BUKU MANUAL APLIKASI
DISTRIBUSI IDS (INTRUSION DETECTION SYSTEM) PADA CLOUD COMPUTING BERBASIS KOMBINASI SNORT DAN *SUPPORT VECTOR MACHINE*

Oleh:

Yuri Ariyanto

Muhammad Dhiyaul Auliya'

POLITEKNIK NEGERI MALANG
NOVEMBER 2023

DAFTAR ISI

BAB 1 PENDAHULUAN

Banyaknya kasus serangan pada jaringan komputer terjadi karena sistem jaringan tidak mengetahui jika terjadi serangan didalam sistem. Salah satu teknologi perkembangan jaringan komputer yaitu cloud computing. Dengan layanan yang dimiliki cloud computing dapat memberikan manfaat, akan tetapi juga memberikan resiko dalam bidang keamanan pada sistem didalamnya. Salah satu cara yang dapat dilakukan untuk mendeteksi resiko serangan adalah dengan menggunakan Intrusion Detection System (IDS). Oleh karena itu, penelitian ini bertujuan untuk menambahkan sebuah algoritma machine learning untuk membantu mendeteksi serangan yang tidak dapat dikenali oleh snort IDS. Salah satu algoritma yang dapat digunakan adalah Support Vector Machine (SVM) yang merupakan algoritma machine learning yang digunakan dalam pengenalan pola, dan deteksi intrusi jaringan tidak normal. SVM dapat mempelajari pola dalam memberikan klasifikasi yang akurat dengan menggunakan label kelas. Klasifikasi akurat dicapai oleh training machine untuk mengklasifikasikan sampel yang tidak diketahui dengan model dataset pelatihan.

Maka dari hasil penelitian ini menghasilkan beberapa akurasi dengan skema pengujian berbeda. Untuk skema pengujian 50%:50% menghasilkan akurasi sebesar 99,74%, sedangkan skema pengujian 70%:30% menghasilkan akurasi sebesar 98,55%, Dan untuk skema 80%:20% menghasilkan akurasi tertinggi sebesar 99.81% dengan model dataset perbandingan 80:20 dari dataset latih dan uji.

BAB 2 PERSIAPAN HARDWARE DAN SOFTWARE

2.1.Perangkat Keras *(Hardware)*

Berikut adalah beberapa perangkat keras yang disiapkan dalam pembuatan sistem media pembelajaran. Spesifikasi *hardware* ditunjukkan pada tabel 2.1.

Tabel 2.1 Kebutuhan Perangkat Keras

No.	Nama Perangkat Keras	Keterangan
1.	Laptop	Processor : Core i3 Gen 7 CPU : 2.30GHz RAM : 4GB

2.2.Perangkat Lunak *(Software)*

Berikut adalah beberapa perangkat lunak yang disiapkan dalam pembuatan sistem media pembelajaran. Spesifikasi *hardware* ditunjukkan pada tabel 2.2.

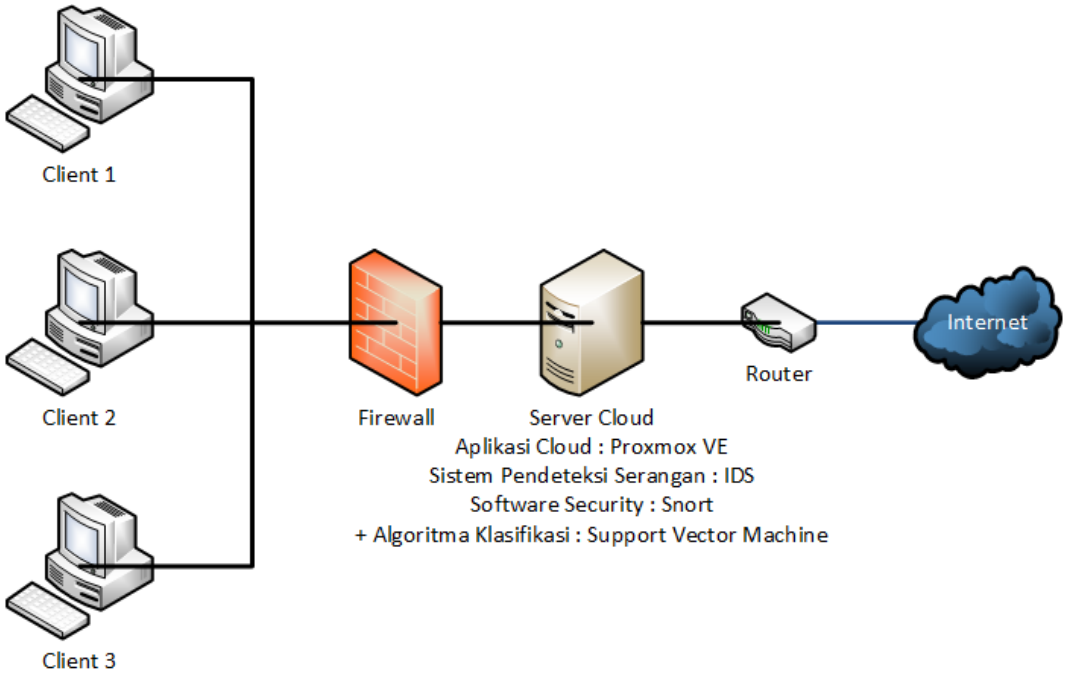
Tabel 2.2 Kebutuhan Perangkat Lunak

No.	Perangkat	Keterangan
1.	Open VPN	Akses server
2.	Proxmox VE	OS server
3.	Ubuntu	OS VM
4.	Snort	*Tools* IDS

BAB 3 PETUNJUK INSTALASI

3.1.Desain Topologi

Secara umum, desain sistem harus mempertimbangkan keamanan, efisiensi, dan akurasi. Keamanan harus menjadi prioritas utama, karena sistem harus dapat memproteksi data penting dan melindungi integritas sistem cloud computing. Efisiensi harus diperhitungkan untuk mengurangi overhead dan memastikan sistem dapat beroperasi dengan cepat dan efisien. Akurasi harus dipertimbangkan untuk memastikan sistem dapat mendeteksi serangan malware dengan benar danmeminimalisir tingkat false positive. Ada beberapa desain sistem yang digunakan dalam penelitian ini.



Gambar 3.1. Desain Topologi

3.2.Desain Alamat IP

Dari hasil pengamatan, pembagian alamat IP mengikuti rentang IP yang telah tersetting oleh server. Pembagian alamat IP menggunakan konfigurasi berjenis statis agar memudahkan identifikasi dan konfigurasi terhadap server. Pembagian alamat IP dapat dilihat pada tabel 3.2.

Nama	**IP**	**Netmask**	**Gateway**	**Username**
Server	192.168.0.3	192.168.0.0/24	192.168.0.1	UBUNTU-0
Klien 1	192.168.0.4	192.168.0.0/24	192.168.0.1	UBUNTU-1
Klien 2	192.168.0.5	192.168.0.0/24	192.168.0.1	UBUNTU-2
Klien 3	192.168.0.6	192.168.0.0/24	192.168.0.1	UBUNTU-3
Penyerang	192.168.0.7	192.168.0.0/24	192.168.0.1	UBUNTU-4

Gambar 3.2. Desain alamat IP

3.3.Spesifikasi VM

Spesifikasi dalam pembuatan VM memiliki kapasitas yang cukup untuk menjalankan sistem penelitian ini. Spesifikasi VM dapat dilihat pada tabel 3.3.

Nama	***Processor***	**RAM**	***Storage***
Server	2 Core	2 Gb	2048 Mb
Klien 1	2 Core	2 Gb	2048 Mb
Klien 2	2 Core	2 Gb	2048 Mb
Klien 3	2 Core	2 Gb	2048 Mb
Penyerang	2 Core	2 Gb	2048 Mb

Gambar 3.3. Spesifikasi VM

BAB IV PETUNJUK FITUR-FITUR APLIKASI

Sistem deteksi serangan tidak langsung sangat berguna bagi keamanan. Ada beberapa tools seperti snort yang dapat digunakan dengan memberikan beberapa fitur yang berguna. Snort menawarkan sejumlah fitur yang mendukung deteksi intrusi yang efektif.

1. **Rule-Based Detection**
   Snort menggunakan aturan atau rulesets untuk mendeteksi pola atau tanda tangan serangan yang telah dikenali sebelumnya. Dashboard untuk pengajar
2. **Pattern Matching**
   Mampu melakukan pencocokan pola atau string dalam lalu lintas jaringan dengan database tanda tangan untuk mengidentifikasi serangan.Tampilan pembuatan soal
3. **Kustomisasi Rulesets**
   Pengguna dapat membuat dan mengonfigurasi rulesets yang sesuai dengan kebutuhan spesifik mereka.
4. **Logging and Reporting**
   Mampu mencatat dan melaporkan aktivitas jaringan yang mencurigakan atau terdeteksi sebagai serangan.

Jika Anda menggabungkan Snort (yang memanfaatkan deteksi berbasis tanda tangan) dengan Support Vector Machine (SVM, yang biasanya digunakan untuk deteksi berbasis anomali), ada beberapa fitur yang dapat Anda manfaatkan dari kedua alat tersebut:

1. **Analisis Gabungan**
   Menggabungkan hasil deteksi berbasis tanda tangan dengan analisis anomali untuk meningkatkan akurasi deteksi.
2. **Pemantauan Kinerja**
   Memantau kinerja dan keandalan deteksi berdasarkan gabungan dari dua pendekatan deteksi yang berbeda.

BAB V PETUNJUK PENGGUNAAN APLIKASI

Langkah-langkah untuk menggunakan distribusi IDS (Intrusion Detection System) dalam lingkungan Cloud Computing dengan kombinasi Snort dan Support Vector Machine (SVM) dapat melibatkan serangkaian proses dan konfigurasi yang kompleks. Berikut adalah panduan langkah-langkah yang mungkin diperlukan:

Langkah 1: Persiapan Lingkungan Cloud

1. Pilih Platform Cloud
   Pilih platform Cloud yang sesuai dengan kebutuhan Anda, misalnya AWS, Azure, Google Cloud, dsb.
2. Konfigurasi Lingkungan
   Buat dan konfigurasi instance yang sesuai untuk pengujian IDS.

Langkah 2: Instalasi dan Konfigurasi Snort

3. Unduh dan Instalasi Snort
   Unduh versi terbaru dari Snort, lalu ikuti petunjuk instalasi yang disediakan.
4. Konfigurasi Snort
   Konfigurasikan Snort sesuai dengan kebutuhan deteksi intrusi yang diinginkan.

Langkah 3: Persiapan dan Pelatihan SVM

5. Data Preparation
   Persiapkan dataset yang akan digunakan untuk pelatihan SVM untuk deteksi anomali.
6. Preprocessing Data
   Bersihkan, normalisasi, dan persiapkan data untuk digunakan dalam pelatihan SVM.
7. Pelatihan SVM
   Lakukan pelatihan SVM menggunakan dataset yang disiapkan.

Langkah 4: Integrasi Snort dan SVM

8. Integrasi Metode Deteksi
   Terapkan hasil pelatihan SVM ke dalam sistem Snort untuk meningkatkan deteksi intrusi.

Langkah 5: Uji Coba dan Evaluasi

9. Pengujian Intrusi

   Lakukan pengujian dengan skenario intrusi yang berbeda untuk menguji efektivitas sistem.

10. Optimasi dan Pemantauan

    Tinjau hasil deteksi, optimalkan model SVM, dan lakukan pemantauan terus-menerus untuk memastikan kinerja yang optimal.

Langkah 6: Implementasi dan Penggunaan

11. Penerapan Sistem IDS

    Terapkan sistem IDS yang sudah dikonfigurasi ke dalam lingkungan Cloud.

12. Pemantauan Real-Time

    Pantau sistem IDS untuk mendeteksi dan merespons ancaman secara real-time.