BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan komputer merupakan salah satu aspek penting dalam pemanfaatan sistem informasi. Celah keamanan *(vulnerability)* yang tidak ditangani dengan baik dapat dimanfaatkan oleh pihak tidak bertanggung jawab melalui serangan logis maupun fisik yang berpotensi merusak sistem [1][2]. Salah satu bentuk ancaman yang sering terjadi adalah *brute force attack*, yaitu upaya mendapatkan akses ilegal dengan mencoba berbagai kombinasi kata sandi hingga menemukan yang benar. Serangan ini dapat menyebabkan kebocoran data, gangguan layanan, dan kerusakan infrastruktur apabila tidak ditangani dengan tepat [2].

Upaya pengamanan jaringan dapat dilakukan menggunakan berbagai mekanisme seperti *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS), serta mekanisme keamanan tambahan seperti *Address Resolution Protocol* (ARP) *List*. Penelitian sebelumnya telah menunjukkan efektivitas mekanisme tersebut. Wahyudi dkk. (2020) membuktikan bahwa Mikrotik mampu memblokir akses tidak sah dan mengatur lalu lintas jaringan skala LAN [3]. Sementara itu, Sari dan Nugroho (2021) menunjukkan bahwa IDS berbasis Snort mampu mendeteksi serangan *brute force* secara signifikan [4].

Penelitian lain oleh Nugraha (2019) menunjukkan bahwa kombinasi dan IDS mampu memberikan perlindungan berlapis pada jaringan perkantoran [5]. Namun, sebagian besar penelitian terdahulu masih mengandalkan perangkat lunak pihak ketiga seperti Snort atau Suricata [6][7]. Padahal, Mikrotik RouterOS sendiri memiliki fitur internal IDS dan IPS yang lebih ringan serta efisien dari sisi perangkat keras maupun biaya [8].

Selain itu, penelitian Hadiyansyah (2022) mengkaji performa rule-based Mikrotik yang terbukti stabil dalam melakukan filtering trafik [9], sedangkan Prasetyo & Widodo (2021) mengembangkan deteksi serangan dengan script

Mikrotik [10]. Lebih lanjut, Lestari & Firmansyah (2023) menyoroti efektivitas IDS open source dalam mengenali pola serangan berulang [11]. Namun, penelitian yang memanfaatkan fitur bawaan IDS/IPS Mikrotik secara mendalam masih sangat terbatas.

Dari berbagai studi tersebut dapat disimpulkan bahwa masih terdapat celah penelitian, khususnya dalam memaksimalkan fitur internal Mikrotik RouterOS, baik melalui IDS, IPS, maupun ARP List, untuk menghadapi ancaman *brute force*. Dengan menggabungkan mekanisme-mekanisme tersebut, diharapkan dapat tercipta sistem keamanan jaringan yang lebih komprehensif, cepat, dan efisien dalam mencegah akses ilegal ke dalam jaringan.

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada perancangan sistem keamanan jaringan menggunakan IDS dan IPS bawaan Mikrotik RouterOS serta implementasi ARP List untuk menangkal serangan *brute force*, sehingga diharapkan mampu menjadi solusi praktis bagi administrator jaringan dalam menjaga stabilitas dan keamanan sistem.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan, maka rumusan masalah dalam penelitian ini adalah:

1. Apakah sistem keamanan jaringan menggunakan IDS Mikrotik RouterOS untuk mampu mendeteksi penyusupan jaringan?
2. Apakah sistem keamanan jaringan menggunakan IPS pada Mikrotik RouterOS mampu untuk menangkal serangan *brute force*?
3. Apakah implementasi ARP List pada Mikrotik RouterOS dapat membatasi akses login router hanya untuk perangkat yang telah terdaftar?

1.3 Batasan Masalah

Agar penelitian ini lebih fokus dan terarah, maka batasan masalah yang ditetapkan adalah:

1. Penelitian ini hanya menggunakan perangkat Mikrotik RouterOS sebagai media konfigurasi *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS), dan ARP List, sehingga tidak membahas perangkat lain seperti Cisco, pfSense, atau Fortinet.
2. Jenis serangan yang diuji dibatasi pada serangan brute force terkontrol menggunakan THC-Hydra, sehingga tidak mencakup bentuk serangan lain seperti *port scanning*, *man-in-the-middle*, *SQL injection*, maupun *distributed denial of service* (DDoS).
3. Implementasi dan pengujian sistem keamanan dilakukan hanya pada jaringan lokal (LAN) skala rumah atau UKM, dan tidak mencakup jaringan skala besar seperti jaringan korporasi atau ISP.
4. Evaluasi efektivitas sistem keamanan hanya dilakukan melalui pencatatan log dan pemantauan lalu lintas jaringan secara real-time, tanpa melibatkan metode uji beban (*stress test*) atau *traffic generator* berskala besar.
5. Penerapan ARP List pada penelitian ini difokuskan pada pembatasan akses login router hanya untuk perangkat yang telah terdaftar secara manual, sehingga tidak membahas otomatisasi manajemen ARP List dengan server autentikasi atau sistem *eksternal* lainnya.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Mengimplementasikan IDS dan IPS pada Mikrotik RouterOS agar bisa mendeteksi lalu menangkal aktivitas penyusupan.
2. Mengimplementasikan ARP List pada Mikrotik RouterOS untuk membatasi akses login router hanya pada perangkat yang telah terdaftar.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini dapat dibagi menjadi dua aspek, yaitu:

a) Secara Teoritis:

- Menambah referensi ilmiah mengenai implementasi ARP List, IDS dan IPS menggunakan Mikrotik RouterOS.
- Memberikan wawasan mengenai keamanan jaringan komputer dan metode mitigasi serangan siber.
- Memberikan gambaran tentang fungsi ARP List dalam mendukung sistem keamanan jaringan selain IDS, dan IPS.

b) Secara Praktis:

- Memberikan solusi praktis bagi adminisator jaringan dalam mengamankan sistem dari serangan *brute force*.
- Menjadi acuan dalam membangun sistem deteksi dan pencegahan intrusi pada jaringan lokal skala kecil hingga menengah.
- Menjadi acuan bagi administrator jaringan dalam menggunakan ARP List sebagai lapisan keamanan tambahan untuk mencegah akses ilegal ke router.

1.6 Tolak Ukur Penelitian

Tolak ukur penelitian ini ditetapkan untuk menilai keberhasilan implementasi IDS, IPS, dan ARP List pada Mikrotik RouterOS dalam mencegah serangan *brute force*. Adapun indikator keberhasilan penelitian adalah sebagai berikut:

1. Kemampuan IDS dalam mendeteksi serangan *brute force*, dengan tingkat keberhasilan minimal 90% berdasarkan jumlah deteksi yang tercatat pada log RouterOS.
2. Kemampuan IPS dalam memblokir sumber serangan secara otomatis, dengan waktu respon pemblokiran kurang dari 5 detik setelah IDS mendeteksi percobaan login berulang.

3. Efektivitas ARP List dalam membatasi akses login ke router, ditandai dengan keberhasilan menolak 100% perangkat yang tidak terdaftar dalam ARP statis.
4. Tingkat akurasi sistem keamanan, dengan target akurasi keseluruhan minimal 90% dan nilai precision lebih dari 90% berdasarkan hasil pengujian berulang.
5. Tingkat false positive yang rendah, yaitu tidak lebih dari 10% dari seluruh percobaan akses normal yang diuji.

Tolak ukur ini digunakan untuk menilai apakah konfigurasi IDS, IPS, dan ARP List pada Mikrotik RouterOS telah efektif dan sesuai dengan tujuan penelitian dalam mencegah serangan *brute force* pada jaringan lokal.

1.7 Sistematika Penulisan

Sistematika penulisan laporan penelitian ini adalah sebagai berikut:

- BAB I PENDAHULUAN, berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.
- BAB II TINJAUAN PUSTAKA, membahas landasan teori yang relevan dengan topik penelitian, termasuk konsep dasar keamanan jaringan, IDS, Mikrotik RouterOS, dan serangan *brute force*.
- BAB III METODE PENELITIAN, menjelaskan metode yang digunakan dalam penelitian, objek penelitian, teknik pengumpulan data, perancangan sistem, dan implementasi konfigurasi pada Mikrotik RouterOS.
- BAB IV HASIL DAN PEMBAHASAN, berisi hasil implementasi sistem IPS dan IDS, analisis efektivitas sistem, serta pembahasan terhadap hasil pengujian.
- BAB V PENUTUP, berisi kesimpulan dari hasil penelitian dan saran untuk pengembangan lebih lanjut atau implementasi nyata.