BAB III
METODOLOGI PENELITIAN

3.1. Desain Penelitian

Penelitian ini dilakukan dengan menggunakan jenis penelitian kuantitatif. Penelitian kuantitatif bertujuan untuk mendapatkan informasi terkait objek analisis dalam bentuk angka dengan menggunakan *tools* pengujian dengan tujuan untuk melakukan analisis pengujian terhadap masalah yang telah ditentukan, sehingga menghasilkan kesimpulan yang sesuai dengan objek penelitian. Hal tersebut memungkinkan dalam mengolah data secara sistematis, sehingga informasi yang diperoleh dapat mudah dianalisis (Syahrizal & Jailani, 2023).

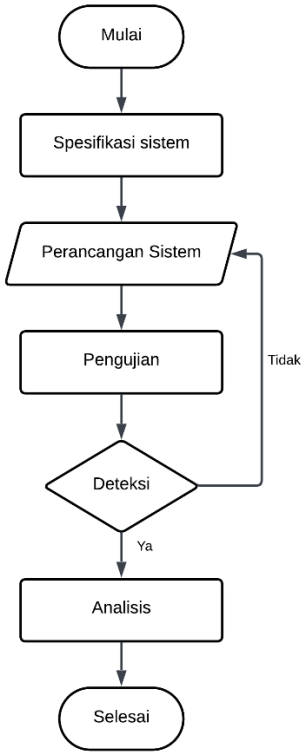
Metode kuantitatif yang digunakan pada penelitian ini adalah metode analisis eksperimen yang bertujuan untuk melakukan pengujian deteksi terhadap studi kasus serangan siber dengan menggunakan *tools* IBM QRadar dan Snort. Analisis eksperimen yang dilakukan untuk menemukan performa dari *tools* yang digunakan dalam pengujian, sehingga pada penelitian ini dilakukan secara sistematis dan sesuai dengan alur penelitian (Zihnil Afif dkk., 2023).

3.2. Studi Literatur

Berdasarkan kajian teori dan metode eksperimen, maka dilakukan studi literatur dari berbagai teori dari sumber yang terdahulu dan relevan dalam melakukan penelitian yang melibatkan pengujian simulasi terhadap masalah yang ditentukan. Pengujian simulasi melibatkan *tools* IBM QRadar dan Snort dalam mendeteksi serangan siber yang bertujuan dalam menganalisis komparasi pada kedua *tools* tersebut dalam menemukan efektivitas yang membutuhkan forensik dalam menemukan efektivitas tersebut.

3.3. Alur Penelitian

Metodologi penelitian memiliki tujuan untuk menyelesaikan masalah yang ada secara terstruktur. Berikut adalah bagan alur metode eksperimen dalam melakukan penelitian ditunjukkan pada gambar 3.1.



Gambar 3.1. Alur penelitian

Alur penelitian yang digunakan dalam melakukan pengujian objek serangan siber adalah mempersiapkan spesifikasi untuk kebutuhan instalasi OS CentOS 7 sebagai linux QRadar dan instalasi Snort dengan OS Ubuntu. Kemudian, melakukan perancangan sistem yang memuat konfigurasi *rules* terhadap serangan siber yang diuji. Lalu, pada tahap pengujian adalah melakukan uji coba pada *tools* terhadap serangan siber. Kemudian, pada tahap deteksi adalah kinerja dari *tools* dalam mendeteksi serangan siber, jika deteksi berhasil maka langsung ke dalam tahap analisis, jika deteksi gagal maka tahapan kembali ke dalam perancangan sistem dalam melakukan konfigurasi *rules*. Selanjutnya adalah analisis dengan *network forensics* sebagai komparasi

dalam menentukan efektivitas *tools* sebagai kesimpulan dalam menerapkan *tools* yang efektif.

Dalam memahami bentuk informasi dari data yang didapatkan harus disederhanakan melalui analisis. Oleh karena itu peneliti menggunakan parameter *network forensics* seperti pada tabel 3.1.

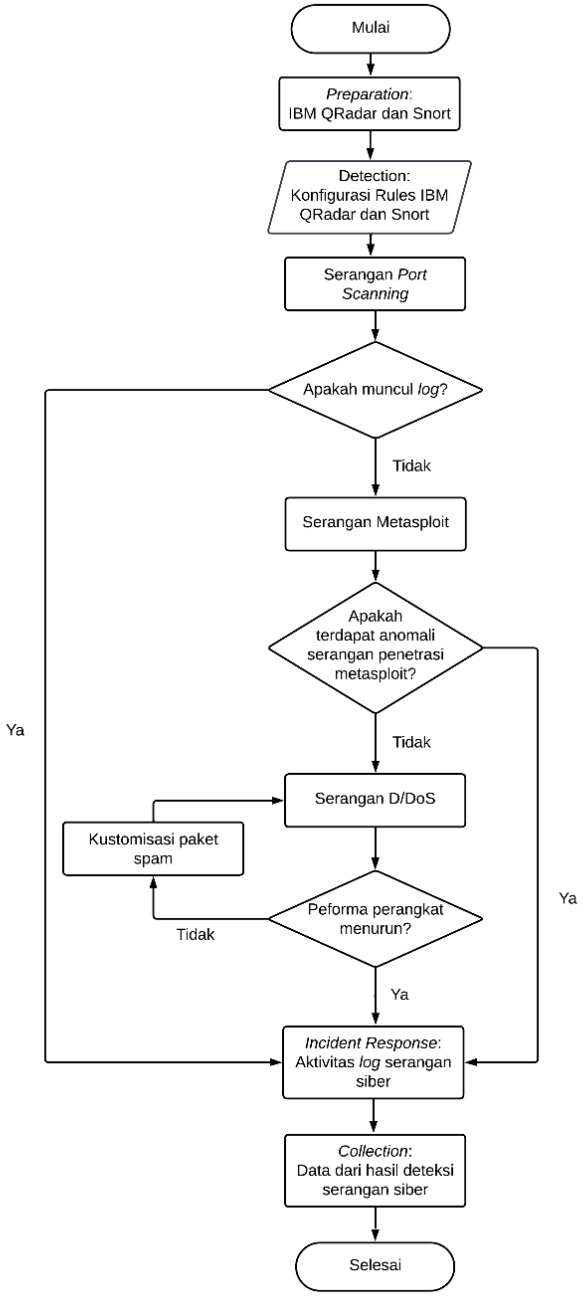
Tabel 3.1. Parameter *network forensics*

Network Forensics		
Parameter	Tools	
	IBM QRadar *Community Edition*	Snort
Preparation	Spesifikasi IBM QRadar: 8 GB RAM, *Disk space* 250 GB, dan CPU 2 *cores*	Spesifikasi Snort: 200 MB RAM, *Disk space* 10 GB, dan CPU 1 *cores*
Detection	*Rules Offense and Log Activity*	*File Rules*
Incident Response	*Event Name, Event Count, and Event Time*	*CLI View and File History* Snort
Collection	*Dashboard*	*Log File*

Alur penelitian yang digunakan dalam meliputi perbandingan dari penggunaan tools IBM QRadar dan Snort dari 4 tahapan *network forensics*. Tahapan dalam melakukan *network forensics*, yaitu 1) *Preparation* dengan mempersiapkan sumber daya investigasi berupa sumber daya spesifikasi pada *tools*, 2) *Detection* yang merupakan tahapan konfigurasi dalam melihat *log source* yang sedang berjalan, 3) *Incident Response* yang merupakan tindakan dari kejadian yang terdeteksi oleh *tools*, dan 4) *Collection* adalah tahapan dalam pengumpulan data dari hasil kejadian pada jaringan.

3.4. Skenario Pengujian

Pengujian yang akan dilakukan pada penelitian ini bertujuan untuk mengetahui proses dalam deteksi dan analisis *tools* IBM QRadar dan Snort terhadap serangan siber. Skenario dalam pengujian ini terdapat dalam *flow chart* pada gambar 3.2.



Gambar 3.2. Flowchart Pengujian

Skema pengujian yang akan dilakukan menggunakan metode *network forensics* yang diimplementasikan pada *tools* IBM QRadar dan Snort terhadap serangan siber pada jaringan yang menjadi objek dalam penelitian, meliputi langkah-langkah sebagai berikut:

1. Penerapan *preparation* pada *tools* IBM QRadar dan Snort dengan mengatur *storage* dan spesifikasi yang dibutuhkan untuk instalasi dan penggunaan.
2. Penerapan *detection* konfigurasi *rules* pada *tools* IBM QRadar dan Snort.
3. Melakukan pengujian serangan *port scanning* menggunakan aplikasi Nmap untuk memindai *port* komputer target.
4. Melakukan pengujian serangan metasploit menggunakan metasploit framework yang bertujuan untuk melakukan meterpreter terhadap komputer target.
5. Melakukan pengujian serangan D/DoS menggunakan *tools* hping3 yang mengirimkan banyak paket spam terhadap komputer target.
6. Mendeteksi *incident response* dengan memperhatikan waktu serangan yang dimulai dan waktu deteksi serangan yang terjadi pada *tools*.
7. Mencatat dan mengumpulkan data *collection log* serangan siber pada *tools*.
8. Menganalisis parameter *network forensics* yang telah dilakukan untuk dianalisa efektivitas dari *tools* yang digunakan.

3.5. Spesifikasi Perangkat dan *Tools* Pengujian

Spesifikasi perangkat keras yang digunakan pada penelitian ini adalah menggunakan perangkat Laptop sebagai berikut seperti pada tabel 3.2.

Tabel 3.2. Spesifikasi Perangkat Keras Laptop

Spesifikasi Laptop	**Keterangan**
Processor	Intel Core i7-6700HQ
Core dan *Threads*	4 cores 8 threads
Kecepatan *Processor*	@2.60 GHz
RAM	8GB *up to* 24GB DDR4
HDD	1TB
SSD	256GB

Spesifikasi *software/tools* yang digunakan pada penelitian ini adalah sebagai berikut:

a. IBM QRadar *Community Edition* (CE) versi 7.3.3;

b. Snort versi 2.9.7.0;
c. Windows 10 sebagai *host* sistem OS pada laptop;
d. VMWare Workstation Pro versi 17.0.2 sebagai platform untuk virtualisasi dalam menjalankan sistem operasi jaringan;
e. Sistem operasi CentOS 7 virtualisasi untuk sistem QRadar dan Windows 10 virtualisasi sebagai *host* target;
f. Sistem operasi Ubuntu 20.04.6 virtualisasi untuk sistem Snort 2.9.7.0.
g. Sistem operasi Kali Linux 2024.1 sebagai media untuk melakukan penyerangan siber.

3.6. Teknik Pengumpulan Data

Data penelitian yang diperoleh melalui kinerja dari *tools* IBM QRadar dan Snort dalam mendeteksi waktu dan paket data *bytes* yang berjalan pada serangan *port scanning*, metasploit/*exploit*, dan D/DoS. Data kinerja *tools* yang didapatkan pada penelitian ini berupa 4 (empat) tahapan awal dari *network forensics* yang menganalisis serangan siber. Selain itu, data yang diperoleh digunakan untuk mengumpulkan bukti digital dari serangan siber.

3.7. Teknik Analisis Data (*Network Forensics*)

Teknik analisis data yang digunakan adalah data analisis hasil pengujian menggunakan analisis forensik. Data yang dianalisis adalah data hasil pendeteksian serangan siber yang mencakup memori perangkat yang dialokasikan, konfigurasi *rules* paket data serangan, *response time*, dan pengumpulan data akhir serangan siber. Analisis dilakukan dengan mengolah data hasil *capture log* yang terdapat pada *tools* IBM QRadar dan Snort untuk mendapatkan analisis perbandingan performansi dengan melakukan implementasi *network forensics* pada penelitian ini untuk mendapatkan efektivitas pada *tools* yang menerapkan 4 tahapan utama yaitu:

1. *Preparation* yang merupakan parameter dalam membandingkan spesifikasi *tools* yang digunakan. Spesifikasi yang efektif terlihat dari tingkat

penggunaan *memory* yang menyesuaikan dalam mendeteksi serangan siber (Adam Zukhruf dkk., 2023).

2. *Detection* yang merupakan parameter konfigurasi *rules* pada perbandingan *tools*. Konfigurasi yang efektif terlihat dari detailnya *rules* dalam mendeteksi ancaman serangan, memodifikasi *rules* yang lebih kompleks dalam mendeteksi dan membaca paket *log* jaringan (Elan Maulani & Faisal Umam, 2023).
3. *Incident Response* yang merupakan parameter *response time* yang efektif. Pada tahap ini dapat dilihat melalui perbandingan kecepatan waktu deteksi pada *tools* pengujian terhadap serangan siber (Riza, 2023).
4. *Collection* yang merupakan parameter dari kumpulan kejadian serangan siber yang didapat dari *tools*. Parameter yang efektif dalam tahapan ini adalah terlihat dari klasifikasi informasi serangan siber yang terdeteksi pada *tools* yang infromatif dan mudah dianalisis (Elan Maulani & Faisal Umam, 2023).