1. Pendahuluan

1.1 Latar Belakang

Dalam lingkungan bisnis kontemporer, meningkatnya kebutuhan akan konektivitas dan operasional jaringan komputer telah menyebabkan meningkatnya frekuensi serangan *Distributed Denial of Service* (DDoS). Serangan ini menargetkan sumber daya sistem seperti bandwidth server, Central Processing Unit (CPU), dan Random Access Memory (RAM) dengan meluncurkan serangan Denial of Service (DoS), yang kemudian didistribusikan ke banyak komputer [1]. Akibatnya, server atau sistem menjadi tidak dapat diakses oleh klien yang sah [2]. Serangan DDoS membahayakan keamanan jaringan, berdampak negatif terhadap perekonomian, dan mengganggu operasi organisasi [3].

Multiple network domains mengacu pada berbagai sistem yang saling berhubungan yang bekerja secara sinergis [4]. Dalam konteks multi-organisasi, domain-domain ini berasal dari entitas yang berbeda namun saling berhubungan. Serangan DDoS, seperti botnet, menimbulkan tantangan signifikan terhadap jaringan komputer dan perangkat di *Internet of Things* (IoT), terutama ketika melibatkan banyak organisasi [5]. Akibatnya, solusi keamanan seperti *Intrusion Detection Systems* (IDS) sangat penting dan telah diadopsi secara luas [6].

Solusi yang diusulkan adalah mengembangkan sistem deteksi serangan DDoS yang mengintegrasikan IDS heterogen dengan platform *Security Information and Event Management* (SIEM), memfasilitasi analisis pemantauan serangan DDoS yang lebih komprehensif untuk Security Operations Center (SOC) di seluruh jaringan multi-organisasi. IDS beroperasi dengan memonitor pristiwa jaringan atau sistem komputer, menganalisisnya untuk potensi ancaman [6]. Namun, IDS memiliki keterbatasan dimana IDS dapat menghasilkan peringatan palsu bahkan tanpa adanya aktivitas serangan, sehingga menyebabkan kesalahan deteksi [7]. Untuk memitigasi hal ini, penggunaan mekanisme alert correlation diperlukan. Mekanisme ini memproses peringatan dari sumber IDS yang heterogen, mengurangi *false positive* dan secara akurat mengidentifikasi pola serangan [8].

SIEM memainkan peran penting dalam mencegah dan mendeteksi serangan siber. SIEM memiliki kemampuan untuk mengumpulkan, menggabungkan, menyimpan, dan menghubungkan peringatan dari berbagai sumber [9]. SIEM terdapat dua bagian, yaitu SIEM *manager* dan SIEM *agent*, dimana SIEM *agent* bertugas untuk mengumpulkan log dari berbagai IDS, sedangkan SIEM *manager* bertugas untuk menerima log dari berbagai SIEM *agent*. Server atau host yang ada pada jaringan komputer akan dikonfigurasikan dengan satu IDS dan SIEM *agent* untuk mendapatkan *alert* dari serangan DDoS, konsep seperti ini biasanya disebut sebagai sistem *multi-agent* dimana banyak *agent* yang akan diinstal pada perangkat yang berbeda untuk mencapai tujuan yang sama [10].

Kontribusi utama dari jurnal ini mencakup integrasi IDS yang heterogen dengan SIEM untuk melakukan pemantauan dan deteksi serangan DDoS yang komprehensif di berbagai organisasi. Sistem ini menggunakan mekanisme *alert correlation* untuk memproses data dari berbagai sumber IDS, mengurangi *false positive*, dan meningkatkan deteksi pola atau anomali yang mengindikasikan serangan DDoS. Selain itu, sistem ini menggunakan pengaturan *multi-agen*, menyebarkan agen IDS di berbagai perangkat untuk meningkatkan pengumpulan data yang terkoordinasi. Penggunaan 2 *open-source tools* menurunkan biaya implementasi sekaligus menjaga keandalan sistem. Dengan mengembangkan sistem deteksi serangan DDoS yang mengintegrasikan IDS heterogen dengan SIEM, agar dapat memastikan keandalan dan ketersediaan sistem dalam menghadapi ancaman tersebut. Pengukuran kinerja sistem dilakukan untuk memastikan kinerjanya dalam mendeteksi.

1.2 Rumusan Masalah

Permasalahan yang dibahas mencakup konsep dan teknologi yang digunakan untuk mengembangkan sistem deteksi serangan DDoS, khususnya IDS heterogen dan SIEM. Permasalahan yang akan dibahas adalah sebagai berikut:

1. Bagaimana bentuk sistem arsitektur dan komponen open-source yang digunakan untuk integrasi IDS yang heterogen dengan SIEM dalam mendeteksi serangan DDoS?
2. Bagaimana hasil kinerja sistem deteksi serangan DDoS dengan integrasi IDS heterogen dengan SIEM untuk mendeteksi serangan DDoS?

1.3 Tujuan

Tujuan dari penelitian ini adalah mengembangkan dan menguji sistem deteksi serangan DDoS dengan integrasi IDS yang heterogen dengan SIEM untuk mendeteksi serangan DDoS dalam jaringan komputer multi-organisasi. Secara khusus, targetnya meliputi:

1. Merancang dan mengimplementasikan arsitektur sistem untuk integrasi antara IDS yang heterogen dengan SIEM dalam mendeteksi serangan DDoS.
2. Menguji kinerja sistem deteksi yang dikembangkan terkait kemampuannya mendeteksi serangan DDoS secara akurat.