BAB V HASIL DAN PEMBAHASAN

5.1. Visualisasi Data

Hasil pengujian metode autentikasi OSPF yang dilakukan terhadap metode none, simple, dan MD5 menunjukkan perbandingan yang signifikan dalam hal efektivitas dalam mendeteksi dan mencegah serangan.

Tabel 4.5 – Perbandingan Metode

Metode Autentikasi	Akurasi (%)	Presisi (%)	Recall (%)	Kelamahan
None	0%	0%	0%	Tidak ada Autentikasi, sehingga rentan terhadap serangan dan manipulasi data
Simple	80%	75%	75%	Rentan terhadap beberapa serangan yang lolos deteksi dan beberapa aktivitas normal terdeteksi salah.
MD5	92,5%	94%	95%	Menyediakan perlindungan terbaik dengan deteksi serangan yang tinggi dan minim false positive

Pengujian menunjukkan bahwa penggunaan metode autentikasi MD5 pada OSPF secara konsisten memberikan hasil yang lebih baik dibandingkan dengan metode none dan simple. Metode autentikasi MD5 mencapai akurasi sebesar 92.5%, dengan presisi dan recall masing-masing mencapai 94%. Hal ini mengindikasikan bahwa metode MD5 efektif dalam mendeteksi dan mencegah serangan terhadap protokol OSPF, dengan kemampuan yang lebih tinggi dalam mengenali aktivitas yang mencurigakan tanpa menghasilkan banyak false positive.

5.2. Pemilihan Autentikasi

Metode autentikasi none tidak menyediakan perlindungan autentikasi sama sekali, sehingga rentan terhadap serangan dan manipulasi data yang tidak diinginkan. Sementara itu, metode autentikasi simple meskipun memberikan perlindungan dasar dengan akurasi 80%, namun masih memiliki kelemahan dalam mendeteksi beberapa serangan dan membingungkan beberapa aktivitas normal sebagai serangan. Hasil pengujian ini memberikan implikasi praktis bagi administrator jaringan untuk mempertimbangkan penggunaan metode autentikasi MD5 sebagai standar keamanan yang lebih efektif dalam implementasi OSPF. Rekomendasi praktis dari penelitian ini adalah untuk mengadopsi metode autentikasi MD5 untuk meningkatkan keamanan jaringan, dengan meminimalkan risiko serangan dan manipulasi data yang mungkin terjadi.

Berdasarkan hasil pengujian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa metode autentikasi MD5 pada OSPF memberikan perlindungan yang lebih baik dibandingkan dengan metode autentikasi none dan simple. Implementasi metode autentikasi MD5 secara signifikan meningkatkan kemampuan dalam mendeteksi dan mencegah serangan terhadap protokol OSPF, sehingga direkomendasikan sebagai pilihan yang optimal untuk meningkatkan keamanan jaringan.

BAB VI KESIMPULAN DAN SARAN

6.1. Kesimpulan

Penelitian Studi ini telah menguji dan membandingkan efektivitas metode autentikasi none, simple, dan MD5 pada protokol OSPF. Hasil pengujian menunjukkan bahwa metode autentikasi MD5 memberikan tingkat keamanan yang lebih tinggi dengan akurasi mencapai 92.5%, presisi 94%, dan recall 94%. Metode ini secara konsisten lebih efektif dalam mendeteksi dan mencegah serangan dibandingkan dengan metode autentikasi none dan simple. Metode autentikasi none tidak memberikan perlindungan autentikasi sama sekali, sementara metode simple, meskipun memberikan perlindungan dasar, masih rentan terhadap beberapa serangan dan kesalahan deteksi.

6.2. Saran

Penelitian ini berfokus pada pengujian dan perbandingan beberapa model Autentikasi yang dipakai di jaringan OSPF. Saran untuk mendukung penelitian ke depan yaitu kolaborasi dengan seorang ahli dalam bidang keamanan jaringan sehingga dapat dilakukan berbagai jenis implementasi serangan untuk mencari atau mengetes keamanan pada tiap Autentikasi di OSPF agar dapat digunakan sesuai dengan kebutuhan. Berikut adalah beberapa rekomendasi:

1. Implementasi metode autentikasi MD5: Disarankan untuk mengadopsi metode autentikasi MD5 sebagai standar keamanan pada implementasi OSPF. Metode ini telah terbukti efektif dalam mendeteksi serangan dan memberikan perlindungan yang lebih optimal terhadap manipulasi data.
2. Peningkatan kesadaran dan pelatihan: Penting bagi administrator jaringan untuk meningkatkan kesadaran dan pengetahuan mengenai keamanan jaringan serta penggunaan metode autentikasi yang tepat. Pelatihan rutin mengenai implementasi dan manajemen keamanan

jaringan dapat membantu dalam mengurangi risiko serangan.

3. Penelitian lanjutan: penelitian ini berfokus pada Mikrotik RouterOS versi 6 dengan tipe Autentikasi yang jadul. Penelitian selanjutnya sebaiknya dilakukan pada RouterOS versi 7 yang menawarkan opsi Autentikasi yang lebih aman seperti SHA1, SHA256, SHA384 dan SHA512.
4. Monitoring dan evaluasi berkala: Selain mengimplementasikan metode autentikasi yang tepat, penting untuk melakukan pemantauan dan evaluasi rutin terhadap keamanan jaringan. Hal ini akan membantu dalam mengidentifikasi dan merespons secara cepat terhadap potensi ancaman yang baru muncul.

Dengan mengikuti saran-saran di atas, diharapkan dapat meningkatkan keamanan jaringan dan mengurangi risiko yang terkait dengan manipulasi dan serangan terhadap protokol OSPF.