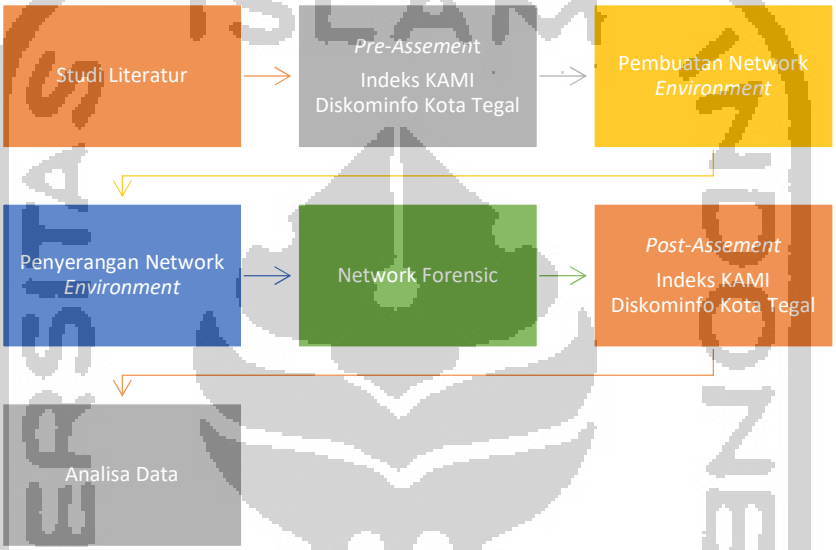
BAB 3
Metode Penelitian

Dalam penelitian ini dibuat dan disusun langkah-langkah penelitian untuk menjaga penelitian ini terarah dan fokus, langkah-langkah tersebut digambarkan pada gambar 3.1 dibawah ini.



Gambar 3.1 Metodologi Penelitian

3.1 Studi Literatur

Tahapan pertama dalam penelitian ini adalah studi literatur untuk mencari referensi dan landasan teori yang digunakan sebagai dasar dalam melakukan penelitian. Studi literatur dilakukan dengan melakukan *review* terhadap jurnal sejenis, membaca berbagai sumber pustaka yang terkait dan *paper* dengan bahasan yang sejenis.

3.2 *Pre-Assesment* Indeks KAMI Dinas Komunikasi dan Informatika Kota Tegal

Sebagai justifikasi awal untuk melihat apakah ada perbedaan jika ada *SIEM* dan tanpa pemasangan *SIEM*, maka perlu dilakukan *assessment* awal terhadap nilai indeks Keamanan Informasi (KAMI) pada Dinas Komunikasi dan Informatika Kota Tegal. Dalam pengukuran indeks Keamanan Informasi (KAMI) Dinas Komunikasi dan Informatika Kota Tegal menggunakan metode kuisioner kepada staf pranata komputer pratama di lingkungan Dinas Komunikasi dan Informatika Kota Tegal. Hasil dari kuisioner tersebut dihitung sesuai

dengan format aplikasi yang dimiliki oleh Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika Indonesia.

3.3 Pembuatan *Network Environment*

Sebagai salah satu tahapan penelitian, perlu dibuatkan *network environtment* yang bisa digunakan dalam melakukan pengujian serangan sebagai *trigger* untuk melihat apakah *SIEM* dapat melihat serangan-serangan yang dilakukan. Dalam penelitian ini digunakan perangkat dan *tool* simulasi yang dibutuhkan dalam penelitian yaitu sebagai berikut:

a. *Mikrotik 751U-2HnD Series*

   Dinas Komunikasi dan Informatika Kota Tegal menggunakan *router Mikrotik* sebagai *core router* mereka dan dalam simulasi dalam penelitian ini digunakan *router Mikrotik 751U-2HnD Series* untuk berperan sebagai *router*. *Mikrotik 751U-2HnD* dikonfigurasi dengan beberapa *service* sesuai dengan kondisi di Dinas Komunikasi dan Informatika Kota Tegal seperti, *DHCP, Hotspot* serta beberapa *service* yang secara *default* sudah berjalan seperti *SSH, FTP, CDP.*

b. *Cisco Catalyt 2950 Series (SWITCH A)*

   Peneliti menggunakan *switch manageable Cisco Catalyt 2950 Series (SWITCH A)* dan menghubungkan *switch* ini menuju ke *SIEM* dan *router Mikrotik* agar dapat melakukan metode *port mirroring/span port* sehingga *sniffer* dapat menangkap trafik komunikasi yang terjadi antara *router Mikrotik* dan *SIEM*.

c. *Cisco Catalyt 3750 Series (SWITCH B)*

   Peneliti menggunakan *switch manageable Cisco Catalyt 3750 Series (SWITCH B)* dan menghubungkan *switch* ini menuju ke *Hacker* dan *router Mikrotik* agar dapat melakukan metode *port mirroring/span port* sehingga *sniffer* dapat menangkap trafik komunikasi yang terjadi antara *router Mikrotik* dan *Hacker*.

d. *Sniffer Software Wireshark Windows Version*

   Selain menggunakan *switch manageable*, agar semua paket yang dikirimkan dari dan ke *hacker*, *router Mikrotik* maupun *SIEM* dapat ditangkap digunakan *wireshark* sebagai pilihan untuk menangkap trafik di jaringan. Aplikasi *wireshark* di install pada komputer berbasis *Windows*. Komputer tersebutpun dipasang dengan jumlah *lan card* 2 buah yang masing terhubung dengan *SWITCH A* dan *SWITCH B.*

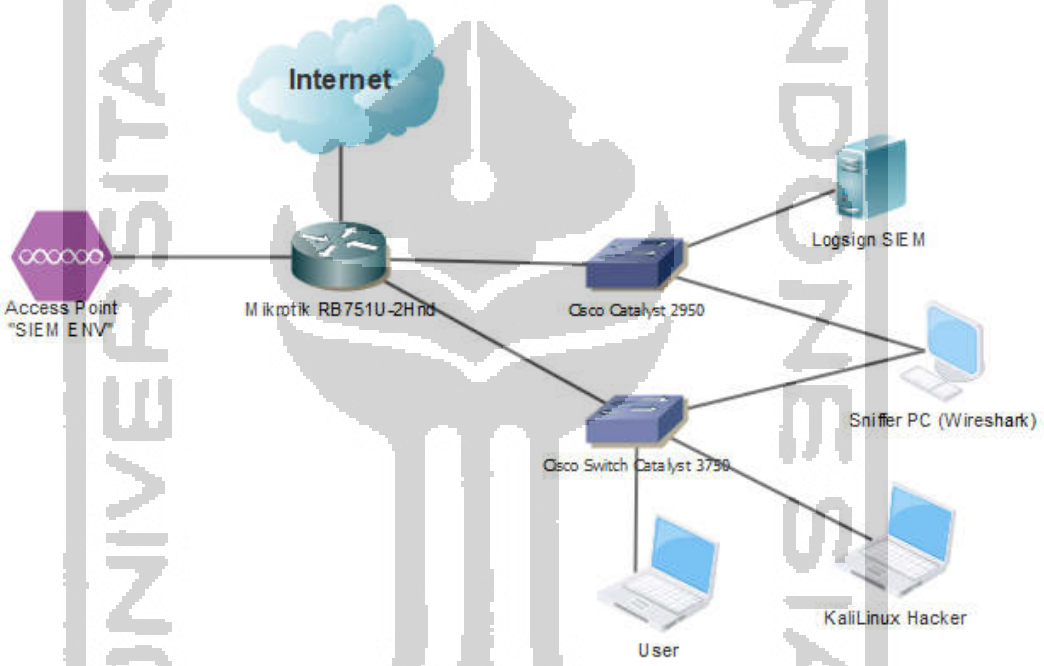
e. *LogSign* Sebagai *SIEM*

   Server LogSign SIEM yang digunakan di install di *Virtual Machine* yang dijalankan pada software *VMware Workstation* dengan *Host OS Windows* dengan spesifikasi minimum yang sesuai dengan minimal *requirement Logsign SIEM*

f. *Hacker* menggunakan *OS KaliLinux*

OS Kalilinux digunakan untuk melakukan serangan ke *router Mikrotik*. *OS* Kalilinux yang digunakan di install di *Virtual Machine* yang dijalankan pada software *VMware Workstation* dengan pilihan *software* yang akan digunakan adalah *Yersinia, Ettercap, Macof* untuk melakukan simulasi serangan seperti *Mac Flooding, Arp Poisioning, CDP Flooding, DHCP Starvation, DHCP Rogue, Syn Flooding, SSH Bruteforce, FTP Bruteforce.*

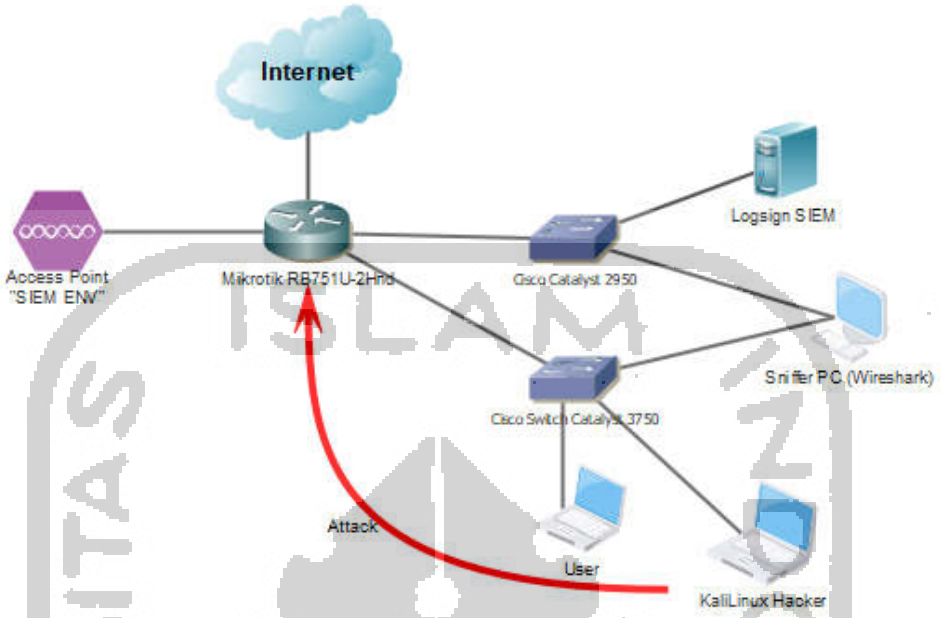
Dan berikut merupakan gambaran topologi jaringan yang akan dijadikan sebagai *network environment* penelitian ini.



Gambar 3.2 Topologi *Network Environment*

Dalam *Network Environment* yang dibuat dalam penelitian ini merupakan infrastruktur jaringan yang berbasis *router Mikrotik* dengan jaringan Hotspot. Peneliti menyediakan 2 jaringan yang terdiri dari jaringan user dimana *hacker* akan masuk dan menyerang aset *router Mikrotik*, serta jaringan dimana *SIEM Logsign* berada untuk menganalisa *log* yang dikirimkan oleh *router Mikrotik* kepada *SIEM* Logsign. *Switch manageable*-pun dipersiapakan untuk dapat menangkap semua trafik agar dapat dianalisa di proses *network forensic*.

3.4 Penyerangan *Network Environment*



Gambar 3.3 Topologi *Network Environment with Attack*

Setelah melakukan Pembuatan *Network Environment* dan konfigurasi *LogSign SIEM*, ditindaklanjuti dengan melakukan penyerangan terhadap infrastruktur jaringan yang telah dibuat dengan beberapa tipe serangan dan beberapa *tools.* Peneliti melakukan penyerangan terhadap *router Mikrotik* dari Jaringan Internal *(Private Network).* Dan berikut merupakan daftar serangan dan *tool* yang digunakan dalam simulasi serangan, yaitu:

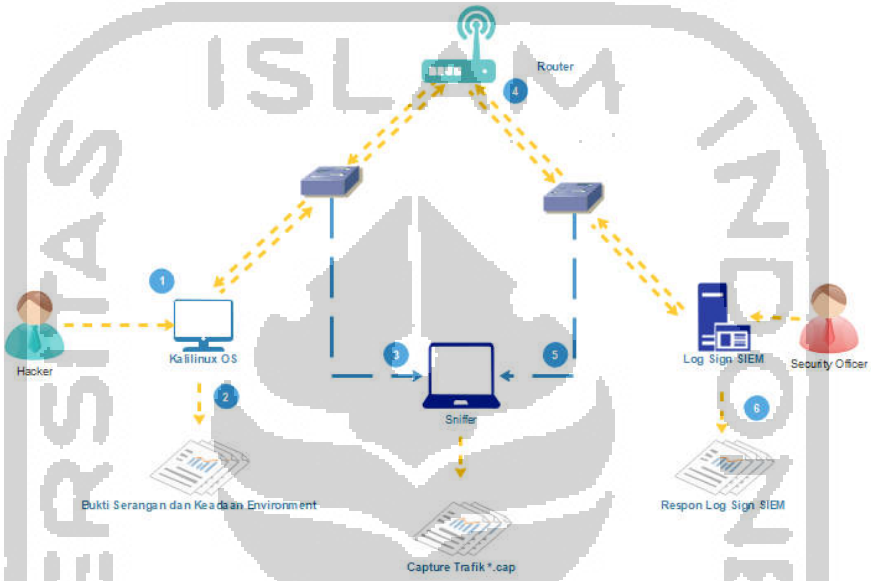
Tabel 3.1: Tipe serangan di *Network* dan *Tools*

***Layer* Serangan**	**Teknik Serangan**	***Tools***
Link Layer Attack	*Mac Flooding*	*MacOF*
	Arp Poisioning	*Ettercap*
	CDP Flooding	*Yersinia*
Internet Layer Attack	*DHCP Starvation*	*Yersinia*
	DHCP Rogue	*Yersinia*
Transport Layer Attack	*Syn Flooding*	*Hping3*
Application Layer Attack	*SSH Bruteforce*	*Hydra*
	FTP Bruteforce	*Hydra*

Peneliti menggunakan serangan-serangan diatas untuk mewakili layer yang ada pada *TCP/IP*

3.4.1 Skenario Penyerangan

Dalam proses simulai ini dibuat skenario penyerangan untuk memperjelas bagaimana proses penyerangan yang dilakukan oleh *hacker* dan bagaimana proses pencarian barang bukti yang dilakukan dalam penelitian ini, mencakup proses penyerangan, proses *capture* sesuai dengan gambar 3.3 yang menunjukan langkah-langkah berikut ini



Gambar 3.4 Skenario Simulasi Serangan

Dalam penelitian ini dilakukan penyerangan sesuai dengan langkah langkah berikut ini

1. *Hacker* dengan mengunakan *OS Kalilinux* melakukan penyerangan kedalam *network environment* yang ada sesuai dengan tipe serangan yang sudah ditentukan pada tabel 3.1.
2. Disaat bersamaan proses penyerangan didokumentasikan baik dari sisi *Hacker* maupun *Mikrotik*
3. Komunikasi yang dilakukan antara *Hacker* dengan *router Mikrotik* akan ditangkap oleh *sniffer*
4. *Router Mikrotik* merespon dan berkomunikasi dengan *SIEM*
5. Pada saat bersamaan *sniffer* juga menyimpan semua trafik yang dikrimkan dari *router Mikrotik* ke *SIEM*
6. Respon dari *SIEM* akan dicatat dan di *capture* sesuai dengan kebutuhan penelitian
7. Dalam penelitian ini skenario ini dilakukan sebanyak 7 kali sesuai sesuai dengan tipe serangan yang sudah ditentukan pada tabel 3.1.

3.5 Network Forensik

Setelah simulasi serangan dilakukan pada saat bersamaan dilakukan penyadapan terhadap semua aktifitas yang berjalan dan menangkap semua traffic dari *SWITCH A* dan *SWITCH B*. Dalam penelitian ini dilakukan penyadapan trafik komunikasi antara *hacker* dan *router Mikrotik* serta *router Mikrotik* ke *SIEM* dengan menggunakan *Wireshark*.

Wireshark adalah aplikasi yang ditujukan untuk menganalisis paket data pada jaringan. Dengan aplikasi ini, semua aktifitas yang terjadi dan melalui jaringan akan tertangkap dan dapat dilakukan analisa. Pada penelitian ini digunakan *Wireshark* untuk membantu dalam melakukan analisis terhadap paket data yang lewat dijaringan. Aplikasi dapat di *download* pada alamat (http://wireshark.org/download.html).

Dalam proses analisa yang dilakukan dipenelitian ini mengikuti metodelogi yang ada dengan menggunakan metodologi *OSCAR (Obtain Information –》 Strategize –》 Collect Evidence –》 Analyze –》 Report)* akan tetapi disesuaikan dengan kebutuhan penelitian

Dalam proses yang ada di OSCAR

1. *Obtain Information*

   Dalam tahap ini adalah investigator mencari informasi yang mendukung proses forensik, segala informasi yang berhubungan dengan proses investigasi forensik,, seperti bentuk topologi jaringan, serangan apa yang terjadi di jaringan dan *environment network* itu sendiri. Karena sifat dari penelitian ini adalah simulasi dengan topologi yang dibuat sampling, maka proses ini bisa dilewati. Dalam penelitian ini untuk mendapatkan informasi sudah ditentukan objek mana saja yang akan

2. *Strategies*

   Dalam tahap ini investigator melakukan prioritasi terhadap objek apa saja yang bisa dijadikan sebagai barang bukti. Dalam proses ini juga *investigator* menentukan bagaimana proses penanganan barang bukti. Dan dalam penelitian ini ditentukan proses *capturing packet* serta monitoring langsung *router Mikrotik* dan *SIEM*

3. *Collect evidence*

   Dalam penelitian ini peneliti mengumpulkan data dengan mengumpulkan dengan melakukan *sniffing* dan melihat kondisi *SIEM* dan *router Mikrotik* Dalam proses ini peneliti menggunakan data *sniffing* komunikasi *hacker – Mikrotik,* kondisi *router Mikrotik*. *sniffing* komunikasi *Mikrotik - SIEM* dan kondisi *SIEM* sebagai barang bukti yang digunakan.

4. *Analyze*

   Dalam penelitian ini dilakukan analisa semua barang bukti yang ada yaitu menggunakan data *sniffing* komunikasi *hacker – Mikrotik,* kondisi *router Mikrotik*. *sniffing* komunikasi *Mikrotik - SIEM* dan kondisi *SIEM* sebagai barang bukti yang digunakan

5. *Report*

   Segala proses yang ada didokumentasikan dalam bentuk tabel agar membantu dalam dokumentasi penelitian

Dari metodologi yang *OSCAR* yang digunakan, peneliti mencoba untuk lebih mendetailkan 3 proses terakhir yaitu *collect evidence, analyze* dan *reporting* untuk membantu peneliti lebih mendetailkan apa yang akan dilakukan di proses selanjutnya dan gambar 3.5 merupakan gambaran detail dari 3 proses tersebut.

Gambar 3.5 Proses Analisis Serangan dan *SIEM*

Dari hasil *capture* serangan yang dilakukan ditahap sebelumnya dilakukan analisa pada *Log Sign SIEM* dan mendata apakah serangan serangan tersebut memberikan dampak pada jaringan dan melihat apakah *Log Sign SIEM* dapat memdeteksi serangan tersebut.

Dari hasil analisa serangan yang ada akan dibuatkan tabel yang menunjukan status serangan tersebut seperti pada contoh tabel 3.2 dibawah ini

Tabel 3.2: Rangkuman *Network Forensic* Serangan

Serangan	**Trafik *Mikrotik-Hacker***	**Respon *Mikrotik***	**Trafik *Mikrotik - SIEM***	**Respon *SIEM***	**Hasil Serangan *SIEM***
Jenis serangan	Gambaran analisa trafik	Gambaran respon *Mikrotik*	Gambaran analisa trafik	Gambaran respon *SIEM*	Apakah *SIEM* dapat melihat serangan atau tidak

3.6 *Post-Assesment* Indeks KAMI Dinas Komunikasi dan Informatika Kota Tegal

Setelah melakukan proses *network forensic* terhadap simulasi serangan, dan melihat hasil *network forensic* yang dilakukan, dilakukan paparan mengenai hasil simulasi serangan dan *network forensic* kepada responden yang dalam hal ini adalah Staff Pranata Komputer Dinas Komunikasi dan Informatika kota Tegal. Dan memberikan *post-assesment* indeks Keamanan informasi (KAMI) untuk mengukur nilai indeks Keamanan informasi (KAMI) instansi tersebut setelah *SIEM* ada, penulis menggunakan metode kuisioner kepada Staff Pranata Komputer di lingkungan Dinas Komunikasi dan Informatika kota Tegal. Hasil dari kuisioner tersebut dihitung sesuai dengan format aplikasi yang dimiliki oleh Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika Indonesia.

3.7 Analisa Serangan

Dari hasil *network forensic* yang didapatkan dari tahap sebelumnya, dirangkumlah dan dianalisa 7 macam serangan yang ada dan dianalisa dan disimpulkan apakah *Log Sign SIEM* mengenali serangan tersebut atau tidak.

Tabel 3.3: Kolerasi Serangan dan *SIEM*

No	Layer Serangan	Jenis Serangan	Tool	Hasil di *SIEM*	Hasil pada *Mikrotik*	Output Kesimpulan
1	Link Layer	*Mac Flooding*	*MacOF*			
2		*Arp Poisioning*	*Ettercap*			
3		*CDP Flooding*	*Yersinia*			
4	Network Layer	*DHCP Starvation*	*Yersinia*			
5		*DHCP Rogue*	*Yersinia*			
6	Transport Layer	*Syn Flooding*	*Hping3*			
7	Application Layer	*SSH Bruteforce*	*Hydra*			
8		*FTP Bruteforce*	*Hydra*			

Dalam penelitian ini juga dilakukan analisa implikasi penggunaan SIEM terhadap nilai indeks Keamanan Informasi (KAMI), dalam penelitian ini dibandingkan hasil nilai *pre* dan *post-assement* nilai indeks Keamanan Informasi (KAMI) Dinas Komunikasi dan Informatika Kota Tegal

3.8 Hipotesa

Dengan analisa yang ada maka dalam penelitian ini diharapkan mampu mendapatkan informasi mengenai serangan apa saja yang bisa di kenali oleh *SIEM*, serta rekomendasi apakah memang perlu adanya *SIEM* dalam menjaga keamanan di *network environment* yang dimiliki oleh suatu instansi, dalam penelitian ini juga diharapkan mampu menjawab apakah penggunaan *SIEM* dapat menaikan indeks Keamanan Informasi (KAMI) sebagai tolak ukur keamanan di suatu instansi.