

Sterownik Floodlight jako reaktywny firewall przeciwdziałający atakowi typu ARP spoofing

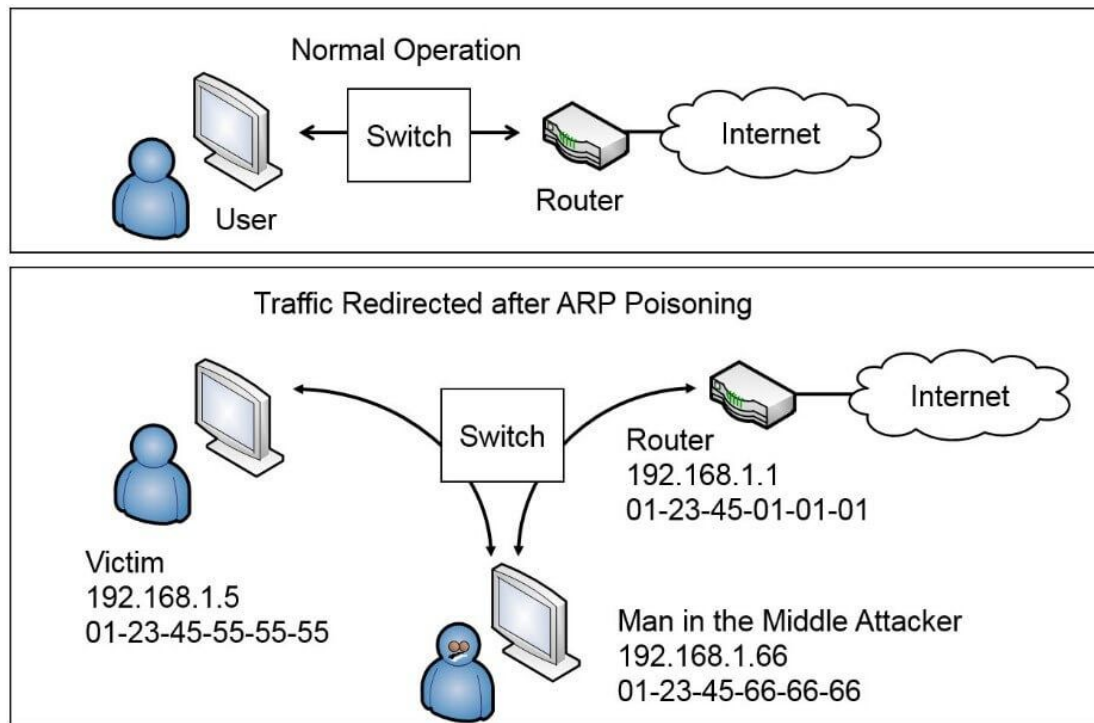
25.01.2024

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie
AGH University of Krakow

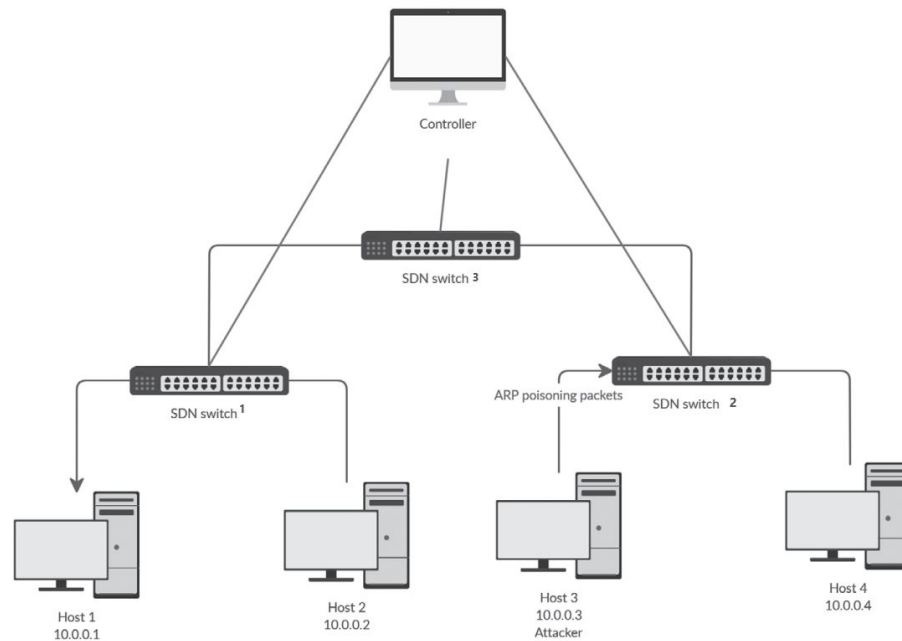
Cel projektu

Głównym celem projektu jest implementacja mechanizmów w kontrolerze Floodlight, które skutecznie wykrywają i przeciwdziałają atakom ARP spoofing w sieci, zwiększając jej bezpieczeństwo i eliminując potencjalne zagrożenia.

ARP Spoofing



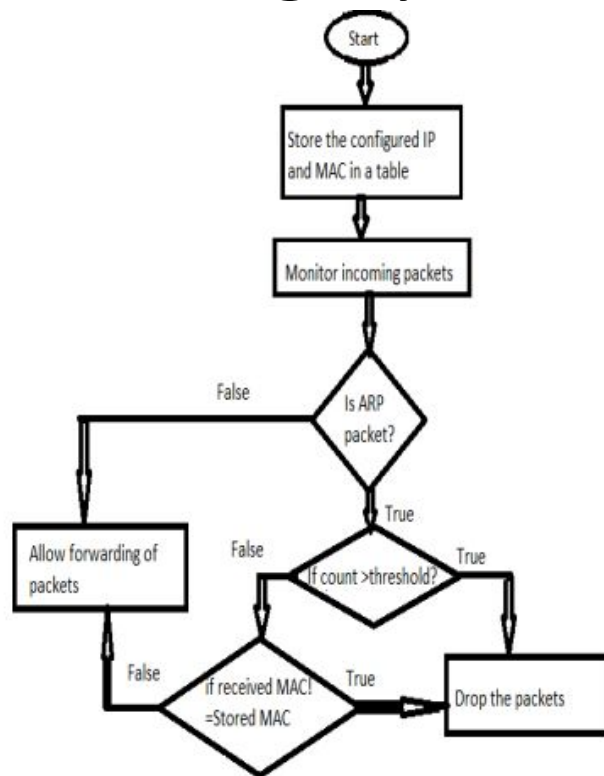
Topologia



Narzędzia

- iperf - generowanie ruchu
- arpspoof - generowanie ataku typu ARP Spoofing

Algorytm



Prezentacja działania projektu

