|  |  |
| --- | --- |
| **http://www.po.opole.pl/media/logotypy/2014/logotyp-politechnika-opolska-02.jpg** | **Politechnika Opolska**  **Wydział Elektrotechniki, Automatyki i Informatyki**  **Katedra Informatyki** |
| **Rok akademicki** | 2023/2024 |
| **Przedmiot** | Bazy danych w praktyce |
| **Prowadzący zajęcia** | Dr hab. inż. Mariusz Rząsa |
| **Nr grupy** | 1 |

|  |
| --- |
| **Atak DDOS** |

|  |  |
| --- | --- |
| **Nazwisko i imię** | **Nr indeksu** |
|
| **Dominik Boguszewski** | **98784** |

|  |
| --- |
| **Uwagi** |
|  |

1. **Cel ćwiczenia**

Celem ćwiczenia jest konfiguracja oraz przeprowadzenie ataku DDOS z użyciem skryptów pythonowych do utworzenia serwera command & control oraz tzw. bota. do analizowania pakietów sieciowych posłużył program wireshark.

1. **Przebieg ćwiczenia**

Podczas przeprowadzanego ćwiczenia, korzystano z trzech laptopów połączonych w sieć lokalną. Realizacja zadania opierała się na zastosowaniu skryptów oraz botów. Pierwszy z laptopów pełnił rolę serwera, obsługując centralną funkcję w całym scenariuszu. Na drugim laptopie uruchomione były kontenery dockera z dedykowanym skryptem do obsługi botów. Te boty następnie nawiązywały połączenie z serwerem znajdującym się na pierwszym laptopie. Trzeci laptop był specjalnie przygotowaną "ofiarą", na którą skierowane były działania botów w ramach ćwiczenia.



Atak UDP Flood:

**

Analiza pakietów:

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, numer

Opis wygenerowany automatycznie

Atak TCP Flood:

Obraz zawierający tekst, zrzut ekranu, Czcionka, oprogramowanie

Opis wygenerowany automatycznie

Atak SYN Flood:

*Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznie*

Atak SYN w wireshark:

*Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznie*

Atak http:

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie