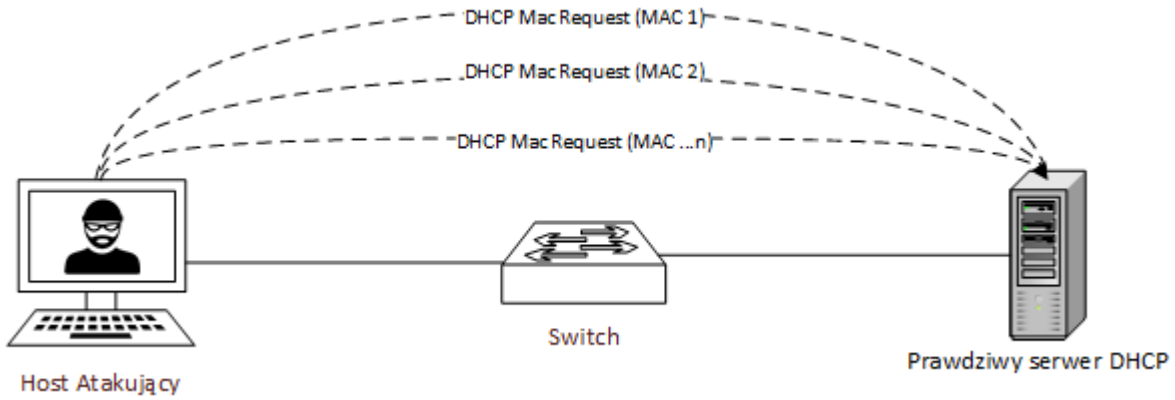
Opis ataku

Prezentowany atak składa się z dwóch części:
- Atak DHCP starvation
- Atak DHCP spoofing
Działają one jeden po drugim, blokując usługę DHCP na serwerze w sieci i tworząc nowy, fałszywy serwer.

Atak DHCP starvation:
Atak typu Denial of Service (DoS). Polega na “wygłodzeniu” serwera DHCP, czyli wykorzystaniu wszystkich dostępnych adresów IP, które serwer oferuje.
Atakujący wysyła w formie broadcast wiadomości DHCP Request z fałszywymi adresami MAC urządzeń. Takie zapytania trafiają do serwera DHCP znajdującego się w sieci. Po wysłaniu odpowiednio dużej liczby zapytań - w zależności od puli dostępnych adresów na serwerze DHCP - następuje wyczerpanie dostępnych adresów i serwer nie może już świadczyć usług DHCP dla prawdziwych użytkowników sieci.



Atak DHCP spoofing:
Polega na podszyciu się hosta w sieci pod serwer DHCP. Atakujący odpowiada na zapytania DHCP Request wiadomościami DHCP ACK i świadczy usługę DHCP. Dodatkowo atakujący może rozgłaszać swój adres jako bramę domyślną (DHCP Option 3) lub serwer DNS (DHCP Option 6). Pozwala to atakującemu na przechwytywanie całego ruchu wychodzącego z sieci, a także rozwiązywanie zapytań DNS. Dzięki takiej konfiguracji atakujący może przeprowadzać ataki Man in the Middle i przechwytywać dane wysyłane przez użytkowników sieci.