BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi infomasi merupakan hal yang penting bagi masyarakat saat ini dalam internet. Dengan adanya internet membuat komunikasi dan informasi sangat mudah didapatkan. Kemudahan ini menyebabkan terjadinya kejahatan di dunia maya. Kejahatan cyber dapat menyerang jaringan komputer, menyusup kedalam jaringan mengambil data – data rahasia dan melumpuhkan sistem jaringan komputer. Dalam mengatasi kejahatan yang akan terjadi, dibutuhkan sistem yang dilengkapi *firewall* dan *Intrusion Detection System*(IDS). *Firewall* dan *Intrusion Detection System*(IDS) sebagai fiitur keamanan jaringan yang dapat melindungi server, melindungi jaringan internal, dan memblok serangan. Fitur *Firewall* dan *Intrusion Detection System*(IDS) dapat diterapkan dalam Tools OPNSense. OPNsense merupakan *operating system* yang bersifat *open source* yang digunakan untuk konfigurasi *firewall* dan *Routing*. OPNSense memberikan kemudahan dalam melakukan berbagai macam pengaturan melalui antarmuka web (web GUI / *graphical users interface*).

Dengan demikian Proyek Akhir ini berjudul "**Membangun Sistem Keamanan Jaringan Berbasis Firewall dan IDS Menggunakan Tools OPNSense** ". Dengan tools OPNSense memberikan solusi melindungi server dan memblokir serangan, mencatat log serangan. ketika terjadi serangan berupa Serangan *Port Scanning*, *Denial of Service*(DOS).

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka dapat dirumuskan permasalahan sebagai berikut.

1. Bagaimana cara konfigurasi firewall dan IDS menggunakan tools OPNSense ?
2. Bagaimana cara melakukan pengujian Scanning port, Serangan (DDoS), Web Filter?

3. Bagaimana cara memonitoring jaringan pada saat terjadinya aktifitas peretasan?

1.3 Tujuan

Adapun tujuan yang ingin dicapai dalam pembuatan laporan tugas akhir ini adalah:

1. Konfigurasi Firewall dan IDS dilakukan dengan cara mengkonfigurasi rules pada Firewall dan IDS.
2. Pengujian scanning port menggunakan tools Masscan, untuk DoS menggunakan LOIC, dan Web filter menggunakan rules yang ada pada Firewall.
3. Untuk Memonitoring jaringan pada saat terjadinya peretasan bisa dilihat pada menu Log.

1.4 Batasan Masalah

Untuk menghindari luasnya pembahasan masalah yang akan di teliti maka terdapat beberapa Batasan yaitu :

1. Menggunakan Aplikasi VirtualBox sebagai media pengerjaan Proyek Akhir.
2. Tidak menggunakan aplikasi Firewall lain selain OPNSense.
3. Menggunakan fitur Masscan untuk melakukan scanning port pada web server yang akan di retas.
4. Menggunakan 1 buah laptop.
5. Menggunakan aplikasi LOIC untuk melakukan penyerangan berupa DDOS.
6. Menggunakan firmware suricata untuk *Intrusion Detection System(IDS)* pada Tools OPNSense.
7. Menggunakan layanan Web pada Sistem Operasi Ubuntu 21.04.