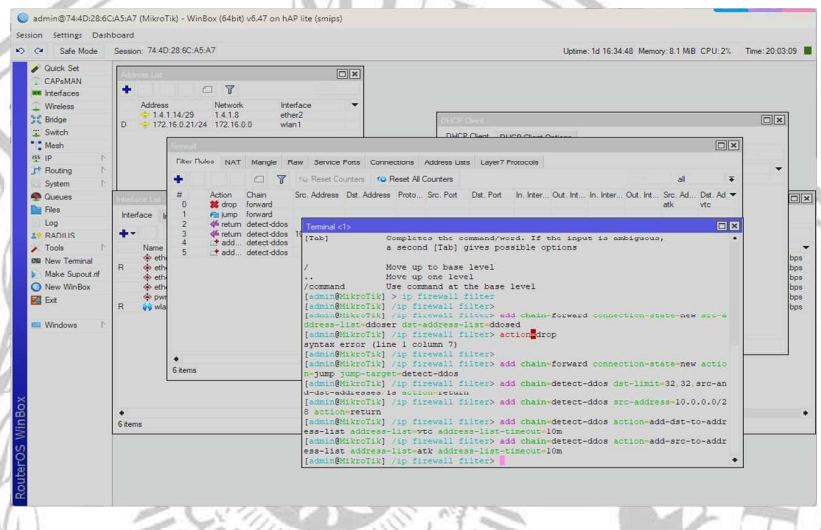
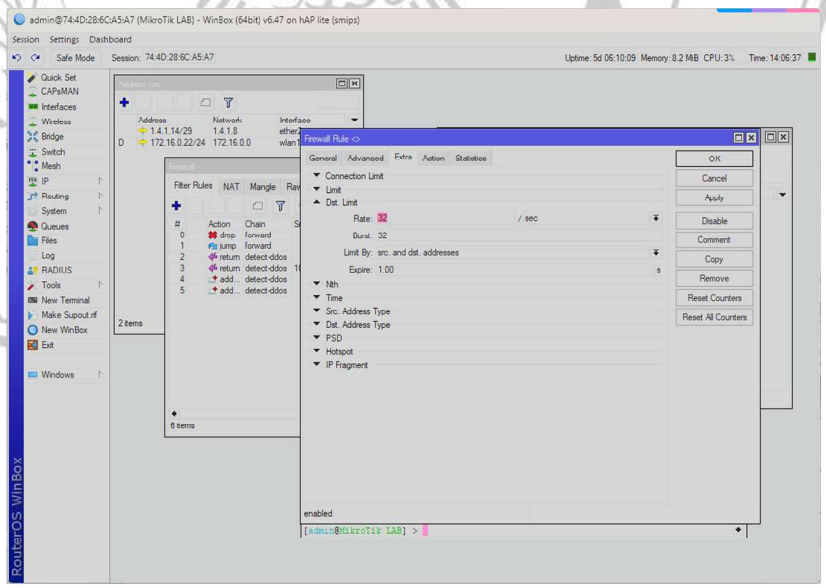
BAB III
Metodologi Penelitian

3.1. Mitigasi Serangan

Teknik mitigasi yang digunakan dalam penelitian ini adalah *custom firewall* mikrotik yang dikonfigurasi untuk melakukan mitigasi serangan DDoS.



Gambar 3.1 Konfigurasi *firewall*



Gambar 3.2 Konfigurasi *custom firewall*

Pada gambar 3.1 dan 3.2, dijelaskan tentang konfigurasi *custom firewall* mikrotik, yang membedakan antara *custom firewall* dengan *firewall* pada umumnya adalah kebebasan *user* dalam mengkonfigurasi *firewall*. Pada konfigurasi ini adalah konfigurasi *burst* & *rate/sec*, dimana angka yang dimasukkan bebas dan tergantung dari kebutuhan *user*, untuk penelitian ini angka yang digunakan adalah 15 *rate/sec* dan 15 *burst*. Untuk *rule* mitigasi DDoS, peneliti menggunakan konfigurasi yang telah disediakan pada halaman resmi mikrotik.

/ip *firewall* address-list

add list=ddos-attackers

add list=ddos-targets

/ip *firewall* filter

add action=return chain=detect-ddos dst-limit=32,32,src-and-dst-addresses/10s

add action=add-dst-to-address-list address-list=ddos-targets address-list-timeout=10m chain=detect-ddos

add action=add-src-to-address-list address-list=ddos-attackers address-list-timeout=10m chain=detect-ddos

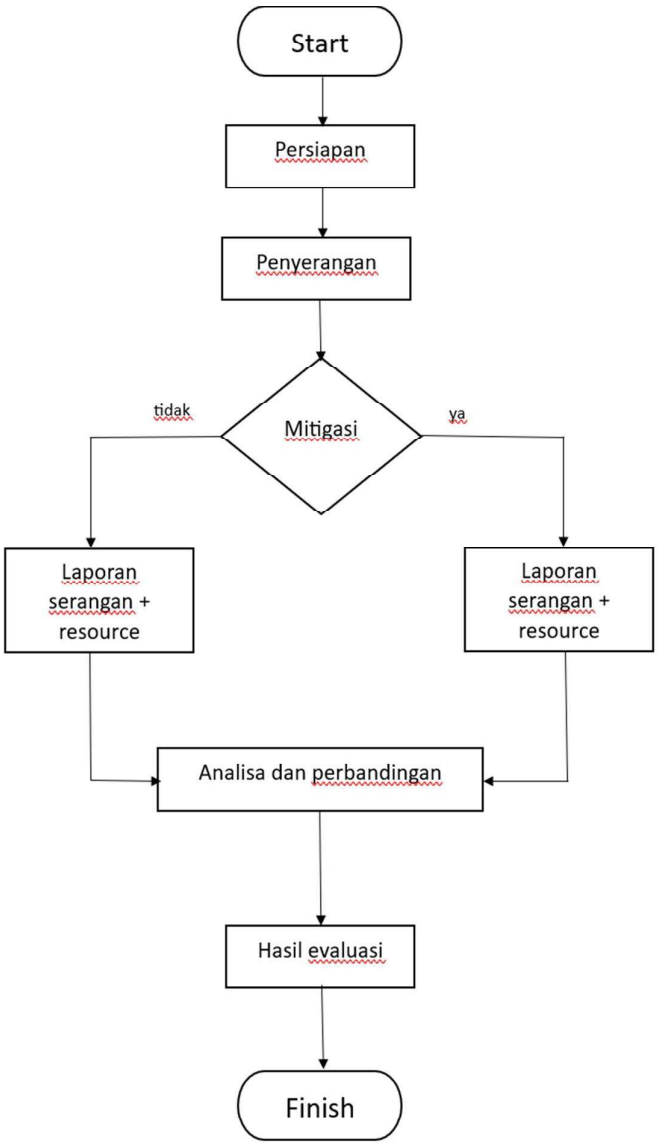
/ip *firewall* raw add action=drop chain=prerouting dst-address-list=ddos-targets src-address-list=ddos-attackers

Khusus untuk SYN *flood*, terdapat konfigurasi tambahan yaitu.

/ip/settings/set tcp-syncookies=yes

3.2. Alur Penelitian

Berikut adalah alur penelitian yang akan dilakukan:



Gambar 3.3 Alur penelitian

Pada gambar 3.3 bagian **Start**, semua persiapan dilakukan. dimulai dari perangkat yang akan digunakan, konfigurasi dasar jaringan, *software* yang akan digunakan untuk menyerang yakni mausezahn, slowloris, hping3, dan *software* untuk mendeteksi serangan yakni LUCID.

Pada gambar 3.2 bagian **Persiapan**, konfigurasi untuk simulasi dijalankan. Beberapa *software monitoring* dijalankan pada *server* dan *router* sebelum serangan dimulai, normal *user* juga dijalankan untuk mengakses *server* untuk memastikan *server* berjalan normal. Scanning terhadap target juga dilakukan untuk mendapatkan informasi,

Pada gambar 3.2 bagian **Penyerangan**, serangan dilakukan dengan menggunakan beberapa *software* seperti hping3 untuk tipe serangan DNS *flood* dan Smurf, mausezahn untuk tipe serangan SYN *flood* dan UDP *flood*, slowloris untuk tipe serangan HTTP *flood*. Serangan DDoS di targetkan pada *server* tanpa batasan apapun, yang berarti serangan hanya terbatas pada kecepatan CPU. Serangan dilakukan menggunakan komputer *zombie* untuk mensimulasikan serangan seperti serangan DDoS pada aslinya.

Pada gambar 3.2 bagian **Mitigasi**, skenario serangan DDoS dibagi menjadi 2 bagian, yaitu sebelum dilakukan mitigasi dan setelah dilakukan mitigasi. Hal ini dilakukan untuk mendapatkan perbandingan terhadap serangan DDoS pada saat sebelum dan sesudah dilakukan mitigasi. Mitigasi dilakukan dengan menggunakan *custom firewall* mikrotik, *custom firewall* yang digunakan adalah gabungan set *rule* untuk mendeteksi tingkat kerapatan antara paket trafik dan berat masing-masing paket, apabila ada paket yang melanggar aturan maka paket akan di *drop*.

Pada gambar 3.2 bagian **Laporan serangan** + *resource*, semua serangan yang telah dilakukan, baik yang dimitigasi maupun yang tidak, akan dilakukan pencatatan. Hal yang dicatat adalah tingkat persentase serangan DDoS, *resource* CPU pada *server*, dan *resource* CPU pada mikrotik. Pengumpulan data dilakukan setiap 10 detik dalam waktu total 60 detik untuk setiap serangan, baik sebelum maupun setelah dilakukan mitigasi. Pengumpulan data dilakukan secara *live* agar terkesan seperti pada aslinya, bukan dari paket yang sudah di *capture*. Pengumpulan data setiap 10 detik dilakukan berdasarkan rekomendasi dari *software* LUCID dikarenakan softwarenya didesain untuk mengumpulkan data setiap 10 detik.

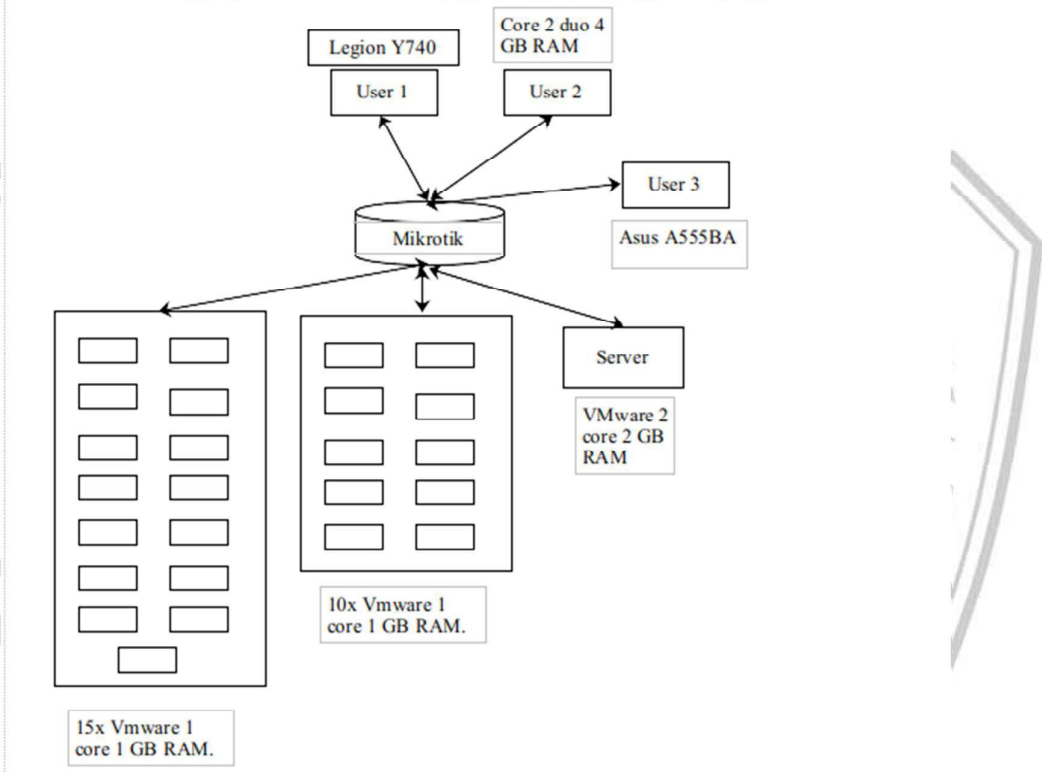
Pada gambar 3.2 bagian **Analisa dan perbandingan**, semua data yang telah dicatat akan dibandingkan. Data yang dibandingkan adalah tingkat persentase serangan DDoS, *resource* CPU *server*, dan *resource* mikrotik sebelum dan sesudah dilakukan mitigasi. Selanjutnya adalah tahapan Hasil evaluasi dimana semua data perbandingan yang telah diolah akan disajikan dalam bentuk grafik untuk mempermudah pembaca. Tingkat

efektifitas dibagi menjadi 4 bagian dengan skala 1-100%, 1-25% berarti kurang efektif, 25-50% berarti cukup efektif, 50-75% berarti efektif, dan 75-100% berarti sangat efektif.

Pada gambar 3.2 bagian **Finish**, setelah semua pengujian dilakukan, semua konfigurasi akan dikembalikan pada *default*. Pengecekan pada perangkat juga dilakukan untuk meminimalisir resiko *freeze*, *lag*, dan *error*. Restart terkadang dibutuhkan untuk merefresh kembali semua perangkat yang digunakan.

3.3. Topologi

Berikut adalah topologi yang digunakan dalam penelitian.



Gambar 3.4 Topologi penelitian

Pada gambar 3.4, terdapat komputer *zombie* yang dibagi menjadi 2 grup karena keterbatasan *resource*, 3 *user* normal, dan 1 *server*. Berikut adalah spesifikasi dari perangkat yang digunakan:

- Mikrotik RB941-2nD sebagai *router* dengan spesifikasi 650MHz cpu & 32 MB RAM.
- 15x VMware 1 core & 1 GB RAM (*zombie*) dalam komputer dengan spesifikasi Ryzen 7 5800X dan 32 GB RAM.

- 10x VMware 1 core & 1 GB RAM (*zombie*) dalam laptop Legion Y740 dengan spesifikasi i7-9750H dan 16 GB RAM.
- VMware 2 core & 2 GB RAM (*server*) dalam laptop Asus A456UQ dengan spesifikasi i7-6500U & 8 GB RAM.
- Asus X555BA dengan spesifikasi AMD A9-9420 dan 4GB RAM sebagai normal *user*3.
- Lenovo Legion Y740 Intel core i7-9750H 6 core & 16GB RAM sebagai normal *user* 1.
- Intel core 2 duo e8400 @3.5GHz dan 4GB RAM sebagai normal *user* 2.

3.4. Skenario Pengujian

- **Skenario 1**

  Komputer *zombie* menyerang *server* target menggunakan beberapa *software* seperti mausezahn, hping3, dan slowloris, penyerangan dilakukan sebelum *rule firewall* mikrotik dikonfigurasi. Kemudian *server* akan mencatat tingkat serangan DDoS menggunakan *software* LUCID, dan penggunaan *resource* menggunakan *software psutil*. Pada saat yang sama, apabila *router* tidak *crash*, maka penggunaan *resource* mikrotik juga dicatat dengan waktu yang telah ditentukan, yaitu setiap 10 detik selama 60 detik, jika *router* mengalami *crash* maka yang dicatat adalah berapa *zombie* yang dibutuhkan untuk membuat *router crash*. Setelah 60 detik, serangan DDoS dan pencatatan dihentikan, kemudian data yang telah dicatat dimasukkan Pada tabel yang nantinya akan dibandingkan.

- **Skenario 2**

  Setelah *rule* kustom *firewall* mikrotik dikonfigurasi dan diaktifkan, Komputer *zombie* menyerang *server* target menggunakan beberapa *software* seperti mausezahn, hping3, dan slowloris, Kemudian *server* akan mencatat tingkat serangan DDoS menggunakan *software* LUCID, dan penggunaan *resource* menggunakan *software* psutil. Pada saat yang sama, apabila *router* tidak *crash*, maka penggunaan *resource* mikrotik juga dicatat dengan waktu yang telah ditentukan, yaitu setiap 10 detik selama 60 detik, jika *router* mengalami *crash* maka yang dicatat adalah berapa *zombie* yang dibutuhkan untuk membuat *router crash*. Setelah 60 detik, serangan DDoS dan pencatatan dihentikan, kemudian data yang telah dicatat dimasukkan Pada tabel yang nantinya akan dibandingkan.