BAB III
METODE PENELITIAN

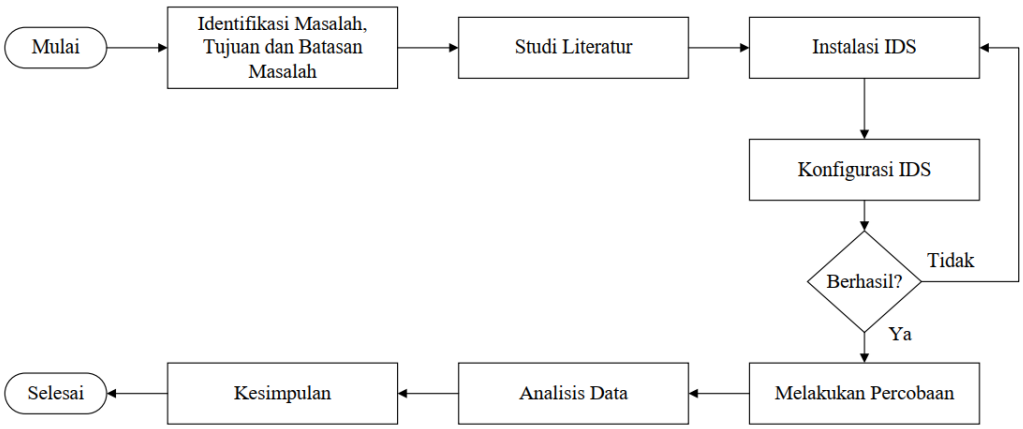
3.1 Desain Penelitian

Paramita (2021) menjelaskan bahwa penelitian kuantitatif mengacu pada pandangan filsafat positivisme. filsafat positivisme memandang suatu bahwa fenomena dalam penelitian dapat diklasifikasikan, relatif tetap, konkrit, teramati, terukur, dan hubungan gejala bersifat sebab akibat. Menurut Paramita (2021) jenis penelitian *Research and Development* (R&D) bukan hanya untuk menggambarkan hubungan antara keadaan sekarang, tetapi juga untuk menyelidiki perkembangan dan perubahan yang terjadi sebagai fungsi waktu. Penelitian dan pengembangan memiliki dua bagian, yaitu: penelitian dan pengembangan.

Dalam penerapannya desain penelitian menggunakan metode kuantitatif dengan pendekatan R&D. Desain penelitian yang digunakan bermaksud untuk membandingkan performa IDS, dengan mempertimbangkan parameter TPR, FPR, TNR, FNR kecepatan deteksi serangan, *CPU usage*, *memory usage*, dan *network usage*.

3.2 Alur Penelitian

Alur penelitian dibuat bermaksud untuk mengarahkan penelitian dengan struktur yang sistematis, serta mempermudah dalam memahami proses alur penelitian. Berikut merupakan ilustrasi alur penelitian yang dijelaskan pada Gambar 3.1:



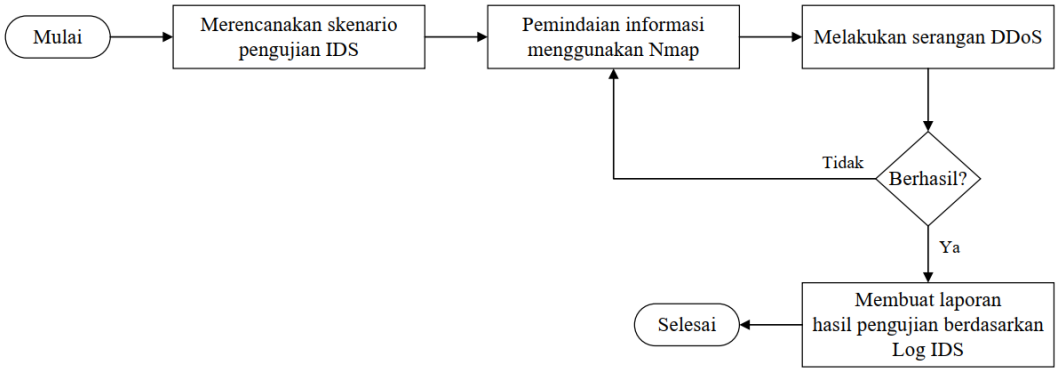
Gambar 3. 1. Alur Penelitian

Farhan Maulana, 2024
Analisis Perbandingan Performa Intrusion Detection System (IDS) Dalam Mendeteksi Serangan Port Scanning dan Distributed Denial of Service (DDoS)
Universitas Pendidikan Indonesia | repository.upi.edu | Perpustakaan.upi.edu

1. Identifikasi Masalah, serta menganalisis sumber yang relevan dengan topik yang diangkat untuk mendapatkan pemahaman yang komprehensif tentang penelitian yang akan dilakukan.
2. Instalasi IDS, pada tahap ini peneliti akan menentukan NIDS *tools* yang akan digunakan untuk penelitian dan melakukan proses instalasi NIDS tools yang digunakan untuk dilakukan uji coba, *tools* yang digunakan pada penelitian ini yaitu *Snort 3*, *Suricata* dan *Zeek*.
3. Konfigurasi IDS, pada tahap ini peneliti akan mengkonfigurasi NIDS *tools* yang sudah diinstal, kemudian akan dilakukan pengaturan dengan menyesuaikan kebutuhan yang diperlukan untuk dilakukan pengujicobaan.
4. Melakukan percobaan, pada tahap ini peneliti akan melakukan percobaan terhadap NIDS *tools* yang telah diinstalasi dan dikonfigurasi menggunakan skenario yang digunakan untuk mendapatkan data yang akan dianalisis.
5. Analisis data, pada tahap ini peneliti akan menganalisis data hasil percobaan dan mengolah data berdasarkan parameter yang digunakan. Hasil data primer terbagi menjadi dua, yang diantaranya yaitu data log deteksi NIDS, dan data monitoring *resource usage*. Data Log kemudian dianalisis untuk mendapatkan parameter TPR, FPR, TNR dan FNR, data *monitoring* kemudian dianalisis untuk mendapatkan parameter *resource usage*. Kemudian hasil analisis data dapat dijadikan kesimpulan penelitian.
6. Kesimpulan, pada tahap ini peneliti akan menyimpulkan analisis data dari hasil percobaan yang dilakukan, kemudian disusun menjadi beberapa poin penting.

3.3 Alur Percobaan

Alur percobaan dibuat dengan bermaksud untuk mempermudah dalam memahami proses alur percobaan. Berikut merupakan ilustrasi tahapan alur percobaan yang dijelaskan pada Gambar 3.2:



Gambar 3. 2. Alur Percobaan

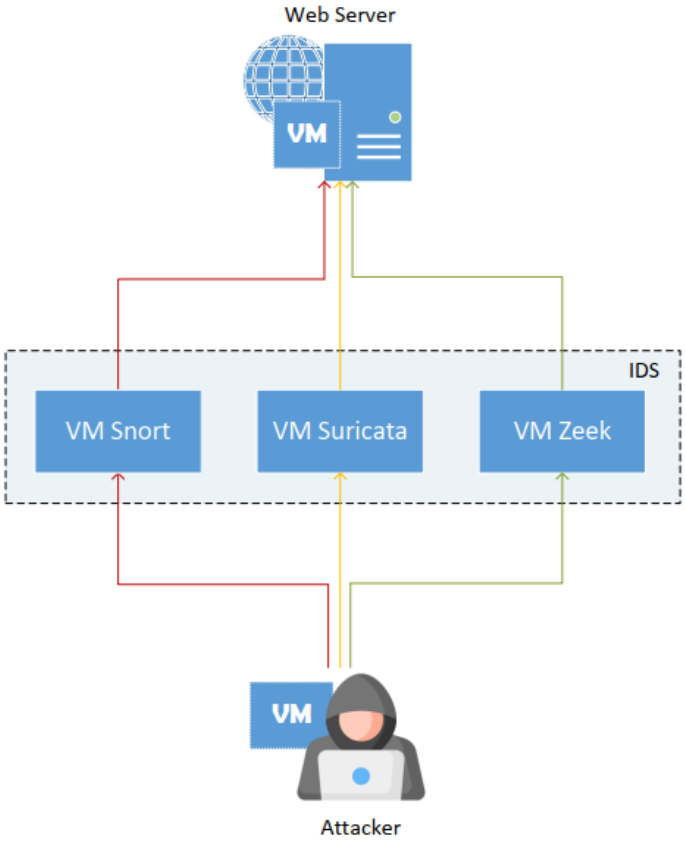
1. *Planning*, pada tahap ini peneliti akan merencanakan skenario penelitian dengan mempersiapkan terlebih dahulu IDS yang digunakan, seperti *Snort 3, Suricata*, dan *Zeek.*
2. *Discovery*, pada tahap ini peneliti akan melakukan pemindaian informasi target terlebih dahulu dengan cara menggunakan serangan PS untuk mengindentifikasi *port* dan layanan jaringan. Kemudian, peneliti akan menganalisis kerentanan berdasarkan hasil pemindaian.
3. *Attack*, pada tahap ini peneliti akan melakukan serangan DDoS dengan acuan kerentanan *port*, layanan jaringan dengan tujuan untuk mengeksploitasi kerentanan yang ada pada target.
4. *Report*, pada tahap ini laporan dibuat dimulai dari tahap *planning* hingga tahap *attack*, peneliti akan melaporankan hasil pengumpulan informasi kerentanan hingga hasil serangan yang telah dilakukan yang diambil dari log IDS yang terdeteksi.

3.4 Perancangan Sistem

Perancangan sistem dimaksudkan untuk memberikan informasi penting untuk memberikan informasi perancangan topologi jaringan, skenario penelitian.

3.4.1 Topologi Jaringan

Topologi jaringan yang akan digunakan pada penelitian ini yaitu dengan menggunakan simulasi melalui *virtual machine* (VM). Berikut merupakan ilustrasi topologi jaringan yang akan digunakan pada penelitian ini, yang dijelaskan pada Gambar 3.3:

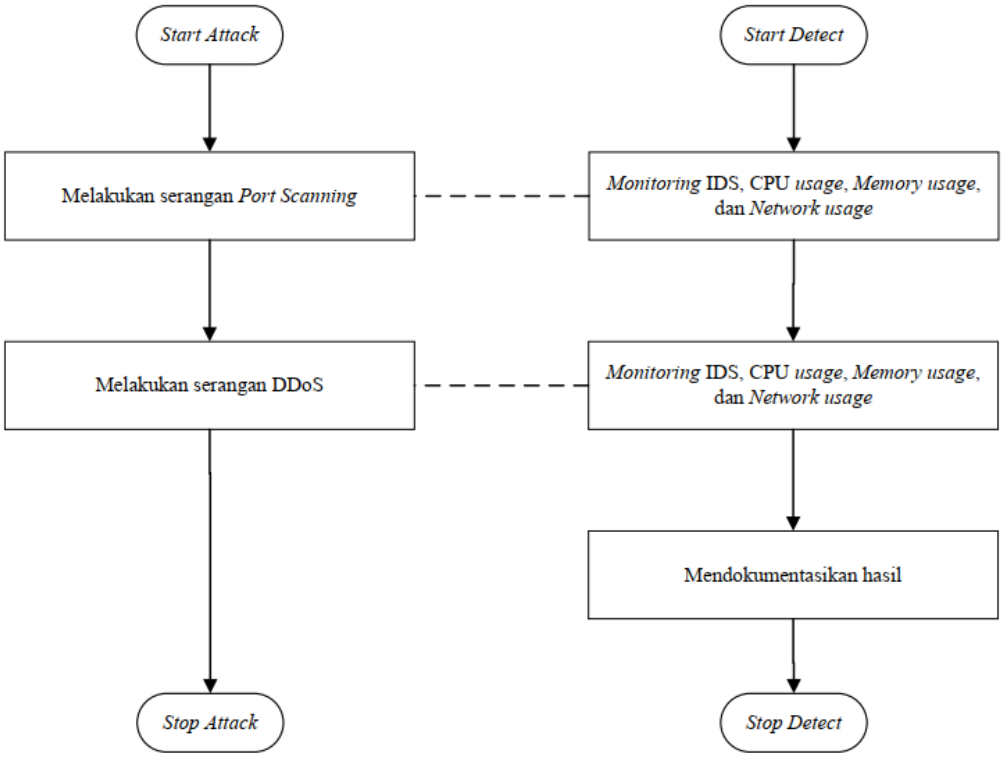


Gambar 3. 3. Topologi Jaringan

Gambar 3.3 merupakan topologi jaringan yang peneliti gunakan, pada penelitian ini *attacker* melakukan serangkaian penyerangan PS dengan menggunakan *Nmap* dan DDoS menggunakan *Hping3*. Kemudian dideteksi oleh IDS. Pengujian serangan dan deteksi menggunakan IDS dilakukan melalui beberapa tahapan yang terpisah melalui tiga alur yang berbeda, yang ditunjukan menggunakan alur warna. IDS *Snort* ditunjukan melalui alur warna merah, IDS *Suricata* ditunjukan melalui alur warna kuning, IDS *Zeek* ditunjukan melalui alur warna hijau.

3.4.2 Skenario Penelitian

Perancangan skenario penelitian dimaksudkan untuk menggambarkan proses serta mempermudah memahami proses skenario. Skenario penelitian dilakukan secara berulang-ulang selama proses pengumpulan data penelitian. Berikut merupakan proses alur skenario yang dijelaskan pada Gambar 3.4:



Gambar 3. 4. Skenario Penelitian

Skenario pengujian pada penelitian ini menggunakan 3 skenario yang diantaranya dijelaskan sebagai berikut:

1. Skenario pertama yaitu ketika dilakukan serangan PS dan DDoS terhadap web server yang kemudian dideteksi oleh IDS *Snort*.
2. Skenario kedua yaitu ketika dilakukan serangan PS dan DDoS terhadap web server yang kemudian dideteksi oleh IDS *Suricata*.
3. Skenario ketiga yaitu ketika dilakukan serangan PS dan DDoS terhadap web server yang kemudian dideteksi oleh IDS *Zeek*.

3.5 Pengukuran Data

Dalam proses analisis data, diperlukannya pengukuran data untuk membandingkan hasil nilai parameter yang didapat. Pada penelitian ini, peneliti akan melakukan repetisi sebanyak 100 kali. Hal ini dikarenakan menurut Prabowo dkk (2023) data yang dikumpulkan dari percobaan yang diulang-ulang memberikan dasar yang lebih kuat untuk analisis dan interpretasi. Formula yang digunakan untuk pengukuran data untuk menghitung nilai rata-rata yaitu sebagai berikut:

$$\overline{x} = \frac{x1 + x2 + x3 + x4 + x5 + x6 + x7 + x8 + \ldots + xn}{\text{n}} \quad (5)$$

Berdasarkan formula pengukuran data diatas, dibawah ini dijelaskan penjelasan mengenai persamaan diatas, berikut merupakan keterangannya:

$\overline{x}$ = Nilai Rata-rata

$x(n)$ = Data repetisi ke-n

n = Banyak data

3.6 Alat dan Bahan

Dalam proses penelitian, diperlukan alat dan bahan yang dapat mendukung keberhasilan proses penelitian. Tabel 3.1 menampilkan tentang perangkat keras yang digunakan serta spesifikasi perangkat, Tabel 3.2 berisi tentang perangkat lunak yang digunakan serta spesifikasinya.

Tabel 3. 1. Informasi Hardware

No	*Hardware*	Spesifikasi
1.	PC #1 (*host*)	Intel (R) Core (TM) i5-10210U CPU @ 1.60 GHz (4 Core), N 2.1 GHz - 12 GB RAM.
2.	PC #2 *Snort* IDS	2 Core - 4 GB RAM
3.	PC #3 *Suricata* IDS	2 Core - 4 GB RAM.
4.	PC #4 *Zeek* IDS	2 Core - 4 GB RAM.
5.	PC #5 (*attacker*)	2 Core - 4 GB RAM.
6.	PC #6 (web server)	1 Core – 2 GB RAM.

Tabel 3. 2. Informasi Software

No	*Software*	Spesifikasi
1.	*Operating System* PC #1	*Windows 11 Home Single Language 64-bit.*
2.	*Operating System* PC #2	*Ubuntu Dekstop LTS 22.04 64-bit*
3.	*Operating System* PC #3	*Ubuntu Dekstop LTS 22.04 64-bit*
4.	*Operating System* PC #4	*Ubuntu Dekstop LTS 22.04 64-bit*
5.	*Operating System* PC #5	*Kali Linux 2022.3, Debian 64-bit*
6.	*Operating System* PC #6	*Ubuntu Dekstop LTS 22.04 64-bit*
7.	*Snort* 3	*Version 3.1.72.0*
8.	*Suricata*	*Version 7.0.1*
9.	*Zeek*	*Version 6.0.1*

10.	*Oracle Virtual Box*	*Version 7.0.10*
11.	*System Activity Report*	*Version 2023*

Lingkungan tempat peneliti melakukan konfigurasi dan penyebaran tiga NIDS *Snort, Suricata,* dan *Zeek* didasarkan pada mesin fisik yang dilengkapi dengan prosesor Intel (R) Core (TM) i5-10210U CPU @ 1.60 GHz (4 Core), N 2.1 GHz dengan kapastias RAM sebesar 12 GB. Analisis perbandingan dilakukan dalam lingkungan simulasi yang didasarkan pada perangkat lunak *Virtual box*.

Lingkungan simulasi penelitian terdiri dari sejumlah lima VM, tiga NIDS *Snort, Suricata,* dan *Zeek* dan web server sebagai *victim* atau pihak yang diserang oleh *attacker* dan satu *attacker*, penulis membuat skenario yang dimana NIDS dipasangkan dan dikonfigurasi pada *interface victim*. Penulis membuat kofigurasi VM NIDS dengan memiliki 2 *core* untuk CPU, dan 4 GB RAM, dan 25 GB *Harddisk,* dengan sistem operasi yang digunakan yaitu Ubuntu 22.04 LTS.

3.7 Jadwal Penelitian

Jadwal penelitian yang meliputi persiapan, perencanaan, pelaksanaan dan penyusunan laporan penelitian.

Tabel 3. 3. Jadwal Penelitian

No.	Kegiatan	Bulan			
		1	2	3	4
1.	Perumusan Topik Penelitian				
	a. Penentuan Judul dan Arah Penelitian				
	b. Pengumpulan Studi Literatur				
2.	Pengajuan Rancangan Penelitian				
3.	Pelaksanaan Penelitian				
	a. Percobaan Penelitian				
	b. Analisis Percobaan Penelitian				
4.	Penyusunan Laporan				