AKADEMIA GÓRNICZO-HUTNICZA
IM. STANISŁAWA STASZICA W KRAKOWIE
AGH UNIVERSITY OF KRAKOW

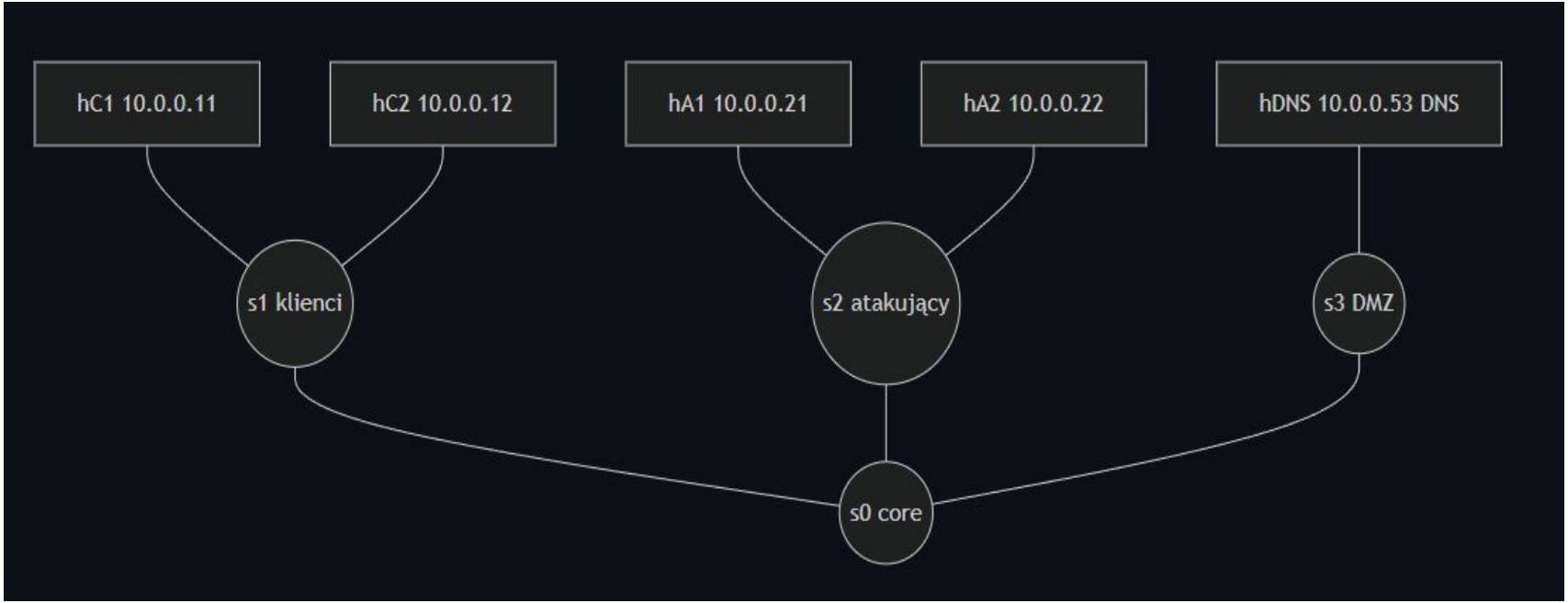
Reaktywny Firewall w Floodlight przy atakach DNS Flooding

Piotr Gwardys
Andrzej Filipowski
Wiktor Kowalski
Tymoteusz Pilarz

Cel projektu

- Wykrywanie ataku DNS flooding
- Blokada adresów IP atakujących hostów

Topologia


hC1 10.0.0.11
hC2 10.0.0.12
hA1 10.0.0.21
hA2 10.0.0.22
hDNS 10.0.0.53 DNS
s1 klienci
s2 atakujący
s3 DMZ
s0 core

Narzędzia

- **dig**
- **dnsmasq**
- **bash**
- **mininet**
- **floodlight na VMce**

Algorytm

Algorithm 1 Hybrydowy model wykrywania DNS Flooding (per-domena + entropia)

Require: Strumień zapytań DNS, okno czasowe Δt, liczba okien referencyjnych W, współczynniki k_N, k_H

Ensure: Decyzja o wystąpieniu ataku DNS Flooding

$L_N[d] \leftarrow \emptyset$ {Historia liczby zapytań dla domeny d}
$L_H[d] \leftarrow \emptyset$ {Historia entropii dla domeny d}
while system aktywny **do**
  $Q \leftarrow$ zbiór zapytań DNS w oknie Δt
  for all domena bazowa d w Q **do**
    $S_d \leftarrow$ zbiór subdomen domeny d w Q
    $N_d \leftarrow |S_d|$
    $H_d \leftarrow -\sum_{i=1}^{|S_d|} p_i \log_2 p_i$ {Entropia Shannona subdomen: p_i to prawdopodobieństwo subdomeny i}
    dodaj N_d do $L_N[d]$
    dodaj H_d do $L_H[d]$
    if $|L_N[d]| \geq W$ **then**
      $\mu_N \leftarrow \frac{1}{W} \sum_{i=1}^{W} L_N[d]_i$ {Średnia liczby zapytań}
      $\sigma_N \leftarrow \sqrt{\frac{1}{W} \sum_{i=1}^{W} (L_N[d]_i - \mu_N)^2}$ {Odchylenie standardowe}
      $\mu_H \leftarrow \frac{1}{W} \sum_{i=1}^{W} L_H[d]_i$ {Średnia entropii}
      $\sigma_H \leftarrow \sqrt{\frac{1}{W} \sum_{i=1}^{W} (L_H[d]_i - \mu_H)^2}$ {Odchylenie standardowe}
      $TH_N \leftarrow \mu_N + k_N \cdot \sigma_N$ {Próg dla liczby zapytań}
      $TH_H \leftarrow \mu_H + k_H \cdot \sigma_H$ {Próg dla entropii}
      if $N_d > TH_N \vee H_d > TH_H$ **then**
        zgłoś atak DNS Flooding dla domeny d
      end if
      usuń najstarszy element z $L_N[d]$
      usuń najstarszy element z $L_H[d]$
    end if
  end for
end while

DEMO

prosze działaj…