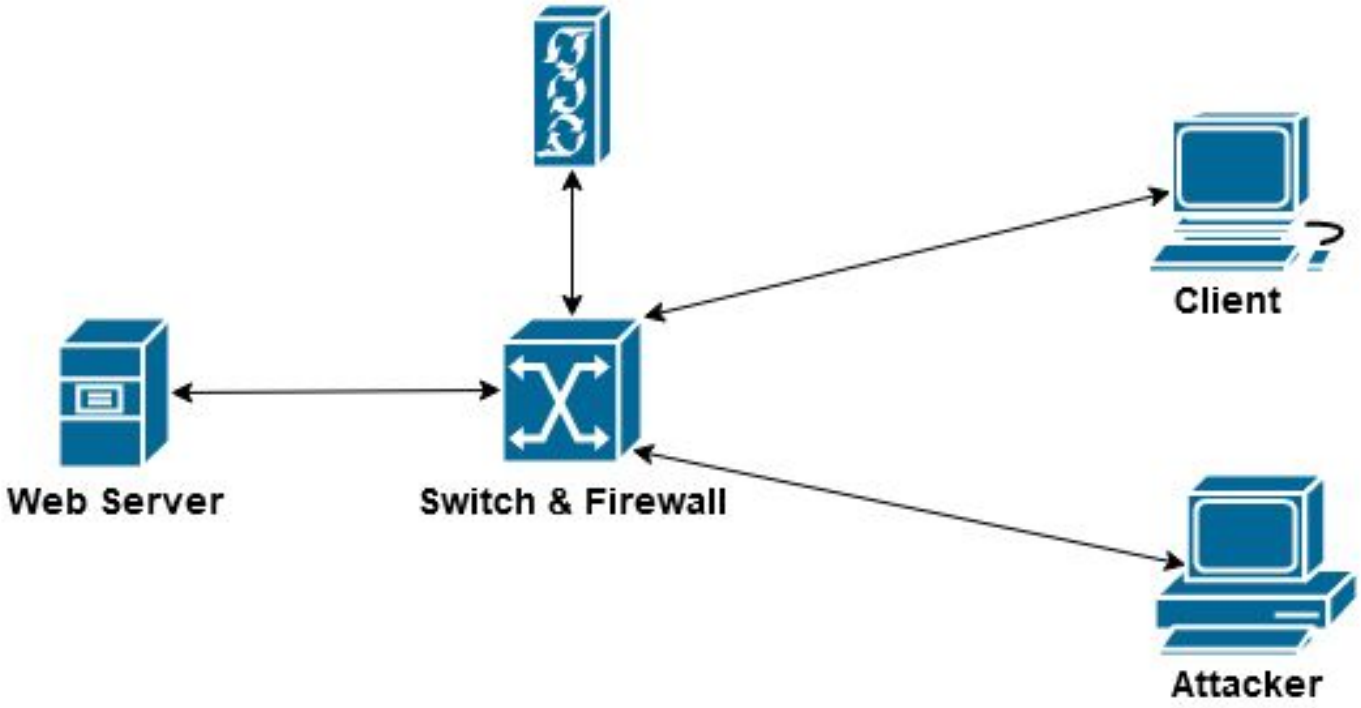
Firewall chroniący przed atakiem DoS

Andrzej Pencak, Kamil Kryczka

Założenia projektu

- Wykorzystanie kontrolera Floodlight
- Moduł blokujący użytkownika nawiązującego wiele połączeń do serwera WWW w celu przeprowadzenia ataku DoS
- SlowLoris do jednoczesnego nawiązywania wielu sesji TCP
- Testy modułu z wykorzystaniem środowiska Mininet
- Projekt wykonywany w metodologii Scrum

Topologia testowa



Zasada działania

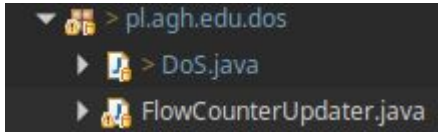
- Zliczane są połączenia z serwerem, nawiązane przez jednego klienta w określonym czasie
- Przekroczenie dozwolonego limitu połączeń skutkuje zablokowaniem całego ruchu przychodzącego od danego klienta
- Odliczany jest czas, przez który atakujący jest odcięty od naszej sieci
- Po upływie czasu blokowania, dostęp do serwera jest wznawiany
- Inni klienci nie są afektowani przez atak i cały czas mają dostęp do serwera

Wartości liczbowe

Wszystkie liczniki w aplikacji można zmienić:

- liczba przepływów z jednego adresu powodująca blokowanie użytkownika: 15
- przepływ brany pod uwagę przez 10 sekund od pierwszego pakietu
- po 50 sekundach użytkownik zostaje odblokowany
- hardTimeout wpisów w tablicy przepływów wynosi 0s
- idleTimeout wpisów w tablicy przepływów wynosi 120s

Struktura modułu pl.agh.edu.dos



- klasa DoS
  - startUp
  - receive (wywołanie metody przetwarzającej pakiet w klasie FlowCounterUpdater)
  - blockHostByIpAddress (instalacja w tablicy przepływów wpisu blokującego adres źródłowy)
  - unblockHostByIpAddress (odblokowanie zablokowanego wcześniej adresu)

Struktura modułu pl.agh.edu.dos

- klasa FlowCounterUpdater
  - analyzePacket
  - getIpAddressFromPacket
  - extractTcpDataFromPacket (trzy powyższe metody służą do uzyskania adresu IP i flag TCP przychodzących pakietów)
  - updateCounter (inkrementacja licznika pakietów lub dodanie nowego wpisu do licznika)
  - scheduleCounterDecrementation (odliczanie w nowym wątku czasu do dekrementacji licznika)
  - decrementFlowCounter (dekrementacja licznika przepływów po określonym czasie)

Live demo

Pytania

Dziękujemy za uwagę