BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring dengan meningkatnya jumlah dan kompleksitas serangan terhadap infrastruktur IT, keamanan server menjadi prioritas utama dalam manajemen sistem informasi, terutama untuk web server. Dalam konteks ini, server menjadi target utama bagi pihak-pihak tidak bertanggung jawab karena perannya yang krusial dalam mendukung operasional bisnis modern. Salah satu tantangan utama yang dihadapi administrator server adalah melindungi server dari berbagai bentuk serangan yang memanfaatkan port terbuka, seperti port scanning, brute force, dan serangan otomatis lainnya.

Port terbuka, seperti port 22 untuk remote SSH dan port 80 untuk HTTP, sering menjadi pintu masuk bagi penyerang. Melalui port scanning, penyerang dapat memetakan port-port yang terbuka pada server dan menggunakannya sebagai langkah awal untuk melakukan serangan lebih lanjut. Dalam banyak kasus, serangan semacam ini tidak hanya menyebabkan downtime server tetapi juga berpotensi mencuri data sensitif, yang dapat mengganggu operasional bisnis dan merusak reputasi organisasi. Meskipun firewall telah menjadi standar dalam pengamanan server, ketergantungan penuh pada firewall saja sering kali tidak cukup untuk melindungi server dari serangan yang semakin canggih. Firewall hanya berfungsi sebagai penjaga gerbang yang menyaring lalu lintas jaringan, tetapi tidak memberikan mekanisme otentikasi yang lebih kompleks. Oleh karena itu, diperlukan solusi keamanan tambahan yang dapat memperkuat perlindungan server tanpa mengurangi fleksibilitas pengelolaannya.

Salah satu metode yang dapat digunakan adalah port knocking. Metode ini memungkinkan administrator untuk menyembunyikan port-port penting dari akses langsung. Dengan menggunakan pola atau urutan tertentu untuk membuka port, hanya pengguna yang mengetahui kombinasi yang benar yang dapat mengakses server. Port knocking tidak hanya menyulitkan serangan otomatis tetapi juga memberikan lapisan keamanan tambahan yang melindungi server dari upaya brute force. Selain itu, implementasi Intrusion Detection System (IDS) sangat penting untuk mendeteksi aktivitas mencurigakan atau berbahaya dalam jaringan. IDS dapat memberikan peringatan dini kepada administrator tentang potensi serangan sebelum serangan tersebut berhasil mengeksploitasi sistem. Dengan memonitor

lalu lintas jaringan secara real-time, IDS membantu mencegah serangan dengan memberikan wawasan mendalam tentang aktivitas yang terjadi di dalam jaringan.

Ubuntu Server, sebagai salah satu platform server yang populer, menyediakan dukungan yang luas untuk implementasi port knocking dan IDS. Dengan alat-alat seperti Knockd untuk port knocking dan Snort atau Suricata untuk IDS, administrator dapat dengan mudah mengkonfigurasi langkah-langkah keamanan ini. Kombinasi dari kedua metode ini tidak hanya meningkatkan keamanan tetapi juga memastikan bahwa server tetap efisien dan fleksibel untuk dikelola. Dengan latar belakang tantangan keamanan yang semakin kompleks, implementasi port knocking dan IDS pada web server berbasis Ubuntu menjadi langkah strategis untuk mengamankan infrastruktur IT. Dengan pendekatan yang tepat, administrator dapat memastikan bahwa server tidak hanya terlindungi dari berbagai ancaman tetapi juga tetap dapat diakses dan dikelola secara efisien.

1.2 Rumusan Masalah

Berdasar latar belakang masalah seperti di 1.1, beberapa rumusan masalah sebagai berikut :

1. Bagaimana meningkatkan keamanan akses terhadap *server Ubuntu* yang dikelola dari jarak jauh menggunakan metode *port knocking*?
2. Bagaimana peran IDS pada *server Ubuntu* untuk mendeteksi aktivitas mencurigakan?
3. Bagaimana memastikan bahwa implementasi *port knocking* dan IDS tidak mengganggu kinerja dan operasional normal dari *server Ubuntu*?

1.3 Batasan Masalah

Berikut adalah beberapa Batasan masalah berdasar latar belakang pada 1.1:

1. Penelitian ini hanya akan mengkaji implementasi *port knocking* dan IDS pada *Ubuntu server* versi 24.04 LTS
2. Penelitian ini terbatas pada penggunaan metode *port knocking* sebagai mekanisme autentikasi untuk membuka akses ke *server*.
3. Penelitian ini terbatas pada penggunaan IDS yang menggunakan *tools PortSentry*
4. Tipe *server* yang dilakukan implementasi adalah *web server*
5. *Port knocking* terbatas pada pembatasan port 22 dan 80

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah untuk menganalisis efektivitas port knocking dalam meningkatkan keamanan akses ke *server Ubuntu* dan IDS *port sentry* dalam mendeteksi aktivitas mencurigakan. Penelitian juga bertujuan mengidentifikasi tantangan dalam mengintegrasikan *port knocking* dan IDS.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah memberikan solusi untuk meningkatkan keamanan akses jarak jauh ke *server Ubuntu* melalui implementasi *port knocking* dan IDS. Penelitian ini akan menghasilkan panduan praktis bagi *administrator* dalam mengkonfigurasi dan mengelola mekanisme keamanan tersebut, sehingga mempermudah penerapan langkah-langkah yang efektif. Implementasi IDS akan membantu mendeteksi dan merespons ancaman lebih cepat, mencegah kerusakan atau kebocoran data yang lebih parah. Evaluasi dampak *port knocking* dan IDS terhadap kinerja *server* akan membantu menemukan keseimbangan antara keamanan dan performa, memastikan operasional *server* tetap optimal. Identifikasi tantangan integrasi memberikan wawasan untuk pengembangan solusi yang lebih efisien, menambah pengetahuan di bidang keamanan IT, dan meningkatkan efisiensi manajemen *server*.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN, berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA, berisi studi literatur, dan dasar-dasar teori yang digunakan.

BAB III METODE PENELITIAN, terdapat tinjauan umum tentang objek penelitian, alur penelitian, serta alat dan bahan.

BAB IV HASIL DAN PEMBAHASAN bab ini merupakan tahapan yang penulis lakukan dalam mengembangkan aplikasi, testing hingga penerapan aplikasi di objek penelitian.

BAB V PENUTUP, berisi kesimpulan dan saran yang dapat peneliti rangkum selama proses penelitian.