BAB III
METODE PENELITIAN

3.1 Desain Penelitian

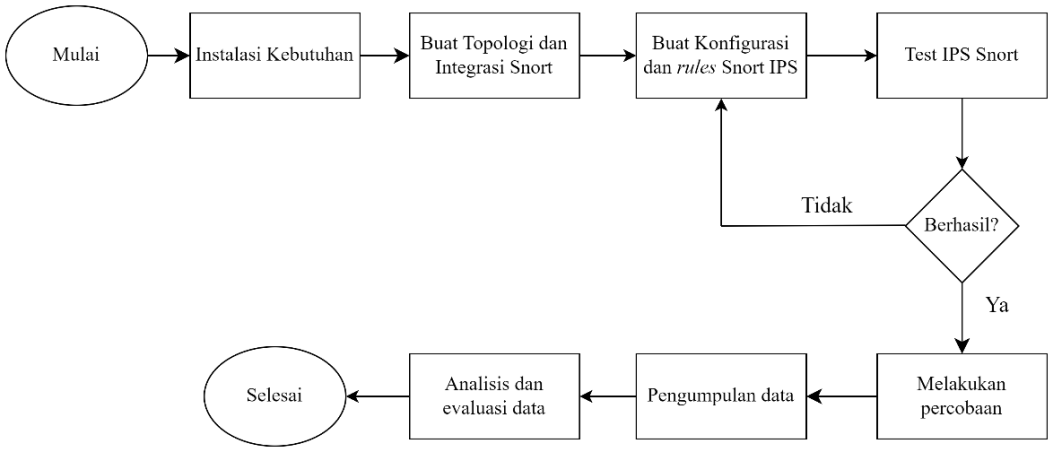
Penelitian yang akan dilaksanakan oleh penulis menggunakan metode penelitian kuantitatif dengan pendekatan *Research and Development* (R&D). Metode penelitian kuantitatif menurut (Ramdhan, 2021) merupakan suatu pendekatan sistematis dalam mengumpulkan data yang dapat diukur terkait sebuah kejadian yang terjadi dengan menggunakan teknik statistik, matematik maupun komputasi. Metode penelitian ini memungkinkan penulis untuk mengukur variabel-variabel tertentu dan menganalisis data secara objektif, yang akan menghasilkan suatu kesimpulan yang dapat digeneralisasi.

Pendekatan R&D sendiri meskipun sering kali dikaitkan dengan penelitian pengembangan, sebenarnya mencakup dua fase utama yaitu penelitian dan pengembangan. Dengan pendekatan ini, penulis melakukan penelitian untuk mempelajari temuan-temuan yang berkaitan dengan produk yang akan dikembangkan. Selanjutnya penulis akan mengembangkan dan merevisi produk yang mempunyai kekurangan tersebut sehingga menghasilkan produk akhir yang lebih baik (Paramita dkk., 2021).

Desain penelitian dengan menggunakan metode penelitian berupa kuantitatif dengan pendekatan R&D bermaksud untuk membandingkan keadaan performa jaringan SDN pada saat sebelum serangan, saat serangan tanpa IPS dan saat serangan menggunakan IPS. Dengan pengukuran performa yang di pertimbangkan yaitu *Quality of Service* (QoS) seperti *throughput*, *delay*, dan *packet loss*, kemudian *resource usage* yaitu CPU *usage* dan *memory usage*.

3.2 Alur Penelitian

Alur penelitian yang dilaksanakan oleh penulis dalam melakukan penelitian ini yaitu dijelaskan pada gambar 3.1. Alur penelitian ini digunakan oleh penulis sebagai pedoman untuk melaksanakan penelitian agar hasil penelitian tidak menyimpang dan juga sesuai dengan tujuan yang telah ditentukan oleh penulis.



Gambar 3. 1 Alur Penelitian

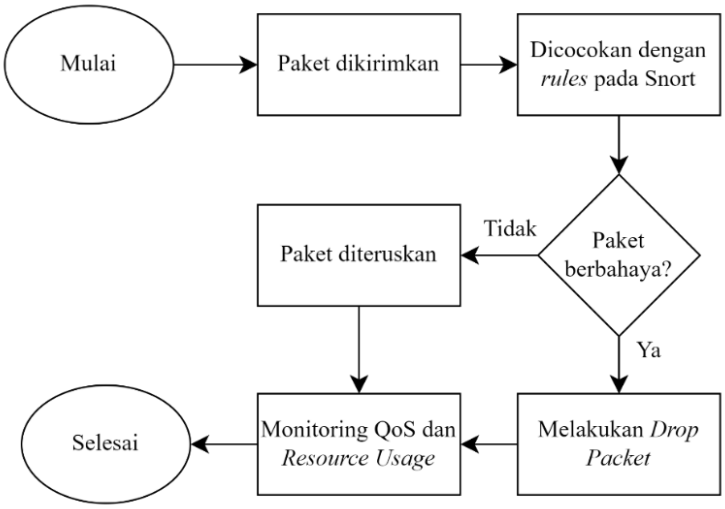
Berdasarkan gambar 3.1 alur penelitian yang dilakukan oleh penulis, dapat dijelaskan sebagai berikut:

1. Instalasi kebutuhan, tahap awal dimulai dengan menginstal semua perangkat lunak dan dependensi yang dibutuhkan untuk menjalankan simulasi dan analisis. Hal ini mencakup sistem operasi, Snort sebagai sistem IPS, perangkat lainnya yang relevan dengan penelitian yang dilakukan.
2. Pembuatan topologi dan integrasi Snort, pada tahap ini penulis membuat topologi jaringan menggunakan mininet dan mengintegrasikan Snort ke dalam topologi tersebut.
3. Pembuatan konfigurasi dan *rules* Snort IPS, setelah topologi dibuat, langkah selanjutnya yaitu melakukan konfigurasi agar Snort berjalan sebagai IPS. Setelahnya menetapkan *rules* yang akan digunakan Snort untuk mencegah serangan, *rules* ini dibuat berdasarkan jenis serangan yang diantisipasi dalam pengujian.
4. Melakukan percobaan, setelah memastikan Snort berfungsi dengan baik, penulis kemudian melakukan percobaan dengan menjalankan berbagai serangan DDoS yang telah direncanakan. Kemudian Snort diaktifkan untuk memantau dan mencegah serangan-serangan selama percobaan berlangsung.
5. Pengumpulan data, selama percobaan berlangsung penulis mengumpulkan semua data untuk dilakukan analisis, data ini cukup penting dalam memahami bagaimana serangan dan aktivasi IPS mempengaruhi jaringan.

6. Analisis dan evaluasi data, pada tahap terakhir ini penulis menganalisis data yang telah dikumpulkan untuk dilakukan evaluasi terkait dampak dari serangan dan efektivitas Snort IPS dalam menjaga performa jaringan.

3.3 Alur Percobaan

Alur percobaan yang akan dilaksanakan oleh penulis dapat dilihat pada gambar 3.2. Alur percobaan ini untuk memudahkan penulis dalam melakukan alur percobaan penelitian.



Gambar 3. 2 Alur Percobaan

Pada gambar 3.2 merepresentasikan alur dari Konfigurasi Sistem IPS untuk penjelasan untuk setiap bagiannya sebagai berikut:

1. Dimulai dengan mengirimkan paket baik paket dari *Host* yang berperan sebagai *Attacker* dan dari *Host* yang berperan sebagai *User* yang sah.
2. Kemudian paket yang datang ke sistem Snort akan dicocokkan dengan *rules* yang sudah ditetapkan oleh penulis. Jika Paket yang datang tidak berbahaya paket akan diteruskan ke tujuan, sedangkan paket yang berbahaya akan di *drop* oleh Snort.
3. Dilakukan monitoring yang akan memperlihatkan hasilnya dalam bentuk *log file*. Untuk monitoring QoS berupa *throughput*, *delay*, dan *packet loss* menggunakan *tools* D-ITG. Sedangkan untuk *Resource Usage* yang terdiri atas CPU *Usage* dan *Memory Usage* menggunakan dstat.

3.4 Karakteristik Objek Penelitian

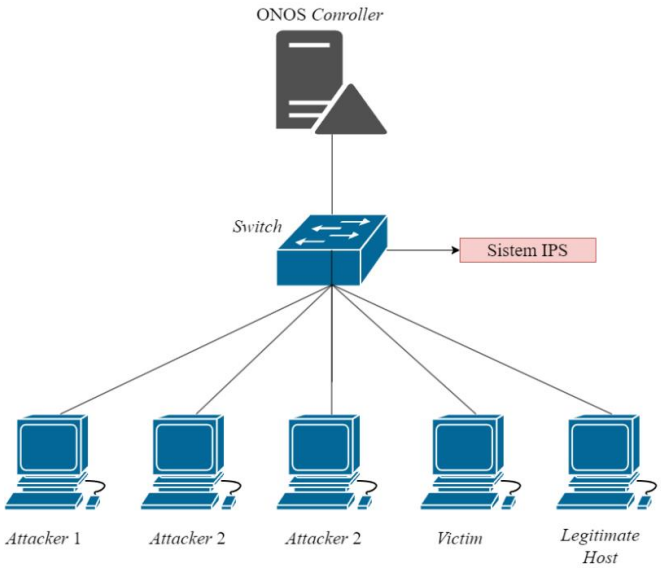
Penelitian yang dibangun oleh penulis berfokus pada analisis efektifitas sistem IPS dalam lingkungan SDN. Tujuan utama dari penelitian ini adalah untuk

mengevaluasi implementasi IPS dengan menggunakan Snort untuk melakukan deteksi dan pencegahan terhadap berbagai jenis serangan dalam jaringan yang dikendalikan oleh *controller* SDN. Karakteristik objek penelitian ini mencakup elmen-elmen utama yang dirancang untuk memberikan pemahaman mendalam mengenai jaringan SDN, sistem IPS, serta serangan DDoS yang digunakan. Berikut untuk rincian terkait dengan karakteristik objek penelitian.

3.4.1 Jaringan SDN

Jaringan SDN ini adalah jaringan yang memisahkan antara lapisan kontrol dari lapisan data. Jaringan tersebut dikendalikan secara penuh oleh sebuah *controller* terpusat yang memungkinkan adanya konfigurasi dan menejeman jaringan secara dinamis. Untuk cara kerjanya sendiri *controller* SDN akan bertindak sebagai otak jaringan dalam mengelola semua kebijakan dan konfigurasi secara terpusat, untuk melakukan komunikasi dengan perangkat jaringan *controller* menggunakan API seperti *OpenFlow* untuk mengatur lalu lintas dan kebijakan jaringan. Selain itu, SDN memungkinkan virtualisasi jaringan yang mempermudah pengelolaan dan pemantauan jaringan.

Adapun topologi jaringan SDN yang digunakan pada penelitian yang dilakukan oleh penulis adalah topologi *custom* sederhana, dengan menggunakan 1 *controller*, 1 *switch*, dan 5 *Host* dengan perannya masing-masing. *Host* 1 sampai *Host* 3 berperan sebagai *attacker*, *Host* 4 berperan sebagai target (*victim*), dan *Host* 5 berperan sebagai penggunaan yang sah (*legitimate host*). Simulasi ini akan dijalankan menggunakan emulator mininet dengan *Controller* yang digunakan adalah ONOS *Controller*, untuk ilustrasi topologi lebih jelasnya dapat dilihat pada gambar 3.3.



Gambar 3. 3 Topologi Jaringan

3.4.2 Sistem IPS

Sistem IPS berguna dalam memantau, mendeteksi, dan mencegah segala ancaman dari lalu lintas jaringan. Selain itu, sistem IPS juga dirancang untuk melakukan perlindungan jaringan dari serangan dengan secara aktif memblokir aktivitas berbahaya. Untuk cara kerja dari IPS sendiri ialah dengan menganalisis paket data yang melewati jaringan untuk mencapai pola serangan. Kemudian menanggapi ancaman yang hadir dengan memblokir atau menolak paket data yang terindikasi berbahaya. Sistem IPS ini dapat diimplementasikan pada jaringan SDN dengan berbagai cara, namun pada penelitian yang dilakukan oleh penulis IPS diterapkan melalui konfigurasi *port mirroring*.

Topologi jaringan SDN yang dirancang dengan ilustrasi yang terlihat pada gambar 3.3 menunjukan bahwa topologi yang dipilih ini dapat memudahkan pengamatan langsung terhadap dampak serangan pada jaringan, meminimalkan variabel yang dapat mempengaruhi hasil, serta menguji dan memastikan fokus utama pada efektivitas IPS yang dipasang melalui konfigurasi *port mirroring* pada *switch*. *Port mirroring* diterapkan pada *switch* dengan tujuan untuk mengarahkan lalu lintas jaringan ke *interface* enp0s3 (untuk *input*) dan enp0s9 (untuk *output*) yang terhubung ke IPS. Kedua *interface* tersebut merupakan *interface* jaringan yang telah disediakan oleh penulis pada *virtual machine* berbasis ubuntu yang digunakan. Sistem IPS yang digunakan oleh penulis ialah menggunakan *OpenSource* Snort dalam mode *inline* dengan parameter -Q dan modul DAQ *afpacket*. Dalam mode

inline ini, Snort melakukan analisis paket secara langsung saat melewati *interface* yang telah ditentukan tersebut.

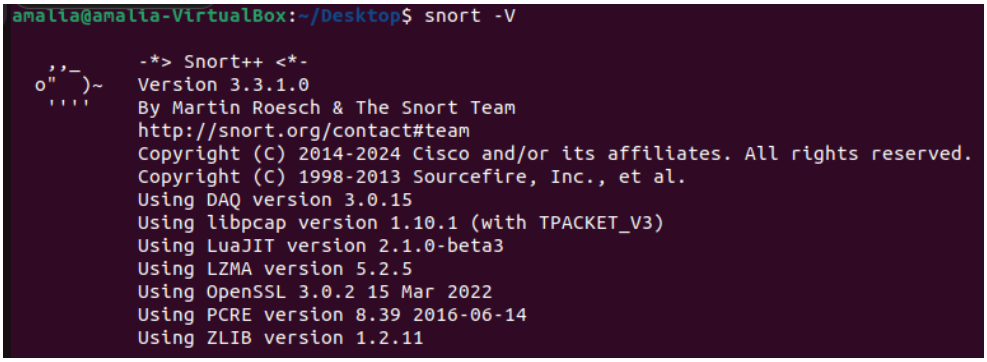
Snort melakukan pemeriksaan lalu lintas yang masuk melalui *interface* enp0s3, di dalam *interface* tersebut jika terdeteksi adanya ancaman berdasarkan aturan yang diterapkan maka Snort dapat langsung menjatuhkan paket tersebut tanpa meneruskannya ke *interface* enp0s9. Namun jika paket yang datang terdeteksi sebagai *user* yang sah, paket tersebut akan diteruskan ke *interface* enp0s9 yang kemudian diteruskan kembali ke *Host* tujuan. berikut terkait proses dari instalasi dan konfigurasi IPS dengan menggunakan Snort.

3.4.2.1 Instalasi Snort

Berikut ini adalah perintah yang digunakan dalam untuk melakukan instalasi Snort yang mendukung sistem IPS.

```
$sudo apt install build-essential libpcap-dev libpcre3-dev libnet1-dev zlib1g-dev luajit hwloc libdnet-dev libdumbnet-dev bison flex liblzma-dev openssl libssl-dev pkg-config libhwloc-dev cmake cpputest libsqlite3-dev uuid-dev libcmocka-dev libnetfilter-queue-dev libmnl-dev autotools-dev libluajit-5.1-dev libunwind-dev
$sudo mkdir snort-source-files
$cd snort-source-files
$sudo git clone https://github.com/snort3/libdaq.git
$cd libdaq
$sudo ./configure
$sudo make install
$wget
https://github.com/gperftools/gperftools/releases/download/gpertools2.8/gpertools-2.8.tar.gz
$sudo tar xzf gpertools-2.8.tar.gz
$cd gpertools-2.8/
$sudo ./configure
$sudo make install
$git clone git://github.com/snortadmin/snort3.git
$cd snort3
$ sudo ./configure_cmake.sh prefix=/ usr /local --enable-tcmalloc
$cd build
$sudo make install
$sudo ldconfig
```

Setelah proses instalasi sudah selesai, untuk memverifikasi jika Snort telah berhasil terinstal dengan baik dapat dilakukan dengan cara yang terlihat pada gambar 3.4 yang menunjukan jika versi Snort yang digunakan pada penelitian ini adalah Snort versi 3.



Gambar 3. 4 Versi Snort

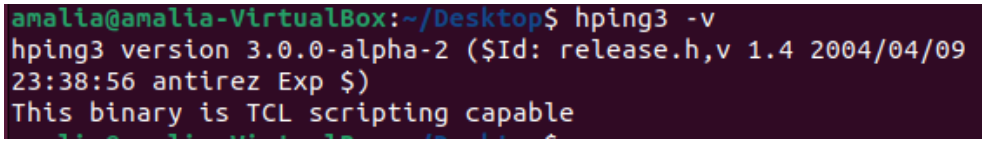
3.4.2.2 Konfigurasi Snort

Penggunaan Snort sebagai sistem IPS melalui beberapa konfigurasi agar dapat dijalankan dengan baik. Adapun proses dari konfigurasi yang dilakukan oleh penulis yaitu menyiapkan 2 (dua) *interface* terlebih dahulu dengan tanpa adanya IP *address*, kemudian dilakukan konfigurasi *interface* pada file snort.lua, konfigurasi *rules* dan *logging*. Berikut adalah perintah yang dapat digunakan untuk konfigurasi Snort.

```
$sudo ip link set dev enp0s3 promisc on
$sudo ethtool -K enp0s3 gro off lro off
$sudo nano /usr/local/etc/snort/snort.lua
$sudo nano /usr/local/etc/snort/rules /local.rules
```

3.4.3 Serangan DDoS

Serangan DDoS yang dilakukan oleh penulis bertujuan untuk membanjiri jaringan SDN agar dapat melihat dampak dari serangan juga pengaruh dari IPS yang diterapkan pada jaringan SDN ketika terjadi serangan. Serangan DDoS yang dilakukan oleh penulis ini berfokus pada jenis serangan *Protocol Attacks* dan *Volume-Based Attacks* yaitu menyasar kerentanan dalam *protocol* jaringan untuk menghabiskan sumber daya server dan menargetkan *bandwidth* jaringan dengan volume lalu lintas yang sangat besar. Dalam melakukan serangannya penulis menggunakan *tools* Hping3 sebagai alat serangan, Adapun untuk melakukan instalasi Hping3 sendiri dapat hanya menggunakan perintah `sudo apt-get install hping3`. Kemudian lakukan konfirmasi versi Hping3 yang terinstal dengan menggunakan perintah `hping3 -v`, lebih jelasnya dapat lihat pada gambar 3.5.



Gambar 3. 5 Versi Hping3

Serangan DDoS yang dilakukan oleh penulis yaitu dengan jenis serangan yang diterapkan berbeda-beda yaitu SYN *Flood* ditandai dengan perintah -S, UDP *Flood* ditandai dengan perintah -2, dan ICMP *Flood* ditandai dengan baris perintah -1.

3.4.4 Perangkat Lunak

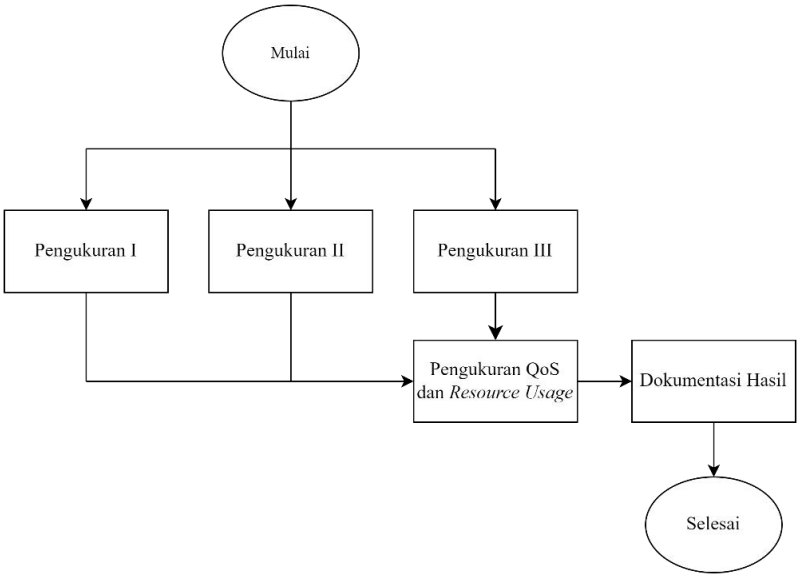
Penelitian yang akan dilaksanakan oleh penulis untuk mencapai keberhasilan penelitian dibutuhkan suatu alat dan bahan yang mendukung penelitian tersebut. Untuk detail alat dan bahan yang dibutuhkan dalam menunjang penelitian dapat dilihat pada tabel 3.1.

Tabel 3. 1 Perangkat Lunak

Item	Spesifikasi
Laptop	AMD Ryzen 5 7520U with Radeon Graphics 2.80 GHz, *operatingsystem*, x64-*based processor*
Operating System	Windows *11 Home Single Language*
	Ubuntu Desktop 22.04.6 LTS
Oracle Virtual Box	*Version* 6.1
Tools IPS	Snort*3*
Tools Attacker	Hping3
Simulator Jaringan	Mininet
Pengujian Trafik	D-ITG
Controller	ONOS *Controller*

3.5 Teknik Pengumpulan Data

Pada bagian ini akan dilakukan suatu pengukuran pengujian yang dibagi ke dalam 3 (tiga) pengukuran pengujian. Adapun untuk perancangan Pengukuran pengujian yang akan dilaksanakan oleh penulis dalam menggambarkan prosesnya dapat dilihat pada gambar 3.4.



Gambar 3. 6 Proses Pengukuran Penelitian

Dari gambar 3.4 terlihat jika dilakukan pengujian dengan menggunakan 3 (tiga) Pengukuran. Setiap Pengukuran dilakukan untuk menilai rata-rata dan mengevaluasi kinerja dari jaringan SDN. Adapun tujuan dari setiap Pengukuran yaitu:

1. Pengukuran I: mempunyai tujuan untuk menentukan *baseline* performa jaringan tanpa adanya gangguan atau serangan, hal ini menggambarkan kondisi jaringan dalam keadaan normal.
2. Pengukuran II: mempunyai tujuan melihat seberapa besar pengaruh atau dampak serangan terhadap performa jaringan.
3. Pengukuran III: mempunyai tujuan untuk mengevaluasi efektivitas sistem IPS dalam melindungi jaringan dari serangan.

Untuk penjelasan lebih ringkasnya terkait Pengukuran dan parameter yang diukur dapat dilihat pada tabel 3.2.

Tabel 3. 2 Pengukuran Penelitian

Pengukuran	Serangan	*Intrusion Prevention System* (IPS)	Parameter
I	Tidak	Tidak	- *Throughput* - *Delay* - *Packet loss* - CPU *Usage* - *Memory Usage*
II	Ya	Tidak	
III	Ya	Ya	

Kemudian untuk teknik pengumpulan data yang digunakan oleh penulis dimulai dari studi literatur yang didapatkan dari *e-book*, jurnal *online*, media *online*, dan referensi yang mendukung lainnya sebagai bahan tinjauan pustaka yang mempunyai kaitan dengan penelitian yang dilakukan. Pada penelitian ini, diperlukan adanya pengukuran yang dilakukan secara berulang untuk menghasilkan nilai rata-rata rata-rata performa jaringan.

Dalam penelitian yang dilakukan penulis, pengulangan atau repetisi dilakukan sebanyak 15 kali untuk setiap pengujian pada berbagai interval waktu yaitu 10 detik, 20 detik, 30 detik, 40 detik, 50 detik, dan 60 detik. Setiap pengulangan ini menghasilkan data yang kemudian dihitung rata-ratanya untuk memberikan gambaran yang akurat mengenai performa jaringan. Penggunaan interval waktu yang berbeda ini memungkinkan penulis mengamati juga menganalisis bagaimana performa jaringan berfluktuasi atau stabil dalam berbagai kondisi waktu pengujian.

Adapun formula yang digunakan dalam pengukuran data dalam menghitung nilai rata-rata rata-rata yaitu:

$$\bar{x} = \frac{x_1 + x_2 \ldots + x_n}{\text{n}} \quad \text{(3.1)}$$

Keterangan:

$\bar{x}$ = Nilai rata-rata rata-rata

x_n = Nilai rata-rata Repetisi ke-n

n = Jumlah Repetisi

3.6 Teknik Analisis Data

Setelah dilakukan serangkaian pengujian baik Pengukuran I, Pengukuran II, dan Pengukuran III, Langkah selanjutnya yaitu dengan melakukan analisis data untuk menginterpretasikan hasil pengujian dan mengevaluasi kinerja Jaringan SDN. Adapun proses analisis data sendiri terdiri dari serangkaian berikut:

1. Pengelolaan data awal, yaitu untuk setiap parameter yang diukur seperti *throughput*, *delay*, *packet loss*, penggunaan CPU, dan penggunaan memori dihitung rata-ratanya dari hasil Pengukuran I, Pengukuran II, dan Pengukuran III. Perhitungan tersebut bertujuan untuk memberikan gambaran umum mengenai performa jaringan dalam setiap Pengukuran yang diujikan.
2. Perbandingan Antar Pengukuran, dilakukan dua perbandingan diantaranya yaitu:

- Perbandingan Pengukuran I dan Pengukuran II: analisis dilakukan dengan membandingkan performa jaringan sebelum terjadinya serangan dengan performa saat serangan berlangsung tanpa IPS, dengan melihat setiap nilai rata-rata pada parameter yang diukur.
- Perbandingan Pengukuran II dan Pengukuran III: untuk melakukan mengevaluasi efektivitas IPS dilakukan perbandingan antara performa jaringan saat terjadinya serangan tanpa IPS dan saat serangan dengan IPS aktif. Fokus analisisnya yaitu pada peningkatan *throughput*, penurunan *delay*, penurunan *packet loss* juga melihat nilai rata-rata penggunaan CPU dan Memori.

3. Analisis Selisih Pengukuran terdiri atas dua hal diantaranya:
   - Perhitungan selisih performa: Selisih performa dihitung antara sebelum serangan, saat serangan tanpa IPS dan saat serangan dengan IPS ini digunakan untuk mengevaluasi dampak serangan serta efektivitas dari mitigasi yang dilakukan oleh IPS.
   - Evaluasi Pengaruh Waktu Pengukuran:berdasarkan hasil pengujian yang dilakukan pada berbagai waktu pengukuran, dilakukan analisis untuk melihat apakah setiap durasi pengukuran mempengaruhi hasil.
4. Visualisasi Data, yaitu data hasil pengukuran divisualisasikan dalam bentuk garafik dalam melakukan perbandingan performa jaringan untuk setiap Pengukuran yang berbeda.
5. Interprestasi Hasil, terdiri dari 3 bagian diantaranya adalah sebagai berikut:
   - Evaluasi Serangan: dari perbandingan performa jaringan sebelum terjadinya serangan dengan saat terjadinya serangan dilakukan pengamatan terkait pengaruh serangan terhadap jaringan SDN dengan melihat nilai rata-rata setiap parameter yang diukur.
   - Evaluasi Efektivitas IPS: dari perbandingan antara performa jaringan saat serangan tanpa IPS dan saat serangan dengan IPS aktif, dilakukan evaluasi terhadap efektivitas IPS dalam mengembalikan kondisi nilai rata-rata pada setaip parameter yang diukur terkait konsep dari QoS.

- Analisis *Overhead* Sistem: analisis terhadap penggunaan CPU dan memori dalam setaip pengukuran untuk melihat *overhead* yang dihasilkan dari serangan dan penerapan IPS.

6. Kesimpulan, dari hasil analisis data ditarik suatu kesimpulan mengenai dampak dari serangan DDoS dan efektivitas implementasi Snort IPS dalam lingkungan jaringan SDN. Kesimpulan ini diharapkan dapat menjawab rumusan masalah serta memberikan panduan untuk pengembangan dan implementasi lebih lanjut dari sistem IPS pada jaringan SDN.