BAB I
PENDAHULUAN

A. Latar Belakang

Dalam era digital yang terus berkembang pesat, keamanan jaringan menjadi prioritas utama bagi organisasi dan individu yang mengandalkan konektivitas untuk berbagai keperluan, terutama pada jaringan dengan kategori jaringan lokal [1]. Salah satunya dengan memanfaatkan pembentukan jaringan LAN, WLAN, hingga WAN dengan skema yang didukung oleh perangkat router sebagai peran sentral dalam mengamankan aliran data yang melintasinya, terutama router pada kategori *low-cost*, atau level konsumer [1], [2].

Router level konsumer hasil manufaktur MikroTik yang berbasis sistem operasi RouterOS dan arsitektur MIPS mendominasi infrastruktur jaringan di berbagai skala, mulai dari pengguna rumahan, sekolah, hingga instansi-instansi yang menghubungkan ribuan sistem jaringan [2]. Popularitas ini didorong oleh biaya rendah dan fleksibilitas konfigurasi, namun diikuti oleh risiko keamanan yang signifikan akibat kesamaan arsitektur antara pengguna dan ketergantungan pada konfigurasi *default*, terbukti dengan kerentanan CVE-2018-14847 yang menyerang router pada level ini [2]. Analisis global terhadap penggunaan perangkat MikroTik menunjukkan bahwa lebih dari 4 juta perangkat terpapar di internet, dengan mayoritas berlokasi di negara berkembang yang mengutamakan efisiensi biaya dalam pembangunan infrastruktur jaringan [3]. Fakta ini menjadikan perangkat tersebut target ideal bagi para pembobol, terutama karena layanan manajemen seperti Winbox (*port* 8291), SSH (22), dan API (8728) umumnya aktif secara default dan jarang dikonfigurasi ulang oleh pengguna [2], [3].

Serangan terhadap perangkat MikroTik tercatat berskala besar dan berkelanjutan hingga saat ini [4], [5]. Dalam studi *honeypot* selama 45 hari, tercatat lebih dari 17 juta paket serangan dan 1,5 juta catatan log dari 399.235 alamat IP unik, dengan 200.000 di antaranya melakukan *brute force* terhadap layanan manajemen [5]. Sebanyak 85% dari serangan *brute force* tersebut menggunakan *signature* botnet Mirai, yang secara khusus menargetkan kredensial lemah pada perangkat IoT dan router [5].

Kerentanan ini juga diperparah oleh praktik pemeliharaan yang buruk [3], [4]. Lebih dari dua juta perangkat diperkirakan masih rentan terhadap *Common Vulnerabilities and Exposures* (CVE) karena penggunaan versi RouterOS yang usang, meskipun vendor telah merilis puluhan pembaruan keamanan [3]. Fakta bahwa vendor router konsumen kerap mengalihdayakan pengembangan *firmware* dan kesulitan mendorong pengguna untuk memperbarui perangkat memperluas ruang lingkup eksploitasi pada perangkat ini [4], [5]. Hal ini menciptakan kondisi di mana ancaman dengan standar lama tetap efektif, seperti yang ditunjukkan oleh temuan bahwa 17 kerentanan yang diungkap lebih dari satu dekade lalu masih aktif digunakan dalam serangan modern [4].

Indonesia menghadapi eskalasi ancaman siber yang bersifat masif dan berkelanjutan. Badan Siber dan Sandi Negara (BSSN) mencatat 3,64 miliar serangan siber atau anomali lalu lintas hanya dalam rentang Januari hingga Juli 2025, dengan angka yang hampir menyamai total serangan selama lima tahun sebelumnya [7]. Mayoritas serangan tersebut berbasis *malware* (83,68%), sedangkan akses tidak sah (*unauthorized access*) dan eksploitasi sistem menyumbang 4,32% dan 0,64% secara berurutan. Data ini menegaskan bahwa ancaman keamanan jaringan bukan lagi potensi, melainkan realitas operasional yang memengaruhi infrastruktur digital nasional. Namun, respons terhadap ancaman ini terhambat oleh rendahnya literasi keamanan digital di masyarakat dan institusi, sehingga banyak sistem tetap rentan meskipun regulasi seperti UU PDP dan UU ITE telah diberlakukan [8].

Kerentanan ini diperparah oleh praktik konfigurasi dan pemeliharaan perangkat jaringan yang tidak memadai, terutama pada router berbiaya rendah seperti MikroTik yang dominan di jaringan pribadi, lingkungan pendidikan, UMKM, dan pemerintahan daerah [9] [10]. Studi di berbagai institusi akademik Indonesia menunjukkan bahwa router MikroTik kerap dibiarkan dalam konfigurasi default, dengan layanan manajemen seperti WinBox (*port* 8291), SSH (22), dan API (8728) tetap aktif tanpa autentikasi kuat atau proteksi tambahan [10]. Analisis terhadap jaringan di lingkungan Pendidikan, seperti laboratorium komputer perguruan tinggi dan sekolah menengah, mengungkapkan bahwa *port* terbuka, kredensial lemah, dan ketiadaan mekanisme deteksi serangan otomatis, menjadikan

infrastruktur tersebut sasaran ideal bagi *brute force* dan *probing* berkelanjutan [10]. Temuan serupa muncul dalam penelitian regional, di mana *firewall* bawaan MikroTik hanya memberikan mitigasi parsial terhadap serangan DoS, sementara *brute force* terhadap layanan manajemen tetap efektif karena tidak adanya pembatasan percobaan *login* atau penyembunyian *port* [10].

Kesenjangan antara kesadaran ancaman dan implementasi pertahanan teknis menciptakan jendela eksploitasi yang luas. Di satu sisi, penelitian akademik di Indonesia mulai mengadopsi kerangka kerja keamanan seperti NIST CSF untuk mengevaluasi postur jaringan [10]. Namun di sisi lain, keterbatasan sumber daya manusia dan anggaran menghambat penerapan solusi yang komprehensif [9]. Akibatnya, banyak jaringan LAN tetap mengandalkan konfigurasi dasar tanpa lapisan keamanan adaptif [9] [10].

Serangan *brute force* menjadi fokus utama dalam penelitian ini karena secara langsung mengeksploitasi dua kelemahan struktural pada router MikroTik level konsumen, yaitu ketersediaan layanan manajemen yang aktif secara default, seperti WinBox (*port* 8291) dan SSH (*port* 22) dan tidak adanya mekanisme bawaan untuk membatasi percobaan *login* berulang. Router MikroTik rentan terhadap upaya otomatisasi masuk menggunakan kombinasi kredensial umum atau kredensial lemah, yang telah terbukti digunakan secara masif oleh *botnet* seperti Mirai, yang bertanggung jawab atas 85% serangan *brute force* terhadap perangkat MikroTik [5], serta lebih dari 200.000 alamat IP unik secara aktif melakukan *brute force* terhadap layanan manajemen MikroTik dalam rentang waktu hanya 45 hari [11], dan kerentanan ini tetap efektif karena jutaan perangkat masih beroperasi dengan versi RouterOS lama dan konfigurasi default [12] [13].

Meskipun *brute force* menjadi ancaman yang paling terdokumentasi, kelemahan struktural yang sama pada layanan manajemen MikroTik turut membuka celah bagi sejumlah vektor serangan lanjutan yang secara langsung berkaitan dengan siklus hidup sebuah serangan jaringan [13]. Tiga vektor utama, yaitu *reconnaissance*, penyalahgunaan mekanisme *port knocking*, dan *spoofing* pasca-pemblokiran, merupakan tahapan yang secara realistis akan dihadapi oleh sebuah sistem pertahanan jaringan, sehingga pengujian yang hanya berfokus pada *brute force* tidak cukup merepresentasikan ketahanan sistem secara menyeluruh.

Atas dasar ini, penelitian ini memperluas cakupan pengujian ke empat fokus utama yang saling berkaitan, yaitu: (1) ketahanan terhadap *brute force* pada layanan manajemen, (2) ketahanan terhadap *reconnaissance* dan *sniffing* pasca-implementasi *port knocking*, (3) keamanan mekanisme *port knocking* itu sendiri terhadap upaya penyalahgunaan *sequence*, dan (4) ketahanan sistem terhadap IP *spoofing* setelah penyerang diblokir.

Maka dari itu, untuk melindungi jaringan LAN, WLAN, maupun WAN terhadap berbagai vektor serangan tersebut, diperlukan analisis mendalam terhadap kerentanan yang ada serta penerapan metode penanganan yang efektif. Keamanan berbasis *port knocking* dan *scripting* otomatis tidak hanya relevan, tetapi menjadi kebutuhan operasional untuk menutup celah yang tidak terjangkau oleh *firewall* statis atau konfigurasi default semata.

Port knocking sendiri merupakan metode keamanan jaringan yang berfungsi sebagai penyembunyi layanan manajemen router dari akses eksternal dengan memaksa klien melewati rangkaian "ketukan" *port* terenkripsi sebelum akses diberikan, sehingga mencegah penyerang bahkan mendeteksi keberadaan *port* kritis seperti WinBox (8291) atau SSH (22) [14]. Metode ini secara langsung menanggulangi fase awal serangan *brute force*, yaitu *discovery*, karena penyerang tidak dapat mengidentifikasi keberadaan *port* manajemen yang menjadi sasaran eksploitasi [12] [13] [14]. Studi implementasi di lingkungan pendidikan menunjukkan bahwa *port knocking* mampu mencegah akses tidak sah meskipun penyerang mengetahui kredensial valid, karena tanpa menyelesaikan urutan ketukan, koneksi ke router tidak pernah terbentuk [14] [15] [16]. Namun demikian, mekanisme ketukan *port* itu sendiri berpotensi menjadi target baru apabila penyerang mencoba menebak atau membuat *probe* urutan ketukan secara otomatis, sehingga keamanan *port knocking* turut perlu diuji terhadap upaya penyalahgunaan *sequence* tersebut.

Di sisi lain, *scripting* otomatis pada RouterOS memungkinkan deteksi real-time terhadap aktivitas mencurigakan, seperti percobaan login berulang dan meresponsnya melalui pemblokiran IP [17], serta pemberitahuan instan kepada administrator melalui bot Telegram, yang telah terbukti meningkatkan responsivitas dan kesadaran situasional dalam pengelolaan insiden keamanan [18] [19].

Rancangan serupa dapat diperluas untuk mendeteksi pola penyalahgunaan pada urutan ketukan *port*, serta memvalidasi bahwa pemblokiran tetap berlaku meskipun penyerang mengganti alamat IP atau MAC *address* setelah teridentifikasi. Kombinasi keduanya menciptakan lapisan pertahanan dinamis yang menutup celah antara *detection* dan *response*, khususnya dalam lingkungan dengan sumber daya terbatas [17] [18] [19].

Untuk mendukung proses analisis sekaligus pengujian metode keamanan, penelitian ini memanfaatkan dua kerangka metodologis, yaitu *Design Science Research* (DSR) dan NIST SP 800-115. DSR digunakan sebagai pendekatan konstruktif yang menekankan penciptaan solusi melalui siklus berulang antara perancangan model keamanan, evaluasi praktis, dan penyempurnaan berbasis *feedback* [20]. Dalam konteks penelitian ini, DSR berperan dalam merancang, menerapkan, dan menilai model keamanan berupa konfigurasi *port knocking* serta *script* otomatis berbasis *alerting*. Sementara itu, NIST SP 800-115 berfungsi sebagai panduan teknis yang menyediakan standar prosedur pengujian penetrasi secara sistematis, mulai dari tahap pengintaian, pemindaian, eksploitasi, hingga analisis pasca-serangan, sehingga efektivitas desain dapat divalidasi secara objektif dan terukur [21].

Kombinasi keduanya jarang ditemui dalam penelitian keamanan jaringan berbasis MikroTik, di mana sebagian besar studi hanya fokus pada implementasi tanpa evaluasi teknis berbasis standar nasional atau internasional, atau sebaliknya, yang hanya melakukan pengujian tanpa menghasilkan model desain yang dapat direplika. Integrasi DSR dan NIST SP 800-115 memungkinkan penelitian ini tidak hanya menghasilkan solusi yang berfungsi, tetapi juga terverifikasi melalui penggunaan metodologi pengujian yang diakui secara global.

Penelitian ini bertujuan untuk menganalisis serta mengatasi kerentanan keamanan pada jaringan LAN dan WLAN yang menggunakan perangkat router MikroTik, khususnya kategori *low-cost* yang sering dibiarkan dalam konfigurasi default dengan layanan manajemen terbuka, kredensial lemah, dan tanpa mekanisme deteksi serangan [21] [22].

Dengan menggunakan DSR dan NIST SP 800-115 sebagai metode analisis serta pengujian, merupakan langkah strategis dan efisien untuk mengidentifikasi,

menilai, dan mengatasi kerentanan keamanan secara menyeluruh pada jaringan LAN dan WLAN. DSR memastikan solusi yang dibangun bersifat inovatif, terukur, dan berbasis masalah nyata, sementara NIST SP 800-115 menjamin bahwa pengujian terhadap solusi tersebut dilakukan secara sistematis, mencakup seluruh siklus serangan terhadap layanan manajemen MikroTik. Dengan demikian, penerapan kedua metode ini diharapkan dapat memperkuat keamanan jaringan LAN dan WLAN melalui desain yang teruji, efektif, dan siap diadopsi dalam konteks operasional nyata untuk melindungi informasi serta data dari ancaman *brute force*.

B. Perumusan Masalah

Berdasarkan permasalahan yang diuraikan dalam latar belakang, adapun perumusan masalah dalam penelitian ini sebagai berikut:

1. Bagaimana implementasi rancangan keamanan berlapis berbasis *port knocking* dengan enkripsi WireGuard, dan mekanisme deteksi otomatis pada router MikroTik kategori *low-cost* untuk mengamankan layanan manajemen dari ancaman *reconnaissance*, *sniffing*, *brute force,* dan *spoofing* pada jaringan LAN, WLAN, dan WAN?
2. Bagaimana efektivitas mekanisme deteksi penyalahgunaan *knock sequence, knock abuse*, dan IP spoofing pada arsitektur gabungan *port knocking* dan *auto-blocking* terhadap router MikroTik kategori *low-cost* pada jaringan LAN, WLAN, dan WAN?

C. Batasan Penelitian

Adapun batasan masalah yang diterapkan dalam penelitian ini guna mencegah penyimpangan dan menjaga penelitian agar tetap fokus, memudahkan pembahasan, dan konsisten pada tujuan penelitian ialah sebagai berikut:

1. Penelitian mengevaluasi efektivitas rancangan keamanan berlapis berbasis *port knocking*, enkripsi WireGuard, dan mekanisme deteksi otomatis pada router MikroTik sebagai mekanisme pertahanan utama dari ancaman *reconnaissance*, *sniffing*, dan *brute force* pada jaringan LAN, WLAN, dan WAN Topologi jaringan yang digunakan merepresentasikan jaringan LAN, WLAN, dan WAN

dengan konfigurasi menggunakan perangkat *router* MikroTik pada kategori *low-cost.*

2. Seluruh mekanisme pertahanan diimplementasikan secara *native* menggunakan fitur bawaan RouterOS tanpa menggunakan pada perangkat lunak atau perangkat keras keamanan eksternal.
3. Simulasi serangan dilakukan menggunakan dua sistem operasi penyerang (Kali Linux dan Windows) dengan *tools* pengujian standar (Nmap, Hydra, Wireshark, knockd, hping3), mencakup empat skenario ancaman, yaitu *reconnaissance* dan *sniffing*, *brute force*, *knock sequence abuse*, dan *spoofing*.
4. Pengujian sumber WAN dilakukan melalui VPS berbasis Ubuntu 20.04 yang dikonfigurasi sebagai *transparent relay* menggunakan protokol L2TP dan aturan DNAT pada iptables, sehingga alamat IP asli penyerang tetap dipertahankan selama pengujian berlangsung.

D. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah:

1. Merancang dan mengimplementasikan arsitektur keamanan berlapis pada router MikroTik hAP lite yang mencakup *port knocking* dengan enkripsi WireGuard, dan mekanisme deteksi otomtais berbasis *scripting* RouterOS terhadap ancaman *reconnaissance*, *sniffing*, *brute force,* dan *spoofing* pada jaringan LAN, WLAN, dan WAN
2. Menganalisis efektivitas setiap lapisan pertahanan dalam menahan ancaman *reconnaissance*, *sniffing*, *brute force*, *knock sequence abuse*, dan *IP spoofing* dengan metode *port knocking* dalam mencegah serangan *brute force* berdasarkan hasil pengujian penetrasi pada perangkat MikroTik kategori *low-cost*.

E. Manfaat Penelitian

1. Bagi Pembaca

   Penelitian ini menyediakan referensi akademis yang memadukan implementasi teknis dan analisis keamanan terhadap desain pertahanan berlapis pada router MikroTik, khususnya melalui kombinasi *port knocking* dan *scripting* otomatis

berbasis *alerting*. Temuan ini dapat menjadi dasar pengembangan penelitian lanjutan di bidang keamanan jaringan berbiaya rendah, terutama dalam konteks mitigasi serangan *brute force* terhadap layanan manajemen perangkat.

2. Bagi Institusi Pendidikan Tinggi

   Hasil penelitian memberikan kerangka kerja teruji untuk integrasi prinsip keamanan adaptif ke dalam kurikulum jaringan komputer, khususnya dalam praktikum berbasis MikroTik. Desain yang dihasilkan, lengkap dengan mekanisme deteksi, respons otomatis, dan notifikasi *real-time*, dapat diadopsi sebagai bahan ajar untuk memperkuat kompetensi mahasiswa dalam merancang sistem keamanan jaringan yang proaktif dan berbasis ancaman nyata.

3. Bagi Masyarakat

   Penelitian ini menawarkan solusi keamanan jaringan yang efisien, terjangkau, dan dapat di replikasi oleh administrator jaringan dengan sumber daya terbatas. Dengan memanfaatkan fitur bawaan RouterOS dan integrasi notifikasi berbasis Telegram, metode ini memungkinkan respons insiden yang cepat tanpa bergantung pada perangkat atau lisensi pihak ketiga, sehingga mendorong adopsi praktik keamanan siber yang realistis di lingkungan UMKM, pendidikan, atau infrastruktur lokal.