BAB III
METODE PENELITIAN

3.1. Subjek dan Objek Penelitian

Subjek penelitian ini proses pengamatan dan penerapan *tools* IPS pada *website* yang akan diserang oleh serangan *cyber* DDoS. Admin akan mengetahui jika *website* tersebut tidak bisa diakses sementara waktu. Objek penelitian ini adalah hasil pengamatan dan penerapan *tools* IPS pada keamanan sebuah *website*.

3.2. Alat dan Bahan

Alat dan Bahan yang akan digunakan dalam penelitian ini antara lain :

3.2.1. Perangkat Keras

Perangkat keras yang dibutuhkan dalam proses penelitian ini adalah sebagai berikut :

1. Spesifikasi PC untuk Penyerang :
    a. Prosesor Intel® Core™ i5 8250u.
    b. Memory 4GB DDR4.
    c. Storage 1TB SATA HDD .
    d. Display 15” FHD (1920x1080).
    e. Graphic Nvidia MX230
2. Spesifikasi PC untuk Sistem IPS :
    a. Prosesor AMD Ryzen 5 3500U.
    b. Memory 8GB DDR4.
    c. Storage 1TB SATA HDD.
    d. Display 14” FHD.
    e. Graphic Radeon Vega Mobile GFX.

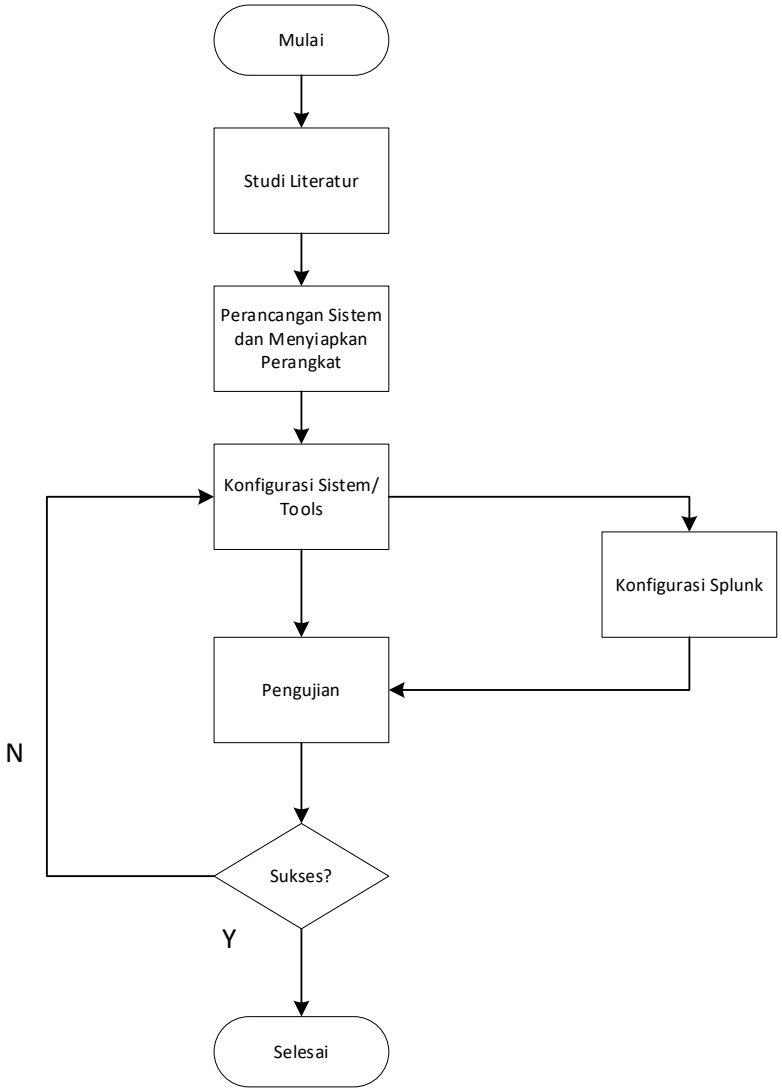
3.2.2. Perangkat Lunak

Perangkat lunak yang dibutuhkan dalam penelitian ini adalah sebagai berikut :

1. Perangkat Lunak Kali Linux sebagai sistem operasi bagi penyerang DDoS
2. *Tools* Splunk.

3. *Tools* Slowloris.
4. *Website* (http://www.kesekolah.com/)

3.3. Diagram Alur Penelitian



Gambar 3.1 Diagram Alur Penelitian

3.3.1. Studi Literatur

Tahapan penelitian ini melakukan pengujian terhadap *website* yang telah disiapkan. Peneliti melakukan literatur mengenai *website* yang akan diserang dan *tools* Slowloris yang akan digunakan. Kemudian *tools* Splunk digunakan untuk mengumpulkan data, pencarian data, dan *log monitoring* data yang masuk. Data yang diperoleh berupa jurnal, buku maupun artikel. Tujuan dari literatur adalah untuk memperkuat permasalahan yang diangkat pada penelitian ini serta menjadi dasar untuk melakukan pengembangan selanjutnya.

3.3.2. Perancangan Sistem dan Menyiapkan Perangkat

Pada penelitian ini akan merancang sebuah sistem yang akan diteliti, yaitu menyiapkan *tools* Splunk yang akan dipakai dalam melakukan pencegahan. Perangkat yang dibutuhkan untuk pengkonfigurasian sistem sampai pengujian sistem, antara lain yaitu :

1. Satu unit PC sebagai Penyerang.
2. Satu unit PC sebagai server *Intrusion Prevention System* (IPS).
3. Satu unit PC sebagai *User*.

Lalu sistem akan diuji menggunakan serangan sesuai dengan scenario pengujian yang dirancang.

3.3.3. Konfigurasi Sistem

Pada tahap ini akan dilakukan penkonfigurasian sistem yang dimana akan mensetting *tools* IPS dan sebuah *website* dan dilakukan serangan *cyber*, *tools* tersebut akan digunakan untuk melakukan *defence* dan memberikan notifikasi paket serangan yang masuk. Pada penelitian ini terbagi menjadi dua program yaitu program untuk melakukan serangan ke *website* dalam bentuk DDoS dan program *tools* Splunk pada laptop yang sudah di konfigurasikan. Pada program serangan terhadap *website* menggunakan serangan *cyber* DDoS yang nantinya *website* tidak bisa digunakan atau tidak bisa diakses baik *user* maupun *admin*. Pada program Splunk akan dikonfigurasikan sebagai *defence*.

3.3.4. Pengujian Sistem

Pada tahap ini akan dilakukan pengujian terhadap *website* yang akan diserang. Kegiatan ini bertujuan untuk mengetahui tingkat keamana *website* dari

serangan DDoS. Pengujian yang akan dilakukan adalah pengujian fungsionalitas sistem untuk mengetahui sistem dapat berjalan dengan baik, pengujian serangan slowloris untuk mengetahui serangan sukses dilakukan, kemudian pengujian sistem splunk untuk mengetahui serangan berhasil di deteksi oleh sistem.

1. Pengujian fungsionalitas sistem

   Pengujian fungsionalitas sistem dilakukan dengan cara menyerang website sebanyak 2 (dua) kali penyerangan dan dilakukan pengecekan pada *website* tersebut menggunakan *tools* Slowloris menyerang dengan *packet* yang sudah disetting yaitu 1000 *packet* selama 5 menit.

2. Pengujian serangan Slowloris dan sistem Splunk.

   Pengujian serangan slowloris dilakukan dengan mengirimkan *packet* sebesar 1000 *packet*. Pengujian ini bertujuan untuk menguji *website* yang diserang, dan pada sistem Splunk akan mendeteksi *packet* serangan Slowloris yang masuk, dan akan di *block* oleh Splunk.

Mekanisme pengujian dilakukan dengan melihat kondisi normal *traffic* 200 *packet request*/1 detik secara normal, disaat *website* tersebut diserang Slowloris *request* pada *website* naik sampai 1000-1200 *packet request*/1 detik yang masuk