



Wykrywanie ataków DDOS

Olga Siwak
Karolina Głowińska
Marek Kobosko
Michał Ryba



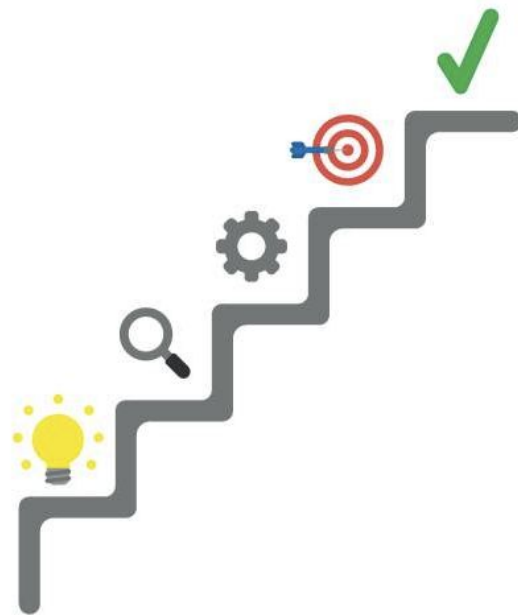
Cel

Stworzenie systemu wykrywania ataków DDoS typu flood z użyciem sterownika Ryu.



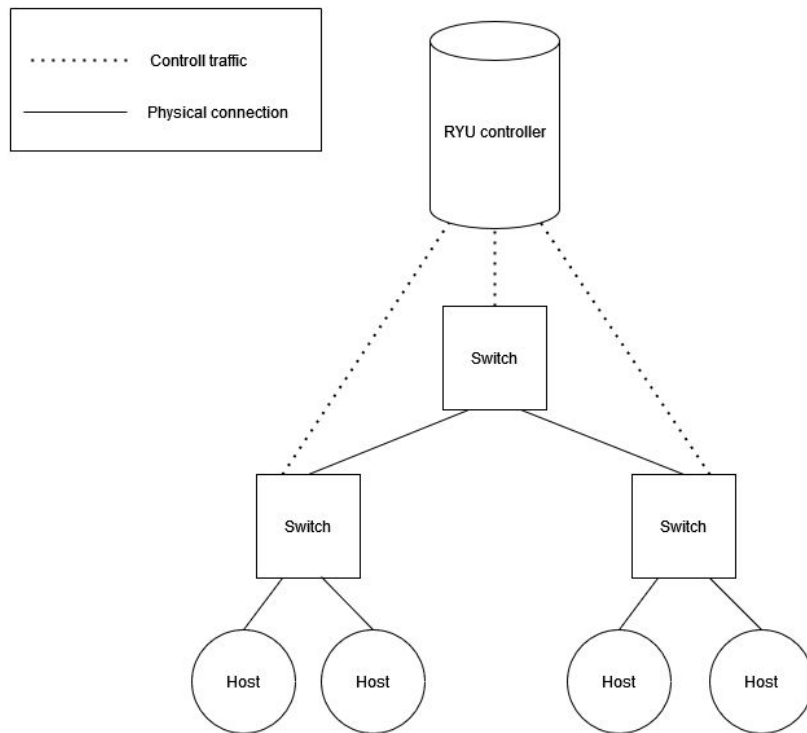
Kroki wykonania projektu

- Sformułowanie problemu
- Przygotowanie pseudo kodu
- Zdefiniowanie topologii
- Implementacja
- Dokumentacja



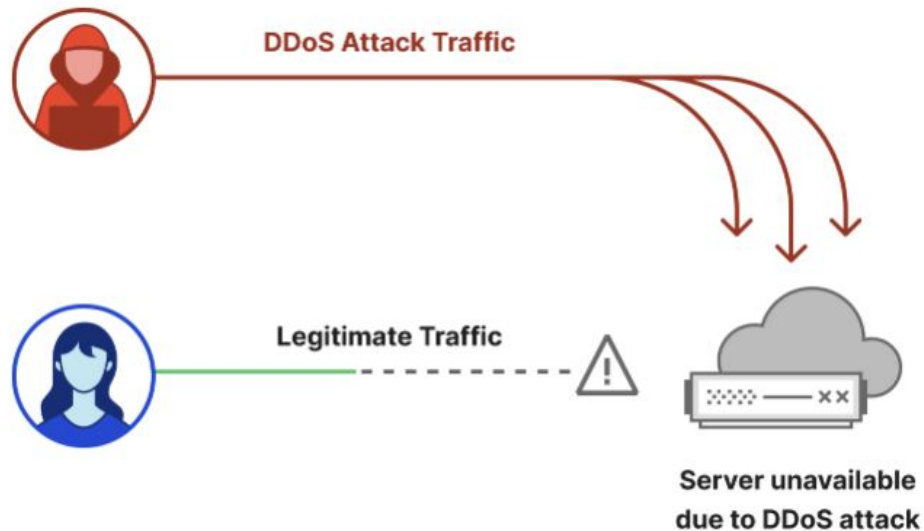
Topologia

- 4 hosty
- 3 przełączniki
- sterownik RYU



Funkcjonalność

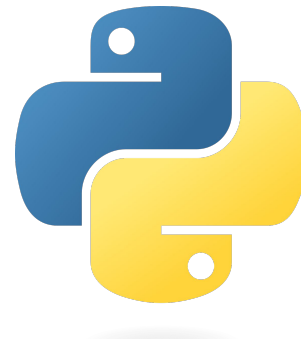
- Generowanie ruchu poprawnego
- Generowanie ataków typu flood
- Monitoring sieci
- Wykrywanie ataku





Implementacja

- Python
- mininet
- Ryu





Sposób wykrywania ataku

1. Sterownik odpytuje co 2 s przełączniki o statystyki przepływów
2. Sterownik przegląda przepływy otrzymane z przełącznika
3. Sterownik na podstawie wielkości ruchu przepływu wykrywa atak



Demo i dokumentacja

<https://github.com/rybam/DDOS-attack-detection-using-Ryu-controller>





Dziękujemy za uwagę