BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era meningkatnya urgensi pemanfaatan jaringan komputer, terutama di konteks pendidikan dan dunia profesional, menandakan perlunya penekanan khusus pada aspek keamanan jaringan. Pengelolaan jaringan yang efektif membutuhkan pemahaman mendalam terhadap kompleksitas keamanan, terutama mengingat intensitas akses yang semakin meluas[1]. Hal ini membuka pintu lebar terhadap potensi risiko kejahatan yang dapat terjadi dalam jaringan tersebut.

Terdapat beberapa jenis kejahatan jaringan berupa cracking, spoofing dan serangan DDoS Adapun cara atau metode yang dapat diterapkan untuk mereduksi tingkat kejahatan dalam jaringan.

Salah satu teknik yang sering digunakan dalam melindungi jaringan lokal adalah melalui implementasi sistem keamanan firewall security port. Penggunaan firewall security port karena dapat membantu mengidentifikasi lalu lintas yang mencurigakan dan memblokirnya serta meningkatkan keamanan jaringan dengan cara memblokir mac address dan ip address device yang asing. Berdasarkan [2] Firewall security port merupakan suatu teknologi yang memungkinkan hanya pengguna yang memiliki otoritas untuk mengakses jaringan melalui port yang telah ditetapkan pada perangkat router dan switch. Oleh karena itu, fokus dalam penelitian ini adalah penerapan firewall security port guna meningkatkan keamanan pada jaringan.

Penentuan jenis firewall memiliki dampak signifikan pada integritas sistem keamanan jaringan. Karena untuk memahami konteks lalu lintas jaringan dan memutuskan diizinkan atau tidak suatu paket dan memberikan tingkat keamanan lebih tinggi, Dalam penelitian ini menggunakan metode NDLC. Tahap yang dilakukan adalah melakukan Analisis kebutuhan dan analisis permasalahan lalu Pembuatan Design jaringan IP Adress dan topologi jaringan interkoneksi yang akan dibangun setelah itu Melakukan Simulasi menggunakan Cisco Packet Tracer untuk

melihat kinerja jaringan sebelum dilakukan Implementasi menggunakan GNS3. Sticky port security merupakan keamanan jaringan yang secara otomatis dapat memblokir mac address yang tidak terdaftar, serta di kombinasikan dengan firewall bertujuan untuk meningkatkan efisiensi manajemen sistem keamanan jaringan, sekaligus mencegah akses yang tidak sah.

1.2 Rumusan Masalah

1. Bagaimana Firewall security port dalam mencegah akses yang tidak sah pada jaringan VLAN?
2. Bagiamana pengujian firewall security port menggunakan Hping3 dan macof?

1.3 Batasan Masalah

1. Firewall security port akan diterapkan di dalam VLAN.
2. Metode yang dianalisis mencakup ACLS & Sticky port security

1.4 Tujuan Penelitian

Unjuk kerja dari Firewall security port.

1.5 Manfaat Penelitian

1. Sebagai alternatif pilihan untuk sistem keamanan jaringan.
2. Sebagai materi pembelajaran dalam konteks keamanan jaringan.
3. Sebagai rekomendasi dalam pemilihan metode keamanan jaringan.

1.6 Metode Penelitian

Peneliti menggunakan metode penelitian NDLC. NDLC ialah merupakan sebuah metode yang dapat diterapkan dalam proses pengembangan suatu infrastruktur jaringan computer serta untuk melakukan pengujian terhadap suatu permasalahan dengan menerapkan teori tertentu guna memperoleh hasil pengujian yang sesuai antara permasalahan yang diangkat dan teori yang diterapkan.

1.7 Sistematika Penulisan

BAB I PENDAHULUAN

Membahas tentang latar belakang, rumusan masalah, Batasan masalah, tujuan penelitian, manfaat penelitian, dan metode penelitian yang disesuaikan dengan judul penelitian.

BAB II LANDASAN TEORI

Dalam Bab II ini menjelaskan mengenai studi literatur dan dasar teori dari penelitian yang dilakukan.

BAB III METODE PENELITIAN

Berisi tentang perlengkapan prosedur penelitian mulai dari bahan, alat, alur penelitian.

BAB IV HASIL DAN PEMBAHASAN

Membahas tentang hasil akhir dan pengujian serta pembahasan.

BAB V PENUTUP

Berisi kesimpulan dan saran dari penelitian yang sudah dilakukan.