# BAB III

# METODE PENELITIAN

## 3.1. Metodologi Penelitian

Berikut ini pada gambar 3.1 merupakan tahapan-tahapan yang akan dilakukan dalam penelitian ini.


Gambar 3.1 Tahapan penelitian

Tahap awal penelitian dilakukan proses analisis sistem untuk menentukan aplikasi dan *operating system* yang akan dilakukan untuk melakukan implementasi dan pengujian pada penelitian ini. Tahap selanjutnya yaitu mengidentifikasi kebutuhan hardware dan software untuk mendukung implementasi penelitian. Setelah itu melakukan perancangan atau skenario yang akan dilakukan dalam pengujian aplikasi IDS. Setelah itu dilakukanlah implementasi dari perancangan pengujian yang telah dibuat sebelumnya untuk mendapatkan sebuah data yang akan dijadikan bahan perbandingan aplikasi. Tahap terakhir dari penelitian ini adalah membandingkan kinerja aplikasi *snort* dan *suricata* dari data yang didapatkan dalam pengujian.

## 3.2. Analisis Sistem

Pada tahap ini dilakukan analisis terhadap ruang lingkup umum sistem yang menjadi fokus penelitian. Pengukuran kinerja IDS melibatkan perangkat lunak, perangkat keras, *tools* khusus yang dapat digunakan untuk melakukan pengujian atau serangan terhadap IDS.

## 3.3. Identifikasi Kebutuhan Hardware dan Software

Terdapat beberapa hardware dan software yang harus disedikan untuk melakukan percobaan pada penelitian ini. Spesifikasi hardware yang digunakan pada penelitian ini ditampilkan pada Tabel 3.1.

Tabel 3.1 Spesifikasi *hardware* yang digunakan

| No | Item | Versi/Spesifikasi |
|---|---|---|
| 1 | Processor | Intel(R) Core(TM) i3-5005U CPU @ 2.00GHz |
| 2 | Memory | 12 GB |
| 3 | Harddisk | 512 GB |

Pembagian spesifikasi pada virtualisasi yang dilakukan pada implementasi pengujian ditampilkan pada Tabel 3.2.

Tabel 3.2 Pembagian spesifikasi virtualisasi

| No | Operating System | Memori | Storage |
|---|---|---|---|
| 1 | Ubuntu Server | 4 GB | 10 GB |
| 2 | Router OS (Pfsense) | 2 GB | 3 GB |
| 3 | Kali Linux (*Attacker*) | 2 GB | 10 GB |

Spesifikasi software yang digunakan pada percobaan dalam penelitian ini ditampilkan pada Tabel 3.3.

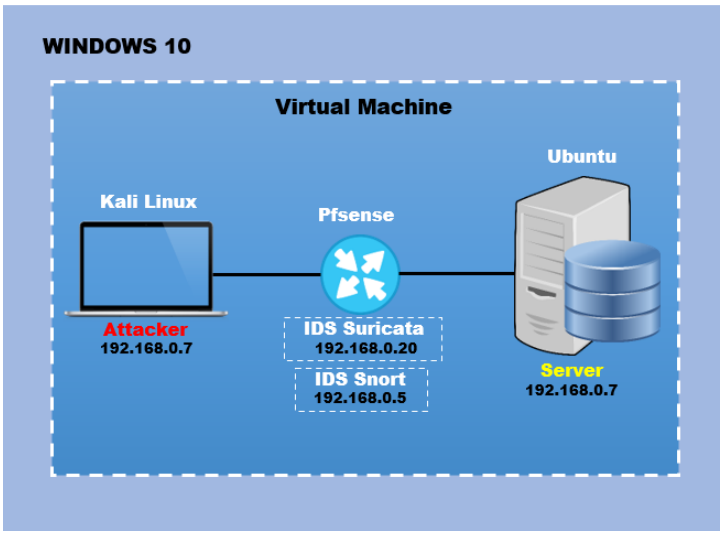
Tabel 3.3 Spesifikasi *software* yang digunakan

| No | Kebutuhan | Versi/Spesifikasi |
|---|---|---|
| 1 | Operating System | Windows 10 Pro |
| 2 | Oracle Virtual Box | 6.1 |
| 3 | Server Linux Ubuntu | 20.04 |
| 4 | Web Server Nginx | 1.18.0 |

| | | |
|---|---|---|
| 5 | Kali Linux | 2021.1 |
| 6 | Pentmenu | 1.7.4 |
| 7 | SNORT | 4.1.4_3 |
| 8 | Pfsense | 2.5.0 |
| 9 | Suricata | 6.0.0_11 |

### 3.4. Perancangan Arsitektur Sistem

Arsitektur jaringan yang dibuat pada percobaan dalam penelitian ini dibangun dalam lingkungan *virtual machine*. Terdapat 3 komponen utama dalam jaringan yang perlu dipersiapakan untuk percobaan, yaitu *server* yang dijadikan target serangan, IDS yang akan mencoba mencatat serangan yang diarahkan ke *server*, dan *attacker* yang bertindak melakukan serangan. Secara umum arsitektur sistem yang dikembangkan ditampilkan pada gambar 3.2.




Gambar 3.2 Skema Jaringan Penelitian

### 3.5. Implementasi dan Pengujian

Aktifitas yang dilakukan pada tahap implementasi diawali dengan instalasi *Virtual Machine*. Instalasi Ubuntu, Instalasi Pfsense Router, Instalasi Kali Linux,

semuanya dilakukan pada machine. Pada *Pfsense Router* dilakukan instalasi *Snort* dan *Suricata*. Konfigurasi IP Address dan IDS sesuai dengan gambar 3.2.

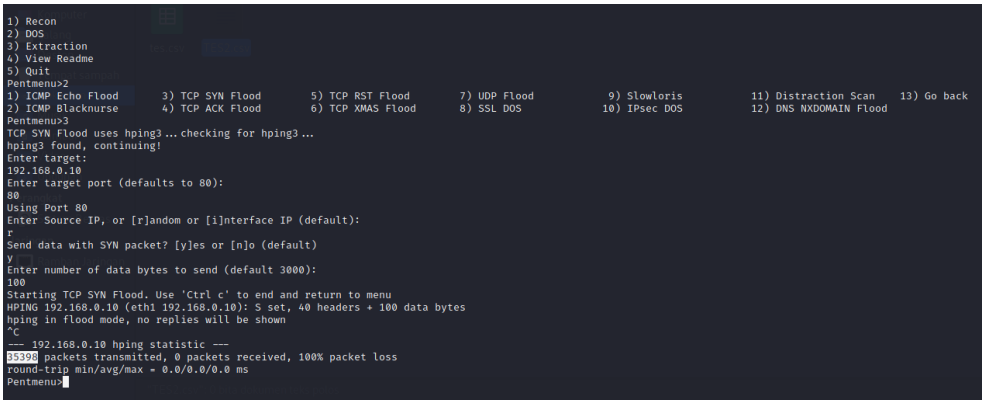
Pengujian yang dilakukan pada penelitian ini, dibuat menjadi sepuluh percobaan yang akan dicari data untuk dijadikan bahan pengukuran kinerja aplikasi IDS, percobaan pada tabel 4 menjelaskan percobaan yang digunakan untuk mencari data kinerja dari jenis serangan TCP *Syn Flooding*, TCP *All Flag* (XMAS *Flooding*), dan *Slowloris Attack*. Secara umum data yang dicoba pada pengujian ditampilkan pada Tabel 3.4.

Tabel 3.4 Skenario pengujian

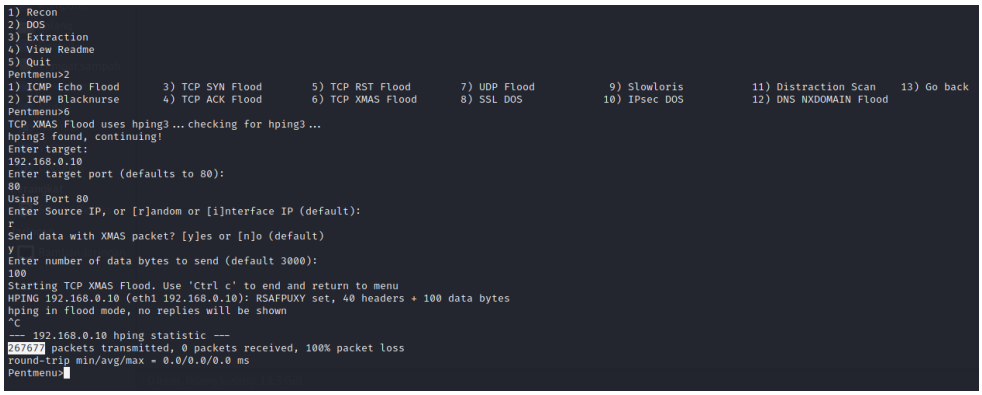
| Percobaan ke | Syn Flooding | | XMAS Flood | | Slowloris |
|---|---|---|---|---|---|
| | Packet Size (byte) | Waktu Pengujian (second) | Packet Size (byte) | Waktu Pengujian (second) | Open Connection |
| 1 | 100 | 30 | 100 | 30 | 100 |
| 2 | 200 | 30 | 200 | 30 | 200 |
| 3 | 300 | 30 | 300 | 30 | 300 |
| 4 | 400 | 30 | 400 | 30 | 400 |
| 5 | 500 | 30 | 500 | 30 | 500 |
| 6 | 600 | 30 | 600 | 30 | 600 |
| 7 | 700 | 30 | 700 | 30 | 700 |
| 8 | 800 | 30 | 800 | 30 | 800 |
| 9 | 900 | 30 | 900 | 30 | 900 |
| 10 | 1000 | 30 | 1000 | 30 | 1000 |

Berdasarkan percobaan serangan *syn flooding, xmas flood,* dan *slowloris* menggunakan aplikasi serangan yang bernama *pentmenu*. Aplikasi ini dapat menguji target dengan berbagai jenis serangan dari *denial of service*. Serangan *syn flood* dan *xmas flood* akan dilakukan dengan *packet size* sebesar 100 byte sampai 1000 byte dengan paket yang dikirim per *IP address* sebanyak 40 paket, sedangkan untuk serangan *slowloris* menguji dengan membuka koneksi sebanyak 100 sampai

1000 koneksi. Gambar 3.3 dan Gambar 3.4 merupakan data yang akan diambil serta bukti mengirimkan 40 paket per IP *address*.

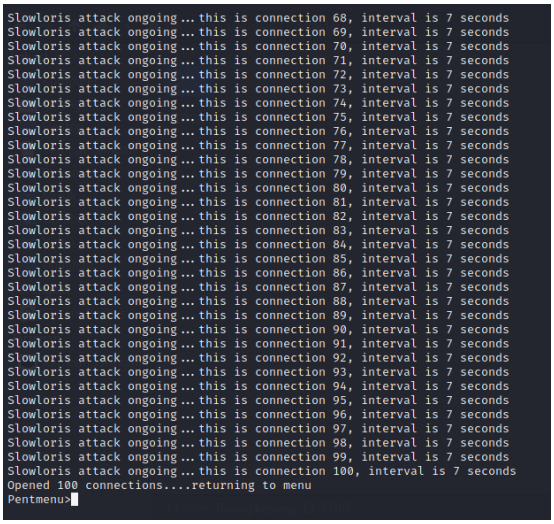



Gambar 3.3 Contoh total paket terkirim serangan *syn flood*




Gambar 3.4 Contoh total paket terkirim serangan *xmas flood*

Serangan selanjutnya yaitu *slowloris* melakukan pengujian dengan membuka koneksi. Gambar 3.5 merupakan total koneksi terbuka dengan serangan *slowloris.*




Gambar 3.5 Contoh total koneksi terbuka serangan *slowloris*

## 3.6. Pengukuran Hasil Pengujian

Setiap percobaan yang dilakukan, akan menghasilkan data yang dicatat pada tabel. Pengukuran hasil percobaan difokuskan pada 4 parameter, diantaranya: jumlah deteksi serangan, penggunaan CPU, penggunaan memori, dan *load average*. Setelah dilakukan 10 kali percobaan, dihitung nilai rata-rata dari data yang diperoleh. Hasil perhitungan juga disajikan dalam bentuk grafik.