BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil perancangan, implementasi, serta pengujian sistem keamanan jaringan menggunakan IDS, IPS, dan ARP List pada Mikrotik RouterOS, dapat diambil beberapa kesimpulan sebagai berikut:

1. **Sistem IDS pada Mikrotik RouterOS mampu mendeteksi serangan brute force dengan akurasi yang cukup tinggi.**

   Hasil pengujian menunjukkan nilai True Positive Rate (TPR) sebesar 90%, yang berarti IDS dapat mengenali mayoritas aktivitas login mencurigakan berdasarkan pola koneksi berulang. Meskipun tidak sekompleks Snort atau Suricata, IDS bawaan Mikrotik cukup efektif untuk jaringan berskala kecil.

2. **IPS berhasil memberikan perlindungan aktif terhadap brute force attack dengan waktu respons yang cepat.**

   Dari hasil pengukuran, rata-rata waktu pemblokiran setelah deteksi adalah 3,9 detik, menunjukkan bahwa integrasi IDS dan IPS mampu menghentikan serangan secara real-time tanpa keterlibatan manual oleh administrator.

3. Berdasarkan hasil pengujian, sistem IDS/IPS yang diimplementasikan pada Mikrotik RouterOS mampu mendeteksi 90% serangan brute force dengan rata-rata waktu pemblokiran 3,9 detik. Tingkat akurasi sistem mencapai 90% dengan nilai precision sebesar 94,7%.

   Meskipun demikian, terdapat tingkat false positive sebesar 10%, yang menunjukkan bahwa terdapat percobaan login normal yang salah dikenali sebagai serangan. Hal ini dapat disebabkan oleh konfigurasi aturan yang terlalu ketat atau batasan threshold percobaan login yang rendah. Untuk mengurangi false positive, diperlukan penyesuaian (tuning) pada aturan dan parameter IDS.

   Secara keseluruhan, sistem IDS/IPS Mikrotik RouterOS terbukti cukup andal dalam mendeteksi dan memblokir serangan brute force

pada jaringan lokal skala kecil. Namun, perbaikan konfigurasi dan pengujian lanjutan pada kondisi jaringan yang lebih kompleks masih diperlukan untuk meningkatkan performa dan reliabilitas sistem.

4. **Implementasi ARP List terbukti sangat efektif dalam membatasi akses perangkat.**

   Dengan mode reply-only, router hanya merespons perangkat yang alamat IP dan MAC-nya telah terdaftar. Hal ini membuat perangkat asing ditolak bahkan sebelum proses autentikasi, sehingga brute force tidak dapat dilakukan oleh perangkat yang tidak dikenal. Waktu penolakan rata-rata melalui ARP List tercatat kurang dari 4 detik..

5.2 Saran

Berdasarkan pengalaman dan keterbatasan dalam penelitian ini, beberapa saran yang dapat diberikan untuk pengembangan lebih lanjut adalah:

1. Optimalisasi Konfigurasi IDS/IPS

   Perlu dilakukan tuning lebih lanjut terhadap aturan dan parameter IDS agar tingkat false positive dapat diminimalisasi tanpa mengurangi efektivitas deteksi serangan.

2. Pengujian pada Skala Jaringan Lebih Besar

   Penelitian ini dilakukan pada jaringan lokal skala rumah/UKM. Implementasi pada jaringan dengan jumlah pengguna lebih banyak dan lalu lintas lebih kompleks dapat memberikan gambaran yang lebih komprehensif mengenai performa sistem.

3. Integrasi dengan Sistem Monitoring Eksternal

   Penggunaan remote syslog server atau SIEM (Security Information and Event Management) dapat memperkuat proses pemantauan, analisis, dan forensik keamanan jaringan.

4. Pengembangan Lapisan Keamanan Tambahan

   Selain IDS, IPS, dan ARP List, sistem keamanan dapat ditingkatkan dengan enkripsi komunikasi, autentikasi berbasis sertifikat, serta integrasi dengan VPN untuk mengurangi risiko eksploitasi.

5. Perluasan Jenis Serangan yang Diuji

   Penelitian selanjutnya diharapkan tidak hanya berfokus pada serangan brute force, tetapi juga mencakup serangan lain seperti port scanning, man-in-the-middle attack, atau distributed denial of service (DDoS) agar hasil penelitian lebih komprehensif.