BAB I PENDAHULUAN

I.1 Latar Belakang

Keamanan jaringan merupakan elemen yang krusial dalam mendukung sistem informasi di era digital saat ini. Pertumbuhan teknologi informasi dan komunikasi telah membawa dampak positif terhadap efisiensi operasional, namun di sisi lain juga membuka potensi risiko terhadap keamanan data. Ancaman siber seperti pencurian data, serangan *brute force*, dan eksploitasi konfigurasi sistem menjadi tantangan yang perlu dihadapi dengan pendekatan yang sistematis dan adaptif (Susanto et al., 2023).

Dalam konteks pengamanan komunikasi jaringan, pendekatan VPN telah lama digunakan untuk menyediakan konektivitas yang terenkripsi dan privat bagi pengguna jarak jauh. OpenVPN sebagai salah satu implementasi *open-source* dari VPN banyak diadopsi karena mendukung beragam metode autentikasi, enkripsi, dan fleksibilitas konfigurasi (Akinsanya et al., 2024). Seiring berkembangnya kebutuhan akan manajemen akses yang lebih terkendali, konsep ZTNA muncul sebagai pendekatan yang dirancang untuk mengelola akses terhadap sumber daya digital secara ketat, berdasarkan prinsip verifikasi berkelanjutan terhadap identitas dan hak akses pengguna (Khan, 2023).

ZTNA memanfaatkan konsep seperti *identity-based access, micro-segmentation,* serta *continuous verification* untuk mengontrol konektivitas dalam jaringan. Salah satu platform yang digunakan untuk mendemonstrasikan pendekatan ini adalah OpenZiti, yang menawarkan pendekatan berbasis identitas dalam pengelolaan trafik jaringan secara *overlay*.

Penelitian ini dilakukan untuk memprofilkan mekanisme fungsi kontrol keamanan. Beberapa jenis simulasi ancaman yang digunakan dalam eksperimen meliputi *port scanning, brute force login*, serta manipulasi konfigurasi seperti modifikasi *token* dan pengaturan koneksi. Masing-masing sistem diuji untuk memperoleh gambaran teknis terkait pencatatan *log*, respons terhadap aktivitas tidak sah, serta perilaku sistem saat menangani trafik.

Selain fungsi kontrol, penelitian ini juga mencatat sejumlah metrik teknis seperti *response time, log granularity*, dan jaringan/performa sistem, guna menyusun profil karakteristik operasional dari kedua sistem dalam konteks yang telah ditentukan. Pemanfaatan pendekatan eksperimen berbasis sistem *blackbox* digunakan agar penilaian lebih fokus pada output yang dihasilkan oleh sistem ketika menghadapi ancaman eksternal.

Dengan pendekatan ini, hasil penelitian tidak ditujukan untuk menilai keunggulan atau kelemahan masing-masing pendekatan, melainkan untuk menyediakan data dan profil teknis yang dapat menjadi referensi dalam memahami karakteristik dari solusi keamanan jaringan yang diuji. Informasi ini diharapkan berguna dalam mendukung pengambilan keputusan teknis dalam pengelolaan infrastruktur jaringan yang aman dan terukur.

I.2 Perumusan Masalah

1. Bagaimana fungsi kontrol terhadap serangan siber yang diterapkan dalam ZTNA dan VPN?
2. Bagaimana *profiling* terhadap *output* sistem ZTNA dan VPN dalam menghadapi kategori serangan siber?
3. Bagaimana profil metrik keamanan dan *performance* jaringan pada sistem ZTNA dan VPN?

I.3 Tujuan Penelitian

Berdasarkan perumusan masalah yang ada, tujuan yang ingin dicapai dari penelitian ini adalah sebagai berikut :

1. Menganalisis penerapan fungsi kontrol yang mencakup IAAA (*Identification, Authentication, Authorization* dan *Accounting*) pada platform OpenZiti dan OpenVPN.
2. Melakukan profiling terhadap *output* sistem OpenZiti dan OpenVPN dalam menghadapi kategori serangan siber seperti *port scanning*, *brute force*, dan *configuration manipulation*.

3. Menggambarkan profil metrik yang terdiri dari *response time*, *granularity*, dan *performance* jaringan pada masing-masing sistem berdasarkan hasil eksperimen.

I.4 Batasan Penelitian

Adapun batasan dalam melakukan penelitian ini, sebagai berikut:

1. Penelitian dilakukan dengan pendekatan *blackbox* berbasis eksperimen, tanpa mengakses atau menganalisis struktur internal kode sumber perangkat lunak.
2. Jenis serangan yang disimulasikan dan dianalisa mencakup *port scanning*, *brute force*, dan *configuration manipulation*.
3. Jenis *Performance* jaringan yang disimulasikan dan dianalisa mencakup *Download Speed, Upload Speed, Latency, Jitter, Packet Loss, Network Throughput, File Download Time,* dan *Data Transfer Rate.*

I.5 Manfaat Penelitian

Adapun manfaat yang didapatkan dengan adanya penelitian Tugas Akhir ini adalah sebagai berikut:

1. Secara teoritis
    a. Memberikan gambaran mendalam mengenai penerapan fungsi kontrol pada sistem OpenZiti dan OpenVPN.
    b. Mengembangkan pemahaman terhadap metrik teknis seperti *response time*, *log granularity*, dan *performance* jaringan dalam konteks pengujian keamanan jaringan.

2. Secara praktis

    a. Menyediakan profil teknis yang dapat dijadikan gambaran dalam implementasi dan konfigurasi sistem akses jaringan berbasis VPN dan ZTNA.

    b. Mengetahui cara penggunaan *software* OpenZiti dan OpenVPN, dan *software* untuk menguji fungsi kontrol dan *performance*.