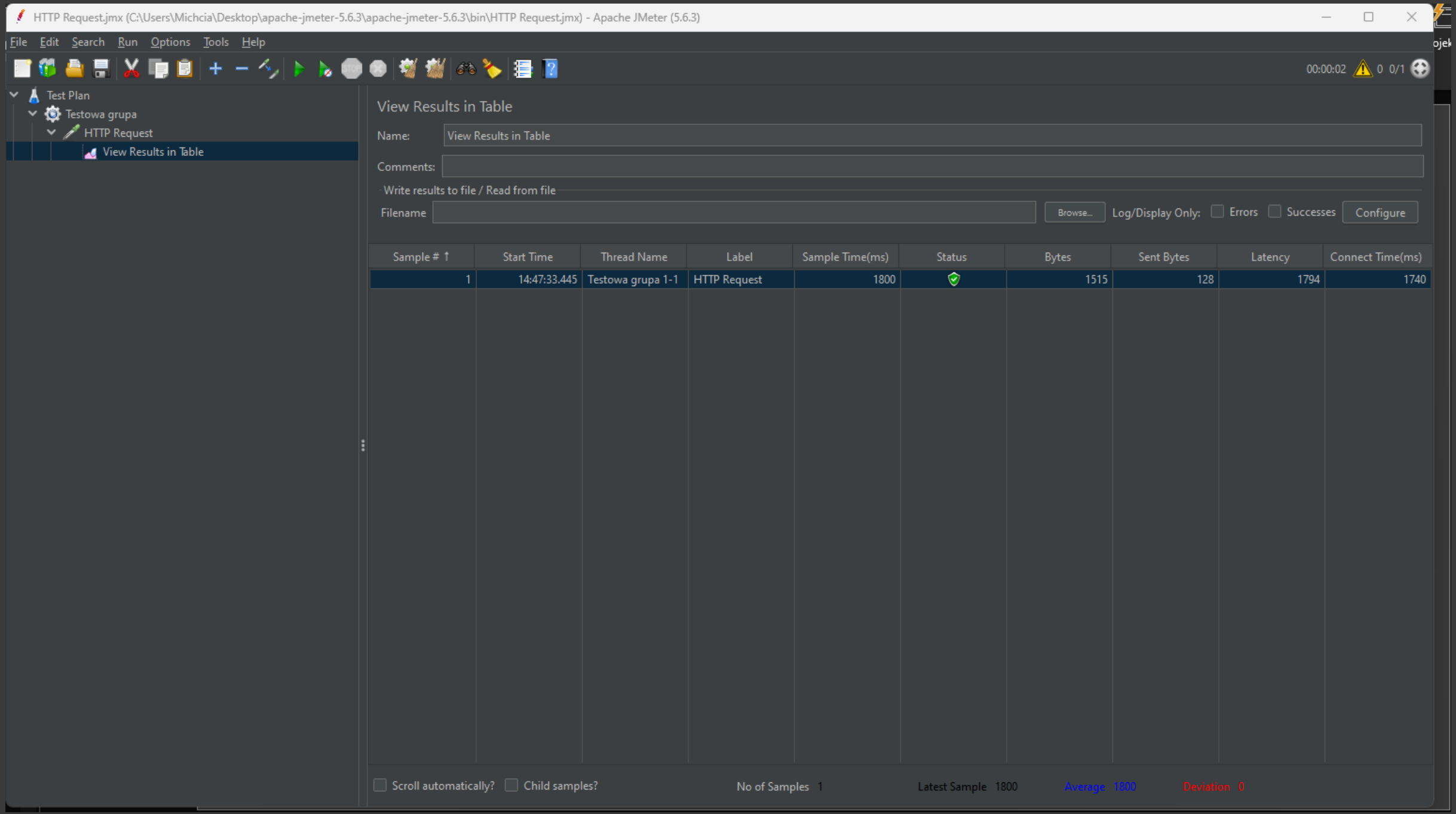


SAMPLER -> określenie, jakiego rodzaju zapytania będziemy wysyłać. Będziemy komunikować się ze stroną, dlatego wybieramy HTTP Request


Apache JMeter (5.6.3)
File Edit Search Run Options Tools Help
Test Plan
Testowa grupa
HTTP Request
HTTP Request
Name: HTTP Request
Comments:
Basic Advanced
Web Server
Protocol [http]:
Server Name or IP:
Port Number:
HTTP Request
GET
Path:
Content encoding:
Redirect Automatically
Follow Redirects
Use KeepAlive
Use multipart/form-data
Browser-compatible headers
Parameters
Body Data
Files Upload
Send Parameters With the Request:
Name:
Value
URL Encode?
Content-Type
Include Equals?
Detail
Add
Add from Clipboard
Delete
Up
Down
Protokół, po którym będziemy się łączyć (my skorzystamy z https)
ścieżka dostępowa na stronie. Dla strony głównej to "/", a np. gdyby istniała podstrona "Kontakt" to najpewniej byłoby to "/kontakt"
adres serwera (strony) z jaką się będziemy łączyć. Może to być adres IP albo domena
numer portu, musi on odpowiadać protokołowi, np. dla https to 443, dla http -> 80

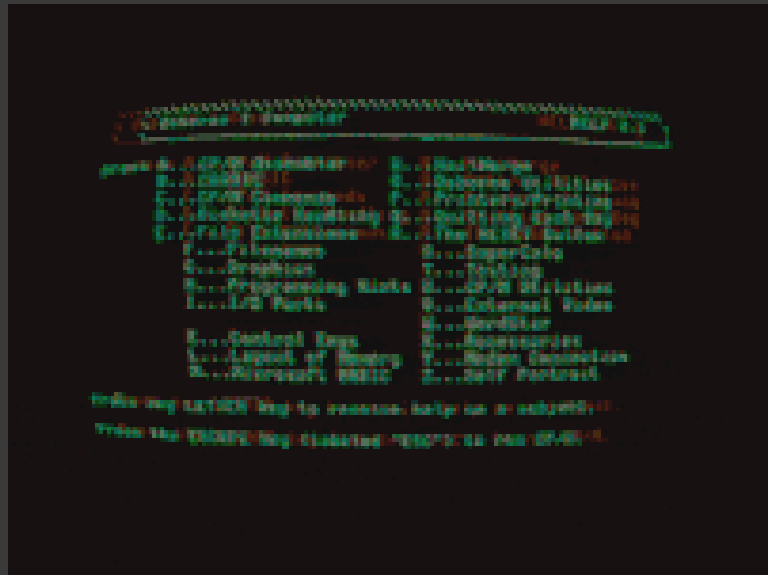


LISTENER **–> tzw. *nasłuchiwacz*; pozwala on wyświetlić rezultaty wysyłanych pakietów. W tym wypadku dodajemy wyniki w tabeli. Możemy też dodać raport podsumowujący (Summary Report)**


HTTP Request.jmx (C:\Users\Michcia\Desktop\apache-jmeter-5.6.3\apache-jmeter-5.6.3\bin\HTTP Request.jmx) - Apache JMeter (5.6.3)
File Edit Search Run Options Tools Help
00:00:02 0 0/1
Test Plan
Testowa grupa
HTTP Request
View Results in Table
View Results in Table
Name: View Results in Table
Comments:
Write results to file / Read from file
Filename
Browse...
Log/Display Only: Errors Successes
Configure
Sample # Start Time Thread Name Label Sample Time(ms) Status Bytes Sent Bytes Latency Connect Time(ms)
1 14:47:33.445 Testowa grupa 1-1 HTTP Request 1800 1515 128 1794 1740
Scroll automatically? Child samples?
No of Samples 1
Latest Sample 1800
Average 1800
Deviation 0

Podsumowanie

1. Na czym polega atak DoS?
2. Czym różni się DoS od DDoS'a?



Podsumowanie

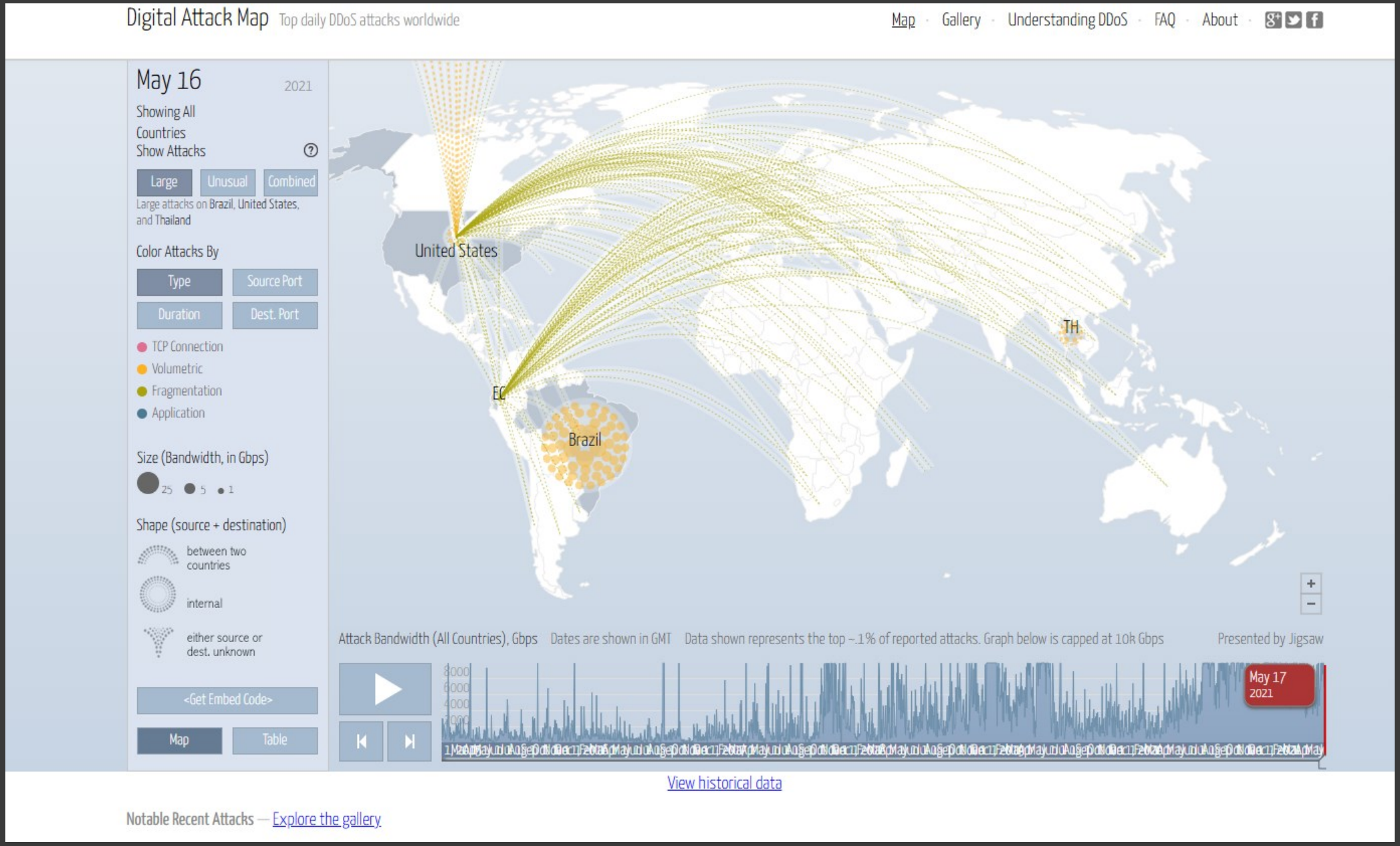
1. Na czym polega atak DoS?
   blokada usługi (ang. *denial of service*) polega na wysyłaniu nadmiarowej ilości połączeń np. do serwera aby wymusić zatrzymanie konkretnej usługi, „zapchania” zasobów czy zapełnienia wszystkich portów

2. Czym różni się DoS od DDoS’a?

Podsumowanie

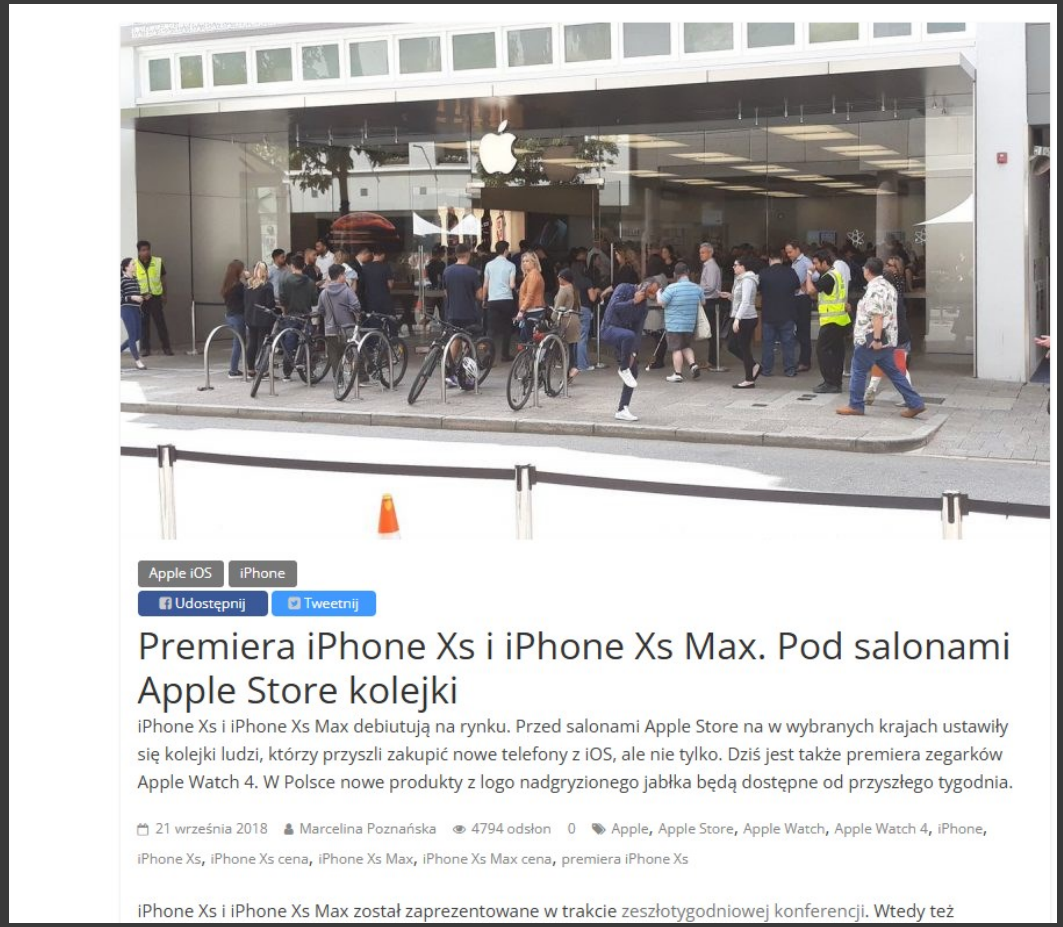
1. Na czym polega atak DoS?
   blokada usługi (ang. *denial of service*) polega na wysyłaniu nadmiarowej ilości połączeń np. do serwera aby wymusić zatrzymanie konkretnej usługi, „zapchania" zasób czy zapełnienia wszystkich portów

2. Czym różni się DoS od DDoS'a?
   DoS jest wykonywany przez jeden komputer, wówczas gdy DDoS (*distributed denial of service*) wykorzystuje sieć wielu (nawet kilku tysięcy) komputerów „zombie", których zasoby są wykorzystywane nielegalnie, bez wiedzy ich właścicieli najczęściej zainfekowane przez wirusa (robaka, trojana).



https://www.digitalattackmap.com/

Polecam!



Apple iOS iPhone

Udostępnij Tweetnij

Premiera iPhone Xs i iPhone Xs Max. Pod salonami Apple Store kolejki

iPhone Xs i iPhone Xs Max debiutują na rynku. Przed salonami Apple Store na w wybranych krajach ustawiły się kolejki ludzi, którzy przyszli zakupić nowe telefony z iOS, ale nie tylko. Dziś jest także premiera zegarków Apple Watch 4. W Polsce nowe produkty z logo nadgryzionego jabłka będą dostępne od przyszłego tygodnia.

21 września 2018 Marcelina Poznańska 4794 odsłon 0 Apple, Apple Store, Apple Watch, Apple Watch 4, iPhone, iPhone Xs, iPhone Xs cena, iPhone Xs Max, iPhone Xs Max cena, premiera iPhone Xs

iPhone Xs i iPhone Xs Max został zaprezentowane w trakcie zeszłotygodniowej konferencji. Wtedy też

ŹRÓDŁO:
Tablety.pl: https://www.tablety.pl/apple_ios/2018-09-21/premiera-iphone-xs-max-apple/

Polecam!

Salon Xiaomi, Galeria Mokotów. Ogromna kolejka przed otwarciem sklepu

REDAKCJA WARSZAWA
14 grudnia 2019, 9:52

Skomentuj (1) Udostępnij

Salon Xiaomi, Galeria Mokotów. Ogromna kolejka przed otwarciem sklepu czytelnik

ŹRÓDŁO:
Warszawa Nasze Miasto: https://warszawa.naszemiasto.pl/salon-xiaomi-galeria-mokotow-ogromna-kolejka-przed/ar/c1-7468771

Polecam!

ŹRÓDŁO:
YouTube: https://www.youtube.com/watch?v=_Uzx8_ygzec

Polecam!

ŹRÓDŁO:
YouTube: https://youtu.be/tUMObU3T6zo