Bab 3 Metodologi Penelitian

Bab ini menjelaskan bagaimana cara penelitian ini dilakukan, sehingga dapat memberikan rincian tentang alur atau langkah-langkah yang dibuat secara sistematis serta dapat digunakan dijadikan pedoman dengan jelas dalam menyelesaikan masalah, membuat analisa terhadap hasil penelitian, serta kesulitan yang digadapi. Adapun tahapan-tahapan atau langkah-langkah pada penelitian ini dapat dilihat pada Gambar 3.1.

Gambar 3. 1 Alur Metodologi Penelitian

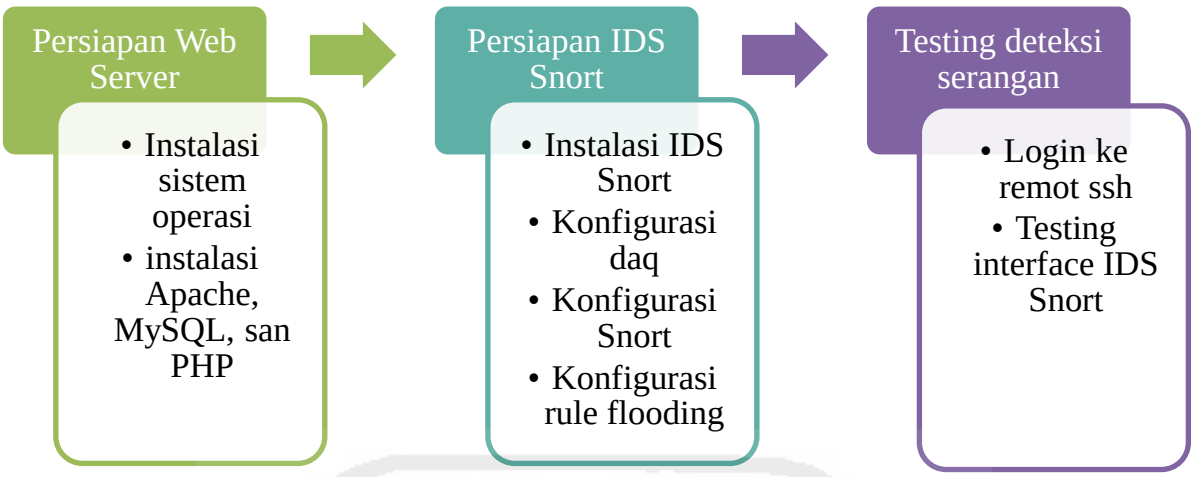
3.1 Literatur Review

Literatur review dilakukan untuk mendapatkan informasi mengenai topik-topik yang akan diteliti yang dapat diperoleh dari buku,dokumen, artikel, atau bahan tertulis lainnya yang berupa buku laporan, teori, maupun penemuan lainya yang bersifat *online* maupun *offline* yang bertujuan memberikan informasi.

Review atau kajian pustaka dilakukan untuk tujuan terhadap dilkukannya penelitian yang terkait dengan masalah-masalah yang terkait untuk mendeteksi serangan berbasis *Intrusion Detection System* (IDS), berikut juga metode yang digunakan untuk melakukan proses deteksi agar dapat menunjang tujuan ahir dalam penelitian ini.

3.2 Identifikasi Sistem

Merupakan tahap perancangan dan implementasi sistem jaringan *Intrusion Detection System* (IDS) yang akan digunakan sebagai objek penelitian pada Gambar 3.2. Terdiri dari beberapa komponen berupa, persiapan system, persiapan IDS dan testing deteksi serangan.

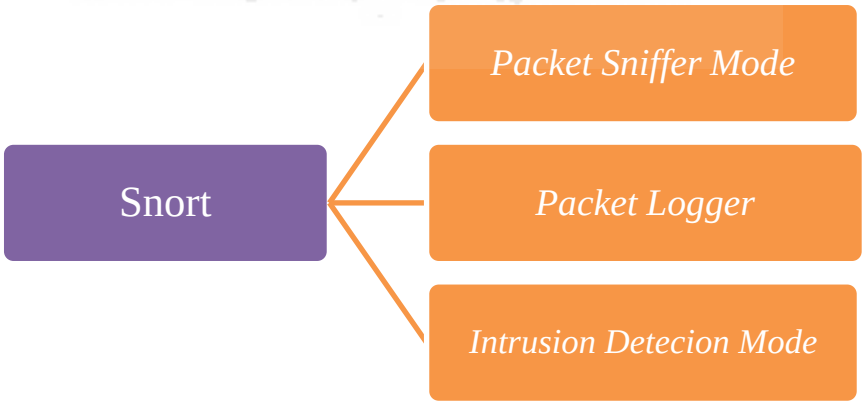


Gambar 3. 2 Tahapan Implementasi Intrusion Detection System (IDS) Snort

3.3 Konfigurasi Snort

Mempersiapkan *Intrsion Detection System* (IDS) Snort yang merupakan paket utama yang dibutuhkan dalam sistem, paket yang digunakan adalah paket *default snort* dari ubuntu yang dapat diinstal langsung dari *terminal console linux*, melakukan Konfigurasi *snort* merupa konfigurasi daq, konfigurasi *rules* yang tujuannya adalah menganalisis *packet* berdasarkan *rule* yang ada untuk mengenali adanya upaya serangan *hacker*. Sedangkan konfigurasi ini dilakukan agar *log* pada *Snort* dapat terbaca oleh *databse*.

Untuk memudahkan dalam memahami sistem pendeteksi penyusup oleh snort dapat di jelaskan pada Gambar 3.3 sebagai berikut:



Gambar 3. 3 Prinsip Kerja Sistem Snort

Dari Gambar 3.3 Dapat dijelaskan sebagai berikut:

1. *Snort*

   Snort merupakan aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas dalam sebuah jaringan, melakukan analisis dan mencari bukti dari percobaan *intrusi* (penyusupan).

2. *Packet sniffer mode*

   Dalam packet sniffer mode, *snort* bekerja sebagai sniffer sama seperti Wireshark. yang dapat melihat lalu lintas data pada jaringan komputer. Dikarenakan data mengalir secara bolak-balik pada jaringan, menangkap tiap-tiap paket dan kadang-kadang menguraikan isi dari RFC (Request for Comments) atau spesifikasi yang lain.

3. *Packet Logger*

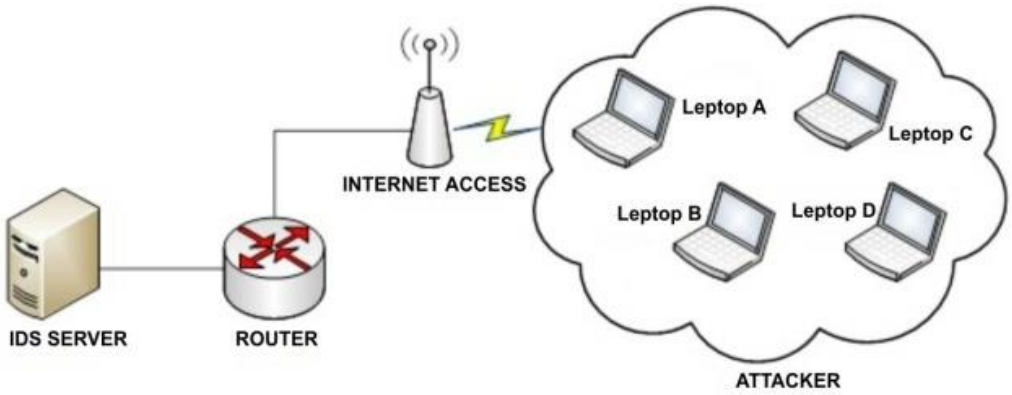
   Mencatat semua paket yang lewat pada jaringan untuk dapat di analisis.

4. *Intrusion Detection Mode*

   Pada mode ini Snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan computer. Untuk menggunakan mode IDS ini diperlukan setup dari berbagai jenis rule atau aturan yang akan membedakan sebuah paket normal dengan paket yang membawa serangan. Contoh Rule untuk membuat file baru # nano /etc/snort/rules/local.rules dan isi dengan code alert tcp any any → 192.168.1.0/24 111 (content:"|00 01 86 a5|";msg:"mountd access";).

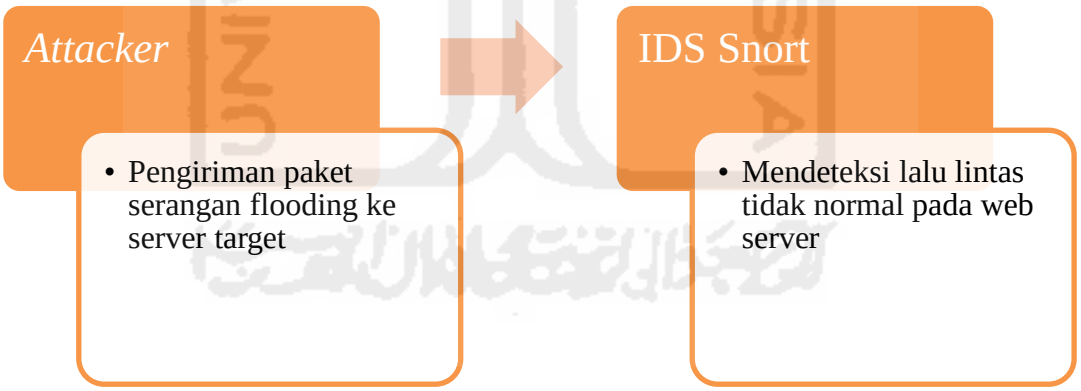
3.4 Simulasi Kasus

Merupakan tahap dilakukannya simulasi kasus untuk mencoba mengimplementasikan snort dalam mendeteksi penyusupan atau serangan. Simulasi kasus bertujuan untuk melakukan pengujian terhadap snort dalam mendeteksi penyusup atau serangan yang melakukan tindak kejahatan pada web server target yang digunakan untuk melindungi jaringan dengan kemampuan untuk merespon sesuai dengan kebijakan keamanan dari IDS Snort. Simulasi kasus *Intrusion Detection System* (IDS) Snort yang akan dijalankan mengguankan skenario pengiriman paket serangan menggunakan beberapa tool untuk menyerang web server target sekaligus menunjukkan bahaya yang dapat ditimbulkan oleh serangan. Gambar 3.4 menunjukkan gambaran umum dari skenario kasus deteksi serangan *flooding* pada web server.



Gambar 3. 4 Simulasi Kasus

Skema serangan adalah ketika *attacker* mengirimkan paket *flood* kepada target web server maka *Intrution Detection System* (IDS) akan mendeteksi adanya serangan lalu lintas trafik yang meningkat sesuai dengan rule flood yang telah ditentukan pada *Intrusion Detection System* (IDS). Pengiriman paket tersebut akan menyebabkan akses web server lambat, bahkan server akan mati ketika pengiriman serangan paket tersebut melebihi beban yang dimiliki server. Gambar 3.5 menunjuukan tahapan simulasi kasus deteksi serangan *flooding* pada web server yang menunjukkan *attacker* dalam mengirimkan serangan *flooding* ke target, sehingga *Intrusion Detection System* (IDS) mendeteksi lalu lintas pada web.



Gambar 3. 5 Tahap Simulasi Serangan Flooding Pada Web Server

3.5 Analisis

Menurut Muh Al Azhar forensik adalah suatu proses ilmiah atau suatu usaha ilmiah yang didasari ilmu pengetahuan dalam memngumpulkan, menganalisa dan menghadirkan bukti dalam suatupersidangan di pengadilan untuk membantu pengungkapan suatu kejahatan melalui pengungkapa bukti-bukti yang sah menurut undang-undang dan peraturan yang berlaku. Digital

forensik merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum (pro justice), yang dalam hal ini adalah untuk membuktikan kejahatan berteknologi tinggi atau computer crime secara ilmiah (scientific) sehingga bisa mendapatkan bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan tersebut. Disinilah tugas untuk para investigator dalam menangani kasus penyelidikan untuk dapat merecover ulang ejadian peristiwa tindak kriminal.

Sebelum dilakukannya proses model forensic maka terlebih dahulu melakukan uji tes deteksi serangan *flooding* menggunakan simulasi serangan yang nantinya akan dicocokkan dengan *rule* yang telah ditentukan ke dalam *Intrution Detection System* (IDS) Snort. Tahap deteksi serangan *flooding* ini terdiri dari beberapa proses, yaitu:

1. Tahap Pengoleksian (collection)

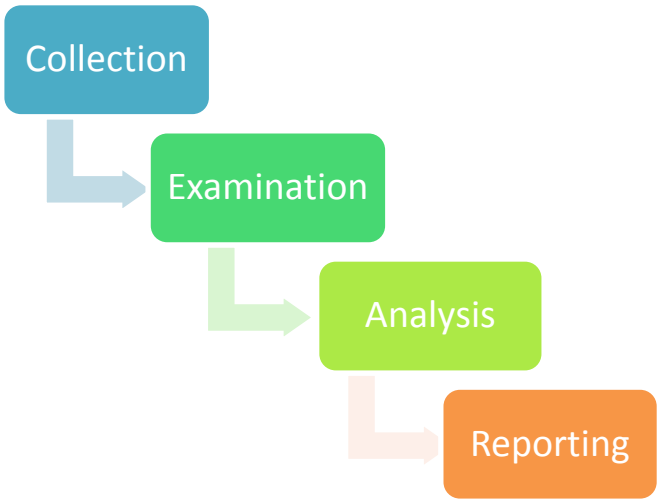
Proses pengoleksian merupakan proses pertama dalam model proses forensic untuk meneliti dan mencari barang bukti, pengenalan terhadap bukti-bukti penusupan, dan pengumpulan bukti dari *Intrution Detection System* (IDS) Snort yang melewati jaringan. Sehingga jika ada paket yang mencurigakan dan sesuai dengan aturan lalu lintas mengirimkan pesan *alert* dan menimpan sebagai log snort.

2. Tahap Pemeriksaan (Examination)

Pada tahap permeiksaan ini digunakan untuk mencari informasi yang tersembunyi dan mengungkapkan dokumen file log snort yang telah tersimpan sebagai alert dan hasil capture trafik web server untuk diperiksa.

3. Tahap Analisis

Pada tahap proses analisis dilakukan terhadap file log snort untuk mengetahui serangan apa yang terjadi, IP siapa yang melakukan serangan, kapan serangan terjadi, dimana serangan itu terjadi, bagaimana serangan tersebut bisa terjadi, dan mengapa itu terjadi. analisis dapat dilakukan dengan *tool* Wireshark. Model proses forensik ini dapat dilihat pada Gamabr 3.6 berikut ini.



Gambar 3. 6 Model Proses Forensik

Hasil dari model proses forensik akan dipresentasikan seperti tampak pada table dibawah ini kolom *timesstamp, source address, destination address, protocol, source port, destination port* dan *payload* atau isi pesan pada tabel 3.1 dibawah ini:

Tabel 3. 1 Pengelompokan Data

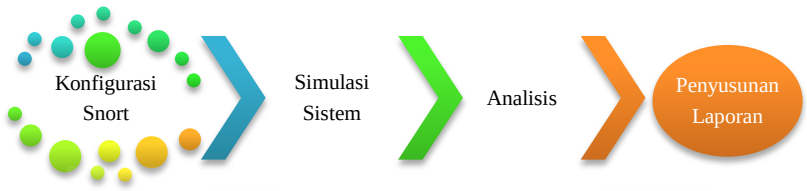
No	Timestamp	Source Address	Dest. Address	Protocol	Source Port	Dest. Port	Payload/Pesan

Setelah dikumpulkan barang bukti forensic log snort maka di dapat jumlah IP addres yang mencoba melakukan serangan *flooding* pada web server di lingkungan Univeritas Muhammadiyah Magelang.

3.6 Laporan

Merupakan tahap pembuatan laporan dan hasil pembuktian identifikasi serangan yang masuk ke dalam snort untuk pengujian mendeteksi penyusupan serta dapat mendapatkan informasi mengenai penyerang berdasarkan Tabel 3.1 dan 3.2 agar dapat mengurangi tingkat kerentanan terhadap serangan. Laporan berisi mengenai pendahuluan, litelatur review, metodologi penelitian, hasil dan pembahasan, serta penutup.

Kesimpulan yang diperoleh dari peelitian ini akan dimasukkan ke dalam bagian penutup dari laporan, berikut juga saran untuk penelitian-penelitian selanjutnya, khususnya yang mengambil penelitian tentang network *Intrusion Detection System* (IDS). Gambar 3.7 menunjukkan tahapan penusunan laporan dalam penelitian.



Gambar 3. 7 Tahapan Penyusunan Laporan

Laporan yang disusun pada ahirnya diharapkan dapat memberikan gambaran secara meyeluruh mengenai topik penelitian ini, serta dapat memberikan rekomendasi yang bermanfaat untuk penelitian selanjutnya.