BAB I PENDAHULUAN

1.1. Latar Belakang Masalah

Pengguna Keamanan jaringan merupakan isu kritis dalam pengelolaan jaringan komputer. Jaringan yang tidak aman dapat rentan terhadap serangan yang dapat mengakibatkan kerusakan pada integritas dan kerahasiaan data yang ada di dalamnya. Protokol routing OSPF (Open Shortest Path First) merupakan protocol routing yang digunakan untuk menghubungkan router-router yang berada dalam satu Autonomous System (AS), sehingga protocol routing ini termasuk juga kategori Interior Gateway Protocol [2]. Namun, OSPF memiliki potensi kerentanan yang dapat dimanfaatkan oleh pihak yang tidak berwenang untuk mengakses atau merusak data jaringan. Salah satu cara untuk meningkatkan keamanan OSPF adalah dengan menggunakan mekanisme autentikasi yang dapat memastikan bahwa pesan OSPF yang dikirim dan diterima adalah dari sumber yang sah dan tidak dimanipulasi oleh pihak yang tidak berwenang. Terdapat beberapa metode autentikasi yang dapat diterapkan pada OSPF, seperti none, simple, dan MD5. Namun, metode autentikasi yang diterapkan dalam OSPF memiliki berbagai tingkat efektivitas dalam menghadapi ancaman keamanan. Metode autentikasi "None" tidak menawarkan perlindungan sama sekali, memungkinkan semua pesan routing diterima tanpa verifikasi, sehingga sangat rentan terhadap serangan. Di sisi lain, metode autentikasi "Simple" memberikan perlindungan dasar dengan akurasi deteksi serangan mencapai 80%. Meskipun demikian, metode ini masih memiliki kelemahan signifikan, yaitu beberapa serangan dapat lolos dari deteksi dan beberapa aktivitas normal dapat terdeteksi salah sebagai serangan.

Penelitian lebih lanjut menunjukkan bahwa penggunaan metode autentikasi MD5 pada OSPF memberikan tingkat keamanan yang lebih tinggi dibandingkan dengan metode none maupun simple. Metode autentikasi MD5 memiliki akurasi deteksi serangan yang mencapai 92.5%, serta presisi dan

recall masing-masing sebesar 94%. Hal ini menjadikannya metode yang sangat efektif dalam mendeteksi dan mencegah serangan, memberikan perlindungan yang lebih optimal bagi jaringan yang menggunakan OSPF. Dengan latar belakang tersebut, penelitian ini bertujuan untuk mengevaluasi efektivitas metode autentikasi yang berbeda dalam OSPF, khususnya dalam menghadapi ancaman keamanan yang semakin kompleks dan canggih. Penelitian ini diharapkan dapat memberikan wawasan yang lebih mendalam mengenai pentingnya pemilihan metode autentikasi yang tepat untuk meningkatkan keamanan jaringan dan mengurangi risiko penyusupan serta manipulasi data.

1.2. Rumusan Masalah

Penerapan Autentikasi pada OSPF merupakan salah satu solusi yang dapat diterapkan dalam mengamankan suatau link pada router OSPF didalam jaringan

Berdasarkan hal di atas, maka dapat dirumuskan masalahnya sebagai berikut :

1. Bagaimana cara mengimplementasikan autentikasi pada protokol routing OSPF (Open Shortest Path First) dengan menggunakan metode autentikasi None, Simple, dan MD5.
2. Apa perbedaan antara ketiga metode autentikasi OSPF (None, Simple, dan MD5) dalam hal efektivitas dan efisiensi dalam meningkatkan keamanan jaringan.
3. Bagaimana efektivitas metode autentikasi MD5 dibandingkan dengan metode none dan simple dalam hal tingkat keamanan pada protokol OSPF?.
4. Apakah terdapat potensi kelemahan atau kerentanan pada implementasi masing-masing metode autentikasi OSPF (None, Simple, dan MD5) dalam melindungi keamanan jaringan, dan bagaimana mengidentifikasinya
5. Seberapa besar akurasi, presisi, dan recall metode autentikasi simple dalam mendeteksi dan mencegah serangan pada OSPF?.

1.3. Batasan Masalah

Batasan masalah dari penelitian ini adalah

1. Penelitian ini dilakukan secara studi kasus dengan menggunakan jaringan dan pengujian pada PT. Integrasi Data Nusantara Cabang Semarang (ID-Networkers Semarang).
2. Penelitian menggunakan router berbasis MikroTik RouterBOARD.
3. Penelitian ini akan difokuskan pada autentikasi pada OSPF (Open dengan menerapkan metode autentikasi None, Simple, dan MD5.
4. Penelitian ini tidak akan membahas aspek lain dari keamanan jaringan, seperti enkripsi data, proteksi terhadap serangan lainnya selain serangan terhadap autentikasi OSPF, atau analisis kebijakan keamanan yang lebih luas.
5. Penelitian ini akan dilakukan dengan memperhatikan standar dan pedoman yang berlaku dalam penggunaan autentikasi OSPF, namun tidak akan membahas pengembangan protokol OSPF baru atau modifikasi protokol OSPF yang ada

1.4 Tujuan

Penelitian ini bertujuan untuk mengevaluasi, mengimplementasikan, dan menganalisis efektivitas metode autentikasi none, simple, dan MD5 pada protokol OSPF. Penelitian ini akan mengukur akurasi, presisi, dan recall dari masing-masing metode dalam mendeteksi dan mencegah serangan, mengidentifikasi kelemahan metode simple, serta menentukan keunggulan metode MD5. Selain itu, penelitian ini akan memberikan rekomendasi untuk penerapan autentikasi OSPF yang lebih aman dan efisien guna melindungi jaringan komputer.

1.5 Manfaat

Penelitian ini diharapkan meningkatkan keamanan jaringan OSPF dengan mengevaluasi efektivitas metode autentikasi none, simple, dan MD5. Hasilnya akan menyediakan rekomendasi praktis untuk penerapan autentikasi yang lebih aman dan efisien, serta membantu memahami kelemahan metode simple dan keunggulan metode MD5. Selain itu, penelitian ini akan menjadi dasar yang kuat untuk penelitian lanjutan dalam bidang keamanan jaringan, khususnya autentikasi protokol routing.