# BAB I
# PENDAHULUAN

## A. Latar Belakang

Di era digital saat ini, lanskap ancaman siber telah berevolusi secara dramatis. Serangan terhadap infrastruktur digital, terutama pada *web server* yang merupakan garda terdepan dalam menyediakan layanan, tidak lagi terbatas pada upaya sederhana. Pelaku ancaman modern menggunakan taktik, teknik, dan prosedur (TTP) yang canggih untuk mendapatkan akses awal, kemudian melakukan pergerakan lateral (*lateral movement*) di dalam jaringan untuk mencapai target bernilai tinggi.

Sebagai contoh nyata, kasus kebocoran data Equifax pada tahun 2017 menjadi pelajaran penting. Penyerang berhasil mendapatkan akses awal dengan mengeksploitasi kerentanan pada perangkat lunak framework Apache Struts yang berjalan di salah satu web server Equifax [1]. Setelah berhasil masuk, mereka tidak berhenti di situ. Selama beberapa minggu, penyerang bergerak secara lateral di dalam jaringan internal, tidak terdeteksi, hingga berhasil menemukan dan mengekstrak data pribadi sensitif milik jutaan orang. Kasus ini membuktikan bahwa pertahanan perimeter saja tidak cukup; tanpa adanya monitoring di level host dan segmentasi jaringan yang kuat, penyerang yang berhasil masuk dapat leluasa bergerak untuk mencapai tujuan utamanya.

Menghadapi tantangan serupa, berbagai penelitian terdahulu telah menawarkan solusi keamanan dengan pendekatan yang berbeda-beda. Adha, Rizal, dan Ismail dalam penelitiannya mengimplementasikan sistem keamanan jaringan berbasis OPNsense, yang terbukti efektif dalam memantau dan menyaring lalu lintas jaringan yang mencurigakan di perimeter [2]. Sementara itu, fokus pada keamanan aplikasi *web* telah diteliti oleh Prasetyo menggunakan *Web Application Firewall* (WAF) ModSecurity [3]. Di sisi lain, pemanfaatan Wazuh sebagai sistem deteksi juga telah diuji oleh Nova, Pratama, dan Prayama untuk mendeteksi serangan DoS [4].

Meskipun penelitian-penelitian tersebut memberikan kontribusi signifikan, sebagian besar masih berfokus pada mekanisme pertahanan tunggal atau parsial. Ketergantungan pada satu lapisan keamanan sering kali menyisakan celah (*security*

*gap*) jika *firewall* perimeter ditembus, tidak ada mekanisme deteksi sekunder yang memadai di level internal.

Oleh karena itu, diperlukan pendekatan strategis yang lebih komprehensif namun tetap fleksibel. Konsep pertahanan berlapis (*defense-in-depth*) muncul sebagai respons paling efektif terhadap ancaman modern. Filosofi ini didasarkan pada prinsip bahwa tidak ada satu pun lapisan keamanan yang sempurna. Dengan menerapkan berbagai lapisan pertahanan mulai dari *firewall* di perimeter jaringan hingga sistem deteksi intrusi di level *host* sebuah organisasi dapat secara signifikan mengurangi kemungkinan keberhasilan serangan.

Penelitian ini merupakan implementasi praktis dari filosofi pertahanan berlapis, yang berfokus pada pengamanan web server. Dengan mengintegrasikan firewall *open-source* OPNsense sebagai pertahanan jaringan dan Wazuh sebagai platform SIEM (*Security Information and Event Management*) untuk monitoring di level host[5], penelitian ini bertujuan untuk menganalisis efektivitas arsitektur keamanan gabungan tersebut terhadap simulasi serangan siber yang realistis, guna menutupi kelemahan yang ditemukan pada sistem pertahanan tunggal.

.

## B. Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah dalam penelitian ini adalah bagaimana efektivitas sistem pertahanan yang dibangun dapat diverifikasi dan dianalisis melalui simulasi serangan nyata terhadap web server?

## C. Batasan Penelitian

Pembatasan Penelitian digunakan agar pembahasan sesuai dengan yang dimaksudkan dan tidak menimbulkan permasalahan yang baru, maka peneliti memberikan batasan masalah sebagai berikut:

1. Lingkungan penelitian dibangun sepenuhnya secara virtual dengan data *dummy*. menggunakan perangkat lunak VMware Workstation.
2. Perangkat lunak yang digunakan adalah OPNsense sebagai firewall, Wazuh sebagai SIEM, Ubuntu Server sebagai *web server* target, dan Kali Linux sebagai mesin penyerang.

3. Konfigurasi jaringan mencakup tiga segmen: WAN (NAT), Management LAN (*Host-only*), dan DMZ Network (*Host-only*).
4. Simulasi serangan yang dilakukan terbatas pada *dos attack* dan *brute force* SSH untuk menguji respons firewall dan sistem deteksi intrusi.

## D. Tujuan Penelitian

Berdasarkan rumusan masalah yang telah disebutkan, maka Penelitian ini bertujuan untuk mengevaluasi efektivitas arsitektur keamanan berlapis (*Defense in Depth*) yang mengintegrasikan OPNsense dan Wazuh pada lingkungan *web server*. Validasi sistem dilakukan melalui simulasi serangan nyata, yakni *Denial of Service* (DoS) dan *Brute Force*, guna menguji keandalan mekanisme deteksi serta mitigasi yang dibangun.

## E. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Memberikan pemahaman praktis bagi mahasiswa mengenai implementasi konsep *defense-in-depth* dalam mengamankan infrastruktur server menggunakan teknologi *open-source*.
2. Menyediakan model atau referensi arsitektur keamanan jaringan yang efektif dari segi biaya bagi organisasi skala kecil hingga menengah untuk melindungi aset digital mereka, khususnya *web server*.
3. Memberikan pengalaman langsung dalam melakukan instalasi, konfigurasi, integrasi, dan pengujian OPNsense dan Wazuh dalam sebuah lingkungan lab yang terkontrol.