BAB III
METODE PENELITIAN

3.1 ALUR PENELITIAN

Pada suatu penelitian diperlukan sebuah alur penelitian agar proses yang dilakukan dapat lebih terstruktur dan berjalan dengan baik dan efisien. Salah satu bentuk alur penelitian yaitu *flowchart*, suatu *flowchart* berfungsi untuk menjelaskan secara singkat alur atau proses dari penelitian. *Flowchart* pada penelitian ini ditampilkan pada gambar 3.1.

Gambar 3.1 Diagram Alur Penelitian

Pada bagan *flowchart* diatas dapat dijelaskan secara singkat bahwa penelitian ini awalnya dimulai dengan melakukan studi litelatur berupa mencari dan membandingkan beberapa jurnal yang diambil sebagai referensi melalui internet.sehingga dapat digunakan

sebagai bahan riset pada penelitian ini. Pada blok perancangan topologi merupakan tahap penentuan bentuk topologi yang bertujuan membuat dan menghubungkan berbagai perangkat untuk membuat suatu jaringan internet. Pada blok perancangan Sistem dan Skenario uji yaitu merupakan proses untuk membuat sistem keamanan IPS agar dapat diimplementasikan pada jaringan topologi yang telah dibuat serta pembuatan skenario *rule*s untuk pengujian yang akan dilakukan yang pada hal ini berupa serangan pada jaringan topologi.

Pada blok Pengujian berhasil atau tidak merupakan proses pengujian sistem dan topologi yang telah dibuat dengan parameter keberhasilan berupa keberhasilan sistem keamanan IPS pada jaringan topologi dengan memblokir serangan DoS oleh penyerang yang telah dilakukan secara 30 kali, jika serangan DoS berhasil diblokir dan akan menuju proses pengambilan data dan apabila gagal akan kembali ke blok perancangan sistem dan skenario uji., Pada blok pengambilan data berupa proses mengambil data hasil dari pengujian skenario yang telah dilakukan dan dikumpulkan menjadi data-data pengujian yang valid. Pada blok Analisa dan pengambilan kesimpulan merupakan proses menganalisis data yang ada dan merumuskan hasilnya menjadi kesimpulan dari penelitian yang telah dilakukan.

3.2 ALAT YANG DIGUNAKAN

3.2.1 Perangkat Keras (*Hardware*)

Pada penelitian ini menggunakan 1 perangkat atau device untuk menjalankan aplikasi simulator pada penelitian Implementasi *Intrusion Prevention System* Pada *Software Defined Network* Menggunakan Ryu *Controller* dengan keterangan spesifikasi pada tabel 3.1

Tabel 3.1 Spesifikasi Laptop

Spesifikasi	
Processor	Intel Core I5-5200U (2.20 Ghz (4 CPUs) – 2.2 Ghz)
RAM	4 GB DDR3
Hardisk	500 GB

3.2.2 Perangkat Lunak (*Software*)

Pada penelitian ini menggunakan perangkat lunak sistem operasi Ubuntu dengan *tools* dan aplikasi untuk menjalankan simulasi penelitian *Intrusion Prevention System* Pada *Software Defined Network* Menggunakan Ryu *Controller* dengan spesifikasi pada tabel 3.2..

Tabel 3.2 Perangkat Lunak

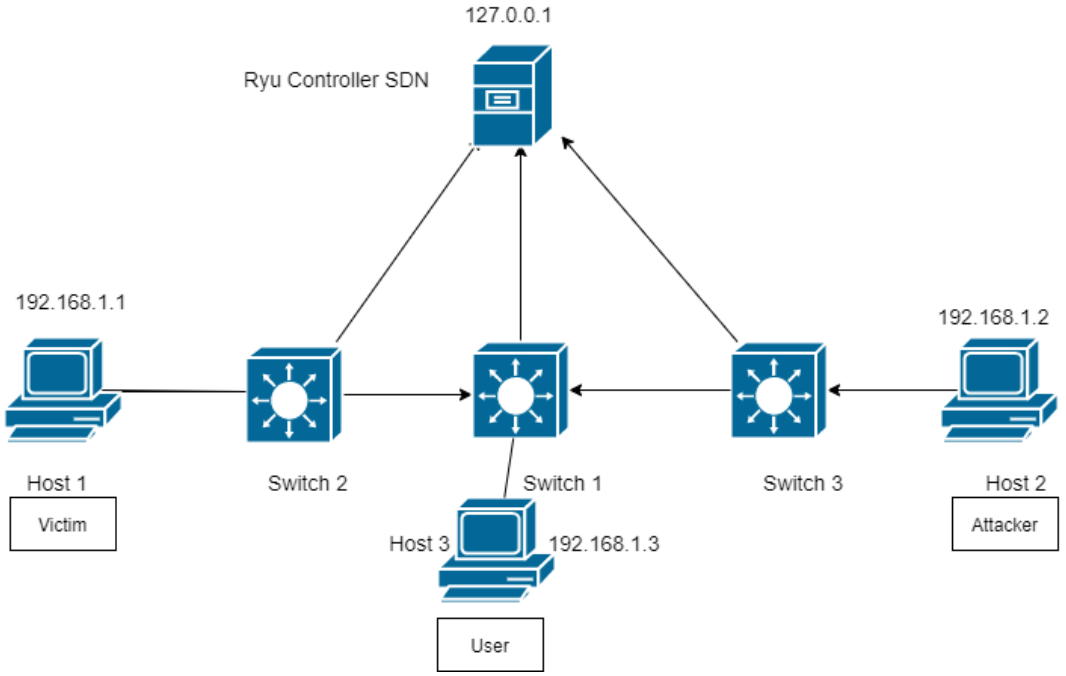
No	Nama Perangkat Lunak	Versi	Fungsi
1	Ubuntu	20.04.2.0	Sistem Operasi
2	Mininet	2.2.2	Simulasi SDN
3	Ryu	4.34	*Controller* SDN
4	Snort	3.0	Aplikasi menjalankan IPS
5	Phyton	3	Bahasa pemrograman untuk menjalankan Ryu
6	Hping3	3.0	Aplikasi Pengujian
7	Iperf	3.9	Aplikasi untuk cek *Bandwidth*

3.3 TOPOLOGI JARINGAN

Pada perancangan topologi jaringan yang digunakan pada penelitian ini berfungsi untuk alur konektivitas pada beberapa perangkat yang berbeda menjadi sebuah suatu jaringan. Pada gambar dibawah perangkat yang digunakan menggunakan 3 switch untuk menyalurkan data, 2 *Host* sebagai pengguna,1 *Host* sebagai penyerang dan 1 perangkat *controller* untuk mengatur dan mengkonfigurasi perangkat yang ada serta sebagai sistem keamanan IPS untuk mencegah dan memblokir tindakan yang mencurigakan pada trafik jaringan dan serangan yang muncul.

Serangan yang dilakukan akan berfokus pada penyerangan yang akan membuat *throughput* jaringan menjadi terganggu dan menyebabkan trafik tinggi sehingga jaringan tersebut akan tidak dapat berjalan. Sehingga sistem keamanan IPS akan menyaring paket data yang masuk dan memblokir akitivitas yang mencurigakan pada paket dan memblokir serangan yang ada dengan penurunan kecepatan *throughput* seminimal mungkin yang

disebabkan pengecekan paket data yang masuk pada sistem keamanan IPS. Kecepatan *throughput* tersebut akan diperiksa menggunakan aplikasi iperf dan *bandwidth* pada jaringan dapat diperiksa dan datanya akan ditampilkan pada bentuk grafik.



Gambar 3.2 Topologi Jaringan

Tabel 3.3 Pengalamatan Ip *Address*

Host	IP *Address*
Host 1 (*Victim*)	192.168.1.1
Host 2 (Attacker)	192,168.1.2
Host 3 (User)	192.168.1.3
Controller	127.0.0.1

1. *Controller* SDN

   Berfungsi untuk mengontrol seluruh *Traffic* atau lalu lintas data pada jaringan SDN. *Controller* yang digunakan adalah Ryu
2. *Host* (*User*)

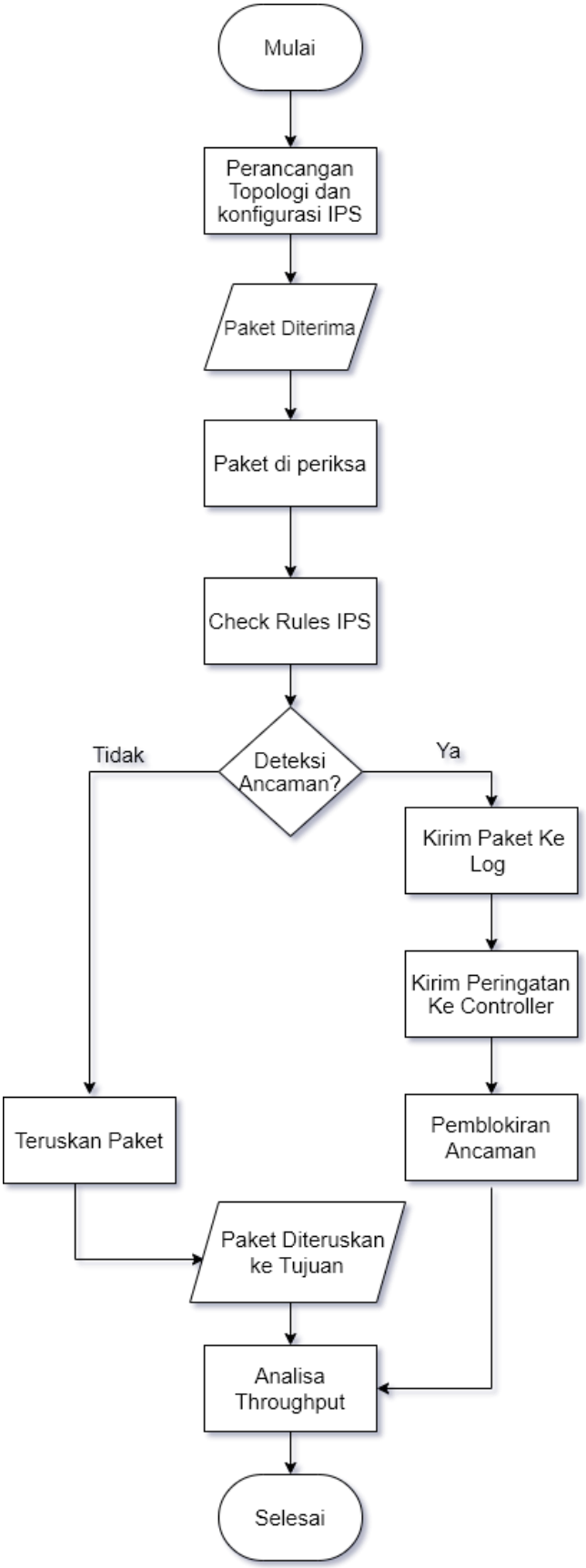
   Host 1-3 Merupakan pengguna yang terhubung pada switch dan dapat mengakses data yang akan menjadi korban hasil serangan *Host* 2
3. *Attacker*

Host 4 merupakan pengguna yang bertujuan untuk menyerang *Controller* ryu yang mengontrol sistem keamanan IPS dengan serangan DoS SYN *Flooding* menggunakan aplikasi hping3.

4. Switch(data plane).
   Merupakan data plane yang berfungsi mengirimkan atau menuruskan paket data ke tujuan.

3.4 PERANCANGAN SISTEM

Penerapan sistem keamanan IPS pada jaringan SDN berfungsi untuk mengidentifikasi dan mencegah serangan DoS SYN *Flooding* yang akan datang. Sistem keamanan IPS menggunakan aplikasi Snort untuk memeriksa paket data yang masuk sesuai dengan *rule*s yang telah dibuat dan paket data yang masuk melalui switch pada data *plane* akan diteruskan ke *controll plane* yaitu *controller* Ryu. Data *plane* dan *controll plane* dapat berkomunikasi menggunakan protokol openflow yang berfungsi menghubungkan data *plane* dan *controll plane*. Paket data SYN yang berbahaya akan diblokir oleh *controller* Ryu dan yang aman akan diteruskan ketujuan. Penjelasan alur perancangan sistem pada penelitian ini akan ditampilkan pada gambar 3.3.



Gambar 3.3 Diagram Alur Sistem

Pada diagram alur sistem penelitian pada gambar 3.3 dijelaskan pada langkah pertama dilakukan konfigurasi topologi jaringan menggunakan aplikasi mininet dan

aplikasi ryu untuk *controller*nya yang hasil topologinya ada pada gambar 3.2 serta konfigurasi sistem keamanan IPS menggunakan aplikasi snort yang telah ditentukan *rule*s untuk memblokir serangan DoS SYN *Flooding*. Selanjutnya paket data masuk ke jaringan yang dikirimkan dari *host* akan melalui switch yang bertindak sebagai data *plane* yang meneruskan paket data tersebut ke *controller* Ryu yang berfungsi sebagai *control plane*. Selanjutnya paket data tersebut akan di *check* sesuai *rules* yang pada. Tahap ini paket data akan disesuaikan dengan aturan *rule*s pada IPS menggunakan aplikasi snort dan apabila paket data yang masuk tidak berbahaya maka akan langsung diteruskan ke data *plane* yang nantinya paket data tersebut dikirimkan ke *host* tujuan.

Pada *host*2 yang terhubung dengan switch 3 yang akan bertindak sebagai penyerang mengirimkan serangan DoS SYN *Flooding* menggunakan apikasi Hping3 akan mengirimkan paket data SYN melalui switch yang bertindak sebagai data *plane* yang meneruskan paket daya SYN tersebut ke ke *host* 1 yang bertindak sebagai korban dan disesuaikan dengan *rule*s yang telah dibuat sehingga jika terdeteksi berbahaya paket data SYN tersebut akan dikirim ke log dan peringatan akan dikirimkan ke *controller* Ryu dan paket data SYN pada serangan SYN *flooding* dilakukan pemblokiran oleh snort dan akan ada notifikasi pemblokiran pada *controller* ryu. Paket data yang dianggap aman akan dikirimkan *controller* ke tujuan melalui switch yang bertindak sebagai data *plane*. Langkah terakhir paket data yang diterima akan dilakukan analisa *throughput* jaringan yang bertujuan untuk mengetahui kinerja dan kecepatan dari sistem keamanan IPS.

3.5 SKENARIO PENGUJIAN

Pada pengujian yang dilakukan pada penelitian ini difokuskan untuk menguji *avaibility* atau sumber daya jaringan dengan melakukan uji coba serangan *Denial Of Service* (DoS) dengan tipe serangan *Traffic Flooding* dengan bentuk serangan *SYN Flooding* menggunakan aplikasi Hping3 dari *Host2* yang terhubung dengan switch2 yang bertindak sebagai penyerang. *Host* 2 akan mengirimkan paket SYN ke arah *Host 1* dengan pengujian sebanyak 30x. Paket SYN normalnya berisi alamat sumber yang menunjukan sistem aktual yang bertujuan memulai koneksi ke server atau target secara penuh sedangkan paket SYN *Flooding* berisi alamat sumber yang tidak aktual yang berfungsi memulai koneksi ke target tanpa menyelesaikan koneksi sehingga target harus menghabiskan sumber daya untuk menunggu koneksi yang setengah terbuka dan menyebabkan target atau server tidak dapat melayani permintaan *Host*.. Pengujian dan pengambilan data QoS berupa *Throughput* , *Latency*, CPU *Load* dan memori yang

dilakukan sebelum serangan,.saat serangan dan saat blokir untuk mengetahui performa dan kecepatan hasil implementasi sistem keamanan IPS setelah pengujian dilakukan. Pengujian Throughput menggunakan aplikasi iperf sedangkan pengujian *latency* menggunakan aplikasi ping dan pengujian CPU *load* dan memori menggunakan perintah htop.

Tabel 3.4 Skenario Pengujian Serangan

No	Jenis Serangan	Parameter	*tools*
1	*SYN Flood*	*Avaibility*	Hping3

3.6 PARAMETER PENGUJIAN

Pengujian Parameter dilakukan untuk mengetahui performa pada jaringan SDN. Dilakukan untuk mengetahui performa jaringan pada saat sebelum serangan,saat serangan dan saat blokir. Parameter yang akan di uji yaitu *Throughput*, *Latency*,CPU *load* serta memori dan akan di uji pada pengguna dan penyerang. Berikut Tabel dari skenario pengujian parameter.

Tabel 3.5 Pengujian *Throughput*

Pengujian	*Throughput*		
	Sebelum Serangan	Saat Serangan	Saat Blokir
	User	*User*	*User*
Percobaan 1			
Percobaan 2			
Percobaan 3			
Percobaan 4			
Percobaan 5			
Percobaan 6			
Percobaan 7			
Percobaan 8			
Percobaan 9			
Percobaan 10-30			

Tabel 3.6 Pengujian *Latency*

Pengujian	*Latency*		
	Sebelum Serangan	Saat Serangan	Saat Blokir
	User	*User*	*User*

Percobaan 1			
Percobaan 2			
Percobaan 3			
Percobaan 4			
Percobaan 5			
Percobaan 6			
Percobaan 7			
Percobaan 8			
Percobaan 9			
Percobaan 10-30			

Tabel 3.7 Pengujian Penggunaan CPU

Pengujian	CPU		
	Sebelum Serangan	Saat Serangan	Saat Blokir
	User	*User*	*User*
Percobaan 1			
Percobaan 2			
Percobaan 3			
Percobaan 4			
Percobaan 5			
Percobaan 6			
Percobaan 7			
Percobaan 8			
Percobaan 9			
Percobaan 10-30			

Tabel 3.9 Pengujian Penggunaan Memori

Pengujian	Memori		
	Sebelum Serangan	Saat Serangan	Saat Blokir
	User	*User*	*User*
Percobaan 1			
Percobaan 2			
Percobaan 3			

Percobaan 4			
Percobaan 5			
Percobaan 6			
Percobaan 7			
Percobaan 8			
Percobaan 9			
Percobaan 10-30			