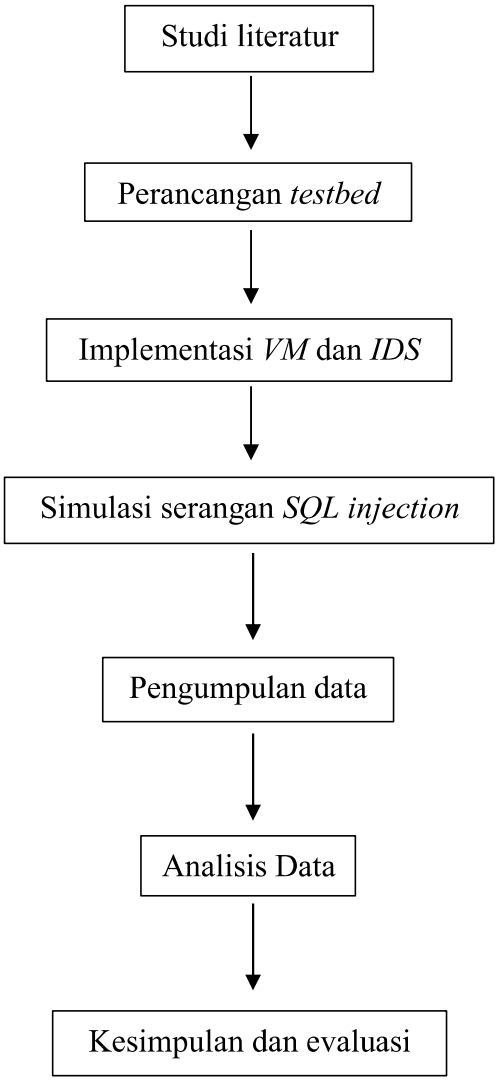
BAB lll

METODE PENELITIAN

3.1 Desain Penelitian

Pada desain penelitian ini menyediakan kerangka dan alur kerja mencangkup sepanjang proses penelitian. Dalam desain penelitian ini, penulis memberi tahapan penelitian yang diangkat sebagai berikut:



Gambar 3. 1 Desain Penelitian

Berdasarkan gambar desain penelitian di atas, berikut adalah penjelasan dari masing masing komponen dalam setiap kotak sebagai berikut:

1. Studi literatur

Tahap awal penelitian dimulai dengan studi literatur yang bertujuan untuk memperoleh pemahaman mengenai topik yang diteliti. Kegiatan ini mencangkup penelusuran jurnal ilmiah, buku, artikel dan sumber relevan untuk mengidentifikasi teori, metode, dan hasil penelitian terdahulu yang berkaitan.

2. Perancangan Testbed

Langkah selanjutnya adalah mempersiapkan perangkat keras dan lunak yang dibutuhkan untuk pelaksanaan penelitian. Dalam hal ini, digunakan satu unit laptop dengan spesifikasi: *RAM* 16 GB, SSD 240 *GB*, dan *prosesor AMD Quad – Core*. Perangkat lunak *IDS Snort* dan *Suricata*, *virtual machine attacker* dan *victim*.

3. Implementasi VM dan IDS

Langkah selanjutnya dilakukan proses konfigurasi sistem sesuai kebutuhan penelitian. Tahap ini mencakup instalasi *software*, pengaturan lingkungan, serta penyesuaian parameter sistem agar mendukung metode dan alat analisis yang akan digunakan.

4. Simulasi serangan SQL Injection

Setelah implentasi *Virtual Machine* dan *Intruction Detection System*, selanjutnya melakukan simulasi serangan menggunakan *SQL Injection manual* di *VM attacker*.

5. Pengumpulan Data

Dalam penelitian ini, *ground truth* dijadikan acuan klasifikasi hasil deteksi, yang diperoleh melalui pelabelan manual terhadap 30 paket data untuk menentukan ada tidaknya serangan *SQL*. Dengan dasar ini, *alert* dari *IDS* dikategorikan menjadi *TP, FP, FN* dan *TN*, sehingga metrik evaluasi seperti *accuracy, precision*, *recall*, dan *F1 score* dapat dihitung secara objektif.

6. Analisis Data

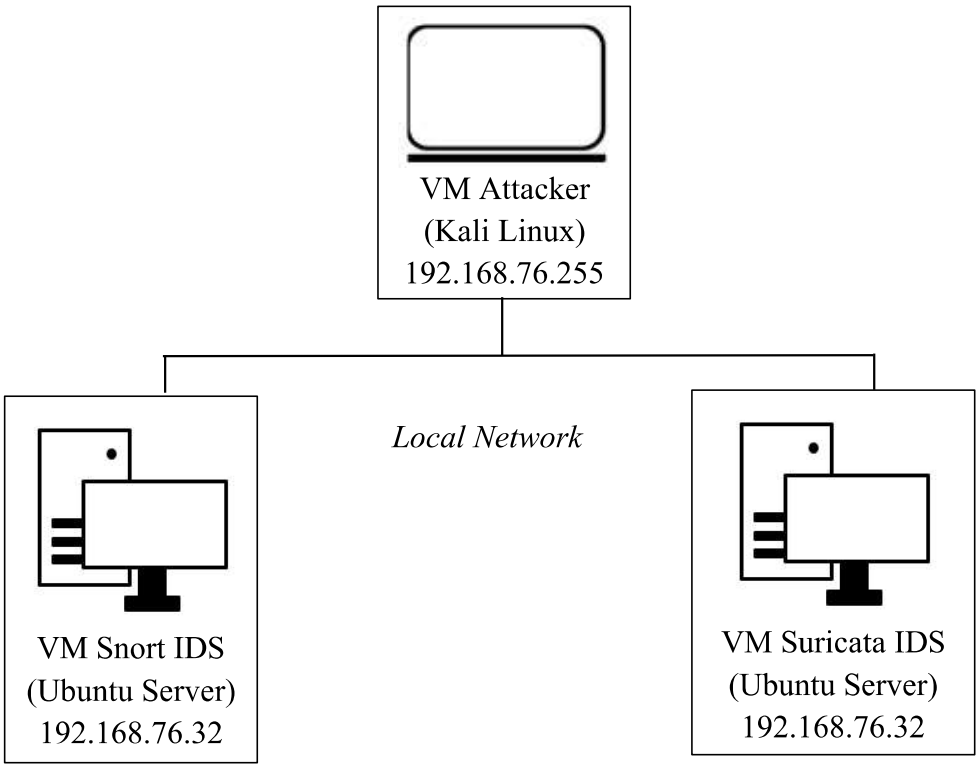
Pada tahap ini merupakan pengambilan hasil data dari sistem yang telah dikonfigurasi sebelumnya, kemudian dilanjutkan dengan proses analisis data. Analisis dilakukan untuk menginterpretasikan hasil yang diperoleh, mengevaluasi kinerja sistem, serta menarik kesimpulan berdasarkan tujuan penelitian.

7. Kesimpulan dan Evaluasi

Tahap terakhir peneliti akan menyimpulkan membahas hasil performa dari kedua *IDS* yaitu *Snort* dan *Suricata* dalam mendeteksi serangan *SQL Injection*, serta evaluasi untuk peneliti kedepannya.

3.2 Topologi

Simulasi ini terdiri dari dua komponen utama: *VM Attacker* (Kali Linux) sebagai pihak penyerang, *VM Snort IDS* dan *Suricata IDS* (Ubuntu Server) sebagai sistem deteksi intruksi, yang terhubung dalam jaringan internal untuk menguji efektivitas kedua *IDS* tersebut.



Gambar 3. 2 Topologi Jaringan

Pada gambar 3.2 topologi yang akan digunakan pada saat proses implementasi. Pada topologi diatas terdapat *Virtual Machine attacker* dan *Virtual Machine server* yang terhubung dalam jaringan *Internet Local*. *IDS* akan berjalan pada *software VirtualBox* dan menggunakan sistem operasi *Ubuntu*. *VM attacker* sendiri akan dilakukan instalasi *Kali linux* dan *SQL Injection manual* sebagai penyerangan. Serangan dilakukan dengan cara menyerang *web DVWA* dengan *rules* yang sudah disiapkan.

3.3 Metode Pengumpulan Data

Metode pengumpulan data penelitian ini menggunakan metode eksperimen, dengan menggunakan deteksi intrusi, yaitu *Snort* dan *Suricata*. Kedua sistem ini digunakan untuk memantau lalu lintas jaringan dan menangkap berbagai jenis data seperti *packet data*, *log* aktivitas, serta *alert* terhadap potensi ancaman. Penelitian

ini menggunakan *ground truth* sebagai acuan kebenaran dalam mengklasifikasikan hasil deteksi. *Ground truth* diperoleh melalui proses klasifikasi manual terhadap 30 jenis paket data yang digunakan dalam pengujian. Setiap paket dianalisis dan diberi label berdasarkan apakah paket tersebut mengandung serangan SQL atau tidak. Dengan adanya *ground truth* ini, setiap alert yang dihasilkan oleh sistem *IDS* dapat diklasifikasikan ke dalam empat kategori utama, yaitu *True Positive* (*TP*), *False Positive* (*FP*), *False Negative* (*FN*), dan *True Negative* (*TN*), sehingga memungkinkan perhitungan metrik evaluasi seperti akurasi, presisi, *recall*, dan *F1-score* secara objektif dan terukur. Data terkumpul dalam bentuk *file log* dan *json* yang berisi lalu lintas jaringan mentah, serta *log file* yang mencatat informasi detail tentang aktivitas yang terdeteksi, seperti alamat *IP* sumber dan tujuan, jenis serangan, dan waktu kejadian. Jumlah data yang yang terkumpul sebanyak 30 jenis paket data. Adapaun rincian fitur yang akan dianalisa adalah sebagai berikut:

3.3.1 *Snort* Data

Berikut merupakan skenario serangan dalam proses pengumpulan data pada *Snort*:

Tabel 3. 1 *Snort* Data

No	Alamat IP	Tujuan	Jenis serangan	Waktu kejadian
1	192.162.72.255	192.168.76.32	' OR 1=1-- -	07/08-06:05:34.112
2	192.162.72.255	192.168.76.32	SELECT * FROM users WHERE id=1	07/08-06:05:45.223
3	192.162.72.255	192.168.76.32	1' UNION SELECT null, version() --	07/08-06:05:56.334

No	Alamat IP	Tujuan	Jenis serangan	Waktu kejadian
4	192.162.72.255	192.168.76.32	GET /index.html HTTP/1.1	07/08-06:06:07.445
5	192.162.72.255	192.168.76.32	' OR EXISTS (SELECT* FROM users) --	07/08-06:06:18.556
6	192.162.72.255	192.168.76.32	UPDATE products SET price=10 WHERE id=5	07/08-06:06:29.667
7	192.162.72.255	192.168.76.32	1' AND SLEEP(5)--	07/08-06:06:40.778
8	192.162.72.255	192.168.76.32	' OR 'a'='a	07/08-06:06:51.889
9	192.162.72.255	192.168.76.32	DELETE FROM logs WHERE date < '2023-01-01'	07/08-06:07:02.990
10	192.162.72.255	192.168.76.32	' UNION SELECT 1,2,3--	07/08-06:07:14.101
11	192.162.72.255	192.168.76.32	https://192.168.76.32 /login.php	07/08-06:07:25.212
12	192.162.72.255	192.168.76.32	1' OR 1=1 LIMIT 1--	07/08-06:07:36.323
13	192.162.72.255	192.168.76.32	' OR (SELECT * FROM users) --	07/08-06:07:47.434
14	192.162.72.255	192.168.76.32	1') AND 1=1 --	07/08-06:07:58.545
15	192.162.72.255	192.168.76.32	INSERT INTO orders	07/08-06:08:09.656

No	Alamat IP	Tujuan	Jenis serangan	Waktu kejadian
			VALUES (1, 'test')	
16	192.162.72.255	192.168.76.32	' OR IF (1=1, BENCHMARK (1000000MD5 ('A')),0)--	07/08-06:08:20.767
17	192.162.72.255	192.168.76.32	' OR 1=1 ORDER BY 1--	07/08-06:08:31.878
18	192.162.72.255	192.168.76.32	1' UNION SELECT 1, database () --	07/08-06:08:42.989
19	192.162.72.255	192.168.76.32	' OR '' = '	07/08-06:08:54.100
20	192.162.72.255	192.168.76.32	' OR 1=1--	07/08-06:09:05.211
21	192.162.72.255	192.168.76.32	1' OR EXISTS (SELECT * FROM users WHERE user='admin') --	07/08-06:09:16.322
22	192.162.72.255	192.168.76.32	' OR 1=1--	07/08-06:09:27.433
23	192.162.72.255	192.168.76.32	1') OR ('1'='1	07/08-06:09:38.544
24	192.162.72.255	192.168.76.32	' OR 1=1 ORDER BY 2--	07/08-06:09:49.655
25	192.162.72.255	192.168.76.32	' UNION SELECT	07/08-06:10:00.766

No	Alamat IP	Tujuan	Jenis serangan	Waktu kejadian
			* FROM users--	
26	192.162.72.255	192.168.76.32	1' AND 1=1	07/08-06:10:11.877
27	192.162.72.255	192.168.76.32	1' AND 1=2	07/08-06:10:22.988
28	192.162.72.255	192.168.76.32	' OR 1=1-- -	07/08-06:10:34.099
29	192.162.72.255	192.168.76.32	https://192.168.76.32/ DVWA/login.php	07/08-06:10:45.210
30	192.162.72.255	192.168.76.32	' OR 1=1-- -	07/08-06:10:56.321

3.3.2 *Suricata* Data

Berikut merupakan skenario serangan dalam proses pengumpulan data pada *Suricata*:

Tabel 3. 2 *Suricata* Data

No	Alamat IP	Tujuan	Jenis serangan	Waktu kejadian
1	192.168.76.245	192.168.76.32	' OR 1=1-- -	07/08-06:15:10.311
2	192.168.76.245	192.168.76.32	SELECT * FROM audit_log	07/08-06:15:24.120
3	192.168.76.245	192.168.76.32	1' UNION SELECT null, version () --	07/08-06:15:32.593
4	192.168.76.245	192.168.76.32	GET / index.html HTTP/1.1	07/08-06:15:41.604
5	192.168.76.245	192.168.76.32	' OR EXISTS (SELECT * FROM users) --	07/08-06:15:56.750

No	Alamat IP	Tujuan	Jenis serangan	Waktu kejadian
6	192.168.76.245	192.168.76.32	' OR 1=1 ORDER BY 2--	07/08-06:16:00.860
7	192.168.76.245	192.168.76.32	1' AND SLEEP(5)--	07/08-06:16:09.971
8	192.168.76.245	192.168.76.32	' OR 'a'='a	07/08-06:16:19.088
9	192.168.76.245	192.168.76.32	UPDATE settings SET value=1	07/08-06:16:29.199
10	192.168.76.245	192.168.76.32	' UNION SELECT 1,2,3--	07/08-06:16:30.310
11	192.168.76.245	192.168.76.32	1' OR 1=1 LIMIT 1--	07/08-06:16:43.421
12	192.168.76.245	192.168.76.32	' OR (SELECT * FROM passwords)--	07/08-06:17:58.532
13	192.168.76.245	192.168.76.32	1') AND 1=1 --	07/08-06:17:11.643
14	192.168.76.245	192.168.76.32	' OR " = '	07/08-06:17:21.754
15	192.168.76.245	192.168.76.32	1' OR EXISTS (SELECT * FROM users WHERE user='admin') --	07/08-06:17:31.865
16	192.168.76.245	192.168.76.32	1' AND 1=1	07/08-06:17:41.976
17	192.168.76.245	192.168.76.32	1' AND 1=2	07/08-06:17:52.087
18	192.168.76.245	192.168.76.32	' OR 1=1 ORDER BY 1--	07/08-06:18:02.198
19	192.168.76.245	192.168.76.32	1' UNION SELECT 1,	07/08-06:18:12.309

No	Alamat IP	Tujuan	Jenis serangan	Waktu kejadian
			database () --	
20	192.168.76.245	192.168.76.32	1') OR ('1'='1	07/08-06:18:22.420
21	192.168.76.245	192.168.76.32	' OR IF (1=1, BENCHMARK(1000000,MD5('A')),0)--	07/08-06:18:32.531
22	192.168.76.245	192.168.76.32	' OR '1'='1'	07/08-06:18:42.642
23	192.168.76.245	192.168.76.32	' OR 1=1-- -	07/08-06:18:52.753
24	192.168.76.245	192.168.76.32	' OR EXISTS(SELECT * FROM admins) --	07/08-06:19:02.864
25	192.168.76.245	192.168.76.32	' UNION SELECT * FROM credit_cards--	07/08-06:19:12.975
26	192.168.76.245	192.168.76.32	1' OR 1=1 LIMIT 1--	07/08-06:19:23.086
27	192.168.76.245	192.168.76.32	' OR 'a'='a	07/08-06:19:33.197
28	192.168.76.245	192.168.76.32	' OR 1=1-- -	07/08-06:19:43.308
29	192.168.76.245	192.168.76.32	1' UNION SELECT null, version() --	07/08-06:19:53.419
30	192.168.76.245	192.168.76.32	' OR 1=1 ORDER BY 2--	07/08-06:20:03.530

3.4 Analisa Kebutuhan Perancangan

Dalam penelitian ini, analisis kebutuhan dilakukan untuk merancang lingkungan eksperimen *Testbed* yang dapat digunakan untuk mengevaluasi

performa sistem deteksi intruksi (*IDS*) *Snort* dan *Suricata* terhadap serangan *SQL Injection*. Analisis kebutuhan mencakup kebutuhan perangkat keras, perangkat lunak, jaringan yang diperlukan dalam perancangan dan pelaksanaan eksperimen.

3.4.1 Kebutuhan Perangkat Keras

Berikut merupakan rincian perangkat keras yang digunakan dalam penelitian ini:

Tabel 3. 3 Kebutuhan Perangkat Keras

Komponen	**Spesifikasi minimun**
Prosesor	*AMD* A12 – 9720P *Radeon* R7, 12 *Compute Cores* 4C + 8G 2,70GHz
RAM	16 *GB*
Penyimpanan	*SSD* 256 *GB*
Jaringan	Koneksi lokal / internal *VM*

3.4.2 Kebutuhan Perangkat Lunak

Berikut merupakan daftar kebutuhan perangkat lunak yang digunakan dalam penelitian ini:

Tabel 3. 4 Kebutuhan Perangkat Lunak

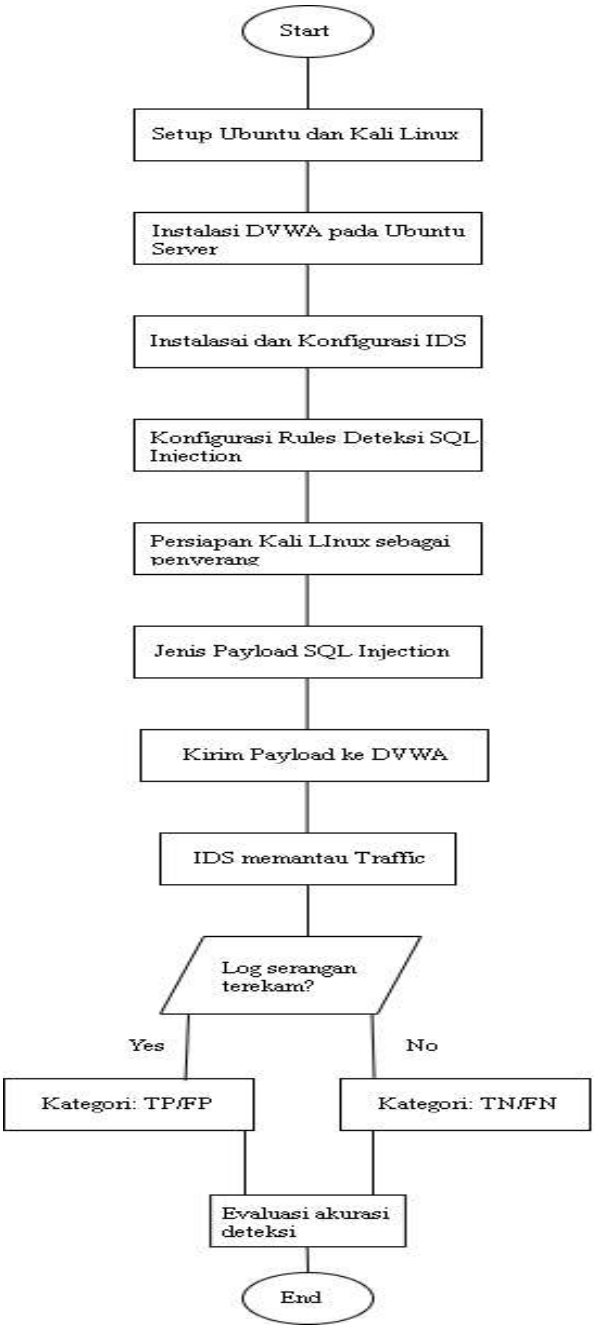
Sistem operasi	**Aplikasi dan tool**
Ubuntu server 20.04 *LTS*	*Snort* 2.9
Kali linux 2023.1	*Suricata* 6.0
VirtualBox 7.0	*DVWA* 1.10

3.4.3 Kebutuhan Jaringan

Semua *Virtual Machine* dikonfigurasi dalam satu jaringan *virtual internal* (*internal network/host-only network*) sehingga komunikasi antar perangkat dapat dipantau oleh *IDS*. *IDS* dapat diletakkan secara *inline* atau menerima salinan *traffic* menggunakan mode *port mirroring*.

3.5 Metode Simulasi Serangan *SQL Injection*

Dalam metode simulasi serangan *SQL Injection* menggunakan *setup Testbed* yang telah diatur, menyertakan perbedaan terminologi, fokus, dan detail teknis dalam simulasi serangan *SQL Injection* dengan *IDS*. Perubahan ini bertujuan untuk meningkatkan akurasi dan isolasi lingkungan pengujian.



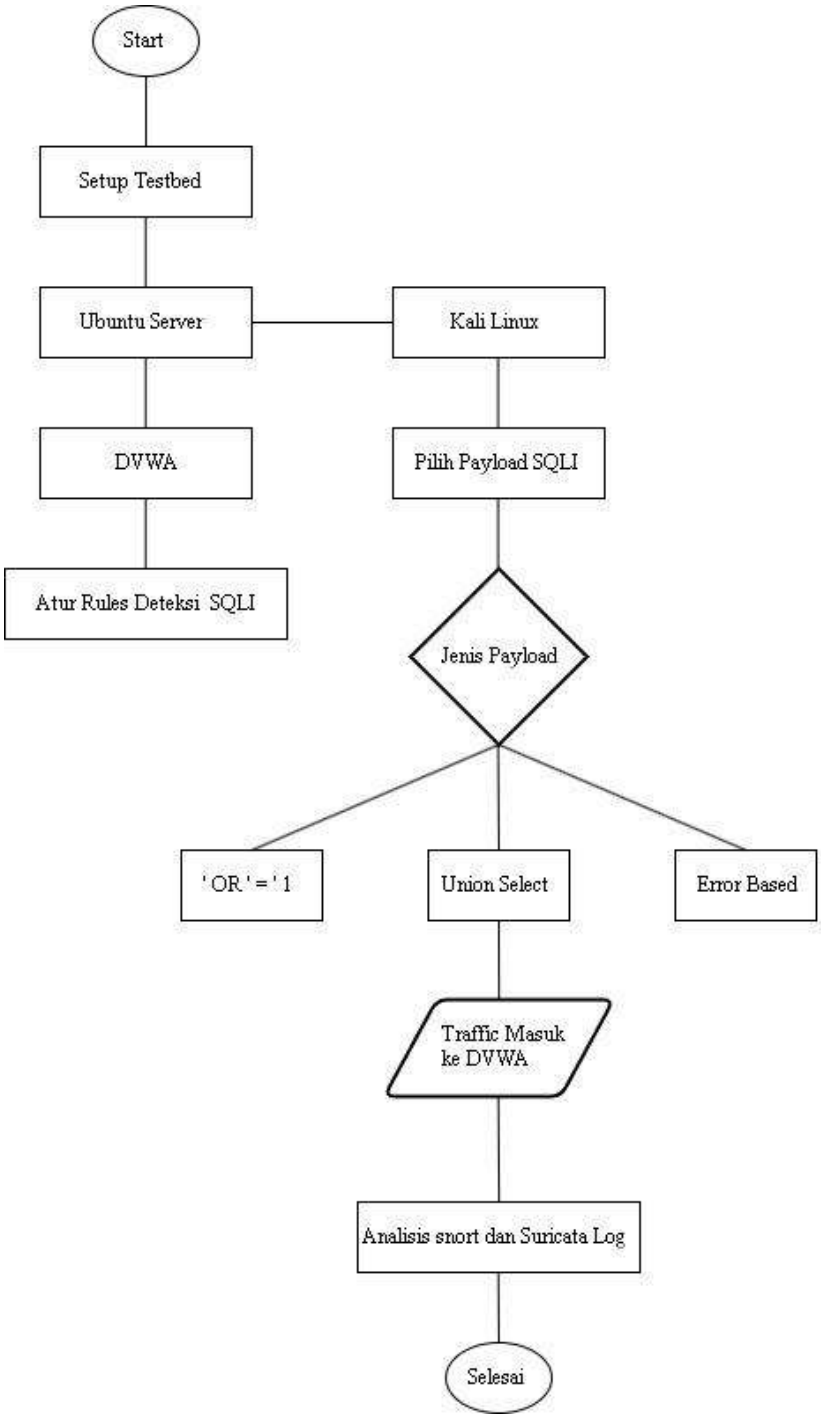
Gambar 3. 3 Flowchar Simulasi Serangan

Pada gambar 3.3 menunjukkan *flowchart* metode simulasi serangan *SQL Injection*, Proses dimulai dengan menyiapkan kedua mesin *virtual machine*, di mana *Damn Vulnerable Web Application* diinstal pada *Ubuntu Server* sebagai target serangan, sementara *Kali Linux* digunakan sebagai mesin penyerang. Setelah

itu, dilakukan instalasi dan konfigurasi *IDS Snort* dan *Suricata* di *Ubuntu Server*, serta pengaturan *rules* khusus untuk mendeteksi pola serangan *SQL Injection*. Di sisi penyerang, dilakukan persiapan *payload* yang akan digunakan untuk menyerang *DVWA*, seperti *'OR'='1*, *UNION SELECT*, dan teknik lainnya. *Payload SQL Injection* dikirimkan ke aplikasi *DVWA*, sementara *IDS* bertugas untuk memantau lalu lintas jaringan yang masuk. Kemudian sistem akan memeriksa apakah *log* serangan berhasil terekam oleh *IDS*. Jika *log* terdeteksi, maka diklasifikasikan ke dalam *True Positive* (*TP*) atau *False Positive* (*FP*) tergantung konteks deteksinya. Sebaliknya, jika log tidak terekam, maka dikategorikan sebagai *True Negative* (*TN*) atau *False Negative* (*FN*). Langkah terakhir adalah melakukan evaluasi terhadap akurasi deteksi *IDS*, dengan mengukur metrik performa seperti akurasi, presisi, *recall*, dan *F1-score*. *Flowchart* ini menggambarkan alur eksperimen deteksi *SQL Injection* secara menyeluruh dari awal hingga analisis hasil.

3.6 Metode Deteksi Serangan

Metode deteksi serangan *SQL Injection* yang menggambarkan interaksi antara *Kali Linux* (penyerang) dan *Ubuntu Server* (korban). Simulasi ini melibatkan *DVWA* sebagai target, *Snort* dan *Suricata* sebagai sistem deteksi intrusi (*IDS*), serta serangan manual dari *Kali Linux* untuk menguji efektivitas deteksi.



Gambar 3. 4 Deteksi serangan

Pada gambar 3.4 Penelitian ini mensimulasikan deteksi serangan *SQL Injection* dalam sebuah *testbed* dengan dua sistem: *Ubuntu Server* sebagai target (*DVWA*) dan *Kali Linux* sebagai penyerang. *IDS* (*Snort* dan *Suricata*) dikonfigurasi dengan

aturan khusus untuk mendeteksi *SQLi*. Penyerang memilih *payload* (seperti *OR*=1, *UNION SELECT*, atau *Error Based*) lalu mengirimkannya ke *DVWA*. Lalu lintas yang masuk dipantau *IDS* dan hasil deteksi dianalisis melalui *log* untuk mengevaluasi efektivitas sistem dalam mengenali *SQLi*.

3.7 Metode Evaluasi

Berikut merupakan penjelasan mengenai metrik evaluasi yang digunakan untuk mengukur kinerja sistem deteksi intrusi dalam penelitian ini. Perhitungan Tingkat *accuracy, precision, recall* dan *F1 score* adalah sebagai berikut:

1. *Accuracy*

Mengukur sejauh mana sistem dapat memberikan prediksi yang benar, baik untuk kasus serangan maupun normal.

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}$$

2. *Precision*

Mengukur ketepatan deteksi, yaitu seberapa banyak alarm yang dihasilkan *IDS* benar-benar serangan.

$$Precision = \frac{TP}{TP + FP}$$

3. *Recall*

Mengukur kemampuan sistem mendeteksi serangan sebenarnya.

$$Recall = \frac{TP}{TP + FN}$$

4. *F1 Score*

Rata-rata harmonis antara *Precision* dan *Recall*. Digunakan untuk menyeimbangkan keduanya.

$$F\ 1\ Score = 2\ \text{x}\frac{Precision\ \text{x}\ Recall}{Precision + \ Recall}$$

- *TP* (*True Positive*): jumlah serangan yang benar terdeteksi.
- *FP* (*False Positive*): jumlah normal *traffic* yang salah terdeteksi sebagai serangan.
- *FN* (*False Negative*): jumlah serangan yang tidak terdeteksi.
- *TN* (*True Negative*): jumlah normal *traffic* yang benar dikenali sebagai normal.

3.8 Jadwal Penelitian

Mengenai skripsi yang harus diselesaikan dalam waktu enam bulan sejak dimulainya dengan fungsi dan judul, pembentukan bab I, bab II, bab III, kemudian (merevisi) hasil karya. Berikut kalender kegiatannya dilakukan selama studi.

Tabel 3. 5 Jadwal Penelitian

No	Kegiatan	Jadwal Penelitian					
		2025					
		Mar	Apr	Mei	Juni	Juli	Agus
1.	Identifikasi masalah dan perumusan masalah						
2.	Perancangan skenario eksperimen						
3	Instalasi dan konfigurasi lingkungan virtual						
4.	pengumpulan data dan analisis hasil						
5.	Kesimpulan dan saran						